Digital Government Branding and Public Trust: Empirical Evidence from Indonesia's Go.id Domain

Maykada Harjono Kurniawan[1], Moh. Wildan[2], and Lisnawati Lisnawati[3]

[1,2,3] Indonesia University of Education, Bandung, Indonesia
maykada@upi.edu

Abstract. This study investigates how digital government branding through Indonesia's of-ficial 'go.id' domain impacts public trust in e-government services. Despite growing digital transformation initiatives, trust in government online platforms remains underexplored, particularly regarding the strategic value of official do-main identity as a branding instrument. Grounded in Brand Identity Theory, Trust Theory, Strategic Public Marketing, and the Technology Acceptance Model, the research examines how institutional credibility and information security shape perceived usefulness, which subsequently drives public trust. A quantitative ap-proach was employed, using Partial Least Squares Structural Equation Modeling (PLS-SEM) to analyze data from 150 government administrators managing go.id-based public services across ministries, agencies, and local authorities in Indonesia. Results confirm that institutional credibility and information security significantly influence perceived usefulness, while perceived usefulness strongly predicts public trust. Institutional credibility emerges as the dominant branding factor, indicating that government legitimacy and reputation outweigh technical security in shaping public perception of digital services. These findings offer practical implications for policymakers seeking to leverage domain identity as a strategic branding asset in building credible, secure, and citizen-oriented digital governance.

Keywords: Digital Government Branding, Public Trust, E-Government, Institutional Credibility, PLS-SEM.

1 Introduction

In the digital era, trust in government is increasingly shaped not only by policy outcomes but also by how public services are delivered online. As governments accelerate digital transformation, the credibility of digital channels has become vital in influencing public trust [1, 2]. In Indonesia, the official government domain 'go.id' functions as a central digital identity for ministries, agencies, and local governments, with 3,570 active domains as of April 2025 [3]. However, digital trust remains a challenge — the National Cyber and Crypto Agency (BSSN) reported that 23% of the 5,780 web de-

© The Author(s) 2026
R. Hurriyati et al. (eds.), *Proceedings of the 10th Global Conference on Business, Management, and Entrepreneurship (GCBME 2025)*, Advances in Economics, Business and Management Research 407,
https://doi.org/10.2991/978-94-6239-819-1_27

facement cases in 2024 targeted government domains [4], underscoring the need to examine 'go.id' not only as technical infrastructure but as a symbol of institutional legitimacy [5, 6].

Despite growing digital transformation initiatives, trust in government online platforms remains underexplored, particularly regarding the strategic value of official domain identity as a branding instrument. This gap is especially evident in the context of digital government branding, where domain names function not only as technical infrastructure but also as symbols of institutional identity and credibility [7, 8]. This study examines how institutional credibility and information security contribute to the perceived usefulness of go.id-based services, and how this subsequently influences public trust. The research integrates four theoretical frameworks: Brand Identity Theory [7], which emphasizes consistent brand image in fostering trust; Trust Theory [9], which identifies ability, integrity, and benevolence as core trust components; Strategic Public Marketing [8], which frames institutional branding as a driver of citizen trust; and the Technology Acceptance Model [10], in which perceived usefulness mediates the relationship between system quality and public trust.

Recent empirical studies affirm the proposed relationships. Taufiqurokhman et al. [11] found that e-service quality significantly shapes public trust in Indonesian e-government platforms, while Kanaan et al. [12] demonstrated that security and privacy factors directly influence citizens' trust and intention to use government digital services. Hooda et al. [13], through a meta-analytic SEM of 67 prior studies, further established that information quality, service quality, and system quality significantly influence e-government trust, with system use mediating the effect of trust on future usage intention. Lee-Geiller [14] similarly confirmed that e-government effectiveness positively associates with public trust.

Building on this evidence, Luo et al. [15] and Kala et al. [16] confirm that perceived usefulness serves as a key mediator between system quality and public trust, while Duan and Dong [17] and Pham et al. [18] further establish that perceived benefits and service trustworthiness are critical drivers of citizen engagement and loyalty in e-government platforms. Based on these foundations, three hypotheses are proposed: **H1**: Institutional Credibility positively influences Perceived Usefulness; **H2**: Information Security positively influences Perceived Usefulness; and **H3**: Perceived Usefulness positively influences Public Trust in e-government services.

2 Research Methods

A quantitative research design was employed using Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS 4.0, suitable for testing complex models with multiple constructs and mediating effects [19]. The model was evaluated in two stages: (1) measurement model assessment covering reliability, convergent validity, and discriminant validity; and (2) structural model assessment covering path coefficients, R-squared values, and hypothesis testing.

Research constructs were operationalized based on Brand Identity Theory, Trust Theory, Strategic Public Marketing, and the Technology Acceptance Model, with indicators derived from 10 measurement items as summarized in Table 1.

Table 1. Variables, Indicators, and Theoretical Foundations

Variable Name	Indicators	Theoretical Foundations
Institutional Credibility (IC)	- Legitimacy of government - Reputation of institution - Compliance with regulations	Brand Identity Theory, Strategic Public Marketing
Information Security (IS)	- Cyber threat mitigation - Security certifications - Protection of personal data	Trust Theory
Perceived Usefulness (PU)	- Efficiency benefits - Alignment with public needs	Technology Acceptance Model (TAM)
Public Trust (PT)	- Intention to reuse - Willingness to recommend	Trust Theory

Source: Author's work

Data were collected from May 22–27, 2025, via an online questionnaire distribut-ed to government institution staff, particularly from regional Communication and Information Technology Departments (Dinas Kominfo) across Indonesia. From 155 responses received, 150 valid responses were retained after excluding 5 unrelated submissions. Respondents consisted of civil servants (75%), contract government employees (7%), and other employment statuses (17%). The instrument employed a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree) across 20 state-ments.

3 Results and Discussion

3.1 Measurement Model Evaluation

Cronbach's Alpha (CA) and Composite Reliability (CR) values exceed 0.70, confirming internal consistency, while Average Variance Extracted (AVE) values above 0.50 confirm convergent validity. The Fornell-Larcker Criterion [20] further confirms adequate discriminant validity, with each construct's √AVE exceeding its correlations with other constructs. All constructs meet the criteria for reliability and validity, as summarized in Table 2.

Table 2. Summary of Measurement Model Evaluation

Construct	CA	CR	AVE	Interpretation
Institutional Credibility	0.885	0.890	0.594	Reliable and valid
Information Security	0.882	0.890	0.590	Reliable and valid

Construct	CA	CR	AVE	Interpretation
Perceived Usefulness	0.826	0.834	0.742	High reliability and strong convergent validity
Public Trust	0.755	0.787	0.674	Reliable and valid

Source: Autor's work

3.2 Structural Model and Hypothesis Testing

The R^2 value for Perceived Usefulness is 0.625, indicating that Institutional Credibility and Information Security jointly explain 62.5% of its variance. The R^2 value for Public Trust is 0.537, reflecting moderate-to-substantial predictive power based on Chin's [19] criteria. All hypothesized paths are positive and statistically significant at a 95% confidence level (t-statistic > 1.96, $p < 0.05$), as presented in Table 3.

Table 3. Structural Model Evaluation and Hypothesis Testing Results

Path	Coefficient	T-Statistic	p-value	Result
H1: Institutional Credibility → Perceived Usefulness	0.667	12.167	0.000	Supported
H2: Information Security → Perceived Usefulness	0.201	3.584	0.000	Supported
H3: Perceived Usefulness → Public Trust	0.733	14.741	0.000	Supported

Source: Author's work

The path diagram in Figure 1 illustrates the structural relationships among the four constructs, confirming the dominant role of Institutional Credibility over Information Security in driving Perceived Usefulness, and the central mediating function of Perceived Usefulness in predicting Public Trust.

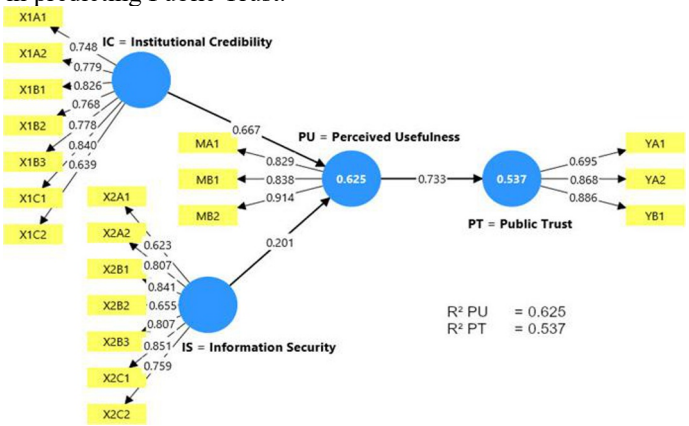

Fig. 1. Path analysis of the model with variable IC, IS, PU, and PT.

3.3 Discussion

The findings confirm that institutional credibility is the dominant driver of perceived usefulness (β = 0.667, t = 12.167), suggesting that government legitimacy and reputation play a more decisive role than technical security in shaping citizens' perception of digital government value. This strong effect indicates that citizens primarily evaluate go.id-based services through the lens of institutional authority and compliance, rather than technical features alone. This is consistent with prior research demonstrating that institutional reputation is a primary driver of e-government trust [2, 14], and that accountability and responsiveness are foundational to sustaining public engagement with digital platforms [11, 15].

Information security, while comparatively weaker (β = 0.201, t = 3.584), remains statistically significant and cannot be overlooked — a pattern similarly observed in studies on security and privacy in e-government adoption [12, 18]. The R^2 value for Perceived Usefulness (0.625) confirms that both constructs jointly provide substantial explanatory power. Most importantly, perceived usefulness emerges as a robust mediator of public trust (β = 0.733, t = 14.741, R^2 = 0.537), supporting TAM and Trust Theory [15, 16] and affirming that citizens are more likely to trust digital government platforms when they perceive tangible benefits from their use [17, 18]. Overall, these findings position the ‘go.id’ domain as a strategic digital brand asset whose credibility and security collectively shape civic trust in e-government services [1, 5].

4 Conclusions

This study demonstrates that the ‘go.id’ domain plays a strategic role as a govern-ment digital brand asset in fostering public trust in digital government services. Insti-tutional credibility emerges as the dominant factor shaping perceived usefulness, indicating that government legitimacy and reputation are more influential than tech-nical security in determining how citizens perceive the value of digital government platforms. Perceived usefulness is confirmed as a significant mediator between insti-tutional credibility, information security, and public trust, consistent with TAM-based e-government studies. These findings affirm that the ‘go.id’ domain functions not merely as an administrative web address, but as a digital identity symbol that en-hances legitimacy, service value, and civic confidence in government digital systems.

These results highlight the importance of strengthening institutional credibility and professionalism as the foundation of government digital strategy. Although information security exerts a comparatively lower influence, it remains critical given escalating cyber threats targeting government domains. Therefore, integrating robust security policies with effective institutional communication is essential. The ‘go.id’ do-main should be strategically leveraged as a national digital branding element, with consistent and professional governance maintained across all government agencies.

References

1. Djatmiko, G.H., Sinaga, O., Pawirosumarto, S.: Digital Transformation and Social Inclusion in Public Services. Sustainability **17**(7), Article 2908 (2025)
2. Sharma, S., Kar, A.K., Gupta, M.P.: Building Accountability in E-Government Services. Australasian Journal of Information Systems **29**, 1–28 (2025)
3. Kementerian Komunikasi dan Digital Republik Indonesia: Layanan Nama Domain Instansi Pemerintah. https://domain.go.id/, last accessed 2025/05/30
4. Nurhidayat, T., Windarta, S., Trianto, N., Shofiyuddin, M.F.M., et al.: Buku Lanskap Keamanan Siber 2024. Id-SIRTII/CC – Badan Siber dan Sandi Negara, Jakarta (2024)
5. Zukis, B.: Digital and Cybersecurity Governance Around the World. Annals of Corporate Governance 7(1), 1–92 (2022)Author, F.: Article title. Journal **2**(5), 99–110 (2016)
6. Melaku, H.M.: A Dynamic and Adaptive Cybersecurity Governance Framework. Journal of Cybersecurity and Privacy **3**(3), 327–350 (2023)
7. Kapferer, J.N.: The New Strategic Brand Management: Advanced Insights and Strategic Thinking. 5th edn. Kogan Page, London (2012)
8. Kotler, P., Lee, N.R.: Marketing in the Public Sector: A Roadmap for Improved Performance. Wharton School Publishing, Upper Saddle River, NJ (2007)
9. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An Integrative Model of Organizational Trust. Academy of Management Review **20**(3), 709–734 (1995)
10. Davis, F.D.: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly **13**(3), 319–340 (1989)
11. Taufiqurokhman, T., et al.: The Impact of E-Service Quality on Public Trust and Public Satisfaction in E-Government Public Services. International Journal of Data and Network Science **8**(2), 765–772 (2024)
12. Kanaan, A., et al.: The Effect of Quality, Security and Privacy Factors on Trust and Intention to Use E-Government Services. International Journal of Data and Network Science **7**(1), 185–198 (2023)
13. Hooda, A., Gupta, P., Jeyaraj, A., Dwivedi, Y.K.: Clarifying the Role of E-Government Trust in E-Government Success Models: A Meta-Analytic Structural Equation Modeling Approach. Australasian Journal of Information Systems **27**, Article 4079 (2023)
14. Lee-Geiller, S.: The Moderating Effect of Digital Literacy on the Link Between E-Government Effectiveness and Trust in Government. Journal of Policy Studies **39**(4), 77–101 (2024)
15. Luo, C., Hasan, N.A.M., Zamri bin Ahmad, A.M.: Exploring Satisfaction and Trust as Key Drivers of E-Government Continuance Intention. Sustainability **16**(24) (2024)
16. Kala, D., Chaubey, D.S., Meet, R.K., Al-Adwan, A.S.: Impact of User Satisfaction with E-Government Services on Continuance Use Intention and Citizen Trust Using TAM-ISSM Framework. Interdisciplinary Journal of Information, Knowledge, and Management **19** (2024)
17. Duan, Y., Dong, X.: Does Digital Literacy Matter for E-Government Usage Behavior? An Empirical Analysis Based on Data from Rural Women in China. SAGE Open **15**(3) (2025)
18. Pham, L., Limbu, Y.B., Le, M.T.T., Nguyen, N.L.: E-Government Service Quality, Perceived Value, Satisfaction, and Loyalty: Evidence from a Newly Emerging Country. Journal of Public Policy **43**(4), 812–833 (2023)

19. Chin, W.W.: The Partial Least Squares Approach to Structural Equation Modeling. In: Marcoulides, G.A. (ed.) Modern Methods for Business Research, pp. 295–336. Lawrence Erlbaum Associates, Mahwah, NJ (1998)
20. Fornell, C., Larcker, D.F.: Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research **18**(1), 39–50 (1981)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

