AUTENTIKASI SERTIFIKAT DIGITAL BERBASIS DIGITAL SIGNATURE DENGAN ALGORITMA EdDSA

SKRIPSI

Oleh:

KARINA DESI LIADY
NIM. 221111905
VINCENT STANLEY
NIM. 221110003
WILSON TOVANO
NIM. 221113421

PROGRAM STUDI S-1 TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
UNIVERSITAS MIKROSKIL
MEDAN
2026

DIGITAL CERTIFICATE AUTHENTICATION BASED ON DIGITAL SIGNATURE WITH EdDSA ALGORITHM

UNDERGRADUATE THESIS

By:

KARINA DESI LIADY
NIM. 221111905
VINCENT STANLEY
NIM. 221110003
WILSON TOVANO
NIM. 221113421

UNDERGRADUATE PROGRAM OF COMPUTER SCIENCE
FACULTY OF INFORMATICS
UNIVERSITAS MIKROSKIL
MEDAN

2026

LEMBARAN PENGESAHAN

AUTENTIKASI SERTIFIKAT DIGITAL BERBASIS DIGITAL SIGNATURE DENGAN ALGORITMA EDDSA

SKRIPSI

Diajukan untuk Melengkapi Persyaratan Guna
Mendapatkan Gelar Sarjana
Program Studi S-1 Teknik Informatika

Oleh:

KARINA DESI LIADY
NIM. 221111905
VINCENT STANLEY
NIM. 221110003
WILSON TOVANO
NIM. 221113421

Disetujui Oleh:

Dosen Pembimbing I,

Syanti Irviantina, S.Kom., M.Kom.

Dosen Pembimbing II,

Darwin, S.Kom., M.Kom.

Medan, 23 Juli 2026
Diketahui dan Disahkan Oleh:

Ketua Program Studi
S-1 Teknik Informatika,

Carles Juliandy, S.Kom., M.Kom.

HALAMAN PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Program Studi S-1 Teknik Informatika Universitas Mikroskil Medan dengan identitas mahasiswa sebagai berikut:
Nama : Karina Desi Liady
NIM : 221111905

Saya telah melaksanakan penelitian dan penulisan Skripsi dengan judul dan tempat penelitian sebagai berikut:
Judul Skripsi : AUTENTIKASI SERTIFIKAT DIGITAL BERBASIS DIGITAL SIGNATURE DENGAN ALGORITMA EDDSA
Tempat Penelitian : Universitas Mikroskil
Alamat Tempat Penelitian : Jl. Thamrin No. 140, Medan
No. Telp. Tempat Penelitian : (061) 4573767

Sehubungan dengan Skripsi tersebut, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Skripsi tersebut merupakan hasil karya saya sendiri (tidak menyuruh orang lain yang mengerjakannya) dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar. Bila di kemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya (membuatnya), maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh Universitas Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Universitas Mikroskil Medan Hak Bebas Royalti Non-eksklusif (Non-exclusive Royalty Free Right) atas Skripsi saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, Universitas Mikroskil Medan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangakalan data (database), merawat, dan mempublikasikan Skripsi saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja dalam bentuk format tercetak dan/atau elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebaga pemilk hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Skripsi saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak/sistem informasi.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 7 Juli 2026
Saya yang membuat pernyataan,

Karina Desi Liady

HALAMAN PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Program Studi S-1 Teknik Informatika Universitas Mikroskil Medan dengan identitas mahasiswa sebagai berikut:
Nama : Vincent Stanley
NIM : 221110003

Saya tela melaksanakan penelitian dan penulisan Skripsi dengan judul dan tempat penelitian sebagai berikut:

Judul Skripsi	: AUTENTIKASI SERTIFIKAT DIGITAL BERBASIS DIGITAL SIGNATURE DENGAN ALGORITMA EDDSA
Tempat Penelitian	: Universitas Mikroskil
Alamat Tempat Penelitian	: Jl. Thamrin No. 140, Medan
No. Telp. Tempat Penelitian	: (061) 4573767

Sehubungan dengan Skripsi tersebut, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Skripsi tersebut merupakan hasil karya saya sendiri (tidak menyuruh orang lain yang mengerjakannya) dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar. Bila di kemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya (membuatnya), maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh Universitas Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Universitas Mikroskil Medan Hak Bebas Royalti Non-eksklusif (Non-exclusive Royalty Free Right) atas Skripsi saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, Universitas Mikroskil Medan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangakalan data (database), merawat, dan mempublikasikan Skripsi saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja dalam bentuk format tercetak dan/atau elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebaga pemilk hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Skripsi saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak/sistem informasi.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 7. Juli 2026
Saya yang membuat pernyataan,

Vincent Stanley

HALAMAN PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Program Studi S-1 Teknik Informatika Universitas Mikroskil Medan dengan identitas mahasiswa sebagai berikut:
Nama : Wilson Tovano
NIM : 221113421

Saya telah melaksanakan penelitian dan penulisan Skripsi dengan judul dan tempat penelitian sebagai berikut:
Judul Skripsi : AUTENTIKASI SERTIFIKAT DIGITAL BERBASIS DIGITAL SIGNATURE DENGAN ALGORITMA EDDSA
Tempat Penelitian : Universitas Mikroskil
Alamat Tempat Penelitian : Jl. Thamrin No. 140, Medan
No. Telp. Tempat Penelitian : (061) 4573767

Sehubungan dengan Skripsi tersebut, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Skripsi tersebut merupakan hasil karya saya sendiri (tidak menyuruh orang lain yang mengerjakannya) dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar. Bila di kemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya (membuatnya), maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh Universitas Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Universitas Mikroskil Medan Hak Bebas Royalti Non-eksklusif (Non-exclusive Royalty Free Right) atas Skripsi saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, Universitas Mikroskil Medan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangakalan data (database), merawat, dan mempublikasikan Skripsi saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja dalam bentuk format tercetak dan/atau elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebaga pemilk hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Skripsi saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak/sistem informasi.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 7 Juli 2026
Saya yang membuat pernyataan,

Wilson Tovano

AUTENTIKASI SERTIFIKAT DIGITAL BERBASIS DIGITAL SIGNATURE DENGAN ALGORITMA EdDSA

Abstrak

Sertifikat digital semakin banyak digunakan sebagai bukti kompetensi dan kualifikasi individu di era digital, namun penggunaannya menghadapi tantangan berupa pemalsuan dan manipulasi data oleh pihak yang tidak berwenang. Sistem autentikasi konvensional yang mengandalkan kode QR berisi tautan ke situs web verifikasi eksternal juga rentan terhadap serangan phishing dan pengalihan ke situs palsu. Penelitian ini bertujuan mengembangkan sistem autentikasi sertifikat digital berbasis digital signature menggunakan algoritma Edwards-curve Digital Signature Algorithm (EdDSA) varian Ed25519, di mana informasi kriptografi disimpan langsung dalam kode QR sehingga proses verifikasi digital signature tidak bergantung pada situs web verifikasi eksternal. Proses autentikasi memanfaatkan Optical Character Recognition (OCR) untuk mengekstraksi teks sertifikat sebagai basis data penandatanganan dan verifikasi. Tanda tangan digital kemudian disematkan ke dalam kode QR bersama kunci publik. Pengujian menggunakan metode blackbox testing menunjukkan bahwa sistem dapat menjalankan seluruh fungsionalitas sesuai kebutuhan. Hasil penelitian menunjukkan bahwa sistem berhasil mendeteksi modifikasi teks, modifikasi kode QR, dan status pencabutan sertifikat dengan waktu pembuatan sertifikat rata-rata 7,08 detik dan verifikasi 4,52 detik. Proses penandatanganan Ed25519 membutuhkan waktu 0,92 milidetik.

Kata kunci: *sertifikat digital, tanda tangan digital, EdDSA, kode QR, OCR*

Abstract

Digital certificates are increasingly utilized as evidence of individual competence and qualifications in the digital era; however, their implementation faces critical challenges regarding data forgery and unauthorized manipulation. Conventional authentication systems relying on QR codes that link to external verification websites are highly vulnerable to phishing attacks and fraudulent redirections. This study aims to develop a self-contained digital certificate authentication system based on digital signatures using the Ed25519 variant of the Edwards-curve Digital Signature Algorithm (EdDSA). By embedding the cryptographic information directly into the QR code, the digital signature verification process eliminates any dependency on external verification websites. The authentication process utilizes Optical Character Recognition (OCR) to extract certificate text as the baseline data for signing and verification. The generated digital signature is then embedded into the QR code alongside the public key. Functional evaluation conducted via black-box testing demonstrates that the system completely satisfies all operational requirements. The empirical results show that the system successfully detects text modifications, QR code tampering, and certificate revocation status, achieving an average certificate generation time of 7.08 seconds and a verification time of 4.52 seconds. Furthermore, the Ed25519 signing process requires a remarkably low computational time of only 0.92 milliseconds.

Keywords: *digital certificate, digital signature, EdDSA, QR code, OCR*

KATA PENGANTAR

Ucapan syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas segala berkat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul "AUTENTIKASI SERTIFIKAT DIGITAL BERBASIS DIGITAL SIGNATURE DENGAN ALGORITMA EdDSA".

Skripsi ini disusun untuk memenuhi salah satu persyaratan dalam menyelesaikan pendidikan Strata Satu (S-1) pada Program Studi Teknik Informatika, Universitas Mikroskil Medan.

Penulis menyadari bahwa penyusunan skripsi ini tidak terlepas dari bantuan, bimbingan, dukungan, serta doa dari berbagai pihak. Oleh karena itu, pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Ibu Syanti Irviantina, S.Kom., M.Kom. selaku Dosen Pembimbing I yang telah memberikan arahan, masukan, dan bimbingan selama penulisan Skripsi ini.
2. Bapak Darwin, S.Kom., M.Kom. selaku Dosen Pembimbing II yang telah memberikan arahan, masukan, dan bimbingan selama penulisan Skripsi ini.
3. Bapak Hardy, S.Kom., M.Sc., Ph.D., selaku Rektor Universitas Mikroskil Medan.
4. Bapak Sunaryo Winardi, S.Kom., M.T., selaku Dekan Fakultas Informatika Universitas Mikroskil Medan.
5. Bapak Carles Juliandy, S.Kom., M.Kom., selaku Ketua Program Studi S-1 Teknik Informatika Fakultas Informatika Universitas Mikroskil Medan.
6. Orang tua dan keluarga serta seluruh pihak yang telah memberikan doa, dukungan dan motiva selama masa studi hingga penyusunan skripsi ini dapat diselesaikan.

Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi penyempurnaan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat bagi pembaca dan pihak-pihak yang membutuhkan.

Medan, 07 Juli 2026

Penulis,

Karina Desi Liady

Vincent Stanley

Wilson Tovano

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL