



ISSN 2621- 458X

Keamanan Identitas Digital dan Mekanisme Autentikasi dalam Pelayanan Pemerintahan Digital: Analisis Risiko Tata Kelola SPBE di Indonesia

Kurnia Yuliani Nur

Program Studi Magister Administrasi Publik, ITBA Al Gazali Barru
kurniayulianinur@algazali.ac.id

ABSTRAK

Transformasi digital dalam penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) menjadikan identitas digital sebagai komponen strategis dalam penyediaan layanan publik yang aman, efisien, dan terintegrasi. Namun, peningkatan penggunaan layanan digital juga diikuti oleh berbagai risiko keamanan, seperti pencurian identitas, penyalahgunaan akun, kebocoran data pribadi, serta lemahnya mekanisme autentikasi. Penelitian ini bertujuan menganalisis keamanan identitas digital dan mekanisme autentikasi dalam penyelenggaraan SPBE di Indonesia melalui perspektif risiko tata kelola. Penelitian menggunakan metode kualitatif dengan pendekatan studi kepustakaan (*library research*). Data diperoleh dari artikel ilmiah, buku, standar internasional, dan dokumen kelembagaan yang relevan, kemudian dianalisis menggunakan teknik *content analysis*. Hasil penelitian menunjukkan bahwa tantangan utama implementasi identitas digital meliputi fragmentasi sistem autentikasi, belum optimalnya interoperabilitas antarinstansi, tingginya risiko penyalahgunaan data pribadi, serta masih rendahnya literasi keamanan digital masyarakat. Penelitian ini juga menegaskan bahwa penerapan autentikasi berbasis risiko, penguatan tata kelola perlindungan data pribadi, penerapan *Multi-Factor Authentication* (MFA), *Single Sign-On* (SSO), serta federasi identitas menjadi strategi penting dalam meningkatkan keamanan layanan pemerintahan digital. Penelitian ini memberikan rekomendasi konseptual bagi penguatan tata kelola SPBE melalui integrasi regulasi, teknologi, dan peningkatan kapasitas pengguna sehingga mampu mewujudkan pelayanan publik digital yang aman, terpercaya, inklusif, dan berkelanjutan.

Kata kunci: identitas digital, autentikasi, SPBE, keamanan siber, tata kelola digital.



lisensi CC BY

ABSTRACT

Digital transformation in the implementation of Indonesia's Electronic-Based Government System (SPBE) has positioned digital identity as a strategic component for delivering secure, efficient, and integrated public services. However, the rapid expansion of digital government services has also increased cybersecurity risks, including identity theft, account compromise, personal data breaches, and weaknesses in authentication mechanisms. This study aims to analyze digital identity security and authentication mechanisms in the implementation of SPBE from a governance risk perspective. The research employed a qualitative approach using a library research method. Data were collected from scholarly articles, books, international standards, and institutional publications and analyzed through content analysis. The findings indicate that the primary challenges in implementing digital identity include fragmented authentication systems, limited interoperability among government agencies, increased risks of personal data misuse, and insufficient public awareness of cybersecurity practices. The study further demonstrates that risk-based authentication, stronger personal data governance, the implementation of Multi-Factor Authentication (MFA), Single Sign-On (SSO), and identity federation are essential strategies for strengthening the security of digital government services. This research offers conceptual recommendations for enhancing SPBE governance through the integration of regulatory frameworks, technological innovation, and user capacity development to establish secure, trustworthy, inclusive, and sustainable digital public services.

Keywords: digital identity, authentication, electronic-based government system, cybersecurity, digital governance.

A.PENDAHULUAN

Transformasi digital telah menjadi agenda strategis berbagai negara dalam meningkatkan kualitas tata kelola pemerintahan dan pelayanan publik. Perkembangan teknologi informasi mendorong pemerintah untuk mengintegrasikan berbagai layanan secara elektronik agar lebih efektif, efisien, transparan, dan berorientasi pada kebutuhan masyarakat. Di Indonesia, transformasi tersebut diwujudkan melalui implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) yang mengintegrasikan proses administrasi pemerintahan, pelayanan publik, dan tata kelola data secara digital. Namun, keberhasilan SPBE tidak hanya ditentukan oleh tersedianya infrastruktur teknologi, tetapi juga oleh kemampuan pemerintah dalam menjamin keamanan identitas digital setiap pengguna layanan. Identitas digital menjadi fondasi utama dalam memastikan bahwa setiap individu yang mengakses sistem merupakan pihak yang sah, sehingga mampu mencegah penyalahgunaan layanan, pencurian identitas, maupun akses tanpa kewenangan. Oleh karena itu, penguatan identitas digital merupakan salah satu prasyarat penting dalam

membangun pemerintahan digital yang aman, terpercaya, dan berkelanjutan (Temoshok et al., 2025; Republik Indonesia, 2023).

Perkembangan identitas digital saat ini tidak lagi dipandang sekadar sebagai akun untuk mengakses layanan elektronik, melainkan sebagai representasi resmi individu yang terhubung dengan berbagai layanan pemerintahan, keuangan, kesehatan, pendidikan, hingga transaksi elektronik lainnya. Standar Digital Identity Guidelines yang diterbitkan oleh National Institute of Standards and Technology (NIST) menjelaskan bahwa sistem identitas digital harus dibangun melalui tiga komponen utama, yaitu *identity proofing*, *authentication*, dan *federation* untuk menjamin tingkat kepercayaan identitas pengguna dalam lingkungan digital. Pendekatan tersebut menekankan bahwa proses autentikasi yang kuat harus didukung oleh pembuktian identitas yang valid serta mekanisme pertukaran identitas yang aman antarpemangku layanan. Dengan demikian, identitas digital tidak hanya berfungsi sebagai sarana login, tetapi juga menjadi infrastruktur kepercayaan (*trust infrastructure*) yang mendukung interoperabilitas berbagai layanan pemerintahan digital secara aman dan terintegrasi (Temoshok et al., 2025).

Dalam konteks Indonesia, implementasi identitas digital memperoleh perhatian yang semakin besar seiring dengan diterapkannya Identitas Kependudukan Digital (IKD), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Peraturan Presiden Nomor 82 Tahun 2023 mengenai Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional. Berbagai kebijakan tersebut menunjukkan komitmen pemerintah untuk membangun ekosistem pemerintahan digital yang terintegrasi sekaligus memberikan perlindungan terhadap data pribadi masyarakat. Meskipun demikian, implementasi identitas digital masih menghadapi berbagai tantangan, antara lain fragmentasi sistem autentikasi antarinstansi, belum optimalnya interoperabilitas layanan, meningkatnya ancaman serangan siber, serta rendahnya tingkat literasi keamanan digital masyarakat. Kondisi tersebut mengindikasikan bahwa transformasi digital memerlukan tata kelola keamanan informasi yang komprehensif agar mampu menjaga kepercayaan publik sekaligus menjamin keberlangsungan pelayanan pemerintahan digital di Indonesia (Republik Indonesia, 2022; Republik Indonesia, 2023).

Meningkatnya ancaman terhadap identitas digital, seperti *phishing*, pencurian kredensial, penyalahgunaan data pribadi, hingga pengambilalihan akun (*account takeover*), menunjukkan

bahwa mekanisme autentikasi konvensional berbasis kata sandi dan *One-Time Password* (OTP) tidak lagi memadai untuk melindungi layanan pemerintahan digital yang memproses data strategis. Oleh karena itu, berbagai standar internasional mendorong penerapan autentikasi berbasis risiko melalui *Multi-Factor Authentication* (MFA), *passkey*, autentikasi berbasis kriptografi, serta federasi identitas untuk meningkatkan tingkat jaminan keamanan. Selain aspek teknologi, keberhasilan implementasi identitas digital juga memerlukan tata kelola perlindungan data pribadi, pengawasan akses, serta peningkatan literasi digital masyarakat agar keamanan sistem dapat berjalan seiring dengan kemudahan penggunaan layanan. Berdasarkan kondisi tersebut, penelitian ini bertujuan menganalisis keamanan identitas digital dan mekanisme autentikasi dalam pelayanan pemerintahan digital melalui perspektif risiko tata kelola SPBE di Indonesia sehingga dapat memberikan rekomendasi penguatan kebijakan maupun implementasi teknis yang lebih efektif di masa mendatang (Temoshok et al., 2025; Mazzocca et al., 2024).

Perkembangan teknologi digital telah mengubah paradigma penyelenggaraan pemerintahan di berbagai negara, termasuk Indonesia, dari layanan yang bersifat administratif menjadi layanan yang terintegrasi, adaptif, dan berorientasi pada kebutuhan masyarakat. Dalam konteks tersebut, identitas digital menjadi komponen fundamental yang memungkinkan setiap pengguna memperoleh akses terhadap berbagai layanan pemerintah secara aman dan efisien. Pemerintah Indonesia melalui implementasi SPBE telah mendorong integrasi layanan digital lintas instansi sebagai bagian dari percepatan transformasi digital nasional. Namun, peningkatan jumlah layanan digital juga diikuti oleh meningkatnya risiko keamanan siber, seperti pencurian identitas, penyalahgunaan akun, kebocoran data pribadi, serta serangan *phishing* yang dapat mengurangi kepercayaan masyarakat terhadap layanan pemerintah. Oleh karena itu, penguatan keamanan identitas digital tidak hanya menjadi kebutuhan teknis, tetapi juga merupakan strategi untuk menjaga keberlanjutan tata kelola pemerintahan digital yang akuntabel, transparan, dan berorientasi pada kepentingan publik (Temoshok et al., 2025; Republik Indonesia, 2023).

Sejalan dengan perkembangan tersebut, berbagai organisasi internasional menekankan bahwa sistem identitas digital modern harus dibangun berdasarkan prinsip keamanan, interoperabilitas, perlindungan privasi, dan pengalaman pengguna (*user experience*). NIST melalui SP 800-63-4 menegaskan bahwa pengelolaan identitas digital tidak hanya mencakup proses autentikasi, tetapi juga manajemen risiko, perlindungan data pribadi, serta evaluasi

berkelanjutan terhadap tingkat jaminan identitas (*Identity Assurance Level*), autentikator (*Authenticator Assurance Level*), dan federasi identitas (*Federation Assurance Level*). Di sisi lain, perkembangan teknologi *Verifiable Credentials* dan *Decentralized Identifiers* yang telah direkomendasikan oleh W3C memberikan paradigma baru dalam pengelolaan identitas digital yang lebih berpusat pada pengguna (*user-centric identity*), sehingga memungkinkan proses verifikasi identitas dilakukan secara kriptografis tanpa harus memperlihatkan seluruh data pribadi kepada penyedia layanan. Pendekatan tersebut dinilai mampu meningkatkan keamanan sekaligus memperkuat perlindungan privasi pengguna dalam ekosistem pemerintahan digital.

Di Indonesia, penguatan keamanan identitas digital semakin memperoleh dasar hukum yang kuat melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional. Kedua regulasi tersebut menegaskan bahwa pengelolaan data pribadi harus dilaksanakan secara bertanggung jawab dengan mengedepankan prinsip legalitas, akuntabilitas, transparansi, serta keamanan informasi. Walaupun demikian, implementasi di lapangan masih menghadapi berbagai tantangan, seperti belum seragamnya mekanisme autentikasi antarinstansi, keterbatasan interoperabilitas sistem, lemahnya pengendalian hak akses, dan belum optimalnya penerapan standar keamanan informasi secara nasional. Kondisi tersebut menunjukkan bahwa keberhasilan implementasi SPBE tidak hanya ditentukan oleh pembangunan infrastruktur digital, tetapi juga oleh kesiapan tata kelola keamanan identitas yang mampu mengurangi risiko penyalahgunaan data sekaligus meningkatkan kepercayaan masyarakat terhadap layanan pemerintah berbasis elektronik.

Berdasarkan berbagai permasalahan tersebut, penelitian ini memfokuskan kajian pada analisis keamanan identitas digital dan mekanisme autentikasi dalam perspektif risiko tata kelola SPBE di Indonesia. Kajian ini menjadi penting karena sebagian besar penelitian sebelumnya lebih banyak membahas aspek teknis keamanan informasi atau implementasi SPBE secara umum, sedangkan kajian yang mengintegrasikan keamanan identitas digital, mekanisme autentikasi berbasis risiko, perlindungan data pribadi, dan tata kelola pemerintahan digital masih relatif terbatas. Penelitian ini diharapkan dapat memberikan kontribusi konseptual dalam pengembangan model tata kelola identitas digital yang selaras dengan perkembangan standar internasional serta memberikan rekomendasi praktis bagi pemerintah dalam memperkuat kebijakan keamanan

identitas digital, meningkatkan interoperabilitas layanan publik, serta membangun sistem autentikasi yang aman, inklusif, dan berkelanjutan sebagai fondasi transformasi pemerintahan digital di Indonesia.

B.METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kualitatif dengan pendekatan studi kepustakaan (*library research*) yang bertujuan menganalisis keamanan identitas digital dan mekanisme autentikasi dalam penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) di Indonesia. Pendekatan studi kepustakaan dipilih karena memungkinkan peneliti melakukan kajian secara sistematis terhadap berbagai teori, konsep, kebijakan, standar internasional, serta hasil penelitian terdahulu yang relevan dengan topik penelitian. Menurut Snyder (2019), *library research* memberikan landasan konseptual yang kuat untuk mengidentifikasi kesenjangan penelitian sekaligus menghasilkan sintesis ilmiah yang komprehensif. Data penelitian diperoleh dari berbagai sumber sekunder berupa artikel jurnal internasional dan nasional, prosiding ilmiah, buku referensi, standar internasional, serta dokumen kelembagaan yang membahas keamanan identitas digital, autentikasi, perlindungan data pribadi, keamanan siber, dan tata kelola pemerintahan digital. Literatur utama yang menjadi rujukan meliputi Digital Identity Guidelines yang diterbitkan oleh National Institute of Standards and Technology (NIST), pedoman keamanan identitas digital dari European Union Agency for Cybersecurity (ENISA), rekomendasi Verifiable Credentials dari World Wide Web Consortium (W3C), serta berbagai publikasi mengenai tata kelola pemerintahan digital dan identitas digital (Temoshok et al., 2025; ENISA, 2023; W3C, 2025).

Teknik pengumpulan data dilakukan melalui tahapan identifikasi, seleksi, evaluasi kritis, klasifikasi, dan sintesis terhadap berbagai literatur yang relevan dengan fokus penelitian. Selanjutnya, data dianalisis menggunakan analisis isi (*content analysis*) untuk mengidentifikasi pola, konsep, hubungan antartema, serta merumuskan interpretasi yang berkaitan dengan risiko keamanan identitas digital dan mekanisme autentikasi dalam penyelenggaraan SPBE. Analisis dilakukan melalui tahapan reduksi data, pengelompokan berdasarkan tema, penyajian hasil analisis secara sistematis, dan penarikan kesimpulan sesuai dengan tujuan penelitian. Untuk meningkatkan validitas hasil penelitian, dilakukan triangulasi sumber dengan membandingkan berbagai hasil

penelitian, standar internasional, serta dokumen ilmiah dari lembaga yang memiliki otoritas dalam bidang identitas digital dan keamanan siber sehingga diperoleh sintesis yang objektif, konsisten, dan komprehensif mengenai penguatan keamanan identitas digital dalam tata kelola pemerintahan digital (Krippendorff, 2019; Bowen, 2009).Keamanan Identitas Digital dan Mekanisme Autentikasi dalam Pelayanan Pemerintahan Digital: Analisis Risiko Tata Kelola SPBE di Indonesia.



Gambar 1 Kerangka Konseptual Penelitian Keamanan Identitas Digital, Mekanisme Autentikasi, dan Tata Kelola SPBE di Indonesia

Gambar 1 menggambarkan kerangka konseptual penelitian yang menunjukkan keterkaitan antara **keamanan identitas digital**, **mekanisme autentikasi**, dan **tata kelola Sistem Pemerintahan Berbasis Elektronik (SPBE)** di Indonesia. Keamanan identitas digital merupakan fondasi utama dalam menjamin kerahasiaan, integritas, dan keaslian identitas pengguna pada layanan pemerintahan digital. Aspek ini menjadi sangat penting mengingat semakin meningkatnya penggunaan layanan elektronik pemerintah yang memproses data pribadi dan informasi strategis masyarakat. Untuk menjaga keamanan tersebut, diperlukan mekanisme autentikasi yang mampu memastikan bahwa setiap akses ke sistem hanya dilakukan oleh pengguna yang memiliki hak dan kewenangan sesuai ketentuan. Dengan demikian, autentikasi berfungsi sebagai lapisan pengamanan yang menghubungkan identitas digital dengan proses akses terhadap layanan pemerintahan secara aman dan terpercaya.

Selanjutnya, penerapan keamanan identitas digital dan mekanisme autentikasi yang efektif akan mendukung terwujudnya tata kelola SPBE yang lebih baik. Tata kelola SPBE tidak hanya menekankan integrasi teknologi informasi, tetapi juga mencakup pengelolaan keamanan informasi, perlindungan data pribadi, interoperabilitas sistem, akuntabilitas, serta peningkatan kualitas pelayanan publik. Hubungan ketiga komponen tersebut menunjukkan bahwa keberhasilan implementasi SPBE bergantung pada sinergi antara pengelolaan identitas digital yang aman, penerapan autentikasi yang sesuai dengan tingkat risiko layanan, serta tata kelola yang mampu menjamin kepercayaan masyarakat terhadap penyelenggaraan pemerintahan digital. Oleh karena itu, kerangka konseptual ini menjadi dasar dalam menganalisis risiko keamanan identitas digital sekaligus merumuskan strategi penguatan tata kelola SPBE yang aman, efektif, dan berkelanjutan di Indonesia.

B.HASIL PENELITIAN DAN PEMBAHASAN

➤ Hasil penelitian

Implementasi identitas digital dalam Sistem Pemerintahan Berbasis Elektronik (SPBE) menunjukkan bahwa keamanan identitas merupakan fondasi utama dalam penyelenggaraan pelayanan pemerintahan digital. Identitas digital tidak lagi dipahami hanya sebagai akun untuk mengakses aplikasi pemerintah, melainkan sebagai representasi resmi warga negara yang digunakan untuk memperoleh berbagai layanan publik secara elektronik. Oleh karena itu, identitas digital harus mampu menjamin bahwa setiap individu yang mengakses sistem benar-benar merupakan pihak yang berhak melalui proses verifikasi dan autentikasi yang dapat dipertanggungjawabkan. Dalam konteks SPBE, penerapan identitas digital menjadi instrumen penting untuk meningkatkan efisiensi layanan sekaligus membangun kepercayaan masyarakat terhadap transformasi digital pemerintahan. Hasil kajian menunjukkan bahwa keberhasilan implementasi identitas digital sangat dipengaruhi oleh kemampuan pemerintah dalam menjaga kerahasiaan, integritas, dan ketersediaan data pengguna melalui tata kelola keamanan informasi yang komprehensif.

Hasil penelitian juga menunjukkan bahwa implementasi Identitas Kependudukan Digital (IKD) memberikan berbagai manfaat dalam mempercepat proses pelayanan administrasi publik,

seperti verifikasi data kependudukan, pengurangan penggunaan dokumen fisik, serta integrasi layanan antarinstansi. Namun demikian, digitalisasi identitas tersebut juga menghadirkan berbagai risiko keamanan yang semakin kompleks. Konsentrasi data pribadi dalam satu ekosistem digital meningkatkan potensi penyalahgunaan identitas apabila sistem autentikasi dan pengendalian akses tidak dirancang secara memadai. Risiko tersebut meliputi pencurian identitas, manipulasi data, akses tidak sah terhadap layanan publik, hingga menurunnya tingkat kepercayaan masyarakat terhadap pemerintah. Oleh karena itu, implementasi identitas digital harus disertai dengan penerapan prinsip perlindungan data pribadi, pembatasan akses berdasarkan kewenangan, serta mekanisme audit yang mampu mendeteksi setiap aktivitas yang berpotensi mengancam keamanan sistem.

Selain aspek perlindungan data, penelitian ini menemukan bahwa tantangan terbesar dalam tata kelola identitas digital di Indonesia masih berkaitan dengan fragmentasi sistem autentikasi antarinstansi pemerintah. Sebagian besar layanan publik masih menerapkan mekanisme login secara terpisah sehingga masyarakat harus memiliki banyak akun, menggunakan kata sandi yang berbeda, serta melakukan verifikasi identitas secara berulang. Kondisi tersebut tidak hanya menurunkan kualitas pengalaman pengguna, tetapi juga meningkatkan risiko keamanan akibat penggunaan kembali kata sandi pada berbagai aplikasi pemerintah. Di sisi lain, penggunaan autentikasi berbasis kata sandi dan One-Time Password (OTP) sebagai mekanisme utama masih memiliki berbagai keterbatasan karena rentan terhadap serangan phishing, malware, rekayasa sosial, maupun pengambilalihan nomor telepon. Temuan ini menunjukkan bahwa peningkatan interoperabilitas SPBE perlu diiringi dengan penerapan standar autentikasi yang lebih kuat dan terintegrasi agar keamanan identitas digital dapat terjaga secara optimal.

Temuan berikutnya menunjukkan bahwa implementasi identitas digital tidak hanya menghadapi tantangan teknis, tetapi juga tantangan sosial yang berkaitan dengan inklusivitas layanan digital. Sebagian masyarakat masih mengalami keterbatasan akses terhadap perangkat digital, jaringan internet, maupun literasi teknologi sehingga berpotensi mengalami kesulitan dalam memanfaatkan layanan pemerintahan berbasis digital. Selain itu, meningkatnya interoperabilitas data antarinstansi menimbulkan kebutuhan akan tata kelola yang lebih akuntabel terkait pemanfaatan data pribadi masyarakat. Pertukaran data antarinstansi harus dilakukan berdasarkan tujuan yang jelas, memperhatikan prinsip minimisasi data, serta dilengkapi

mekanisme pengawasan yang transparan agar hak-hak pemilik data tetap terlindungi. Dengan demikian, keberhasilan implementasi identitas digital dalam SPBE tidak hanya ditentukan oleh kecanggihan teknologi autentikasi, tetapi juga oleh kemampuan pemerintah membangun sistem tata kelola yang aman, transparan, akuntabel, dan inklusif bagi seluruh lapisan masyarakat.

Tabel 1 Peta Risiko Keamanan Identitas Digital dan Strategi Mitigasi dalam Pelayanan Pemerintahan

No	Risiko Utama	Kondisi yang Berpotensi Terjadi	Dampak terhadap Pelayanan Publik	Strategi Mitigasi
1	Pencurian kredensial akun	Phishing, malware, penggunaan ulang kata sandi	Pengambilalihan akun, penyalahgunaan layanan pemerintah	Multi-Factor Authentication (MFA), edukasi anti-phishing, deteksi perangkat, pemulihan akun yang aman
2	Kelemahan autentikasi OTP	OTP dicuri melalui SIM swap atau rekayasa sosial	Akses tidak sah terhadap layanan digital	Authenticator Application, autentikasi berbasis kriptografi (Passkey/FIDO2), pembatasan penggunaan OTP
3	Penyalahgunaan data biometrik	Penggunaan biometrik tanpa pengamanan yang memadai	Kebocoran data biometrik dan pelanggaran privasi	Perlindungan template biometrik, liveness detection, pembatasan tujuan penggunaan, persetujuan pengguna
4	Fragmentasi identitas digital	Setiap instansi menggunakan sistem autentikasi berbeda	Duplikasi data, rendahnya interoperabilitas, lemahnya audit	Single Sign-On (SSO), Federated Identity, standar autentikasi nasional
5	Eksklusi digital	Keterbatasan perangkat, jaringan internet, dan literasi digital	Rendahnya akses masyarakat terhadap layanan digital	Alternatif autentikasi, layanan bantuan langsung, peningkatan literasi digital
6	Penyalahgunaan akses internal	Hak akses petugas melebihi kewenangan	Kebocoran data, penyalahgunaan wewenang, menurunnya kepercayaan publik	

Sumber: Disusun oleh penulis berdasarkan sintesis berbagai referensi mengenai keamanan identitas digital, tata kelola SPBE, perlindungan data pribadi, dan standar autentikasi digital.

Mekanisme autentikasi merupakan komponen utama dalam menjamin keamanan identitas digital pada penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE). Hasil penelitian menunjukkan bahwa penerapan autentikasi sebaiknya disesuaikan dengan tingkat risiko setiap jenis layanan publik. Layanan yang hanya menyediakan informasi umum dapat menggunakan autentikasi dasar karena tidak melibatkan data pribadi yang sensitif. Sebaliknya, layanan yang berkaitan dengan perubahan data kependudukan, perpajakan, bantuan sosial, layanan kesehatan, maupun transaksi administratif yang memiliki konsekuensi hukum memerlukan mekanisme autentikasi yang lebih kuat. Pendekatan berbasis risiko tersebut memungkinkan pemerintah menerapkan pengamanan secara proporsional sesuai tingkat ancaman yang dihadapi, sehingga keseimbangan antara keamanan, kemudahan penggunaan, dan efisiensi pelayanan tetap dapat terjaga. Selain itu, penggunaan autentikasi berlapis (Multi-Factor Authentication/MFA) perlu diarahkan pada teknologi yang lebih aman dibandingkan metode konvensional berbasis kata sandi dan OTP, sehingga mampu meminimalkan potensi serangan siber terhadap akun pengguna layanan pemerintahan digital.

Hasil penelitian juga menunjukkan bahwa keberhasilan implementasi identitas digital tidak hanya bergantung pada kekuatan autentikasi, tetapi juga pada tata kelola perlindungan data pribadi yang diterapkan oleh setiap instansi pemerintah. Integrasi layanan digital melalui SPBE memungkinkan pertukaran data antarinstansi berlangsung lebih cepat dan efisien, namun kondisi tersebut juga meningkatkan risiko penyalahgunaan data apabila tidak disertai mekanisme pengendalian yang memadai. Oleh karena itu, setiap proses pemanfaatan data harus memiliki dasar hukum yang jelas, tujuan pemrosesan yang spesifik, pembatasan hak akses sesuai kewenangan, serta mekanisme audit yang mampu mencatat seluruh aktivitas penggunaan data. Tata kelola yang akuntabel menjadi prasyarat penting untuk menjaga kepercayaan masyarakat terhadap pelayanan pemerintahan digital sekaligus memastikan bahwa perlindungan hak-hak pemilik data tetap menjadi prioritas utama dalam setiap proses transformasi digital pemerintahan.

Temuan berikutnya menunjukkan bahwa tingkat keberhasilan implementasi identitas digital sangat dipengaruhi oleh kesiapan masyarakat dalam memanfaatkan teknologi digital. Perbedaan kemampuan literasi digital, keterbatasan perangkat, akses internet, maupun kemampuan menggunakan aplikasi menjadi faktor yang menentukan tingkat adopsi layanan pemerintahan digital. Oleh karena itu, desain sistem autentikasi tidak hanya harus memenuhi aspek

keamanan, tetapi juga harus memperhatikan kemudahan penggunaan (usability), aksesibilitas, serta kebutuhan kelompok masyarakat yang memiliki keterbatasan teknologi. Pemerintah perlu menyediakan mekanisme pemulihan akun yang sederhana namun tetap aman, layanan bantuan bagi masyarakat yang mengalami kendala autentikasi, serta edukasi keamanan digital yang mudah dipahami. Pendekatan tersebut diyakini mampu meningkatkan tingkat adopsi layanan digital sekaligus mengurangi risiko kegagalan autentikasi akibat rendahnya literasi keamanan informasi di masyarakat.

Berdasarkan keseluruhan hasil kajian, penelitian ini menunjukkan bahwa penguatan keamanan identitas digital dalam SPBE memerlukan tata kelola yang terintegrasi antara aspek regulasi, teknologi, dan pelayanan publik. Dari sisi regulasi diperlukan harmonisasi kebijakan mengenai perlindungan data pribadi, identitas digital, dan interoperabilitas layanan pemerintah. Dari sisi teknologi dibutuhkan penerapan standar autentikasi nasional yang mampu mengakomodasi berbagai tingkat risiko layanan, disertai pengelolaan hak akses, pencatatan aktivitas sistem, serta mekanisme pengawasan yang berkelanjutan. Sementara itu, dari sisi pelayanan publik diperlukan desain layanan yang mudah digunakan, inklusif, serta mampu memberikan rasa aman kepada masyarakat ketika memanfaatkan layanan pemerintahan digital. Dengan pendekatan tersebut, implementasi SPBE di Indonesia diharapkan tidak hanya meningkatkan efisiensi pelayanan publik, tetapi juga memperkuat kepercayaan masyarakat terhadap transformasi digital pemerintahan secara berkelanjutan. Pada bagian implikasi penelitian, seluruh pembahasan difokuskan pada penguatan kebijakan, tata kelola data, mekanisme pemulihan akun, dan evaluasi berkala tanpa mengaitkan rekomendasi penggunaan perangkat lunak analisis tertentu.

Tabel 2 Rekomendasi Mekanisme Autentikasi Berdasarkan Tingkat Risiko Layanan Pemerintahan

Tingkat Risiko	Jenis Layanan	Dampak Apabila Terjadi Penyalahgunaan	Rekomendasi Mekanisme Autentikasi
Rendah	Informasi publik, pelacakan status layanan umum	Dampak minimal terhadap pengguna	Kata sandi yang kuat, CAPTCHA, dan pemantauan aktivitas
Menengah	Permohonan surat, pembaruan profil, akses dokumen pribadi	Perubahan data tanpa hak dan penyalahgunaan akun	Multi-Factor Authentication (MFA), notifikasi aktivitas akun, deteksi perangkat
Tinggi	Perubahan data kependudukan, layanan perpajakan, kesehatan, bantuan sosial	Kerugian hukum, finansial, dan sosial	MFA berbasis autentikator, autentikasi adaptif berbasis risiko, verifikasi ulang identitas
Sangat Tinggi	Penandatanganan dokumen elektronik, akses administrator sistem, basis data nasional	Kebocoran data strategis dan gangguan layanan pemerintahan	Autentikasi berstandar tinggi, pengelolaan hak akses berlapis, audit real-time, prinsip <i>least privilege</i>

Sumber: Disusun oleh penulis berdasarkan sintesis berbagai referensi mengenai standar autentikasi digital dan manajemen risiko keamanan informasi.

Tabel 3 Kerangka Penguatan Keamanan Identitas Digital dalam Tata Kelola SPBE

Aspek Penguatan	Tujuan	Instrumen Utama	Indikator Keberhasilan
Regulasi	Menjamin kepastian hukum, perlindungan data pribadi, dan pembagian kewenangan	Kebijakan SPBE, regulasi perlindungan data pribadi, standar interoperabilitas	Kepatuhan regulasi meningkat, mekanisme audit berjalan efektif, hak pengguna terlindungi
Teknologi	Menjamin keamanan identitas dan transaksi digital	Multi-Factor Authentication (MFA), Single Sign-On (SSO), Federated Identity, Role-Based Access Control (RBAC), pencatatan aktivitas sistem	Penurunan insiden keamanan, meningkatnya keberhasilan autentikasi, audit keamanan terdokumentasi
Pelayanan Publik	Mewujudkan layanan digital yang aman, mudah digunakan, dan inklusif	Desain layanan yang ramah pengguna, kanal bantuan, literasi digital, alternatif autentikasi	Peningkatan adopsi layanan digital, berkurangnya keluhan pengguna, meningkatnya kepercayaan masyarakat

Sumber: Disusun oleh penulis berdasarkan sintesis literatur mengenai tata kelola SPBE, keamanan identitas digital, dan transformasi pemerintahan digital.

➤ Pembahasan

Implementasi identitas digital dalam Sistem Pemerintahan Berbasis Elektronik (SPBE) merupakan fondasi utama dalam mewujudkan transformasi pelayanan publik yang efektif, efisien, dan terpercaya. Hasil penelitian menunjukkan bahwa identitas digital tidak hanya berfungsi sebagai sarana autentikasi pengguna, tetapi juga sebagai instrumen untuk menjamin validitas identitas, integritas transaksi, dan perlindungan data pribadi masyarakat. Temuan ini sejalan dengan kerangka digital identity yang dikembangkan oleh National Institute of Standards and Technology (NIST), yang menempatkan proses pembuktian identitas, autentikasi, dan pengelolaan akses sebagai satu kesatuan dalam sistem keamanan layanan digital. Dengan demikian, keberhasilan implementasi SPBE tidak cukup diukur dari jumlah layanan yang telah terdigitalisasi, tetapi juga dari kemampuan pemerintah dalam membangun sistem identitas digital yang aman, terintegrasi, dan mampu meningkatkan kepercayaan masyarakat terhadap pelayanan publik berbasis elektronik. Hal tersebut menunjukkan bahwa keamanan identitas digital merupakan prasyarat utama bagi keberlanjutan transformasi digital sektor pemerintahan.

Temuan penelitian juga mengindikasikan bahwa tantangan utama implementasi SPBE di Indonesia masih terletak pada fragmentasi sistem autentikasi antarinstansi, penggunaan mekanisme autentikasi yang belum sepenuhnya adaptif terhadap tingkat risiko layanan, serta belum optimalnya tata kelola perlindungan data pribadi. Kondisi tersebut menyebabkan masyarakat harus menggunakan banyak akun untuk mengakses berbagai layanan pemerintah, sehingga meningkatkan risiko penggunaan ulang kata sandi, pencurian kredensial, maupun penyalahgunaan identitas digital. Oleh karena itu, penerapan autentikasi berbasis risiko melalui Multi-Factor Authentication (MFA), Single Sign-On (SSO), Federated Identity, serta pengendalian hak akses berdasarkan prinsip *least privilege* menjadi kebutuhan strategis dalam penguatan keamanan SPBE. Integrasi autentikasi nasional tidak hanya mampu meningkatkan efisiensi pelayanan publik, tetapi juga memperkuat interoperabilitas sistem pemerintahan serta mempermudah proses audit keamanan antarinstansi pemerintah.

Selain aspek teknologi, hasil penelitian menunjukkan bahwa keberhasilan implementasi identitas digital sangat dipengaruhi oleh tata kelola perlindungan data pribadi dan tingkat literasi digital masyarakat. Pertukaran data antarinstansi yang semakin luas dalam ekosistem SPBE harus

didukung oleh prinsip akuntabilitas, transparansi, dan pembatasan pemrosesan data sesuai tujuan penggunaannya. Penerapan prinsip *privacy by design* menjadi sangat penting agar perlindungan data telah diintegrasikan sejak tahap perancangan sistem, bukan hanya diterapkan setelah layanan beroperasi. Di sisi lain, pemerintah juga perlu meningkatkan literasi keamanan digital masyarakat melalui edukasi mengenai penggunaan autentikasi yang aman, perlindungan akun, serta kewaspadaan terhadap berbagai bentuk serangan siber seperti phishing dan rekayasa sosial. Pendekatan tersebut akan meningkatkan kemampuan masyarakat dalam memanfaatkan layanan pemerintahan digital secara aman sekaligus memperkuat kepercayaan publik terhadap implementasi SPBE.

Secara keseluruhan, penelitian ini menunjukkan bahwa penguatan keamanan identitas digital memerlukan pendekatan yang bersifat holistik melalui integrasi aspek regulasi, teknologi, tata kelola data, dan peningkatan kapasitas pengguna. Regulasi yang harmonis, standar autentikasi nasional, mekanisme pengawasan keamanan informasi, serta desain layanan yang inklusif harus berjalan secara sinergis untuk menghasilkan sistem pemerintahan digital yang andal. Selain itu, evaluasi keamanan perlu dilakukan secara berkala melalui pengukuran tingkat kepatuhan, efektivitas mekanisme autentikasi, jumlah insiden keamanan, serta tingkat kepercayaan masyarakat terhadap layanan digital pemerintah. Dengan pendekatan tersebut, implementasi SPBE di Indonesia tidak hanya mampu meningkatkan kualitas pelayanan publik, tetapi juga membangun ekosistem pemerintahan digital yang aman, adaptif, dan berkelanjutan dalam menghadapi perkembangan ancaman keamanan siber di masa mendatang.

D.KESIMPULAN DAN SARAN

➤ Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan bahwa keamanan identitas digital merupakan elemen fundamental dalam mendukung keberhasilan implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) di Indonesia. Penguatan mekanisme autentikasi, perlindungan data pribadi, dan tata kelola identitas digital menjadi faktor utama dalam membangun layanan pemerintahan digital yang aman, terpercaya, dan berkelanjutan. Hasil kajian menunjukkan bahwa berbagai tantangan, seperti fragmentasi sistem autentikasi, rendahnya interoperabilitas

antarinstansi, tingginya risiko penyalahgunaan data pribadi, serta keterbatasan literasi keamanan digital masyarakat, masih menjadi hambatan dalam optimalisasi SPBE. Oleh karena itu, diperlukan penerapan autentikasi berbasis risiko, penguatan *Multi-Factor Authentication* (MFA), *Single Sign-On* (SSO), federasi identitas, serta tata kelola perlindungan data yang selaras dengan standar internasional. Sinergi antara regulasi, teknologi, kelembagaan, dan peningkatan kapasitas sumber daya manusia diharapkan mampu meningkatkan kepercayaan masyarakat sekaligus mewujudkan ekosistem pemerintahan digital yang lebih efektif, inklusif, aman, dan berorientasi pada pelayanan publik yang berkualitas.

➤ Saran

Berdasarkan hasil penelitian, pemerintah perlu memperkuat tata kelola keamanan identitas digital melalui penyusunan standar autentikasi nasional yang terintegrasi pada seluruh layanan SPBE dengan menerapkan pendekatan autentikasi berbasis risiko, *Multi-Factor Authentication* (MFA), *Single Sign-On* (SSO), dan federasi identitas untuk meningkatkan keamanan serta interoperabilitas antarinstansi. Selain itu, penguatan perlindungan data pribadi perlu diikuti dengan penerapan prinsip *privacy by design*, pengendalian hak akses, audit keamanan secara berkala, serta peningkatan kapasitas sumber daya manusia dalam pengelolaan keamanan informasi. Di sisi lain, pemerintah juga perlu meningkatkan literasi keamanan digital masyarakat melalui program edukasi yang berkelanjutan agar masyarakat mampu memanfaatkan layanan pemerintahan digital secara aman dan bertanggung jawab. Penelitian selanjutnya disarankan mengembangkan kajian empiris melalui survei, studi kasus, atau pendekatan kuantitatif untuk mengukur tingkat kematangan keamanan identitas digital, efektivitas mekanisme autentikasi, serta pengaruhnya terhadap kepercayaan masyarakat dan kualitas implementasi SPBE di Indonesia.

DAFTAR PUSTAKA

- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
- ENISA. (2023). *European Digital Identity Wallet: Cybersecurity and Privacy Considerations*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications>
- Krippendorff, K. (2019). *Content Analysis: An Introduction to Its Methodology* (4th ed.). SAGE Publications.

- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Temoshok, D., Choong, Y.-Y., Galluzzo, R., LaSalle, C., Regenscheid, A., Proud-Madruga, D., Gupta, S., & Lefkowitz, N. (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>
- World Wide Web Consortium (W3C). (2025). *Verifiable Credentials Data Model v2.0*. <https://www.w3.org/TR/vc-data-model-2.0/>
- Bowen, G. A. (2009). *Document analysis as a qualitative research method*. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
- ENISA. (2023). *European Digital Identity Wallet: Cybersecurity and Privacy Considerations*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications>
- Krippendorff, K. (2019). *Content analysis: An introduction to its methodology* (4th ed.). SAGE Publications.
- Mazzocca, C., Acar, A., Uluagac, A. S., Montanari, R., Bellavista, P., & Conti, M. (2024). *A survey on decentralized identifiers and verifiable credentials*. arXiv. <https://doi.org/10.48550/arXiv.2402.02455>
- Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>
- Republik Indonesia. (2023). *Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional*. <https://jdih.setneg.go.id>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Temoshok, D., Choong, Y.-Y., Galluzzo, R., LaSalle, C., Regenscheid, A., Proud-Madruga, D., Gupta, S., & Lefkowitz, N. (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>
- World Wide Web Consortium. (2025). *Verifiable Credentials Data Model v2.0*. <https://www.w3.org/TR/vc-data-model-2.0/>