INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES
HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2222-6990

National Digital Identity: Current Landscape, Emerging Technologies and Future Directions

Faiz Zulkifli, Rozaimah Zainal Abidin, Mohamed Imran Mohamed Ariff, Nahdatul Akma Ahmad, Noreen Izza Arshad, Usman Ependi, Mohamad Sharmizi Ab Razak

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v13-i3/16603 DOI:10.6007/IJARBSS/v13-i3/16603

Received: *09* January 2023, ***Revised:*** *12* February 2023, ***Accepted:*** *26* February 2023

Published Online: *01* March 2023

In-Text Citation: (Zulkifli et al., 2023)

To Cite this Article: Zulkifli, F., Abidin, R. Z., Ariff, M. I. M., Ahmad, N. A., Arshad, N. I., Ependi, U., & Razak, M. S. A. (2023). National Digital Identity: Current Landscape, Emerging Technologies and Future Directions. *International Journal of Academic Research in Business and Social Sciences*, *13*(3), 1225 – 1242.

Vol. 13, No. 3, 2023, Pg. 1225 – 1242

http://hrmars.com/index.php/pages/detail/IJARBSS | **JOURNAL HOMEPAGE**

Full Terms & Conditions of access and use can be found at
http://hrmars.com/index.php/pages/detail/publication-ethics

INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES
HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2222-6990

National Digital Identity: Current Landscape, Emerging Technologies and Future Directions

Faiz Zulkifli, Rozaimah Zainal Abidin
College of Computing, Informatics, and Media Universiti Teknologi MARA, Perak Branch, Tapah Campus, 35400 Tapah Road, Perak Malaysia

Mohamed Imran Mohamed Ariff, Nahdatul Akma Ahmad
College of Computing, Informatics, and Media Universiti Teknologi MARA, Perak Branch, Tapah Campus, 35400 Tapah Road, Perak Malaysia

Noreen Izza Arshad
Department of Computer and Information Sciences Faculty of Science and Information Technology Universiti Teknologi Petronas, Seri Iskandar, Perak Malaysia

Usman Ependi
Universitas Bina Darma, Jl. A Yani No. 3 Seberang Ulu I, Palembang, Indonesia 30264

Mohamad Sharmizi Ab Razak
TM Bhd, Jalan Stesyen, 35400 Tapah Road, Perak Malaysia

Abstract
The proliferation of digital services has led to an increasing demand for secure and reliable digital identity verification, resulting in the development of national digital identity (NDI) systems. These systems provide individuals with a trusted method of verifying their online identity, a necessary prerequisite for accessing a wide range of services, such as banking, healthcare and government services. This review paper takes an in-depth look at the evolution of NDI systems and the advanced technologies that have improved their security and reliability. It looks at the notable NDI systems and digital identity programmes that have been introduced in different countries and analyses both their successes and limitations. In addition, the paper examines emerging technologies such as blockchain and their potential impact on NDI systems. Based on the assessment of these systems and technologies, practical recommendations and best practises are provided for the future development and implementation of NDI systems in other countries.
Keywords: National Digital Identity, Digital Identity, Digital Identity Verification, Biometrics, Blockchain.

Introduction

The development of National Digital Identity (NDI) systems has attracted significant attention worldwide as governments have recognised the need for secure, reliable and efficient online identity verification for various transactions. NDI systems provide a government-issued digital identity representation that allows individuals to securely verify their identity online (Hilowle et al., 2022). With the increasing use of digital services, the need for a trusted digital identity has become paramount. Therefore, this review paper aims to provide a comprehensive analysis of NDI or digital identity (DI), focusing on its history, benefits, challenges and possible future developments.

This study is important because it highlights the importance of the need for secure digital identity verification, which is essential for accessing a range of services, including banking, healthcare and government services. In addition, the study highlights the need for a user-centric approach that focuses on ease of use and convenience, while ensuring that privacy and security remain paramount. It also sheds light on the potential of NDI systems to reduce fraud and exclusion of people who do not have access to digital technologies or have limited digital skills. The findings of this study can be of great importance to policymakers, technology providers, data protectors and civil society organisations in their efforts to improve the usefulness and effectiveness of NDI systems.

This paper first examines the evolution of DI systems, from the earliest attempts to the most current solutions. It analyses the benefits of DI, such as increased security, privacy and efficiency in digital transactions, and the challenges of implementing DI systems, including privacy and interoperability issues.

In addition, the paper analyses case studies of countries that have implemented NDI or DI systems, including India's Aadhaar programme, Estonia's e-Residency programme and Singapore's SingPass system. It examines the successes and failures of these systems and explores how they can guide the design and implementation of DI systems in other countries.

Finally, it explores possible future developments in the field of DI, including emerging technologies such as blockchain and biometrics, and their potential impact on DI systems. This comprehensive analysis of DI is intended to inform policy makers, researchers and practitioners working in the field of DI verification. Based on these findings, it is suggested that governments and organisations looking to implement NDI systems should take a user-centred approach, focusing on ease of use and convenience, while ensuring that privacy and security are paramount. Collaboration with stakeholders such as technology providers, data privacy advocates and civil society organisations can also improve the effectiveness and transparency of NDI systems.

An Overview of the Development of NDI

The development of NDI systems has been driven by the increasing need for secure and reliable digital identity verification as the use of digital services becomes more widespread. NDI systems provide individuals with a secure way to verify their identity online, which is essential for accessing various services such as banking, health and government services. This has been highlighted in recent studies (Mentasti, 2022; Udwan et al., 2020; Rim, 2022). Initially, most NDI systems were based on usernames and passwords, but as security threats have increased, the use of biometrics and other advanced technologies has become prevalent

(Mahula et al., 2021). For example, facial recognition, fingerprints and iris scans are used in some NDI systems to verify identity.

Estonian e-Residency, launched in 2014, is one of the earliest and best-known NDI schemes that provides non-residents with a secure digital identity to access Estonian e-services, including banking and business registration. This programme has successfully attracted entrepreneurs and businesses from around the world to use Estonia's advanced digital infrastructure (Tammpuu & Masso, 2019). Similarly, India's Aadhaar programme, launched in 2009, assigns a unique 12-digit identity number to each resident of India and uses biometrics to verify identity, including fingerprints and iris scans. The programme is widely used to access various government services and has been praised for reducing fraud and corruption (Chowdhry et al., 2021). Other countries have also implemented NDI or digital identity schemes to varying degrees, as described in Appendix A.

In summary, the evolution of NDI systems is characterised by a shift towards more secure and reliable digital identity verification, with a focus on improving user experience and convenience, while privacy and security remain paramount. To achieve this, governments and organisations looking to implement NDI systems should prioritise a user-centred approach, collaborate with stakeholders such as technology providers, privacy advocates and civil society organisations, and continuously develop and update their systems to address new security threats and meet the changing needs of their users.

NDI and Its Advantages

Various countries around the world have adopted NDI systems, which offer numerous benefits, such as enhanced data protection, greater security and more efficient digital transactions. According to Beduschi (2019), NDI provides a secure and reliable way for individuals to prove and authenticate their identity online. It also reduces identity fraud by securely identifying individuals (Makarim & Kom, 2020). In Germany, the identity card offers a digital signature that verifies the authenticity of electronic documents, reducing fraudulent activity (Sobczak, 2013). Itsme in Belgium offers two-factor authentication, ensuring that only authorised people can access their personal accounts (Mahula et al., 2021).

Furthermore, NDI strengthens privacy by giving individuals control over their personal data and the ability to decide who can access it. Estonia's e-Residency provides individuals with a digital identity that allows them to sign documents and conduct business online without revealing their physical location or citizenship (Tammpuu & Masso, 2019). Similarly, in Peru, the Documento Nacional de Identidad (DNI) provides a unique identification number that can be used to access government services and benefits, while protecting personal information from disclosure to unauthorised parties (Sen, 2019).

NDI systems also enable more efficient digital transactions, allowing individuals to access online services and conduct transactions without having to physically identify themselves. In Singapore, SingPass provides access to more than 1,000 government services and allows individuals to transact with the government quickly and easily (World Bank, 2022). In Canada, SecureKey Concierge allows access to multiple government services with a single login, making it easier to get the services you need (Boysen, 2021).

In addition, NDIs offer greater convenience and accessibility for citizens, allowing them to access a wide range of government and private services from anywhere in the world without the need for physical documents or face-to-face interactions (Kirilova & Naydenov, 2021; Abesamis & Caramancion, 2022). They also have the potential to promote financial

inclusion, especially in developing countries where large numbers of people do not have access to traditional forms of identification (Mentasti, 2022).

NDIs can also improve the efficiency and effectiveness of public services such as healthcare, education and social care. In Estonia, for example, the e-Residency programme enables non-Estonians to set up and manage businesses in Estonia entirely online, while in India the Aadhaar system is used to distribute government benefits to eligible citizens more efficiently and with less fraud (Tammpuu & Masso, 2019; Chowdhry et al., 2021).

Furthermore, NDIs can promote greater transparency and accountability in government by enabling more accurate and reliable data collection and analysis (Third et al., 2018). By providing a consistent and standardised means of identity verification, NDIs can help governments better understand the needs and preferences of their citizens and make more informed public policy decisions.

In summary, NDIs offer a range of benefits that are diverse and far-reaching. They have the potential to change the way governments and citizens interact with each other and the world around them.

Challenges in NDI Implementation

The implementation of NDI systems is fraught with various challenges that can affect the effectiveness, usability and security of the system. One of the biggest challenges is ensuring the security and privacy of personal data (Beduschi, 2019). Hackers and cybercriminals are always on the lookout for ways to exploit security vulnerabilities to access sensitive information. For example, in 2018, Estonia's digital system ID was found to have a vulnerability that could allow hackers to steal users' identities. The vulnerability could have affected over 760,000 ID cards issued since 2014 (Tammpuu & Masso, 2019).

Another challenge is the potential exclusion of people who do not have access to digital technologies or have limited digital skills (Cuadrado & Levratto, 2021). In India, for example, many people, especially in rural areas, do not have access to the internet or smartphones, making it difficult for them to participate in the digital economy (Chowdhry et al., 2021). This exclusion could lead to inequality and further marginalise these people.

In addition, the adoption of DI systems requires significant financial investment in infrastructure and training, which can be challenging for countries with limited financial resources (Mentasti, 2022). In Peru, for example, the cost of implementing the national DI system was estimated at $58 million (Sen, 2019).

In addition, standardisation and interoperability of DI systems in different countries can be challenging. Different countries have different legal frameworks, technological infrastructures and cultural practises that can affect the implementation of DI systems (Sullivan, 2018). For example, although the EU has developed a common standard for electronic identification (eID), there is still a lack of interoperability between eID systems in different countries (Andersen, 2021). This lack of interoperability can hinder cross-border transactions and limit the potential benefits of DI 's systems.

In addition to the challenges already mentioned, the implementation of DI systems also faces several other challenges. One of these challenges is ensuring accessibility and inclusion of all members of society, especially marginalised and vulnerable populations (Mentasti, 2022). This includes addressing issues such as language barriers, access to technology and cultural issues.

Another challenge is ensuring interoperability and compatibility between different systems and across different jurisdictions (Sen, 2019). In a globalised world, individuals may

need to authenticate their identities across borders and use different identity systems, which can pose technical and legal challenges.

Next, DI systems need to be developed with a strong focus on protecting users' privacy and data (Andersen, 2021). This includes implementing robust security measures such as encryption and secure data storage, as well as developing clear policies and protocols for handling and accessing data.

Finally, it is critical to ensure public trust in DI systems (Jackson et al., 2019). This can be achieved through transparent and accountable governance structures, meaningful stakeholder engagement and effective communication strategies to raise awareness and educate the public about the benefits and risks of DI.

NDI Case Studies: Successes and Failures

The implementation of NDI systems is of great interest to governments worldwide. Many countries have introduced NDI systems with varying degrees of success. One such country is Estonia, which introduced the e-Residency programme in 2014. The programme allows anyone in the world to apply for a DI and access Estonia's e-services remotely. The programme has been successful, with over 80,000 people from 170 countries registering for e-Residency by 2021. One of the main reasons for the success of the e-Residency programme is the focus on digitalisation and the use of advanced technologies to provide seamless and secure services to citizens (Tammpuu & Masso, 2019).

Similarly, South Korea's MyNumber system has also been successful. The system provides each citizen with a single, unique identification number that is used for various government and private sector services (Rim, 2022). The MyNumber system has been praised for its ease of use and for significantly reducing the time and cost of accessing government services. Another successful example is the SingPass system in Singapore, which provides access to more than 1,200 government services, including tax returns and health services. The system has been successful because of its ease of use and high security standards (World Bank, 2022).

However, there have also been failures in implementing NDI systems. One example is India's Aadhaar system, which has been criticised for its lack of transparency and privacy concerns (Chowdhry et al., 2021). The system was originally introduced to give each citizen a unique identification number, but it has been plagued by problems such as data breaches and privacy violations. The Aadhaar system has highlighted the importance of building trust and transparency into NDI systems and ensuring that citizens have control over their personal data.

Another example is the UK's Verify system, which was introduced in 2016 to enable access to government services (Harbinja, 2017). The system struggled with several issues, including low adoption rates and concerns about the security of personal data. The Verify system demonstrates the importance of NDI systems being user-friendly and citizens having confidence in the security of their personal data.

These case studies provide valuable insights into the successes and failures of DI's systems and can inform the design and implementation of NDI systems in other countries. Successful systems prioritise security and privacy while providing a user-friendly and convenient way for citizens to access government services. It is important to consider privacy and data accessibility concerns, especially for marginalised populations who may find access difficult. In addition, systems that are too complicated or too expensive may not be sustainable in the long run. By learning from these case studies, other countries can develop

effective and sustainable NDI systems that promote digital transformation and improve access to government services for all citizens. Appendix A also provides a summary of the other case countries.

What's Next for NDI?

The field of NDI is evolving rapidly, and new technologies such as blockchain and biometrics are playing an important role in shaping the future of these systems. Blockchain technology, for example, could provide a secure and decentralised platform for storing and sharing personal information, making NDI systems more transparent, efficient and resilient to cyberattacks (Mahula et al., 2021). Biometric authentication, on the other hand, could improve the accuracy and convenience of identity verification by using features such as fingerprints, facial recognition or iris scans. However, these technologies also raise important privacy, security and data protection issues that need to be addressed through robust legal frameworks, technical standards and governance mechanisms.

In addition to blockchain and biometrics, there are several other potential future developments in the field of NDI. One of these is the use of artificial intelligence (AI) and machine learning (ML) to improve the performance and security of NDI systems (Mir et al., 2022). AI and ML can help detect and prevent fraud, automate verification processes and provide a more personalised user experience.

Another potential development is the use of decentralised identity systems (DID) (Rim, 2022). DID Systems allow individuals to control their identity and personal data and share certain information with authorised parties while maintaining control over their data. DID Systems can potentially improve privacy and security in NDI systems.

The development of Internet of Things (IoT) devices and their integration into NDI systems is another potential future development. The integration of IoT devices can enable seamless and secure authentication and authorisation processes, creating a more efficient and user-friendly experience for individuals.

Finally, the introduction of global NDI standards and interoperability between different NDI systems is another possible future development. The introduction of standards and interoperability can help to increase security, reduce fraud and promote the cross-border use of NDI systems.

Furthermore, integrating new technologies into NDI systems requires significant investment, expertise and collaboration between governments, the private sector and civil society. It is therefore important to carefully weigh the potential benefits and risks of these developments and ensure that they serve the needs and interests of all citizens, including marginalised and vulnerable groups.

Conclusion

In summary, NDI systems have become an important tool for governments to enable secure and efficient digital transactions while enhancing the privacy and security of their citizens. Our review of case studies from around the world shows that NDI systems in various forms have been successfully implemented in several countries, with varying degrees of success and challenges.

Countries such as Estonia, the Netherlands and New Zealand have had great success with their NDI systems, which can provide secure and efficient digital services to their citizens. However, some countries have encountered challenges with their NDI systems, such as

privacy concerns and data breaches. Nonetheless, many countries continue to strive to improve their NDI systems and overcome these challenges.

In addition, new technologies such as blockchain and biometrics hold immense potential for further improving NDI systems. Blockchain technology can provide secure and decentralised storage of identity data, while biometric authentication methods such as facial recognition and fingerprint scanning can improve security and the user experience. However, challenges remain in terms of data protection and standardisation of these technologies across different systems and countries.

Based on the findings of this review, we recommend that governments and organisations intending to implement NDI systems should prioritise a user-centred approach. This approach should prioritise usability and convenience while ensuring that privacy and security are paramount. In addition, effective collaboration with stakeholders such as technology providers, privacy advocates and civil society organisations can help increase the efficiency and transparency of NDI systems. Such collaboration can help overcome the challenges of implementing NDI systems and increase public trust in them.

Furthermore, it is crucial that NDI systems are interoperable across different systems and countries to enable seamless and secure cross-border transactions. To achieve this, standardisation of identity data formats and authentication protocols is required.

Overall, NDI systems hold immense potential to enable secure and efficient digital transactions while enhancing the privacy and security of citizens. However, careful consideration of privacy and security concerns and collaboration with stakeholders are essential for the successful development and implementation of these systems.

Acknowledgement

We would like to express our sincere gratitude to MCMC (Malaysian Communications and Multimedia Commission) for providing us with the Digital Society Research Grant 2022, Cycle 2 under the RMC file no. 100-TNCP/GOV 16/6/2 (070/2022). This funding has been instrumental in supporting our research efforts and facilitating the completion of our project. We would also like to thank Universiti Teknologi MARA (UiTM) for providing the necessary resources and facilities for this study.

Corresponding Author

Rozaimah Zainal Abidin

College of Computing, Informatics, and Media, Universiti Teknologi MARA, Perak Branch, Tapah Campus, 35400 Tapah Road, Perak, Malaysia

Email: faiz7458@uitm.edu.my.

References

Abesamis, P. P. R., & Caramancion, K. M. (2022). Multiple-Case Study on the Perceived Impacts of Philippine Identification System in Organizational Control: Focusing on E-government Services. In *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance* (pp. 279-287).

Aksar, I. A., Firdaus, A., & Pasha, S. A. (2023). Virtual vs. Real Self: Gendered Presentation and Everyday Performance of Virtual Selfhood–A Case Study of Pakistan. *Journal of Communication Inquiry*, *47*(1), 84-114.

Andersen, M. S. (2021). Towards the Design of a Privacy-preserving Attribute Based Credentials-based Digital ID in Denmark–usefulness, Barriers, and Recommendations.

In *Proceedings of the 16th International Conference on Availability, Reliability and Security* (pp. 1-8).

Arunwatanamongkol, P., Nupairoj, N., & Tanlamai, U. (2021). Innovative Delegation Application in Thai National Digital Identity Platform. *International Journal of Interactive Mobile Technologies*, *15*(14).

Australian Productivity Commission and New Zealand Productivity Commission (2019). *Growing the digital economy in Australia and New Zealand: maximising opportunities for SMEs*. Productivity Commission.

Beduschi, A. (2019). Digital Identity: Contemporary Challenges for Data Protection, Privacy and Non-discrimination Rights. *Big Data & Society*, *6*(2), 2053951719855091.

Boysen, A. (2021). Decentralized, Self-sovereign, Consortium: the Future of Digital Identity in Canada. *Frontiers in Blockchain*, 11.

Buccafurri, F., Fotia, L., Lax, G., & Mammoliti, R. (2015). Enhancing Public Digital Identity System (Spid) to Prevent Information Leakage. In *Electronic Government and the Information Systems Perspective: 4th International Conference, EGOVIS 2015, Valencia, Spain, September 1–3, 2015, Proceedings 4* (pp. 57-70). Springer International Publishing.

Chowdhry, B., Goyal, A., & Ahmed, S. A. (2021). Digital Identity in India. *The Palgrave handbook of technological finance*, 837-853.

Cuadrado, R. A., & Levratto, V. (2021). La Construcción De La Identidad Digital en Las Redes Sociales: Un Estudio Cuantitativo en Argentina Y España: La Imagen Como Elemento Determinante en La Identidad Y Acción Digital. *Revista Latinoamericana de Estudios sobre Cuerpos, Emociones y Sociedad*, (36), 23-32.

Duffy, K., Goudovitch, P., & Fedorov, P. (2016). The Application of Digital Identity in the United States. *Recuperado de https://static1. squarespace. com/static/59aae5e9a803bb10bedeb03e*, *5*, 1517277404196.

Gunnlaugsson, H., & Jonasson, J. O. (2016). Is Digital Crime Victimization Increasing in Iceland–may the Me-too Movement Influence How Victimization is Experienced. *Nordisk Tidsskrift for Kriminalvidenskab*, *107*(1), 24-40.

Harbinja, E. (2017). Digital Inheritance in the United Kingdom. *J. Eur. Consumer & Mkt. L.*, *6*, 253.

Hilowle, M., Yeoh, W., Grobler, M., Pye, G., & Jiang, F. (2022). Users' Adoption of National Digital Identity Systems: Human-Centric Cybersecurity Review. *Journal of Computer Information Systems*, 1-16.

Inal, S. F. M. (2022). Importance of Fintechs in Digital Age for Turkey and the Role of Information Technologies. *Digitalization in Business and Economy*, 53.

Jackson, M., Prego, J., & Hernandez Varela, J. (2019). Building a Framework for Trust Services in Uruguay. In *12th International Conference on Theory and Practice of Electronic Governance (ICEGOV 2019)*.

Kirilova, K., & Naydenov, A. (2021). The State of E-government and Digital Administrative Services in the Republic of Bulgaria. *Busines Management*.

Kostrikova, N. (2021). Assessment of Blockchain Technology Adoption Factors and Scenarios Within the Economy of Latvia. In *Innovations in Smart Cities Applications Volume 4: The Proceedings of the 5th International Conference on Smart City Applications* (pp. 714-729). Springer International Publishing.

Mahula, S., Tan, E., & Crompvoets, J. (2021). With Blockchain or Not? Opportunities and Challenges of Self-sovereign Identity Implementation in Public Administration: Lessons

From the Belgian Case. In *DG. O2021: The 22nd Annual International Conference on Digital Government Research* (pp. 495-504).

Makarim, E., & Kom, S. (2020). Digital Identity and Personal Data Protection: Analysis of Rights to Erasure and Data Portability in Indonesia. In *Advancing Rule of Law in a Global Context* (pp. 247-261). CRC Press.

Mentasti, E. (2022). Digital Identity in Italy: Challenges and Opportunities for the Adoption in Banking, Insurance and Utility Sectors.

Mir, U., Kar, A. K., & Gupta, M. P. (2022). AI-enabled Digital Identity–inputs for Stakeholders and Policymakers. *Journal of Science and Technology Policy Management*, *13*(3), 514-541.

Mooij, A. M. (2023). Reconciling Transparency and Privacy Through the European Digital Identity. *Computer Law & Security Review*, *48*, 105796.

Rim, H. (2022). Decentralized Identity (Did): New Technology Adoption and Diffusion in South Korea. *Transforming Government: People, Process and Policy*, (ahead-of-print).

Sen, S. (2019). A Decade of Aadhaar: Lessons in Implementing a Foundational ID System. *ORF Issue Brief No*, *292*.

Sobczak, A. (2013). *Traditional vs. Virtual Archives-The Evolving Digital Identity of Archives in Germany*. Uniwersytet Szczecinski (Poland).

Sullivan, C. (2018). Digital Identity–from Emergent Legal Concept to New Reality. *Computer Law & Security Review*, *34*(4), 723-731.

Tammpuu, P., & Masso, A. (2019). Transnational Digital Identity as an Instrument for Global Digital Citizenship: the Case of Estonia's E-residency. *Information Systems Frontiers*, *21*, 621-634.

Third, A., Quick, K., Bachler, M., & Domingue, J. (2018). Government Services and Digital Identity. *Knowledge Media Institute of the Open University*.

Udwan, G., Leurs, K., & Alencar, A. (2020). Digital Resilience Tactics of Syrian Refugees in the Netherlands: Social Media for Social Support, Health, and Identity. *Social Media+ Society*, *6*(2), 2056305120915587.

World Bank. (2022). National Digital Identity and Government Data Sharing in Singapore: A Case Study of Singpass and APEX.

Young, A., & Verhulst, S. (2018). Self-Sovereign Identity for Government Services in Zug, Switzerland.

APPENDIX A

No.	Country Name	Year	Programme	Description	Official website	Implementation status
1	Argentina	2016	Mi Argentina	Platform that provides citizens with access to public services and allows them to manage their personal data.	https://www.argentina.gob.ar/miargentina	The system has been successful in providing easy access to services such as health records, driving license renewal, and tax payments. However, there have been some concerns around privacy and security, with reports of data breaches and unauthorized access to personal information (Cuadrado & Levratto, 2021).
2	Austria	2000	Bürgerkarte	Digital ID card that allows citizens to access online services securely and sign documents electronically.	https://www.buergerkarte.at/	The system provides a secure and reliable form of digital identification, with strong encryption and advanced security features. One of the key successes of the system is the integration with a range of government services, including tax payments, social security, and health insurance. However, there have been some challenges around the complexity of the system and the need for ongoing maintenance and updates (Hilowle et al., 2022).
3	Belgium	2017	Itsme	Mobile app that provides secure access to online services and allows users to confirm their identity for online transactions.	https://www.itsme-id.com/	The system has been successful in achieving high levels of adoption, with over 2.7 million registered users to date. Itsme uses a combination of biometric and PIN-based authentication, with strong encryption and privacy protections. However, there have been some concerns around the usability of the system, particularly for older or less tech-savvy users (Mahula et al., 2021).
4	Bulgaria	2008	Electronic Identity Card (eID)	Smart card that allows citizens to access online services and sign documents electronically.	https://psc.egov.bg/en/psc-electronic-identification	The system has been successful in providing easy access to government services such as tax payments and healthcare, with high levels of adoption among citizens. However, there have been some challenges around the complexity of the system, particularly for older or less tech-savvy users, and concerns around privacy and security (Kirilova & Naydenov, 2021).
5	Canada	2012	SecureKey Concierge	Service that allows Canadians to use their online banking credentials to securely access government	https://www.canada.ca/en/shared-services/corporate/transparency/access-information-privacy/publications/securekey-concierge-credential-broker-service.html	The system has seen success in improving the security and convenience of digital transactions, particularly in the financial sector. However, the system has faced challenges in gaining widespread adoption due to concerns about privacy and data protection. To inform the design of NDI systems in other countries, the SecureKey Concierge system highlights the importance of balancing the need for security and convenience

				services online.		with the protection of personal data (Boysen, 2021).
6	Chile	2019	Clave Única:	DI platform that provides citizens with access to online services and allows them to sign documents electronically.	https://claveunica.gob.cl/	The system has been successful in increasing access to government services and reducing fraud. However, it has also faced criticism for being too centralized and for potentially exposing users to government surveillance. The case of Clave Única highlights the importance of ensuring that NDI systems are designed to protect user privacy and are subject to appropriate oversight and accountability mechanisms.
7	Cyprus	2016	Electronic Identity (e-ID)	Smart card that allows citizens to access online services and sign documents electronically.	https://ega.ee/project/creating-eid-cyprus/	The system has been successful in reducing bureaucracy and improving the efficiency of government services. However, it has faced challenges in gaining widespread adoption due to concerns about data protection and the potential for identity theft. The case of Cyprus's e-ID system emphasizes the importance of ensuring that NDI systems are designed to be user-friendly and accessible to all citizens, regardless of their level of digital literacy.
8	Denmark	2022	MitID	Digital ID that allows citizens to securely access online services and sign documents electronically.	https://www.mitid.dk/en-gb/about-mitid/	The system has been successful in improving the efficiency of government services and reducing fraud. However, it has also faced challenges in terms of technical issues and user experience. To inform the design of NDI systems in other countries, the case of MitID highlights the importance of ensuring that systems are designed with the end-user in mind, and that appropriate technical support and user education are provided to ensure widespread adoption and success (Andersen, 2021).
9	Estonia	2014	e-Residency	Program that provides non-Estonian citizens with a government-issued digital ID card that allows them to establish and manage an online	https://e-resident.gov.ee/	The program allows anyone in the world to apply for a digital ID, which provides secure access to Estonia's e-government services and enables entrepreneurs to establish and run businesses in Estonia remotely. The system has streamlined bureaucratic processes and enhanced Estonia's global reputation as a tech-savvy nation. However, concerns have been raised about potential security risks and the need to ensure the privacy of users' data (Tammpuu & Masso, 2019).

				business in Estonia.		
10	Germany	2010	Personalausweis	Smart card that allows citizens to access online services and sign documents electronically.	https://www.personalausweisportal.de/	The system provides secure identification for German citizens and facilitates access to government services, but has faced criticism for being overly complex and difficult to use. Furthermore, there have been concerns about data protection and the security of the system, which has led to calls for increased transparency and accountability (Sobczak, 2013).
11	Iceland	2000	Rafræn skilríki	Digital ID card that allows citizens to access online services and sign documents electronically.	https://www.skra.is/english/	The system provides secure digital identification and allows citizens to access government services online, including tax returns and voting. The success of the system has been attributed to its user-centric design, which takes into account the needs and preferences of citizens. However, concerns have been raised about potential security vulnerabilities and the need to ensure data privacy (Gunnlaugsson & Jónasson, 2013).
12	India	2009	Aadhaar	Biometric ID program that provides citizens with a unique ID number and allows them to access government services and benefits.	https://uidai.gov.in/	The system has been successful in reducing fraud and improving access to government services, but has also faced criticism for privacy violations and security breaches. The Indian government has implemented measures to address these concerns, including strengthening data protection laws and increasing transparency (Chowdhry et al., 2021).
13	Indonesia	2011	e-KTP	Smart card that serves as a national ID card and allows citizens to access online services.	https://www.e-ktp.com/	The system has been successful in reducing fraud and identity theft, as well as facilitating more efficient government services. However, there have been concerns about data privacy and security, with reports of personal information being sold on the black market. The system's success can inform other countries on the importance of strong data protection measures and ongoing monitoring of potential vulnerabilities (Makarim & Kom, 2020).

14	Italy	2016	SPID	DI system that allows citizens to access online services from different public and private organizations with a single set of credentials.	https://www.spid.gov.it/	The system has enabled increased interoperability between different public and private sector services. However, there have been challenges in ensuring widespread adoption, as some users have reported difficulties in the registration process. The system's success can inform other countries on the importance of effective communication and user-friendly design to encourage adoption (Mentasti, 2022).
15	Kazakhstan	2019	Mobile citizens (mGov)	Mobile app that provides citizens with access to public services and allows them to manage their personal data.	https://egov.kz/cms/en/articles/mobilecitizen	The system has also enabled greater transparency in government services and reduced corruption. However, there have been concerns about data privacy and security, as well as a lack of awareness and understanding among citizens. The system's success can inform other countries on the importance of comprehensive education and outreach efforts to ensure public trust and understanding (Duffy et al., 2016).
16	Latvia	2019	eID Card	Smart card that allows citizens to access online services and sign documents electronically.	https://www.pmlp.gov.lv/en/identity-card-eid	The system has been praised for its strong encryption and high security standards. However, there have been concerns raised regarding the accessibility of the system, as it requires the use of a smart card reader and a compatible computer. Additionally, there have been some reported issues with the card's chip, which has caused some difficulties in accessing certain services (Kostrikova, 2021).
17	Lithuania	2020	Electronic Identity Card (eID)	Smart card that allows citizens to access online services and sign documents electronically.	https://www.eid.lt/	The system has been widely adopted and has enabled citizens to access a range of government services online. However, there have been some concerns raised regarding the level of privacy protection provided by the system, as well as its accessibility. For example, some users have reported difficulties in obtaining the necessary hardware to use the system (Sullivan, 2018).
18	Luxembourg	2005	LuxTrust	DI and authentication service that allows citizens to securely access online services and sign documents electronically.	https://www.luxtrust.lu/en/	The system is widely used by both the public and private sectors, and has been praised for its strong security and privacy protections. However, there have been concerns raised regarding the complexity of the system, which can be difficult for some users to navigate (Mooji, 2023).

19	Netherlands	2006	DigiD	DI system that allows citizens to access online services from different public and private organizations with a single set of credentials.	https://www.digid.nl/en/	The system has been widely adopted and has enabled citizens to access a range of government services online. The system has been praised for its simplicity and ease of use. However, there have been some concerns raised regarding the system's security, with reports of fraudulent activity and identity theft. As a result, the government has made efforts to improve the security of the system, such as implementing two-factor authentication (Udwan et al., 2020).
20	New Zealand	2013	RealMe	DI system that allows citizens to securely access online services and sign documents electronically.	https://www.realme.govt.nz/	The system uses biometric authentication and encrypted data storage to protect users' personal information. One of the key factors in RealMe's success has been the collaboration between the government and private sector, with a range of businesses now accepting RealMe as a trusted form of identification. However, there have been some concerns raised about the security of RealMe, and the potential for it to be used as a tool for surveillance (Australian Productivity Commission & New Zealand Productivity Commission, 2019).
21	Pakistan	2000	National Database and Registration Authority (NADRA)	National database that provides citizens with a unique ID number and allows them to access government services and benefits.	https://www.nadra.gov.pk/	NADRA has implemented a range of measures to ensure the security and integrity of its database, including biometric verification and encryption technologies. The system has been successful in enabling citizens to access a range of services, including voting, banking, and healthcare. However, there have been reports of corruption and data breaches, highlighting the ongoing challenges in maintaining the security and privacy of large-scale DI systems (Aksar et al., 2023).
22	Peru	2013	Documento Nacional de Identidad (DNI)	Smart card that serves as a national ID card and allows citizens to access online services.	https://www.gob.pe/235-documento-nacional-de-identidad-dni	The system uses biometric authentication and data encryption to protect users' personal information, and has been integrated with a range of government services, including healthcare, education, and banking. One of the key challenges facing the DNI system has been ensuring that it is accessible to all citizens, particularly those in rural or remote areas, who may not have access to the necessary technology or infrastructure (Sen, 2019).
23	Philippines	2019	PhilSys	National ID system that provides citizens with a unique ID number and allows them to access government	https://psa.gov.ph/philsys	The system uses biometric authentication and data encryption to protect users' personal information, and has been integrated with a range of government services, including social security, healthcare, and financial services. One of the key challenges facing PhilSys has been ensuring that all citizens are enrolled in the system, particularly

				services and benefits.		those in marginalized communities who may be less likely to have access to the necessary technology or information (Abesamis & Caramancion, 2022).
24	Singapore	2003	SingPass	DI system that allows citizens to access online services from different public and private organizations with a single set of credentials.	https://www.singpass.gov.sg/	The system has been widely adopted, with over 4 million users and over 1,000 services available through the platform. The success of SingPass is attributed to its ease of use, security, and reliability. However, there have been concerns about privacy and data protection, leading the government to implement additional measures such as two-factor authentication and data encryption (World Bank, 2022).
25	South Korea	2020	MyNumber	National ID number system that allows citizens to access government services and benefits.	https://www.kojinbango-card.go.jp/en/	The system has enabled more efficient and convenient financial transactions. However, there have been concerns about potential security vulnerabilities and data breaches. The system's success can inform other countries on the importance of ongoing monitoring and proactive measures to address potential security risks (Rim, 2022).
26	Spain	2015	DNI electrónico	Smart card that allows citizens to access online services and sign documents electronically.	https://www.dnielectronico.es/PortalDNIe/	The system has been praised for its security features, including digital signatures and encryption, and its interoperability with other systems. However, there have been issues with the accessibility of the system, with some users experiencing difficulty obtaining and using the smart card. Additionally, there have been concerns about data privacy and security breaches (Buccafurri et al., 2015).
27	Switzerland	2016	SwissID	DI and authentication service that allows citizens to securely access online services and sign	https://www.swissid.ch/en/	The system has been praised for its high level of security and user-friendliness, and has been widely adopted by various companies and government agencies. However, there have been challenges in ensuring interoperability with other systems, as well as concerns about data protection and privacy (Young & Verhulst, 2018).
28	Thailand	2021	National Digital ID	DI platform that aims to provide a secure and convenient way for Thai citizens to access government services and	https://www.ndid.co.th/	The system has been widely adopted, with over 20 million users registered in the first few months of its launch. However, there have been concerns about data privacy and security, as well as the potential for misuse of biometric data. Additionally, there have been challenges in ensuring accessibility for all users, particularly those in rural areas (Arunwatanamongkol, 2021).

				conduct transactions online.		
29	Turkey	2008	Elektronik Kimlik Kartı (E-Devlet)	DI platform that provides Turkish citizens with a range of online services, including government services, banking, and e-commerce.	https://www.turkiye.gov.tr/	Citizens can access over 5,000 government services online, from filing taxes to registering for social security. The system also allows for secure electronic voting and has contributed to a reduction in bureaucracy and paperwork. However, there have been concerns about the security and privacy of personal information stored on the system, and there have been reports of identity theft and fraud (Inal, 2022).
30	United Arab Emirates	2018	UAE PASS	DI platform that provides Emirati citizens and residents with secure and convenient access to a range of government and private sector services.	https://selfcare.uaepass.ae/	The system has been successful in promoting digital transformation in the country and streamlining government services. It also provides a secure and convenient way for citizens and residents to access their personal information and conduct transactions online. However, there have been concerns about data privacy and security, particularly as the system collects a vast amount of personal data (Third et al., 2018).
31	United Kingdom	2016	Verify	DI platform that enables UK citizens to access a range of government services online.	https://www.signin.service.gov.uk/	The system allows users to create a DI by verifying their personal information through a third-party identity provider. While the system has been successful in increasing access to digital services and reducing fraud, it has also faced criticism for being overly complicated and difficult to use. In addition, there have been concerns about the cost of implementing the system and the lack of support for smaller businesses (Harbinja, 2017). This led to the announcement of its closure on October 28, 2022; no new accounts would be accepted after the middle of December 2022, and all Verify services would be discontinued by April 2023.
32	Uruguay	2015	Cédula de Identidad Electrónica (e-CI)	DI card that provides Uruguayan citizens with secure and efficient access to government services online.	https://www.dgi.gub.uy/	The system allows citizens to access their personal information and conduct transactions online, including voting and tax filing. The system has also contributed to a reduction in bureaucracy and improved efficiency in government services. However, there have been concerns about the accessibility of the system for elderly and low-income citizens who may not have

						access to the necessary technology or internet connectivity (Jackson et al., 2019).