PERANCANGAN PROTOKOL *SELF-SOVEREIGN IDENTITY* UNTUK AUTENTIKASI SISTEM LAYANAN KAMPUS PADA STT TERPADU NURUL FIKRI

Yudha Rizky Alvingky[1], Yaasir Aidil Fitrah[2], Salman El Farisi[3]
Program Studi Teknik Informatika,
Sekolah Tinggi Teknologi Terpadu Nurul Fikri[1,2,3]
Jl. Setu Indah No.116, Tugu, Kec. Cimanggis, Kota Depok, Jawa Barat
riskyyudha678@gmail.com[1], yaasiraidilfitrah@gmail.com[2], salman@nurulfikri.ac.id[3]

Abstrak

Sistem autentikasi layanan kampus di sebagian besar perguruan tinggi masih mengandalkan kata sandi yang rentan terhadap kebocoran data dan serangan siber. *Self-Sovereign Identity* (SSI) hadir sebagai paradigma identitas digital yang memberikan kendali penuh kepada pengguna, namun implementasinya umumnya masih bergantung pada infrastruktur *blockchain* yang kompleks. Penelitian ini bertujuan merancang protokol autentikasi berbasis SSI tanpa *blockchain* untuk sistem layanan kampus di STT Terpadu Nurul Fikri. Metode penelitian yang digunakan adalah pendekatan rekayasa dengan tahapan meliputi studi literatur, perancangan arsitektur, pengembangan prototipe, dan evaluasi melalui pengujian fungsional, pengujian kinerja, serta *User Acceptance Testing* (UAT). Arsitektur yang dirancang menggunakan metode *did:web* untuk identitas digital kampus, did:key untuk identitas pengguna, serta protokol SIOPv2 dan OID4VP untuk autentikasi. Hasil pengujian fungsional menunjukkan seluruh skenario berhasil dijalankan. Pengujian kinerja menunjukkan rata-rata waktu pembuatan VC 384 ms, resolusi did.json 404 ms, dan *login* SIOPv2 112 ms, yang lebih cepat dibandingkan pendekatan berbasis *blockchain*. Hasil UAT melalui demonstrasi kepada mitra menunjukkan sistem dinilai mudah digunakan dan layak diterapkan.

Kata kunci: *decentralized identifier*, *self-sovereign identity*, SIOPv2, *verifiable credential*, autentikasi tanpa kata sandi

Abstract

Campus service authentication systems in most universities still rely on passwords that are vulnerable to data breaches and cyber attacks. Self-Sovereign Identity (SSI) emerges as a digital identity paradigm that gives users full control, yet its implementation generally depends on complex blockchain infrastructure. This study aims to design a blockchain-free SSI-based authentication protocol for campus service systems at STT Terpadu Nurul Fikri. The research employs an engineering approach with stages including literature study, architecture design, prototype development, and evaluation through functional testing, performance testing, and User Acceptance Testing (UAT). The designed architecture uses the did:web method for campus digital identity, did:key for user identity, and SIOPv2 and OID4VP protocols for authentication. Functional testing results show all scenarios passed. Performance testing shows average VC creation time of 384 ms, did.json resolution of 404 ms, and SIOPv2 login of 112 ms, which is faster than blockchain-based approaches. UAT results through demonstration to partners indicate the system is considered easy to use and feasible to implement.

Keywords*: decentralized identifier, self-sovereign identity, SIOPv2, verifiable credential, passwordless authentication*

PENDAHULUAN

Sistem layanan kampus di sebagian besar perguruan tinggi masih mengandalkan arsitektur autentikasi terpusat yang menyimpan data pengguna dalam satu basis data sehingga menimbulkan risiko *Single Point of Failure* (SPOF) yang rentan terhadap serangan siber maupun kegagalan teknis (Goel & Rahulamathavan, 2024). Beberapa insiden kebocoran data mahasiswa di perguruan tinggi Indonesia dalam beberapa tahun terakhir (Kemendikdasmen, 2024; Tempo.co, 2024) serta kebiasaan penggunaan ulang kata sandi (IBM Security, 2021) memperkuat urgensi perbaikan sistem autentikasi. Konsep *Self-Sovereign Identity* (SSI) hadir sebagai paradigma baru yang memberikan kendali penuh kepada pengguna atas data identitasnya tanpa bergantung pada otoritas pusat (Schardong & Custódio, 2022), namun implementasi SSI yang ada umumnya masih bertumpu pada infrastruktur *blockchain* yang kompleks dan mahal. Penelitian ini bertujuan merancang protokol

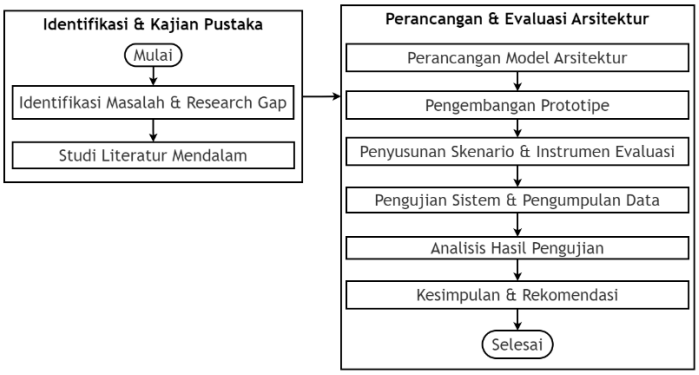
autentikasi berbasis SSI tanpa *blockchain* yang sesuai dengan karakteristik sistem layanan kampus di STT Terpadu Nurul Fikri. Rumusan masalah dalam penelitian ini adalah pertama, protokol SSI manakah yang paling sesuai dengan kebutuhan autentikasi sistem layanan kampus, dan kedua, bagaimana merancang arsitektur autentikasi berbasis protokol SSI terpilih. Tujuan penelitian ini adalah mengidentifikasi dan memilih protokol SSI yang sesuai serta merancang arsitektur autentikasi berbasis protokol tersebut. Manfaat penelitian ini secara teoretis adalah memperkaya kajian manajemen identitas digital di lingkungan pendidikan, sedangkan secara praktis memberikan acuan teknis bagi institusi yang ingin menerapkan autentikasi tanpa kata sandi serta mendukung kendali pengguna atas kredensial akademiknya melalui dompet digital.

PENELITIAN RELEVAN

Penelitian tentang *Self-Sovereign Identity* (SSI) di lingkungan pendidikan dapat dikelompokkan menjadi tiga pendekatan. Pendekatan pertama membangun sistem identitas mandiri yang sama sekali baru seperti Sovrin (Windley, 2021), CanDID (Maram dkk., 2021), dan SIBERIA (Paredes-García dkk., 2025), namun ketiganya tidak dapat terhubung dengan sistem autentikasi kampus yang sudah ada. Pendekatan kedua mencoba menjembatani sistem lama dengan SSI seperti yang dilakukan pada proyek EBSI (Tan dkk., 2023), pengembangan protocol OIDC4VC (De Prisco dkk., 2024), dan pengamanan sistem autentikasi menggunakan NFT (Yousra dkk., 2023), tetapi semuanya masih memerlukan teknologi *blockchain* yang rumit dan mahal. Pendekatan ketiga berfokus pada penerbitan kredensial akademik digital seperti DAVE-CC (Tran dkk., 2025), platform sertifikat digital (Stefan-Robert & Butincu, 2024), dan sistem manajemen kredensial mahasiswa (Mansoori & Maheshwari, 2022) yang juga masih bergantung pada *blockchain*. Penelitian ini menawarkan solusi yang berbeda karena tidak menggunakan *blockchain* maupun protokol tambahan lainnya, melainkan memanfaatkan protokol standar SIOPv2 dan OID4VP yang dapat berjalan di server web kampus yang sudah tersedia.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan rekayasa yang bertujuan merancang arsitektur autentikasi berbasis *Self-Sovereign Identity* (SSI) untuk sistem layanan kampus di STT Terpadu Nurul Fikri. Pendekatan ini dipilih karena penelitian berorientasi pada hasil berupa rancangan teknis, bukan pengujian hipotesis. Penelitian mengasumsikan bahwa kampus telah memiliki infrastruktur web yang memadai serta pengguna memiliki perangkat seluler untuk menjalankan dompet digital. Tahapan penelitian terbagi ke dalam dua kelompok utama sebagaimana diilustrasikan pada Gambar 1.



Gambar 1. Tahapan Penelitian

Kelompok pertama adalah identifikasi dan kajian pustaka. Tahap ini mencakup pengenalan masalah pada sistem autentikasi kampus yang masih bergantung pada kata sandi, serta mempelajari berbagai konsep seperti identitas digital mandiri (SSI), pengenal identitas terdesentralisasi (*Decentralized Identifier*/DID), kredensial digital yang dapat diverifikasi (*Verifiable Credential*/VC), dan protokol autentikasi terkait. Sumber yang digunakan berasal dari dokumen standar internasional, jurnal ilmiah, dan buku teks kriptografi.

Kelompok kedua adalah perancangan dan evaluasi arsitektur. Perancangan mencakup identifikasi tiga entitas utama, yaitu penerbit (*Issuer*), pemegang (*Holder*), dan pemeriksa (*Verifier*), serta alur penerbitan dan penggunaan kredensial. Berdasarkan rancangan tersebut, dikembangkan prototipe sebagai implementasi awal untuk menguji kelayakan teknis. Setelah prototipe tersedia, disusun skenario evaluasi yang mencakup tiga aspek pengujian sebagaimana dirangkum pada Tabel 1.

Tabel 1. Skenario Pengujian Protokol SSI

No	Komponen Protokol	Aspek yang Diuji
1	Pembuatan VC: *Issuer* mengisi data dan menekan *Create VC*	Fungsional: VC terbit dan QR muncul; Kinerja: waktu pembuatan VC; UAT: kemudahan input
2	Penyimpanan VC: *Holder* memindai QR dan menyimpan VC	Fungsional: QR terbaca dan VC tersimpan; Kinerja: waktu resolusi did.json; UAT: kemudahan *scan* dan simpan
3	Autentikasi SIOPv2: Simulasi permintaan *login* ke *backend*	Fungsional: backend merespons sesuai standar; Kinerja: waktu *login*; UAT: dijelaskan secara konseptual

Pengumpulan data dilakukan melalui tiga cara, yaitu studi literatur, observasi terhadap sistem layanan kampus yang sudah berjalan, dan pengujian kinerja protokol menggunakan skrip otomatisasi. Pengujian kinerja mengukur waktu pembuatan VC, waktu resolusi did.json, dan waktu login SIOPv2 pada server pengujian.

Metode pengujian menggunakan pendekatan *Black Box Testing* untuk aspek fungsional, pengukuran waktu respons untuk aspek kinerja, dan *User Acceptance Testing* (UAT) melalui demonstrasi kepada mitra LTSI untuk aspek penerimaan pengguna. Skenario 1 dan 2 didemonstrasikan langsung, sedangkan skenario 3 dijelaskan secara konseptual karena dompet digital belum mendukung fitur autentikasi SIOPv2 secara penuh.

Analisis data dilakukan dalam tiga aspek. Pertama, analisis fungsional dengan membandingkan hasil aktual terhadap hasil yang diharapkan. Kedua, analisis kinerja secara deskriptif dengan menghitung rata-rata, nilai minimum, dan nilai maksimum dari setiap parameter yang diukur. Ketiga, analisis UAT dengan merangkum tanggapan mitra untuk menentukan kelayakan sistem.

HASIL DAN PEMBAHASAN

Analisis Kebutuhan Kredensial

Sebelum merancang arsitektur autentikasi, dilakukan observasi terhadap sistem layanan kampus STT Terpadu Nurul Fikri untuk mengidentifikasi jenis pengguna, kebutuhan atribut kredensial, serta variasi peran. Hasil observasi menunjukkan keberadaan tiga peran utama, yaitu mahasiswa, dosen, dan staf administrasi. Seluruh peran tersebut memerlukan kredensial digital dengan spesifikasi yang berbeda sebagaimana dirangkum pada Tabel 2.

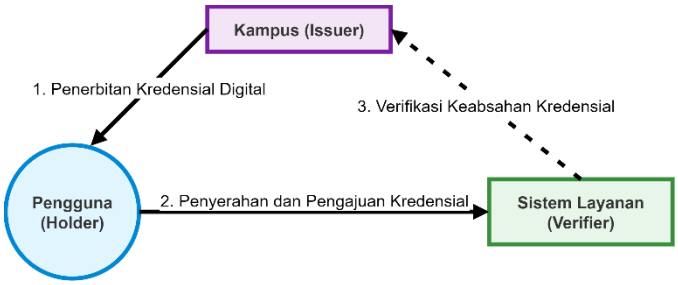
Tabel 2. Analisis Kebutuhan Atribut Kredensial Pengguna

No	Atribut	Kebutuhan	Sifat
1	name	Identitas fundamental untuk seluruh pengguna	Wajib
2	faculty	Membedakan unit kerja dosen atau program studi mahasiswa	Kondisional
3	angkatan	Mengidentifikasi tahun masuk akademik mahasiswa	Kondisional
4	id_number	Pengenal unik administratif seperti NIM atau NIP	Wajib
5	role	Penentu jenis kredensial pengguna (mahasiswa, dosen, staf)	Wajib

Tabel 2 menunjukkan bahwa atribut nama, id_number, dan role merupakan komponen esensial yang bersifat wajib bagi seluruh tipe pengguna. Sementara itu, atribut faculty dan angkatan bersifat kontekstual dan diterapkan secara dinamis sesuai profil pengguna. Variasi kebutuhan ini menuntut perancangan arsitektur *Self-Sovereign Identity* (SSI) yang fleksibel, sehingga sistem mampu mengakomodasi perluasan atribut tanpa merombak struktur dasar *Verifiable Credential* (VC).

Model Arsitektur Kredensial

Merujuk pada analisis kebutuhan kredensial, arsitektur yang dirancang menghubungkan tiga entitas utama, yaitu Kampus, Pengguna, dan Sistem Layanan, sebagaimana diilustrasikan pada Gambar 2.



Gambar 2. Representasi Arsitektur Kredensial Berbasis *Trust Triangle*

Dalam konteks teknis SSI, Kampus berperan sebagai penerbit (*Issuer*) yang menerbitkan kredensial digital. Mahasiswa, dosen, dan staf bertindak sebagai pemegang (*Holder*) yang menyimpan kredensial di dalam dompet digital pada perangkat seluler masing-masing. Sistem layanan, seperti portal akademik atau aplikasi internal, berperan sebagai pemeriksa (*Verifier*) yang memeriksa keaslian kredensial sebelum memberikan akses.

Gambar 2 memperlihatkan alur kerja arsitektur yang berlangsung dalam tiga tahapan interaksi utama. Pertama, pada proses penerbitan, *Issuer* memverifikasi data pengguna secara administratif dan menghasilkan VC yang ditandatangani secara kriptografis. Kredensial ini memuat atribut spesifik pengguna yang formatnya telah disesuaikan dengan analisis kebutuhan pada Tabel 2. Kedua, pada alur pengajuan kredensial, *Holder* menyerahkan kredensial dari dompet digital kepada *Verifier* saat meminta akses layanan. Ketiga, pada fase pembuktian, *Verifier* memvalidasi keaslian dokumen melalui pemeriksaan tanda tangan digital yang melekat pada VC. Garis putus-putus pada Gambar 2 mengindikasikan bahwa *Verifier* dapat memverifikasi kredensial secara mandiri hanya dengan menggunakan kunci publik yang diperoleh dari server web kampus, tanpa perlu menghubungi server *Issuer*.

Perancangan Identitas Digital Kampus

Berdasarkan model Trust Triangle, kampus berperan sebagai penerbit yang wajib memiliki identitas digital yang sah terlebih dahulu agar kredensial yang diterbitkan dapat dipercaya. Penelitian ini mengadopsi metode did:web untuk identitas institusi (Gribneau dkk., 2026). Pendekatan ini dipilih karena dokumen *Decentralized Identifier* (DID) dapat dikelola secara mandiri melalui infrastruktur server web aman (HTTPS) kampus yang telah ada. Secara teknis, server kampus cukup menempatkan berkas ‘did.json’ pada jalur ‘/.well-known/did.json’. Verifier nantinya memperoleh dokumen ini melalui proses resolusi DID dengan format ‘did:web:domain.ac.id’. Proses penyiapan identitas digital kampus diuraikan pada Algoritma 1.

Algoritma 1. Proses Penyiapan DID Kampus

```
INPUT  : Elliptic Curve P-256
OUTPUT : Berkas did.json di server kampus

BEGIN
1. Menghasilkan pasangan kunci (key pair) EC P-256
2. Menyimpan kunci privat secara aman di server
3. Menyusun dokumen DID dengan properti: id, verificationMethod,
   authentication, assertionMethod, capabilityInvocation,
   capabilityDelegation, service
4. Menyimpan sebagai berkas did.json
5. Mengunggah ke direktori /.well-known/did.json
END
```

Struktur dokumen DID disajikan pada Tabel 3.

Tabel 3. Struktur *DID Document* Kampus

Properti	Fungsi
Id	Identitas unik kampus dalam format did:web
VerificationMethod	Menyimpan kunci publik untuk verifikasi tanda tangan digital
Authentication	Autentikasi identitas pengontrol DID
AssertionMethod	Otorisasi penandatanganan VC
CapabilityInvocation	Otorisasi pemanggilan kapabilitas DID

CapabilityDelegation	Mendukung delegasi kapabilitas ke pihak lain
Service	Titik akhir yang menghubungkan DID dengan layanan kampus

Berdasarkan Tabel 3, parameter authentication, assertionMethod, capabilityInvocation, dan capabilityDelegation direferensikan menggunakan DID URL yang mengarah pada kunci publik yang sama. Melalui desain ini, satu kunci publik dapat digunakan secara efisien untuk berbagai mekanisme verifikasi. Penyusunan dokumen ini mengikuti standar W3C DIDs v1.0 (Sporny dkk., 2022), dengan representasi kunci publik merujuk pada standar *JSON Web Key* (RFC 7517).

Perancangan Identitas Digital Pengguna

Setelah kampus memiliki identitas digital sebagai penerbit, tahapan selanjutnya adalah penyediaan identitas bagi pengguna. Dalam arsitektur SSI, pengguna seperti mahasiswa, dosen, dan staf bertindak sebagai pemegang (*Holder*) yang menyimpan dan mengelola kredensial dari penerbit. Penelitian ini mengadopsi metode did:key untuk identitas pengguna karena tidak memerlukan infrastruktur *hosting* maupun teknologi *blockchain*, serta dapat dibuat secara mandiri di dalam dompet digital. Proses pembuatan identitas pengguna diuraikan pada Algoritma 2.

Algoritma 2. Proses Pembuatan Identitas Digital Pengguna

```
INPUT  : Instruksi inisiasi identitas pada dompet digital
OUTPUT : Pengenal did:key dan pasangan kunci terenkripsi

BEGIN
1. Menginisiasi pembuatan pasangan kunci (key pair) EC P-256
2. Menyimpan kunci privat secara aman di penyimpanan lokal perangkat
3. Mengonversi kunci publik menjadi pengenal unik did:key
4. Menyimpan pengenal did:key dan kunci publik ke penyimpanan lokal
5. Mengembalikan status identitas digital berhasil disusun
END
```

Pembentukan did:key dieksekusi sepenuhnya di dalam perangkat pengguna tanpa memerlukan interaksi dengan server eksternal. Pendekatan ini memastikan bahwa pengguna memegang kendali penuh atas identitas digitalnya sejak proses inisiasi. Untuk keperluan operasional VC, kunci publik yang menjadi landasan did:key direpresentasikan dalam format JWK (RFC 7517). Penyusunan identitas ini mengikuti standar W3C DIDs v1.0 (Sporny dkk., 2022) dengan spesifikasi teknis merujuk pada The did:key Method v0.9 (Longley dkk., 2025). Spesifikasi tersebut menetapkan bahwa penggunaan kurva P-256 akan menghasilkan awalan ‘zDna’ pada string identitas.

Penerbitan *Verifiable Credential*

Setelah kampus dan pengguna masing-masing memiliki identitas digital, tahapan selanjutnya adalah penerbitan VC. VC berfungsi sebagai bukti digital yang memvalidasi status keanggotaan pengguna di lingkungan kampus, sekaligus menggantikan peran kredensial konvensional seperti nama pengguna dan kata sandi. Secara struktural, VC disusun mengikuti standar W3C VC Data Model 2.0 (Sporny dkk., 2025) yang terdiri atas tiga komponen utama. Pertama, *Credential Metadata* yang mendefinisikan informasi operasional seperti identitas penerbit, waktu penerbitan, dan masa berlaku. Kedua, *Credential Claims* yang memuat atribut data pengguna. Ketiga, *Credential Proof* sebagai mekanisme pembuktian kriptografis yang menjamin keaslian dan integritas data. Struktur *payload* VC dirangkum pada Tabel 4.

Tabel 4. Struktur *Payload Verifiable Credential*

Properti	Fungsi	Komponen
@context	Merujuk standar W3C VC Data Model 2.0	*Credential Metadata*
type	Mendeklarasikan tipe ‘VerifiableCredential’ dan ‘AcademicCredential’	*Credential Metadata*
issuer	Berisi pengenal did:web kampus	*Credential Metadata*
validFrom	Menetapkan tanggal mulai berlaku VC	*Credential Metadata*
validUntil	Menetapkan tanggal kedaluwarsa VC	*Credential Metadata*
credentialSubject	Memuat atribut pengguna: id (did:key), name, id_number, faculty, angkatan, role	*Credential Claims*

Atribut pengguna pada credentialSubject sepenuhnya mengacu pada hasil analisis kebutuhan kredensial yang telah diidentifikasi pada Tabel 2. Komponen *Credential Proof* belum tercantum dalam *payload* awal karena baru akan disematkan saat proses penandatanganan kriptografis oleh kampus. Proses penandatanganan diuraikan pada Algoritma 3.

Algoritma 3. Proses Penandatanganan *Verifiable Credential*

```
INPUT  : Payload VC (JSON), kunci privat kampus
OUTPUT : Token VC-JWT siap dikirim ke pengguna

BEGIN
1. Menyusun payload VC secara terstruktur
2. Menandatangani payload menggunakan kunci privat kampus (ES256)
3. Mengodekan hasil tanda tangan ke format Base64URL
4. Menggabungkan Header, Payload, dan Signature menjadi token VC-JWT
5. Mengembalikan token VC-JWT yang telah terbentuk
END
```

Proses penandatanganan menghasilkan token VC-JWT dengan format 'Header.Payload.Signature' sesuai standar JWS (RFC 7515). Bagian *Header* memuat parameter algoritma ES256 dan pengenal kunci (*kid*) yang menautkan token ke kunci publik resmi kampus. Tanda tangan yang dihasilkan bertindak langsung sebagai komponen *Proof*. Struktur ini memastikan bahwa VC tidak dapat dimanipulasi serta hanya dapat diterbitkan oleh pihak kampus yang sah.

Setelah token VC-JWT terbentuk, dokumen didistribusikan ke dompet digital pengguna melalui mekanisme klaim. Pengguna mengakses antarmuka klaim pada sistem layanan kampus dan memindai kode QR yang disediakan. Dompet digital kemudian meminta token VC-JWT melalui protokol HTTPS untuk disimpan secara lokal di dalam perangkat. Dengan tersimpannya VC di dompet digital, pengguna telah memiliki kredensial yang berdaulat dan siap digunakan untuk autentikasi pada berbagai sistem layanan kampus.

Autentikasi Menggunakan *Verifiable Credential*

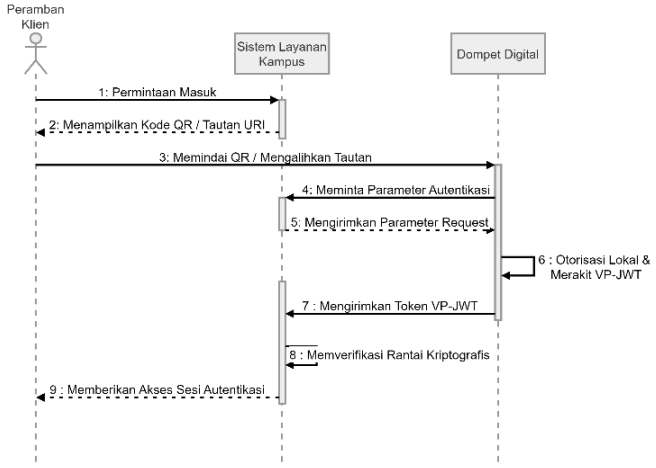
Setelah VC tersimpan di dompet digital, tahap selanjutnya adalah autentikasi ke sistem layanan kampus. Penelitian ini menggunakan dua standar protokol, yaitu SIOPv2 (*Self-Issued OpenID Provider v2*) (Yasuda dkk., 2023) untuk membuktikan identitas pengguna dan OID4VP (*OpenID for Verifiable Presentations*) (Yasuda dkk., 2022) untuk mengirimkan VP sebagai bukti kepemilikan kredensial. Kedua token tersebut dirancang untuk dikirim secara bersamaan dalam satu respons autentikasi.

Arsitektur ini mendukung dua skenario autentikasi melalui pemanggilan skema URI 'siopv2://'. Skenario pertama adalah lintas perangkat (*cross-device*), yaitu ketika pengguna mengakses layanan melalui komputer tetapi dompet digital berada di ponsel. Pada skenario ini, sistem menampilkan kode QR yang dipindai pengguna. Skenario kedua adalah perangkat tunggal (*same-device*), yaitu ketika seluruh proses terjadi di satu ponsel. Pada skenario ini, sistem menggunakan tautan langsung yang membuka dompet digital. Perbedaan teknis antara kedua skenario dirangkum pada Tabel 5.

Tabel 5. Spesifikasi Alur Autentikasi

Aspek	***Cross-Device***	***Same-Device***
Metode Pemanggilan	Kode QR	*Pengalihan Tautan* (*Deep Link*)
Parameter URL	Hanya 'client_id' dan 'request_uri'	'scope', 'response_type', 'client_id', 'redirect_uri', 'response_mode', 'nonce'
Pengiriman Respons	HTTP POST	Pengalihan URL dengan *Fragment*
Response Mode	'direct_post'	'fragment'

Fase permintaan diawali saat sistem layanan kampus menampilkan antarmuka masuk. Diagram sekuens pada Gambar 3 mengilustrasikan alur komunikasi untuk kedua skenario.



Gambar 3. Diagram Sekuens Autentikasi Kredensial

Alur autentikasi dimulai ketika sistem layanan kampus menyusun permintaan autentikasi berisi parameter client_id, redirect_uri, scope, dan nonce. Parameter nonce disertakan untuk mencegah serangan ulang (*replay attack*). Permintaan disampaikan ke dompet digital melalui kode QR atau tautan langsung. Dompet digital kemudian menampilkan notifikasi kepada pengguna dan meminta persetujuan. Sebelum melanjutkan, dompet digital memverifikasi autentikasi lokal pengguna melalui PIN atau biometrik untuk memastikan kunci privat tidak pernah meninggalkan perangkat.

Jika pengguna menyetujui, dompet digital membangun dua token. Token pertama adalah 'id_token' sebagai bukti identitas yang berisi klaim tentang pengguna. Token kedua adalah 'vp_token' yang berisi VC dalam bentuk VP. VP dibuat dengan memasukkan VC ke dalam 'EnvelopedVerifiableCredential', lalu ditandatangani dengan kunci privat pengguna menjadi VP-JWT. Dokumen tersebut kemudian dimasukkan ke dalam 'EnvelopedVerifiablePresentation' dan ditandatangani kembali menjadi VP-JWT final. Seluruh proses penandatanganan mengikuti standar Securing Verifiable Credentials using JOSE (Jones dkk., 2025).

Dompet digital mengirimkan kedua token kembali ke sistem layanan. Pada skenario lintas perangkat, token dikirim melalui HTTP POST. Pada skenario perangkat tunggal, token dikirim melalui pengalihan URL dengan *fragment*. Sistem layanan kemudian melakukan verifikasi kriptografis berlapis yang diuraikan pada Algoritma 4.

Algoritma 4. Proses Verifikasi Kriptografis pada *Verifier*

```
INPUT  : id_token dan vp_token dari dompet digital
OUTPUT : Keputusan Autentikasi (Diberikan / Ditolak)

BEGIN
1. Mengekstrak payload dari id_token dan vp_token
2. Memvalidasi kecocokan nilai nonce (cegah replay attack)
3. Memverifikasi klaim penerbit pada id_token (iss = sub)
4. Melakukan resolusi did:key untuk memperoleh kunci publik pengguna
5. Memverifikasi tanda tangan VP-JWT menggunakan kunci publik pengguna
6. Mengekstrak VC-JWT dari dalam VP-JWT yang telah tervalidasi
7. Melakukan resolusi did:web untuk memperoleh kunci publik kampus
8. Memverifikasi tanda tangan VC-JWT menggunakan kunci publik kampus
9. IF seluruh rantai verifikasi valid THEN
      Berikan sesi akses sistem layanan kampus
   ELSE
      Tolak akses dan putus koneksi
END
```

Dalam standar SIOPv2, sistem layanan kampus berperan sebagai *Relying Party* (RP), yaitu pihak yang meminta dan memverifikasi identitas pengguna. Dompet digital pada ponsel pengguna berperan sebagai *Self-Issued OP*, yaitu pihak yang menyimpan kredensial dan menerbitkan bukti identitas. Alur penerapan di STT Terpadu Nurul Fikri dimulai ketika RP mengirimkan permintaan autentikasi ke Self-Issued OP melalui kode QR atau tautan langsung. *Self-Issued OP* kemudian mengirimkan 'id_token' dan 'vp_token' kembali ke RP. RP mengambil kunci publik dari server kampus melalui

metode did:web untuk memverifikasi token yang diterima. Jika seluruh verifikasi berhasil, RP memberikan akses kepada pengguna. Mekanisme ini memungkinkan verifikasi dilakukan secara mandiri tanpa menghubungi server penerbit, sesuai dengan prinsip *stateless verification* yang menjadi keunggulan arsitektur SSI.

Hasil Pengujian dan Pembahasan

Pengujian protokol SSI dilakukan melalui tiga skenario yang mencakup seluruh alur utama: penerbitan VC, penyimpanan VC, dan autentikasi menggunakan SIOPv2. Setiap skenario diuji dari tiga aspek: fungsionalitas, kinerja, dan penerimaan pengguna.

Pada Skenario 1, *issuer* mengisi data mahasiswa dan menekan tombol *Create VC*. Sistem berhasil menerbitkan VC dan menampilkan kode QR. Pada Skenario 2, holder memindai kode QR dan menyimpan VC ke dompet digital. Sistem berhasil memverifikasi tanda tangan digital dan menyimpan VC dengan data yang sesuai. Pada Skenario 3, *backend* berhasil merespons permintaan *login* sesuai standar protokol SIOPv2, meskipun pengujian masih melalui *terminal* karena dompet digital belum mendukung fitur pemrosesan URI khusus. Hasil fungsional ketiga skenario dirangkum pada Tabel 6.

Tabel 6. Hasil Pengujian Fungsional

No	Skenario	Hasil yang Diharapkan	Hasil Aktual	Status
1	*Issuer* membuat VC	VC terbit dan QR ditampilkan	Berhasil	Pass
2	*Holder* memindai QR dan menyimpan VC	VC tersimpan di dompet digital	Berhasil	Pass
4	*Backend* merespons *login* SIOPv2	Merespons sesuai standar	Berhasil	Pass

Keberhasilan seluruh skenario pada Tabel 6 membuktikan bahwa pendekatan SSI tanpa *blockchain* dapat bekerja dengan baik untuk autentikasi kampus. Penggunaan metode did:web dan did:key memungkinkan seluruh proses berjalan di atas infrastruktur web standar yang sudah tersedia, tanpa perlu membangun jaringan baru yang mahal. Hal ini menjadi keunggulan utama dibandingkan penelitian sebelumnya yang masih bergantung pada *blockchain* atau protokol kustom, sebagaimana telah diuraikan pada bagian Penelitian Relevan.

Pengujian kinerja dilakukan untuk mengukur efisiensi protokol. Waktu pembuatan VC diukur sebanyak 10 kali iterasi, waktu resolusi did.json sebanyak 10 kali iterasi, dan waktu *login* SIOPv2 sebanyak 5 kali iterasi karena keterbatasan akses *session Id* yang harus diambil secara manual dari halaman *login*. Hasilnya dirangkum pada Tabel 7.

Tabel 7. Hasil Pengujian Kinerja Protokol

Parameter	Rata-rata	Minimum	Maksimum
Waktu Pembuatan VC	384 ms	71 ms	1069 ms
Waktu Resolusi did.json	404 ms	67 ms	1138 ms
Waktu *Login* SIOPv2	112 ms	77 ms	203 ms

Tabel 7 menunjukkan bahwa seluruh parameter memiliki rata-rata di bawah 500 ms dengan tingkat keberhasilan 100%. Nilai maksimum yang terlihat tinggi pada pembuatan VC (1069 ms) dan resolusi did.json (1138 ms) terjadi pada iterasi awal. Hal ini disebabkan oleh proses *cold start* server, di mana permintaan pertama memerlukan waktu lebih lama untuk inisialisasi koneksi. Pada iterasi berikutnya, koneksi yang sudah terjalin membuat waktu menurun drastis hingga di bawah 100 ms. Pola serupa juga terlihat pada *login* SIOPv2 yang menunjukkan variasi kecil dengan rata-rata hanya 112 ms. Fluktuasi ini wajar pada pengujian berbasis HTTP dan tidak mencerminkan kelemahan protokol.

Dibandingkan dengan penelitian sebelumnya, protokol ini menunjukkan keunggulan kecepatan yang signifikan. Penelitian berbasis *blockchain* mencatat waktu autentikasi sekitar 1,5 detik akibat proses konsensus jaringan, sementara kredensial lintas *blockchain* memerlukan hingga 2,4 detik. Protokol dalam penelitian ini hanya memerlukan rata-rata 112 ms untuk verifikasi. Perbedaan signifikan ini disebabkan oleh tidak adanya proses *blockchain* dalam arsitektur yang dirancang, sehingga verifikasi hanya melibatkan operasi kriptografi lokal yang ringan. Dengan demikian, pendekatan ini tidak hanya lebih sederhana dari sisi infrastruktur, tetapi juga lebih cepat dalam proses autentikasi.

Dari sisi penerimaan pengguna, UAT dilakukan melalui demonstrasi Skenario 1 dan 2 kepada mitra LTSI. Mitra menyaksikan proses pembuatan VC dan penyimpanan VC, kemudian memberikan tanggapan sebagaimana dirangkum pada Tabel 8.

Tabel 8. Hasil User Acceptance Testing

Peran	Pertanyaan	Tanggapan	Status
Issuer	Apakah proses input data dan pembuatan VC terlihat mudah?	Mudah	Diterima
Holder	Apakah proses pemindaian QR terlihat mudah?	Mudah	Diterima
Holder	Apakah proses menyimpan VC ke dompet terlihat mudah?	Mudah	Diterima
Holder	Apakah data di dompet sesuai dengan input *Issuer*?	Sesuai	Diterima

Tabel 8 menunjukkan bahwa mitra memberikan tanggapan positif pada seluruh aspek yang didemonstrasikan. Proses pembuatan VC oleh *issuer* dinilai mudah karena hanya melibatkan pengisian formulir dan satu kali klik. Proses pemindaian kode QR dan penyimpanan VC oleh *holder* juga dinilai mudah karena alurnya serupa dengan pengalaman pengguna sehari-hari saat memindai kode QR. Kesesuaian data antara input *issuer* dan tampilan di dompet juga terkonfirmasi, yang menunjukkan bahwa tidak ada kehilangan atau perubahan data selama proses penerbitan dan penyimpanan kredensial. Tanggapan positif ini menunjukkan bahwa alur kerja yang dirancang mudah dipahami oleh pengguna dengan latar belakang yang beragam, tidak hanya dari bidang teknologi. Mitra menyatakan sistem layak diterapkan di STT Terpadu Nurul Fikri dengan catatan agar fitur autentikasi SIOPv2 diselesaikan hingga berjalan secara utuh dari dompet digital hingga sistem layanan kampus.

Secara keseluruhan, hasil pengujian menunjukkan bahwa protokol SSI yang dirancang berfungsi dengan baik, memiliki kinerja yang efisien, dan mudah digunakan. Namun, penelitian ini memiliki beberapa keterbatasan. Fitur verifikasi VP otomatis dan pencegahan serangan ulang belum diimplementasikan. Pengujian masih dilakukan pada lingkungan simulasi dengan beban terbatas, bukan pada kondisi produksi dengan banyak pengguna. Mekanisme pencabutan kredensial sebelum masa berlaku habis juga belum dicakup. Keterbatasan ini membuka peluang pengembangan pada penelitian selanjutnya.

SIMPULAN

Berdasarkan hasil penelitian, protokol *Self-Sovereign Identity* yang paling sesuai untuk sistem layanan kampus STT Terpadu Nurul Fikri adalah SIOPv2 dan OID4VP. Pemilihan ini didasarkan pada kompatibilitas dengan sistem autentikasi kampus yang sudah ada, kemudahan implementasi, serta ketersediaan standar internasional dari OpenID Foundation. Telah dirancang arsitektur autentikasi berbasis kedua protokol tersebut yang mencakup metode did:web untuk identitas digital kampus, metode did:key untuk identitas digital pengguna, alur penerbitan *Verifiable Credential* (VC), serta alur autentikasi menggunakan kredensial digital. Hasil pengujian fungsional menunjukkan bahwa seluruh skenario berhasil dijalankan. Pengujian kinerja menunjukkan rata-rata waktu pembuatan VC 384 ms, resolusi did.json 404 ms, dan *login* SIOPv2 112 ms, yang jauh lebih cepat dibandingkan pendekatan berbasis *blockchain* yang memerlukan waktu sekitar 1,5 detik. Hasil *User Acceptance Testing* melalui demonstrasi kepada mitra LTSI menunjukkan bahwa sistem dinilai mudah digunakan dan layak diterapkan. Kontribusi utama penelitian ini adalah pengembangan arsitektur SSI tanpa *blockchain* pada infrastruktur web standar yang menjadi alternatif lebih ringan bagi institusi pendidikan.

Penelitian ini memiliki beberapa keterbatasan yang dapat menjadi arah pengembangan selanjutnya. Fitur autentikasi SIOPv2 pada dompet digital perlu diselesaikan agar sistem dapat berjalan secara utuh. Verifikasi VP otomatis dan pencegahan serangan ulang perlu diimplementasikan. Mekanisme pencabutan kredensial sebelum masa berlaku habis juga perlu dikembangkan. Pengujian interoperabilitas dengan implementasi SSI lain serta uji coba pada skala yang lebih besar dengan pengguna nyata disarankan untuk mengukur performa sistem pada kondisi produksi.

DAFTAR PUSTAKA

De Prisco, R., Shevchenko, S., & Faruolo, P. (2024). Enhancing OpenID Connect for Verifiable Credentials with DIDComm. *Proceedings of the 21st International Conference on Security and Cryptography - SECRYPT*, 844–849. https://doi.org/10.5220/0012850800003767

Goel, A., & Rahulamathavan, Y. (2024). A Comparative Survey of Centralised and Decentralised Identity Management Systems: Analysing Scalability, Security, and Feasibility. *Future Internet*, *17*(1), 1. https://doi.org/10.3390/fi17010001

Gribneau, C., Prorock, M., Steele, O., Xu, M., & Zagidulin, D. (2026). *did:web Method Specification*. https://w3c-ccg.github.io/did-method-web/

IBM Security. (2021, Juni 15). IBM Survey: Pandemic-Induced Digital Reliance Creates Lingering Security Side Effects. *IBM Newsroom*. https://uk.newsroom.ibm.com/2021-06-15-IBM-Survey-Pandemic-Induced-Digital-Reliance-Creates-Lingering-Security-Side-Effects

Jones, M., Prorock, M., & Cohen, G. (2025). *Securing Verifiable Credentials using JOSE and COSE* (W3C Recommendation). https://www.w3.org/TR/vc-jose-cose/

Kemendikdasmen. (2024, Maret 26). Kemendikbudristek Bersiap Menjadi Bagian Infrastruktur Informasi Vital (IIV) Sektor Bidang Pendidikan. *EduCSIRT*. https://educsirt.kemendikdasmen.go.id/portal/berita/196

Longley, D., Zagidulin, D., & Sporny, M. (2025). *The did:key Method v0.9* (W3C Community Group). https://w3c-ccg.github.io/did-key-spec/

Mansoori, S. Al, & Maheshwari, P. (2022). HEI-BCT: A Framework to Implement Blockchain-Based Self-Sovereign Identity Solution in Higher Education Institutions. *2022 8th International Conference on Information Technology Trends (ITT)*, 6–10. https://doi.org/10.1109/ITT56123.2022.9863933

Maram, D., Malvai, H., Zhang, F., Jean-Louis, N., Frolov, A., Kell, T., Lobban, T., Moy, C., Juels, A., & Miller, A. (2021). CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability. *2021 IEEE Symposium on Security and Privacy (SP)*, *2021-May*, 1348–1366. https://doi.org/10.1109/SP40001.2021.00038

Paredes-García, D., Fernández-Carrasco, J. Á., López, J. A. M., Vasquez-Correa, J. C., Yoldi, I. J., Moreno-Acevedo, S. A., González-Docasal, A., Irazusta, H. A., Muniain, A. Á., & Loinaz, Y. de D. (2025). SIBERIA: A Self-Sovereign Identity and Multi-Factor Authentication Framework for Industrial Access. *Applied Sciences*, *15*(15), 8589. https://doi.org/10.3390/app15158589

Schardong, F., & Custódio, R. (2022). Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. *Sensors*, *22*(15), 5641. https://doi.org/10.3390/s22155641

Sporny, M., Longley, D., Chadwick, D., & Herman, I. (2025). Verifiable Credentials Data Model v2.0. Dalam *World Wide Web Consortium Recommendation*. https://www.w3.org/TR/vc-data-model-2.0/

Sporny, M., Longley, D., Sabadello, M., Reed, D., Steele, O., & Allen, C. (2022). *Decentralized Identifiers (DIDs) v1.0* (W3C Recommendation). https://www.w3.org/TR/did-1.0/

Stefan-Robert, C., & Butincu, C. N. (2024). Decentralized Blockchain-based Platform for Managing and Issuing Academic Certificates. *2024 28th International Conference on System Theory, Control and Computing (ICSTCC)*, 570–575. https://doi.org/10.1109/ICSTCC62912.2024.10744729

Tan, E., Lerouge, E., Du Caju, J., & Du Seuil, D. (2023). Verification of Education Credentials on European Blockchain Services Infrastructure (EBSI): Action Research in a Cross-Border Use Case between Belgium and Italy. *Big Data and Cognitive Computing*, *7*(2), 79. https://doi.org/10.3390/bdcc7020079

Tempo.co. (2024, Juli 1). *6 Dampak Serangan Ransomware ke Server PDNS*. https://www.tempo.co/digital/6-dampak-serangan-ransomware-ke-server-pdns-44346

Tran, T.-D., Bao, H. P. G., Cam, N. T., & Pham, V.-H. (2025). DAVE-CC: A decentralized, access-controlled, verifiable ecosystem for cross-chain academic credential management. *Journal of Information Security and Applications*, *94*, 104238. https://doi.org/10.1016/j.jisa.2025.104238

Windley, P. J. (2021). Sovrin: An Identity Metasystem for Self-Sovereign Identity. *Frontiers in Blockchain*, *4*. https://doi.org/10.3389/fbloc.2021.626726

Yasuda, K., Jones, M. B., & Lodderstedt, T. (2023). Self-Issued OpenID Provider v2 - draft 13. Dalam *openid.net*. https://openid.net/specs/openid-connect-self-issued-v2-1_0.html

Yasuda, K., Lodderstedt, T., Chadwick, D., Nakamura, K., & Vercammen, J. (2022). *OpenID for Verifiable Credentials*. https://openid.net/wordpress-content/uploads/2022/05/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials_FINAL_2022-05-12.pdf

Yousra, B., Yassine, S., Yassine, M., Said, S., Lo'ai, T., & Salah, K. (2023). A Novel Secure and Privacy-Preserving Model for OpenID Connect Based on Blockchain. *IEEE Access*, *11*, 67660–67678. https://doi.org/10.1109/ACCESS.2023.3292143