PROPOSAL TUGAS AKHIR – ET234801

"Arsitektur Terdesentralisasi untuk *Self-Sovereign Identity* (SSI) Berbasis *Decenterlize Identity* (DID) dan *Verifiable Credential* (VC) yang Berorientasi pada Mekanisme Pencegahan Manipulasi"

DWIYASA NAKULA

NRP 5027221001

Dosen Pembimbing I

Hafara Firdausi, S. Kom., M. Kom.

NIP 2022199812030

Dosen Pembimbing II

Fuad Dary Rosyadi, S.Kom., M.Kom.

NIP 199609102024061003

Program Studi S1 Teknologi Informasi

Departemen Teknologi Informasi

Fakultas Teknologi Elektro dan Informatika Cerdas

Institut Teknologi Sepuluh Nopember

Surabaya

2025

LEMBAR PENGESAHAN

“Arsitektur Terdesentralisasi untuk Self- Sovereign Identity (SSI) Berbasis Decenterlize Identity (DID) dan Verifiable Credential (VC) yang Berorientasi pada Mekanisme Pencegahan Manipulasi”

PROPOSAL TUGAS AKHIR

Diajukan untuk memenuhi salah satu syarat

memperoleh gelar Sarjana Komputer pada

Program Studi S-1 Teknologi Informasi

Departemen Teknologi Informasi

Fakultas Teknologi Elektro dan Informatika Cerdas

Institut Teknologi Sepuluh Nopember

Oleh : DWIYASA NAKULA

NRP. 5027221001

Disetujui oleh Tim Penguji Proposal Tugas Akhir :

Ditandatangani oleh HAFARA FIRDAUSI (LOHFAF8151)
Ditandatangani pada 13 Februari 2026 13:22:46

1. Hafara Firdausi, S.Kom., M.Kom. Pembimbing
   NIP 2022199812030

2. Fuad Dary Rosyadi, S.Kom., M.Kom. Ko-pembimbing
   NIP 199609102024061003

SURABAYA

Februari, 2026

APPROVAL SHEET

"A Decentralized Architecture for Self-Sovereign Identity (SSI) Based on Decentralized Identifiers (DID) and Verifiable Credentials (VC) with a Focus on Manipulation-Prevention Mechanisms"

FINAL PROJECT PROPOSAL

Submitted to full one of the requirements

For obtaining Bachelor degree at

Undergraduate Study Program of Information Technology

Department of Information Technology

Faculty of Intelligent Electrical and Informatics Technology

Institut Teknologi Sepuluh Nopember

By : DWIYASA NAKULA

NRP. 5027221001

Approved by Final Project Examiner Team: :

Ditandatangani oleh HAFARA FIRDAUSI (LOHFAF8151)
Ditandatangani pada 13 Februari 2026 13:22:48

1. Hafara Firdausi, S.Kom., M.Kom. Advisor
   NIP 2022199812030

2. Fuad Dary Rosyadi, S.Kom., M.Kom. Co-advisor
   NIP 199609102024061003

SURABAYA

February, 2026

ABSTRAK

Arsitektur Terdesentralisasi untuk Self-Sovergn Identity (SSI) Berbasis Decenterlize Identity (DID) dan Verifiable Credential (VC) yang Berorientasi pada Mekanisme Pencegahan Manipulasi

Nama Mahasiswa / NRP	**:**	**Dwiyasa Nakula / 5027221001**
Departemen	**:**	**Teknologi Informasi FTEIC - ITS**
Dosen Pembimbing I	**:**	**Hafara Firdausi, S.Kom., M.Kom.**
Dosen Pembimbing II	**:**	**Fuad Dary Rosyadi, S.Kom., M.Kom.**

Abstrak

Perkembangan layanan digital yang semakin masif meningkatkan kebutuhan akan sistem identitas yang aman, privat, dan tidak bergantung pada otoritas tunggal. Model identitas tradisional yang tersentralisasi terbukti rentan terhadap kebocoran data, penyalahgunaan akses, serta kurangnya kontrol pengguna terhadap informasi pribadinya. *Self-Sovereign Identity* (SSI) hadir sebagai paradigma alternatif yang mengutamakan kedaulatan pengguna melalui penggunaan *Decentralized Identifiers* (DID) dan *Verifiable Credentials* (VC). Namun, sejumlah implementasi SSI modern masih menghadapi isu pseudo-desentralisasi, ketergantungan pada operator tunggal, risiko manipulasi proses revocation, serta kurangnya mekanisme privasi yang kuat dalam proses verifikasi. Proposal ini mengusulkan rancangan arsitektur SSI yang lebih terdistribusi dan tahan manipulasi melalui integrasi beberapa komponen kunci, yakni *verifiable data registry* (VDR) berbasis *multi-node*, *verification gateway* (VG) yang mendukung *selective disclosure* dan *zero-knowledge proof* (ZKP), serta transparency log untuk memberikan jejak audit yang tidak dapat diubah (*tamper-evident*). Selain itu, mekanisme *multi-validator* dan *threshold signature* (k-of-n) diterapkan untuk memastikan bahwa proses penerbitan, pembaruan, dan pencabutan kredensial tidak dapat dikendalikan atau dimodifikasi oleh satu pihak saja. Rancangan arsitektur ini dievaluasi secara konseptual dan eksperimental melalui empat aspek utama: keamanan, privasi, kinerja, serta desentralisasi dan model kepercayaan. Evaluasi dilakukan dengan membandingkan rancangan terhadap standar dan kerangka kerja internasional seperti W3C, eIDAS 2.0 dan EUDI Wallet, Pan-Canadian Trust Framework, serta praktik desain dari berbagai penelitian SSI modern.

Kata kunci: ***Self-Sovereign Identity, Decentralized Identifier, Verifiable Credential, Tamper-Prevention, Desentralisasi.***

ABSTRACT

A Decentralized Architecture for Self-Sovereign Identity (SSI) Based on Decentralized Identifiers (DID) and Verifiable Credentials (VC) with a Focus on Manipulation-Prevention Mechanisms

Student Name / NRP	**:**	**Dwiyasa Nakula / 5027221001**
Department	**:**	**Teknologi Informasi FTEIC - ITS**
Advisor I	**:**	**Hafara Firdausi, S.Kom., M.Kom.**
Advisor II	**:**	**Fuad Dary Rosyadi, S.Kom., M.Kom.**

Abstract

The rapid growth of digital services has intensified the need for identity systems that are secure, privacy-preserving, and independent of a single authority. Traditional centralized identity models have proven vulnerable to data breaches, unauthorized access, and limited user control over personal information. Self-Sovereign Identity (SSI) emerges as an alternative paradigm that prioritizes user autonomy using Decentralized Identifiers (DID) and Verifiable Credentials (VC). However, many modern SSI implementations still face issues such as pseudo-decentralization, reliance on single operators, risks of revocation manipulation, and insufficient privacy mechanisms during verification. This proposal introduces a more distributed and tamper-resistant SSI architecture by integrating several key components, including a multi-node Verifiable Data Registry (VDR), a Verification Gateway (VG) supporting selective disclosure and zero-knowledge proofs (ZKP), and a transparency log that provides immutable audit trails. Furthermore, a multi-validator governance model and threshold signatures (k-of-n) are employed to ensure that credential issuance, updates, and revocation cannot be controlled or modified by a single entity. The proposed architecture is evaluated conceptually and experimentally across four main dimensions: security, privacy, performance, and decentralization with its associated trust model. The evaluation is conducted by comparing the design against international standards and frameworks such as the W3C, eIDAS 2.0 and the EUDI Wallet, the Pan-Canadian Trust Framework, as well as design practices found in recent SSI research.

Keywords: ***Self-Sovereign Identity, Decentralized Identifier, Verifiable Credential, Tamper-Prevention, Desentralisasi.***

DAFTAR ISI

DAFTAR GAMBAR

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Dalam dunia yang semakin terhubung, di mana setiap transaksi dan interaksi meninggalkan jejak digital, perlindungan identitas menjadi lebih krusial dari sebelumnya, berbagai macam identitas semakin sering digunakan dalam interaksi daring, transaksi elektronik, dan proses pemerintahan digital. Sistem identitas tradisional banyak bergantung pada otoritas pusat, seperti pemerintah, bank, atau penyedia layanan besar yang menyimpan dan mengelola data identitas pengguna secara terpusat. Model ini rentan terhadap kebocoran data, penyalahgunaan akses, serta kehilangan kontrol pengguna atas data pribadinya (Giannopoulou & Wang, 2021).

Dalam lima tahun terakhir, Indonesia mencatat lonjakan signifikan insiden kebocoran data, yang mengindikasikan kerentanan dalam sistem pengelolaan identitas digital nasional. Pada Juli 2023, Kementerian Komunikasi dan Informatika menyelidiki dugaan bocornya 337 juta data kependudukan Dukcapil yang dijual di forum peretas (Fathur Rochman & Siti Zulaikha, 2023). 2 bulan sebelumnya, pada Mei 2023, kelompok ransomware LockBit 3.0 mengklaim telah mencuri 15 juta data nasabah dan karyawan Bank Syariah Indonesia (BSI), dan mengancam akan menyebarkannya di dark web (M. Khory Alfarizi, 2023). Selain itu, insiden kebocoran 279 juta data penduduk pada Mei 2021 yang diperkirakan berasal dari data BPJS Kesehatan (Chaterine, R. N. & Prabowo, D., 2021). Rangkaian kasus ini tidak hanya mengancam privasi individu, tetapi juga membuka peluang kejahatan lintas negara yang memanfaatkan data pribadi. Sebagai respons, pemerintah kemudian mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), meskipun efektivitas penegakan undang-undang tersebut masih menjadi perhatian publik dan pakar. (Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, 2022).

Seiring meningkatnya skala layanan daring dan jumlah identitas digital, tantangan baru muncul dengan mempertimbangkan banyaknya kasus kebocoran data yang pernah terjadi, yaitu memastikan identitas dapat diverifikasi dengan aman tanpa menyimpan semua data pribadi di satu titik kontrol, serta meminimalkan risiko manipulasi sistem oleh entitas dengan akses tinggi. Tantangan tersebut dijawab melalui Self-Sovereign Identity (SSI), yang mengembalikan kendali atas identitas digital langsung ke individu, implementasinya di dunia nyata masih menghadapi sejumlah tantangan signifikan. Banyak sistem SSI yang ada saat ini belum sepenuhnya terdesentralisasi. Sebagian besar masih bergantung pada satu atau beberapa entitas pengelola yang menjalankan fungsi kritis, seperti *validator node* atau governance, dan ini menghadirkan risiko manipulasi atau kontrol sentral. Misalnya, pada jaringan Sovrin, hanya entitas tertentu yang disebut Stewards yang diizinkan untuk menjalankan *node validator* dalam *ledger permissioned*-nya (Sovrin Foundation, 2018, 2020). Meskipun *ledger*-nya terdistribusi, keputusan penting seperti siapa yang boleh menjadi Steward atau mengubah konfigurasi jaringan tetap diatur oleh Sovrin Foundation melalui *governance framework* (Sovrin Foundation, 2023). Ketergantungan semacam ini menimbulkan risiko: entitas pengelola tersebut punya kemampuan untuk memanipulasi identitas, menetapkan aturan, atau melakukan perubahan sistem tanpa partisipasi penuh dari semua pengguna. Ini bisa memicu kebocoran data pribadi atau penyalahgunaan akses, meskipun klaim sistem "desentralisasi" tetap digaungkan (Schardong & Custódio, 2022).

Kritikan lainnya seperti dari (Giannopoulou, 2023), juga mencatat bahwa meski arsitektur SSI secara teori mendistribusikan kontrol, dalam praktiknya masih terdapat titik sentral yang rentan terhadap manipulasi dan kegagalan operasional. Ditambah lagi, dengan ketergantungan yang besar pada teknologi blockchain dan ledger terdistribusi, sejumlah ahli memperingatkan bahwa mekanisme verifikasi identitas melalui bukti kriptografis VC (*verifiable credentials*)

mungkin tidak cukup untuk mencegah manipulasi data oleh pihak dengan hak administratif tinggi (Giannopoulou & Wang, 2021). Semua hal ini menunjukkan perlunya lapisan perlindungan tambahan terutama pada mekanisme pencegahan manipulasi yang lebih kuat.

Untuk menjawab kelemahan tersebut, penelitian ini mengusulkan desain arsitektur terdesentralisasi untuk sistem *Self- Sovereign Identity* (SSI) berbasis DID (*Decentralized Identifiers*) dan VC (*Verifiable Credentials*) yang mengintegrasikan mekanisme pencegahan manipulasi. Arsitektur ini tidak hanya mendistribusikan pengelolaan identitas melalui jaringan *validator* dan *ledger*, tetapi juga menggunakan teknik kriptografi selektif, seperti *selective disclosure* dan *threshold signature*, untuk memastikan integritas dan otonomi pengguna, sekaligus mengurangi potensi manipulasi oleh entitas tunggal. Pendekatan ini memungkinkan verifikasi identitas oleh pihak ketiga tanpa mengungkapkan data pribadi yang sensitif, hanya terbatas pada status yang relevan, seperti "usia ≥ 18" (Schardong & Custódio, 2022).

Dalam prakteknya, sejumlah negara seperti Estonia dan Kanada telah memulai penerapan sistem identitas digital yang terdesentralisasi, meskipun dengan pendekatan yang bervariasi. Estonia menggunakan identitas digital terintegrasi dalam layanan publik sejak 2002 dalam bentuk kartu identitas nasional, dan baru-baru ini mengadopsi teknologi blockchain untuk memastikan integritas data identitas digital warganya melalui Guardtime's KSI (*Keyless Signature Infrastructure*) (Grech et al., 2017; Semenzin et al., 2022). Di sisi lain, Kanada mengembangkan identitas digital terdesentralisasi berbasis *Verifiable Credentials* (SSI) melalui kerangka Pan-Canadian Trust Framework (PCTF). Individu dapat menyimpan kredensial digital di dompet pribadi dan mengontrol data apa yang dibagikan. Sebagai bukti, Pemerintah British Columbia telah melakukan *proof-of-concept* penerbitan VC, di mana pengguna memiliki kontrol penuh atas kredensial digital mereka (DIACC, 2021; DIACC's Trust Framework Expert Committee, 2023). Pendekatan-pendekatan ini menawarkan wawasan penting dalam perancangan sistem identitas yang lebih aman dan terdesentralisasi, yang tidak hanya mengurangi ketergantungan pada entitas tunggal, tetapi juga meningkatkan kepercayaan pengguna terhadap keamanan dan privasi data mereka.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, rumusan masalah yang akan dikaji dalam penelitian ini adalah:

1. Bagaimana merancang dan mengembangkan arsitektur terdesentralisasi untuk *Self-Sovereign Identity* (SSI) berbasis DID dan VC serta memiliki mekanisme pencegahan manipulasi (*tamper-prevention*) yang kuat?
2. Bagaimana performa komponen dan mekanisme dalam proses penerbitan, penyimpanan, dan verifikasi kredensial terhadap ketahanan manipulasi (tampering), integritas, keaslian data, serta efisiensi proses pada arsitektur terdesentralisasi?
3. Bagaimana menjamin keamanan dan privasi pengguna tanpa mengorbankan efisiensi proses verifikasi?

1.3 Batasan Masalah

Agar penelitian ini tetap fokus dan sesuai dengan ruang lingkup studi sarjana, batasan masalah ditetapkan sebagai berikut:

1. Penelitian ini berfokus pada perancangan arsitektur dan implementasi prototipe terbatas (*proof-of-concept*) sistem *Self-Sovereign Identity* (SSI) berbasis DID dan VC, tanpa membangun sistem berskala produksi atau melakukan deployment sistem operasional jangka panjang maupun sistem berskala lapangan.
2. Lingkup penelitian dibatasi pada komponen inti dalam ekosistem SSI, yaitu *issuer*, *holder*, *verifier*, *verification gateway*, dan *verifiable data registry* (VDR), tanpa

membahas integrasi dengan sistem eksternal seperti IAM, *e-government*, atau platform komersial tertentu.
3. Evaluasi sistem mencakup pengujian keamanan, privasi, dan performa secara terbatas melalui simulasi dan eksperimen terkontrol, termasuk pengukuran *latency* dan efisiensi proses, namun tidak mencakup pengujian pada lingkungan produksi nyata, skala nasional, atau beban pengguna lapangan dalam jangka panjang.
4. Aspek hukum, kebijakan, dan regulasi (seperti eIDAS, UU PDP, atau kebijakan nasional) dibahas secara konseptual sebagai konteks desain, dan tidak mencakup analisis kepatuhan hukum, implikasi yuridis, maupun studi kebijakan mendalam.
5. Penelitian ini tidak membahas aspek pengalaman pengguna (user experience), adopsi sosial, maupun analisis ekonomi dan biaya implementasi dari sistem SSI yang diusulkan.
6. Mekanisme kriptografi yang digunakan (seperti *threshold signature*, *zero-knowledge proof*, dan *accumulator*) diasumsikan aman berdasarkan literatur dan standar yang ada, tanpa melakukan pembuktian keamanan formal atau analisis kriptografi tingkat rendah.
7. Meskipun arsitektur sistem bersifat terdesentralisasi secara logis, penelitian ini tidak mencakup implementasi distributed computing atau pemrosesan komputasi terdesentralisasi berbasis multi-perangkat pada level infrastruktur.

1.4 Tujuan

Tujuan utama dari penelitian ini adalah:

1. Merancang dan mengimplementasikan arsitektur *Self-Sovereign Identity* (SSI) berbasis DID dan VC yang terdesentralisasi serta memiliki mekanisme pencegahan manipulasi (*tamper-resistant*).
2. Mengidentifikasi dan mengevaluasi komponen arsitektural serta mekanisme kriptografi dalam proses penerbitan, penyimpanan, dan verifikasi kredensial, termasuk performa mekanisme tersebut dalam menjamin integritas, keaslian data, dan ketahanan terhadap manipulasi pada arsitektur terdesentralisasi.
3. Menganalisis kemampuan rancangan arsitektur dalam menjamin keamanan dan privasi pengguna tanpa mengorbankan efisiensi proses verifikasi, berdasarkan hasil pengujian dan evaluasi yang dilakukan.

1.5 Manfaat

Penelitian ini diharapkan memberikan beberapa manfaat sebagai berikut:

- Manfaat Akademik: Memberikan kontribusi pengetahuan baru mengenai desain arsitektur SSI yang mengintegrasikan prinsip desentralisasi dan *tamper-prevention*.
- Manfaat Praktis: Menjadi referensi bagi lembaga pemerintah, organisasi, atau pengembang dalam merancang sistem identitas digital yang aman dan tahan manipulasi.
- Manfaat Sosial: Meningkatkan kesadaran masyarakat terhadap pentingnya privasi dan kepemilikan data pribadi di era digital.
- Manfaat Teknologis: Menjadi dasar bagi penelitian lanjutan mengenai penerapan teknologi kriptografi modern seperti *threshold signatures* dan *zero-knowledge proofs* pada sistem SSI.

BAB 2 TINJAUAN PUSTAKA

2.1 Hasil Penelitian Terdahulu

Penelitian mengenai *Self-Sovereign Identity (SSI)* semakin berkembang pesat dalam beberapa tahun terakhir seiring meningkatnya kebutuhan akan sistem identitas digital yang aman, terdesentralisasi, dan berorientasi pada privasi. Kajian-kajian pada Tabel 2.1 menjadi dasar bagi pengembangan arsitektur yang diusulkan dalam penelitian ini.

Tabel 2.1 Kontribusi penelitian terdahulu pada penelitian

No	Penulis	Ringkasan (Fokus, Temuan, Relevansi)
1	*Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy.*	
	(Schardong & Custódio, 2022)	Penelitian ini memberikan tinjauan sistematis dan taksonomi SSI berdasarkan infrastruktur, model kepercayaan, dan teknik kriptografi. Mengidentifikasi tantangan seperti keamanan, interoperabilitas, dan resistensi manipulasi. Temuan tersebut menjadi dasar konseptual untuk merancang arsitektur SSI yang aman dan benar-benar terdesentralisasi.
2	*Self-Sovereign Identity.*	
	(Giannopoulou & Wang, 2021)	Meninjau SSI dari perspektif tata kelola dan kebijakan global, menyoroti risiko pseudo-desentralisasi ketika kontrol tetap terpusat pada entitas tertentu. Temuan tersebut menjadi dasar desain arsitektur yang tidak bergantung pada otoritas tunggal dan tahan manipulasi.
3	*Self-Sovereign Identity as a Service: Architecture in Practice.*	
	(Ding & Sato, 2022)	Mengusulkan arsitektur SSI berbasis layanan dengan interaksi modular antara *issuer*, *holder*, dan *verifier*. Studi ini menjadi dasar implementasi yang dapat diadaptasi untuk pencegahan manipulasi, dan menjadi referensi utama dalam desain arsitektur.
4	*Empirical Evaluation of Self-Sovereign Identity Technology.*	
	(Siqueira et al., 2023)	Mengevaluasi kinerja SSI berbasis *Hyperledger Indy/Aries* dan menemukan isu skalabilitas serta ketergantungan tinggi pada *operator node*. Temuan ini menguatkan kebutuhan mekanisme *tamper-resistance* untuk mencegah penyalahgunaan wewenang *node*.
5	*A Critical Approach of Self-Sovereign Identity.*	
	(Giannopoulou, 2023)	Memberikan analisis kritis terhadap implementasi SSI di berbagai negara, menunjukkan bahwa banyak sistem masih memusatkan kontrol pada satu operator. Hal ini menginspirasi pengembangan mekanisme pencegahan manipulasi berbasis *multi-validator* dan *threshold signature* dalam penelitian ini.

Berdasarkan kelima penelitian pada Tabel 2.1, dapat disimpulkan bahwa rancangan SSI modern harus mengintegrasikan prinsip-prinsip berikut:

1. Desentralisasi penuh dalam pengelolaan dan verifikasi identitas.
2. Kedaulatan pengguna dalam kendali data (*self-sovereignty*).
3. Mekanisme pencegahan manipulasi (*tamper-prevention*) berbasis teknik kriptografi seperti *threshold signature*, *selective disclosure*, dan catatan audit transparan.
4. Keterlacakan yang aman, masih bisa di audit namun tetap privat, melalui ledger transparan dan terdistribusi.
5. Independensi dari otoritas tunggal sebagai respons terhadap masalah pseudo-desentralisasi seperti yang ditemukan pada Sovrin dan Indy.

2.2 Dasar Teori

2.2.1 Dokumen Identitas

Dokumen identitas dapat dibedakan menjadi tiga format representasi utama. Pertama adalah dokumen fisik tradisional, seperti kartu plastik atau dokumen kertas yang memuat atribut identitas seseorang. Dokumen ini dibuat dengan mekanisme keamanan tertentu untuk meminimalkan risiko pemalsuan. Ketika diperlukan verifikasi identitas, pemegang hanya perlu menyerahkan dokumen tersebut; pihak verifikasi (*relying party*) kemudian membaca atribut yang tercantum. Salah satu fitur penting dari dokumen ini adalah foto wajah, yang digunakan sebagai alat autentikasi visual (Schardong & Custódio, 2022).

Kedua adalah dokumen identitas digital, yang merupakan versi digital dari dokumen fisik. Dokumen ini biasanya disimpan di perangkat seluler, dan integritas serta keasliannya dijamin melalui teknik kriptografi seperti tanda tangan digital. Atribut identitas dan tanda tangan digital tersebut sering dikodekan dalam bentuk kode QR agar pihak verifikasi dapat memeriksa validitas dokumen tanpa perlu koneksi internet langsung (Schardong & Custódio, 2022).

Ketiga adalah dokumen identitas elektronik, yang dirancang dari awal untuk digunakan dalam ekosistem daring. Tidak seperti dokumen digital yang pada dasarnya adalah representasi visual, dokumen elektronik sepenuhnya digital dan menggunakan mekanisme keamanan seperti autentikasi multi-faktor serta kriptografi kunci publik untuk menjamin otentikasi. Contohnya, suatu sistem dapat mengombinasikan password dengan *time-based one-time password (TOTP)* melalui layanan OTP berbasis waktu sebagai lapis keamanan tambahan ((Ometov et al., 2018) sebagaimana dikutip dalam (Schardong & Custódio, 2022)).

Pada praktiknya, beberapa dokumen identitas diterbitkan secara mandiri oleh individu (misalnya kartu nama atau *curriculum vitae*), tetapi sebagian besar identitas resmi dikeluarkan oleh pihak ketiga tepercaya. Contoh penerbit tersebut antara lain pemerintah (melalui paspor atau SIM) atau organisasi swasta yang telah diotorisasi, misalnya sistem verifikasi identitas nasional digital seperti GOV.UK Verify(Schardong & Custódio, 2022).

2.2.2 Identitas Elekronik

Di dunia fisik, pembentukan kepercayaan antar entitas mensyaratkan identifikasi pihak-pihak yang berkomunikasi. Bukti identitas diperoleh melalui faktor autentikasi yang telah disepakati sebelumnya atau dengan bantuan pihak ketiga yang tepercaya, misalnya penggunaan perangkat fisik sebagai faktor autentikasi, seperti menunjukkan dokumen identitas dan kemudian melakukan verifikasi wajah (*face badge*) (Schardong & Custódio, 2022).

Identitas elektronik umumnya didefinisikan sebagai kumpulan atribut yang menjelaskan atau membedakan suatu entitas (Schardong & Custódio, 2022). Beberapa penulis membatasi definisi tersebut dalam konteks tertentu dengan hanya menyertakan atribut relevan demi akurasi ((Miyata et al., 2006), (El Maliki & Seigneur, 2007), (Md. Sadek Ferdous, 2015) sebagaimana dikutip dalam (Schardong & Custódio, 2022)). Oleh karena itu, identitas elektronik bukan sekadar representasi digital dari dokumen fisik seperti paspor, melainkan entitas yang dibuat, digunakan, dan bahkan dihapus sesuai keinginan pemegang identitas, dengan hanya menyertakan atribut yang diperlukan untuk suatu tujuan spesifik (Schardong & Custódio, 2022).

Baik identitas fisik maupun elektronik mensyaratkan verifikasi kepemilikan melalui proses identifikasi dan autentikasi (Schardong & Custódio, 2022). Pemegang identitas elektronik akan memperlihatkan atribut unik dalam konteks tertentu, misalnya, alamat email saat mendaftar ke layanan sebagai bentuk identifikasi (Schardong & Custódio, 2022). Kemudian, autentikasi dilakukan melalui metode keamanan seperti kata sandi rahasia atau tanda tangan digital, menjamin bahwa pemegang identitas memang pemilik sah (Schardong & Custódio, 2022). Misalnya, verifikasi email dengan memasukkan kode yang dikirim atau mengklik tautan yang diterima melalui email adalah mekanisme umum untuk mengonfirmasi kepemilikan (Schardong & Custódio, 2022).

Karena identifikasi dan autentikasi memungkinkan akses warga ke layanan digital, proses tersebut biasanya dioperasikan oleh layanan khusus yang dipercaya oleh semua pihak yang terlibat. Sistem semacam ini dikenal sebagai *Identity and Access Management* (IAM), yang mengelola identitas elektronik dan menetapkan bagaimana identitas dapat diverifikasi dan diotorisasi (Schardong & Custódio, 2022).

2.2.3 Evolusi Identitas dan Akses Manajemen (IAM) Model

Pada masa awal web, penyedia layanan (*Service Provider/SP*) harus membangun sistem Identitas dan Akses Manajemen (IAM) mereka sendiri untuk mengidentifikasi dan mengautentikasi klien agar bisa menyediakan layanan yang dipersonalisasi. Karena itu, model ini disebut *otoritas terpusat*. Namun, model tersebut menimbulkan sejumlah masalah kegunaan (*usability*) untuk pengguna. Banyak pengguna akhirnya memakai kata sandi yang sama atau sederhana di berbagai sistem, yang membuka celah keamanan. Akibatnya, muncul berbagai inisiatif untuk meningkatkan kesadaran keamanan, dengan memberi edukasi bahwa penggunaan ulang kata sandi sederhana sangat berisiko (Schardong & Custódio, 2022).

Evolusi selanjutnya adalah model IAM dengan pihak ketiga, yakni *Identity Provider* (IdP). Dalam paradigma ini, pengguna hanya perlu terdaftar pada beberapa IdP saja untuk mengakses banyak layanan, sementara SP harus bekerja sama dengan IdP atau federasi IdP tertentu agar bisa mengidentifikasi dan mengautentikasi pengguna. Protokol seperti SAML, OAuth 2.0, dan OpenID Connect digunakan untuk menstandarisasi interaksi antara IdP, SP, dan pengguna. Kemudian muncul model identitas yang lebih berpusat pada pengguna (*user-centric identity*), di mana ide dasarnya adalah pengguna bisa menggunakan perangkat otentikasi pribadi (*Personal Authentication Devices*/PAD), seperti smartphone atau smartcard untuk menyimpan dan menyajikan kredensial autentikasi dari SP tanpa selalu bergantung pada IdP pihak ketiga.

2.2.4 Self-Sovereign Identity (SSI)

Self-Sovereign Identity (SSI) adalah paradigma identitas digital yang menempatkan kendali penuh atas identitas pada individu, bukan pada otoritas terpusat seperti pemerintah atau perusahaan (Schardong & Custódio, 2022). Dalam model ini, pengguna menyimpan kredensial di perangkat pribadi (misalnya dompet digital) dan hanya membagikan aspek identitas yang diperlukan (*selective disclosure*), tanpa mengungkap semua data pribadi sekaligus. Konsep SSI lahir sebagai reaksi terhadap kelemahan model identitas tradisional: penyimpanan pusat rentan terhadap kebocoran, penyalahgunaan data, dan kehilangan kontrol oleh pemilik identitas (Schardong & Custódio, 2022).

SSI beroperasi berdasarkan beberapa prinsip inti: desentralisasi, otonomi, transparansi, dan portabilitas. Dengan desentralisasi, tidak ada satu pihak yang memegang kendali penuh atas identitas, berarti pengguna memiliki kontrol penuh atas

data identitas mereka sendiri. Portabilitas memungkinkan identitas berpindah antar layanan tanpa bergantung pada penyedia identitas Tunggal (Giannopoulou & Wang, 2021). Hal ini juga mencakup interoperabilitas, SSI diharapkan dapat bekerja lintas platform dan domain.

2.2.5 Decentralized Identifier (DID)

Decentralized Identifier (DID) adalah pengenal unik yang dikelola secara desentralisasi, tanpa ketergantungan pada otoritas pusat, dan merupakan fondasi identitas dalam SSI. Struktur dasar DID biasanya adalah did:<method>:<identifier>, di mana <method> menentukan protokol atau ledger yang digunakan, dan <identifier> adalah bagian unik yang mengidentifikasi subjek. Sebuah DID "*resolve*" ke sebuah DID Document, yaitu dokumen yang menyimpan informasi kriptografis seperti *public key, service endpoint*, dan metode verifikasi. Menurut spesifikasi W3C, untuk membuktikan kontrol atas sebuah DID, controller harus melakukan dua langkah: (1) resolusi DID ke DID Document, (2) verifikasi bahwa id dalam DID Document sesuai dengan DID yang diselesaikan. Selain itu, metode untuk membuktikan kepemilikan kunci publik dapat bersifat statis (menandatangani DID Document) atau dinamis (*protokol challenge-response*). (World Wide Web Consortium (W3C), 2019, 2022, 2025b)

2.2.6 Verifiable Credential (VC)

Verifiable Credential (VC) adalah representasi digital dari klaim (*claims*) yang dibuat oleh penerbit (*issuer*) kepada pemegang (*holder*) dan dapat diverifikasi oleh pihak ketiga (*verifier*) secara kriptografis (Satybaldy et al., 2020). Model data VC pada dasarnya terdiri dari beberapa elemen: metadata (seperti tipe kredensial, penerbit, tanggal penerbitan, status pencabutan), subjek (*subject*), klaim (atribut identitas), dan bukti kriptografis (*proof*), seperti tanda tangan digital (*digital signature*) (Gaidhani & Gopal Krishna Sharma, 2025).

Siklus hidup sebuah VC berinteraksi antara empat komponen utama yaitu *Issuer*, *Holder*, *Verifier*, dan *Registry*. Proses dimulai ketika *Issuer* menerbitkan kredensial kepada Holder tepat satu kali, yang kemudian dapat dikelola oleh Holder, seperti menyimpannya, memindahkannya, mempresentasikannya kepada *Verifier* secara berulang, atau bahkan menghapusnya jika diperlukan. Saat *Holder* mempresentasikan VC, *Verifier* melakukan verifikasi atas bukti kriptografis serta memeriksa status kredensial melalui *Registry* untuk memastikan apakah kredensial tersebut masih berlaku atau telah dicabut. Issuer juga memiliki kemampuan untuk mencabut kredensial melalui mekanisme revocation, yang kemudian tercatat di Registry dan dapat diperiksa oleh Verifier.

Dalam konteks SSI, VC memungkinkan mekanisme privasi seperti s*elective disclosure*, pemegang hanya menunjukkan bagian dari klaim yang relevan untuk verifikasi, bukan seluruh set data. Selain itu, ZKP (Zero-Knowledge Proof) dapat digunakan agar pemegang bisa membuktikan atribut tertentu (misalnya "berusia ≥ 18 tahun") tanpa mengungkap data sensitif penuh. Beberapa penelitian dan proposal kriptografi juga mengusulkan skema yang lebih efisien seperti compact disclosure agar presentasi kredensial menjadi ringkas tetapi tetap aman (Buldini et al., 2025).

2.2.7 Distributed Ledger / Verifiable Data Registry (VDR)

Dalam SSI, ledger terdistribusi atau sering disebut *Verifiable Data Registry* (VDR) berfungsi memainkan peranan penting sebagai penyimpan metadata identitas seperti DID

Document, public keys, dan registri pencabutan (revocation registry). Ledger semacam ini bisa diimplementasikan sebagai blockchain publik, jaringan konsorsium, atau jenis Distributed Ledger Technology (DLT) (European Union Agency for Cybersecurity., 2022). Keunggulan menggunakan ledger terdistribusi adalah sifatnya yang immutability atau data yang ditulis tidak bisa diubah begitu saja tanpa konsensus dan auditability atau jejak publik dari transaksi identity dapat dilacak. Setiap perubahan, seperti pembaruan DID Document atau pencabutan VC, dicatat dan bisa diverifikasi oleh pihak mana pun dengan akses ledger (European Union Agency for Cybersecurity., 2022).

Beberapa platform populer yang banyak dikaji dalam konteks SSI adalah Hyperledger Indy, Sovrin, dan ION (di atas Bitcoin). Hyperledger Indy, misalnya, dirancang khusus sebagai ledger untuk identitas terdesentralisasi yang mendukung DIDs, ZKP, dan revocation registry (Hyperledger Indy maintainer and contributor, 2025). Sovrin, di sisi lain, menyimpan DIDs publik, skema kredensial, definisi kredensial, serta registri pencabutan di ledger publiknya (World Wide Web Consortium (W3C), 2025a). Sementara itu, ION (layer-2 di atas Bitcoin) memungkinkan pencatatan operasi DID dengan anchoring ke blockchain Bitcoin, tanpa menjaga semua data sensitif langsung di chain utama (Andrej Novak, 2025).

2.2.8 zero-knowledge proof (ZKP)

Privasi adalah pilar utama dalam prinsip SSI, dan kriptografi menjadi mekanisme teknis yang memungkinkan penggunaan selective disclosure: pemegang kredensial dapat memilih klaim mana yang dibagikan dan dengan siapa, tanpa membuka seluruh data identitas (Jeonghyuk Lee et al., 2021; Joseph Cutler et al., n.d.). Teknik ini memungkinkan verifikasi klaim yang spesifik, seperti "usia ≥ 18", tanpa mengungkap atribut lain yang bersifat sensitif, melalui mekanisme *zero-knowledge proof* (ZKP) yang sangat efisien.

ZKP adalah teknik di mana seorang prover dapat membuktikan kepada verifier bahwa pernyataan tertentu benar tanpa mengungkap nilai sebenarnya dari pernyataan tersebut (Jeonghyuk Lee et al., 2021). Dalam konteks SSI, skema ZKP seperti zk-SNARK memungkinkan pemegang VC untuk menghasilkan bukti kriptografis yang valid, yang bisa diverifikasi publik, sementara nilai-nilai sensitif tetap tidak terungkap. Penelitian terbaru mengusulkan skema ZKP yang dioptimalkan agar waktu pembuatan bukti lebih cepat dan praktis untuk penggunaan nyata (Jeonghyuk Lee et al., 2021).

Selain itu, ZKP dapat digunakan untuk memverifikasi status pencabutan kredensial tanpa mengungkap identitas unik pemegang. Dengan melakukan ini, pemegang dapat menunjukkan bahwa kredensial mereka masih sah tanpa membuka data detail dari kredensial tersebut (Liu et al., 2024). Dalam beberapa implementasi SSI modern, juga dipertimbangkan mekanisme kriptografi threshold signature atau multi-party supervision sehingga ada pengawasan bersama, misalnya regulator, sekaligus tetap menjaga kerahasiaan data pengguna (Liu et al., 2024).

2.2.9 Implementasi dan Studi Kasus

2.2.9.1 Uni Eropa – Inisiatif EUDI Wallet & eIDAS 2.0

Uni Eropa kini mendorong penerapan dompet identitas digital (*European Digital Identity Wallet* / EUDI Wallet) sebagai bagian dari revisi regulasi eIDAS (eIDAS 2.0) (bundesdruckerei., 2024). Menurut rencana, setiap negara anggota wajib menyediakan identitas digital yang diakui lintas negara pada dompet digital warga

negara paling lambat 2026, dan paling tidak 80% warga diharapkan mengadopsinya pada 2030 (bundesdruckerei., 2024).

Secara teknologi, EUDI Wallet akan mendukung verifikasi atribut tambahan (seperti lisensi mengemudi, sertifikat pendidikan) dan menggunakan mekanisme identitas digital yang memungkinkan kontrol pengguna atas data pribadi mereka (bundesdruckerei., 2024). Karena eIDAS 2.0 di desain untuk interoperabilitas di seluruh Uni Eropa, identitas digital yang disajikan di satu negara akan diterima di negara lain, meningkatkan mobilitas digital.

2.2.9.2 Kanada – Kerangka Kerja Pan-Canadian Trust Framework (PCTF)

Kanada mengembangkan *Pan-Canadian Trust Framework* (PCTF) melalui *Digital ID & Authentication Council of Canada (DIACC)* sebagai landasan untuk infrastruktur identitas digital nasional yang tepercaya dan interoperabel (DIACC's Trust Framework Expert Committee, 2023). Kerangka PCTF menetapkan aturan, praktik, dan spesifikasi teknis yang harus dipatuhi oleh penyedia layanan identitas (*issuer*), verifikator, dan dompet digital dalam ekosistem digital Kanada (DIACC's Trust Framework Expert Committee, 2023). Dalam versi PCTF final, DIACC juga menyertakan *Trust Registry* sebagai bagian penting tata kelola identitas terdesentralisasi, untuk mencatat identitas penerbit dan verifikator yang telah disertifikasi (DIACC's Trust Framework Expert Committee, 2023).

PCTF sangat menekankan prinsip *privacy by design*. Dalam dokumen rekomendasi privasi PCTF versi 1.2, DIACC menetapkan bahwa peserta ekosistem harus menerapkan mekanisme persetujuan pengguna (consent), meminimalkan data yang dibagikan, dan menjamin transparansi dalam penggunaan identitas digital (DIACC's Trust Framework Expert Committee, 2024). Kanada memilih model ini karena negara ini ingin menciptakan identitas digital yang aman, tepercaya, dan tidak terpusat di satu entitas pemerintahan tunggal, agar warga memiliki kontrol atas data mereka dan agar sistem bisa diadopsi sektor publik dan swasta. Selain itu, kerangka ini dirancang agar sangat fleksibel dan dapat digunakan oleh organisasi lintas provinsi.

2.2.9.3 Riset / Proyek Akademik SSI (NSSIA) & (SSIaaS)

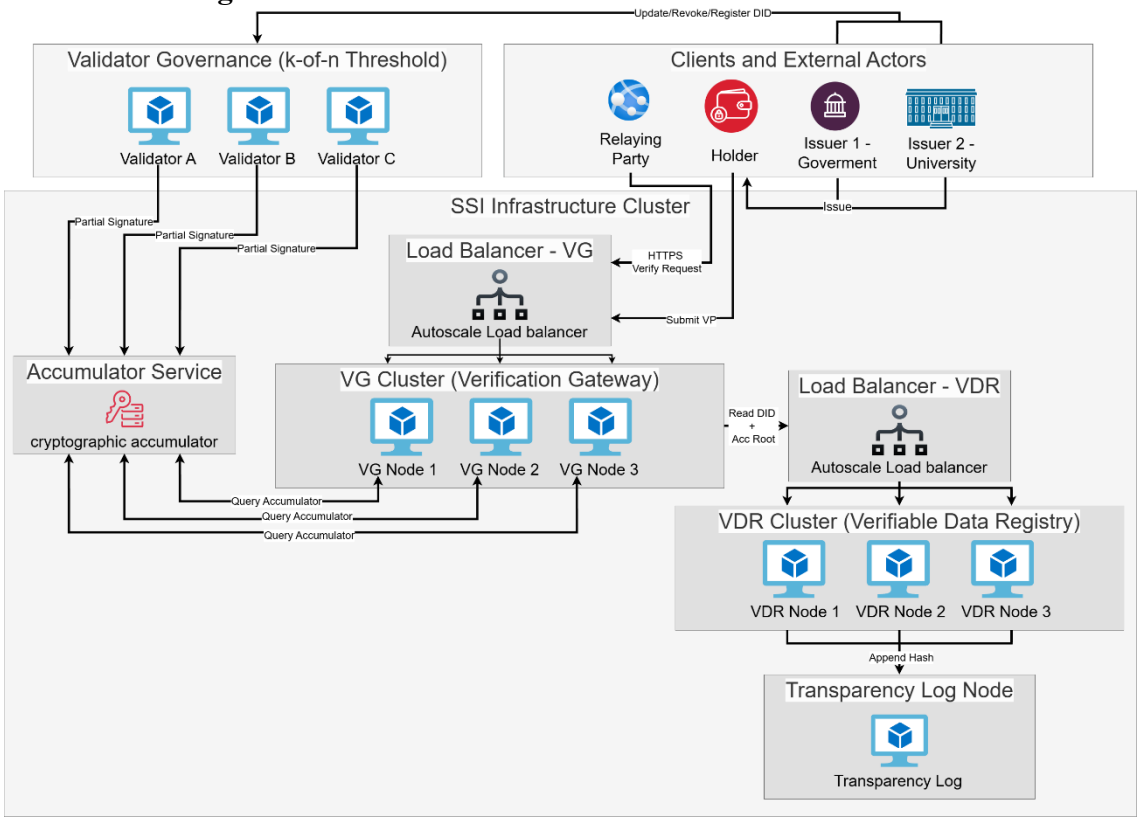
Di ranah riset akademik, beberapa skema SSI telah diusulkan untuk mengatasi tantangan kedaulatan identitas dan regulasi. Salah satu skema penting adalah NSSIA (New Self-Sovereign Identity Scheme with Accountability), yang dirancang untuk menyeimbangkan antara privasi pengguna dan akuntabilitas. Dalam NSSIA, setiap pengguna memiliki "avatar digital" spesifik dengan biometrik, dan skema *threshold signature* digunakan agar beberapa otoritas regulasi bisa melakukan pengawasan seperti yang di ilustrasikan pada gamabr 2.2.13 (Lyu et al., 2022).

Skema lain yang menarik adalah konsep *SSI as a Service* (SSIaaS), yang diusulkan oleh (Ding & Sato, 2022). Dalam arsitektur ini, organisasi bisa mengadopsi SSI tanpa membangun infrastruktur ledger sendiri: penyedia SSIaaS akan menjalankan layanan issuer dan verifikator, kemudian organisasi klien cukup menggunakan API untuk menerbitkan kredensial dan memverifikasi identitas. Keuntungan utama adalah mengurangi biaya dan kompleksitas adopsi SSI sambil tetap menjaga desentralisasi dan kontrol pengguna.

BAB 3 METODOLOGI

3.1 Metode yang digunakan

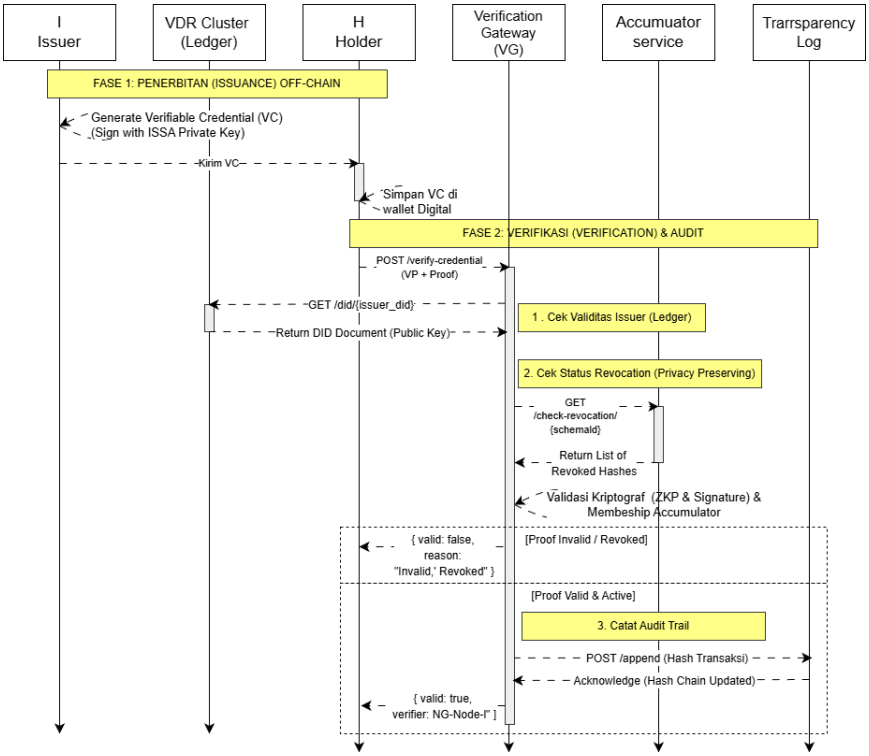
3.1.1.1 Rancangan Arsitektur Sistem



Gambar 3.1 Rancangan arsitektur sistem

Gambar 3.1 menggambarkan arsitektur lengkap sistem identitas digital berbasis Self-Sovereign Identity (SSI) yang terdiri dari empat komponen utama: (1) klien dan pihak eksternal, (2) validator governance dengan skema threshold, (3) Verification Gateway (VG) cluster, dan (4) Verifiable Data Registry (VDR) serta Transparency Log. Seluruh elemen ini bekerja sama untuk memastikan proses penerbitan, verifikasi, dan pencabutan credential dapat dilakukan dengan aman, terdistribusi, serta bebas dari *single point of failure*. Untuk penjelasan alur arsitektur akan di jelaskan pada subbab 3.1.1.1, 3.1.1.2, dan 3.1.1.3.

3.1.1.2 Issuance–Verification

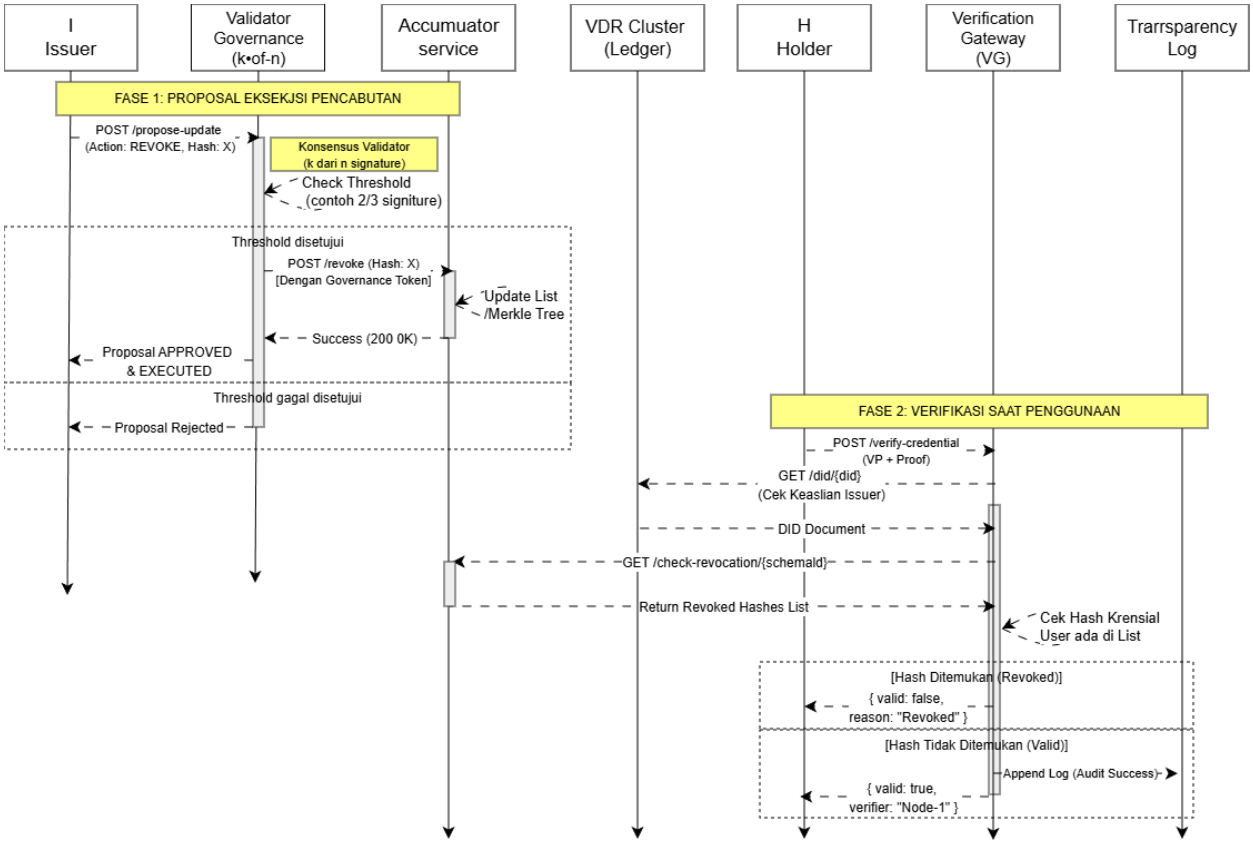


Gambar 3.2 Diagram alur penerbitan dan verifikasi

Gambar 3.2 menunjukkan alur penerbitan dan verifikasi credential dalam arsitektur SSI, beserta alasan mengapa setiap langkah diperlukan. Proses dimulai ketika Issuer membuat dan menandatangani *Verifiable Credential* (VC), karena hanya pihak berwenang yang dapat menjamin keaslian dan integritas data identitas. Kredensial kemudian disimpan oleh *Holder* di wallet lokal, sesuai prinsip SSI bahwa pengguna harus memegang kendali penuh atas identitasnya tanpa ketergantungan pada server terpusat. Ketika *Holder* (H) ingin mengakses layanan, *Relying Party* (RP) mengirimkan *challenge-code* sebagai bukti permintaan baru yang mencegah penyalahgunaan atau pengulangan (*anti-replay*). *Holder* menjawab *challenge* ini dengan membuat *Verifiable Presentation* (VP) yang hanya memuat atribut yang diperlukan (*selective disclosure*) dan menyertakan *challenge* sebagai nonce, sehingga bukti yang dikirim benar-benar terkait dengan permintaan tersebut.

VP dikirim ke *Verification Gateway* (VG), yang kemudian memverifikasi tanda tangan *Issuer* untuk memastikan bahwa data berasal dari sumber yang tepercaya, memeriksa status revocation untuk memastikan credential tidak dicabut, serta memvalidasi *Zero-Knowledge Proof* (ZKP) agar verifikasi dapat dilakukan tanpa mengungkap data pribadi yang tidak relevan. Jika seluruh pemeriksaan berhasil, VG menerbitkan token verifikasi sementara yang ditandatangani menggunakan *threshold signature* (k-of-n), mekanisme yang menjamin hasil verifikasi tidak dapat dipalsukan oleh satu *validator* saja dan meningkatkan ketahanan terhadap kompromi *node*. Token ini dikirim kembali ke *Holder* dan diteruskan kepada RP sebagai bukti sah bahwa identitas telah diverifikasi oleh infrastruktur yang tepercaya. Terakhir, aktivitas penting dicatat sebagai hash anonim pada *transparency log* untuk memastikan auditabilitas tanpa melanggar privasi, sehingga setiap tindakan dapat ditelusuri tanpa mengungkap identitas pengguna.

3.1.1.3 Revocation



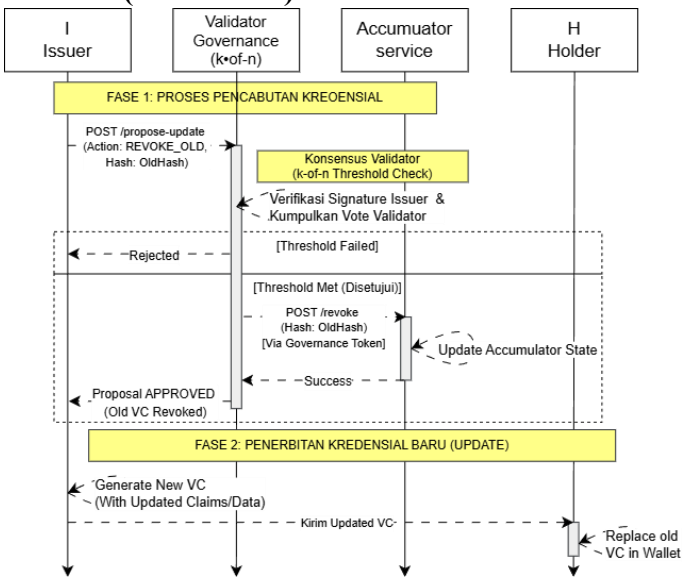
Gambar 3.3 Diagram alur pencabutan identitas

Gambar 3.3 memperlihatkan alur mekanisme revocation berbasis *cryptographic accumulator* tipe RSA/BLS, yang menyimpan representasi *hash credential* dan memungkinkan pembuktian *non-membership* melalui *Zero-Knowledge Proof* (ZKP). Proses dimulai ketika *Issuer* melakukan *revocation* dengan memasukkan *hash credential* ke *accumulator*, bukan *Credential ID*, sehingga ledger hanya menyimpan nilai matematis tunggal yang mewakili seluruh elemen set. Nilai *accumulator* baru (Acc_t) dipublikasikan secara *append-only*, memastikan riwayat perubahan tidak dapat diubah oleh satu pihak dan tetap aman untuk keperluan audit.

Setiap pembaruan *accumulator* mengharuskan *Holder* memperbarui *witness* miliknya, yaitu bukti matematis untuk menunjukkan kredensial miliknya tidak berada dalam daftar *revoked*. Pada *accumulator* RSA/BLS, *witness* dihitung ulang menggunakan operasi eksponensiasi modular atau *bilinear pairing*, sehingga perubahan sekecil apa pun pada *accumulator* membuat *witness* lama tidak valid. Mekanisme ini memastikan *Holder* tidak dapat menggunakan bukti lama, dan sistem dapat mendeteksi pemalsuan atau penyalahgunaan secara otomatis.

Saat verifikasi, *Holder* membuat *ZKP non-membership* menggunakan *witness* dan nilai *accumulator* terbaru. ZKP ini membuktikan bahwa kredensial tidak ada dalam *accumulator* tanpa mengungkap *Credential ID*, *hash*, atau isi VC. VP yang dikirim ke *Verification Gateway* (VG) berisi *selective disclosure* VC, *ZKP non-membership*, *signature Holder*, dan *nonce* dari RP. VG memverifikasi bukti dengan mengambil Acc_t dari *ledger*, memvalidasi *witness*, aturan matematika *accumulator*, *signature*, dan *nonce*. Jika valid maka credential dianggap tidak dicabut, jika tidak maka credential ditandai sebagai revoked.

3.1.1.4 Update Credential (Reissuance)



Gambar 3.4 Diagram alur pembaruan identitas

Gambar 3.4 menggambarkan alur pembaruan kredensial melalui mekanisme *reissuance*, bukan modifikasi langsung, karena *Verifiable Credential* (VC) bersifat *immutable* dan tidak bisa diubah setelah diterbitkan. Pendekatan ini menjaga integritas, auditability, dan jejak historis yang dapat diverifikasi, di mana setiap perubahan data dilakukan dengan mencabut VC lama dan menerbitkan VC baru.

Proses dimulai ketika *Holder* mengajukan pembaruan informasi, misalnya perubahan nama, alamat, atau atribut lain yang sudah tidak valid. *Issuer* kemudian mencabut VC lama dengan menulis *entri revocation* ke *Ledger/VDR*, menandai kredensial sebagai tidak berlaku tanpa menghapus data lama sehingga riwayat perubahan tetap dapat diaudit. *Ledger* mengonfirmasi pencabutan ini dengan memperbarui *status revocation* dan nilai accumulator untuk menjaga konsistensi verifikasi di masa depan.

Setelah VC lama dicabut, *Issuer* menerbitkan VC baru yang telah diperbarui, menandatanganinya, dan mengirimkannya ke Holder untuk disimpan di wallet. *Verification Gateway* (VG) memvalidasi VC baru dengan mengecek tanda tangan *Issuer*, *status revocation* di ledger, dan konsistensi DID kedua pihak. *Ledger* memastikan VC baru sah dan tidak berada dalam daftar *revocation*, sehingga VG dapat mengonfirmasi pembaruan berhasil dan kredensial terbaru dapat digunakan dengan aman.

3.2 Metode Evaluasi

Evaluasi kualitas rancangan sistem identitas digital berbasis SSI dilakukan melalui simulasi dan analisis konseptual, merujuk pada praktik-praktik dalam penelitian sebelumnya seperti NSSIA, SSIaaS, Walt.id SSI Benchmarking, Pan-Canadian Trust Framework, EUDI Wallet & eIDAS 2.0, serta rekomendasi W3C DID/VC.

3.5.1 Evaluasi Keamanan

Evaluasi keamanan bertujuan untuk menilai ketahanan rancangan arsitektur terhadap ancaman dasar dan potensi manipulasi, khususnya pada proses penerbitan, verifikasi, dan pencabutan kredensial. Analisis dilakukan melalui skenario ancaman representatif, simulasi

serangan terbatas, serta pemetaan ancaman menggunakan kerangka threat modeling yang relevan. Fokus evaluasi diarahkan pada kemampuan sistem dalam menjaga integritas data, keaslian kredensial, dan pencegahan penyalahgunaan mekanisme verifikasi.

3.5.2 Evaluasi Privasi

Evaluasi privasi difokuskan pada perlindungan data pengguna dan pencegahan pengungkapan informasi yang tidak diperlukan selama proses verifikasi. Analisis dilakukan dengan meninjau aliran data sepanjang siklus hidup kredensial, serta mengevaluasi efektivitas mekanisme privasi yang diusulkan, seperti *selective disclosure* dan penggunaan *zero-knowledge proof*. Pendekatan evaluasi mengacu pada prinsip *privacy-by-design* dan kerangka penilaian privasi yang digunakan dalam standar SSI modern.

3.5.3 Evaluasi Kinerja

Evaluasi kinerja dilakukan untuk memberikan gambaran karakteristik performa arsitektur yang diusulkan, berdasarkan hasil simulasi dan eksperimen terbatas di lingkungan terkontrol. Parameter kinerja yang diamati mencakup waktu pemrosesan pada tahap penerbitan dan verifikasi kredensial, serta dampak mekanisme keamanan terhadap efisiensi sistem secara umum. Evaluasi ini tidak bertujuan untuk mengukur performa sistem berskala produksi, melainkan untuk mengidentifikasi tren dan potensi bottleneck pada rancangan arsitektur.

3.5.4 Evaluasi Desentralisasi dan Model Kepercayaan

Evaluasi desentralisasi dan model kepercayaan bertujuan untuk menilai sejauh mana rancangan sistem menghindari ketergantungan pada satu entitas tunggal serta mendistribusikan kontrol dan kewenangan secara proporsional. Analisis dilakukan dengan meninjau struktur governance, peran validator, dan batas kepercayaan antar komponen sistem. Hasil evaluasi dibandingkan secara konseptual dengan praktik dan model kepercayaan yang digunakan pada kerangka SSI modern dan standar internasional yang relevan.

3.3 Bahan dan peralatan yang digunakan

3.3.1 Laptop

Digunakan untuk pemodelan, pembuatan diagram, dan pengujian lokal dilakukan pada laptop dengan spesifikasi sebagai berikut:

- Merek: HP Victus 16-s00010ax
- CPU: AMD Ryzen 7 7840HS
- GPU: NVIDIA GeForce RTX 4060 8 GB dan Radeon 780M Graphics 512 MB
- RAM: 24 GB
- SSD: 1024 GB

3.3.2 Server

Digunakan untuk simulasi *node* terdistribusi dan lingkungan multi-validator dilakukan pada Server dengan spesifikasi sebagai berikut:

- CPU: Intel Core i9-14900K
- GPU: NVIDIA GeForce RTX 4060 8 GB
- RAM: 128 GB
- SSD & HDD: 1024 GB & 2048 GB

3.3.3 Perangkat Lunak Pendukung

Beberapa software pendukung yang digunakan antara lain dan tidak terbatas pada Docker, Draw.io, VS Code, Kubernetes.

3.4 Tahapan Penelitian

Tahapan penelitian dijelaskan sebagai berikut:

3.4.1 Perancangan Kebutuhan dan Spesifikasi Sistem

Menentukan kebutuhan fungsional dan non-fungsional berdasarkan arsitektur SSI yang telah dirancang. Hasilnya digunakan sebagai dasar implementasi seluruh komponen sistem.

3.4.2 Implementasi Arsitektur SSI

Membangun seluruh komponen arsitektur seperti VDR, VG, accumulator, transparency log, dan load balancer sesuai gambar 3.1. Setiap komponen diinstansikan menggunakan Docker atau Kubernetes untuk mensimulasikan lingkungan terdistribusi.

3.4.3 Implementasi Alur Kredensial

Merealisasikan alur *issuance*, *verification*, *revocation*, dan *update* sesuai gambar 3.2, 3.3, dan 3.4.

3.4.4 Implementasi Mekanisme Keamanan

Mengimplementasikan tanda tangan kriptografi, ZKP, accumulator, transparency log, dan threshold signatures.

3.4.5 Pengujian Keamanan dan Privasi

Melakukan pengujian terhadap manipulasi *revocation*, *replay attack*, korelasi identitas, dan ketahanan validator. Hasil pengujian mengevaluasi efektivitas mekanisme keamanan dan privasi.

3.4.6 Evaluasi Sistem

Membandingkan hasil implementasi dengan standar modern seperti W3C, eIDAS 2.0, dan PCTF. Evaluasi mencakup aspek keamanan, privasi, kinerja, dan desentralisasi.

3.4.7 Penyusunan Laporan

Mendokumentasikan seluruh proses, hasil implementasi, dan evaluasi secara sistematis. Laporan disusun sebagai keluaran akhir penelitian.

3.5 Jadwal Penelitian

Tabel 3.1 Jadwal Penelitian

No	Kegiatan Penelitian	Feb	Mar	Apr	Mei
1	Perancangan Kebutuhan dan Spesifikasi Sistem				
2	Implementasi Arsitektur SSI				
3	Implementasi Alur Kredensial				
4	Implementasi Mekanisme Keamanan				
5	Pengujian Keamanan dan Privasi				
6	Evaluasi Sistem				
7	Penyusunan laporan				

DAFTAR PUSTAKA

Adrian Doerk. (2024, June). EUDI-Wallet: Illustration of the eIDAS roles and relationships. *Lissi*. https://www.lissi.id/blog/eudi-wallet-illustration-of-the-eidas-roles-and-relationships

Andrej Novak. (2025). Designing Decentralized Identity Systems with Self-Sovereign Principles. *ACE Journal*.

Ayang Macdonald. (2025, November 5). DIACC certifies ID verification for legal industry to Canada's trust framework [News]. *BIOMETRIC UPDATE*. https://www.biometricupdate.com/202511/diacc-certifies-id-verification-for-legal-industry-to-canadas-trust-framework

Buldini, A., Mazzocca, C., Montanari, R., & Uluagac, S. (2025). *Compact and Selective Disclosure for Verifiable Credentials* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2506.00262

bundesdruckerei. (2024). Self-sovereign identity: Data sovereignty in the digital world [Goverment]. *Bundesdruckerei*. https://www.bundesdruckerei.de/en/innovation-hub/self-sovereign-identity-data-sovereignty-digital-world?utm_source=chatgpt.com

Chaterine, R. N. & Prabowo, D. (2021, Mei). Kemenkominfo Duga 279 Juta Data Penduduk yang Bocor Identik dengan Data BPJS Kesehatan. *Kompas*. https://nasional.kompas.com/read/2021/05/21/15192491/kemenkominfo-duga-279-juta-data-penduduk-yang-bocor-identik-dengan-data-bpjs

Christopher Allen. (2016, April 26). *The Path to Self-Sovereign Identity*. Life With Alacrity. https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/

Decentralized Identity – A look into Decentralized Identity (DID). (2019, July 2). https://anarsolutions.com/decentralized-identity/

Dheeraj Panyam. (2025, February 11). Difference between OAuth vs SAML vs OpenID. *D3Vtech*. https://www.d3vtech.com/insights/difference-between-oauth-vs-saml-vs-openid/

DIACC. (2021, October 20). *BC Government's Verifiable Credential Issuer Kit Proof of Concept Report*. DIACC. https://diacc.ca/wp-content/uploads/2021/10/DIACC_BC-Governments-Verifiable-Credential-Issuer-Kit_Proof-of-Concept-Report_ENG.pdf

DIACC's Trust Framework Expert Committee. (2023, April 19). *Pan-Canadian Trust Framework*. DIACC. https://diacc.ca/wp-content/uploads/2024/10/PCTF-Digital-Wallet_Final-Rec-V1.0_Compressed_ENG.pdf

DIACC's Trust Framework Expert Committee. (2024). *PCTF Privacy Final Recommendation V1.2*. DIACC. https://diacc.ca/wp-content/uploads/2024/10/PCTF-Privacy_Final-Rec-V1.2_Compressed_ENG.pdf

Ding, Y., & Sato, H. (2022). Self-Sovereign Identity as a Service: Architecture in Practice. *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, 1536–1543. https://doi.org/10.1109/COMPSAC54236.2022.00244

El Maliki, T., & Seigneur, J.-M. (2007). A Survey of User-centric Identity Management Technologies. *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*, 12–17. https://doi.org/10.1109/SECUREWARE.2007.4385303

European Union Agency for Cybersecurity. (2022). *Digital identity: Leveraging the SSI concept to build trust.* Publications Office. https://data.europa.eu/doi/10.2824/8646

Fathur Rochman & Siti Zulaikha. (2023, July 17). Kemenkominfo periksa dugaan bocornya 337 juta data kependudukan. *ANTARA*. https://www.antaranews.com/berita/3639033/kemenkominfo-periksa-dugaan-bocornya-337-juta-data-kependudukan

Gaidhani, S., & Gopal Krishna Sharma, Dr. (2025). Comparative Analysis of Self-Sovereign Identity (SSI) Solutions. *INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS*, *13*(7). https://doi.org/10.56975/ijcrt.v13i7.291952

Giannopoulou, A. (2023). Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity. *Digital Society*, *2*(2), 18. https://doi.org/10.1007/s44206-023-00049-z

Giannopoulou, A., & Wang, F. (2021). Self-sovereign identity. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1550

Grech, A., Camilleri, A. F., Inamorato dos Santos, A., & European Commission (Eds.). (2017). *Blockchain in education*. Publications Office. https://doi.org/10.2760/60649

Hyperledger Indy maintainer and contributor. (2025, February 11). *Indy DID Method*. Github. https://github.com/hyperledger/indy-did-method

IDunion. (n.d.). IDunion Human-centric Vaccination & Immunization Management using Verifiable Credential. *OwnYourData*.

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, *51*(8), 56–59. https://doi.org/10.1109/MC.2018.3191268

Jeonghyuk Lee, Jaekyung Choi, Jihye Kim, & Hyunok Oh. (2021). *Privacy-preserving Identity Management System*. https://eprint.iacr.org/2021/1459.pdf

Jerry Fishenden. (2020). *Federated Identity for Access to UK Public Services 1997-2020*.

Joseph Cutler, J. DAX HANSEN, & CHARLYN HO. (n.d.). *Self-Sovereign Identity and Distributed Ledger Technology: Framing the Legal Issues*. Perkins Coie LLP. Retrieved November 18, 2025, from https://perkinscoie.com/sites/default/files/media/Perkins-Coie-Self-Sovereign-Identity-and-Distributed-Ledger-Tech_0.pdf

Liu, J., Liang, Z., & Lyu, Q. (2024). Empowering Privacy Through Peer-Supervised Self-Sovereign Identity: Integrating Zero-Knowledge Proofs, Blockchain Oversight, and Peer Review Mechanism. *Sensors*, *24*(24), 8136. https://doi.org/10.3390/s24248136

Lyu, Q., Cheng, S., Li, H., Liu, J., Shen, Y., & Wang, Z. (2022). NSSIA: A New Self-Sovereign Identity Scheme with Accountability. *Security and Communication Networks*, *2022*, 1–17. https://doi.org/10.1155/2022/1607996

M. Khory Alfarizi. (2023, Mei). *BSI Tak Bayar Tebusan Serangan Ransomware, LockBit Bocorkan Data Nasabah di Dark Web?* https://www.tempo.co/ekonomi/bsi-tak-bayar-tebusan-serangan-ransomware-lockbit-bocorkan-data-nasabah-di-dark-web--187473

Md. Sadek Ferdous. (2015). *User-controlled Identity Management Systems using mobile devices* [Doctoral (Phd Thesis), University of Glasgow]. https://theses.gla.ac.uk/6621/

Miyata, T., Yuzo KOGA, Paul MADSEN, Shin-ichi ADACHI, Yoshitsugu TSUCHIYA, Yasuhisa SAKAMOTO, & Kenji TAKAHASHI. (2006). A Survey on Identity Management Protocols and Standards. *IEICE Transactions on Information and Systems*, *E89-D*(1), 112–123. https://doi.org/10.1093/ietisy/e89-d.1.112

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Resnick, P., Zeckhauser, R., Swanson, J., & Lockwood, K. (2006). The value of reputation on eBay: A controlled experiment. *Experimental Economics*, *9*(2), 79–101. https://doi.org/10.1007/s10683-006-4309-2

Satybaldy, A., Nowostawski, M., & Ellingsen, J. (2020). Self-Sovereign Identity Systems: Evaluation Framework. In M. Friedewald, M. Önen, E. Lievens, S. Krenn, & S. Fricker (Eds.), *Privacy and Identity Management. Data for Better Living: AI and Privacy* (Vol.

576, pp. 447–461). Springer International Publishing. https://doi.org/10.1007/978-3-030-42504-3_28

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

Semenzin, S., Rozas, D., & Hassan, S. (2022). Blockchain-based application at a governmental level: Disruption or illusion? The case of Estonia. *Policy and Society*, *41*(3), 386–401. https://doi.org/10.1093/polsoc/puac014

Siqueira, A., Da Conceição, A. F., & Rocha, V. (2023). Empirical Evaluation of Self-Sovereign Identity Technology. *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1–4. https://doi.org/10.1109/ICBC56567.2023.10174979

Sovrin Foundation. (2018, December 8). Is Sovrin 'Permissioned'? [Non-profit project]. *Is Sovrin 'Permissioned'?* https://sovrin.org/faq/is-sovrin-permissioned

Sovrin Foundation. (2020, February 4). Second pillar of an SSI network: Network operations [Non-profit project]. *Second Pillar of an SSI Network: Network Operations*. https://sovrin.org/second-pillar-of-an-ssi-network-network-operations

Sovrin Foundation. (2023, August). *Sovrin Governance Framework*. Sovrin Foundation. https://sovrin.org/library/sovrin-governance-framework/?utm_source=chatgpt.com

Tim Bouma. (2020, February 25). Version 1.1 of the Pan-Canadian Trust Framework is now available. *Medium*. https://trbouma.medium.com/version-1-1-of-the-pan-canadian-trust-framework-is-now-available-feacc883d190

Truvera. (2025, November 14). *Self-Sovereign Identity: The Ultimate Guide 2025*. https://www.dock.io/post/self-sovereign-identity

Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, No. 27 (2022). https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

World Wide Web Consortium (W3C). (2019, August 10). *Decentralized Identifiers (DIDs) v0.13*. World Wide Web Consortium (W3C). https://w3c-ccg.github.io/did-spec/CGFR/2019-08-10

World Wide Web Consortium (W3C). (2022, July 19). *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations*. W3C Recommendation. https://www.w3.org/TR/did-core/

World Wide Web Consortium (W3C). (2025a, April 3). *Sovrin DID Method Specification*. World Wide Web Consortium (W3C). https://sovrin-foundation.github.io/sovrin/spec/did-method-spec-template.html

World Wide Web Consortium (W3C). (2025b, May 15). *Verifiable Credentials Data Model v2.0*. W3C Recommendation. https://www.w3.org/TR/vc-data-model/