

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

Schubungan 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 pangkalan 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 pemilik 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 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 pangkalan 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 pemilik 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 Tavano

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 pangkalan 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 sebagai pemilik 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 Tavano

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 motivasi 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 Tavano

DAFTAR ISI

Abstrak	i
KATA PENGANTAR	ii
DAFTAR ISI	iii
DAFTAR GAMBAR	v
DAFTAR TABEL	viii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan	2
1.4 Manfaat	3
1.5 Ruang Lingkup.....	3
BAB II KAJIAN LITERATUR	4
2.1 Sertifikat.....	4
2.2 Kriptografi.....	4
2.2.1 Kriptografi Simetris	5
2.2.2 Kriptografi Asimetris.....	6
2.2.3 <i>Hashing</i>	7
2.2.4 <i>Digital Signature</i>	8
2.2.5 Elliptic Curve Cryptography (ECC)	10
2.2.6 Edwards-curve Digital Signature Algorithm (EdDSA).....	13
2.2.7 Kurva Edwards	14
2.2.8 Ed25519.....	15
2.2.9 <i>Key Generation</i>	18
2.2.10 <i>Signing</i>	19
2.2.11 <i>Verification</i>	20
2.2.12 Perbandingan EdDSA dengan Algoritma-Algoritma <i>Digital Signature</i> Lain... 21	
2.3 Kode QR	23
2.4 Optical Character Recognition (OCR)	27
2.5 Penerapan <i>Digital Signature</i> dalam Kode QR pada Aplikasi Autentikasi Sertifikat Digital.....	28
2.6 Metode Waterfall	30
BAB III TAHAPAN PELAKSANAAN	32
3.1 Analisis.....	33
3.1.1 Analisis Proses Sistem.....	34

3.1.2 Analisis Kebutuhan Fungsional.....	63
3.1.3 Analisis Kebutuhan Non-Fungsional	71
3.2 Perancangan	72
3.2.1 Perancangan Tampilan	72
3.2.2 Perancangan Basis Data	89
BAB IV HASIL DAN PEMBAHASAN	93
4.1 Hasil	93
4.1.1 Implementasi Sistem	93
4.1.2 Hasil Implementasi Antarmuka	93
4.1.3 Hasil Pengujian Fungsionalitas	104
4.1.4 Hasil Pengujian Pembangkitan Kunci dan Penandatanganan EdDSA	110
4.1.5 Hasil Pengujian Verifikasi Sertifikat	111
4.2 Pembahasan.....	114
4.2.1 Analisis Kinerja Sistem.....	115
4.2.2 Analisis Peran OCR (Optical Character Recognition)	117
4.2.3 Efisiensi Penyimpanan <i>Public Key</i> dalam Kode QR.....	118
4.2.4 Efektivitas Penerapan Algoritma EdDSA dalam Sistem.....	120
4.2.5 Pengaruh Tampilan Visual Sertifikat Digital terhadap Sistem.....	121
BAB V PENUTUP	123
5.1 Kesimpulan	123
5.2 Saran.....	123
DAFTAR PUSTAKA.....	124
DAFTAR RIWAYAT HIDUP	129

DAFTAR GAMBAR

Gambar 2. 1 Kategori Kriptografi	5
Gambar 2. 2 Skema Kriptografi Simetris	6
Gambar 2. 3 Skema Kriptografi Asimetris	7
Gambar 2. 4 Visualisai Proses <i>Hashing</i>	8
Gambar 2. 5 Skema <i>Digital signature</i>	9
Gambar 2. 6 Bentuk-Bentuk Kurva Eliptik	10
Gambar 2. 7 Bentuk Kurva Eliptik Persamaan $y^2 = x^3 + ax + b$	11
Gambar 2. 8 Proses Penjumlahan Titik	12
Gambar 2. 9 Bentuk <i>Edwards Curves</i> dengan Persamaan Matematika	14
Gambar 2. 10 Contoh Kode QR	23
Gambar 2. 11 Alur Proses Kode QR	24
Gambar 2. 12 Versi-Versi Kode QR.....	25
Gambar 2. 13 Bagian-Bagian Kode QR	26
Gambar 2. 14 Alur Proses OCR	28
Gambar 3. 1 (a) Alur Penelitian Utama (b) Metode Waterfall	32
Gambar 3. 2 (a) Proses <i>Signing</i> Sertifikat (b) Proses <i>Verifying</i> Sertifikat.....	34
Gambar 3. 3 Alur OCR.....	35
Gambar 3. 4 Contoh Masukan Sertifikat	35
Gambar 3. 5 Pra-Pemrosesan Gambar	36
Gambar 3. 6 Proses Deteksi Area Teks di Sertifikat	36
Gambar 3. 7 Contoh Isi Teks Sertifikat	37
Gambar 3. 8 Alur SHA-512.....	38
Gambar 3. 9 Alur per Blok SHA-512 [64]	38
Gambar 3. 10 Alur <i>Message Scheduling Expansion</i> [64].....	40
Gambar 3. 11 Alur <i>Message Schedule & Compression Loop</i> [64].....	47
Gambar 3. 12 Tahapan Memperbarui Nilai <i>Words</i> [64].....	47
Gambar 3. 13 80 Konstanta SHA-512 dalam Heksadesimal [65]	48
Gambar 3. 14 Nilai Pada Variabel- Variabel W_0	52
Gambar 3. 15 Nilai Pada Variabel- Variabel $W_1 - W_5$	53
Gambar 3. 16 Nilai Pada Variabel- Variabel W_{79}	53
Gambar 3. 17 Nilai Variabel- Variabel Awal Sebelum <i>Update</i>	54
Gambar 3. 18 Nilai Variabel- Variabel Awal Setelah <i>Update</i> Penjumlahan $\text{mod } 2^{64}$	54

Gambar 3. 19 Nilai Variabel- Variabel Awal Setelah <i>Update</i> dalam Heksadesimal	55
Gambar 3. 20 Alur <i>Key Generation</i> EdDSA	56
Gambar 3. 21 Alur <i>Signing</i> EdDSA	57
Gambar 3. 22 Alur <i>Encoding</i> Kode QR.....	59
Gambar 3. 23 Hasil <i>Encode</i> Kode QR.....	59
Gambar 3. 24 Hasil Keluaran Sertifikat dengan Kode QR <i>Digital Signature</i>	60
Gambar 3. 25 Alur <i>Decoding</i> Kode QR	61
Gambar 3. 26 Hasil <i>Decode</i> Kode QR.....	61
Gambar 3. 27 Alur <i>Verifying</i> EdDSA.....	62
Gambar 3. 28 <i>Use Case Diagram</i>	63
Gambar 3. 29 Tampilan Perancangan Halaman Beranda Publik	73
Gambar 3. 30 Tampilan Perancangan Halaman <i>Login</i>	74
Gambar 3. 31 Tampilan Perancangan Halaman Beranda Admin	75
Gambar 3. 32 Tampilan Perancangan Halaman “Kelola Peserta”	76
Gambar 3. 33 Tampilan Perancangan Dialog Tambah Peserta	77
Gambar 3. 34 Tampilan Perancangan Dialog Ubah Data Peserta	78
Gambar 3. 35 Tampilan Perancangan Dialog Hapus Peserta	79
Gambar 3. 36 Tampilan Perancangan Halaman “Buat Sertifikat”	80
Gambar 3. 37 Tampilan Perancangan Halaman “Buat Sertifikat” Setelah Gambar Diunggah	81
Gambar 3. 38 Tampilan Perancangan Halaman “Sertifikat Berhasil Dibuat”	82
Gambar 3. 39 Tampilan Perancangan Halaman “Daftar Sertifikat”	83
Gambar 3. 40 Tampilan Perancangan Dialog Cabut Sertifikat	84
Gambar 3. 41 Tampilan Perancangan Halaman “Beranda Peserta”	85
Gambar 3. 42 Tampilan Perancangan “Halaman Sertifikat Saya”	86
Gambar 3. 43 Tampilan Perancangan Halaman “Detail Sertifikat Peserta”	87
Gambar 3. 44 Tampilan Perancangan Halaman “Verifikasi Sertifikat”	88
Gambar 3. 45 Tampilan Perancangan Halaman Hasil Verifikasi Sertifikat	89
Gambar 3. 46 <i>Entity Relationship Diagram</i>	90
Gambar 4. 1 Tampilan Halaman Beranda Publik	94
Gambar 4. 2 Tampilan Halaman <i>Login</i>	94
Gambar 4. 3 Tampilan Halaman Beranda Admin	95
Gambar 4. 4 Tampilan Halaman Kelola Peserta	95
Gambar 4. 5 Tampilan Halaman Dialog Tambah Peserta	96

Gambar 4. 6 Tampilan Halaman Dialog Ubah Data Peserta	97
Gambar 4. 7 Tampilan Halaman Dialog Hapus Peserta	97
Gambar 4. 8 Tampilan Halaman Buat Sertifikat	98
Gambar 4. 9 Tampilan Halaman Buat Sertifikat Setelah Gambar Diunggah.....	99
Gambar 4. 10 Tampilan Halaman Sertifikat Berhasil Dibuat.....	100
Gambar 4. 11 Tampilan Halaman Daftar Sertifikat Semua Peserta	100
Gambar 4. 12 Tampilan Halaman Dialog Cabut Sertifikat	101
Gambar 4. 13 Tampilan Halaman Beranda Peserta	101
Gambar 4. 14 Tampilan Halaman Sertifikat Saya	102
Gambar 4. 15 Tampilan Halaman Detail Sertifikat Peserta	102
Gambar 4. 16 Tampilan Halaman Verifikasi Sertifikat	103
Gambar 4. 17 Tampilan Halaman Hasil Verifikasi Sertifikat	104
Gambar 4. 18 Hasil Pembangkitan Kunci	110
Gambar 4. 19 Hasil <i>Digital signature</i>	110
Gambar 4. 20 Isi kode QR	111
Gambar 4. 21 Status Sertifikat Digital Valid dan Terdaftar	112
Gambar 4. 22 Status Sertifikat Tidak Valid Telah Dimodifikasi	113
Gambar 4. 23 Status Sertifikat Format QR Tidak Valid	113
Gambar 4. 24 Status Sertifikat Telah Dicabut	114

DAFTAR TABEL

Tabel 2. 1 Parameter-Parameter Utama dalam Ed25519	15
Tabel 2. 2 Performa Algoritma <i>Digital signature</i> untuk Tingkat Keamanan 128-bit	21
Tabel 2. 3 Performa Algoritma <i>Digital signature</i> untuk Tingkat Keamanan 192-bit	22
Tabel 2. 4 Performa Algoritma <i>Digital signature</i> untuk Tingkat Keamanan 256-bit	22
Tabel 3. 1 <i>Fixed Initial Values</i> (IV).....	39
Tabel 3. 2 Daftar W_0 hingga W_{15} untuk Masukan “abc”	40
Tabel 3. 3 Daftar W_0 hingga W_{79} untuk Masukan “abc”	42
Tabel 3. 4 Peran Aktor pada <i>Use Case Diagram</i>	63
Tabel 3. 5 Deskripsi <i>Use Case</i>	64
Tabel 3. 6 Skenario <i>Use Case</i> : Melakukan <i>Login</i>	64
Tabel 3. 7 Skenario <i>Use Case</i> : Mengelola Data Peserta	65
Tabel 3. 8 Skenario <i>Use Case</i> : Membuat Sertifikat	66
Tabel 3. 9 Skenario <i>Use Case</i> : Melihat Sertifikat Peserta	68
Tabel 3. 10 Skenario <i>Use Case</i> : Mencabut Sertifikat Peserta	69
Tabel 3. 11 Skenario <i>Use Case</i> : Melihat Detail Sertifikat	70
Tabel 3. 12 Skenario <i>Use Case</i> : Memverifikasi sertifikat	70
Tabel 3. 13 Tabel <i>PIECES</i>	72
Tabel 3. 14 Tabel <i>Users</i>	90
Tabel 3. 15 Tabel <i>Certificate</i>	91
Tabel 3. 16 Tabel <i>VerificationLog</i>	92
Tabel 4. 1 Tabel Hasil Pengujian Menu <i>Login</i>	104
Tabel 4. 2 Tabel Hasil Pengujian Menu Mengelola Peserta	105
Tabel 4. 3 Tabel Hasil Pengujian Menu Pembuatan Sertifikat	107
Tabel 4. 4 Tabel Hasil Pengujian Menu Mengelola Sertifikat Peserta	108
Tabel 4. 5 Tabel Hasil Pengujian Menu Mengakses Daftar Sertifikat Peserta	109
Tabel 4. 6 Tabel Hasil Pengujian Menu Verifikasi Sertifikat Digital	109
Tabel 4. 7 Metrik Durasi Waktu Komputasi Pembuatan Sertifikat	115
Tabel 4. 8 Metrik Durasi Waktu Komputasi Verifikasi Sertifikat	116