TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 120-127
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.9963

Analisis Validitas dan Keandalan Tanda Tangan Digital pada Dokumen PDF

Chriscel Novian*, Hanif Al Fatta

Fakultas Ilmu Komputer, Program Studi Magister Informatika, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia
Email: [1*]chriscelnovian@gmail.com, [2]hanif.a@amikom.ac.id
Email Penulis Korespondensi: chriscelnovian@gmail.com

Abstrak–Penelitian ini bertujuan untuk menganalisis tingkat validitas, mengukur konsistensi sebagai acuan serta mengidentifikasi faktor-faktor metadata teknis yang berpengaruh terhadap hasil validasi tanda tangan digital. Batasan penelitian mencakup dokumen PDF yang memiliki sertifikat dari lembaga otoritas resmi atau Certificate Authority (CA) maupun yang ditandatangani sendiri atau self-signed yang diuji pada lingkungan Windows 11 menggunakan Adobe Reader, Foxit Reader, Google Chrome, dan Microsoft Edge. Metode kuantitatif eksperimental digunakan melalui pendekatan teknis dengan pemrosesan data otomatis berbasis skrip Python untuk ekstraksi metadata. Hasil penelitian menunjukkan tingkat konsistensi validasi yang tidak seragam antar aplikasi; Foxit Reader mencapai akurasi tertinggi (96,67%), diikuti oleh Adobe Reader (91,67%) dan Microsoft Edge (90,00%), sementara Google Chrome (0%) terbukti gagal total akibat ketiadaan modul komputasi kriptografi. Inkonsistensi teridentifikasi bersumber dari perbedaan arsitektur parser, batas toleransi keamanan lokal, dan dukungan pustaka cipher suite dari perangkat lunak. Analisis diagnostik lebih lanjut menemukan kerentanan akibat absennya pihak ketiga seperti Timestamp Authority serta celah keamanan injeksi pada Microsoft Edge yang gagal mendeteksi serangan injeksi direktori. Dapat disimpulkan bahwa dengan ketiadaan standarisasi penguraian PDF yang baku dapat memicu status validasi lintas platform yang saling bertentangan, dimana keandalannya secara mutlak didikte oleh integritas algoritma hash, cipher suite, status penerbit, dan kelengkapan timestamp. Kontribusi penelitian ini berupa penyusunan benchmark interoperabilitas validasi tanda tangan digital PDF, pengembangan matriks konsistensi untuk evaluasi lintas platform, serta identifikasi faktor metadata teknis yang menjadi determinan utama keberhasilan validasi. Hasil penelitian diharapkan menjadi referensi bagi pengembang aplikasi, penyelenggara sertifikat elektronik, dan organisasi dalam meningkatkan keamanan serta konsistensi validasi dokumen digital.

Kata Kunci: Tanda Tangan Digital; PDF; Infrastruktur Kunci Publik; Algoritma Kriptografi; Metadata

Abstract–This research aims to analyze the level of validity, measure consistency as a benchmark, and identify the technical metadata factors that influence the validation results of digital signatures. The research scope includes PDF documents with certificates from official authorities or Certificate Authorities (CA) as well as self-signed ones, tested in a Windows 11 environment using Adobe Reader, Foxit Reader, Google Chrome, and Microsoft Edge. An experimental quantitative method was used through a technical approach with automated data processing based on Python scripts for metadata extraction. The research results show a non-uniform level of validation consistency across applications; Foxit Reader achieved the highest accuracy (96.67%), followed by Adobe Reader (91.67%) and Microsoft Edge (90.00%), while Google Chrome (0%) proved to fail completely due to the absence of a cryptographic computation module. The inconsistencies were identified to stem from differences in parser architectures, local security tolerance limits, and software cipher suite library support. Further diagnostic analysis found vulnerabilities due to the absence of third parties such as a Timestamp Authority, as well as an injection security flaw in Microsoft Edge, which failed to detect directory injection attacks. It can be concluded that the absence of standardised PDF parsing can lead to conflicting cross-platform validation results, the reliability of which is entirely dictated by the integrity of the hash algorithm, the cipher suite, the publisher's status, and the completeness of the timestamp. The contributions of this research include the development of an interoperability benchmark for PDF digital signature validation, the creation of a consistency matrix for cross-platform evaluation, and the identification of technical metadata factors that are the primary determinants of successful validation. The research findings are expected to serve as a reference for application developers, electronic certificate authorities, and organisations in enhancing the security and consistency of digital document validation.

Keywords: Digital Signature; PDF; Public Key Infrastructure; Cryptographic Algorithm; Metadata

1. PENDAHULUAN

Transformasi digital yang kian masif telah mendisrupsi secara fundamental mekanisme pengelolaan tata usaha dan peredaran dokumen pada berbagai lapisan organisasi. Transisi dari konvensional ke ranah elektronik ini mengandalkan teknologi tanda tangan digital sebagai instrumen mutlak guna menjamin aspek integritas, pelacakan autentisitas, serta kepastian hukum dari suatu berkas elektronik (Xu, 2025). Format Portable Document Format (PDF) sejauh ini telah memantapkan posisinya sebagai standar operasional utama dalam sirkulasi dokumen resmi karena memiliki kapabilitas untuk menyematkan token kriptografi secara langsung ke dalam kerangka berkasnya. Akan tetapi, reliabilitas praktis dari sistem verifikasi ini di lingkungan nyata ternyata jauh lebih rumit dibandingkan dengan formulasi kriptografinya di atas kertas. Tingkat kepercayaan publik terhadap arsitektur keamanan ini sangat bergantung pada konsistensi perlakuan setiap perangkat lunak terhadap berkas yang dievaluasi (Raavi et al., 2025). Standarisasi internasional semacam PDF Advanced Electronic Signatures (PAdES) sejatinya telah digagas untuk menciptakan keselarasan interoperabilitas antar platform. Namun, pada praktiknya, pengguna sering kali dihadapkan pada fenomena ambiguitas validasi. Sebuah berkas legal yang dinyatakan sepenuhnya valid oleh perangkat lunak pendedikasi seperti Adobe Acrobat Reader, tidak jarang memunculkan indikator galat atau peringatan tak teridentifikasi saat dirender menggunakan sistem pembaca internal pada peramban web modern. Disparitas hasil komputasi ini sangat berisiko mereduksi legitimasi sistem pertukaran dokumen elektronik secara keseluruhan (Zain et al., 2026).

TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 120-127
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.9963

Konteks ketidakkonsistenan ini menjelma menjadi isu yang kian meruncing di Indonesia, khususnya jika dikaitkan dengan dorongan masif pemerintah dalam mengeskalasi program Sistem Pemerintahan Berbasis Elektronik (SPBE). Institusi Penyelenggara Sertifikat Elektronik (PSrE) domestik telah dibentuk untuk memfasilitasi kebutuhan sertifikasi identitas digital berskala nasional. Dinamika kebijakan kerja hibrida turut mengamplifikasi sirkulasi dokumen administratif yang sangat bergantung pada kepastian validasi tanda tangan elektronik setiap detiknya. Interoperabilitas kemudian menjadi batu sandungan yang serius ketika sertifikat yang dienkripsi oleh PSrE lokal ini mengalami penolakan hierarki kepercayaan (chain of trust) oleh aplikasi penampil berskala global. Benturan lintas platform ini bukan sekadar ketidaknyamanan teknis, melainkan dapat mengeskalasi krisis kepercayaan publik terhadap keabsahan dokumen vital kenegaraan. Lebih jauh lagi, celah interoperabilitas ini secara langsung mengekspos dokumen pada kerentanan manipulasi siber yang canggih. Modifikasi struktural yang dikategorikan sebagai anomali fatal oleh satu aplikasi, bisa saja diabaikan oleh aplikasi lain karena minimnya standardisasi penguraian data (Rautenstrauch et al., 2023).

Diskursus akademis mengenai keamanan tanda tangan digital PDF dalam beberapa tahun ke belakang telah berhasil memetakan pelbagai titik kelemahan komputasional. Kajian yang dikemukakan oleh (Felisberto et al., 2024) mendemonstrasikan bagaimana celah struktural pada sistem parser dokumen dapat memfasilitasi serangan pemalsuan tanda tangan universal pada beberapa implementasi perangkat lunak. Eksplorasi serupa juga mengungkap kerentanan manipulasi lapisan objek tersembunyi yang memungkinkan penyerang mengubah isi dokumen tanpa memicu peringatan invalidasi dari sistem keamanan PDF(Nguyen et al., 2025). Di sisi lain, penyelidikan formal terhadap pedoman baku keamanan PDF juga memverifikasi eksistensi celah ambiguitas logika yang dapat dimanipulasi melalui struktur kriptografinya (Lalem et al., 2023). Analisis teknis tentang tata cara konstruksi sertifikat berbasis Public Key Infrastructure (PKI) juga telah dipaparkan untuk mengamankan data secara preventif, meskipun tidak mendalami aspek penerimaan dari sisi aplikasi pembaca (Mainka et al., 2021). Evaluasi otomatis menggunakan kerangka kerja diagnostik juga mulai diimplementasikan untuk mendeteksi kerentanan fundamental dari perangkat lunak penampil dokumen itu sendiri (Kim et al., 2023).

Selain analisis celah peretasan, sejumlah peneliti berfokus pada inovasi arsitektural untuk menambal kelemahan tersebut. Pengembangan arsitektur keamanan berlapis yang menggabungkan metode enkripsi, sertifikasi digital, dan penandaan air (watermarking) diusulkan untuk mendeteksi modifikasi yang tidak diotorisasi dengan lebih presisi (Iavich et al., 2025). Evaluasi menyeluruh terhadap kinerja efisiensi komputasi dari algoritma asimetris modern seperti ECDSA dan EdDSA juga menyoroti adanya kesenjangan antara kecepatan dekripsi dengan kemampuan sistem dalam mengelola manajemen kunci secara universal (Wicaksono et al., 2025). Tinjauan dari kacamata yurisprudensi dan efisiensi korporat pun menegaskan kembali bahwa integrasi teknologi kriptografi sangat vital untuk operasional bisnis yang berkelanjutan dan harus diakomodasi oleh kerangka hukum perlindungan data yang kuat (Octora Ginting et al., 2023). Tantangan interoperabilitas dalam pertukaran identitas digital antar platform juga diupayakan solusinya melalui rancangan arsitektur tanpa titik kegagalan tunggal (García-Cid et al., 2025). Saat ancaman komputasi kuantum mengintai, lanskap penelitian bahkan telah bergerak menuju perancangan dan evaluasi ketahanan algoritma kriptografi pasca-kuantum sebagai bentuk langkah mitigasi di masa depan (El Mane et al., 2021).

Penelaahan atas literatur-literatur mutakhir di atas mengonfirmasi bahwa arah riset saat ini terlalu terkonsentrasi pada dua sumbu ekstrem, yakni eksploitasi celah keamanan spesifik dan pembaruan struktur algoritma kriptografi teoretis (Nejatollahi et al., 2019). Terdapat celah investigasi empiris yang substansial mengenai bagaimana aplikasi penampil PDF populer di pasaran menerjemahkan dan mengkalkulasi parameter metadata tanda tangan digital yang sudah ada pada skenario operasional sehari-hari. Kajian ini menawarkan kontribusi kebaruan (*state of the art*) berupa kuantifikasi perbandingan ketahanan dan konsistensi dari berbagai mesin validasi populer secara komparatif untuk merumuskan matriks benchmark interoperabilitas (Yalamuri et al., 2022). Tujuan dari penelitian ini mencakup pengukuran akurasi individual dari tiap penampil PDF, penganalisisan tingkat konsistensi persentase validasi secara silang, serta pengidentifikasian komponen metadata teknis spesifik yang memegang kendali paling dominan terhadap fluktuasi respons keamanan aplikasi. Melalui pendekatan kuantitatif yang komprehensif, penelitian ini diharapkan dapat mereduksi kesenjangan teknis antar sistem sekaligus memberikan landasan yang solid bagi pengembang dan korporasi dalam menyempurnakan arsitektur kepercayaan elektronik (Lee & Park, 2021).

Kontribusi penelitian ini terletak pada penyusunan benchmark interoperabilitas validasi tanda tangan digital PDF berbasis pengujian empiris lintas platform yang melibatkan Adobe Reader, Foxit Reader, Google Chrome, dan Microsoft Edge. Penelitian ini juga menawarkan matriks konsistensi sebagai instrumen evaluasi untuk mengukur tingkat kesesuaian hasil validasi terhadap kondisi aktual dokumen (ground truth). Selain itu, penelitian ini mengidentifikasi faktor-faktor metadata teknis yang paling berpengaruh terhadap keberhasilan validasi, meliputi integritas algoritma hash, dukungan cipher suite, status kepercayaan penerbit sertifikat, dan keberadaan timestamp. Temuan tersebut memberikan dasar praktis bagi pengembang perangkat lunak, penyelenggara sertifikat elektronik, serta organisasi pengguna dokumen digital dalam meningkatkan interoperabilitas, keamanan, dan keandalan sistem tanda tangan digital pada dokumen PDF (Suhail et al., 2021).


TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 120-127
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.9963

2. METODOLOGI PENELITIAN

2.1 Kerangka Dasar Penelitian

Studi ini dikonstruksi menggunakan desain penelitian kuantitatif eksperimental yang berfokus pada pengujian validitas tanda tangan digital melalui observasi variabel teknis dan perlakuan platform viewer yang bervariasi. Sifat penelitian ini adalah deskriptif kuantitatif, yang mana fenomena interoperabilitas dipetakan berdasarkan data numerik yang konkret, seperti kalkulasi jumlah dokumen yang valid, distribusi persentase penolakan terhadap sertifikat self-signed, serta pengukuran tingkat konsistensi hasil verifikasi lintas platform. Pendekatan eksperimen teknis ini dijalankan dengan mengintegrasikan sistem pemrosesan data otomatis berbasis bahasa pemrograman Python untuk menjamin efisiensi pengujian arsitektur keamanan secara masif, serupa dengan metode investigasi forensik digital pada instrumen sekuriti perangkat lunak. Objek penelitian ini berfokus pada dua variabel utama. Variabel independen mencakup jenis perangkat lunak penampil PDF dan anomali metadata teknis yang disuntikkan ke dalam struktur dokumen, sedangkan variabel dependen adalah status validasi yang dihasilkan oleh sistem verifikasi viewer. Analisis dilakukan melalui inspeksi struktural secara terisolasi guna mendeteksi kerentanan laten tanpa harus merusak format asli dari dokumen yang diuji. Dalam implementasinya, metodologi ini selaras dengan prinsip rekonstruksi data untuk mengamankan autentisitas teknis dari berbagai bentuk manipulasi evasif.

2.2 Tahapan Penelitian

Penelitian dilaksanakan melalui alur sistematis yang mencakup fase persiapan, pembuatan dataset, eksekusi eksperimen, hingga analisis diagnostik. Fase persiapan dimulai dengan menstandarisasi lingkungan uji menggunakan satu perangkat komputer berbasis sistem operasi Windows 11 64-bit untuk menjamin baseline pengujian yang adil. Penelitian ini menggunakan 4 aplikasi penampil PDF yaitu Adobe Reader, Foxit Reader, Google Chrome, dan Microsoft Edge yang diinstall pada pengaturan bawaan murni (*default*) tanpa modifikasi pengaturan lokal atau penambahan komponen eksternal lainnya. Otomatisasi dikembangkan menggunakan skrip Python yang memanfaatkan ekosistem pustaka (*library*) yang kaya untuk membedah struktur internal PDF. Pustaka PyHanko dan PyPDF2 digunakan untuk membaca entri kamus tanda tangan, sementara modul kriptografi dikerahkan untuk menghasilkan puluhan berkas uji secara konsisten. Tahapan ini juga mencakup penggunaan instrumen OpenSSL untuk memproduksi sertifikat digital *self-signed* yang akan menjadi komponen inti dalam simulasi skenario anomali. Prosedur otomatisasi ini tidak hanya mempercepat ekstraksi metadata, tetapi juga memfasilitasi visualisasi hubungan antara integritas biner dan respon keamanan aplikasi.

2.3 Teknik Pengumpulan Dataset

Dataset dikumpulkan melalui teknik *purposive sampling* dengan menetapkan kriteria relevansi yang ketat untuk menjawab rumusan masalah. Populasi pengujian terdiri dari 60 dokumen PDF yang disegmentasi menjadi dua kelompok besar. Kelompok pertama berisi 20 berkas yang ditandatangani oleh Otoritas Sertifikat (CA) resmi di Indonesia untuk mewakili standar kepercayaan publik. Kelompok kedua terdiri dari 40 berkas yang ditandatangani secara mandiri (*self-signed*), di mana skrip otomasi menyuntikkan berbagai variasi metadata kriptografi dan anomali struktural. Skenario pengujian pada dataset self-signed mencakup manipulasi pada algoritma *hash* (SHA-1 hingga SHA-512), variasi panjang kunci RSA (1024 hingga 4096-bit), serta penggunaan algoritma modern seperti ECDSA dan EdDSA. Selain itu, dilakukan penyisipan anomali pada aspek integritas visual, seperti koordinat tampilan di luar batas dokumen, transparansi 0%, hingga injeksi skrip XSS dan sintaks basis data untuk menguji ketahanan *parser viewer*. Dokumentasi stempel waktu (*timestamp*) dan status sertifikat kedaluwarsa juga disertakan untuk mengobservasi respon aplikasi terhadap parameter temporal.

2.4 Metode Analisis Data

Data mentah yang diperoleh dari hasil verifikasi tiap viewer dicatat secara sistematis dan dikategorikan ke dalam empat status: Valid Penuh (VP), Valid dengan Peringatan (VW), Tidak Valid (TV), dan Tidak Diketahui (TD). Metode analisis yang digunakan adalah statistik deskriptif kuantitatif untuk memetakan distribusi hasil validasi pada masing-masing aplikasi. Untuk mengukur tingkat interoperabilitas, dikembangkan sebuah Matriks Konsistensi yang membandingkan respon antar-platform terhadap satu dokumen yang sama. Analisis lebih lanjut dilakukan dengan menghitung Skor Konsistensi, di mana luaran aplikasi dikomparasikan langsung dengan nilai kebenaran struktural (ground truth) dokumen. Skor bernilai 1 diberikan jika status aplikasi sesuai dengan kondisi asli dokumen, dan 0 jika terjadi disparitas. Melalui matriks ini, persentase keberhasilan setiap viewer dihitung untuk merumuskan sebuah benchmark kinerja fungsional. Terakhir, analisis korelasi dan diagnostik dilakukan untuk mengidentifikasi komponen metadata biner seperti struktur /ByteRange, fitur *Incremental Update*, dan dukungan *cipher suite* yang menjadi faktor determinan terjadinya inkonsistensi validasi lintas *platform*.

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil dan pembahasan dari penelitian, yang diawali dengan penjelasan metodologi penelitian yang digunakan. Jenis penelitian ini adalah kuantitatif eksperimental yang berusaha menguji dan mengukur status

TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 120-127
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.9963

validasi tanda tangan digital dari dokumen PDF berdasarkan variabel teknis tertentu dan perlakuan platform viewer yang berbeda. Sifat penelitian ini adalah deskriptif kuantitatif, yaitu menggambarkan fenomena yang terjadi berdasarkan data numerik, seperti jumlah dokumen valid, proporsi tanda tangan self-signed yang ditolak viewer, dan tingkat konsistensi antar-platform.

Pendekatan yang digunakan adalah eksperimen teknis dengan pemrosesan data otomatis menggunakan Python. Pengumpulan dokumen PDF dilakukan secara purposive sampling, yang menghasilkan 60 dokumen yang terdiri dari 20 file dari Certificate Authority (CA) resmi di Indonesia dan 40 file self-signed yang dibuat dengan OpenSSL. Pengujian dokumen dilakukan pada satu perangkat bersistem operasi Windows 11 64-bit menggunakan platform viewer Adobe Reader DC, Foxit PDF Reader, Chrome PDF Viewer, dan Microsoft Edge PDF Viewer versi terbaru dengan kondisi default. Metadata teknis diekstraksi menggunakan Python dengan library PyHanko dan PyPDF untuk inspeksi struktur internal yang komprehensif.

3.1 Pemetaan Dataset Eksperimental

Penelitian ini memetakan 60 dokumen PDF tersebut ke dalam dua kelompok utama, yaitu dataset Certificate Authority (CA) dan dataset Self-Signed (SS). Kelompok CA mewakili dokumen dengan sertifikat yang diterbitkan oleh Penyelenggara Sertifikasi Elektronik (PSrE) berinduk resmi, baik dalam kondisi utuh maupun yang telah mengalami manipulasi. Rincian pemetaan kelompok CA disajikan pada Tabel 1.

Tabel 1. Pemetaan Dataset CA

ID File	Instansi Penerbit	Kondisi Dokumen	*Ground Truth*
CA_01	Badan Siber dan Sandi Negara	Asli	Valid
CA_02	Kementerian Komunikasi dan Informatika	Asli	Valid
CA_03	Peruri	Asli	Valid
CA_04	PT Digital Tandatangan Asli	Asli	Valid
CA_05	PT Indonesia Digital Identity	Asli	Valid
CA_06	PT Privy Identitas Digital	Asli	Valid
CA_07	PT Solusi Identitas Global Net	Asli	Valid
CA_08	PT Solusi Net Internusa	Asli	Valid
CA_09	PT Tilaka Nusa Teknologi	Asli	Valid
CA_10	PT Vipas Inovasi Teknologi	Asli	Valid
CA_11	Badan Siber dan Sandi Negara	Manipulasi	Invalid
CA_12	Kementerian Komunikasi dan Informatika	Manipulasi	Invalid
CA_13	Peruri	Manipulasi	Invalid
CA_14	PT Digital Tandatangan Asli	Manipulasi	Invalid
CA_15	PT Indonesia Digital Identity	Manipulasi	Invalid
CA_16	PT Privy Identitas Digital	Manipulasi	Invalid
CA_17	PT Solusi Identitas Global Net	Manipulasi	Invalid
CA_18	PT Solusi Net Internusa	Manipulasi	Invalid
CA_19	PT Tilaka Nusa Teknologi	Manipulasi	Invalid
CA_20	PT Vipas Inovasi Teknologi	Manipulasi	Invalid

Dataset *Self-Signed* dibangun secara mandiri menggunakan modul OpenSSL untuk mewakili berbagai skenario variasi algoritma kriptografi dan anomali struktural tingkat lanjut (seperti modifikasi rentang byte, manipulasi timestamp, hingga injeksi direktori). Parameter teknis dan ketetapan Ground Truth untuk kelompok ini diuraikan pada Tabel 2.

Tabel 2. Pemetaan Dataset SS

ID File	Skenario Uji	Parameter Teknis	*Ground Truth*
SS_01	Kriptografi	RSA 1024-bit + SHA-1	Valid
SS_02	Kriptografi	RSA 1024-bit + SHA-256	Valid
SS_03	Kriptografi	RSA 2048-bit + SHA-256	Valid
SS_04	Kriptografi	RSA 3072-bit + SHA-256	Valid
SS_05	Kriptografi	RSA 4096-bit + SHA-512	Valid
SS_06	Kriptografi	ECDSA P-256 + SHA-256	Valid
SS_07	Kriptografi	ECDSA P-384 + SHA-384	Valid
SS_08	Kriptografi	ECDSA P-521 + SHA-512	Valid
SS_09	Kriptografi	DSA 3072-bit + SHA-256	Valid
SS_10	Kriptografi	EdDSA + SHA-512	Valid
SS_11	Integritas	Manipulasi file SS_01	Invalid
SS_12	Integritas	Manipulasi file SS_02	Invalid
SS_13	Integritas	Manipulasi file SS_03	Invalid
SS_14	Integritas	Manipulasi file SS_04	Invalid

TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 120-127
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.9963

ID File	Skenario Uji	Parameter Teknis	*Ground Truth*
SS_15	Integritas	Manipulasi file SS_05	Invalid
SS_16	Integritas	Manipulasi file SS_06	Invalid
SS_17	Integritas	Manipulasi file SS_07	Invalid
SS_18	Integritas	Manipulasi file SS_08	Invalid
SS_19	Integritas	Manipulasi file SS_09	Invalid
SS_20	Integritas	Manipulasi file SS_10	Invalid
SS_21	Visual UI	Koordinat tampilan diluar batas dokumen	Valid
SS_22	Visual UI	Transparansi tampilan 0%	Valid
SS_23	Parser	Teks Unicode	Valid
SS_24	Parser	Karakter kosong (*null*)	Valid
SS_25	Parser	Injeksi skrip XSS	Valid
SS_26	Parser	Injeksi karakter string identik	Valid
SS_27	Parser	Injeksi sintaks *database*	Valid
SS_28	Incremental Update	Tanda tangan tambahan	Valid
SS_29	Integritas	Manipulasi file SS_21	Invalid
SS_30	Integritas	Manipulasi file SS_22	Invalid
SS_31	Integritas	Manipulasi file SS_23	Invalid
SS_32	Integritas	Manipulasi file SS_24	Invalid
SS_33	Integritas	Manipulasi file SS_25	Invalid
SS_34	Integritas	Manipulasi file SS_26	Invalid
SS_35	Integritas	Manipulasi file SS_27	Invalid
SS_36	Integritas	Manipulasi file SS_28	Invalid
SS_37	Sertifikat	Sertifikat kedaluarsa	Invalid
SS_38	Sertifikat	Sertifikat prematur	Invalid
SS_39	Integritas	Manipulasi LTV	Invalid
SS_40	Integritas	Manipulasi *timestamp* pada tanda tangan	Invalid

3.2 Hasil Uji Validitas

Setelah seluruh dataset dipetakan, tahap selanjutnya adalah melakukan uji interoperabilitas dengan membuka setiap dokumen pada empat perangkat lunak yang berbeda yaitu Adobe Reader, Foxit Reader, Google Chrome dan Microsoft Edge. Tujuan dari pengujian ini adalah untuk merekam respons antarmuka yang dikembalikan oleh masing-masing aplikasi. Rekapitulasi dari keluaran status validitas tersebut didokumentasikan secara lengkap pada Tabel 3.

Tabel 3. Matriks Uji Validitas

ID File	Adobe Reader	Foxit Reader	Google Chrome	Microsoft Edge
CA_01	VW	VW	TD	VW
CA_02	VW	VW	TD	VW
CA_03	VW	VW	TD	VW
CA_04	VW	VW	TD	VW
CA_05	VW	VW	TD	VW
CA_06	VW	VW	TD	VW
CA_07	VW	VW	TD	VW
CA_08	VW	VW	TD	VW
CA_09	VW	VW	TD	VW
CA_10	VW	VW	TD	VW
CA_11	TV	TV	TD	TV
CA_12	TV	TV	TD	TV
CA_13	TV	TV	TD	TV
CA_14	TV	TV	TD	TV
CA_15	TV	TV	TD	TV
CA_16	TV	TV	TD	TV
CA_17	TV	TV	TD	TV
CA_18	TV	TV	TD	TV
CA_19	TV	TV	TD	TV
CA_20	TV	TV	TD	TV
SS_01	VW	VW	TD	VW
SS_02	VW	VW	TD	VW
SS_03	VW	VW	TD	VW
SS_04	VW	VW	TD	VW
SS_05	VW	VW	TD	VW

TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 120-127
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.9963

ID File	Adobe Reader	Foxit Reader	Google Chrome	Microsoft Edge
SS_06	VW	VW	TD	VW
SS_07	VW	VW	TD	VW
SS_08	VW	VW	TD	VW
SS_09	TV	VW	TD	TV
SS_10	TV	VW	TD	TV
SS_11	TV	TV	TD	TV
SS_12	TV	TV	TD	TV
SS_13	TV	TV	TD	TV
SS_14	TV	TV	TD	TV
SS_15	TV	TV	TD	TV
SS_16	TV	TV	TD	TV
SS_17	TV	TV	TD	TV
SS_18	TV	TV	TD	TV
SS_19	TV	TV	TD	TV
SS_20	TV	TV	TD	TV
SS_21	VW	VW	TD	VW
SS_22	VW	VW	TD	VW
SS_23	VW	VW	TD	VW
SS_24	VW	VW	TD	VW
SS_25	VW	VW	TD	VW
SS_26	VW	VW	TD	VW
SS_27	VW	VW	TD	VW
SS_28	VW	VW	TD	VW
SS_29	TV	TV	TD	TV
SS_30	TV	TV	TD	TV
SS_31	TV	TV	TD	TV
SS_32	TV	TV	TD	TV
SS_33	TV	TV	TD	TV
SS_34	TV	TV	TD	TV
SS_35	TV	TV	TD	TV
SS_36	TV	TV	TD	TV
SS_37	VW	VW	TD	VW
SS_38	VW	VW	TD	VW
SS_39	VW	VW	TD	VW
SS_40	TV	TV	TD	VW

Keterangan pada kategori hasil validasi tersebut menunjukkan bahwa VP (Valid Penuh) merupakan status data yang sepenuhnya valid tanpa ditemukan permasalahan. VW (Valid dengan Peringatan) menunjukkan data yang dinyatakan valid, namun terdapat beberapa catatan atau peringatan tertentu. TV (Tidak Valid) menunjukkan bahwa data tidak memenuhi kriteria validasi yang ditetapkan, sedangkan TD (Tidak Diketahui) menunjukkan bahwa status validasi data belum dapat ditentukan atau informasinya belum tersedia.

Untuk membedah alasan dibalik hasil status pada masing-masing aplikasi viewer, dilakukan proses parsing dan ekstraksi mendalam terhadap struktur tanda tangan digital dari setiap dokumen PDF. Ekstraksi ini memunculkan metrik-metrik yang krusial, meliputi parameter Temporal Validity, kehadiran token Timestamp Authority (TSA), kecocokan Cryptographic Hash, hingga deteksi anomali spasial (Trailing Bytes dan Injected Dictionary).

3.3 Matriks Skor Konsistensi

Untuk mengukur akurasi masing-masing viewer, hasil uji validitas dari Tabel 3 dikomparasikan secara langsung dengan nilai ground truth yang telah ditetapkan di awal. Kesamaan antara status aplikasi dengan kebenaran struktural dokumen dihitung untuk menentukan tingkat konsistensi persentase keberhasilan setiap viewer. Hasil skor konsistensi ini disajikan pada Tabel 4.

Tabel 4. Matriks Skor Konsistensi

Hasil	Adobe Reader	Foxit Reader	Google Chrome	Microsoft Edge
Total Skor	55	58	0	54
Persentase	91,67%	96,67%	0%	90%

3.4 Pembahasan

Merujuk pada hasil uji validitas dan interoperabilitas yang disajikan dalam Tabel 3.5, penelitian ini secara jelas mengonfirmasi rumusan masalah terkait tingkat keandalan dan konsistensi tanda tangan digital lintas platform. Ditemukan ketiadaan standarisasi tunggal yang absolut di antara berbagai aplikasi viewer dalam pengujian validasi

TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 120-127
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.9963

tanda tangan digital, di mana uji coba terhadap 60 skenario dataset menghasilkan variansi akurasi yang terfragmentasi secara signifikan. Foxit Reader mencatatkan tingkat konsistensi tertinggi sebesar 96,67% (58 keberhasilan), mengindikasikan arsitektur parser yang mengutamakan fleksibilitas. Adobe Reader menduduki posisi kedua dengan konsistensi 91,67% (55 keberhasilan), di mana ketidaksesuaiannya disebabkan oleh regulasi cipher suite yang terlampau ketat. Microsoft Edge menyusul dengan persentase 90,00% (54 keberhasilan). Sebaliknya, Google Chrome mencatat kegagalan total (0%) karena viewer berbasis browser ini tidak dibekali kapabilitas komputasi kriptografi yang memadai.

Temuan empiris mengenai ketidakkonsistenan dengan selisih capaian antar viewer ini sangat relevan dan menguatkan kajian dari penelitian-penelitian terdahulu yang diulas pada literatur. Penelitian sebelumnya oleh (Kumar, 2022) mendemonstrasikan serangan "Breaking PDF Signatures", yang membuktikan adanya kemungkinan pemalsuan tanda tangan universal pada implementasi tertentu. Meskipun penelitian Mladenov berfokus murni pada eksploitasi serangan, hasil kuantifikasi dalam riset ini memberikan data fundamental yang membuktikan bahwa perbedaan arsitektur pembaca (parser), kebijakan batas toleransi struktural, serta mesin kriptografi lokal merupakan celah bawaan (determinan utama) yang memungkinkan kerentanan semacam itu terjadi .

Lebih lanjut, (Hegde et al., 2023) melakukan analisis keamanan formal dan menemukan potensi ambiguitas teoretis pada standar validasi PDF. Hasil evaluasi benchmark dalam penelitian ini secara nyata menerjemahkan ambiguitas teoretis tersebut menjadi bukti inkonsistensi praktis pada implementasi perangkat lunak viewer di dunia nyata. Selain itu, riset ini melengkapi analisis (Shahid et al., 2020) yang menyoroti kinerja efisiensi algoritma kriptografi modern (seperti ECDSA dan EdDSA). Bukti pada riset ini menemukan bahwa terlepas dari kehebatan algoritma tersebut, pada lapisan aplikasi, viewer seperti Adobe Reader justru sering kali memberikan status false positive (Invalid) akibat pustaka algoritmanya yang terlalu konservatif dalam menerima cipher suite modern (Oratmangun, 2021).

Untuk menjawab pertanyaan penelitian terkait faktor metadata teknis yang memengaruhi validitas, analisis korelasi dilakukan antara komponen metadata dengan keluaran hasil viewer (Murkatik et al., 2020). Integritas Algoritma Hash (Digest Algorithm) berkorelasi secara absolut terhadap validitas; modifikasi sekecil apa pun pada struktur byte secara universal memicu penolakan validitas pada semua aplikasi selain Chrome. Korelasi pada Status Penerbit (Issuer Trust) menunjukkan pola seragam, yaitu ketiadaan Root CA komersial (pada dataset self-signed) memicu peringatan (Warning), namun tidak merusak validitas hash dokumen (Algazy, Sakan, Nyssanbayeva, et al., 2024).

Di sisi lain, diagnostik pada parameter temporal mengungkap kerentanan masif. Ketiadaan token Timestamp Authority (TSA) eksternal pada sertifikat self-signed membuat dokumen rentan terhadap manipulasi waktu lokal (backdating). Mayoritas viewer gagal mendeteksi kecurangan temporal dan tetap mempertahankan status keabsahan selama nilai matematis hash tidak berubah. Diagnostik keamanan terdalam juga ditemukan pada skenario celah injeksi. Saat dilakukan injeksi direktori di luar batas zona tanda tangan (Trailing Bytes), Adobe Reader menetapkan benchmark tertinggi dalam hal keamanan spasial dengan berhasil mendeteksi anomali tersebut dan merespons dengan status Invalid (Algazy, Sakan, Khompysh, et al., 2024). Sebaliknya, Microsoft Edge gagal mendiagnosis anomali struktural ini karena hanya menghitung kecocokan hash di zona aman. Kegagalan viewer bawaan Windows ini membuktikan bahwa komputasi matematis saja tidak mampu menjamin keamanan dokumen jika viewer memiliki celah injeksi, menjadikannya rentan terhadap teknik bypass (Yunus, 2021).

Sebagai kesimpulan, penyusunan benchmark kinerja fungsional ini menunjukkan bahwa tidak ada aplikasi yang sempurna. Adobe Reader memiliki standar keamanan spasial tertinggi namun interoperabilitasnya rendah. Foxit Reader memiliki benchmark kompatibilitas dan interoperabilitas terbaik meskipun batas toleransinya cukup longgar. Microsoft Edge hanya berperan sebagai kalkulator kriptografi tingkat dasar dengan keamanan lemah, dan Google Chrome sama sekali tidak dapat digunakan untuk keperluan audit dokumen bertanda tangan digital. Temuan ini menekankan krusialnya standar penguraian yang baku guna mencegah perbedaan status validasi lintas platform pada ekosistem PDF.

4. KESIMPULAN

Penelitian ini secara empiris menyimpulkan bahwa ketiadaan standardisasi baku dalam arsitektur penguraian dokumen PDF telah memicu tingkat validitas dan keandalan tanda tangan digital yang sangat fluktuatif lintas perangkat lunak. Evaluasi komparatif terhadap enam puluh dataset dokumen menunjukkan bahwa Foxit Reader memiliki tingkat konsistensi tertinggi mencapai 96,67%, mengungguli Adobe Reader yang mencatatkan akurasi sebesar 91,67% serta Microsoft Edge di angka 90%, sedangkan penampil bawaan dari *browser* Google Chrome mengalami kegagalan validasi total sebesar nol persen akibat ketiadaan modul komputasi kriptografi. Inkonsistensi tersebut terbukti dipengaruhi secara mutlak oleh 4 faktor metadata biner yaitu integritas algoritma *hash*, kelengkapan pustaka *cipher suite*, status kepercayaan penerbit, serta eksistensi stempel waktu atau *timestamp*. Penelitian ini juga membuktikan bahwa pengujian matematis kecocokan *hash* semata tidaklah cukup untuk menjamin keamanan struktural, mengingat ditemukannya kerentanan injeksi direktori melalui manipulasi *trailing bytes* yang luput dari deteksi Microsoft Edge, serta ancaman pemalsuan waktu mundur pada dokumen yang tidak dilengkapi token otoritas penanda waktu pihak ketiga. Oleh karena itu, pengembang perangkat lunak direkomendasikan untuk memperketat inspeksi anomali di luar zona tanda tangan dan memperbarui dukungan algoritma modern. Bagi penelitian lanjutan, disarankan untuk


TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 120-127
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.9963

mengekspansi ruang lingkup pengujian komparatif ini ke ekosistem sistem operasi seluler serta mengimplementasikan skenario serangan kriptografi tingkat lanjut seperti serangan tabrakan *hash*.

REFERENCES

Algazy, K., Sakan, K., Khompysh, A., & Dyusenbayev, D. (2024). Development of a New Post-Quantum Digital Signature Algorithm: Syrga-1. *Computers*, *13*(1), 26. https://doi.org/10.3390/computers13010026

Algazy, K., Sakan, K., Nyssanbayeva, S., & Lizunov, O. (2024). Syrga2: Post-Quantum Hash-Based Signature Scheme. *Computation*, *12*(6), 125. https://doi.org/10.3390/computation12060125

El Mane, A., Chihab, Y., & Korchiyne, R. (2021). Digital Signature for data and documents using operating PKI certificates. *SHS Web of Conferences*, *119*, 07004. https://doi.org/10.1051/shsconf/202111907004

Felisberto, M., de Oliveira, J. M. D., Mohr, E. T. B., Celuppi, I. C., Zanotto, W. L., dos Santos, R. A., Scandolara, D. H., dos Santos Fantonelli, M., Cunha, C. L., Hammes, J. F., Wazlawick, R. S., & Dalmarco, E. M. (2024). Digital signatures in electronic health records: a scoping review. *Health and Technology*, *14*(6), 1083–1096. https://doi.org/10.1007/s12553-024-00906-y

García-Cid, M. I., Martín, R., Domingo, D., Martín, V., & Ortiz, L. (2025). Design and Implementation of a Quantum-Assisted Digital Signature. *Cryptography*, *9*(1), 11. https://doi.org/10.3390/cryptography9010011

Hegde, S. B., Jamuar, A., & Kulkarni, R. (2023). Post Quantum Implications on Private and Public Key Cryptography. *2023 International Conference on Smart Systems for Applications in Electrical Sciences (ICSSES)*, 1–6. https://doi.org/10.1109/ICSSES58299.2023.10199503

Iavich, M., Kapalova, N., & Sakan, K. (2025). Efficient Lattice-Based Digital Signatures for Embedded IoT Systems. *Symmetry*, *17*(9), 1522. https://doi.org/10.3390/sym17091522

Kim, J., Kim, P., Choi, D., & Lee, Y. (2023). A Study on the Interoperability Technology of Digital Identification Based on WACI Protocol with Multiparty Distributed Signature. *Sensors*, *23*(8), 4061. https://doi.org/10.3390/s23084061

Kumar, M. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. *Array*, *15*, 100242. https://doi.org/10.1016/j.array.2022.100242

Lalem, F., Laouid, A., Kara, M., Al-Khalidi, M., & Eleyan, A. (2023). A Novel Digital Signature Scheme for Advanced Asymmetric Encryption Techniques. *Applied Sciences*, *13*(8), 5172. https://doi.org/10.3390/app13085172

Lee, J., & Park, Y. (2021). HORSIC+: An Efficient Post-Quantum Few-Time Signature Scheme. *Applied Sciences*, *11*(16), 7350. https://doi.org/10.3390/app11167350

Mainka, C., Mladenov, V., & Rohlmann, S. (2021). Shadow Attacks: Hiding and Replacing Content in Signed PDFs. *Proceedings 2021 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2021.24117

Murkatik, K., Harapan, E., & Wardiah, D. (2020). The Influence of Professional and Pedagogic Competence on Teacher's Performance. *Journal of Social Work and Science Education*, *1*(1), 58–69. https://doi.org/10.52690/jswse.v1i1.10

Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-Quantum Lattice-Based Cryptography Implementations. *ACM Computing Surveys*, *51*(6), 1–41. https://doi.org/10.1145/3292548

Nguyen, T.-T., Nguyen, D.-D., Dao, T.-T., & Luc, N.-Q. (2025). Implementation Efficiency of Falcon Digital Signature Scheme on Arty-7 XC7A35T Board. *Electronics*, *14*(22), 4504. https://doi.org/10.3390/electronics14224504

Octora Ginting, F. S., Veithzal Rivai Zainal, & Aziz Hakim. (2023). Digital Signature Standard Implementation Strategy by Optimizing Hash Functions Through Performance Optimization. *Journal of Accounting and Finance Management*, *3*(6), 362–371. https://doi.org/10.38035/jafm.v3i6.175

Oratmangun, R. (2021). Teacher's Roles As: Classroom Manager And Classroom Instructor. *Cerdika: Jurnal Ilmiah Indonesia*, *1*(2), 164–170. https://doi.org/10.59141/cerdika.v1i2.24

Raavi, M., Khan, Q., Wuthier, S., Chandramouli, P., Balytskyi, Y., & Chang, S.-Y. (2025). Security and Performance Analyses of Post-Quantum Digital Signature Algorithms and Their TLS and PKI Integrations. *Cryptography*, *9*(2), 38. https://doi.org/10.3390/cryptography9020038

Rautenstrauch, J., Pellegrino, G., & Stock, B. (2023). The Leaky Web: Automated Discovery of Cross-Site Information Leaks in Browsers and the Web. *2023 IEEE Symposium on Security and Privacy (SP)*, 2744–2760. https://doi.org/10.1109/SP46215.2023.10179311

Shahid, F., Khan, A., Malik, S. U. R., & Choo, K.-K. R. (2020). WOTS-S: A Quantum Secure Compact Signature Scheme for Distributed Ledger. *Information Sciences*, *539*, 229–249. https://doi.org/10.1016/j.ins.2020.05.024

Suhail, S., Hussain, R., Khan, A., & Hong, C. S. (2021). On the Role of Hash-Based Signatures in Quantum-Safe Internet of Things: Current Solutions and Future Directions. *IEEE Internet of Things Journal*, *8*(1), 1–17. https://doi.org/10.1109/JIOT.2020.3013019

Wicaksono, P., Hatta, P., & Aristyagama, Y. H. (2025). Comparative analysis of PoS and PoA consensus in Ethereum environment for blockchain based academic transcript systems. *Bulletin of Electrical Engineering and Informatics*, *14*(3), 2380–2392. https://doi.org/10.11591/eei.v14i3.9219

Xu, J. (2025). A Comprehensive Study of Digital Signatures: Algorithms, Challenges and Future Prospects. *ITM Web of Conferences*, *73*, 03009. https://doi.org/10.1051/itmconf/20257303009

Yalamuri, G., Honnavalli, P., & Eswaran, S. (2022). A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats. *Procedia Computer Science*, *215*, 834–845. https://doi.org/10.1016/j.procs.2022.12.086

Yunus, Mhd. (2021). Teacher Empowerment Strategy in Improving the Quality of Education. *International Journal of Social Science and Human Research*, *04*(01). https://doi.org/10.47191/ijsshr/v4-i1-05

Zain, S., Mähn, J., Köpsell, S., & Ertel, S. (2026). *Formally-Verified Security Against Forgery of Remote Attestation Using SSProve* (pp. 463–484). https://doi.org/10.1007/978-3-032-07891-9_24