PENERAPAN TANDA TANGAN DIGITAL BERBASIS ECDSA YANG DISEMATKAN DALAM QR CODE UNTUK AUTENTIKASI DOKUMEN DIGITAL

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

EDO RAHMATULLAH

19.83.0441

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

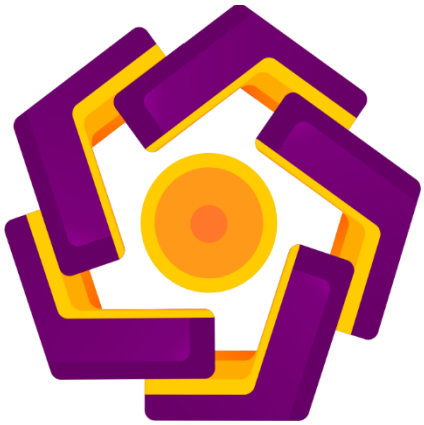
2026

PENERAPAN TANDA TANGAN DIGITAL BERBASIS ECDSA YANG DISEMATKAN DALAM QR CODE UNTUK AUTENTIKASI DOKUMEN DIGITAL

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



disusun oleh

EDO RAHMATULLAH

19.83.0441

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

SKRIPSI

PENERAPAN TANDA TANGAN DIGITAL BERBASIS ECDSA YANG DISEMATKAN DALAM QR CODE UNTUK AUTENTIKASI DOKUMEN DIGITAL

yang disusun dan diajukan oleh

Edo Rahmatullah

19.83.0441

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 22 Juni 2026

Dosen Pembimbing,

Wahid Miftahul Ashari, S.Kom., M.T.
NIK. 190302452

HALAMAN PENGESAHAN

SKRIPSI

PENERAPAN TANDA TANGAN DIGITAL BERBASIS ECDSA YANG DISEMATKAN DALAM QR CODE UNTUK AUTENTIKASI DOKUMEN DIGITAL

yang disusun dan diajukan oleh

Edo Rahmatullah

19.83.0441

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Juni 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Jeki Kuswanto, S.Kom., M.Kom. **NIK. 190302456**	
Muhammad Rudyanto Arief, S.T., M.T. **NIK. 190302098**	
Wahid Miftahul Ashari, S.Kom., M.T. **NIK. 190302452**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Juni 2026

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Edo Rahmatullah
NIM : 19.83.0441

Menyatakan bahwa Skripsi dengan judul berikut:

Penerapan Tanda Tangan Digital Berbasis ECDSA Yang Disematkan Dalam QR Code Untuk Autentikasi Dokumen Digital

Dosen Pembimbing : Wahid Miftahul Ashari, S.Kom., M.T.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 22 Juni 2026

Yang Menyatakan,

Edo Rahmatullah

HALAMAN PERSEMBAHAN

Alhamdulillah wa syukurillah puji syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis mendapatkan kelancaran, kekuatan, dan kemudahan dalam mengerjakan skripsi ini. Penulis juga ingin berterima kasih kepada orang-orang hebat yang telah mendampingi, yang selalu memberikan motivasi, inspirasi, bantuan dan dukungannya baik secara langsung maupun tidak langsung sehingga penulis dapat menyelesaikan skripsi ini dengan sebaik-baiknya. Penulis mempersembahkan skripsi ini kepada :

1. Kedua orang tua tercinta Bapak Suhodo dan Ibu Nety Asmarani yang telah senantiasa memberikan pengorbanan, dorongan, motivasi, restu, doa tanpa henti, dan segala bentuk dukungan dengan penuh kasih sayang, serta telah memberikan kesempatan yang besar bagi penulis untuk bisa menjalani masa perkuliahan ini hingga selesai.
2. Bapak Wahid Miftahul Ashari, S.Kom., M.T. yang telah membimbing dan membantu penulis dalam proses penyusunan skripsi ini.
3. Teman-teman seperjuangan jurusan Teknik Komputer yang telah menemani dan membantu penulis dari awal perkuliahan, terutama kepada mereka yang turut membantu penulis dalam menyelesaikan tugas-tugas kuliah.
4. Serta pada diri sendiri yang telah mau berjuang dan mampu bertahan sampai saat ini serta mampu mencapai titik penting dalam hidup.

Semoga persembahan ini dapat mengungkapkan rasa terima kasih penulis kepada semua yang telah berperan dalam kesuksesan penyelesaian skripsi ini.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT atas berkat, rahmat, dan anugerah-Nya yang memungkinkan penulis untuk menyelesaikan penyusunan skripsi ini dengan baik. Shalawat dan salam senantiasa tercurahkan kepada baginda Nabi Muhammad SAW, beserta keluarga, para sahabat, dan seluruh umatnya hingga akhir zaman.

Penulisan skripsi yang berjudul "**Penerapan Tanda Tangan Digital Berbasis ECDSA Yang Disematkan Dalam QR Code Untuk Autentikasi Dokumen Digital**" ini diajukan sebagai salah satu persyaratan untuk meraih gelar Sarjana pada Program Studi Teknik Komputer di Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.

Dalam proses penyusunan dan penulisan skripsi ini tidak terlepas dari bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin mengucapkan banyak terima kasih atas motivasi, bimbingan, saran dan masukan dari berbagai pihak baik secara rohaniah maupun moral. Dengan penuh kerendahan hati, penulis menyampaikan rasa terima kasih kepada yang terhormat :

1. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
2. Prof. Dr. Kusrini, M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Dony Aryus, S.S., M.Kom selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
4. Bapak Wahid Miftahul Ashari, S.Kom., M.T. selaku Dosen Pembimbing yang selalu memberikan bimbingan, saran, dan masukan dalam proses penulisan skripsi.
5. Bapak Jeki Kuswanto, S.Kom., M.Kom. dan Bapak Muhammad Rudyanto Arief, S.T., M.T. selaku Dosen Penguji yang telah memberikan saran serta masukan agar penelitian ini menjadi jauh lebih baik.

Penulis menyadari bahwa dalam penulisan skripsi ini masih banyak terdapat kekurangan, sehingga penulis mengharapkan untuk mendapatkan saran dan kritik yang membangun demi perbaikan dan penyempurnaan penelitian selanjutnya. Akhirnya, penulis hanya mampu menyerahkan segala puji hanya kepada Allah SWT. Semoga Allah SWT selalu melimpahkan rahmat dan karunia-Nya kepada kita semua.

Yogyakarta, 18 Mei 2026

Penulis

DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PERSETUJUAN ii
HALAMAN PENGESAHAN iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI iv
HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
DAFTAR ISI viii
DAFTAR TABEL x
DAFTAR GAMBAR xi
DAFTAR LAMPIRAN xii
DAFTAR LAMBANG DAN SINGKATAN xiii
DAFTAR ISTILAH xiv
INTISARI xvi
ABSTRACT xvii
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan Penelitian 3
1.5 Manfaat Penelitian 4
1.6 Sistematika Penulisan 4
BAB II TINJAUAN PUSTAKA 5
2.1 Studi Literatur 5
2.2 Dasar Teori 12
BAB III METODE PENELITIAN 25
3.1 Metode Penelitian 25
3.2 Alur Penelitian 25
3.3 Alat dan Bahan 27
BAB IV HASIL DAN PEMBAHASAN 36
BAB V PENUTUP 49
5.1 Kesimpulan 49
5.2 Saran 49

REFERENSI 51
LAMPIRAN.....54

DAFTAR TABEL

Tabel 2.1. Keaslian Penelitian 10
Tabel 3.1. Kebutuhan *Hardware* 27
Tabel 3.2. Kebutuhan *Software* 28
Tabel 4.1. Pengujian Fungsionalitas 47
Tabel 4.2. Pengujian Integritas 47

DAFTAR GAMBAR

Gambar 2.1. ECDSA 15
Gambar 2.2. Contoh QR Code 18
Gambar 2.3. Logo PDF 18
Gambar 2.4. Logo Wifi 20
Gambar 2.5. Logo Python 21
Gambar 2.6. Logo Flask 22
Gambar 2.7. Logo VSCode 22
Gambar 2.8. Jenis *Browser* 23
Gambar 2.9. Logo *Black Box Testing* 24
Gambar 3.1. Alur Penelitian 26
Gambar 3.2. Alur Proses Penandatangan 29
Gambar 3.3. Alur Verifikasi Dokumen 31
Gambar 4.1. Halaman Beranda 38
Gambar 4.2. Halaman *Upload* Dokumen 39
Gambar 4.3. Halaman Hasil *Generate Signature* 39
Gambar 4.4. Dokumen Hasil 40
Gambar 4.5. Halaman Verifikasi *Scan* QR Code 41
Gambar 4.6. Halaman Verifikasi Manual 43
Gambar 4.7. Halaman Verifikasi Status Valid 43
Gambar 4.8. Halaman Verifikasi Status Tidak Valid 44
Gambar 4.9. Halaman Riwayat 44
Gambar 4.10. Halaman Dashboard 45

DAFTAR LAMPIRAN

Lampiran 1. *Main Source Code* 54

DAFTAR LAMBANG DAN SINGKATAN

CA	*Certificate Authority*
CSS	*Cascading Style Sheets*
DOCX	*Document Open XML*
DSA	*Digital Signature Algorithm*
ECC	*Elliptic Curve Cryptography*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
ECDLP	*Elliptic Curve Discrete Logarithm Problem*
GUI	*Graphical User Interface*
HTML	*HyperText Markup Language*
HTTP	*Hypertext Transfer Protocol Secure*
IDE	*Integrated Development Environment*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
JSON	*JavaScript Object Notation*
LAN	*Local Area Network*
NIST	*National Institute of Standards and Technology*
PDF	*Portable Document Format*
PHP	*Hypertext Preprocessor*
QR Code	*Quick Response Code*
RSA	*Rivest-Shamir-Adleman*
SHA	*Secure Hash Algorithm*
SUS	*System Usability Scale*
SWOT	*Strengths, Weaknesses, Opportunities, Threats*
URL	*Uniform Resource Locator*
UX	*User Experience*
WSGI	*Web Server Gateway Interface*
(r, s)	pasangan nilai koordinat matematis hasil dari *signing* ECDSA
n	nilai modulus pada algoritma RSA (hasil perkalian bilangan prima)
2^{64}	batas maksimal panjang bit *input* untuk algoritma SHA-256

DAFTAR ISTILAH

Autentikasi	proses pembuktian atau validasi bahwa suatu dokumen atau identitas benar-benar sah dan berasal dari pihak yang diklaim
Avalanche Effect	karakteristik dalam fungsi *hash* di mana perubahan sekecil apa pun pada *input* akan menghasilkan perubahan yang sangat besar dan acak pada *output hash*
Base64 Encoding	metode penyandian data biner ke dalam bentuk string tekstual ASCII untuk mencegah kerusakan data saat ditranmisikan antar sistem
Black-Box Testing	metode pengujian perangkat lunak yang berfokus pada fungsionalitas luar (*input* dan *output*) tanpa harus memeriksa struktur atau kode internal program
Ciphertext	pesan atau data yang telah melalui proses enkripsi sehingga bentuknya menjadi acak dan tidak dapat dibaca tanpa kunci dekripsi
Client-side	bagian dari aplikasi atau situs *web* yang berjalan langsung di perangkat pengguna
Database (SQLite)	sistem penyimpanan data digital yang terstruktur, ringan, dan efisien yang digunakan aplikasi untuk merekam data secara kronologis
Integritas Dokumen	jaminan atau kondisi yang menyatakan bahwa dokumen digital tetap utuh, asli, dan tidak mengalami modifikasi atau manipulasi oleh pihak yang tidak sah
Micro Framework	kerangka kinerja pengembangan *web* berskala minimalis yang memberikan fungsionalitas dasar yang ringan dan fleksibilitas tinggi bagi pengembang
Non-Repudiation	keadaan di mana pihak pengirim data tidak dapat menyangkal bahwa dialah yang mengirim atau

	menandatangani dokumen tersebut karena proteksi kunci privat
Plaintext	data asli atau teks biasa yang belum dienkripsi dan dapat dibaca secara langsung
Private Key	kunci rahasia dalam kriptografi asimetris yang hanya dipegang oleh pemiliknya dan digunakan untuk membuat tanda tangan digital
Public Key	kunci yang disebarkan secara terbuka dalam kriptografi asimetris yang digunakan oleh penerima untuk memverifikasi tanda tangan digital
Server-side	bagian dari aplikasi *web* yang berjalan di komputer server, berfungsi untuk memproses logika bisnis, keamanan, dan manipulasi data

INTISARI

Perkembangan teknologi mendorong peningkatan penggunaan dokumen elektronik seperti PDF untuk keperluan administrasi. Namun, dokumen digital rentan terhadap manipulasi oleh pihak yang tidak berwenang. Penelitian ini bertujuan untuk membangun sistem autentikasi dokumen digital berbasis web bernama "AuthentiC" menggunakan kombinasi algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) dan *Quick Response Code* (QR Code).

Sistem ini dikembangkan menggunakan bahasa pemrograman Python dengan *framework* Flask, serta pustaka PyMuPDF untuk pemrosesan dokumen. Proses penandatanganan dilakukan dengan melakukan *hashing* dokumen menggunakan SHA-256, enkripsi nilai *hash* menggunakan *private key* untuk menghasilkan tanda tangan digital (r, s), dan pengodean informasi tersebut ke dalam format JSON-Base64 sebelum disematkan sebagai QR Code pada dokumen PDF.

Verifikasi dilakukan dengan memindai QR Code melalui perangkat *mobile* atau mengunggah kembali file ke sistem web. Pengujian fungsional dengan *Black-Box Testing* menunjukkan seluruh fitur berjalan sesuai rancangan. Hasil uji integritas membuktikan sistem mampu mendeteksi manipulasi teks atau struktur file secara instan melalui perubahan nilai *hash*. Penelitian ini berhasil membuktikan bahwa integrasi ECDSA dan QR Code memberikan solusi autentikasi dokumen PDF yang praktis, aman, dan efisien secara waktu dan komputasi.

Kata kunci: Sistem Berbasis Web, Dokumen PDF, ECDSA, QR Code, Flask.

ABSTRACT

The development of technology has driven the increasing use of electronic documents such as PDFs for administrative purposes. However, digital documents are highly vulnerable to unauthorized manipulation. This study aims to develop a web-based digital document authentication system named "AuthentiC" using a combination of the Elliptic Curve Digital Signature Algorithm (ECDSA) and Quick Response Code (QR Code).

The system was developed using the Python programming language with the Flask framework, along with the PyMuPDF library for document processing. The signing process involves hashing the document with SHA-256, encrypting the hash value with a private key to generate a digital signature (r, s), and encoding this information into a JSON-Base64 format before embedding it as a QR Code onto the PDF document.

Verification is performed by scanning the QR Code using a mobile device or re-uploading the file to the web system. Functional testing using Black-Box Testing indicates that all features operate according to design. The integrity test results prove that the system can instantly detect any text or file structure manipulation through changes in the hash value. This study successfully demonstrates that the integration of ECDSA and QR Code provides a digital document authentication solution for PDFs that is practical, secure, and computationally efficient.

Keyword: *Web-Based System, PDF Document, ECDSA, QR Code, Flask*