Acceptance and Use of the National Digital Identity System in Indonesia

Anshul Pachouri, Abhishek Raj, and Kushagra Harshavardhan

National digital identity systems increasingly enable access to public and private services, but their effective use depends not only on technological infrastructure but also on whether users perceive national digital ID as useful and easy to use. This paper examines the acceptance and actual use of Indonesia's national digital ID "e-KTP" through an Extended Technology Acceptance Model. Drawing on a nationally representative mixed-methods study of 1,565 households across five major island groups in Indonesia, the study examines how perceived ease of use, perceived usefulness, institutional trust, regulatory awareness, social acceptance, and mandatory adoption shape users' attitudes, behavioral intention, and actual use of the e-KTP. The findings show that the e-KTP has become a trusted and widely accepted identity because it is familiar, reliable, and consistently recognized across public and private service points. Institutional trust emerges as the strongest factor shaping users' attitudes toward e-KTP and predictability of acceptance of e-KTP by service providers is driving the actual use. An increase in resident's awareness of redressal mechanisms and safeguards may increase the use of the e-KTP for private-sector services. The transition from identity coverage to trusted online use depends on institutional credibility, consistent service acceptance, user awareness of safeguards, and robust data governance.

1 Introduction

National digital identity is increasingly recognized as a foundational digital system that enables people to prove their identity, facilitating trusted interactions between individuals, government, and business (Jabbour and Tullis 2024). It is also central to how people, particularly poor and other vulnerable groups with limited digital literacy, access essential services such as healthcare and social protection, and participate in the digital economy. The national digital ID directly contributes to Sustainable Development

Journal of Online Trust and Safety 3 (3)
DOI: 10.54501/jots.v3i3.323
Research Article

Goal (SDG) 16.9, which aims to provide legal identity for all by 2030 (World Bank 2019). It is also a key enabler and contributor to many SDG targets related to access to finance, gender equality and empowerment, social protection, and access to healthcare, among others.

As service delivery across sectors moves online, the ability to verify identity securely, conveniently, and remotely becomes critical (Desai et al. 2023). The COVID-19 pandemic also highlighted the need for digital identification systems. With lockdowns and movement restrictions, the demand for digital identification to access various public and private services surged dramatically (Marin and Palacios 2022). To overcome this gap, development efforts are underway to provide a legal identity for all, and more importantly, a national digital identity[1] that enables online transactions, allowing individuals to fully participate in the digital economy. A national digital ID with online use capability can support a range of applications, including electronic know-your-customer (e-KYC) processes for opening bank accounts and logging in to public or private service portals, etc.

However, the mere existence of a national digital ID that enables online use is not enough. The deeper question is whether users trust national digital ID, and more importantly, whether it is secure and trustworthy in practice (Maple, Epiphaniou, and Gurukumar 2021). As more services require identity verification and digital onboarding, questions of security, privacy, institutional trust, and user confidence in the national digital ID system become increasingly important. The degree of trust that users, governments, and organizations place in the service and operations of a national digital identity system is linked to its success (Maple, Epiphaniou, and Gurukumar 2021). A well-functioning national digital ID system can indeed lower service delivery costs and boost inclusion. But if the system is perceived as unsafe or experiences a major failure (for instance, a data breach or verification error), the consequences can be negative, especially for the poor and vulnerable segment. Through this paper, we aim to understand adoption of a national digital ID, especially from the dimension of trust, through a case study from Indonesia, a majority world country.

Indonesia provides a useful case for examining these issues. The country has developed a national digital identity system comprising the Kartu Tanda Penduduk Elektronik (e-KTP), an electronic identity card, and Identitas Kependudukan Digital (IKD), a recently launched mobile identity application built on the existing e-KTP infrastructure (Zainudin 2025; Sahatatua et al. 2024). Despite the importance of these systems, the adoption factors including trust affecting national digital ID, such as e-KTP's use to access public and private services remain insufficiently understood. Existing literature on technology adoption and trust is often anchored in Western contexts, which may not fully reflect the

1. National digital ID systems are national ID systems that use digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer (World Bank, n.d.). In this paper, the online use of a national digital ID, simply means using national digital identity credentials to verify a person's identity online, allowing him or her to access various services. (Adapted from Metz, Casher, and Clark 2024)

global majority where digital literacy, infrastructure, state capacity, and service delivery arrangements differ substantially.

This paper draws on a nationally representative mixed-methods study of 1,565 households across Indonesia and examines residents' perceptions of institutional trust, usefulness, ease of use, and actual use of e-KTP in service access contexts. The study applies a Technology Acceptance Model to examine how users form attitudes toward national digital identity and how those attitudes translate into behavioral intention and actual use.

2 Literature Review

The literature review follows a structured approach to synthesize scholarship on national digital identity systems, focusing on trust, platform safety, and technology adoption.

2.1 Trust in National Digital Identity Systems

Trust is widely recognized as a determinant of adoption of any digital system. In information systems literature, trust is conceptualized as a multi-dimensional construct encompassing institutional trust, technical trust, and perceived integrity of systems (Mayer, Davis, and Schoorman 1995; Gefen, Karahanna, and Straub 2003). In the context of national digital identity, trust is especially important because identity systems facilitate access to essential services and often involve the processing of sensitive demographic and biometric information. Maple, Epiphaniou, and Gurukumar (2021) argue that digital identity systems must be "trustworthy-by-design," requiring alignment between governance structures, technical safeguards, and user-facing transparency mechanisms. Similarly, the World Bank's Principles on Identification for Sustainable Development emphasize that identity systems must be inclusive, trusted, and designed to protect user rights and privacy (World Bank 2019).

2.2 Exclusion and Other Risks Associated with National Digital Identity Systems

National digital identity systems are often perceived as enablers of inclusion and efficiency, yet a significant body of literature highlights their socio-technical risks. One major challenge is exclusion arising from authentication failures, data mismatches, or infrastructure limitations. Muralidharan, Niehaus, and Sukhtankar (2022) demonstrate in the context of India that while biometric authentication can improve service delivery and reduce leakage, implementation challenges and weak safeguards can create exclusion risks. Such exclusion risks are particularly severe in contexts where identity verification is tied to essential services and fallback mechanisms are weak or absent. These find-

ings show that identity coverage alone is an incomplete indicator of effectiveness of performance of national digital ID system.

In addition to exclusion risks, the scholarship on national digital identity also establishes privacy and surveillance risks. National digital identity systems are high-value targets because they often possess sensitive personal and biometric data. Acquisti, Brandimarte, and Loewenstein (2015) highlight that the increasing collection and use of personal data in digital systems creates privacy risks and challenges related to individual control over personal information. Cavoukian's (2011) privacy-by-design framework further emphasizes embedding privacy protection into system architecture, including those of national digital ID systems rather than treating them as compliance afterthoughts. The World Bank's guidance on digital identity and data protection underscores that while digital ID systems can improve service delivery, without robust safeguards, such systems can expose individuals to risks of data misuse, unauthorized sharing, and privacy violations (Clark and Daly 2019).

Bennett and Raab (2017) further argue that large-scale identification systems increase the likelihood of surveillance and reduce informational autonomy. A recurring concern in the literature is "function creep," referring to the gradual expansion of identity systems beyond their original administrative purpose into broader surveillance, service integration, or commercial applications. This expansion is often enabled by data linkage across systems and weak institutional constraints on secondary use, raising fundamental governance challenges related to consent, transparency, and accountability (Haggerty and Ericson 2000; Lyon 2009; Bennett and Raab 2017; Clark and Daly 2019). Moreover, these risks are not distributed evenly. People who rely on anonymity, controlled disclosure, or separation between public and private identities may experience digital identity systems differently from majority users. This includes LGBTQIA+ people, whistleblowers, migrants, and other groups whose safety may depend on limiting traceability (Kayyali and Mithani 2025; Masiero 2023). These risks become more complex when national identity systems are used not only by the state but also by banks, telecommunications providers, fintech platforms, and others.

Platform governance and trust and safety research emphasizes on managing online harm such as impersonation, fraud, fake accounts, and coordinated inauthentic behavior (DTSP 2025). Although literature often focuses on social media, marketplaces, and online platforms, it has increasing relevance for national digital identity systems. Identity verification systems are no longer confined to state administrative functions but increasingly operate as infrastructural components of platform trust and safety ecosystems. These systems support platform integrity by enabling authentication, reducing impersonation risks, and strengthening e-KYC processes across digital services (Gillespie 2018; Gorwa, Binns, and Katzenbach 2020; Temoshok et al. 2025; Clark and Daly 2019). However, this relationship is not straightforward. Stronger verification can improve platform integrity and reduce abuse, but it can also increase privacy risks, surveillance concerns, and

overidentification (Masiero 2023). Temoshok et al. (2025) in their risk-based approach, suggest that digital identity assurance should be proportional to the risk of transaction, particularly in online environments where different services carry different risk levels: identity systems must adopt layered assurance levels to mitigate risks across different types of transactions.

National digital identity systems therefore sit at the intersection of state governance and platform governance. They secure transactions, enable authentication, and support account integrity, but they also shape the distribution of privacy and safety across public and private infrastructures.

2.3 Synthesis and Research Gaps

Despite the extensive literature on trust and national digital identity systems, most studies remain focused on either technical architecture or legal frameworks. There is limited empirical research on how users adopt a national digital identity system and perceive trust in everyday identity-enabled transactions, particularly in developing country contexts where institutional and digital constraints intersect.

Four key gaps emerge from literature. First, literature emphasizes system efficiency but under-theorizes adoption drivers and trust in context of national digital identity. Second, platform trust and safety literature examine online harms but rarely integrates national identity systems into its analytical scope. Third, literature focuses on risks but provides limited insight into the lived user experience. Fourth, technology adoption models explain behavioral intention but insufficiently capture institutional and infrastructural complexity. Taken together, these gaps highlight the need for more empirical studies using an integrated framework that combines digital identity systems, trust, and adoption factors.

This study attempts to address these gaps by examining how users perceive and use Indonesia's national digital identity "e-KTP." It brings together digital identity, institutional trust, platform trust and safety, and technology adoption literature within a Technology Acceptance Model.

3 National Digital Identity System in Indonesia: A Brief Overview

Indonesia's national digital identity system comprises the Population Administration Information System database called "SIAK," the unique population identity number issued at birth registration called "NIK," the electronic national ID card available from age 17 called "e-KTP," and the recently launched identity application called "IKD" (World Bank 2023). Together, these components form the backbone of identity verification across public and private services.

3.1 NIK, e-KTP and IKD: Systems and Roles

Indonesia's national digital identity system is primarily built around the population identity number, or *Nomor Induk Kependudukan* (NIK), a 16-digit lifetime identifier assigned to Indonesian citizens at birth registration and available to legal residents with permanent stay permits. Dukcapil generates these centrally. The electronic identity card, or e-KTP, is linked to this number and serves as the dominant identity credential for adult citizens. It covers 97 percent of the eligible population and is issued after biometric deduplication, which supports uniqueness within the identity system.

e-KTP enables access to a wide range of public and essential services. For instance, it is used to avail benefits from social protection programs such as PKH (*Program Keluarga Harapan*, the conditional cash transfer program), BPNT (*Bantuan Pangan Non-Tunai,* the non-cash food assistance program), and PIP (*Program Indonesia Pintar*, the education assistance program). It is also used to access healthcare services and health insurance, including Satu Sehat (the national health data integration platform), to complete e-KYC verification for bank account opening, and to get SIM cards, among others.

Indonesia's identity ecosystem is now in a transitional phase with the introduction of IKD. It allows users to access digital identity information and supports verification through mechanisms such as facial verification and QR-code verification. Its intended role is to enable end-to-end digital service access without requiring residents to present the physical electronic card (e-KTP). However, its adoption and use remain predominantly less mature than e-KTP, and its role in actual service delivery is still emerging (World Bank 2025) .

3.2 Regulatory Landscape

Indonesia's regulatory framework for national digital identity spans population administration, cybersecurity, electronic transactions, electronic signatures, and personal data protection. Among these, population administration law and personal data protection law are the most prominent ones.

Law No. 23 of 2006, as amended by Law No. 24 of 2013, provides the legal foundation for Indonesia's population administration system and the issuance of the electronic identity card (e-KTP). The law establishes the basis for recording population events, assigning identity numbers, maintaining population databases, and issuing official identity documents (SEAP 2026). Its relevance to national digital identity is significant because it defines the administrative infrastructure through which residents are registered, identified, and linked to public records and service delivery systems. In addition to identity law, Indonesia's Personal Data Protection Law, Law No. 27 of 2022, provides the framework for governing the collection, processing, sharing, and protection of personal data. The law establishes obligations for data controllers and processors and includes provisions related to dispute resolution and criminal liability for personal data violations (SEAP

2026). Its relevance to national digital identity is equally important because identity systems depend on the processing of sensitive demographic and biometric information across multiple public agencies and private relying parties.

Taken together, these legal instruments show that Indonesia's national digital identity system is governed both as a population administration system and as a personal data management system. This is noteworthy because users do not experience national digital identity only as a credential or technology. They encounter and experience national digital ID through institutions, services providers, frontline service interactions, identify verification processes, and data-handling practices.

4 Research Design and Methods

4.1 Theoretical Framework

The study is grounded in the Technology Acceptance Model (Davis 1989), which suggests that perceived usefulness and perceived ease of use influence attitudes toward a technology, which in turn shape behavioral intention and actual use. The Technology Acceptance Model (TAM) has been extensively used to explain the adoption of digital technologies. Studies have demonstrated the relevance of the model across a range of technologies, including online platforms, mobile applications, and digital public services (Venkatesh and Davis 2000). In digital systems and e-government, TAM has been widely used to explain citizen adoption of government platforms and digital service delivery systems (Carter and Bélanger 2005). These studies show that citizens are more likely to adopt digital government services when they perceive them as useful, easy to use, and capable of improving the efficiency of interactions with public institutions. The model therefore provides a useful analytical lens for examining how individuals perceive the benefits and usability of national digital identity systems to access various services (Figure 1).

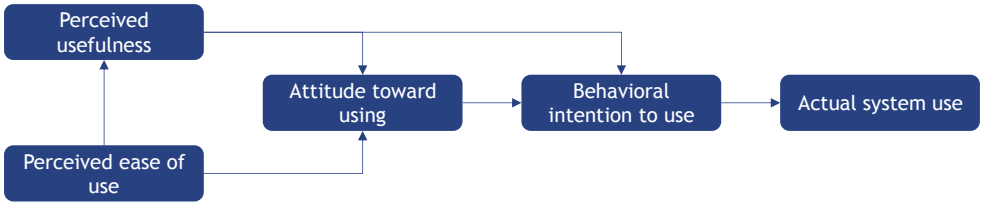

Figure 1: Technology Acceptance Model.

The TAM includes five constructs: perceived usefulness, perceived ease of use, attitude towards using, behavioral intention to use, and actual system use. Building on the existing research, this study expands the original TAM by including additional elements that consider the wider institutional context and complexity of national digital identity systems as highlighted in the literature review. Specifically, the expanded framework

introduces four new factors: institutional trust, regulatory awareness, social acceptance, and mandatory adoption.

The original TAM explains adoption through individual perceptions of usefulness and ease of use, but neither construct captures a citizen's confidence in the institutions that operate the system. Carter and Bélanger (2005) integrated institution-based trust into an extended TAM for e-government, showing that citizens' willingness to transact online with government depends on confidence in the institution itself, not merely the interface. In a national digital identity system institutional trust is inseparable from adoption because the credential is operated by a monopoly state authority. This extends to the private-sector actors, including banks, telecoms, and fintech platforms, who rely on identity data for verification and whose behavior shapes whether users feel safe engaging with national digital ID-enabled online services. The study, therefore, uses institutional trust as a construct in TAM. Institutional trust captures confidence in the government and private-sector actors that manage, verify, or rely on identity data.

Secondly, the TAM and its successors focus on individual perceptions of usability and utility but do not account for users' understanding of the governance environment in which technology operates. In contexts where personal data is collected, processed, and shared by state institutions, the degree to which users are aware of applicable data protection regulations and available redress mechanisms becomes critical. Within e-government adoption research, perceived transparency has been identified as significant determinants of citizen trust in digital services (Colesca 2009; Nguyen et al. 2024) and the absence of regulatory literacy can leave users vulnerable when data misuse occurs. This study, therefore, incorporates regulatory awareness as a TAM construct and captures users' understanding of rules, rights, and remedies related to data management and identity verification.

Further, TAM's formulation conceptualizes technology acceptance as an individual cognitive process and explains it through perceptions of usefulness and ease of use. However, national digital identity systems operate within broader service ecosystems where adoption and use also depends on institutional environment in which credentials are presented and verified, i.e., whether institutions and service providers recognize and accept the credential. Venkatesh and Davis (2000) introduced subjective norm into TAM2 as a social influence construct, and Venkatesh et al. (2003) consolidated this in Unified Theory of Acceptance and Use of Technology (UTAUT). Building on this literature, the study therefore uses social acceptance as a construct for extension of TAM. This construct captures the extent to which the credential is recognized and accepted to access various services by service providers as a valid basis for identity verification. Since national digital ID systems are primarily governed and managed by the public institutions, it's important to also include perceptions of inclusion and fairness in social acceptance.

Lastly, the TAM was developed and validated in voluntary-use environments, and its pre-

dictive structure has been shown to differ meaningfully when technology use is mandated. Brown et al. (2002) directly examined this gap, demonstrating that when technology use is mandated, the underlying relationships of traditional technology acceptance models change. National digital identity systems represent a case of mandated technology. This study, therefore, incorporates mandatory adoption as a TAM construct that captures role of mandated acceptance in system use.

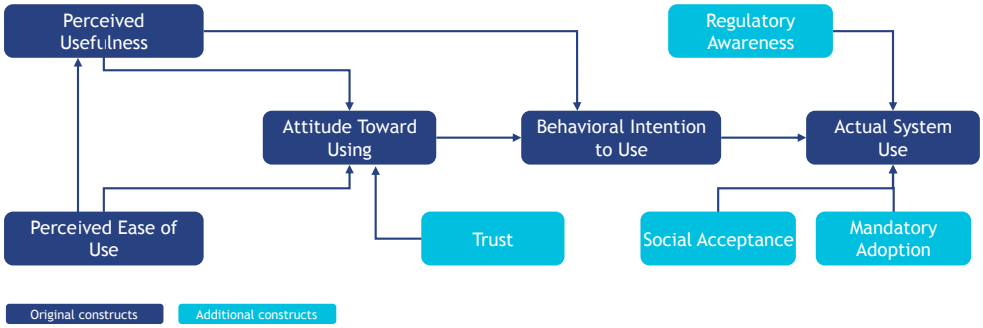

Figure 2: A proposed extension to Technology Acceptance Model.

The proposed extension to TAM (Figure 2), as a result, encompasses two interconnected pathways for the adoption of national digital identity. The original pathway mirrors the attitudinal process outlined in the original TAM; specifically, perceived usefulness and perceived ease of use influence attitudes and subsequent behavioral intentions. The second pathway considers the institutional environment, where the use of a national digital ID is affected by trust, regulatory awareness, social acceptance, and existing mandates.

4.2 Research Questions

This paper applies a Technology Acceptance Model to examine the factors shaping adoption and actual use of Indonesia's national digital identity system. It aims to address the following research questions:

RQ1: How does trust influence users' attitudes, behavioral intention, and actual use of Indonesia's national digital identity "e-KTP"?

RQ2. How do other factors such as perceived usefulness, perceived ease of use, etc. shape users' attitudes and behavioral intention toward Indonesia's national digital identity "e-KTP"?

4.3 Methods

This study uses a mixed-methods research design to answer the research questions. The study combines a nationally representative quantitative survey with qualitative interviews. The quantitative aspect furnishes national-level data concerning awareness, perceptions, trust, and usage trends associated with e-KTP. In addition, the qualitative dimension

elucidates the underlying experiences by which these perceptions are constructed and how trust is affected by interactions at service delivery points. Mixed-method research also allows for the triangulation of findings. While the quantitative survey identifies statistical relationships among different variables, the qualitative interviews provide context for these quantitative results.

4.3.1 Quantitative sampling strategy and geographic coverage

The quantitative survey included 1,565 participants from five major Indonesian island groups: Java, Sumatra, Kalimantan, Sulawesi, and Bali–Nusa Tenggara. These island groups were used as the main sampling strata to ensure national representation. A stratified multistage sampling design was adopted. Initially, island groups served as the primary strata. Afterward, provinces were chosen within each island group to represent regional differences, while also considering the practical aspects of conducting fieldwork. Within the chosen provinces, regencies and cities were identified, and then households and eligible adult respondents were randomly selected. Rural and urban quotas were assigned in proportion to population distribution. To ensure a balanced sample, the study made efforts to include participants of different genders, ages, and income levels.[2]

4.3.2 Qualitative study design

The qualitative study comprised 24 in-depth interviews and six focus group discussions involving 24 participants, designed to contextualize the findings of the quantitative survey. All interviews and discussions were conducted in person. Participants were randomly selected, and qualitative fieldwork was conducted across the same five major island groups covered by the quantitative survey (Java, Sumatra, Kalimantan, Sulawesi, and Bali and Nusa Tenggara), with participants drawn from both urban and rural locations consistent with the study's overall 60:40 urban-rural sampling ratio. Discussions explored users' experiences with e-KTP registration, service access, identity verification, trust in government and private-sector players, concerns about data misuse, and perceptions of online use of e-KTP.

4.3.3 Survey instrument and measures

The survey instrument developed for this study captured a broad range of respondent experiences with e-KTP, covering awareness, enrollment, service access, authentication, and perceptions of e-KTP in terms of trust, security, reliability, and ease of use. Overall, the

2. The sample allocation was conducted using a floor-plus-proportional approach. To ensure fair representation, each island group was assigned a minimum number of respondents. The rest of the sample was then divided based on the size of each group's population. This method allows for conclusions that apply to the entire nation, while also enabling analyses of the different island groups. The required sample size was calculated using Cochran's formula, which is used for estimating proportions (Cochran 1977). To account for the highest possible variance, a population proportion of 0.5 was used. A design effect of 2.3 was included to consider the clustering that occurs in multistage sampling in a country with a wide geographical area. Therefore, the final target sample size was set at about 1,550 participants, which ensured the study had enough statistical power.

survey instrument comprised 63 items, of which 32 items were finally selected to test the constructs of the TAM and its proposed extension. These 32 items were distributed across the nine constructs. Perceived ease of use was measured through two items capturing the effort involved in enrollment and verification interactions. Perceived usefulness was measured through four items capturing beliefs about the functional benefits of e-KTP relative to conventional IDs, including effects on service speed and cost. Attitude toward digital ID was measured through five items capturing confidence, security, reliability, and anticipated future relevance of e-KTP. Institutional trust was measured through six items capturing confidence in the operational reliability of e-KTP and in the data stewardship practices of government entities, banks, and telecom providers. Regulatory awareness was measured through three items capturing respondents' knowledge of data governance frameworks and available complaint and redress mechanisms. Social acceptance was measured through two items capturing the degree to which e-KTP is recognized and accepted within the service ecosystem. Mandatory adoption was measured through a single item assessing whether use of e-KTP under legal or institutional requirement was perceived as improving the service experience. Behavioral intention was measured through four items capturing stated preferences, anticipated future use, and willingness to advocate for e-KTP. Actual use was measured through five items capturing frequency of use and breadth of service contexts in which e-KTP was used in the preceding year.

Attitudinal and perception items were measured using a five-point Likert scale starting at 1 (very low) and ending at 5 (very high), while factual and experience-based items were measured using categorical or frequency response formats as appropriate.

4.3.4 Analysis approach

The quantitative analysis followed a sequential analytical framework comprising data preparation, descriptive analysis, cross tabulation, and structural equation modeling. Survey responses were first subjected to data cleaning and preparation, including consistency checks, treatment of missing values, recoding of categorical and Likert-scale responses, reverse coding of negatively worded items, and harmonization of response categories across the dataset.

Descriptive and inferential statistical analyses were conducted using Stata and IBM SPSS software. Descriptive statistics, including frequencies, percentages, means, and standard deviations, were computed to summarize respondents' demographic characteristics, national digital ID awareness, usage patterns, perceptions, and experiences. Inferential statistical analyses, including tests of association and group differences, were performed to examine relationships among key study variables and test study hypotheses. Depending on the nature of the variables, appropriate statistical tests, including Chi-square tests of association, Fisher's Exact tests, independent-samples t-tests, and other relevant non-parametric tests, were employed. Statistical significance was assessed at conventional significance levels ($p < 0.05$).

To empirically validate the proposed extension of TAM, Partial Least Squares Structural Equation Modeling (PLS-SEM) was employed using RStudio. The PLS-SEM analysis followed a two-stage approach. First, the measurement model was assessed to examine the reliability and validity of the latent constructs. Internal consistency reliability was evaluated using Cronbach's Alpha, Composite Reliability (CR), and rhoA, while convergent validity was assessed through indicator loadings and Average Variance Extracted (AVE). Discriminant validity among constructs was examined using the Heterotrait-Monotrait (HTMT) ratio, where values below the recommended threshold of 0.85 indicated adequate discriminant validity. Potential multicollinearity among indicators was assessed using Variance Inflation Factors (VIF). All VIF values ranged from 1.00 to 1.75, well below the recommended threshold of 3.3, indicating the absence of multicollinearity among indicators. Subsequently, the structural model was estimated to test the hypothesized relationships among constructs within the extended TAM framework. Structural path coefficients (β), coefficients of determination (R^2), and effect directions were estimated. The statistical significance of the hypothesized relationships was assessed through bootstrapping procedures, generating t-statistics, p-values, and confidence intervals. The structural model results enabled the identification of key determinants influencing attitudes, behavioral intentions, and actual usage of e-KTP.

In addition, the qualitative data obtained through in-depth interviews and focus group discussions were analyzed using Atlas.ti software. The analysis followed a thematic analysis approach. Interview transcripts were first reviewed, cleaned, and imported into Atlas.ti for systematic analysis. The transcripts were then subjected to an iterative coding process. Initially, relevant text segments were assigned descriptive codes and labels that reflected respondents' experiences, perceptions, challenges, and suggestions regarding e-KTP. Through repeated review and comparison, similar codes were grouped into broader categories and patterns. Subsequently, these categories were synthesized to identify overarching themes and sub-themes emerging from the data. The thematic analysis facilitated the identification of differences in experiences, and contextual factors influencing the adoption of e-KTP and its use across different respondent groups. The qualitative findings were triangulated with the quantitative results to provide a comprehensive and nuanced understanding of user experiences, perceptions, and barriers with e-KTP.

5 Findings

This section presents empirical findings through the constructs of the proposed extension to the Technology Acceptance Model for e-KTP. For each construct, quantitative findings from the survey (n=1,565) are presented first, followed by qualitative insights from in-depth interviews and focus group discussions. Direct participant quotes appear in italics.

5.1 Perceived Ease of Use

Respondents generally perceived e-KTP as easy to use. Ninety-four percent respondents reported a positive to very positive perception of the e-KTP's ease of use, and 88 percent described their experience with e-KTP registration as very good and without problems. These responses were broadly consistent across both genders and age groups, suggesting that ease of use of e-KTP was not concentrated among a demographic segment but was experienced across the sample. This perception was also reflected in respondents' preference for using e-KTP across service contexts. Sixty-nine percent of respondents preferred e-KTP for government services, while 72 percent preferred it for the private sector services such as bank account opening, SIM card registration, and employment verification. When asked why they chose e-KTP over other forms of identification, respondents cited convenience, ease of carrying the e-KTP card, faster verification, wide acceptance, and higher trust compared with alternatives.

Qualitative findings indicate that users valued e-KTP because it was perceived as consistent and predictable across service settings. Respondents associated ease of use not only with convenience but also with reduced uncertainty during identity verification. This was particularly important in high-stakes settings such as financial services and healthcare enrolment, where failed verification could delay or obstruct access.

5.2 Perceived Usefulness

Respondents demonstrated a clear understanding of the usefulness of e-KTP. Eighty-six percent associated it with access to government services and subsidies, and 75 percent associated it with access to private services. Respondents were able to distinguish e-KTP from conventional paper-based identity documents. Sixty percent cited e-KTP's role as a single credential accepted across multiple government and private-sector services, 57 percent cited its biometric authentication capability, and 56 percent cited the storage of biometric data, such as fingerprints and photographs as key distinguishing factors. Only seven percent saw no meaningful difference between paper IDs and e-KTP.

Respondents also reported service-related gains from using e-KTP. Sixty-five percent of respondents said e-KTP enabled faster access to services than conventional IDs, with 41 percent describing the improvement as significantly faster. Forty-four percent reported reduced effort, fees, or travel required to access services, whereas 53 percent reported no change. Notably, these efficiency gains were not uniformly distributed. Urban respondents reported faster access, reflecting better connectivity and streamlined processes at urban service points. The most direct measure of perceived usefulness was whether e-KTP worked when presented. Ninety-seven percent of respondents reported never having been denied a service when using e-KTP in the past year.

More than half of respondents, 54 percent, associated e-KTP with faster and reliable identity verification. Qualitative interviews reinforce this interpretation. One participant

quoted, *"If I show my e-KTP, I know I will get the service."* Older respondents defined usefulness in terms of a reduced need to carry multiple documents, a reduced risk of being turned away, and a reduced uncertainty about whether a credential would be accepted.

5.3 Trust

Trust in e-KTP seems to be high. Eighty percent of respondents expressed high or complete trust that e-KTP would work reliably, and 78 percent expressed high or complete trust in the government to manage and use their e-KTP data. These findings were broadly consistent across genders and age groups, indicating that trust was not concentrated to any demographic category. The strength of government trust is significant, because it indicates that e-KTP has acquired institutional legitimacy.

Trust in private-sector entities was positive but marginally lower. Sixty-five percent of respondents reported high or complete trust in banks and financial institutions, while 61 percent reported the same for telecom providers. The gap between trust in government (78 percent) and trust in the private sector (61-65 percent) suggests users do not automatically transfer their trust in the state as a data custodian to the private-sector intermediaries that rely on e-KTP for identity verification. The positive perception of security also reinforced the overall trust. Sixty-six percent of respondents considered e-KTP more secure than paper-based IDs.

Qualitative interviews provide further insight into the basis of trust. Respondents frequently associated e-KTP's security with its biometric features, noting that biometrics made the credential more difficult to misuse. One participant stated that *"the use of biometrics makes e-KTP more secure."* At the same time, several respondents expressed concerns about fraud, especially in relation to fintech applications, citing exposure to fraudulent loan offers and unsafe links. One participant, a 39-year-old woman, explained why she chose to visit a Dukcapil office rather than update her e-KTP online: *"I heard about people pretending to be Dukcapil officers and sending fake links. I didn't trust it, so I went directly to the office."* Urban respondents expressed higher concerns about data misuse than rural respondents, with 70 percent of urban respondents reporting such concern compared with 53 percent of rural respondents. This pattern may reflect greater exposure to digital fraud in urban settings.

5.4 Attitude toward Using e-KTP

Respondents' attitudes toward using e-KTP were generally positive. Seventy-two percent of respondents were very or completely confident in their ability to use e-KTP, including through biometric and chip-based identity verification. Only 6 percent reported low or limited confidence. These proportions were consistent across gender and age groups, suggesting that positive attitudes toward e-KTP were widely shared. Perceptions of security and reliability as highlighted above underpinned these attitudes.

The attitude towards using e-KTP has changed positively over time. Thirty-nine percent of respondents stated that their confidence in using e-KTP has increased from their first usage, while 59 percent stated that it had remained stable. Taken together, 98 percent of users had either maintained or strengthened their positive attitude towards using e-KTP over time.

5.5 Regulatory Awareness

Sixty-seven percent of respondents reported fearing that their e-KTP data could be misused by others. It seems that it is partly coming from respondents limited awareness and understanding of the rules and remedies that would apply if misuse occurred. Forty-nine percent of respondents reported that they were entirely unaware of any rules governing the management or sharing of their e-KTP data, while only 20 percent reported being fully informed.

Notably, awareness varies by age. Among respondents aged 51 and above, 62 percent reported that they were unaware of relevant regulations, compared with 43 percent in the 17-30 cohort. This age gradient is important because older respondents may be less equipped to navigate digital environments in which identity data is increasingly used and shared.

The redress gap further compounds the low regulatory awareness. Forty-one percent of respondents reported that they did not know any proper channel to raise a complaint, while 31 percent believed channels existed but could not identify them. Only 28 percent respondents reported that they clearly knew where and how to seek redress. Similarly, in relation to operational failures, 36 percent of respondents reported that they could not identify any channel for raising concern if e-KTP verification failed.

Qualitative findings suggest that respondents who expressed concerns about data misuse did not generally connect those concerns to specific redress mechanisms. Instead, many relied on institutional trust, believing the government, as the issuing authority, would act responsibly.

5.6 Behavioral Intention

Respondents displayed strong behavioral intention to continue using e-KTP. Forty-one percent of respondents expected their use of e-KTP to increase over the next 12 months, while 57 percent expected their use to remain constant. Moreover, 85 percent of respondents said they would recommend e-KTP to others in their community. When respondents recommended e-KTP to family, neighbors, and colleagues, they reinforce the perception that e-KTP works reliably across settings. Ninety-four percent of respondents believed e-KTP would become indispensable in future.

Qualitative discussions indicated continued use of e-KTP is a considered choice between other identity documents. Respondents described e-KTP as a credential that made

everyday transactions easier. As one respondent stated, *"Yes, once you have it, everything becomes easier."* For most respondents, the intention to keep using e-KTP rested on their personal experience.

5.7 Mandatory Adoption

The data suggests that e-KTP has moved beyond mere compliance. Twenty-three percent of respondents stated that they used e-KTP for government services primarily because they felt it was mandatory, and a similar percentage of respondents reported the same for private-sector services. However, when asked hypothetically, if e-KTP were to be mandated, would it improve their experience, 66 percent said it would make the experience better, while 33 percent stated that it would make no difference. This suggests that while many users may initially have adopted e-KTP because of perceived institutional requirements, repeated successful use built the familiarity and confidence that now sustains voluntary preference.

Qualitative interviews reinforced this retrospective acceptance. Respondents who recalled initial friction often described those early difficulties as outweighed by the e-KTP's practical utility in daily life.

5.8 Social Acceptance

Social acceptance of e-KTP within the service ecosystem is high. Ninety-one percent of respondents agreed or strongly agreed that e-KTP is adequately recognized and accepted by the service providers they use. This near-universal acceptance reflects the degree to which e-KTP is recognized and accepted by service providers for identity verification. Qualitative Interviews highlighted that widespread acceptance reduced arbitrary decision-making by service providers, giving users greater confidence that the outcome of an identity verification interaction was not subject to the discretion of individual staff. In this context, wider acceptance is also partly interlinked with perceived usefulness.

At the social level, 99 percent of respondents reported that holding an e-KTP had improved their sense of inclusion in society. Among those who felt more included, 67 percent attributed this to feeling more recognized and accepted, 63 percent to greater personal confidence, and 32 percent to improved access to public benefits. Perceptions of fairness further reinforce this interpretation. Sixty-nine percent of respondents said the e-KTP system treated citizens very fairly, while 23 percent said it treated citizens fairly with some exceptions. Only 8 percent reported unfair or inconsistent treatment.

5.9 Actual Use

All 1,565 respondents used e-KTP at least once in the preceding 12 months. Seventy-nine percent used it one to four times, 14 percent used it five to eight times, and the remaining

seven percent used it more than eight times annually. Reported use included healthcare, financial services, telecommunications, social assistance, elections, labor registration, and education, with healthcare and financial services being the most common sectors of e-KTP use.

Ninety percent of respondents had used a show-of-card as a verification method in the past year, compared with 36 percent who had used fingerprints, 28 percent who had used face recognition, and only 4 percent who had used a chip or card reader. Ninety-six percent described their overall experience with e-KTP verification at service points as generally quick and reliable. This positive experience, however, appears to be driven primarily by the simplicity and predictability of show-of-card verification rather than by the more advanced biometric and electronic capabilities of the credential. When biometric identity verification failed, 58 percent of respondents said staff reverted to show-of-card verification to avoid delays and service disruption.

Qualitative findings help explain this pattern. Respondents described show-of-card verification as simple, fast, and predictable. Frontline staff appear to have internalized this expectation, treating biometric options as optional enhancements rather than standard procedure. The predictability of show-of-card verification had shaped a behavioral norm around carrying the physical card.

5.10 Structural Model Results

The structural model, estimated using PLS-SEM with bootstrapping across 5,000 subsamples, identified the pathways through which proposed extension to TAM constructs shaped attitudes, behavioral intention, and actual use of e-KTP. All VIF values ranged from 1.02 to 1.75, well below the recommended threshold of 3.3, confirming the absence of multicollinearity. HTMT ratios were within acceptable bounds for most construct pairs; ATT–TRUST (0.875) and ATT–SA (0.873) approached the upper threshold, reflecting the conceptual proximity between attitude, trust, and social acceptance in a system where institutional confidence and social norms are deeply intertwined.

Trust was the dominant predictor of attitude (β = 0.66, p < 0.001, R^2 = 0.85; Figure 3), accounting for the largest share of explained variance across all dependent constructs in the model. Perceived ease of use and perceived usefulness each contributed significant but smaller effects on attitude (β = 0.21 and 0.19, p < 0.05), indicating that functional perceptions reinforced but did not drive attitudinal formation. Attitude and perceived usefulness were directionally positive but non-significant predictors of behavioral intention (β = 0.41, p = 0.230; β = 0.35, p = 0.250), a pattern consistent with mandated adoption contexts in which legal and social requirements reduce the explanatory power of individual attitudinal variables overstated intention. Behavioral intention reached significance in predicting actual use (β = 0.17, p < 0.05), alongside social acceptance (β = 0.10, p < 0.01) and mandatory adoption (β = 0.08, p < 0.01).

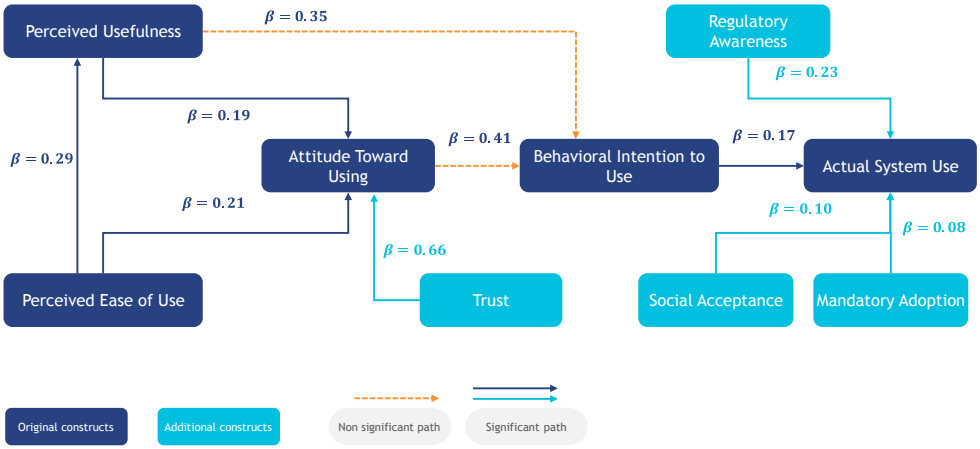

Figure 3: Results from PLS-SEM.

One of the most consequential findings is the highly significant direct path from regulatory awareness to actual use (β = 0.23, p < 0.001): awareness of data governance frameworks predicted what users did, not merely what they intended to do. Taken together, the model explained 85 percent of the variance in attitude, 46 percent in behavioral intention, and 17 percent in actual use.

These results identify two analytically distinct dynamics. The first is an attitudinal pathway in which trust shapes how users feel about the national digital ID system, which in turn informs their intentions. The second is a behavioral pathway in which regulatory awareness, social acceptance, and mandatory adoption drive actual use, bypassing stated intention. The gap between the two pathways has a direct implication: building user confidence and positive attitudes is necessary but may not be sufficient for translating that confidence into consistent, secure use.

6 Discussion

Building on the empirical findings, this study interprets the acceptance of national digital identity through the Extended Technology Acceptance Model (Extended TAM), which incorporates institutional and ecosystem-level factors alongside traditional technology acceptance constructs. The study findings and structural model results bring out many key discussion points on various themes: trust and predictability in acceptance and use; regulatory awareness and user safety; mandatory adoption, social acceptance, and trusted digital transition; and the pathway from coverage of national digital ID to its online use.

6.1 Trust and Predictability in Acceptance and Use

The study extends the technology acceptance literature by showing that adoption of national digital identity cannot be explained by perceived usefulness and perceived ease of use alone. In the case of Indonesia's national digital identity system, trust had the strongest effect on attitudes toward national digital identity. This finding supports e-government scholarship that identifies trust in government as a key determinant of citizen adoption of digital public services (Carter and Bélanger 2005), while extending that argument to the context of national digital identity.

The findings also contribute to digital identity literature by further showing that trust is both institutional and experiential. Users trust the system partly because it is issued by a recognized public authority, but that trust is sustained because the identity credential usually works when presented. Predictability therefore emerged as more than a usability attribute. It functioned as an experiential basis of trust, especially as identity verification extends into online service delivery mechanisms. This distinction is important because institutional legitimacy alone may be insufficient if users encounter frequent identity verification failures or inconsistent access to services. A national digital ID that works reliably across service points generates a stronger form of confidence than one that works only intermittently.

6.2 Regulatory Awareness and User Safety

The findings also contribute to privacy, data protection, and platform governance literature, which highlights the risks that arise when national digital identity systems are linked across multiple public and private services (Bennett and Raab 2017; Haggerty and Ericson 2000; Lyon 2009). Respondents expressed relatively high trust in banks and telecom providers, but their trust in private-sector actors was lower than their trust in government. This distinction matters because national digital identity ecosystems increasingly depend on the private sector service providers that verify, request, process, or store identity-related information.

Limited regulatory awareness intensifies this trust gap. Many respondents feared data misuse but did not know the rules governing data sharing or the channels available for complaint and redress. This suggests that trust in the state may not automatically translate into confident use of national digital ID, especially in online transactions.

As national digital identity becomes embedded in financial services, telecommunications, and platform-based transactions, governance must extend beyond the issuing authority. Clear rules and their communication to residents are needed on what data service providers may access, how long they may retain it, how consent is obtained, and what remedies are available in cases of misuse, fraud, or identity verification failure.

6.3 Mandatory Adoption, Social Acceptance, and Trusted Digital Transition

National digital identity systems complicate standard technology adoption theory because they are often not fully voluntary. The findings show that mandatory adoption can create initial use, but sustained acceptance depends on convenience, recognition, fairness, and inclusion. Mandatory use may or may not lead to trust. The trusted online use of national digital identity requires preserving the predictability that currently underpins confidence in e-KTP while making online transactions.

6.4 Pathway from Coverage of National Digital ID to Its Online Use

The findings suggest that coverage of national digital ID alone doesn't reflect its usage and maturity. e-KTP has wide coverage and strong social acceptance, yet everyday identity verification still relies on physical show-of-card verification rather than biometric or chip-card verification. Show-of-card verification is familiar, fast, and trusted in face-to-face settings. The transition to online use of national digital ID is therefore not merely a technical migration from electronic card to mobile application; it is a structural transition that requires changes in user habits, service providers' delivery mechanisms, and expectations about what counts as reliable identity verification.

7 Conclusion

The paper shows that national digital identity systems should be understood as socio-technical trust infrastructures. Their adoption depends not only on system design or legal mandate, but also on trust, acceptance at service points, regulatory awareness, and other related factors. For Indonesia, the next phase of national digital identity development will depend on whether the confidence built around the physical credential can be translated into equally reliable and trusted online digital ID. These findings have important implications for the broader literature on national digital identity systems, particularly in majority world countries where digital literacy, smartphone access, and service infrastructure vary widely.

As service providers increasingly verify, process, and retain identity-related information, clear rules governing data access, consent, retention, accountability, and user remedies become essential for sustaining trust.

7.1 Limitations

This study is broadly subject to three limitations. First, the sample composition is skewed toward low- and middle-income (LMI) segments (97 percent of respondents, self-reported data), which may over-represent lower-income perspectives and limit generalization. Second, the study relies on self-reported perceptions and usage, which may be affected by recall bias. Third, the cross-sectional design limits causal inference.

References

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. 2015. “Privacy and Human Behavior in the Age of Information.” *Science* 347 (6221): 509–14. https://doi.org/10.1126/science.aaa1465.

Bennett, Colin J., and Charles D. Raab. 2017. *The Governance of Privacy: Policy Instruments in Global Perspective.* London: Routledge.

Brown, Sue A., Anne P. Massey, Mitzi M. Montoya-Weiss, and James R. Burkman. 2002. “Do I Really Have To? User Acceptance of Mandated Technology.” *European Journal of Information Systems* 11 (4): 283–95. https://doi.org/10.1057/palgrave.ejis.3000438.

Carter, Lemuria, and France Bélanger. 2005. “The Utilization of E-Government Services: Citizen Trust, Innovation and Acceptance Factors.” *Information Systems Journal* 15 (1): 5–25. https://doi.org/10.1111/j.1365-2575.2005.00183.x.

Cavoukian, Ann. 2011. *Privacy by Design: The 7 Foundational Principles.* Information and Privacy Commissioner of Ontario.

Clark, Julia, and Conrad Daly. 2019. *Digital ID and the Data Protection Challenge: Practitioner’s Note.* World Bank. https://doi.org/10.1596/32629.

Cochran, William G. 1977. *Sampling Techniques.* 3rd ed. New York: Wiley.

Colesca, Sofia Elena. 2009. “Understanding Trust in E-Government.” *Engineering Economics* 63 (3): 7–15. https://doi.org/10.5755/j01.ee.63.3.11637.

Davis, Fred D. 1989. “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology.” *MIS Quarterly* 13 (3): 319–40. https://doi.org/10.2307/249008.

Desai, Vyjayanti T., Jonathan Marskell, Georgina Marin, and Minita Varghese. 2023. “How Digital Public Infrastructure Supports Empowerment, Inclusion, and Resilience.” World Bank Blogs, March 15, 2023. https://blogs.worldbank.org/en/digital-development/how-digital-public-infrastructure-supports-empowerment-inclusion-and-resilience.

Digital Trust & Safety Partnership. 2025. *Best Practices Framework.* Digital Trust & Safety Partnership. https://dtspartnership.org/wp-content/uploads/2025/07/DTSP_Best_Practices_Framework_2025.pdf.

Gefen, David, Elena Karahanna, and Detmar W. Straub. 2003. “Trust and TAM in Online Shopping: An Integrated Model.” *MIS Quarterly* 27 (1): 51–90. https://doi.org/10.2307/30036519.

Gillespie, Tarleton. 2018. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media.* New Haven, CT: Yale University Press. https://doi.org/10.12987/9780300235029.

Gorwa, Robert, Reuben Binns, and Christian Katzenbach. 2020. "Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance." *Big Data & Society* 7 (1). https://doi.org/10.1177/2053951719897945.

Haggerty, Kevin D., and Richard V. Ericson. 2000. "The Surveillant Assemblage." *The British Journal of Sociology* 51 (4): 605–22. https://doi.org/10.1080/00071310020015280.

Jabbour, Abdallah, and Christopher Tullis. 2024. "Digital Identity: Building the Foundations of Digital Public Infrastructure in Lebanon." World Bank Blogs, June 3, 2024. https://blogs.worldbank.org/en/arabvoices/digital-identity-building-the-foundations-of-digital-public-infrastructure-in-lebanon.

Kayyali, Dia, and Jasmine Mithani. 2025. "Age Verification Is Locking Trans People Out of the Internet." Tech Policy Press, December 8, 2025. https://www.techpolicy.press/age-verification-is-locking-trans-people-out-of-the-internet/.

Lyon, David. 2009. *Identifying Citizens: ID Cards as Surveillance.* Cambridge: Polity.

Maple, Carsten, Gregory Epiphaniou, and Nagananda K. Gurukumar. 2021. *Facets of Trustworthiness in Digital Identity Systems.* Technical Briefing. The Alan Turing Institute. https://www.turing.ac.uk/sites/default/files/2021-05/technical_briefing-facets_of_trustworthiness_in_digital_identity_systems.pdf.

Marin, Georgina, and Robert Palacios. 2022. *The Role of Digital in the COVID-19 Social Assistance Response.* World Bank. https://doi.org/10.1596/38104.

Masiero, Silvia. 2023. "Digital Identity as Platform-Mediated Surveillance." *Big Data & Society* 10 (1). https://doi.org/10.1177/20539517221135176.

Mayer, Roger C., James H. Davis, and F. David Schoorman. 1995. "An Integrative Model of Organizational Trust." *Academy of Management Review* 20 (3): 709–34. https://doi.org/10.5465/amr.1995.9508080335.

Metz, Anna, Claire Casher, and Julia Clark. 2024. *ID4D Global Dataset 2021: Volume 2—Digital Identification Progress & Gaps.* World Bank. https://doi.org/10.1596/41076.

Muralidharan, Karthik, Paul Niehaus, and Sandip Sukhtankar. 2022. "Integrating Biometric Authentication in India's Welfare Programs: Lessons from a Decade of Reforms." *India Policy Forum* 18 (1): 139–72.

Nguyen, Trang Thi Uyen, Phuong Van Nguyen, Hien Thi Ngoc Huynh, Demetris Vrontis, and Zafar U. Ahmed. 2024. "Identification of the Determinants of Public Trust in E-Government Services and Participation in Social Media Based on Good Governance Theory and the Technology Acceptance Model." *Journal of Asia Business Studies* 18 (1): 44–61. https://doi.org/10.1108/JABS-04-2023-0160.

Sahatatua, Richart, Yenrizka Gusmaria, I Ketut Astawa, Ade Maman Suherman, Try Setiady, and Wahyu Donri Tinambunan. 2024. "Cyber Law Analysis of E-KTP Data Leakage: A Case Approach of 102 Million KTP Data Allegedly Leaked from the Ministry of Social Affairs to a Hacker Forum." *Journal of Multidisciplinary Academic and Practice Studies* 2 (3): 151–61. https://doi.org/10.35912/jomaps.v2i3.2219.

Statelessness Encyclopedia Asia Pacific. 2026. "Indonesia," January 29, 2026. Accessed August 7, 2026. https://seap.nationalityforall.org/digital-id/regional-overview/southeast-asia/indonesia/.

Temoshok, David, Diana Proud-Madruga, Yee-Yin Choong, Ryan Galluzzo, Sarbari Gupta, Connie LaSalle, Naomi Lefkovitz, and Andrew Regenscheid. 2025. *Digital Identity Guidelines.* NIST SP 800-63-4. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-4.

Venkatesh, Viswanath, and Fred D. Davis. 2000. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies." *Management Science* 46 (2): 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926.

Venkatesh, Viswanath, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. 2003. "User Acceptance of Information Technology: Toward a Unified View." *MIS Quarterly* 27 (3): 425–78. https://doi.org/10.2307/30036540.

World Bank. 2019. *ID4D Practitioner's Guide: Version 1.0.* 137292. World Bank. https://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf.

———. 2023. *ID for Inclusive Service Delivery and Digital Transformation in Indonesia: Project Appraisal Document.* PAD5112. World Bank.

———. 2025. *ID for Inclusive Service Delivery and Digital Transformation in Indonesia (P175218): Implementation Status & Results Report.* ISR03410. World Bank.

———. n.d. "Types of ID Systems." Identification for Development Practitioner's Guide. Accessed August 7, 2026. https://id4d.worldbank.org/guide/types-id-systems.

Zainudin. 2025. "Digital ID Policy in Support of Digital Transformation in Indonesia." *Jurnal Bina Praja* 17 (1): 1–18. https://doi.org/10.21787/jbp.17.2025.1-18.

Authors

Anshul Pachouri is Global Lead of Technology Policy & Innovation at MSC (MicroSave Consulting). He works at the intersection of emerging technologies, innovation, and social good. Email: anshul.pachouri@microsave.net.

Abhishek Raj is a Manager at MSC, where he works on technology policy, digital public infrastructure, and responsible innovation. He has led and contributed to DPI research and strategy engagements across digital identity, trusted data-sharing systems, data protection and privacy, and artificial intelligence. Email: abhishek.raj@microsave.net.

Kushagra Harshavardhan is a Manager at MSC. His work spans digital public infrastructure, government-to-person (G2P) programs, and social protection systems. Email: kushagra.harshavardhan@microsave.net.

Positionality Statement

The authors have lived their entire lives in the developing world and have been working in the area of national digital ID and inclusion in Asia and Africa for the past many years. As part of MSC, the authors have led multi-country research studies on building and scaling national digital identity systems and trusted data-sharing systems for pro-poor use cases. The research primarily focuses on low- and middle-income countries, examining the contextual, institutional, and capacity dimensions of digital transformation.

The authors have worked closely with the national identity authorities and other government agencies on the design and scale-up of national digital ID systems, combining analytical rigor with implementation-oriented insights. The authors have also contributed policy papers and book chapters on technology policy and digital-led development for academic and multilateral institutions.

Acknowledgments

The authors thank Ashish Singh, Assistant Manager, MSC (MicroSave Consulting), for his valuable support with data analysis. The authors also acknowledge use of AI tools only for language refinement.

Data Availability Statement

Replication files are available at: N/A

Funding Statement

This research was funded by the Gates Foundation.

Ethical Standards

Participation in the study was voluntary, and informed consent was obtained from all respondents before data collection. The study did not involve minors or specifically target any sensitive or vulnerable groups. No personally identifiable information was collected. All responses were anonymized before analysis and were used exclusively for research purposes.

Keywords

National digital identity; digital identity adoption; institutional trust; technology acceptance model; Indonesia.