

# The Influence of Public Trust and Data Privacy on the Level of Use of the Digital Population Identity Application

An Wahyu Irawan<sup>1</sup>, Arif Ginanjar Suryatman<sup>2</sup>, Adie Dwiyanto Nurlukman<sup>3</sup>, Slamet Setiawan<sup>4</sup>, Muljadi<sup>5</sup>

<sup>1-5</sup> Faculty of Social and Political Sciences, Universitas Muhammadiyah Tangerang, Tangerang City, Banten Province, Indonesia

## Article Info

### Article history:

Received Sep, 2026

Revised Sep, 2026

Accepted Sep, 2026

### Keywords:

Public Trust

Data Privacy

Behavioral Intention

Digital Population Identity

E-Government

## ABSTRACT

This study aims to analyze the influence of trust in government and data privacy on the intention to use a public service application, specifically the Digital Population Identity (Identitas Kependudukan Digital/IKD) application, which serves as a digital electronic ID (e-KTP) service. This research employs a quantitative approach with a sample of 100 respondents. Statistical processing was performed with SPSS, comprising instrument validity and reliability checks, descriptive statistics, multiple linear regression, t-tests, F-tests, and computation of the coefficient of determination ( $R^2$ ). Findings indicate that both trust in government and data privacy exert a positive, significant influence on users' intention to adopt the IKD application. The regression output shows a statistically significant effect of trust in government on usage intention ( $t = 2.598$ ;  $\text{sig.} = 0.009$ ), and a similarly significant effect for data privacy ( $t = 2.866$ ;  $\text{sig.} = 0.004$ ). Combined, the two predictors explain 50.1% of the variance in usage intention ( $R^2 = 0.501$ ), with the remaining 49.9% attributable to variables outside this model. These results underline that public confidence in government and reassurance over data-privacy safeguards are both key drivers of intention to use digital government platforms. Accordingly, government institutions need to reinforce transparency, credibility, and personal-data protection to strengthen public acceptance of digital services.

This is an open access article under the [CC BY-SA](#) license.



## Corresponding Author:

Name: An Wahyu Irawan

Institution: Faculty of Social and Political Sciences, Universitas Muhammadiyah Tangerang, Tangerang City, Banten Province, Indonesia

Email: [wahyuirawann2020@gmail.com](mailto:wahyuirawann2020@gmail.com)

## 1. INTRODUCTION

The rapid development of information and communication technology has driven digital transformation across various sectors, including government. The Indonesian government continues to strive to improve the quality of public services through the implementation of e-government and

application-based service digitization, such as the Online Single Submission (OSS), PeduliLindungi, MySAPK BKN, M-Pajak, and various regional administrative service applications. This transformation aims to improve efficiency, transparency, and ease of access for the public in obtaining public services. Earlier research indicates that compliance behavior is shaped jointly by

personal norms and confidence in government, though such confidence does not appear to mediate how personal norms translate into taxpayer compliance [18]. A meta-analytic review of e-government adoption literature similarly concluded that trust in both government and the digital platform itself consistently predicts intention to use e-government services, and that this trust reinforces the link between perceived benefit and actual usage [5].

More than 2.3 billion pieces of personal data allegedly belonging to Indonesian citizens have been traded and circulated freely on various dark forums over the past three years. This phenomenon reflects the increasing intensity and complexity of data breach threats in the digital era. In 2023 alone, approximately 409 million user data records were leaked from various public and commercial services, such as BPJS Kesehatan, the PLN Mobile application, and a number of major e-commerce platforms accessed daily by the public. The scale of these incidents not only indicates weaknesses in cybersecurity systems but also confirms that regulatory enforcement of personal-data protection in Indonesia remains weak in practice [29]. The National Cyber and Crypto Agency (BSSN) recorded at least 103 alleged data breach incidents in Indonesia throughout 2023, indicating that the threat to national information security remains very high and requires more systematic handling. Notably, around 69% of these cases occurred in the government administration sector, which should be at the forefront of managing public information. This dominant percentage reveals that government institutions still have significant weaknesses pointing to persistent gaps in technological readiness, cybersecurity governance, and workforce capacity for safeguarding public data [43].

Previous research shows that the successful implementation of digital government services is influenced by aspects of public trust, service quality, data security, and personal data protection regulations. Research on telemedicine services found that system ease of use, information quality, and

trust in the confidentiality of personal data affect the acceptance of digital services, indicating that data protection is an important factor in building user confidence in electronic systems [41]. Similarly, research on the Personal Data Protection Law confirms that the law plays a strategic role in increasing public trust in e-government implementation, since the public tends to be more accepting of digital services when there are legal guarantees for the security of their data [7]. Meanwhile, other research shows that digital government transformation in Indonesia still faces obstacles in the form of digital divides, limited internet access, and low public awareness of data security, so that the adoption of digital public services has not been optimal [28]. Further research explains that the level of public trust in government is influenced by the quality of public services, transparency, integrity, and the utilization of information technology in governance, meaning that public trust is formed not only by technological aspects but also by the quality of government institutions themselves [21]. A study focused specifically on the Digital Population Identity (IKD) service reported that citizen uptake continues to hinge on how secure users perceive their data to be, alongside their general readiness to embrace digital administrative processes [13]. These prior studies share a common focus on public trust, data security, and acceptance of digital government services, while this study differs in its object and context, as it specifically analyzes the influence of public trust and data security on the level of use of the IKD application as a medium for digital population administration services, which involves a higher level of data sensitivity than other digital services.

In addition, data security and privacy are important issues in the implementation of digital identity. Prior work indicates that although digital population identity provides service efficiency, it also raises risks related to individual privacy and data security, requiring adequate protection and oversight. Theoretically, public trust also plays a major role in adoption of digital government services; existing evidence points to

confidence in both government institutions and the underlying technology as significant drivers of the public's willingness to adopt e-government platforms. Taken together, this body of literature suggests that limited uptake of the Digital Population Identity application cannot be explained by technological factors alone, but is also tied closely to citizens' level of trust and their perceptions of data security. Therefore, research on the influence of public trust and data security on the level of use of the IKD application is important to conduct.

This study offers novelty by simultaneously analyzing the influence of trust in government and data privacy on the intention to use the IKD application as a platform for creating a digital e-KTP. This study also provides a new empirical contribution by examining usage behavior for a digital population administration service that has a higher level of data sensitivity compared to other digital public services. This study is therefore intended to add to the growing body of work on digital government transformation, with particular emphasis on trust, security, and the protection of personal data. Specifically, this study aims to analyze the influence of trust in government and data privacy on public intention to use the IKD application as a medium for creating a digital e-KTP, and further aims to analyze the simultaneous influence of trust in government and data privacy on the intention to use the IKD application as a form of digital transformation in population administration services.

## 2. LITERATURE REVIEW

### 2.1 *Trust in Government (X1)*

Based on the organizational trust model of Mayer, Davis, and Schoorman [cited in the operational framework], trust consists of three main dimensions: ability, benevolence, and integrity. From these dimensions, several indicators of trust in government can be derived for this study. This variable is measured

through five main indicators: the government's ability (Ability), the government's honesty (Integrity), the government's good intentions (Benevolence), the consistency of government policy, and the government's responsibility in public service.

### 2.2 *Data Privacy (X2)*

Data privacy is measured using the Internet Users' Information Privacy Concerns (IUIPC) concept developed by Malhotra, Kim, and Agarwal. This theory explains that privacy concerns arise from how personal information is collected, used, and controlled, as well as users' perceived risk of misuse or leakage of their data. This variable consists of five indicators: data collection, use of data, control over personal data, data security protection, and confidentiality of personal information.

### 2.3 *Intention to Use the Public Service Application (Y)*

The intention to use a public service application is explained using the Technology Acceptance Model (TAM) developed by Fred D. Davis in 1989. In this model, behavioral intention to use describes an individual's desire or tendency to use a system or technology. This variable consists of five indicators: the desire to use the application, plans to use the application in the future, willingness to try the application, preference for using the application over other means, and the intention to continue using it.

## 3. METHODS

This study uses a quantitative approach with a survey method. The

quantitative approach is used to test the influence of trust in government and data privacy on the intention to use a public service application, namely the Digital Population Identity (IKD) application. Data analysis was carried out using the Statistical Package for Social Sciences (SPSS).

This study uses two independent variables, namely Trust in Government (X1) and Data Privacy (X2), and one dependent variable, namely Intention to Use the Public Service Application (Y). The relationships between variables were analyzed using multiple linear regression analysis to determine the effect of each independent variable on the dependent variable, both partially and simultaneously.

### 3.1 Population and Sample

The population in this study consists of all residents of Tangerang City who have completed electronic ID card (e-KTP) recording, based on data from the Tangerang City Population and Civil Registration Office (Disdukcapil) for 2025, totaling 1,401,002 people. This population was selected because the research focuses on the use of the Digital Population Identity (IKD) application as part of the digital transformation of population administration services.

The sample consists of IKD application users from 13 sub-districts (kecamatan) in Tangerang City. The sampling technique used was probability sampling with a cluster sampling method, as the population is spread across several administrative regions, so respondents were grouped by sub-district and then selected proportionally to ensure representation from each sub-district.

Because the total population figure was known, the Slovin formula was applied to determine an appropriate sample size. Applying a 10% margin of error to this formula yielded a target of 100 respondents. The Slovin formula used is:  $n = N / (1 + N \cdot e^2)$ , where  $n$  is the sample size,  $N$  is the population size, and  $e$  is the margin of error. Based on a population of 1,401,002 with a 10% margin of error, the calculated minimum sample size

was  $n = 99.99 \approx 100$ . Accordingly, this study used a sample of 100 respondents, selected proportionally from the 13 sub-districts of Tangerang City.

### 3.2 Data Collection

Data were collected using a combination of online and offline channels. The questionnaire was distributed through online platforms (social media) to ensure broad and efficient access, as well as through offline collection at several strategic locations in each sub-district to reach participants who were more difficult to reach online. An expected response rate of 80% was targeted, with reminder and follow-up procedures used to ensure a high participation rate. To address non-response bias, control strategies included periodic reminders to non-respondents and ensuring proportional participation across strata (based on sub-district and demographic characteristics), consistent with the stratified random sampling technique used.

A five-point Likert scale was used, ranging from "strongly disagree" to "strongly agree". This study was approved by the Research Ethics Committee (IRB), ensuring that the research complied with applicable ethical standards. Before participating, every respondent who received the questionnaire through Google Forms (online channel) or offline collection was given written consent explaining the purpose of the study, the procedures involved, and their rights, including the right to withdraw at any time without consequence. Written consent was also obtained electronically through Google Forms before respondents completed the questionnaire. For personal data protection, a mechanism consistent with the Personal Data Protection (PDP) Law was applied, whereby all respondent data is kept confidential and used solely for the purposes of this research. The collected data was anonymized to protect respondents' identities and was not shared with third parties without explicit respondent consent.

### 3.3 Operational Definition of Variables

Table 1. Operational Definition of Variables

| No. | Variable                                                             | Indicators                                                                                                                                                                                           |
|-----|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | X1 Trust in Government (Mayer, Davis, & Schoorman, 1995)             | Government ability (Ability); Government honesty (Integrity); Government good intentions (Benevolence); Consistency of government policy; Government responsibility in public service                |
| 2   | X2 Data Privacy (Malhotra, Kim & Agarwal, 2004)                      | Data collection (Collection); Use of data (Use of Data); Control over personal data (Control); Data security protection (Data Security); Confidentiality of personal information (Confidentiality)   |
| 3   | Y Intention to Use the Public Service Application (Fred Davis, 1989) | Desire to use the application; Plans to use the application in the future; Willingness to try the application; Preference for using the application over other means; Intention to continue using it |

Source: Processed by the Author (2026)

### 3.4 Data Analysis Technique

Data analysis in this study was conducted using the Statistical Package for Social Sciences (SPSS). Data analysis is the process, after data from all respondents has been collected, of processing and interpreting the data so that it can answer the research problem and test the research hypotheses. The stages of data analysis used in this study are as follows.

- 1) Descriptive statistical analysis is used to describe respondent characteristics and each research variable, including the minimum, maximum, mean, and standard deviation values.
- 2) Validity test determines the extent to which the research instrument measures what it is intended to measure, using the Pearson Product Moment correlation between item scores and total scores. An item is declared valid if  $r\text{-count} > r\text{-table}$  and the significance value is below 0.05.
- 3) Reliability test measures the consistency of the research instrument using Cronbach's Alpha. An instrument is treated as internally consistent when its Cronbach's Alpha coefficient reaches at least 0.70.
- 4) **Classical assumption tests** were performed prior to multiple

linear regression analysis, comprising a normality test (One-Sample Kolmogorov-Smirnov Test, with data considered normally distributed if the significance value exceeds 0.05), a multicollinearity test (based on Tolerance and Variance Inflation Factor/VIF values, with the model considered free of multicollinearity if  $\text{Tolerance} > 0.1$  and  $\text{VIF} < 10$ ), and a heteroscedasticity test (Glejser test, with no heteroscedasticity indicated if the significance value exceeds 0.05).

- 5) Multiple linear regression analysis. o assess how Trust in Government (X1) and Data Privacy (X2) jointly shape Intention to Use the Public Service Application (Y), a multiple linear regression model was estimated in the form  $Y = a + b_1X_1 + b_2X_2 + e$ .
- 6) Partial test (t-test) determines the partial effect of each independent variable on the dependent variable. The hypothesis is accepted if the significance value is below 0.05, and rejected if above 0.05.
- 7) Simultaneous test (F-test) determines whether the

independent variables jointly affect the dependent variable, using the same significance criterion of 0.05.

- 8) Coefficient of determination ( $R^2$ ) measures the ability of the independent variables to explain variation in the dependent variable, ranging from 0 to 1; a

larger  $R^2$  indicates greater explanatory power.

#### 4. RESULTS AND DISCUSSION

##### 4.1 Respondent Demographics

A total of 100 respondents participated in the survey. Their demographic distribution is presented in Table 2.

Table 2. Respondent Demographic Profile

| No. | Description                       | Category               | n  | %   |
|-----|-----------------------------------|------------------------|----|-----|
| 1   | Age                               | 18–22                  | 21 | 21% |
|     |                                   | 23–27                  | 43 | 43% |
|     |                                   | 28–32                  | 13 | 13% |
|     |                                   | 33–37                  | 11 | 11% |
|     |                                   | 38–42                  | 12 | 12% |
| 2   | Gender                            | Male                   | 71 | 71% |
|     |                                   | Female                 | 25 | 25% |
| 3   | Education level                   | Elementary/Junior High | 7  | 7%  |
|     |                                   | Senior High/Vocational | 49 | 49% |
|     |                                   | Diploma (D3)           | 5  | 5%  |
|     |                                   | Bachelor (D4/S1)       | 32 | 32% |
|     |                                   | Master (S2)            | 2  | 2%  |
|     |                                   | Doctorate (S3)         | 1  | 1%  |
| 4   | Internet usage experience (years) | 1–2                    | 5  | 5%  |
|     |                                   | 3–4                    | 12 | 12% |
|     |                                   | 4–5                    | 19 | 19% |
|     |                                   | >6                     | 60 | 60% |

Source: Processed by the Author Using SPSS 27 (2026)

Based on Table 2, respondent characteristics were dominated by the 23–27 age group (43 people, 43%), followed by the 18–22 age group (21 people, 21%). Respondents aged 28–32 numbered 13 people (13%), those aged 33–37 numbered 11 people (11%), and those aged 38–42 numbered 12 people (12%). This indicates that the majority of respondents were of a young, productive age, which is likely associated with a higher level of activity and participation. In terms of gender, respondents were dominated by males (71 people, 71%), while females

numbered 25 people (25%), indicating a gender imbalance in the sample. In terms of education, most respondents had a senior high/vocational school background (49 people, 49%), followed by those with a bachelor's degree (D4/S1) (32 people, 32%). Respondents with elementary/junior high education numbered 7 people, diploma (D3) 5 people (5%), master's degree (S2) 2 people (2%), and doctorate (S3) 1 person (1%). Overall, respondents were dominated by individuals with secondary to undergraduate education, suggesting that most respondents

had a sufficient level of education to understand and respond to the research instrument.

#### 4.2 Instrument Testing

- 1) Validity Test — Table 3 presents the validity test results for the Trust in Government variable

(X1). All indicators show a correlation value above 0.30 and are significant at  $p < 0.01$ . The highest value is found in indicator X1.3 (0.898), while the lowest is in X1.1 (0.757). Accordingly, all indicators are declared valid for measuring variable X1.

Table 3. Validity Test Results for Trust in Government (X1)

| Indicator | Correlation with X1 | Description |
|-----------|---------------------|-------------|
| X1.1      | 0.757**             | Valid       |
| X1.2      | 0.851**             | Valid       |
| X1.3      | 0.898**             | Valid       |
| X1.4      | 0.840**             | Valid       |
| X1.5      | 0.783**             | Valid       |

Source: SPSS Output, Processed Data (2026)

All indicators of the Data Privacy variable (X2) also show correlation values above 0.30, significant at  $p < 0.01$ . The highest

value is found in X2.3 (0.873) and the lowest in X2.5 (0.685). Accordingly, all indicators are declared valid.

Table 4. Validity Test Results for Data Privacy (X2)

| Indicator | Correlation with X2 | Description |
|-----------|---------------------|-------------|
| X2.1      | 0.867**             | Valid       |
| X2.2      | 0.854**             | Valid       |
| X2.3      | 0.873**             | Valid       |
| X2.4      | 0.831**             | Valid       |
| X2.5      | 0.685**             | Valid       |

Source: SPSS Output, Processed Data (2026)

Similarly, all indicators of the Intention to Use the Public Service Application (Y) show correlation values above 0.30, significant at  $p < 0.01$ , with the

highest value at Y3 (0.912) and the lowest at Y1 (0.657). All indicators are therefore declared valid.

Table 5. Validity Test Results for Intention to Use the Application (Y)

| Indicator | Correlation with Y | Description |
|-----------|--------------------|-------------|
| Y1        | 0.657**            | Valid       |
| Y2        | 0.841**            | Valid       |
| Y3        | 0.912**            | Valid       |
| Y4        | 0.867**            | Valid       |
| Y5        | 0.807**            | Valid       |

Source: SPSS Output, Processed Data (2026)

- 2) Reliability Test — The reliability test results (Table 6) show that all variables have Cronbach's Alpha values above 0.70. Variable X1 has the highest value (0.882), followed by X2 (0.874) and Y (0.873). This indicates that all research instruments have good internal consistency and are reliable for further analysis.

Table 6. Instrument Reliability Test

| Variable                 | Cronbach's Alpha | Number of Items | Description |
|--------------------------|------------------|-----------------|-------------|
| X1 (Trust in Government) | 0.882            | 5               | Reliable    |
| X2 (Data Privacy)        | 0.874            | 5               | Reliable    |
| Y (Intention to Use)     | 0.873            | 5               | Reliable    |

Source: SPSS Output, Processed Data (2026)

### 4.3 Classical Assumption Tests

The normality test aims to determine whether the residual data of the regression model is normally distributed, which is important because residual normality affects the accuracy of hypothesis testing through the t-test and F-test. Gujarati and Porter argue that the normality assumption is not an absolute requirement in Ordinary Least Squares (OLS) estimation — the OLS

estimator remains the Best Linear Unbiased Estimator (BLUE) as long as the other classical assumptions are met, and for large samples the residual distribution tends to approach normality based on the Central Limit Theorem (CLT). In this study, the sample size of 100 respondents is considered sufficiently large, so that in theory, a violation of normality does not substantially affect the accuracy of the model estimation.

Table 7. Kolmogorov-Smirnov Normality Test Results

| Residual Variable       | N   | Test Statistic | Asymp. Sig. (2-tailed) | Conclusion |
|-------------------------|-----|----------------|------------------------|------------|
| Unstandardized Residual | 100 | 0.113          | 0.003                  | Not Normal |

Source: SPSS Output, Processed Data (2026)

The Kolmogorov-Smirnov test shows a significance value of  $0.003 < 0.05$ , indicating that the residuals in this study are not normally distributed. However, based on CLT theory and the argument above, this violation of normality is not considered a serious issue given the sufficiently large sample size, and the regression model can still be used for further analysis.

The multicollinearity test aims to determine whether there is a high correlation between independent variables in the regression model, examined via Tolerance and Variance Inflation Factor (VIF) values. If Tolerance  $> 0.10$  and VIF  $< 10$ , it can be concluded that no multicollinearity is present.

Table 8. Multicollinearity Test Results

| Variable                 | Tolerance | VIF   | Conclusion           |
|--------------------------|-----------|-------|----------------------|
| X1 (Trust in Government) | 0.431     | 2.320 | No multicollinearity |
| X2 (Data Privacy)        | 0.431     | 2.320 | No multicollinearity |

Source: SPSS Output, Processed Data (2026)

The results show that both independent variables have Tolerance values

above 0.10 and VIF values below 10. It can therefore be concluded that there is no

multicollinearity in this regression model, indicating that the independent variables do not excessively influence one another and that the model is suitable for use.

The heteroscedasticity test aims to determine whether there is inequality of

residual variance between observations, using the Glejser test, in which the absolute residual value is regressed on the independent variables. Heteroscedasticity is indicated if the significance value is below 0.05.

Table 9. Glejser Heteroscedasticity Test Results

| Variable                 | Sig.  | Conclusion                 |
|--------------------------|-------|----------------------------|
| X1 (Trust in Government) | 0.722 | No heteroscedasticity      |
| X2 (Data Privacy)        | 0.000 | Heteroscedasticity present |

Source: SPSS Output, Processed Data (2026)

The results show that variable X2 has a significance value of  $0.000 < 0.05$ , indicating heteroscedasticity in the regression model. This means that the residual variance is not constant, which can affect the accuracy of the standard error estimates.

To address the heteroscedasticity issue, this study applies the Robust Standard Errors (HC3) approach. Robust standard

errors are used to correct the standard error estimates without changing the regression coefficient values, so that the test results remain valid despite the presence of heteroscedasticity. The HC3 approach is a more conservative robust method that is well-suited to small-to-medium samples because it provides more stable estimates in the presence of non-homogeneous variance.

Table 10. Robust Regression Results (HC3)

| Variable                 | B      | Robust Std. Error | t      | Sig.  |
|--------------------------|--------|-------------------|--------|-------|
| Intercept                | 7.991  | 2.063             | 3.874  | 0.000 |
| X1 (Trust in Government) | -0.021 | 0.095             | -0.223 | 0.824 |
| X2 (Data Privacy)        | 0.669  | 0.116             | 5.768  | 0.000 |

Source: SPSS Output, Processed Data (2026)

After applying robust standard errors, X1 (trust in government) does not have a significant effect on Y (intention to use the public service application), while X2 (data privacy) has a significant positive effect on Y. This indicates that after correcting for heteroscedasticity using the HC3 method, the model estimation becomes more accurate and stable, since the standard errors have been adjusted for potential inequality of residual

variance, making the analysis results more reliable as a basis for the research conclusions.

#### 4.4 Multiple Linear Regression Analysis

Multiple linear regression analysis was used to determine the effect of Trust in Government (X1) and Data Privacy (X2) on the Intention to Use the Public Service Application (Y), using the model  $Y = a + b_1X_1 + b_2X_2 + e$ .

Table 11. Multiple Linear Regression Results

| Variable               | B      | Std. Error | Beta   | t      | Sig.  |
|------------------------|--------|------------|--------|--------|-------|
| Constant               | 7.991  | 1.257      | -      | 6.358  | 0.000 |
| X1 Trust in Government | -0.021 | 0.081      | -0.027 | -0.262 | 0.793 |
| X2 Data Privacy        | 0.669  | 0.088      | 0.772  | 7.576  | 0.000 |

Source: SPSS Output, Processed Data (2026)

Based on the multiple linear regression results, the regression equation obtained is:

$$Y = 7.991 - 0.021X_1 + 0.669X_2$$

This equation shows that the constant of 7.991 indicates that if Trust in Government (X1) and Data Privacy (X2) are held constant (equal to zero), the value of the Intention to Use the Public Service Application (Y) is 7.991. The regression coefficient of the Trust in Government variable (-0.021) indicates a negative relationship with the intention to use the application, while the regression coefficient of the Data Privacy variable (0.669) indicates a positive relationship with the intention to use the application.

#### 4.5 Hypothesis Testing

- 1) Partial Test (t-test). The Trust in Government variable has a calculated t-value of -0.262 with a significance value of 0.793.

Since this significance value is greater than 0.05, Trust in Government does not have a significant effect on the Intention to Use the Public Service Application; hence, the first hypothesis (H1) is rejected. The Data Privacy variable has a calculated t-value of 7.576 with a significance value of 0.000. Since this significance value is less than 0.05, Data Privacy has a positive and significant effect on the Intention to Use the Public Service Application; hence, the second hypothesis (H2) is accepted.

- 2) Simultaneous Test (F-test). The F-test was used to determine whether Trust in Government and Data Privacy jointly affect the Intention to Use the Public Service Application.

Table 12. F-Test Results

| F-value | Sig.  | Conclusion  |
|---------|-------|-------------|
| 63.193  | 0.000 | Significant |

Source: SPSS Output, Processed Data (2026)

The F-test shows a calculated F-value of 63.193 with a significance level of 0.000, which is less than 0.05. It can therefore be concluded that Trust in Government and Data Privacy jointly have a significant effect on the Intention to Use the Public Service Application, and the regression model is suitable for

explaining the relationship between the independent and dependent variables.

- 3) Coefficient of Determination ( $R^2$ ). This coefficient captures the proportion of variance in the dependent variable that the independent variables, taken together, are able to account for.

Table 13. Coefficient of Determination Results

| R     | R Square | Adjusted R Square | Std. Error of the Estimate |
|-------|----------|-------------------|----------------------------|
| 0.752 | 0.566    | 0.557             | 2.749                      |

Source: SPSS Output, Processed Data (2026)

The correlation coefficient (R) of 0.752 indicates that the relationship between Trust in Government and Data Privacy with the Intention to Use the Public Service Application is strong. The R Square value of 0.566 indicates that 56.6% of the variation in the Intention to Use the Public Service Application can be explained by Trust in Government and Data Privacy, while the remaining 43.4% is explained by other factors outside the research model. The Adjusted R Square value of 0.557 indicates that, after adjusting for the number of independent variables in the model, the model explains 55.7% of the variation in the dependent variable.

### Discussion

This study shows that trust in government (X1) does not have a significant effect on the intention to use the Digital Population Identity (IKD) application for creating a digital e-KTP, with a coefficient of -0.021 (t-statistic -0.223;  $p = 0.824$ ). This finding indicates that in the context of a mandatory e-government service, trust in government is no longer a primary factor influencing usage intention.

This aligns with Hooda et al. [54], who argue that within e-government settings trust does not necessarily translate directly into usage intention, and its effect is frequently channeled through other mechanisms such as perceived risk and facilitating conditions. Furthermore, AlAwadhi et al. [55] show that in an extended TAM model, trust is more strongly influenced by information quality and ease of use rather than directly determining users' behavioral intention.

A meta-analytic study by Gupta et al. [12] also confirms that although trust in government generally influences e-government adoption, its effect becomes weaker in the context of mandatory digital services, since users must use the system regardless of their level of trust.

Conversely, data privacy (X2) is shown to have a positive and significant effect on the intention to use the IKD application, with a coefficient of 0.669 (t-statistic 5.768;  $p =$

0.000). This result reinforces Privacy Calculus Theory, which explains that individuals weigh the balance between benefits and risks before using a digital system [57].

This finding is also supported by Chuah et al. [56], who show that privacy concerns and perceived data-security risk are dominant factors in the adoption of application-based e-government services. Hooda et al. [54] further note that both perceived risk and privacy concern exert a direct, significant influence on behavioral intention within e-government contexts.

Simultaneously, the results of this study show that data privacy is the main factor shaping the intention to use the IKD application, while trust in government is not significant. This suggests that the public is more sensitive to the risk of personal data misuse than to their perception of government institutional performance.

This result is further reinforced by Gupta et al. [12], who state that security and privacy issues are key determinants of successful modern e-government implementation, particularly for systems that manage sensitive data such as digital identity.

Accordingly, this study extends the TAM model in the e-government context by confirming that privacy plays a more dominant role than trust in mandatory services such as IKD. This is also consistent with recent research trends showing that integrating TAM with privacy concern and perceived risk variables provides stronger explanatory power for the intention to use digital government technology.

### 5. CONCLUSION

The analysis leads to the conclusion that trust in government (X1) does not significantly shape the public's intention to adopt the Digital Population Identity (IKD) application as a channel for obtaining a digital e-KTP, while data privacy (X2) exerts a positive and significant influence on that intention. The regression analysis with robust standard errors (HC3) shows that the research model is able to explain the relationships between variables more stably after correcting

for heteroscedasticity. These findings indicate that in the context of a mandatory digital government service, trust in government is no longer the primary determinant of usage intention; instead, public perceptions of the security, confidentiality, and protection of personal data are more dominant in influencing the decision to use the IKD application, showing that the public gives greater consideration to risks related to personal data than to their evaluation of government institutions when adopting digital population services. This study therefore concludes that the successful implementation of the IKD application does not depend solely on increasing public trust in government, but is also strongly determined by the government's ability to guarantee personal data protection in a transparent, accountable, and consistent manner.

Consequently, strengthening data security systems and privacy policies is a crucial aspect in encouraging the adoption of digital population services in Indonesia. Future research is recommended to expand the model by incorporating mediating variables such as perceived risk and facilitating conditions, and to extend the sample beyond Tangerang City to improve the generalizability of the findings.

## ACKNOWLEDGEMENTS

The authors would like to thank the Faculty of Social and Political Sciences, Universitas Muhammadiyah Tangerang, and all respondents from the 13 sub-districts of Tangerang City who participated in this research.

## REFERENCES

- [1] N. Aleisa, "Key factors influencing the e-government adoption: a systematic literature review," *J. Innov. Digit. Transform.*, 2025, doi: 10.1108/JIDT-09-2023-0016.
- [2] N. Amahi, C. Febrilyantri, and N. D. Lestari, "Insentif Pajak Dan Tingkat Kepercayaan: Pengaruhnya Terhadap Kepatuhan Wajib Pajak" (in Indonesian), *Jurnal Ekonomi*, vol. 28, no. 1, pp. 1–19, 2023.
- [3] D. A. Anugrah et al., "Analisis Kepuasan Pengguna Aplikasi Identitas Kependudukan Digital (IKD) di Dinas Dukcapil Kota Jambi Menggunakan Metode Technology Acceptance Model" (in Indonesian), *Inov. Kreativitas Ekon.*, vol. 8, no. 6, pp. 68–81, 2024.
- [4] Ario Irawan, "Pengaruh Persepsi Korupsi Pajak dan Persepsi Keadilan Sistem Perpajakan Terhadap Kepatuhan Wajib Pajak Orang Pribadi dengan Kepercayaan Sebagai Variabel Intervening" (in Indonesian), *Prisma: Platf. Riset Mhs. Akunt.*, vol. 1, no. 6, pp. 114–125, 2020.
- [5] D. A. Aslindar, F. Tristiawan, and I. L. Masvika, "Determinan Kepatuhan Wajib Pajak Orang Pribadi" (in Indonesian), *J. Econ. Insights*, vol. 2, no. 2, pp. 23–34, 2023, doi: 10.51792/jei.v2i2.66.
- [6] N. M. Aurelia, "Program Studi Administrasi Publik Fakultas Ilmu Sosial dan Ilmu Politik" (in Indonesian), Undergraduate thesis, Univ. Muhammadiyah Tangerang, 2025.
- [7] H. H. Carlo and F. B. Hirawan, "Urgensi Undang-Undang Perlindungan Data Pribadi dalam Pengembangan Kebijakan e-Government di Indonesia" (in Indonesian), *Perspektif*, vol. 11, no. 4, pp. 1407–1413, 2022, doi: 10.31289/perspektif.v11i4.7267.
- [8] S. P. Collins et al., "Pengaruh Faktor Technology Acceptance Model (TAM) dan Kualitas Laporan Keuangan Terhadap Kepuasan Pengguna Software Akuntansi" (in Indonesian), pp. 167–186, 2021.
- [9] M. R. Desandry, Yuwanto, and Wijayanto, "Analisis Faktor Penyebab Kegagalan Digitalisasi Pelayanan Publik Di Disdukcapil Kabupaten Bogor" (in Indonesian), *J. Polit. Gov. Stud.*, vol. 13, no. 3, pp. 1–13, 2024.
- [10] Fastha Aulia Pradhani and Juwita Sari, "Peran Lingkungan Dalam Memoderasi Penerapan E-Filing Dan Tingkat Kepercayaan Pada Pemerintah Terhadap Kepatuhan Wajib Pajak" (in Indonesian), *J. Akad. Akunt.*, vol. 5, no. 2, pp. 279–295, 2022, doi: 10.22219/jaa.v5i2.20069.
- [11] P. C. Gahung, J. D. L. Warongan, and S. S. E. Mintalangi, "Pengaruh pengetahuan perpajakan, kesadaran wajib pajak, dan kepercayaan masyarakat pada pemerintah terhadap kepatuhan wajib pajak dalam membayar PBB-P2" (in Indonesian), *Riset Akunt. Portof. Investasi*, vol. 2, no. 2, pp. 143–149, 2024, doi: 10.58784/rapi.145.
- [12] P. Gupta, A. Hooda, A. Jeyaraj, J. J. M. Seddon, and Y. K. Dwivedi, "Trust, risk, privacy and security in e-government use: insights from a MASEM analysis," *Inf. Syst. Front.*, vol. 27, no. 3, pp. 1089–1105, 2025, doi: 10.1007/s10796-024-10497-8.
- [13] Gusmeri and T. Huseno, "Penggunaan Layanan Identitas Kependudukan Digital Di Kota Payakumbuh" (in Indonesian), vol. 13, no. 2, pp. 556–573, 2024.
- [14] A. K. M. A. Hamzah, "Akuntabilitas Vertikal dan Horizontal Pengelolaan Dana Desa terhadap Tingkat Kepercayaan Masyarakat Kepada Pemerintah Desa" (in Indonesian), *Equity: J. Akunt.*, vol. 2, no. 2, pp. 131–138, 2023, doi: 10.46821/equity.v2i2.232.
- [15] J. H. Han and H. J. Sa, "Acceptance of and satisfaction with online educational classes through the technology

- acceptance model (TAM): the COVID-19 situation in Korea," *Asia Pac. Educ. Rev.*, vol. 23, no. 3, pp. 403–415, 2022, doi: 10.1007/s12564-021-09716-7.
- [16] P. Handayani and M. A. Setiawan, "Pengaruh Auditor Switching, Komite Audit, dan Audit Capacity Stress terhadap Kualitas Audit" (in Indonesian), *J. Eksplorasi Akunt.*, vol. 6, no. 2, pp. 458–471, 2024, doi: 10.24036/jea.v6i2.735.
  - [17] Herlina, J. F. Andry, and F. M. Susanto, "Analisis Deskriptif Perilaku Konsumen Shopee: Technology Acceptance Model (TAM)" (in Indonesian), *J. Technol. Inform. (JoTI)*, vol. 4, no. 2, pp. 63–68, 2023, doi: 10.37802/joti.v4i2.318.
  - [18] A. Hidayatulloh and K. Fikrianoor, "Does trust in government play a role? Personal norm and taxpayer compliance," *J. Riset Akunt.*, vol. 15, no. 1, pp. 24–33, 2023.
  - [19] A. Hidayatulloh, I. Shofiyah, A. D. Nugroho, E. A. Wiharsanti, and F. P. Ganinda, "Kepatuhan Wajib Pajak Orang Pribadi: Pengaruh Cinta Uang Machiavellianism, Religiusitas, Whistleblowing System, Kepercayaan Terhadap Pemerintah" (in Indonesian), *JAP: J. Akunt. Pajak*, vol. 24, no. 1, pp. 1–9, 2023.
  - [20] Ifatul Latifah and Suci Alifia Wardani, "Peran Etika Dalam Membangun Kepercayaan Publik Terhadap Pemerintah" (in Indonesian), *J. Ilmu Komun. Sos. Polit.*, vol. 2, no. 3, pp. 579–587, 2025.
  - [21] Iin Agustina, Riza Bahtiar Sulistyan, and R. P., "Telaah Kritis Tentang Konsep Kepercayaan Masyarakat: Peran Teknologi, Informasi dan Komunikasi" (in Indonesian), vol. 7, no. 1, pp. 182–187, 2023.
  - [22] R. Ikhsan, G. A. Nursanto, and N. M. Piranti, "Tinjauan Literatur Analisis Aplikasi Pelayanan Publik" (in Indonesian), vol. 4, pp. 8052–8074, 2024.
  - [23] A. Ingrams, "Government openness and public trust: the mediating role of democratic capacity," *Public Adm. Rev.*, pp. 91–109, 2020, doi: 10.1111/puar.13298.
  - [24] B. A. Iswandari, "Jaminan Keamanan Data Pribadi Warga Negara Dalam Penyelenggaraan Urusan Pemerintahan Berbasis Elektronik (E-Government)" (in Indonesian), *Dharmasisya: J. Progr. Magister Hukum FHUI*, vol. 2, no. 1, pp. 3–14, 2022.
  - [25] J. M. Karwur, J. J. Sondakh, and L. Kalangi, "Pengaruh Sikap Terhadap Perilaku, Norma Subyektif, Kontrol Perilaku Yang Dipersepsikan Dan Kepercayaan Pada Pemerintah Terhadap Kepatuhan Wajib Pajak Orang Pribadi Dengan Niat Sebagai Variabel Intervening" (in Indonesian), *J. Riset Akunt. Auditing "Goodwill"*, vol. 11, no. 2, pp. 113–130, 2020.
  - [26] R. Kairoot and M. P. Ersya, "Analisis Tingkat Kepercayaan Masyarakat terhadap Pelaksanaan Kebijakan Penanganan Covid-19 oleh Pemerintah Kecamatan Kubung" (in Indonesian), *J. Civic Educ.*, vol. 4, no. 4, pp. 371–378, 2021.
  - [27] S. A. Kamal, M. Shafiq, and P. Kakria, "Investigating acceptance of telemedicine services through an extended technology acceptance model (TAM)," *Technol. Soc.*, vol. 60, p. 101212, 2020, doi: 10.1016/j.techsoc.2019.101212.
  - [28] A. Kennedy, W. H. Surya, and F. X. Wartoyo, "Tantangan dan Solusi Penerapan E-Government di Indonesia" (in Indonesian), *J. Terapan Pemerintahan Minangkabau*, vol. 4, no. 2, pp. 134–147, 2024.
  - [29] Kompas.id, "Kebocoran Data Pribadi Terus Mengancam, Lembaga Pengawas Tak Kunjung Dibentuk" (in Indonesian), Kompas.id, 2025. [Online]. Available: <https://www.kompas.id/artikel/kebocoran-data-pribadi-terus-mengancam-lembaga-pengawas-tak-kunjung-dibentuk>
  - [30] A. Kumalasari and I. Swasanti, "Digitalisasi pelayanan publik: ketidaksiapan masyarakat dalam penggunaan aplikasi identitas kependudukan digital di Bojonegoro" (in Indonesian), vol. 15, pp. 271–283, 2024.
  - [31] H. Mastour, R. Yousefi, and S. Niroumand, "Exploring the acceptance of e-learning in health professions education in Iran based on the technology acceptance model (TAM)," *Sci. Rep.*, vol. 15, no. 1, pp. 1–14, 2025, doi: 10.1038/s41598-025-90742-5.
  - [32] F. Mufidta and D. Urumsah, "Determinan kesenjangan ekspektasi terhadap tingkat kepercayaan masyarakat pada pengelolaan dana keistimewaan: model konseptual" (in Indonesian), *Proc. Natl. Conf. Account. Finance*, vol. 6, pp. 231–240, 2024.
  - [33] A. R. Municipality, "Citizen trust in e-government strategies: perspectives on e-services at a South African municipality," *Int. J. Public Adm. Digit. Age*, vol. 12, no. 1, pp. 1–28, 2025, doi: 10.4018/IJPADA.385699.
  - [34] J. Nawawi, "Membangun Kepercayaan Dalam Mewujudkan Good Governance" (in Indonesian), *Naukovi Perspektivi*, vol. 1, no. 11(41), pp. 19–29, 2023.
  - [35] R. Nurdianingsih and E. Suryadi, "Jurnal Produktivitas" (in Indonesian), *J. Produktivitas*, vol. 8, pp. 46–55, 2021.
  - [36] F. D. Pawestri and J. Jumino, "Analisis Hubungan Information Privacy Concern dan Perilaku Perlindungan Privasi Pengguna Twitter di Indonesia" (in Indonesian), *Anuva: J. Kaj. Budaya Perpustakaan Inf.*, vol. 5, no. 2, pp. 221–236, 2021, doi: 10.14710/anuva.5.2.221-236.
  - [37] D. Y. Prasetyo, "Analisis Penerimaan Informasi Pengguna Website Dengan Menggunakan Technology Acceptance Model (Studi Kasus: dpmd.inhilkab.go.id)" (in Indonesian), *Selodang Mayang*, vol. 6, no. 3, pp. 178–187, 2020, doi: 10.47521/selodangmayang.v6i3.174.
  - [38] D. Rad et al., "A preliminary investigation of the technology acceptance model (TAM) in early childhood education and care," *BRAIN: Broad Res. Artif. Intell. Neurosci.*, vol. 13, no. 1, pp. 518–533, 2022, doi: 10.18662/brain/13.1/297.
  - [39] K. Rima, A. Suari, and I. M. Sarjana, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia" (in Indonesian), vol. 1, pp. 132–146, 2023, doi: 10.38043/jah.v6i1.4484.
  - [40] Rista Maharani and Andria Luhur Prakoso, "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital" (in Indonesian), *J. USM Law Rev.*, vol. 7, no. 1, pp. 333–347, 2024.
  - [41] A. J. Rusdi, R. D. Prisantanti, F. R. Ikawati, and E. N. Oktoriani, "Kepercayaan Kerahasiaan Data Diri Masyarakat Pada Pelayanan Telemedis: Path Analysis Model" (in Indonesian), *J-REMI: J. Rekam Medik Inf. Kesehatan*, vol. 6, no. 1, pp. 1–8, 2024, doi: 10.25047/j-remi.v6i1.4654.

- [42] B. Santoso and E. Zusrony, "Analisis Persepsi Pengguna Aplikasi Payment Berbasis Fintech Menggunakan Technology Acceptance Model (TAM)" (in Indonesian), *J. Teknol. Inf. Komun.*, vol. 11, pp. 49–54, 2020.
- [43] sibermate, "Krisis Kebocoran Data Pribadi: Tata Kelola yang Buruk di Indonesia" (in Indonesian), 2024. [Online]. Available: <https://sibermate.com/hrmi/krisis-kebocoran-data-pribadi-tata-kelola-yang-buruk-di-indonesia>
- [44] C. P. Sihombing, N. Yusuf, D. Fahreza, and N. Aziz, "Manajemen Keamanan Siber Dalam Perlindungan Data Pada Layanan Aplikasi Transportasi Publik" (in Indonesian), *J. Informatic Inf.*, vol. 5, no. 2, pp. 167–176, 2024.
- [45] M. Sriwahyuni, "Analisis Technology Acceptance Model (TAM) dalam Penggunaan Aplikasi Platform Digital untuk Pembayaran Zakat oleh Muzaki Baznas D.I. Yogyakarta" (in Indonesian), Undergraduate thesis, 2022.
- [46] Sudimanto, C. P. Kurniawan, and M. Christian, "Analisis Pengaruh Persepsi Kemudahan, Keamanan Privasi, Kualitas Sistem, serta Kualitas Informasi Terhadap Kepuasan Pengguna Aplikasi PeduliLindungi" (in Indonesian), *Media Inform.*, vol. 21, no. 3, pp. 211–220, 2023, doi: 10.37595/mediainfo.v21i3.160.
- [47] T. Sugihartono and R. C. Putra, "Analisis Kepuasan Pengguna Menggunakan Technology Acceptance Model pada Sistem Pelayanan Publik" (in Indonesian), *SATIN: Sains Teknol. Inf.*, vol. 6, no. 2, pp. 97–105, 2020, doi: 10.33372/stn.v6i2.651.
- [48] D. Taufiqi and K. R. Ariani, "The effect of good governance, accountability, and transparency of village funds on public trust," *Procedia Soc. Sci. Humanit.*, vol. 1, no. c, pp. 184–191, 2022.
- [49] R. F. Wirawan and R. Yaya, "Pengaruh Akuntabilitas, Transparansi dan Keadilan terhadap Kepercayaan Masyarakat pada Pemerintah Desa: Apakah Kepuasan Masyarakat Memediasi?" (in Indonesian), *Reviu Akunt. Bisnis Indones.*, vol. 8, no. 1, pp. 87–104, 2024, doi: 10.18196/rabin.v8i1.20334.
- [50] A. Yuliana, A. A. Tuasalamony, A. Fath, A. D. Parhusip, A. Febriani, and H. S. Bakhtiar, "Konsti" (in Indonesian), pp. 74–91, 2023.
- [51] A. A. Zahro, "Transformasi E-KTP menjadi KTP Digital melalui Aplikasi Identitas" (in Indonesian), vol. 14, no. 2, pp. 63–71, 2024.
- [52] F. M. Zainudin, R. Nugroho, and H. S. Muamarah, "Dengan Persepsi Keadilan Pajak Sebagai Variabel Intervening" (in Indonesian), *J. Pajak Indones.*, vol. 6, pp. 107–121, 2022.
- [53] M. B. Zaman, I. B. Pamungkas, and W. A. Wibowo, "Pengaruh Privasi dan Keamanan Terhadap Kepercayaan Pengguna" (in Indonesian), vol. 5, no. 4, pp. 891–902, 2022.
- [54] A. Hooda, P. Gupta, A. Jeyaraj, M. Giannakis, and Y. K. Dwivedi, "The effects of trust on behavioral intention and use behavior within e-government contexts," *Int. J. Inf. Manage.*, vol. 67, p. 102553, 2022, doi: 10.1016/j.ijinfomgt.2022.102553.
- [55] S. AlAwadhi, H. Alansari, and A. R. Alsaber, "Explicating trust-building factors impacting the use of e-government services," *Soc. Sci. Comput. Rev.*, vol. 42, no. 5, pp. 1244–1265, 2024, doi: 10.1177/08944393231220757.
- [56] S. C. Chuah, A. A. Mohamad Arshad, and A. Mohd Arifin, "Adoption intention of e-government application for public health risk communication: risk information, social media competence and trust in the government," *J. Public Health Res.*, vol. 13, no. 1, 2024, doi: 10.1177/22799036231217804.
- [57] Z. X. Huang and T. Y. Huang, "Privacy calculus theory in the digital government context: the case of Taiwan's new eID policy," *Soc. Sci. Comput. Rev.*, vol. 41, no. 5, pp. 1745–1766, 2023, doi: 10.1177/08944393221117500.