

Web-Based Birth Certificate Validity Information System for Disdukcapil Magetan Services

Liswardana Gostafi Arifin¹, Ervin Yohannes²

^{1,2} Department of Informatics Engineering, Faculty of Engineering, Universitas Negeri Surabaya

¹febrypratama@unesa.ac.id

²ervinyohannes@unesa.ac.id

Abstract—Digital public services demand strict information security guarantees, particularly in the management of vital civil-registration documents such as birth certificates. This study designs and develops a web-based Birth Certificate Validity System (E-Akta) for the Population and Civil Registration Office (Disdukcapil) of Magetan Regency, replacing an unstructured WhatsApp-based workflow with an application that integrates the principles of an Information Security Management System (ISMS) based on ISO/IEC 27001. The system was built with the Django framework and emphasizes the three pillars of the CIA Triad: Confidentiality, Integrity, and Availability. A custom registration flow records applicant data, followed by mandatory core-data entry, a multi-step document-upload wizard, and a review page prior to permanent storage. The system was evaluated through Black-Box Testing of its functional modules, technical security testing of built-in Django safeguards, and a user-acceptance survey of ten respondents using a five-level Likert scale. The results show that built-in security features—CSRF protection, PBKDF2 password hashing, and server-side validation—successfully preserve data confidentiality and integrity against manipulation attempts, while a real-time status-tracking feature improves service availability for applicants and simplifies monitoring for administrators. Functional testing achieved a 100% success rate, and the user-acceptance survey produced an overall score of 92.8%, categorized as "Very Good."

Keywords—Django; birth certificate validity; information security management system; CIA Triad; Black-Box Testing.

I. INTRODUCTION

The Population and Civil Registration Office (Dinas Kependudukan dan Pencatatan Sipil, Disdukcapil) is the government agency responsible for population administration and civil registration at the district level in Indonesia, as mandated by Law No. 23 of 2006 on Population Administration and its amendment, Law No. 24 of 2013. As one of the institutions responsible for managing vital population data, Disdukcapil of Magetan Regency is required to deliver services that are both fast and secure.

Currently, the process of requesting birth-certificate validity verification—confirming the authenticity of a birth certificate for administrative purposes outside Magetan Regency—still relies on an unstructured communication channel, namely a

WhatsApp-based service called "Pelayanan Administrasi Kependudukan menggunakan WhatsApp" (Pak TuWA). Although convenient, this method has significant weaknesses regarding the security and confidentiality of personal data, and it does not comply with the Information Security Management System (ISMS/SMKI) standards required of public institutions [1].

A birth certificate is an official, stamped document issued by the local civil registration office that records a child's identity—name, date and place of birth, sex, witnesses, and the names of the biological parents—together with the signature of the authorized official. It constitutes proof of the legal relationship between a child and their biological parents [2]. The validity (keabsahan) of research data is likewise a critical concern in scientific work; techniques such as triangulation of sources, methods, and theory are commonly used to verify data authenticity [3].

Indonesia's e-government transformation faces persistent information-security challenges, particularly regarding privacy and data theft, making an effective ISMS aligned with ISO/IEC 27001:2022 an important reference point for public agencies [4]. ISO/IEC 27001 is an international standard for auditing information-system security; it is flexible enough to be tailored to an organization's needs while offering nationally and internationally recognized ISMS certification [5].

Certificate-validity confirmation is a statement issued by Disdukcapil confirming that the data requested by the public matches the previously archived birth-certificate record. It is typically required when an applicant has moved domicile, when the original certificate is damaged or lost, or when discrepancies exist between the submitted data and the archived record.

Based on this background, the objectives of this study are: (1) to design the architecture and user interface of a web-based birth-certificate validity service for Disdukcapil Magetan; (2) to implement the core features of the system, covering account registration, authentication, submission-form completion,

document upload, staff verification, and result download; and (3) to evaluate whether the system satisfies the Confidentiality, Integrity, and Availability principles of an ISMS. The study is scoped to the certificate-validity service only (excluding new-certificate issuance, death certificates, or other population documents), uses simulated data rather than real confidential population records, and focuses its security analysis on the CIA Triad during data exchange and storage.

II. RELATED WORK

Several prior studies have examined the digitalization of civil-registration services. Putri and Sulistio analyzed an official-website-based innovation for birth- and death-certificate services at Disdukcapil Bandar Lampung, finding that online delivery accelerates service and enables access from anywhere, although the website occasionally experienced errors; unlike that work, the present study focuses specifically on certificate-validity confirmation and places stronger emphasis on data-security improvements [6]. Karua and Matasik studied a WhatsApp-based birth-certificate service at Disdukcapil Tana Toraja and found that, while it eased registration and document submission for citizens, the process remained essentially a front-end channel requiring manual verification and was prone to data-handling issues [7]. Ningrum and Nurbaiti evaluated the Sibisa online service in Medan and reported that digitalization accelerated document acquisition, though limited public awareness remained a barrier; this study builds on that finding by designing a deliberately simple registration and login flow while explicitly embedding ISMS principles into the system architecture [8].

III. THEORETICAL FRAMEWORK

A. E-Government and Information Systems

An information system is a foundational concept for digital-era organizations, supporting operations, data-driven decision-making, and service delivery [9]. The adoption of e-government in public bureaucracy leverages information and communication technology to simplify communication and transactional processes between government and citizens [10].

B. Information Security Management System (ISMS)

Information security is the protection of information from unauthorized access, use, disclosure, disruption, modification, or destruction, in order to preserve confidentiality, integrity, and availability. ISO/IEC 27001 is a widely used standard for information-security management, one of whose core processes is risk management—the identification, analysis, evaluation, and control of risks likely to occur. ISO/IEC 27001 defines eleven security-control clauses spanning security policy, organizational security, asset management, human-resources

security, physical and environmental security, communications and operations management, access control, information-system acquisition/development/maintenance, incident management, business-continuity management, and compliance, generally implemented through a Plan–Do–Check–Act (PDCA) management cycle.

C. Django Framework

Django is a web framework that follows the Model-View-Controller (MVC) pattern: the Model is a Python class that interacts with the database layer, the Controller handles application logic and formulates responses to requests, and the View is what users see and interact with. Development guided by the Model-View-Template concept enables applications to be built quickly and effectively, and Django's built-in Model layer accelerates development compared with other object-oriented frameworks [11], [12].

D. Black-Box Testing

Black-box testing treats a system as a "black box" in which the tester observes only inputs and outputs without knowledge of internal implementation details. It is a functional-requirements-focused testing technique that does not require access to source code. Equivalence partitioning, one common black-box technique, groups input values by expected behavior (valid or invalid) to detect defects more efficiently [13], [14].

IV. RESEARCH METHOD

This study follows a Research and Development (R&D) approach, applying software-engineering practices to produce a birth-certificate validity information system that is verified for both functional correctness and information security.

A. Requirements Analysis

Requirements were identified through (1) interviews with prospective applicants and Disdukcapil Magetan staff and analysis of applicable ISMS standards; (2) direct observation of the certificate-validity request process to determine required features; and (3) a literature study of population-administration regulations (Law No. 24 of 2013) and the ISO/IEC 27001 standard. The system was developed on an Apple M1 computer (8 GB RAM, 256 GB SSD, macOS) using Django, Visual Studio Code, draw.io, and Python. Core functional requirements include new-user registration, login, submission-form completion, document upload, staff verification, and delivery of the verified result to the applicant.

B. System Design

Two user roles were identified: applicants (masyarakat), who submit certificate-validity requests, and Disdukcapil staff, who act as administrators/verifiers. Both roles must authenticate

before accessing the system. An applicant submits the required data and uploads supporting documents (JPG format); staff then verify the submission against the archived civil-registry database. If a match is found and approved, the validity document is issued; otherwise, the responsible official decides whether to approve, request revision, or reject the submission. The use-case diagram is shown in Fig. 1.

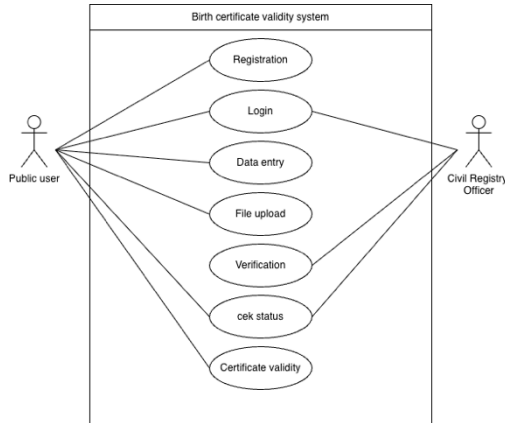


Fig. 1. Use-case diagram of the birth-certificate validity system.

The overall process flow—covering registration, data entry for validity requirements, document upload, staff verification against the archival database, and the approval/rejection decision with accompanying notes—is illustrated in Fig. 2.

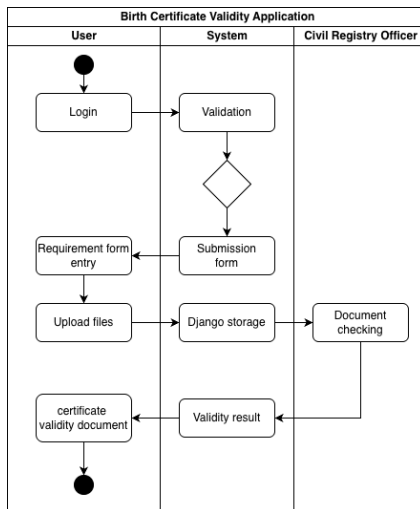


Fig. 2. Activity diagram of the certificate-validity request process.

C. Testing Method

System evaluation combined three approaches: (1) functional Black-Box Testing performed by the researcher; (2) direct technical security testing that simulated unauthorized-access scenarios against the CIA Triad; and (3) a user-acceptance survey completed by ten prospective applicants from Magetan Regency after using the deployed system, distributed via a Google Form shared through WhatsApp. Each Likert item was

scored on a five-level scale (Table I) and summarized using $\text{Percentage} = (\text{Total Score} \div \text{Maximum Score}) \times 100\%$, where the maximum score equals the number of items multiplied by the highest weight (5) and the number of respondents.

TABLE I
FIVE-LEVEL LIKERT ASSESSMENT SCALE

Category	Weight	Percentage Range
Very Good	5	81% – 100%
Good	4	61% – 80%
Fair	3	41% – 60%
Poor	2	21% – 40%
Very Poor	1	0% – 20%

V. RESULTS AND DISCUSSION

A. System Implementation

The system was implemented as a web application with Python 3.9, Django 4.2, an SQLite database (migratable to PostgreSQL), and an HTML5/CSS3/JavaScript front end, organized into three Django apps: accounts (registration, login, e-mail verification, account management), permohonan (submission workflow, document upload, and status notification), and admin_panel (staff dashboard and verification interface). The landing page (Fig. 3) uses a navy-blue, red, and gold color scheme reflecting the identity of the Magetan Regency government.



Fig. 3. System landing page.

Applicants register using their full name, 16-digit National Identity Number (NIK), phone number, e-mail address, and password, with automatic validation of each field; the account is activated only after the applicant confirms an e-mail verification link. Authentication uses the NIK—rather than an arbitrary username—because it is the unique, government-issued identifier already familiar to every applicant. After login, applicants complete a four-step wizard: (1) birth-certificate data entry, (2) upload of five supporting documents (birth certificate, family card, parents' marriage certificate, and

parents' identity cards, accepted as PDF/JPG/PNG up to 5 MB), (3) a review step summarizing all entered data and uploaded files, and (4) formal submission, at which point the system timestamps the request and sets its status to "Submitted." (Fig. 4). Seven status values—Draft, Submitted, Under Verification, Processing, Needs Revision, Completed, and Rejected—are tracked automatically and shown to the applicant in real time, and the finished validity document can be downloaded once the status reaches "Completed."

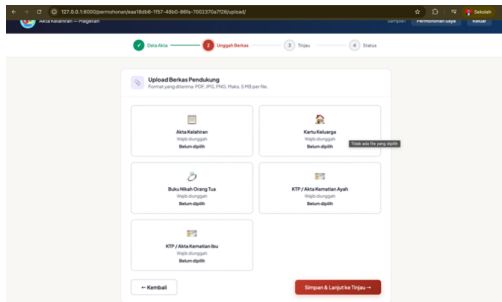


Fig. 4. Multi-step document-upload interface.

Staff access a dedicated administration panel (restricted to accounts with `is_staff = True`) consisting of a dashboard summarizing submissions by status (Fig. 5), a searchable and filterable request list, and a detail view where staff review uploaded documents, change a submission's status, add notes, and upload the signed validity document.

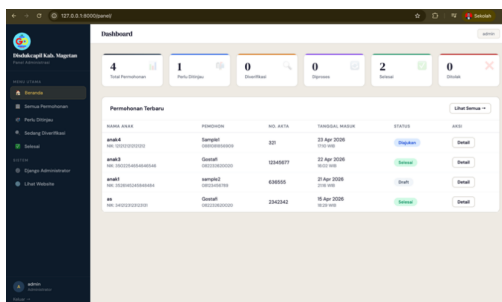


Fig. 5. Administration-panel dashboard.

B. Functional and Technical Security Testing

Black-Box Testing of 48 test cases across 10 system modules achieved a 100% success rate, confirming that registration, authentication, form submission, file upload, staff verification, and document download all behave as specified. Direct technical security testing further verified that Django's built-in safeguards operate correctly: requests without a valid CSRF token are rejected with an HTTP 403 response; passwords are stored as PBKDF2 hashes rather than plaintext; unauthenticated requests to protected URLs are redirected to the login page; non-staff accounts cannot reach the `/panel/` administration routes; one applicant cannot access another applicant's submission by direct URL manipulation; server-side

validation rejects malformed NIK values even when client-side checks are bypassed; and duplicate NIK or e-mail registrations are rejected. All seven technical security scenarios passed, demonstrating that the CSRF protection, PBKDF2 hashing, role-based access control, data isolation, and server-side validation mechanisms jointly satisfy the CIA Triad expected of an ISMS-aligned system. Separately, response-time measurements taken with the browser's network inspector showed that every core page or action (landing page, login, form submission, file upload, status page, document download, and the admin request list) completed in under 800 ms, comfortably within the commonly cited 1,000 ms usability threshold for web applications.

C. User Acceptance Testing

Ten respondents from Magetan Regency—representing civil servants, private employees, students, entrepreneurs, and village officials—tried the deployed system and completed a 21-item Likert questionnaire grouped into four categories: system interface (4 items), functionality and usability (8 items), system security (4 items), and user benefit/satisfaction (5 items). The aggregated results are summarized in Table II.

TABLE II
USER-ACCEPTANCE TESTING RESULTS BY CATEGORY

Category	Items	Score	Max.	%	Category
System interface	4	187	200	93.5%	Very Good
Functionality & usability	8	369	400	92.3%	Very Good
System security	4	182	200	91.0%	Very Good
Benefit & satisfaction	5	236	250	94.4%	Very Good
Overall	21	974	1050	92.8%	Very Good

The overall acceptance score of 92.8% falls within the "Very Good" band (81–100%) of the five-level Likert scale. Respondents rated the interface as clean and easy to understand, the registration and NIK-based login flow as straightforward and trustworthy, and the real-time status tracking as a clear improvement over the previous WhatsApp-based process. One respondent recommended adding a CAPTCHA to the login page to mitigate brute-force or denial-of-service attempts—a suggestion adopted as a direction for future work.

D. Discussion

The multi-step wizard—data entry, document upload, review, and submission—together with stepper indicators, gave applicants a clear sense of progress and reduced confusion relative to a single long form. Using the NIK as the login identifier also proved effective, since it is an identifier applicants already possess and recognize, lowering the barrier to registration compared with an unfamiliar username scheme.

On the security dimension, both the technical tests (Section V-B) and the user-acceptance survey (Section V-C) indicate that the system meets the Confidentiality, Integrity, and Availability principles expected of an ISMS aligned with ISO/IEC 27001. Respondents specifically rated the system as more secure than the prior WhatsApp-based channel (Pak TuWA), supporting the conclusion that the developed system is a suitable and more secure replacement for that informal workflow.

VI. CONCLUSION

A web-based birth-certificate validity information system was successfully designed and implemented for Disdukcapil Magetan using Django 4.2 and Python 3.9, organized into three Django applications (accounts, permohonan, and admin_panel) and a four-step wizard interface (data entry, document upload, review, submission) that applicants found structured and easy to use. All core features—registration with e-mail verification, NIK-based login, form completion, five-document upload, staff verification, and result download—were implemented and validated through Black-Box Testing of 48 test cases across 10 modules, achieving a 100% success rate. The system was further shown to satisfy the Confidentiality, Integrity, and Availability principles of an ISMS aligned with ISO/IEC 27001, evidenced by a 92.8% "Very Good" score from ten user-acceptance respondents and by passing all seven technical security scenarios covering CSRF protection, PBKDF2 password hashing, role-based access control, data isolation, and server-side validation. These results support the system's readiness to replace the previous WhatsApp-based certificate-validity workflow, which did not meet information-security standards.

Future work should include migrating the database from SQLite to PostgreSQL to improve concurrency in production, integrating an SMS-gateway or WhatsApp API for proactive status notifications, and adding a CAPTCHA mechanism on the login page to further mitigate brute-force and denial-of-service risks.

ACKNOWLEDGMENT

The author thanks the supervisor, Ervin Yohannes, S.Kom., M.Kom., M.Sc., Ph.D., for guidance throughout this research, and Disdukcapil Kabupaten Magetan and the survey respondents for their cooperation during system testing.

REFERENCES

- [1] A. Satria and F. Hidayat, "Perancangan Sistem Manajemen Keamanan Informasi (SMKI) pada Dinas Kependudukan dan Pencatatan Sipil Berbasis ISO/IEC 27001:2022 untuk Penguatan Perlindungan Data Pribadi dan Kedaulatan Digital," *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, vol. 8, no. 5, 2025, doi: 10.32672/jnkti.v8i5.9611.
- [2] T. A. Sugeng, "Pentingnya Akta Kelahiran Sebagai Identitas Anak yang Dilahirkan," *Jurnal Fenomena*, vol. 21, no. 2, 2023.
- [3] D. Susanto, Risnita, and M. S. Jailani, "Teknik Pemeriksaan Keabsahan Data Dalam Penelitian Ilmiah," *Jurnal QOSIM Jurnal Pendidikan Sosial & Humaniora*, vol. 1, no. 1, 2023, doi: 10.61104/jq.v1i1.60.
- [4] "Perancangan Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan ISO 27001:2022 (Studi Kasus Data Center Dinas Komunikasi dan Informatika Kota Tangerang Selatan)," *Jurnal Ilmiah Komputasi*, vol. 22, no. 4, 2023, doi: 10.32409/jikstik.22.4.3447.
- [5] A. Setyaningrum, Y. Kurniawan, and R. Setiawan, "Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO 27001:2013 pada Kominfo Kabupaten Malang," *Kurawal – Jurnal Teknologi, Informasi dan Industri*, vol. 6, no. 1, 2023, doi: 10.33479/kurawal.v6i1.1029.
- [6] D. M. Putri and E. B. Sulistio, "Inovasi Pelayanan Akta Kelahiran Dan Akta Kematian Berbasis Online Di Dinas Kependudukan Dan Pencatatan Sipil Kota Bandar Lampung," *Administrativa: Jurnal Birokrasi, Kebijakan dan Pelayanan Publik*, vol. 4, no. 3, 2022, doi: 10.23960/administrativa.v4i3.174.
- [7] G. A. Karua and A. L. Matasik, "Analisis Inovasi Pelayanan Akta Kelahiran Online," *Jurnal Ekonomi, Bisnis dan Terapan (JESIT)*, vol. 3, no. 2, 2023, doi: 10.47178/2qt88j49.
- [8] L. D. Ningrum and Nurbaiti, "Inovasi Pelayanan Administrasi Kependudukan Melalui Sibisa Online di Disdukcapil Kota Medan," *Innovative: Journal of Social Science Research*, vol. 3, no. 4, 2023.
- [9] E. Satu, "Sistem Informasi: Definisi, Manfaat, dan Peran dalam Era Digital," 30 April, 2024.
- [10] H. Heriyanto, "Urgensi Penerapan E-Government Dalam Pelayanan Publik," *Musamus Journal of Public Administration*, vol. 4, no. 2, 2022, doi: 10.35724/mjpa.v4i2.4128.
- [11] H. Sabita, R. Herwanto, Y. Syafitri, and B. D. Prasetyo, "Pengembangan Aplikasi Akreditasi Program Studi Berbasis Framework Django," *Jurnal Informatika*, vol. 22, no. 1, 2022, doi: 10.30873/ji.v22i1.3143.
- [12] H. Raihan and A. Voutama, "Pengujian Black Box Pada Aplikasi Database Perguruan Tinggi dengan Teknik Equivalence Partition," *Antivirus: Jurnal Ilmiah Teknik Informatika*, vol. 17, no. 1, 2023, doi: 10.35457/antivirus.v17i1.2501.
- [13] A. Karim, "Penyuluhan Hukum Tentang Pentingnya Akta Kelahiran Bagi Anak Sebagai Warga Negara," *Jurnal Ilmiah Padma Sri Kreshna*, vol. 3, no. 1, 2021, doi: 10.37631/psk.v3i1.395.
- [14] I. Fadilla, N. Sartika, and R. Bisma, "Perancangan Sistem Informasi Manajemen Risiko berdasarkan ISO 27001:2013 (Sistem Manajemen Keamanan Informasi)," *JEISBI*, vol. 2, 2021.