Saturnus : Jurnal Teknologi dan Sistem Informasi
Volume. 4, Nomor. 2 April 2026
e-ISSN : 3031-9943; dan p-ISSN : 3031-9935; Hal. 29-41
DOI: https://doi.org/10.61132/saturnus.v4i2.1568
Tersedia: https://journal.arteii.or.id/index.php/Saturnus

Rancang Bangun Sistem Pelayanan Surat Berbasis Web dengan Penerapan Tanda Tangan Digital di Nagari Bukit Bais

Mukhtarijal[1*], Hadi Kurnia Saputra[2], Dony Novaliendry[3], Ahmaddul Hadi[4]
[1-4] Universitas Negeri Padang, Indonesia
*Penulis Korespondensi: mukhtarijal6902@gmail.com [1]

Abstract. *Administrative letter services at the village (nagari) level are still largely conducted using conventional methods, resulting in various issues such as limited service hours, slow processing times, and risks of document loss. This study aims to develop a web-based letter service system with the implementation of digital signatures in Nagari Bukit Bais to improve efficiency, security, and transparency of public services. The research adopts the Agile Development method with an iterative approach, including requirement analysis, system design, implementation, and testing. The developed system enables citizens to submit requests online and is equipped with features such as officer verification, digital signing by the village head, automatic notifications, digital archiving, and document verification using QR Codes. Security mechanisms are implemented using SHA-256 cryptographic hashing and RSA-2048 digital signature algorithms, supported by X.509 digital certificates. Functional testing using end-to-end methods shows that all system features operate successfully without failures, while non-functional testing confirms the reliability of document security and integrity. The resulting system is able to automate the entire service process, reduce processing time, and ensure document authenticity and security. Therefore, this system can serve as a solution to support the digital transformation of public services at the village level.*

Keywords*: Digital Signature; Information System; Public Service; RSA; SHA-256.*

Abstrak. Pelayanan administrasi surat di tingkat nagari masih banyak dilakukan secara konvensional sehingga menimbulkan berbagai kendala, seperti keterbatasan waktu layanan, proses yang lambat, serta risiko kehilangan arsip. Penelitian ini bertujuan untuk mengembangkan sistem pelayanan surat berbasis web dengan penerapan tanda tangan digital di Nagari Bukit Bais guna meningkatkan efisiensi, keamanan, dan transparansi layanan publik. Metode yang digunakan adalah Agile Development dengan pendekatan iteratif melalui tahapan analisis kebutuhan, perancangan, implementasi, dan pengujian sistem. Sistem yang dikembangkan memungkinkan masyarakat mengajukan surat secara daring, dilengkapi dengan fitur verifikasi petugas, penandatanganan digital oleh Wali Nagari, notifikasi otomatis, pengarsipan digital, serta verifikasi dokumen menggunakan QR Code. Mekanisme keamanan diterapkan melalui algoritma kriptografi SHA-256 untuk hashing dan RSA-2048 untuk tanda tangan digital, serta penggunaan sertifikat digital X.509. Hasil pengujian fungsionalitas menggunakan metode end-to-end menunjukkan seluruh fitur sistem berjalan dengan baik tanpa kegagalan, sedangkan pengujian non-fungsionalitas membuktikan keandalan aspek keamanan dan integritas dokumen. Sistem yang dihasilkan mampu mengotomasi proses pelayanan secara terintegrasi, mempercepat waktu layanan, serta menjamin keaslian dan keamanan dokumen. Dengan demikian, sistem ini dapat menjadi solusi dalam mendukung transformasi digital pelayanan publik di tingkat nagari.

Kata kunci: RSA; SHA-256; Sistem Informasi; Tanda Tangan Digital; Layanan Publik.

1. LATAR BELAKANG

Pelayanan publik merupakan kebutuhan fundamental masyarakat yang wajib dipenuhi oleh pemerintah secara adil dan merata (Budiman et al., 2022). Dalam struktur pemerintahan Indonesia, pemerintah desa atau nagari memegang peran strategis sebagai ujung tombak pelayanan publik yang berinteraksi langsung dengan masyarakat (Majayanti et al., 2023). Peran tersebut sejalan dengan amanat Undang-Undang Nomor 6 Tahun 2014 tentang Desa yang mewajibkan desa untuk menyelenggarakan serta meningkatkan kualitas pelayanan kepada masyarakat setempat.

Artikel Masuk: 24 Februari 2026; Revisi: 20 Maret 2026; Diterima: 25 April 2026; Terbit: 27 April 2026

Salah satu bentuk pelayanan publik yang paling dibutuhkan masyarakat di tingkat desa atau nagari adalah penerbitan berbagai jenis surat keterangan (Kanda & Algias, 2024). Untuk meningkatkan kualitas pelayanan tersebut, pemerintah Indonesia mendorong transformasi digital melalui pemanfaatan teknologi informasi guna memudahkan akses masyarakat terhadap layanan publik (Hamdillah, 2023). Transformasi ini menjadi sangat krusial untuk mengatasi keterbatasan waktu, jarak, dan birokrasi dengan mengalihkan pelayanan menjadi berbasis daring, kecuali untuk layanan yang tetap memerlukan tatap muka langsung (Yanti et al., 2025).

Meskipun urgensi transformasi digital telah diakui secara luas, kondisi di lapangan menunjukkan adanya kesenjangan antara kebijakan dan implementasi. Pelayanan administrasi di banyak desa dan nagari masih dilaksanakan menggunakan sistem konvensional yang menimbulkan berbagai kendala bagi masyarakat (Romadhon & Maryam, 2023). Sistem pelayanan tersebut dinilai belum mampu memberikan layanan secara optimal, sehingga memunculkan kesenjangan antara harapan masyarakat terhadap pelayanan yang cepat, mudah, dan transparan dengan kenyataan pelayanan yang masih bersifat birokratis serta memerlukan waktu relatif lama (Amrin & Faqih, 2022).

Nagari Bukit Bais di Kecamatan IX Koto Sungai Lasi, Kabupaten Solok, Provinsi Sumatera Barat, merupakan salah satu nagari yang menghadapi permasalahan tersebut. Berdasarkan observasi lapangan dan wawancara dengan petugas nagari, pelayanan surat keterangan masih dilakukan secara konvensional yang mengharuskan masyarakat datang langsung ke kantor nagari dengan membawa persyaratan fisik, kemudian petugas memeriksa kelengkapan berkas dan membuatkan surat menggunakan aplikasi Microsoft Word. Data pelayanan periode Januari hingga Maret 2025 menunjukkan volume penerbitan sebanyak 88 surat dengan rata-rata 29 surat per bulan, bahkan pada periode tertentu dapat mencapai lebih dari 10 pengajuan dalam satu hari. Yang menarik dari kondisi Nagari Bukit Bais adalah ketersediaan infrastruktur teknologi informasi berupa jaringan internet fiber optik sejak tahun 2019 dan menara telekomunikasi sejak tahun 2024, namun infrastruktur ini belum dimanfaatkan secara optimal untuk meningkatkan kualitas pelayanan kepada masyarakat.

Sistem pelayanan secara konvensional yang masih diterapkan saat ini menimbulkan berbagai permasalahan operasional. Masyarakat hanya dapat mengakses layanan pada jam kerja kantor, sehingga warga yang memiliki kesibukan tertentu atau berdomisili di luar daerah mengalami kesulitan dalam mengurus surat yang dibutuhkan. Selain itu, pengelolaan arsip surat yang telah diterbitkan masih dilakukan secara manual dengan menyimpan dokumen fisik dan pencatatan pada buku besar. Kondisi ini menyebabkan proses penelusuran kembali arsip

memerlukan waktu yang relatif lama serta berisiko kehilangan atau kerusakan dokumen (Qadir & Adri, 2022).

Permasalahan lain yang tidak kalah krusial terjadi pada proses penandatanganan surat oleh Wali Nagari. Surat yang telah selesai diproses harus dicetak dan menunggu tanda tangan Wali Nagari sebelum dapat diserahkan kepada masyarakat. Proses penandatanganan tersebut sangat bergantung pada kehadiran fisik Wali Nagari dan tidak dapat dilakukan apabila yang bersangkutan sedang menjalankan tugas di luar kantor (Gunawan et al., 2024). Akibatnya, meskipun petugas telah menyelesaikan pemrosesan dokumen, surat tidak dapat segera diberikan kepada masyarakat karena harus menunggu ketersediaan Wali Nagari untuk melakukan penandatanganan.

Untuk mengatasi permasalahan tersebut, implementasi tanda tangan digital menjadi solusi yang relevan. Tanda tangan digital merupakan mekanisme penandatanganan dokumen elektronik yang memiliki kekuatan hukum setara dengan tanda tangan basah serta mampu menjamin keaslian, integritas, dan non-repudiasi dokumen (Aryasanti et al., 2022). Penerapan tanda tangan digital memungkinkan proses penandatanganan tidak lagi sepenuhnya bergantung pada kehadiran fisik pejabat, sehingga Wali Nagari dapat melakukan penandatanganan dokumen dari lokasi mana pun secara aman.

Beberapa penelitian telah menunjukkan efektivitas penerapan tanda tangan digital dalam pelayanan administrasi. Yusuf et al. (2025) membuktikan bahwa penerapan sistem tanda tangan digital berbasis web pada administrasi desa mampu meningkatkan efisiensi waktu pelayanan secara signifikan, dari rata-rata 2–3 hari menjadi kurang dari 10 menit. Selanjutnya, Atmoko (2024) juga membuktikan bahwa aplikasi layanan masyarakat yang dilengkapi dengan tanda tangan digital mampu menyederhanakan proses administrasi desa, dengan hasil pengujian usability mencapai skor 99% pada kategori “Sangat Setuju”.

Agar tanda tangan digital dapat diterapkan secara aman dan andal, diperlukan dukungan algoritma kriptografi yang mampu menjamin integritas dan autentikasi dokumen elektronik. Dalam proses penandatanganan digital, integritas dokumen dijaga melalui penggunaan algoritma hash SHA-256, yaitu fungsi hash kriptografis yang menghasilkan nilai unik dari suatu data, di mana perubahan sekecil apa pun pada isi dokumen akan menghasilkan nilai hash yang sangat berbeda (Setiadi et al., 2024). Nilai hash tersebut selanjutnya ditandatangani menggunakan algoritma RSA yang bekerja berdasarkan prinsip pasangan kunci publik dan kunci privat, sehingga memungkinkan proses penandatanganan dan verifikasi dokumen dilakukan secara aman serta menjamin keautentikan dokumen yang ditandatangani (Lubis et al., 2024).

Selain penggunaan algoritma kriptografi, keamanan dan keabsahan tanda tangan digital juga sangat bergantung pada penggunaan sertifikat digital yang berfungsi sebagai identitas elektronik yang mengaitkan kunci publik dengan identitas pemiliknya, sehingga dapat memastikan bahwa tanda tangan digital benar-benar dihasilkan oleh pihak yang berwenang (Setiawan & Kertanegara, 2023). Sertifikat digital tersebut merupakan bagian penting dari infrastruktur kunci publik yang digunakan untuk memverifikasi keaslian dan integritas dokumen elektronik, sekaligus membangun kepercayaan dalam penerapan sistem pelayanan administrasi berbasis digital yang dapat diverifikasi oleh pihak terkait (Chia et al., 2021; El Mane et al., 2021).

Untuk memudahkan verifikasi keaslian dokumen oleh pihak ketiga, setiap surat yang diterbitkan akan dilengkapi dengan QR Code. QR Code merupakan kode dua dimensi yang mampu menyimpan berbagai jenis data, seperti teks dan URL, serta dirancang untuk memberikan respons cepat saat dipindai sehingga memungkinkan akses instan ke informasi yang tersimpan (Burhanuddin et al., 2023; Shokeen, 2022). Mekanisme ini penting untuk mencegah pemalsuan dokumen dan memberikan jaminan autentikasi yang dapat dilakukan kapan saja dan di mana saja (Gunawan et al., 2024). Sebagai fitur tambahan, sistem juga menyediakan notifikasi otomatis untuk memberikan informasi real-time kepada masyarakat mengenai status pengajuan surat mereka, sehingga meningkatkan transparansi pelayanan.

Berdasarkan uraian tersebut, Tugas Akhir ini bertujuan untuk mengembangkan sistem pelayanan surat berbasis web di Nagari Bukit Bais dengan menerapkan tanda tangan digital. Sistem yang dikembangkan diharapkan mampu mengatasi kelemahan pelayanan konvensional, memanfaatkan infrastruktur teknologi yang telah tersedia, serta mendukung transformasi digital pelayanan publik di tingkat nagari.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan pengembangan sistem dengan metode Agile Development yang menekankan proses iteratif dan inkremental dalam membangun sistem sesuai kebutuhan pengguna. Tahap awal penelitian dimulai dengan analisis kebutuhan (requirements) melalui observasi dan wawancara dengan pihak Nagari Bukit Bais untuk memahami proses bisnis yang sedang berjalan. Hasil analisis menunjukkan bahwa pelayanan surat keterangan masih dilakukan secara konvensional, di mana masyarakat harus datang langsung ke kantor nagari dengan membawa dokumen persyaratan seperti KTP dan KK. Proses pemeriksaan berkas, pembuatan surat menggunakan aplikasi pengolah kata, hingga pencatatan arsip dilakukan secara manual, sehingga menyebabkan keterbatasan layanan, lamanya waktu

penyelesaian, serta tingginya potensi kesalahan administrasi dan kesulitan dalam penelusuran arsip.

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan perancangan sistem pelayanan surat berbasis web yang mampu mendigitalisasi seluruh alur pelayanan secara terintegrasi. Sistem yang dikembangkan memungkinkan masyarakat melakukan pengajuan surat secara daring, yang kemudian diverifikasi oleh petugas sebelum diteruskan kepada Wali Nagari untuk proses penandatanganan digital. Sistem ini juga dilengkapi dengan fitur notifikasi otomatis melalui WhatsApp, pengarsipan digital, serta verifikasi dokumen menggunakan QR Code guna meningkatkan transparansi, efisiensi, dan keamanan layanan. Dengan demikian, pelayanan tidak lagi terbatas oleh waktu dan lokasi, serta dapat memberikan kemudahan akses bagi masyarakat dalam memperoleh layanan administrasi.

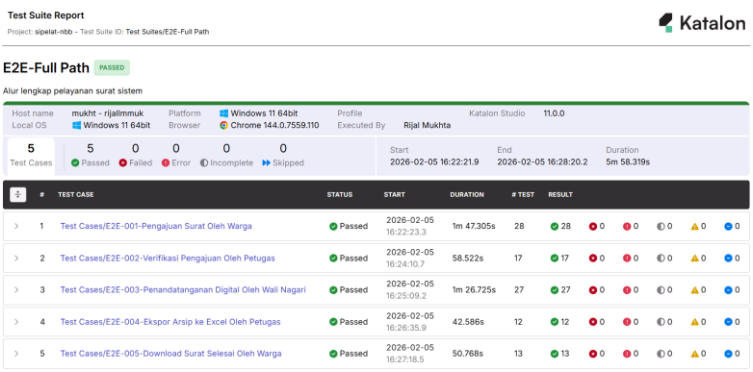
Dalam implementasinya, sistem ini memanfaatkan teknologi kriptografi untuk menjamin keaslian dan integritas dokumen melalui penerapan algoritma SHA-256 sebagai fungsi hash dan algoritma RSA sebagai mekanisme tanda tangan digital. Sertifikat digital berbasis standar X.509 digunakan sebagai identitas elektronik penandatangan yang disimpan dalam format PKCS#12 guna menjaga keamanan kunci privat. Selain itu, pengembangan sistem didukung oleh berbagai library seperti DomPDF, TCPDF, FPDI, OpenSSL, dan PHP QR Code, serta teknologi antarmuka seperti Tailwind CSS dan Alpine.js. Dengan pendekatan ini, sistem yang dihasilkan diharapkan memiliki tingkat keamanan yang tinggi, andal, serta mampu meningkatkan kualitas pelayanan administrasi di lingkungan nagari.

3. HASIL DAN PEMBAHASAN

Pengujian

Pengujian Fungsionalitas

Pengujian fungsionalitas dilakukan menggunakan pendekatan *end-to-end (E2E) testing* untuk memvalidasi alur kerja sistem secara menyeluruh. Pengujian ini mensimulasikan interaksi pengguna dengan sistem mulai dari proses login hingga verifikasi dokumen yang telah ditandatangani digital. Pengujian dilakukan menggunakan Katalon Studio versi 11.0.0 yang memungkinkan otomatisasi pengujian antarmuka web. Ringkasan hasil eksekusi *test suite* E2E dengan Katalon Studio dapat dilihat pada gambar berikut.



Gambar 1. Ringkasan Hasil Eksekusi *Test Suite* E2E Katalon Studio.

Setiap *test case* terdiri dari beberapa langkah pengujian yang mencatat aksi pengguna, hasil yang diharapkan, serta status keberhasilan. Tabel 4.1 menyajikan detail langkah pengujian fungsionalitas sistem secara lengkap.

Tabel 1. Hasil Pengujian Fungsionalitas Sistem.

No	Aktor	Aksi	Hasil yang Diharapkan	Status
1	Warga	Membuka halaman beranda dan mengklik "Login Warga"	Sistem mengarahkan ke halaman login warga	✓
2	Warga	Memasukkan NIK dan Tanggal Lahir yang valid, lalu mengklik "Masuk"	Login berhasil, sistem mengarahkan ke dashboard warga	✓
3	Warga	Melihat notifikasi "Data belum lengkap" dan mengklik "Lengkapi Sekarang"	Sistem mengarahkan ke halaman profil warga	✓
4	Warga	Menambahkan nomor WhatsApp yang valid dan mengklik "Simpan"	Nomor tersimpan, notifikasi berhasil tampil	✓
5	Warga	Mengunggah foto Kartu Keluarga (format JPG, ukuran <2MB)	File berhasil diunggah, notifikasi sukses tampil	✓
6	Warga	Mengunggah foto KTP/KIA (format JPG, ukuran <2MB)	File berhasil diunggah, notifikasi sukses tampil, notifikasi "Profil lengkap" muncul	✓
7	Warga	Kembali ke dashboard, mengklik jenis surat "Surat Keterangan Domisili"	Sistem mengarahkan ke halaman formulir pengajuan surat SKD	✓
8	Warga	Melengkapi semua data formulir pengajuan	Semua field terisi, validasi data berhasil	✓
9	Warga	Mengklik "Ajukan Surat"	Pengajuan berhasil, notifikasi sukses tampil, sistem mengarahkan ke halaman detail pengajuan dengan status "Diajukan", WhatsApp terkirim ke warga dan petugas	✓
10	Warga	Mengklik tombol "Logout"	Sistem mengarahkan ke halaman beranda	✓
11	Petugas	Membuka halaman login petugas dan melakukan login	Sistem mengarahkan ke dashboard petugas yang menampilkan notifikasi "1 pengajuan perlu diproses"	✓
12	Petugas	Mengklik menu pengajuan "Perlu Diproses"	Sistem mengarahkan ke halaman daftar pengajuan dengan status "Diajukan"	✓
13	Petugas	Mengklik aksi "Proses" pada pengajuan	Sistem mengarahkan ke halaman proses verifikasi pengajuan surat	✓
14	Petugas	Memilih aksi "Terima & Proses"	Pengajuan berhasil diterima, status pengajuan berubah menjadi "Menunggu TTD", WhatsApp terkirim ke warga dan Wali Nagari	✓
15	Petugas	Mengklik tombol "Logout"	Sistem mengarahkan ke halaman beranda	✓
16	Wali Nagari	Membuka halaman login Wali Nagari dan melakukan login	Sistem mengarahkan ke dashboard Wali Nagari yang menampilkan notifikasi "1 surat menunggu tanda tangan"	✓
17	Wali Nagari	Mengklik menu "Sertifikat Digital"	Sistem mengarahkan ke halaman daftar sertifikat digital	✓

No	Aktor	Aksi	Hasil yang Diharapkan	Status
18	Wali Nagari	Mengklik "Buat Sertifikat Digital"	Sistem mengarahkan ke halaman pembuatan sertifikat digital	✓
19	Wali Nagari	Memasukkan passphrase keamanan dan konfirmasi passphrase	Muncul indikator konfirmasi passphrase cocok	✓
20	Wali Nagari	Mengklik "Buat Sertifikat Digital"	Sertifikat digital berhasil dibuat, notifikasi sukses tampil, sistem mengarahkan ke halaman daftar sertifikat digital	✓
21	Wali Nagari	Mengklik menu "Tandatangani Surat"	Sistem mengarahkan ke halaman daftar surat dengan status menunggu tanda tangan	✓
22	Wali Nagari	Mengklik "Tinjau & Tandatangani"	Sistem mengarahkan ke halaman pratinjau final surat dalam format PDF	✓
23	Wali Nagari	Mengklik "Tandatangani Dokumen"	Modal input passphrase muncul	✓
24	Wali Nagari	Memasukkan passphrase yang valid dan mengklik "Tanda Tangani"	Surat berhasil ditandatangani, status berubah menjadi "Selesai", WhatsApp terkirim ke warga, sistem mengarahkan ke halaman daftar surat menunggu tanda tangan	✓
25	Wali Nagari	Mengklik tombol "Logout"	Sistem mengarahkan ke halaman beranda	✓
26	Petugas	Melakukan login kembali ke dashboard petugas	Sistem mengarahkan ke dashboard petugas	✓
27	Petugas	Mengklik menu "Arsip Surat"	Sistem mengarahkan ke halaman arsip surat dengan status "Selesai"	✓
28	Petugas	Mengklik tombol "Ekspor Excel"	File Excel berisi daftar arsip surat berhasil diunduh	✓
29	Petugas	Mengklik tombol "Logout"	Sistem mengarahkan ke halaman beranda	✓
30	Warga	Melakukan login kembali dengan NIK dan Tanggal Lahir	Sistem mengarahkan ke dashboard warga	✓
31	Warga	Mengklik menu "Riwayat Pengajuan"	Daftar pengajuan tampil dengan status "Selesai"	✓
32	Warga	Mengklik aksi "Download" pada pengajuan	File PDF bertanda tangan digital terunduh	✓
33	Warga	Membuka file PDF yang diunduh	Dokumen tampil lengkap dengan QR code pada area tanda tangan	✓
34	Publik	Memindai QR code menggunakan perangkat smartphone	QR Code berisi URL yang mengarah ke halaman verifikasi dokumen pada sistem	✓
35	Publik	Melihat halaman verifikasi dokumen	Status "Dokumen Valid" tampil dengan informasi: data surat, pemohon, tanggal penandatanganan, nama Wali Nagari, dan metadata dokumen	✓

Pengujian Non-Fungsionalitas

Pengujian non-fungsionalitas dilakukan menggunakan pendekatan unit testing dengan framework PHPUnit untuk memvalidasi fungsi-fungsi kriptografi secara terisolasi. Pengujian ini difokuskan pada modul yang mengimplementasikan mekanisme keamanan tanda tangan digital, meliputi algoritma hashing SHA-256, enkripsi asimetris RSA-2048, serta alur lengkap penandatanganan dan verifikasi dokumen menggunakan sertifikat digital X.509.

a. Pengujian Algoritma SHA-256

Pengujian algoritma SHA-256 dilakukan untuk memverifikasi karakteristik fungsi *hash* yang digunakan dalam proses penandatanganan digital. Empat skenario pengujian dilaksanakan untuk memvalidasi properti *hash* yang meliputi konsistensi panjang output, sifat deterministik, efek *avalanche*, dan kemampuan deteksi modifikasi dokumen. Tabel 2 menyajikan hasil pengujian algoritma SHA-256.

Tabel 2. Hasil Pengujian Algoritma SHA-256.

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Aktual
1	Output *hash* selalu 64 karakter (256 bit)	Input dengan panjang berbeda menghasilkan *hash* 64 karakter	Input "Halo" (4 karakter) dan input panjang (82 karakter) menghasilkan *hash* 64 karakter
2	Sifat deterministik: input sama menghasilkan output sama	*Hash* yang dihasilkan identik untuk input yang sama	Tiga kali proses *hashing* menghasilkan nilai identik
3	Efek *avalanche*: perubahan 1 karakter mengubah sebagian besar output	Perubahan minimal pada input menghasilkan *hash* yang sangat berbeda	Perubahan 1 huruf mengakibatkan perbedaan 95.3% (61/64 karakter)
4	Verifikasi integritas dokumen PDF	Dokumen yang telah diubah akan memiliki nilai *hash* yang berbeda dari aslinya	Modifikasi 1 byte data pada file PDF terdeteksi mengubah 59 dari 64 karakter *hash*

Sebagai contoh validasi, dokumen sample.pdf (405,657 bytes) menghasilkan nilai hash SHA-256: ea6d7a3c0a0fb097f45011e2b0fb ff00ae234f9c82034aa4abd9ce4e4da03811. Ketika dokumen diubah sebesar 1 byte, *hash* berubah menjadi 701d9654471c66c0745786ce4d5 06262f334157756bb7d43d3c34888ad02e837, menunjukkan 59 dari 64 karakter (92.2%) berubah. Pengujian efek *avalanche* pada teks "Nama: Bapak Ahmad" menghasilkan *hash* 639c5977a458a989bfd625ddca02 1170550cc04ae7c8236faba97b5da8a70056, sedangkan perubahan 1 huruf menjadi "Nama: Bapak Ahmae" menghasilkan *hash* 8bba3713bd 3cfa90677a118a13b9efbb4c1085804f50b34eea97ee58b87fa405.

b. Pengujian Enkripsi RSA-2048

Pengujian enkripsi RSA-2048 dilakukan untuk memverifikasi proses pembangkitan kunci, penandatanganan dokumen, dan verifikasi tanda tangan digital. Lima skenario pengujian dilaksanakan untuk memvalidasi mekanisme kriptografi asimetris yang digunakan dalam sistem. Tabel 4.3 menyajikan hasil pengujian algoritma RSA-2048.

Tabel 3. Hasil Pengujian Algoritma RSA-2048.

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Aktual
1	Pembangkitan pasangan kunci RSA-2048	Kunci privat dan publik berhasil dibuat dengan ukuran 2048 bit	Pasangan kunci berhasil dibuat dengan ukuran akurat 2048-bit dan eksponen 65537
2	Penandatanganan dokumen PDF	*Signature* berhasil dibuat dengan ukuran 256 bytes	Signature (256 bytes) berhasil dibuat dari dokumen PDF 405,657 bytes
3	Verifikasi tanda tangan dengan *public key*	Tanda tangan valid dapat diverifikasi	openssl_verify() mengembalikan nilai 1 (VALID)
4	Deteksi modifikasi dokumen	Dokumen yang dimodifikasi terdeteksi invalid	Modifikasi 1 byte: Hash berbeda 92.2%, Verify: INVALID
5	Kinerja penandatanganan dokumen	Waktu penandatanganan dalam batas yang dapat diterima (<1 detik)	Hashing: 3.69 ms, Signing: 2.75 ms

Proses penandatanganan digital menghasilkan *signature* dengan format heksadesimal sepanjang 256 bytes. Contoh *signature* yang dihasilkan pada penandatanganan dari dokumen sample.pdf adalah: 5745fd85715173912b4836ae3b... . Fungsi openssl_verify() mengembalikan nilai 1 untuk dokumen yang valid dan nilai 0 untuk dokumen yang telah dimodifikasi, membuktikan kemampuan sistem dalam mendeteksi perubahan dokumen.

c. Pengujian Alur Lengkap Tanda Tangan Digital

Pengujian alur lengkap tanda tangan digital dilakukan untuk memverifikasi integrasi seluruh komponen kriptografi dalam satu *workflow* yang simultan. Pengujian ini mencakup dua belas tahapan dari pembangkitan kunci hingga deteksi modifikasi dokumen, serta validasi keamanan. Tabel 4.4 menyajikan hasil pengujian alur lengkap tanda tangan digital.

Tabel 4. Hasil Pengujian Alur Lengkap Tanda Tangan Digital.

No	Proses	Hasil Aktual
1	Pembangkitan kunci RSA-2048	Kunci berhasil dibuat dengan ukuran 2048-bit dan eksponen 010001
2	Pembuatan sertifikat X.509	Sertifikat berhasil dibuat dengan masa aktif 730 hari
3	Ekspor ke format PKCS#12	Sertifikat dan kunci privat diekspor ke file .p12 dengan *passphrase*
4	Penyimpanan berkas .p12	File .p12 berhasil tersimpan di direktori server
5	Pembacaan PKCS#12 dengan *passphrase*	Sertifikat dan kunci privat berhasil diekstrak menggunakan passphrase yang benar
6	Membaca dokumen PDF	File sample.pdf (405,657 bytes) berhasil dimuat oleh sistem
7	Perhitungan *hash* SHA-256	Nilai *hash* (64 karakter) berhasil dihitung dari dokumen
8	Penandatanganan dengan kunci privat	Signature 256 bytes (256 bytes) berhasil dibuat dan disematkan
9	Verifikasi tanda tangan	Dokumen asli belum berubah, status verifikasi VALID
10	Deteksi modifikasi dokumen	Dokumen diubah 1 byte: Hash berbeda 92.2%, Verify: INVALID
11	Penolakan *passphrase* salah	Sistem menolak akses sertifikat saat diberikan *passphrase* yang salah

Nilai *hash* SHA-256 lengkap yang dihasilkan pada Tahap 7 adalah ea6d7a3c0a0fb097f45011e2b0fbff00ae234f9c82034aa4abd9ce4e4da03811. Nilai ini digunakan sebagai input untuk proses penandatanganan pada Tahap 8. Sertifikat X.509 yang dibuat pada Tahap 2 memiliki masa berlaku 2 tahun sejak sertifikat dibuat, dengan informasi *subject* yang mencakup identitas Wali Nagari sebagai pemilik sertifikat.

Pembahasan

Sistem pelayanan surat berbasis web dengan penerapan tanda tangan digital di Nagari Bukit Bais berhasil dikembangkan menggunakan metode *Agile Development*, yang memungkinkan pengembangan sistem dilakukan secara bertahap dan adaptif terhadap

kebutuhan operasional nagari. Pendekatan ini memberikan fleksibilitas dalam penyempurnaan sistem berdasarkan evaluasi pada setiap iterasi. Penggunaan *framework* Laravel dengan arsitektur *Model-View-Controller (MVC)* menghasilkan struktur kode yang terorganisir dan mudah dipelihara, sedangkan MySQL dipilih sebagai basis data karena kemampuannya dalam mengelola relasi data secara konsisten dan stabil.

Sistem yang dikembangkan mampu mengotomasi seluruh alur pelayanan surat, mulai dari pengajuan oleh warga, verifikasi oleh petugas, penandatanganan digital oleh Wali Nagari, hingga pengarsipan dokumen secara digital. Digitalisasi proses ini memberikan dampak signifikan terhadap efisiensi pelayanan karena proses administrasi tidak lagi bergantung pada interaksi tatap muka dan dokumen fisik. Setiap peran pengguna dibekali hak akses yang berbeda sesuai kewenangannya, sehingga operasional sistem berjalan lebih tertib dan terkontrol.

Implementasi tanda tangan digital menjadi inti dari sistem ini yang membedakannya dari sistem pelayanan surat konvensional. Mekanisme tanda tangan digital diterapkan menggunakan kombinasi algoritma kriptografi SHA-256 untuk fungsi *hash* dan algoritma RSA dengan panjang kunci yang sesuai standar keamanan modern untuk enkripsi asimetris. Proses dimulai dengan pembangkitan pasangan kunci menggunakan OpenSSL yang menghasilkan kunci privat dan kunci publik. Kunci privat bersama dengan sertifikat digital X.509 versi 3 disimpan dalam format PKCS#12 yang dilindungi dengan *passphrase* untuk mencegah penyalahgunaan. Sertifikat digital yang digunakan dalam sistem ini merupakan *self-signed certificate* yang dibuat secara mandiri, memuat informasi identitas Wali Nagari sebagai penandatangan yang sah.

Proses penandatanganan dokumen dilakukan dengan menghitung *nilai* hash SHA-256 dari seluruh konten dokumen PDF yang menghasilkan *digest* sepanjang 256 bit. Nilai *hash* ini kemudian dienkripsi menggunakan kunci privat RSA untuk menghasilkan *signature* digital berukuran 256 byte. *Library* TCPDF digunakan untuk menyisipkan *signature* dalam format PKCS#7 *(Cryptographic Message Syntax)* ke dalam struktur PDF, sehingga tanda tangan menjadi bagian integral dari dokumen. Mekanisme ini menjamin tiga aspek keamanan yang krusial, yaitu autentikasi yang memastikan dokumen ditandatangani oleh pihak yang berwenang, integritas yang menjamin dokumen tidak mengalami perubahan setelah ditandatangani, serta *non-repudiation* yang mencegah penandatangan menyangkal telah menandatangani dokumen.

Pengujian fungsionalitas sistem dilakukan menggunakan pendekatan *end-to-end testing* dengan Katalon Studio untuk memvalidasi alur kerja sistem secara menyeluruh dari perspektif

pengguna. Sejumlah skenario pengujian telah dieksekusi yang mencakup seluruh proses bisnis sistem mulai dari autentikasi pengguna, pengelolaan profil dan dokumen kependudukan, pengajuan surat, verifikasi pengajuan oleh petugas, pembuatan sertifikat digital, penandatanganan dokumen, pengarsipan dan ekspor data, hingga verifikasi keaslian dokumen. Seluruh *test case* berhasil dijalankan tanpa kegagalan yang menunjukkan bahwa sistem telah memenuhi kebutuhan fungsional yang telah ditetapkan pada tahap analisis. Hasil pengujian ini mengonfirmasi bahwa integrasi antar modul sistem berjalan dengan baik dan alur pelayanan dapat diselesaikan secara *end-to-end* tanpa hambatan teknis.

Pengujian non-fungsionalitas dilakukan melalui *unit testing* menggunakan *framework* PHPUnit untuk memvalidasi keandalan implementasi algoritma kriptografi secara terisolasi. Pengujian terhadap algoritma SHA-256 membuktikan bahwa fungsi *hash* bekerja sesuai dengan spesifikasi kriptografi yang diharapkan, menghasilkan *output* dengan panjang konsisten, bersifat deterministik, serta menunjukkan efek *avalanche* yang signifikan di mana modifikasi minimal pada input mengakibatkan perubahan signifikan pada nilai hash. Pengujian algoritma RSA memvalidasi seluruh tahapan kriptografi asimetris mulai dari pembangkitan kunci, penandatanganan, hingga verifikasi. Pengujian alur lengkap tanda tangan digital yang mencakup pembangkitan kunci, pembuatan sertifikat X.509 versi 3, ekspor ke PKCS#12, validasi *passphrase*, perhitungan hash, penandatanganan, verifikasi, dan deteksi modifikasi menunjukkan bahwa seluruh komponen kriptografi terintegrasi dengan baik dan memenuhi standar keamanan yang diperlukan untuk menjamin autentikasi, integritas, dan non-repudiation dokumen elektronik.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil perancangan, implementasi, dan pengujian sistem pelayanan surat berbasis web dengan penerapan tanda tangan digital di Nagari Bukit Bais, dapat disimpulkan bahwa sistem yang dikembangkan telah berhasil mengotomasi seluruh proses pelayanan administrasi secara terintegrasi, mulai dari tahap pengajuan oleh masyarakat, verifikasi oleh petugas, penandatanganan digital oleh Wali Nagari, hingga pengarsipan dokumen secara digital. Sistem ini dibangun menggunakan metode Agile dengan dukungan teknologi Laravel dan MySQL, sehingga mampu memberikan fleksibilitas serta kemudahan dalam pengembangan dan pengelolaan sistem. Penerapan mekanisme tanda tangan digital menggunakan algoritma SHA-256 dan RSA terbukti mampu menjamin autentikasi penandatangan, menjaga integritas dokumen, serta mencegah terjadinya penyangkalan (non-repudiation). Selain itu, implementasi sertifikat digital X.509 versi 3 berbasis self-signed

menggunakan OpenSSL yang disimpan dalam format PKCS#12 terenkripsi turut meningkatkan keamanan dalam pengelolaan kunci privat dan identitas elektronik penandatangan.

Di sisi lain, sistem juga menunjukkan kinerja yang andal melalui penerapan fitur arsip digital yang dilengkapi dengan fungsi pencarian, filter, dan ekspor data, sehingga mempermudah proses penyimpanan dan penelusuran dokumen serta meminimalkan risiko kehilangan atau kerusakan data. Hasil pengujian end-to-end menggunakan Katalon Studio menunjukkan bahwa seluruh alur sistem berjalan sesuai dengan rancangan tanpa ditemukan kegagalan, sementara pengujian unit menggunakan PHPUnit membuktikan keandalan implementasi algoritma kriptografi yang digunakan. Meskipun demikian, pengembangan lebih lanjut masih diperlukan, seperti integrasi dengan Penyelenggara Sertifikasi Elektronik (PSrE) yang tersertifikasi secara nasional untuk meningkatkan tingkat kepercayaan terhadap sertifikat digital, pengembangan aplikasi mobile berbasis Android dan iOS guna meningkatkan aksesibilitas layanan, serta penerapan mekanisme pencadangan data otomatis secara berkala untuk menjaga ketersediaan dan keamanan data dalam jangka panjang.

DAFTAR REFERENSI

Amrin, A., & Faqih, A. (2022). Sistem informasi pelayanan pembuatan surat pada masyarakat desa. *INSANtek, 3*(2), 55-60. https://doi.org/10.31294/instk.v3i2.1529

Aryasanti, A., Hardjianto, M., Brotosaputro, G., & Roeswidiah, R. (2022). Implementasi tanda tangan digital menggunakan RSA dan SHA-512. *Jurnal Ticom, 10*(3), 181-186.

Atmoko, R. Y. (2024). Pengembangan aplikasi layanan masyarakat secara digital dengan digital signature. *Integrative Perspectives of Social and Science Journal, 1*(1), 78-97.

Budiman, A. F. F., Putri Setia, A. A., & Jauza, D. (2022). Penerapan etika pelayanan publik dalam mewujudkan good governance. *Jurnal Dialektika: Jurnal Ilmu Sosial, 19*(1), 64-74. https://doi.org/10.54783/dialektika.v19i1.65

Burhanuddin, A., Nugraha, F., Fithri, D. L., Handayani, P. K., & Susanti, N. (2023). Pemanfaatan QR Code untuk sistem informasi kependudukan. *Jurnal SITECH, 6*(2), 85-92. https://doi.org/10.24176/sitech.v6i2.9824

Chia, J., Heng, S., Chin, J., Tan, S., & Yau, W. (2021). An implementation suite for a hybrid public key infrastructure. *Symmetry, 13*, 1535. https://doi.org/10.3390/sym13081535

Gunawan, R., Rahmatulloh, A., & Rizal, R. (2024). Implementasi digital signature berbasis QR Code. *STRING, 9*(2), 133. https://doi.org/10.30998/string.v9i2.21407

Hamdillah, H. (2023). Inovasi pelayanan publik dan transformasi birokrasi. *Resolusi: Jurnal Sosial Politik, 6*(2), 91-102. https://doi.org/10.32699/resolusi.v6i2.5672

Kanda, A. S., & Algias, M. S. (2024). Refleksi performa pelayanan administrasi di tingkat kelurahan atau desa Gunung Halu. *Lokawati: Jurnal Penelitian Manajemen dan Inovasi Riset, 2*(2), 229-242. https://doi.org/10.61132/lokawati.v2i2.661

Lubis, Y., Rusydi, I., & Elyas, A. H. (2024). Implementasi algoritma RSA pada tanda tangan digital. *Warta Dharmawangsa, 18*(4), 1429-1439. https://doi.org/10.46576/wdw.v18i4.5247

Majayanti, D., Hariadi, B., & Adnani, A. (2023). Peranan pemerintahan nagari dalam meningkatkan pelayanan masyarakat di nagari persiapan Bandua. *JAPan: Jurnal Administrasi dan Pemerintahan, 1*(1). https://doi.org/10.55850/japan.v1i1.72

Mane, A., Chihab, Y., & Korchiyne, R. (2021). Digital signature for data and documents using PKI certificates. *SHS Web of Conferences*.

Qadir, S. A., & Adri, M. (2022). Rancang bangun sistem pelayanan kantor wali nagari berbasis web. *ALGORITMA, 6*(1).

Romadhon, A. L., & Maryam, M. (2023). Rancang bangun sistem informasi layanan administrasi desa berbasis web. *JIPI, 8*(2), 514-524. https://doi.org/10.29100/jipi.v8i2.3553

Setiadi, I., Widianti, S., & Kayuan, I. P. P. (2024). Implementasi kriptografi menggunakan AES-256 dan SHA-256. *Jurnal Penelitian Rumpun Ilmu Teknik, 3*(4), 153-178.

Setiawan, H., & Kertanegara, A. M. Z. R. (2023). Perancangan infrastruktur kunci publik berbasis web. *Computer Based Information System Journal, 11*(1), 1-11. https://doi.org/10.33884/cbis.v11i1.6504

Shokeen, G. (2022). QR Code analysis. *International Journal for Research in Applied Science and Engineering Technology, 10*(12), 747-752. https://doi.org/10.22214/ijraset.2022.47978

Yanti, R. P., Jufri, Y., & Putra, S. (2025). Pelayanan administrasi interaktif berbasis digital masyarakat nagari Ampalu. *FOKUS: Publikasi Ilmiah, 23*(1).

Yusuf, A. M., Putra, W. P., Irawan, J., Iswanto, M. E., & Borjulius, R. (2025). Penerapan sistem digital signature untuk administrasi desa. *GANESHA: Jurnal Pengabdian Masyarakat, 5*(2), 841-851. https://doi.org/10.36728/ganesha.v5i2.5377