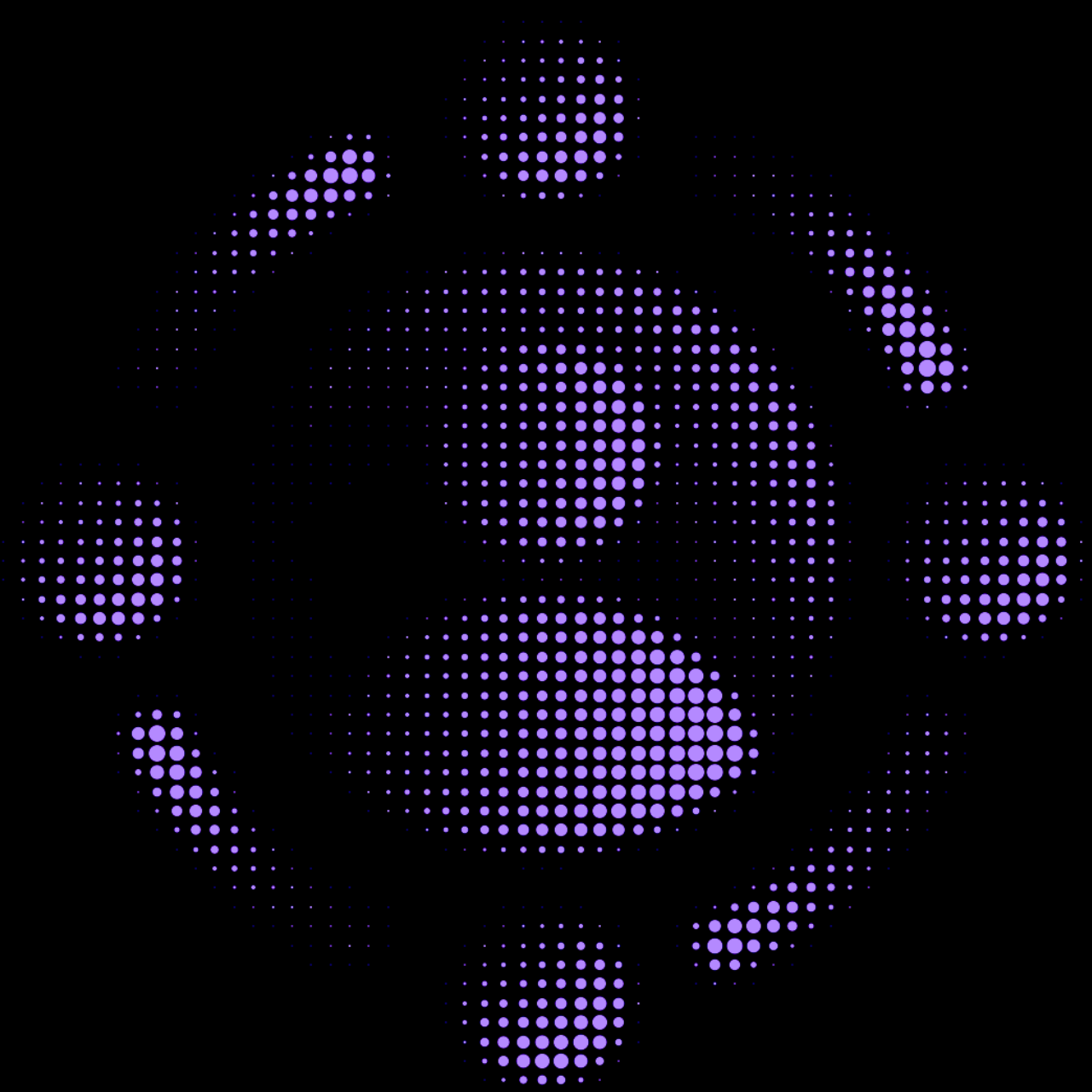


Should Govt Issued IDs be Decentralized?

A Primer

Government IDs verify identities but face challenges. Decentralized Identity offers control, reshaping how IDs impact individuals, governments, and society. Understanding its advantages is crucial for navigating this paradigm shift.



WHAT'S INSIDE!

- | | |
|---|--|
| 1 Decentralized vs Centralized Identity for Govts | 2 Identity credential Issuing process of governments today |
| 3 Government functions & decentralized identity suitability | 4 Decentralized identity long-term outcome |

Decentralized vs Centralized Identity for Govts

Decentralization of government-issued IDs is a complex issue with potential benefits and drawbacks.

On the one hand, decentralization could help address privacy and security concerns. Giving individuals more control over their data and identity could avoid data breaches, hacking, and other cybercrimes. Also, governments are the largest trustable identity credential provider in the world, making them the key player with the possibility to make this the next evolution in Identity Management:

- According to the World Bank, as of 2017, there were an estimated 7.6 billion people worldwide. Of those, 5.9 billion had a government-issued ID card. This means governments are responsible for issuing IDs for over 78% of the world's population.
- In the United States, the Social Security Administration (SSA) is the primary issuer of government-issued IDs. As of 2022, the SSA has issued over 450 million Social Security cards.

- In India, the Unique Identification Authority of India (UIDAI) is the primary issuer of government-issued IDs. As of 2022, UIDAI has issued over 1.3 billion Aadhaar cards.
- In China, the Ministry of Public Security (MPS) is the primary issuer of government-issued IDs. As of 2022, the MPS has issued over 1.4 billion ID cards.

On the other hand, decentralization could pose challenges for law enforcement and other government agencies that rely on centralized databases to verify identity and prevent fraud. It could also lead to inconsistencies in identification standards and create difficulties in cross-border identification and verification.

Whether government-issued IDs should be decentralized depends on many factors, including the specific needs and priorities of the country in question, the state of its technological infrastructure, and the potential risks and benefits of such a shift.

Any decisions regarding decentralization should be carefully considered and implemented with caution to ensure that they do not compromise citizens' security or privacy or undermine government programs' effectiveness.

What is a Credential?

A credential is an information, whether in digital or non-digital form, used to establish and verify an individual's identity, qualifications, or authorization. It serves as evidence or proof that allows one to authenticate the holder's identity or gain access to specific resources, systems, or privileges. Credentials can be digital in the form of usernames and passwords, digital certificates, and biometric data. While traditionally, credentials existed in physical documents like identification cards or licenses, badges, and tokens. In the case of a decentralized Identity system, the next evolution is verifiable credentials.

SECTION 02

Identity Credential Issuing Process of Governments Today

Government-issued credentials provide a foundation for identity management, qualification validation, and regulatory compliance, facilitating interactions between individuals, organizations, and the government.

Governments issue credentials (commonly referred to as ID) in a variety of ways, but the most common process is as follows:

- The applicant provides proof of identity, such as a birth certificate, passport, or other government-issued document (if available)
- Govt authority takes Biometrics information.
- A government official verifies the applicant's data.
- The applicant is issued an ID card or other form of identification.

The different types of IDs that governments issue vary from country to country. However, some of the most common types of IDs include:

- Driver's licenses
- Passports
- National ID cards

- Voter registration cards
- Social security cards

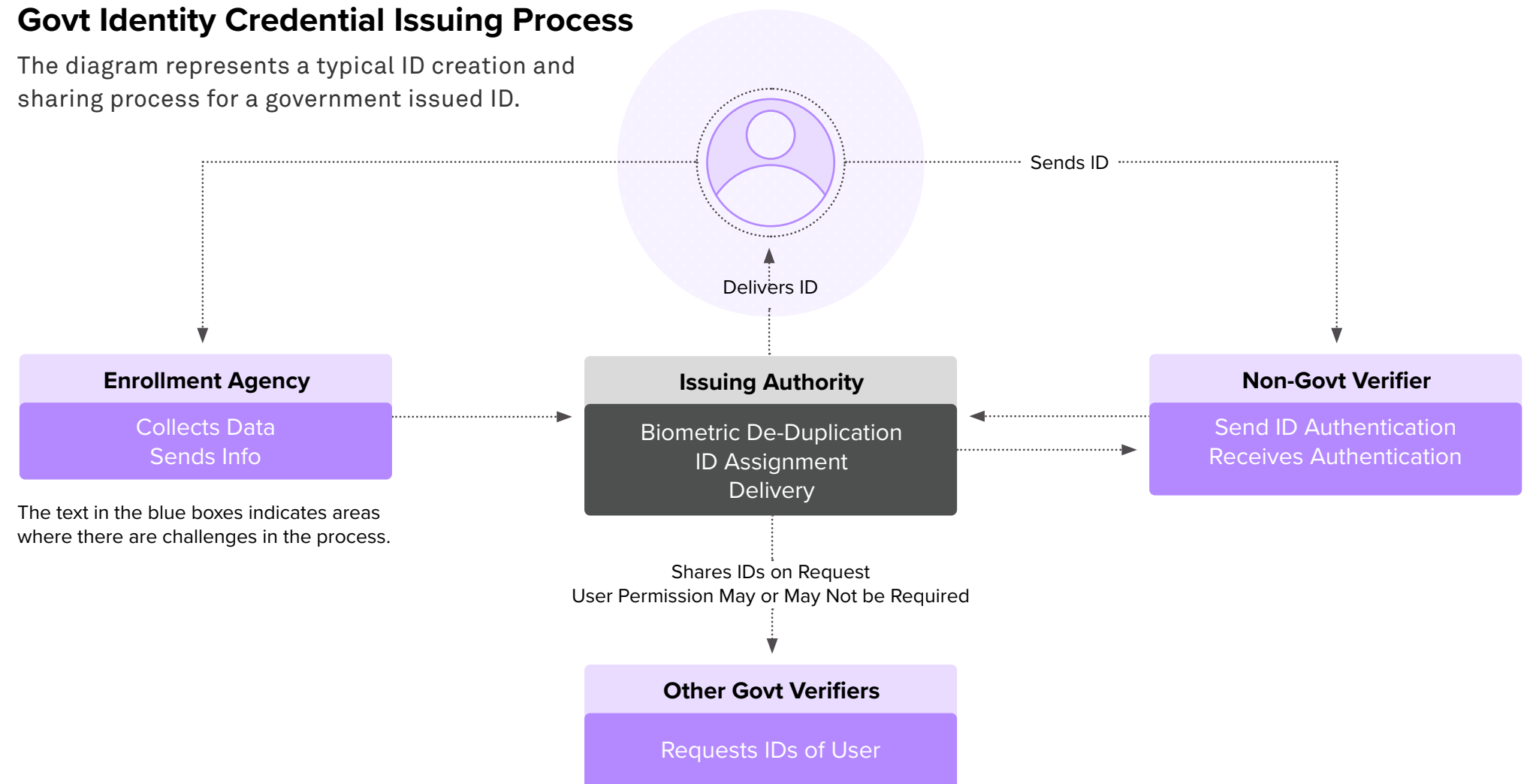
IDs issued by governments are, in turn, used in a

variety of situations and by a variety of entities that include:

- Banks & Financial Institutions
- Airports

Govt Identity Credential Issuing Process

The diagram represents a typical ID creation and sharing process for a government issued ID.



The text in the blue boxes indicates areas where there are challenges in the process.

- Road & Rail Travel
- Educational Institutions
- Hotels and for other residential stay verification

Here are some of the challenges with the current process of how governments issue IDs:

Susceptible to Forgery

Traditional systems often rely on physical documents, such as passports or driver's licenses, which can be counterfeited or altered. These documents may lack robust security features, making them susceptible to duplication.

Verification Infrastructure

Current Identity system verification of a user requires a dedicated technology infrastructure and process to ensure the right user has access to eligible services.

Data Silos & Lack of Interoperability

The current process of issuing IDs often results in data silos, which are separate databases containing different information about a person. This reduces the operational efficiency across the processes due to the limitation of interoperability, as most times same information would be required to be stored in multiple data silos.

All or None

It is currently not possible to share partial information related to the government ID. E.g., a user may want to share only the age details with a liquor store or for watching a movie. But a govt issued id would have other details, such as DOB or address, which are unnecessary for the transaction.

Decentralized Identity can help to solve some of these challenges by:

Decentralizing Control

Decentralized Identity functions on the principles of a decentralized ledger. This means that no single entity controls a person's credentials, and cannot be hacked or stolen.

Eliminating Data Silos

In the case of a decentralized identity system, the sensitive information about the user is stored in the user's wallet, with complete control of data sharing being self-sovereign. It eliminates the data silos that need to be maintained across multiple processes, in turn increasing operational efficiency by facilitating interoperability.

Making IDs Portable

It can port a person's identity from one service to

another, making it easier for people to use their IDs online, and it can also make it easier for people to move from one country to another.

Share Only Partial Information as Required

The ability of selective disclosure can be built into the system, which allows the user to choose what information is allowed to be shared from a pool of information associated with an issued ID.

Overall, it could revolutionize how governments issue and manage IDs. Implementation would result in governments improving security, reducing fraud, increasing convenience, and increasing privacy.

However, the challenge is that governments require a certain amount of surveillance, especially in National security, distribution of services, and law and order. Therefore, it is important to identify which government functions would benefit from using a Decentralized Identity System and which others may require a tweak to an ideal version of Decentralized ID.

Government Functions & Decentralized Identity Suitability

Govts have centralized administration functions with multiple branches and functions reporting to them. While the transactional efficiency of a decentralized identity system is far superior, along with the benefits of data security and privacy, the benefit of technology will vary from one function to another. The suitability factor can be viewed on the matrix of Need for Scrutiny vs. Complexity of the process shown in the figure.

Education & Skill Certification

Each university and vocational institute in the country needs affiliation to provide a govt approved Skill certification to be used by the user for occupational purposes. The Education function would be one of the ideal use cases for Decentralized Identity implementation, as the function lies in the ideal state of low complexity and coordination combined with a low Need for Scrutiny. The institute can provide the User/candidate a Verifiable credential of the degree/diploma/certificate as proof of skill which can be

verified by any hiring organization with instant authentication. At the same time, preserving users' privacy and keeping them in control of their data.

Elections

With the rise of distrust in the election process across major democracies, as per the YouGov/Economist poll of May '22, ~40% of surveyed US citizens did not have confidence in the legitimacy of the last presidential election. Decentralized Identity has the potential to provide the elections with the integrity it needs by allowing individuals to verify their own identities and ensure that their votes are counted accurately. However, a centralized identity system does provide greater consistency and standardization in voter registration and verification. An ideal solution would require a hybrid approach incorporating privacy-imbibed voter confidence, standardization, and process transformation to ensure all eligible voters can participate.

Law Enforcement / National Security

Law enforcement and national security agencies often rely on centralized identity systems allowing government agencies to verify identities, monitor potential security threats more effectively, and prevent fraud. A centralized identity system could provide a clear chain of command and hierarchy, making it easier for these agencies to identify and address security threats. As this function needs high scrutiny, a decentralized identity here will make law enforcement more difficult. It will make accessing and verifying identity information difficult to prevent fraud.

Immigration

Immigration is a closely linked function to national security and relief and benefits, creating a balance between the need for a private and efficient system and the need to ensure a certain level of centralization to ensure national security. A centralized identity system would provide greater consistency and standardization in immigration

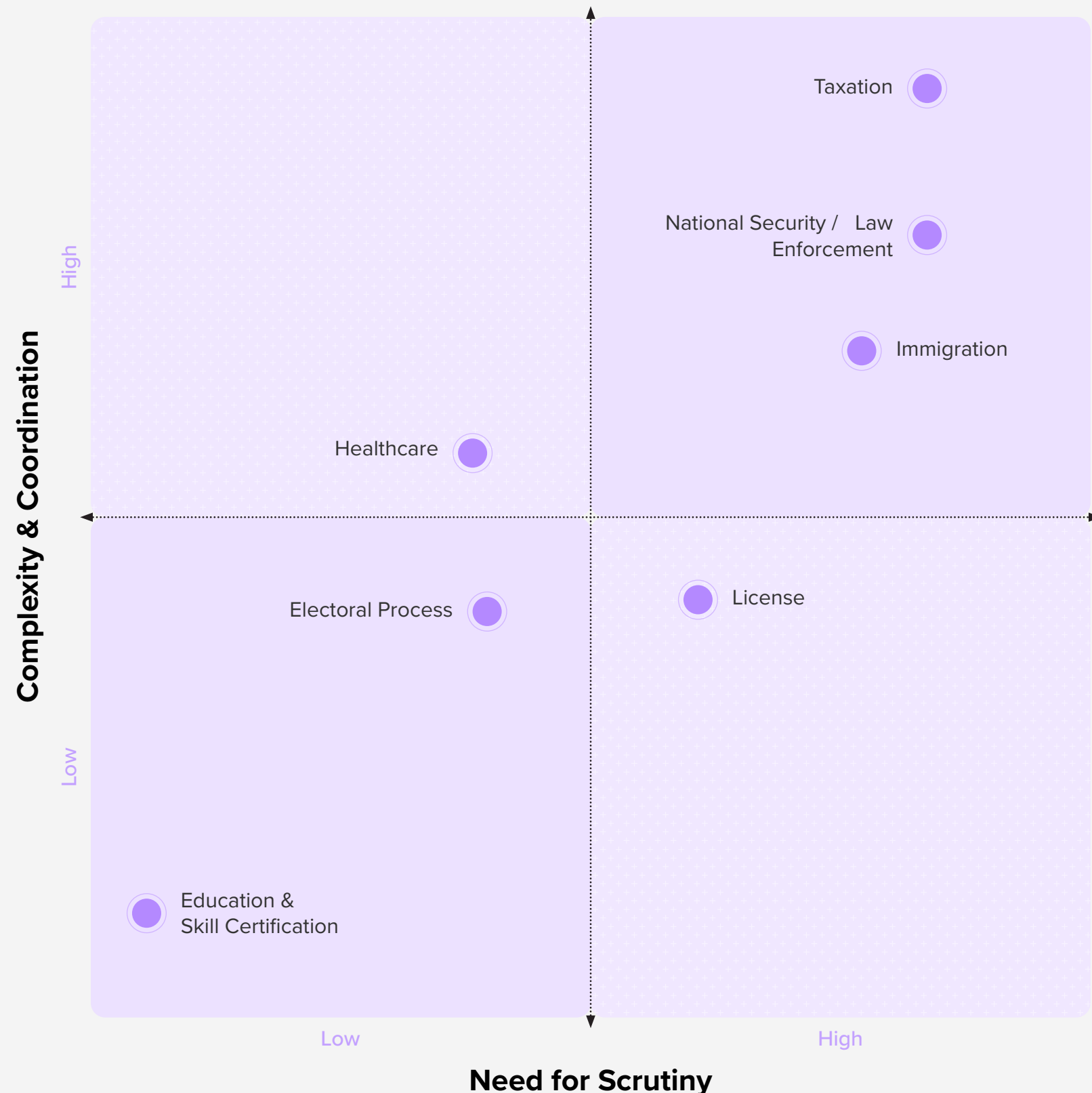
In the U.S., healthcare Billing and Insurance-Related (BIR) expenses are \$496 billion yearly; National Academy of Medicine (NAM) estimates half could be saved with efficient systems.

documentation and verification, making it easier for immigration agencies to process applications and ensure all applicants meet the requirements.

Healthcare

In healthcare, decentralized identity could help protect patients' privacy and improve accessibility by allowing individuals to access and control their medical records. However, a decentralized identity system would require the implementation of certain standardization in medical records to make it easier for healthcare providers to access and share information across different systems and jurisdictions. A more detailed use case in healthcare is covered in another Decentralized Identity use case document by Lab45.

Govt Functions and DID Suitability



Functions low on the need for Scrutiny scale are better fits for DID

Taxation

The taxation function is a complex network where banking and all financial services are linked with taxation IDs like PAN (Permanent Account Number), creating a paper trail of everyone to ensure accurate taxation and user accountability. While a Decentralized Identity System can make the verification process a lot more efficient while preserving the user's financial information, it also disables the tax authorities from accessing those records. Hence, a centralized identity system could provide greater consistency and standardization in taxation documentation and verification, making it easier for tax agencies to process returns and ensure that all taxpayers meet their obligations.

Licenses

Licensing as a function can be viewed in multiple domains, from business licenses giving them accessibility to a nation's market, to licenses to operate machinery and recreational licenses like a fishing license in some constituencies. In all cases, licenses are proof of eligibility to access certain abilities and services. Decentralized Identity would be able to provide a viable solution where post the completion of required criteria,

an individual or entity can be granted a license as a Verifiable credential, ensuring only valid and authorized users have access to those services. While the information is sensitive and user privacy is important in certain cases, it does require a certain level of scrutiny, e.g., traffic violations associated with a driver's license. A transformed process would require to include the best of both worlds for an ideal solution.

Is Decentralized Identity Suitable for all Forms of Governments?

From an authoritarian state to a direct democracy, the functions follow a comparable process with certain policy differences, irrespective of the form of government. What would make a Decentralized Identity System a viable solution would be primarily based on the Scrutiny requirements as stated by the policies. While the solution suitability will be more function-specific, direct democracies like Switzerland could utilize the benefits of Decentralized Identity in the shorter term than others. Switzerland enables its citizens the power to participate in decision-making through referendums and popular initiatives. This means that citizens can propose new laws or changes to existing ones, which are then voted on by the population. These votes happen about five times a year. A decentralized Identity solution would make this referendum voting process very efficient with an instant and reliable verification process.

Decentralized Identity Long-Term Outcome

The digitization of public services has made verifying identity and personal information increasingly important to access benefits and services. Some governments have implemented digital driver's licenses and similar solutions for verifying basic details like contact information and date of birth. Scalability and adaptability to evolving digital identities are necessary for truly valuable solutions.

Scalability is Paramount

Government interactions require individuals to verify various details beyond their name and date of birth. For example, income verification for nutrition benefits, license validation for business owners, and lead paint inspection validation for landlords. Furthermore, digital identities and associated information will keep evolving. Credentials like medical marijuana licenses, vaccine cards, or TSA Pre-Check status have emerged in the past two decades. Decentralized Identity solutions need to be scalable and interoperable to cater to these changes.

Ensuring Equity

Decentralized Identity solutions offer improved security, data privacy, and the potential to promote equity and accessibility for all residents.

Many individuals who require government services face significant challenges in providing proof of identity, with about 22% of the population in the world (World Bank Report) lacking any form of government-issued ID. Physical documents like birth certificates or social security cards are also susceptible to loss or damage. Paired with the tedious process of existing identity verification processes that operate independently, burdening individuals with job constraints, physical limitations, or limited access to transportation. Decentralized identity solutions can address these barriers, ensuring privacy and data security while eliminating access obstacles.

Restoring Trust in Government

Public trust in the current system for their control over their data is dramatically low. Pew Research reports that 80% of Americans feel a

lack of control over their data collected by public institutions or private companies. However, Decentralized Identity solutions grant residents full ownership and control over their data. Access can be revoked, and verification happens through a public ledger, allowing proof without revealing sensitive information. Decentralized Identity solutions can rebuild trust in public institutions by empowering residents with data control.

Authors@lab45

Abhigyan Malik 

Sujay Shivram 



Ambitions Realized.

Wipro Limited

Doddakannelli
Sarjapur Road
Bengaluru – 560 035
India

Tel: +91 (80) 2844 0011

Fax: +91 (80) 2844 0256

wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading technology services and consulting company focused on building innovative solutions that address clients' most complex digital transformation needs. Leveraging our holistic portfolio of capabilities in consulting, design, engineering, and operations, we help clients realize their boldest ambitions and build future-ready, sustainable businesses. With over 250,000 employees and business partners across 66 countries, we deliver, on the promise of helping our customers, colleagues, and communities thrive in an ever-changing world.

For more information, please write to us at info@wipro.com