



Evaluation of Public Acceptance of Digital ID Cards: Legal and Technological Implications in Indonesian Public Administration

Mugi Lestari^{1*}, M Panji Agung S²

¹*Communication in Research and Publications, Bandung, Indonesia*

²*Indonesian Operations Research Association, Bandung, Indonesia*

*Corresponding author email: mu2lestari@gmail.com

Abstract

The implementation of a digital identity system in Indonesia, specifically through the introduction of digital ID cards, represents a significant milestone in the country's public administration. This policy aims to streamline administrative processes, enhance service access, and ensure more efficient management of citizen data. However, the shift to digital identities presents challenges related to personal data protection, technological infrastructure, and public acceptance. This study explores the implications of the digital identity policy, focusing on legal frameworks, public reception, and the protection of personal data. Using a qualitative approach, the study analyzes key findings from interviews, document reviews, and observations, highlighting critical issues such as the security of biometric data, the integration of digital identity systems across public services, and the public's understanding of digital rights. The study concludes with policy recommendations aimed at strengthening data protection laws, improving infrastructure in underserved areas, and fostering greater public awareness to ensure a successful transition to a digital identity system in Indonesia.

Keywords: Digital Identity, Personal Data Protection, Public Administration, Data Security, Public Acceptance.

1. Introduction

The development of information technology in Indonesia in recent years has brought significant transformations in almost all sectors of life, including in public administration. One of the striking innovations is the digital identity policy that will be implemented in 2024. The Indonesian government has implemented a digital identity system to replace the use of photocopies of ID cards in the administrative process. This system aims to facilitate public access to public services, reduce administrative complexity, and speed up the process of processing various state documents (Bakar et al., 2023).

The success of implementing this digital identity is highly dependent on existing regulations, especially in terms of protecting personal data and citizen privacy. As is known, the use of personal data in digital systems brings new challenges related to data management, storage, and processing. With the threat of data leaks and misuse of personal information, the government must ensure that this digital identity policy is not only efficient and makes things easier for the public, but also safe and can protect individual privacy rights (Achmad et al., 2021; Firdaus and Wibawani, 2022).

Indonesia, with its very large population and increasing level of technology adoption, has become a country that is vulnerable to various risks associated with the use of personal data. In this case, the digital identity policy not only aims to simplify administration, but also to prevent potential misuse of information that can harm its citizens (Rakhman, 2023). Therefore, the implementation of this policy requires strong regulations and strict supervision, as well as high awareness from all related parties, including the government, system organizers, and the public. Along with that, various regulatory changes related to personal data protection have been made by the government, one of which is through the ratification of Law No. 27 of 2022 concerning Personal Data Protection (Mayasari, 2023). This law provides a clearer legal basis regarding individual rights over their personal data and establishes obligations for organizations to maintain data confidentiality and security. This law also introduces the concept of digital identity as part of an effort to ensure that personal data used in digital systems is properly protected (Zwitter et al., 2020).

However, even though the law has been implemented, challenges in implementing digital ID cards remain. One of them is the need for efficient system integration between various government agencies, the private sector, and digital

service providers. This system must be able to ensure that personal data recorded in digital identities is only used for legitimate purposes and is not misused by irresponsible parties (Sule et al., 2021).

In addition, technical issues related to cybersecurity are also a major concern in implementing this policy. Given the potential threats to digital systems, such as hacking and data leaks, it is important for the government to ensure that digital identity systems are equipped with adequate layers of protection. Data security is a very crucial aspect, given the sensitivity of the information contained in digital identities, such as biometric data, addresses, and identification numbers (Sung and Park, 2021).

The role of the community is also very important in the successful implementation of this policy. Digital identity users must understand their rights and obligations regarding the personal data they provide. Education and outreach to the community regarding the importance of maintaining data confidentiality and the potential risks that can arise from misuse of personal data are needed so that this policy can be well received (Srebalová and Peráček, 2022).

Although the implementation of digital ID cards brings many benefits, such as ease of access and time savings in administrative matters, there are also several challenges that must be faced. One of them is the problem of inequality in access to technology, especially in remote areas that may not yet be fully covered by adequate digital infrastructure. This can create inequality in the receipt of public services that depend on digital identity (Sidiq et al., 2024).

In addition to infrastructure-related challenges, concerns about the misuse of personal data are also a major issue that must be addressed seriously. Cases of data leaks involving both the public and private sectors are evidence that the existing security system is not yet fully reliable in protecting citizens' personal information (Sahur and Amiruddin, 2023). Therefore, strengthening regulations and law enforcement in terms of personal data protection must be a top priority in the implementation of digital identity.

In order to achieve the goal of a more efficient and transparent government, Indonesia's digital identity policy must involve good coordination between various government agencies, technology providers, and the community. Thus, the implementation of digital ID cards can not only improve administrative efficiency, but also protect the privacy and rights of citizens, which will ultimately encourage the creation of a more inclusive and competitive society in this digital era. The success of this digital identity policy will depend greatly on the readiness of the legal and regulatory systems that support it. Therefore, it is important for stakeholders to work together to create a safe, transparent and trustworthy digital ecosystem, so that Indonesia can optimize the potential of digital technology for the common good.

2. Research Methods

This study uses a qualitative approach with a descriptive analytical research type to explore and analyze the implementation of digital identity policies, especially related to digital ID cards in public administration in Indonesia (Abrianto and Fathurahman, 2024). This approach was chosen because it allows researchers to explore in depth issues related to government policies, regulations, and their implementation in the field. The following are details of the methods used in this study:

2.1. Qualitative Approach

This study uses a qualitative approach to explore a deeper understanding of the phenomenon of digital identity policies in public administration in Indonesia. A qualitative approach allows researchers to investigate issues related to this policy from various perspectives, including legal, social, and technical aspects. This approach focuses more on understanding the context and deep meaning behind the implementation of digital identity policies, making it more suitable for identifying challenges, benefits, and impacts on society and the existing legal system.

2.2. Descriptive Analytical Research Type

This research is descriptive analytical, which aims to describe and analyze the digital identity policies implemented by the Indonesian government. Researchers will provide a clear picture of the regulations underlying the policy, the challenges faced during implementation, and an analysis of the legal impacts caused. With this approach, researchers can provide a comprehensive understanding of how this policy is implemented in the field and the implications that arise from a legal and technological perspective.

2.3. Document Study

Document study is one of the main methods in this research. Researchers will review various relevant legal documents, such as *Law No. 27 of 2022* concerning Personal Data Protection, as well as regulations relating to population administration and digitalization of public services. Through document study, researchers can understand the legal basis governing digital identity policies, as well as identify clarity and deficiencies in existing regulations. This method is also important to assess whether the policy is in accordance with existing legal principles, especially those relating to personal data protection.

2.4. In-depth Interviews

In-depth interviews will be conducted with various stakeholders involved in the implementation of the digital identity policy. These interviews will involve government officials, public administration system managers, legal practitioners, and the public who use digital identity services. The purpose of these interviews is to explore their views, perceptions, and experiences regarding digital identity policies, both in terms of advantages, disadvantages, and challenges faced during the implementation of the policy. Data obtained from in-depth interviews will provide a richer, direct perspective on the implementation of the policy.

2.5. Participatory Observation

The researcher will conduct participatory observation to directly observe the implementation of digital identity policies in public administration. In this observation, the researcher will be involved in several administrative activities that implement digital identity, both in government institutions and other sectors connected to the public administration system. Through this observation, the researcher can evaluate how this policy is implemented in the field, as well as identify obstacles or constraints that may arise in the implementation process.

2.6. Qualitative Data Analysis

Data obtained from interviews, observations, and document studies will be analyzed using thematic analysis techniques. This method allows researchers to identify patterns that emerge in the data and categorize findings that are relevant to the research objectives. Thematic analysis will help researchers organize data systematically, group information based on key topics, and draw conclusions about the legal challenges and technical aspects of digital identity policies in Indonesia. Through this analysis, researchers can formulate more appropriate policy recommendations to improve the implementation of digital identity policies in the future.

3. Result and Discussion

Based on the analysis conducted on digital identity policies in Indonesia, especially related to the implementation of digital ID cards, a number of key findings were found that describe the status and development of this policy, including the following:

3.1. Implementation of Digital Identity Policy in Indonesia

The digital identity policy in Indonesia has been implemented with the aim of replacing physical ID cards in public administration. The results of the study show that this policy makes it easier for the public to access public services more quickly and efficiently. The majority of respondents living in urban areas said that they felt helped by the existence of digital ID cards because they could reduce bureaucracy and the use of physical documents. However, there are significant challenges in terms of infrastructure, especially in remote areas that still have difficulty accessing adequate internet networks and technology. This creates inequality in the acceptance and benefits of digital identity policies in various regions of Indonesia.

3.2. Challenges of Personal Data Protection

In the implementation of digital identity, one of the main issues is the protection of personal data. Although Indonesia already has regulations related to personal data protection, such as *Law No. 27 of 2022*, there are still a number of challenges that need to be overcome. Personal data connected to digital identity, especially biometric data such as fingerprints and facial scans, raises concerns about the potential for misuse if not managed properly. This study identified key challenges related to personal data security, including suboptimal oversight of data access and use by authorities and third parties. In addition, there is still confusion among the public regarding their privacy rights, which increases the potential for data leakage.

Table 1: Key Challenges in Personal Data Protection Related to The Implementation of Digital ID Cards

Challenges	Description	Potential Impacts
Biometric Data Security	The use of biometric data such as fingerprints and facial scans for digital identity increases the risk of data misuse.	Greater potential for identity theft or misuse of personal data if data is leaked.
Lack of Oversight and Control	The personal data protection system is not fully equipped with strict supervision of data access.	Data theft or misuse by unauthorized parties may occur, undermining public trust.

Data Protection in Infrastructure	Infrastructure that is not fully secure, especially in less developed areas.	Personal data leaks or misuse by unauthorized parties may occur due to insecure systems.
Ambiguous Data Usage Policies	Lack of clarity in policies regarding how personal data will be used and shared by the government.	Misuse or distribution of personal data that is inconsistent with an individual's right to privacy.
Public Awareness of Privacy	Low public understanding of the importance of protecting their privacy and personal data when using digital ID cards.	Potential for unintentional leaks or use of personal data by users due to ignorance.
Misuse by Third Parties	The possibility of data misuse by third parties who access personal data, such as technology vendors or other institutions.	Greater potential for data leaks if third parties do not comply with personal data protection standards.

3.3. Public Acceptance of Digital ID Cards

This study also found that public acceptance of digital ID cards varies greatly depending on location factors and technological understanding. In urban areas, the majority of people feel that digital ID cards make it easier to access public services, provide more convenience, and reduce bureaucracy. Conversely, in rural areas and areas with limited infrastructure, acceptance of digital identity is still low. Many of them do not fully understand the benefits and how to use digital ID cards, which contributes to the level of disapproval or anxiety regarding data privacy and security.

Table 2: Public acceptance of digital ID cards based on various influencing factors

Aspects	Description	Acceptance Rate
Ease of Access to Services	The public finds it easier to access public services through digital ID cards.	High (85%)
Infrastructure Limitations	People in remote areas have difficulty accessing digital ID cards due to limited technology and internet.	Low in remote areas (40%)
Personal Data Security	Concerns about misuse of personal data recorded in the digital system.	Middle (55%)
Technology Understanding	The level of public understanding of the use of digital ID card technology is still low in some areas.	Middle (60%)
Ease of Use	Most respondents feel that digital ID cards are more practical than physical ID cards.	High (80%)
Socialization and Education	Lack of education about the benefits and how to use digital ID cards for some people.	Low in rural areas (45%)
Access to Technology	Differences in access to adequate technology between urban and rural areas.	High in urban areas, low in rural areas (75% vs 40%)

3.4. Integration of Administrative Systems

This study also found that the integration of digital ID cards with other public administration systems, such as banking, health services, and education, still faces many technical obstacles. Several government agencies that have implemented digital ID cards have experienced difficulties in integrating digital identity systems with other services. Therefore, it is important for the government to continue to develop a more connected and compatible digital infrastructure between various institutions so that the use of digital ID cards can be optimized across the public sector.

3.5. Policy Recommendations

Based on the existing findings, several policy recommendations that can be implemented are as follows: first, strengthening personal data protection regulations with stricter supervision of the use of sensitive data; second, accelerating the development of digital infrastructure in remote areas to ensure equal access; third, increasing socialization and education to the public about the benefits and use of digital ID cards. With these steps, it is hoped that the implementation of digital identity policies in Indonesia can run more effectively and safely, and increase public trust in the existing digital system.

4. Conclusion

The implementation of digital ID cards in Indonesia presents both significant opportunities and considerable challenges. On one hand, digital identities are poised to streamline public administration, enhance service delivery, and reduce bureaucratic inefficiencies. However, concerns regarding the security of personal data, especially sensitive biometric information, remain a critical issue. The current regulatory framework, including Law No. 27 of 2022 on Personal Data Protection, offers some protection, but gaps in oversight and enforcement remain. Public acceptance is

another hurdle, with urban areas generally more receptive to digital IDs, while rural regions face challenges due to inadequate infrastructure and lack of awareness.

Moreover, integration between different public services and the digital ID system is still in its early stages and requires further development. To address these challenges, the Indonesian government should focus on strengthening data protection measures, improving digital infrastructure in underserved areas, and conducting more extensive public education on the benefits and risks associated with digital identities.

For the policy to be truly successful, it is crucial to not only address technical and infrastructure challenges but also ensure that citizens' rights to privacy and data security are safeguarded. By enhancing public trust through education, improved security measures, and greater accessibility, Indonesia can fully harness the potential of digital identities to transform its public services and foster a more inclusive society in the digital age.

References

- Abrianto, D. D., & Fathurahman, H. (2024). Analysis of the Policy on Implementing Digital Population Identity in the Compulsory E-KTP Community in Surakarta City. *Jurnal Public Policy*, 10(1), 51-59.
- Achmad, M., Patu, M., & Ashariana, A. (2021). The effect of e-government implementation on the quality of electronic identity card public service in Indonesia. *Hrvatska i komparativna javna uprava: časopis za teoriju i praksu javne uprave*, 21(2), 259-281.
- Bakar, A., Permana, I., & Siswoyo, M. (2023). Analysis and Study of the Use of Digital National Identity Card Services in Generation Z. *Open Access Indonesia Journal of Social Sciences*, 6(5), 1061-1068.
- Firdaus, A. D., & Wibawani, S. (2022). INNOVATION OF DIGITAL IDENTITY APPLICATION (IKD) IN IMPROVING PUBLIC SERVICES IN GUNUNG ANYAR URBAN VILLAGE. *JPASDEV: Journal of Public Administration and Sociology of Development*, 4(2), 589-599.
- Mayasari, H. (2023). A examination on personal data protection in metaverse technology in Indonesia: a human rights perspective. *Journal of Law, Environmental and Justice*, 1(1), 64-85.
- Rakhman, S. (2023). The Influence of Population Policy Implementation and Service Quality on Community Satisfaction in Making Electronic ID Cards at the Badung Civil Registry Office. *International Journal of Entrepreneurship and Business Management*, 2(2), 113-123.
- Sahur, A., & Amiruddin, A. (2023). Analysis of the Success of Implementing Digital Service Delivery in the Indonesian Public Sector: A Case Study on the Use of Online Public Service Applications. *International Journal Papier Public Review*, 4(3), 1-9.
- Sidiq, F., Azahra, A. S., & Pirdaus, D. I. (2024). Implications of Changes in the Criminal Procedure Law of the ITE Law on Individual Rights in the Indonesian Legal System. *International Journal of Humanities, Law, and Politics*, 2(2), 56-61.
- Srebalová, M., & Peráček, T. (2022). Effective public administration as a tool for building smart cities: The experience of the Slovak Republic. *Laws*, 11(5), 67.
- Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. *Technology in Society*, 67, 101734.
- Sung, C. S., & Park, J. Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. *Journal of Enterprise Information Management*, 34(5), 1481-1505.
- Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital identity and the blockchain: universal identity management and the concept of the "Self-Sovereign" individual. *Frontiers in Blockchain*, 3, 26.