SISTEM IDENTITAS DAN PROFIL WAJIB PAJAK BERBASIS SSI (*SELF-SOVEREIGN IDENTITY*) UNTUK KEABSAHAN, KEAMANAN DAN KEMUDAHAN AKSES

UJIAN KUALIFIKASI

I MADE SUGIADA

NPM : 99222006

PROGRAM DOKTOR TEKNOLOGI INFORMASI
UNIVERSITAS GUNADARMA
JUNI 2024

DAFTAR ISI

BAB I. PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Batasan dan Tujuan 4
1.3. Kontribusi 4
BAB II. TINJAUAN PUSTAKA 6
2.1. Sistem Manajemen Identitas Umum 6
2.2. Sistem Manajemen Identitas Terdesentralisasi 9
2.3. Perbandingan Sistem Manajemen Identitas 14
BAB III. METODOLOGI 16
3.1. Motivasi 16
3.2. Framework Riset 16
3.3. Pendekatan 20
DAFTAR PUSTAKA 21

BAB I. PENDAHULUAN

1.1. Latar Belakang

Direktorat Jenderal Pajak (DJP) telah memanfaatkan teknologi informasi dalam menjalankan administrasi perpajakan sejak tahun 1999. Dalam kurun waktu lebih dari 20 tahun, DJP memiliki basisdata wajib pajak yang lengkap dan bisa dijadikan dasar untuk membentuk informasi profil wajib pajak yang komprehensif. Inisiatif terkait hal ini sudah mulai dilakukan sejak tahun 2017 dalam bentuk pengembangan *Taxpayer Account Management* (*TAM*). *TAM* merupakan terminologi umum pengembangan profil wajib pajak yang diimplementasikan baik untuk aplikasi internal DJP (yang digunakan oleh pegawai), maupun aplikasi eksternal DJP (yang digunakan oleh wajib pajak). *TAM* untuk aplikasi internal DJP terdiri dari 3 modul yaitu *Revenue Accounting System (RAS), Taxpayer Profile,* dan *Potential Revenue.* Untuk bagian TAM yang ditampilkan ke wajib pajak melalui aplikasi eksternal DJP (DJP Online) diberi nama e-TPA / *Electronic Taxpayer Account* (DJP, 2021).

Sejak tahun 2020, e-TPA mulai dipasang di DJP Online untuk melengkapi informasi profil wajib pajak yang sebelumnya sudah ada. Informasi profil wajib pajak yang sebelumnya hanya berisikan npwp, nama, alamat dan informasi umum lainnya, dengan adanya e-TPA wajib pajak dapat melihat informasi detil tentang riwayat pelaporan SPT (Surat Pemberitahuan), riwayat pembayaran pajak dan hutang pajak. Informasi ini sangat berguna bagi wajib pajak untuk mengetahui status kepatuhannya. Kedepan dalam sistem informasi DJP yang baru (yang saat ini sedang dikembangkan), informasi profil wajib pajak akan lebih lengkap lagi dengan konsep yang diberi nama *360^0 Taxpayer Overview* (Tim PSIAP DJP, 2022).

Data yang terkandung dalam profil wajib pajak, khususnya data SPT dapat merepresentasikan aktifitas ekonomi yang dilakukan oleh wajib pajak. Data ini sangat bagus untuk melihat apakah seorang wajib pajak memiliki kemampuan ekonomi yang baik atau tidak. Oleh karena itu, ada keinginan dari pihak ketiga khususnya jasa keuangan (perbankan dan pemberi pinjaman) untuk menjadikan data omzet pada SPT sebagai salah satu rujukan dalam melakukan proses *credit scoring*.

Saat ini keinginan di atas sangat sulit dipenuhi karena alasan-alasan berikut:

1. DJP terikat dengan aturan pasal 34 ayat 1 Undang-undang Nomor 28 Tahun 2007 tentang Ketentuan Umum Perpajakan (UU KUP) yang menyatakan : "Setiap pejabat dilarang memberitahukan kepada pihak lain segala sesuatu yang diketahui atau diberitahukan kepadanya oleh wajib pajak dalam rangka jabatan atau pekerjaannya untuk menjalankan ketentuan peraturan perundang-undangan perpajakan". Ini artinya DJP tidak bisa memberikan data wajib pajak kepada pihak manapun, kecuali untuk keperluan tertentu yang diatur secara khusus oleh undang-undang;
2. Sistem informasi yang dimiliki DJP saat ini merupakan sistem terpusat dan berbasis web. Layanan yang disediakan untuk wajib pajak adalah untuk keperluan pemenuhan kewajiban perpajakan mulai dari proses pendaftaran, penghitungan pajak, pembayaran dan pelaporan pajak. Tidak tersedia fasilitas bagi wajib pajak untuk mendapatkan data profilnya sendiri secara sah untuk keperluan selain perpajakan.

Pada tahun 2022 lahir suatu undang-undang yang memberikan perlindungan hukum terkait data perorangan yaitu Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Beberapa pasal yang mengatur tentang hak subjek data pribadi yaitu :

1. Pasal 7 : subjek data pribadi berhak mendapatkan akses dan memperoleh salinan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan;
2. Pasal 13 ayat 1 : subjek data pribadi berhak mendapatkan dan/atau menggunakan data pribadi tentang dirinya dari pengendali data pribadi dalam bentuk yang sesuai dengan struktur dan/atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik;
3. Pasal 13 ayat 2 : subjek data pribadi berhak menggunakan dan mengirimkan data pribadi tentang dirinya ke pengendali data pribadi lainnya, sepanjang sistem yang digunakan dapat saling berkomunikasi secara aman sesuai dengan prinsip pelindungan data pribadi berdasarkan undang-undang ini.

Melihat ketentuan pada undang-undang perlindungan data pribadi di atas, negara telah menjamin setiap individu berhak atas kepemilikan dan pemanfaatan data pribadinya sendiri. Jika dicek kembali ketentuan pada pasal 34 ayat 1 UU KUP, yang dilarang untuk memberikan data wajib pajak adalah petugas pajak. Jika yang memberikan data profil wajib pajak kepada pihak lain adalah wajib pajak sendiri, maka tidak ada peraturan yang melarang hal tersebut.

Dengan kondisi di atas, maka perlu dibuatkan suatu metode baru dalam mengelola informasi profil wajib pajak. Metode baru tersebut diharapkan dapat mengakomodir kebutuhan wajib pajak dan pihak ketiga sesuai dengan ketentuan pada undang-undang perlindungan data pribadi. Di sisi lain DJP tetap masih bisa patuh pada ketentuan pasal 34 ayat 1 UU KUP.

Beberapa tahun belakangan ini, berkembang suatu metode pengelolaan identitas pengguna yang dikenal dengan nama *Self-Sovereign Identity (SSI)*. SSI adalah pendekatan identitas baru terdesentralisasi yang memungkinkan entitas (misalnya individu, organisasi, dan objek) untuk sepenuhnya mengontrol identitas digital mereka tanpa bergantung pada otoritas eksternal (Cucko and Turkanovic, 2021). Dengan kata lain, tidak ada pihak yang mengatur berjalannya sistem, dan pengguna memiliki otoritas penuh untuk melakukan kontrol terhadap identitas dan atribut yang dimilikinya. Pendekatan ini sangat berbeda dengan sistem pengelolaan identitas tersentral maupun federasi, dimana identitas dibuat oleh pihak ketiga dan bukan oleh individu yang bersangkutan (Dib and Toumi, 2020). SSI dapat berkembang karena didukung oleh salah satu DLT (*Distributed Ledger Technologies*) yang cukup populer yaitu *blockchain*. Meskipun *blockchain* adalah teknologi yang relatif baru, *blockchain* memiliki sifat transparansi, kekekalan, kredibilitas, ketahanan terhadap gangguan, dapat ditelusuri, dan desentralisasi yang diperlukan untuk berbagai aplikasi, termasuk dalam hal ini untuk pengembangan SSI (Ahmed, et al., 2022).

Pada penelitian ini akan dilakukan perancangan sistem identitas dan profil wajib pajak, khususnya membuat modul baru yang memungkinkan wajib pajak membagikan profilnya sendiri kepada pihak lain dengan cara yang absah, aman dan mudah. Ruang lingkup penelitian dibatasi pada perancangan sistem identitas dan profil wajib pajak dengan menggunakan pendekatan SSI dan dibuatkan interoperabilitas dengan sistem informasi DJP.

Hasil perancangan di atas selanjutnya akan diuji dari aspek-aspek berikut :

1. Aspek Keabsahan / Validitas

   Untuk menguji apakah desain yang dibuat dapat menghasilkan identitas dan profil wajib yang absah / valid sesuai dengan ketentuan hak-hak subjek data pribadi yang ada pada Undang-undang Perlindungan Data Pribadi, dan tentunya juga memenuhi ketentuan pasal 34 ayat 1 Undang-undang KUP.
2. Aspek Keamanan

   Menguji keamanan data profil wajib pajak, baik saat disimpan secara terdistribusi maupun saat pengiriman data kepada pihak lain.

3. Aspek Kemudahan Akses

   Menguji kemudahan akses terhadap informasi profil wajib pajak pada desain yang dibuat, baik akses oleh wajib pajak sendiri maupun pihak yang diberikan informasi.

1.2. Batasan dan Tujuan

Penelitian ini dibatasi hanya melakukan perancangan sistem identitas dan profil wajib pajak dan mengujinya dari berbagai aspek. Alasan pembatasan ini adalah sebagai berikut :

1. Sistem informasi DJP sangat kompleks dan terdiri dari berbagai komponen, namun tidak keseluruhan komponen tersebut ada relevansinya dengan topik yang diteliti.
2. Penelitian ingin fokus hanya pada permasalahan yang dihadapi yaitu:
   a. Wajib pajak tidak memiliki kontrol penuh atas data profil dirinya yang disajikan oleh sistem informasi DJP, padahal di sisi lain ada undang-undang yang mengatur tentang hak-hak subjek data pribadi;
   b. DJP ingin memberikan layanan terbaik kepada wajib pajak dan masyarakat, namun ketentuan pasal 34 ayat 1 UU KUP tidak mengijinkan DJP untuk berbagi data wajib pajak kepada pihak lain selain kepada wajib pajak sendiri. Pengecualian terhadap hal ini hanya diberikan untuk keperluan tertentu, diatur dengan aturan yang sangat ketat, dan harus seijin Menteri Keuangan.

Tujuan penelitian ini adalah untuk mengetahui apakah Rancangan Sistem Identitas dan Profil Wajib Pajak yang dibangun menggunakan *framework SSI (Self-Sovereign Identity)* dapat menyelesaikan permasalahan yang dihadapi DJP terkait identitas dan profil wajib pajak, khususnya ditinjau dari aspek keabsahan, keamanan dan kemudahan akses.

1.3. Kontribusi

Penelitian ini diharapkan dapat memberikan kontribusi kepada berbagai pihak, antara lain:

1. Memberikan usulan metode baru kepada Direktortat Jenderal Pajak dalam mengelola identitas dan profil wajib pajak dengan cara yang sah secara hukum (tetap patuh pada ketentuan pasal 34 ayat 1 UU KUP), namun tetap dapat memberikan layanan yang terbaik kepada masyarakat (sesuai ketentuan pada Undang-undang Perlindungan Data Pribadi).

2. Bagi wajib pajak tercipta kedaulatan dan transparansi dalam pengelolaan data profilnya. Wajib pajak berwenang penuh atas data tersebut untuk digunakan sesuai kebutuhan wajib pajak.
3. Bagi masyarakat maupun pihak ketiga lainnya tersedia mekanisme yang sah untuk mendapatkan data wajib pajak tertentu sesuai dengan keperluannya.

BAB II. TINJAUAN PUSTAKA

2.1. Sistem Manajemen Identitas Umum

Solusi manajemen identitas umumnya dirancang untuk memfasilitasi pengelolaan identitas dan operasi digital seperti otentikasi, dan telah banyak digunakan dalam berbagai aplikasi (Liu et al., 2020). Sistem Manajemen Identitas (SMI) adalah kumpulan kebijakan dan teknologi yang bekerja sama untuk memastikan bahwa pengguna yang relevan dalam suatu organisasi memiliki akses ke sumber daya teknologi seperti aplikasi, sistem, layanan spesifik, data, dan platform *cloud* (Ahmed, et al., 2022). Tujuan dari penggunaan SMI adalah untuk meningkatkan keamanan data dan produktivitas sistem sekaligus menurunkan biaya, dan tugas yang berulang.

Sistem Manajemen Identitas yang sudah umum digunakan saat ini (SMI tradisional), memiliki arsitektur yang dapat dikelompokkan menjadi 3 jenis. Ilustrasi terkait arsitektur SMI dapat dilihat pada gambar 2.1 dan detil penjelasannya sebagai berikut (Liu et al., 2020) :

1. Arsitektur Manajemen Identitas Independen (Manajemen Identitas Terisolasi)

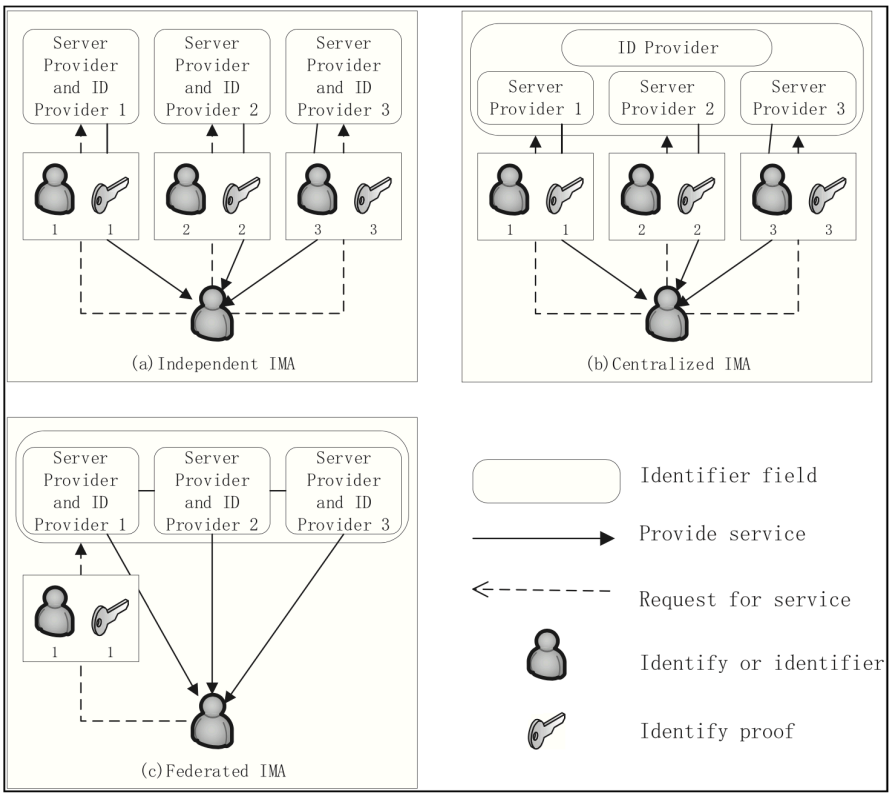
   Dalam arsitektur ini, setiap penyedia layanan memiliki data identitas penggunanya masing-masing. Dengan kata lain, identitas penyedia layanan yang berbeda tidak dapat dioperasikan. Meskipun strukturnya sederhana, namun tidak dapat diskalakan seiring bertambahnya jumlah penyedia layanan (misalnya implikasi terhadap kebutuhan penyimpanan di penyedia layanan). Arsitektur ini juga memerlukan kapasitas penyimpanan yang tinggi untuk setiap penyedia layanan (Seyam and Habbal, 2023). Selain itu, tidak praktis bagi pengguna untuk mengingat informasi identitas setiap penyedia layanan, tanpa menggunakan kembali atau mendaur ulang kredensial pengguna mereka.
2. Arsitektur Manajemen Identitas Tersentral

   Manajemen Identitas Tersentral hanya memiliki satu pengidentifikasi dan penyedia identitas di domain tepercaya. Artinya semua penyedia layanan di domain tepercaya yang sama akan berbagi identitas pengguna. Oleh karena itu, pengidentifikasi harus dipilih dengan cermat, dan identitas unik dalam domain tepercaya adalah pilihan yang umum. Penerapan sistem identitas terpusat saat ini begitu meluas (Dib and Toumi, 2020). Kebanyakan otentikasi saat ini dibuat melalui verifikasi yang cocok antara login dan kata sandi. Akun digital biasanya dibuat oleh pengguna dan disimpan dalam database penyedia layanan. Seorang pengguna biasanya

memiliki satu akun untuk setiap penyedia layanan. Kualitas data dalam sistem identitas tersebut bervariasi sesuai dengan kebijakan layanan.

3. Arsitektur Manajemen Identitas Federasi

   Arsitektur ini menetapkan domain tepercaya dan terdiri dari beberapa penyedia identitas di federasi. Domain tepercaya terdiri dari beberapa penyedia layanan dalam federasi yang mengenali identitas pengguna dari penyedia layanan lain. Misalnya, akademisi yang berbasis di AS dapat memilih untuk masuk ke Research.gov menggunakan informasi identitas National Science Foundation (NSF) atau kredensial organisasinya. Model ini memungkinkan pengguna untuk mendaftar satu kali dan membawa informasi identitas mereka ke penyedia layanan lain dengan menggunakan kumpulan kredensial yang sama (Seyam and Habbal, 2023). Contoh lain yang lebih umum adalah kemudahan bagi pengguna Facebook, mereka dapat memilih untuk masuk ke situs web lain menggunakan informasi identitas mereka untuk situs web tersebut atau informasi akun Facebook mereka (Ngo et al, 2023).



Gambar 2.1. Arsitektur Sistem Manajemen Identitas

Sistem Manajemen Identitas yang baik harus dapat memenuhi kriteria-kriteria yang ada pada hukum Cameron terkait identitas, yaitu (Liu et al., 2020) :

1. Kontrol dan Persetujuan Pengguna

   Sistem identitas teknis hanya boleh mengungkapkan informasi yang mengidentifikasi pengguna dengan persetujuan pengguna.
2. Pengungkapan Minimal untuk Penggunaan Terbatas

   Solusi yang mengungkapkan informasi identitas paling sedikit dan membatasi penggunaannya adalah solusi jangka panjang yang paling stabil.
3. Pihak yang Dapat Dibenarkan

   Sistem identitas digital harus dirancang sedemikian rupa sehingga pengungkapan informasi identitas dibatasi pada pihak-pihak yang mempunyai tempat yang diperlukan dan dapat dibenarkan dalam hubungan identitas tertentu
4. Identitas yang Diarahkan.

   Sistem identitas universal harus mendukung pengidentifikasi “omni-arah” untuk digunakan oleh entitas publik dan pengidentifikasi “searah” untuk digunakan oleh entitas swasta, sehingga memfasilitasi penemuan sekaligus mencegah pelepasan pegangan korelasi yang tidak perlu.
5. Pluralisme Operator dan Teknologi.

   Sistem identitas universal harus menyalurkan dan memungkinkan kerja sama berbagai teknologi identitas yang dijalankan oleh banyak penyedia identitas.
6. Integrasi Manusia.

   Identitas universal harus mendefinisikan pengguna manusia sebagai komponen sistem terdistribusi yang terintegrasi melalui mekanisme komunikasi manusia dan mesin yang menawarkan perlindungan terhadap serangan identitas.
7. Pengalaman yang Konsisten di Seluruh Konteks

   Identitas pemersatu harus menjamin penggunanya mendapatkan pengalaman yang sederhana dan konsisten sekaligus memungkinkan pemisahan konteks melalui berbagai operator dan teknologi.

Sistem Manajemen Identitas menjadi bagian penting dari sistem informasi suatu organisasi. Oleh karena itu banyak peneliti yang fokus melakukan penelitian pada bidang ini. Akibatnya

Sistem Manajemen Identitas secara terus menerus mengalami evolusi untuk mendapatkan sistem identitas yang baik dan sesuai kebutuhan. Ilustrasi terkait evolusi ini dapat dilihat pada gambar 2.2 (Ngo et al, 2023). Disamping ketiga jenis arsitektur di atas, beberapa tahun belakangan ini mulai hadir arsitektur yang lain yaitu Manajemen Identitas Berpusat Pada Pengguna dan Manajemen Identitas Terdesentralisasi. Arsitektur Manajemen Identitas Berpusat Pada Pengguna memberdayakan pengguna untuk mengontrol identitas digital mereka sendiri. Pengguna mempunyai hak untuk memilih kredensial mereka ketika merespons permintaan autentikasi atau atribut dan hal ini memberi pengguna lebih banyak hak dan tanggung jawab atas informasi identitas mereka. Selanjutnya untuk Manajemen Identitas Terdesentralisasi akan dijelaskan pada bagian di bawah ini.

Gambar 2.2. Evolusi Sistem Manajemen Identitas

2.2. Sistem Manajemen Identitas Terdesentralisasi

Pada Sistem Manajemen Identitas Umum di atas, identitas pengguna dibuat oleh pihak ketiga. Sebaliknya, dalam paradigma identitas terdesentralisasi, entitas itu sendiri ditempatkan sebagai inti pertukaran dan kebutuhan pihak ketiga untuk mengelola identitas dihilangkan (Dib and Toumi, 2020). Disinilah letak perbedaannya, Sistem Manajemen Identitas Terdesentralisasi memberikan otoritas penuh kepada pengguna untuk mengelola identitasnya.

Perkembangan Sistem Manajemen Identitas Terdesentralisasi ini sangat pesat dengan semakin matangnya teknologi *blockchain*. *Blockchain* awalnya populer karena menjadi platform implementasi mata uang kripto (Bitcoin dan berbagai mata uang kripto lainnya), namun dalam perkembangan selanjutnya digunakan untuk berbagai keperluan, salah satunya sebagai platform untuk manajemen identitas. Sebagai infrastruktur pusat untuk mata uang kripto, sistem blockchain menyimpan data dalam node dengan status yang sama dan bukan di server pusat. Setiap node memproses data secara independen, memastikan integritas sistem blockchain dan mengurangi

tekanan peningkatan volume data pada sumber daya sistem. Secara desain, *blockchain* terdesentralisasi karena keputusan tidak didasarkan pada satu titik, melainkan keputusan tersebut merupakan hasil konsensus dari node yang berpartisipasi dalam rantai.

Sistem Manajemen Identitas Terdesentralisasi berbasis *blockchain* ini terbagi dalam dua kategori yaitu SSI (*Self-Sovereign Identity*) dan DTI (*Decentralized Trusted Identity*). Meskipun SSI dan DTI serupa dalam banyak hal, SSI lebih banyak digunakan dalam konsep manajemen identitas berbasis *blockchain* (Ahmed, et al., 2022). Hal ini dikarenakan pendekatan SSI sangat memberikan kedaulatan penuh pada pengguna atas datanya.

2.2.1. SSI (*Self-Soveregin Identity*)

Individu dan organisasi menuntut kendali atas identitas mereka dan berkomunikasi sebagai mitra atau rekan kerja (Ahmed, et al., 2022). SSI memberikan peluang untuk mewujudkan hal tersebut. Pengguna dapat dengan bebas menggunakan dompet digitalnya untuk memverifikasi identitas sendiri tanpa menyerahkan kendali informasi pribadi ke banyak basisdata saat pengguna ingin mengakses produk layanan baru.

Ada 3 pilar dalam pendekatan SSI, yaitu (www.dock.io, 2023) :

1. *Blockchain*

   Basisdata terdesentralisasi yang dibagikan antar komputer di suatu jaringan dan mencatat informasi sedemikian rupa sehingga sangat sulit untuk mengubah, meretas, atau menipu sistem.

2. *Verifiable Credential (VC)*

   Kredensial versi digital yang sangat aman secara kriptografis dan dapat diberikan kepada pihak lain yang membutuhkannya untuk keperluan verifikasi.

3. *Decentralized Identifier (DID)*

   Pengidentifikasi yang dapat diverifikasi secara kriptografis, dibuat dan dimiliki oleh pengguna dan independen dari organisasi manapun. DID berbentuk teks dan tidak mengandung data pribadi.

Lebih lanjut, C. Allen mendetilkan properti yang harus dimiliki oleh sistem manajemen identitas dengan pendekatan SSI, sebagai berikut (Ahmed, et al., 2022) :

1. Keberadaan

   Pengguna dengan SSI harus memiliki identitas di dunia nyata. Setiap identitas online dikaitkan dengan identitas non-digital yang mewakili dan mengontrol identitas online.
2. Kontrol

   Pengguna harus memiliki kendali penuh atas identitas/kredensial mereka dan harus memiliki wewenang untuk independen dalam pilihan dan tindakan mereka.
3. Akses.

   Pengguna harus dapat mengakses data mereka dan mengklaimnya kembali kapan saja. Tidak ada perantara yang dapat mempengaruhi atau menyebarkan data jika mereka tidak memiliki akses terhadapnya.
4. Transparansi

   Prosedur sistem harus terbuka untuk berpartisipasi dan terbuka dalam tata kelola, sedangkan algoritmanya harus bersifat open source dan independen.
5. Keteguhan

   Karakter harus berumur panjang dan pengidentifikasi harus dapat diakses selama pemilik identitas menginginkannya.
6. Portabilitas

   Data SSI seperti layanan dan informasi harus dapat dipindahkan tanpa memerlukan pihak ketiga.
7. Interoperabilitas

   Identitas harus luas, tidak terbatas pada instansi mana pun, namun harus berfungsi pada sebanyak mungkin instansi atau layanan.
8. Persetujuan

   Pengguna harus memiliki persetujuan yang jelas tentang akses data. Pengguna harus selalu menentukan data mana yang akan dibagikan dan kepada siapa dengan memberikan persetujuannya.
9. Minimisasi

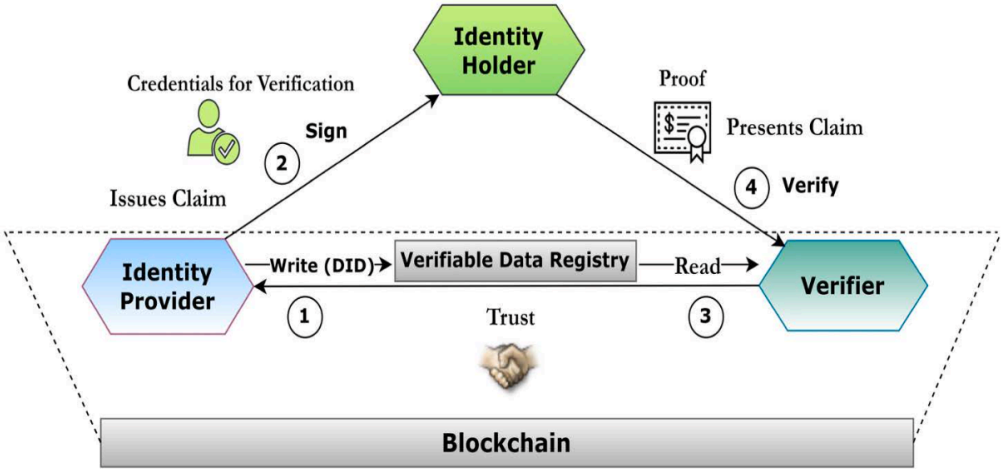
   Pengungkapan data klaim harus diminimalkan. Oleh karena itu, hanya jumlah terkecil yang diperlukan untuk menyelesaikan tugas yang diperlukan yang harus diungkapkan.
10. Perlindungan

    Hak-hak pengguna harus dilindungi dan dihormati jika terjadi konflik.

2.2.2. Verifiable Credential (VC)

Kredensial yang dapat diverifikasi (VC) adalah spesifikasi yang distandarisasi oleh kelompok kerja World Wide Web Consortium (W3C). Ini adalah alternatif digitalisasi yang aman secara kriptografis, dapat dibaca mesin, dan tahan terhadap kerusakan dibandingkan kredensial fisik di dunia nyata seperti paspor, KTP, atau SIM (Ahmed, et al., 2022). Ini adalah proses terdesentralisasi dan melibatkan interaksi struktur kepercayaan antara tiga aktor berbeda, yaitu pemegang identitas, penyedia, dan verifikator. Selain itu, terdapat registri data (VDR) yang dapat dibaca secara publik dan dapat diverifikasi, yang dapat berupa blockchain, DL, atau penyimpanan terdesentralisasi aman lainnya. Penyedia identitas (IdP) menerbitkan VC terutama yang berkaitan dengan individu atau terkadang organisasi. Verifikator spesifik itu sendiri yang menentukan apakah suatu penyedia dapat diandalkan atau tidak. Pihak tersebut dapat berupa pihak terpercaya seperti universitas, perusahaan tersertifikasi, bank, lembaga medis, atau lembaga pemerintah yang telah diberikan tingkat kepercayaan tertentu untuk menyampaikan informasi.

Seperti yang ditunjukkan pada Gambar 2.2 pada langkah (1) dan (2), IdP dapat mengeluarkan kredensial pribadi untuk pengguna dan menulis DID publik ke VDR. VC terdiri dari serangkaian klaim tentang atribut pemegang, seperti nama, tanggal lahir, ID, atau informasi terkait lainnya yang ingin diberikan penyedia kepada penerima. Entitas pemegang menerima VC berdasarkan permintaan dari penerbit dan memiliki kendali penuh atas pengendalian dan verifikasinya. Entitas pemegang mengelola kredensialnya di dompet digital yang dimiliki pemegangnya. Pada langkah (3) dan (4), verifikator memverifikasi integritas dan legitimasi kredensial pengguna tersebut ketika pengguna mengajukan klaim. Verifikator meminta kepada masing-masing pemegang tentang informasi identitas atau atributnya. Ia mengumpulkan bukti bahwa organisasi yang berwenang mengeluarkan VC dengan membaca catatan dari VDR. Situs web yang meminta kredensial dari kliennya adalah contoh verifikator. VDR dapat memodulasi pembuatan dan verifikasi identitas, kunci publik kriptografi, skema untuk VC, pencabutan registrasi, dan data terkait lainnya yang mungkin memerlukan penggunaan VC. Bantuan pengungkapan selektif oleh VC memungkinkan pemegang untuk mengautentikasi identitas mereka tanpa mengungkapkan lebih banyak informasi daripada yang mereka perlukan untuk melakukan tindakan tertentu. Pengungkapan selektif menggunakan metode *zero-knowledge proof* (ZKP) untuk menentukan sejauh mana data yang akan diungkapkan.



Gambar 2.2. *Framework* SSI dan alur kerja aktornya

2.2.3. Decentralized Identifier (DID)

Agar proses VC berfungsi, IdP, pemegang, dan verifikator diharuskan menggunakan Pengidentifikasi Terdesentralisasi (DID). Ini adalah mitra kriptografi untuk VC dan bekerja dengan VC untuk membuat kerangka SSI berfungsi dengan baik (Ahmed, et al., 2022). DID adalah pengidentifikasi kriptografi yang berbeda secara global, permanen, dan aman dari subjek DID. Ketika sebuah organisasi menerbitkan VC, mereka menyertakan DID publiknya. DID publik yang sama juga dicatat di *blockchain*, lihat langkah (1) dan (2) pada Gambar 2.2. Ketika pemegang berbagi VC dengan verifikator, verifikator dapat memeriksa DID di *blockchain* untuk melihat siapa yang memberikan kredensial, lihat langkah (3) dan (4) Gambar 2.2. Verifikator dapat melakukannya tanpa menghubungi pihak penyedia.

2.3. Perbandingan Sistem Manajemen Identitas

Pemilihan suatu metode atau pendekatan yang akan diimplementasikan tentunya ditentukan oleh berbagai faktor, khususnya kebutuhan organisasi itu sendiri. Pada tabel 2.1. disampaikan beberapa faktor yang menjadi pertimbangan untuk memilih Sistem Manajemen Identitas.

Tabel 2.1. Perbandingan Sistem Manajemen Identitas

Faktor	**Sistem Manajemen Identitas**			
	Independen	**Tersentral**	**Federasi**	**Terdesentralisasi**
Kompleksitas	Rendah, bisa diterapkan di setiap penyedia layanan dengan mudah	Sedang, perlu koordinasi dan kesepakatan dengan beberapa penyedia layanan yang menggunakan SMI ini	Tinggi, perlu koordinasi dan kesepakatan penyedia layanan dalam satu federasi.	Tinggi, perlu implementasi infrastruktur *blockchain*
Kemudahan Implementasi	Sederhana, langsung bisa diimplementasikan	Sedang, perlu membuat kesepakatan dengan bebebrapa penedia layanan	Tinggi, perlu membuat kesepakatan dengan beberapa penyedia layanan dalam satu federasi	Tinggi, perlu implementasi infrastruktur *blockchain*
Skalabilitas	Susah, hanya terbatas pada satu layanan saja	Sedang, bisa dilakukan skalabilitas untuk beberapa layanan	Sedang, bisa dilakukan skalabilitas untuk layanan dalam federasi	Mudah, karena hanya perlu bergabung pada infrastruktur *blockchain* (penambahan node relatif mudah)

Keamanan: sudut pandang organisasi	Rendah, data pengguna berada di setiap layanan, ada resiko pengambilan data yang tidak terkontrol.	Sedang, sangat rentan terhadap teori *single point of failure (SPOF)* karena tersentral	Sedang, sangat rentan terhadap teori *single point of failure (SPOF)* karena tersentral	Tinggi, tehindar dari SPOF karena data tersebar di berbagai *nodes*.
Keamanan: sudut pandang pengguna	Rendah, data pengguna berada di setiap layanan, ada resiko pengambilan data yang tidak terkontrol.	Sedang, untuk memperkuat pengamanan bisa ditambahkan 2FA (*Two Factor Authentication*)	Sedang, untuk memperkuat pengamanan bisa ditambahkan 2FA (*Two Factor Authentication*	Tinggi, secara alamiah *blockchain* sudah berbasis kriptografi (data sangat aman), tidak perlu tambahan metode pengaman lain lagi
Kemudahan Akses Informasi Pengguna	Sangat tergantung kebijakan organisasi	Sangat tergantung kebijakan organisasi	Sangat tergantung kebijakan organisasi	Mudah, karena kedaulatan dan kontrol penggunaan data ada di pengguna sendiri

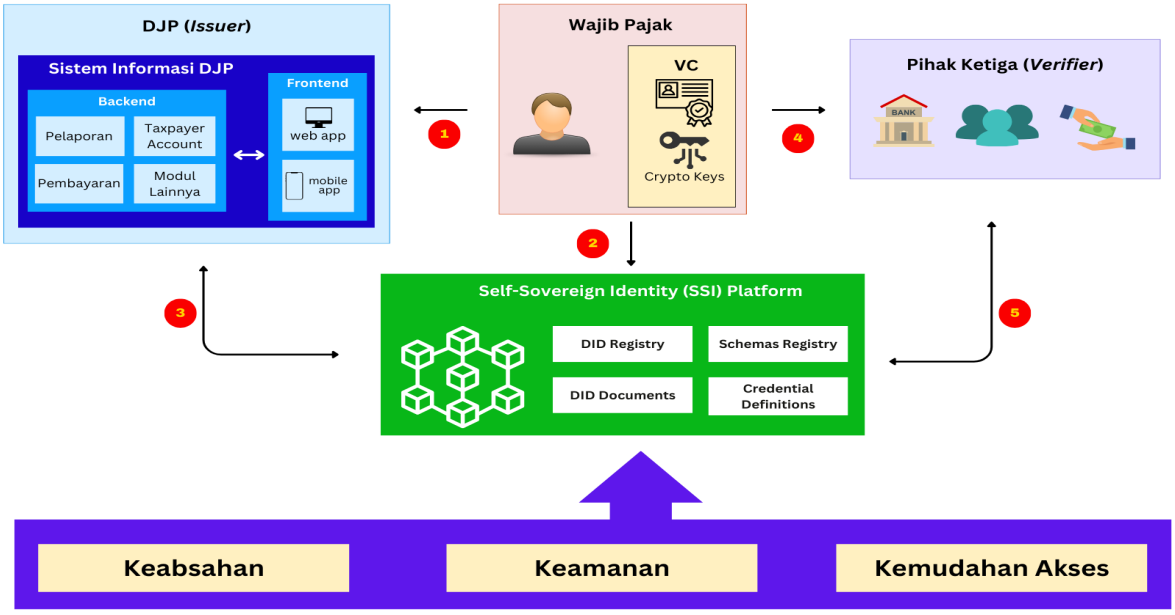
Sesuai dengan tujuan dari penelitian ini yaitu untuk memberikan kemudahan dan keamanan akses data oleh pengguna, maka pendekatan yang dipilih dalam penelitian ini adalah Sistem Manajemen Identitas Terdesentralisasi.

BAB III. METODOLOGI

3.1. Motivasi

SSI (*Self-Sovereign Identity*) adalah sebuah pendekatan identitas terdesentralisasi yang berpusat pada pengguna dan memanfaatkan teknologi terdesentralisasi yang sudah ada sebelumnya (Cucko and Turkanovic, 2021). Pendekatan ini menyediakan sarana identifikasi digital tanpa bergantung pada otoritas eksternal mana pun dan memungkinkan entitas untuk mengontrol identitas dan aliran data mereka selama interaksi digital sekaligus meningkatkan keamanan dan privasi. Dari sudut pandang penelitian akademis, Sistem Manajemen Identitas berbasis *blockchain* ini mendapatkan banyak perhatian dari para peneliti dan mereka mengusulkan berbagai solusi inovatif untuk keperluan identitas digital (Ahmed, et al., 2022). Para peneliti melakukan penelitian di berbagai bidang seperti lingkungan *cloud*, catatan kesehatan elektronik, IoT (*Internet of Things*), pendaftaran properti dan tanah, dan berbagai bidang lainnya. Berdasarkan penelusuran literatur, belum ditemukan penelitian yang mengimplementasikan SSI secara khusus pada bidang perpajakan. Hal inilah yang menjadikan motivasi untuk melakukan penelitian ini.

3.2. *Framework* Riset

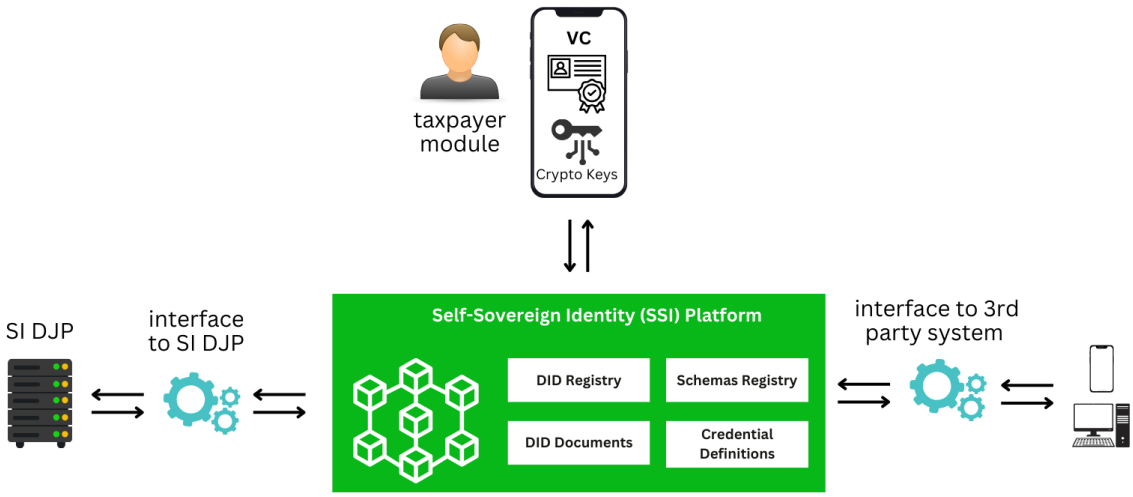


Gambar 3.1. Diagram SSI, Pengembangan Sistem Identitas dan Profil Wajib Pajak, dan Metode Pengujiannya

Pada penelian ini akan dilakukan pembuatan desain dan prototipe Sistem Identitas dan Profil Wajib Pajak, sekaligus melakukan pengujian dari aspek keabsahan, kemananan dan kemudahan akses. Secara umum cara kerja dari sistem yang akan dibangun adalah seperti pada gambar 3.1. dan penjelasannya sebagai berikut:

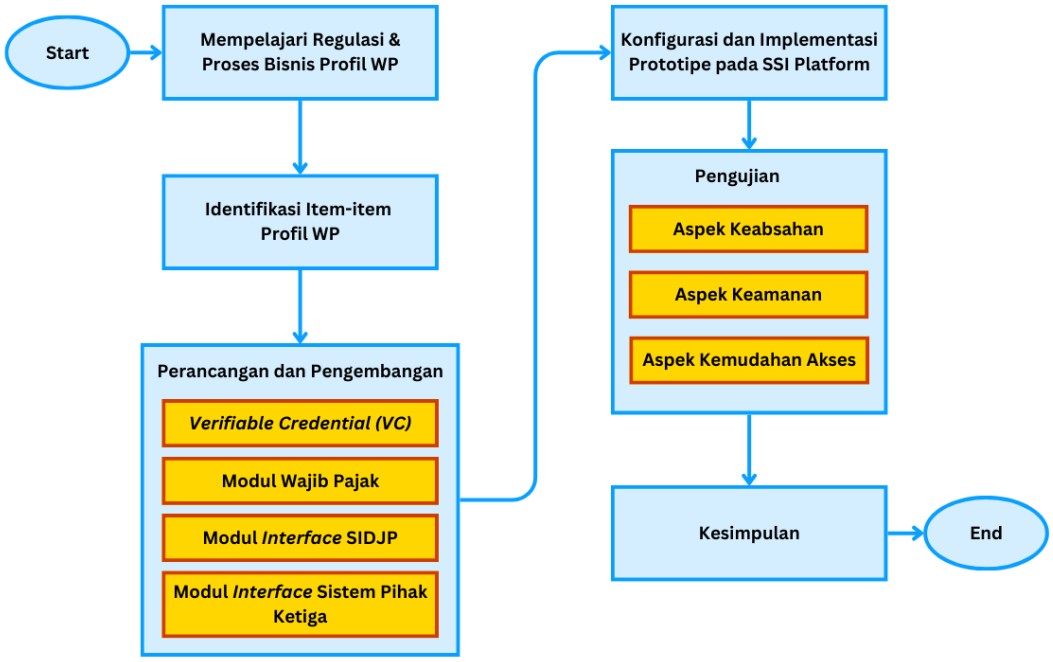
1. Wajib pajak (WP) melakukan transaksi pada Sistem Informasi DJP (SI DJP) dalam rangka pemenuhan kewajiban perpajakan seperti biasa, yaitu melakukan pendaftaran NPWP, pelaporan SPT, pembayaran pajak maupun pelayanan lainnya.
2. WP selanjutnya melakukan pendaftaran pada Sistem Identitas dan Profil Wajib Pajak melalui *user interface* yang terhubung ke SSI Platform. Pendaftaran ini akan menghasilkan DID yang tersimpan pada *device* WP (*smartphone*).
3. Pada SI DJP akan dibuatkan modul untuk mengkonversi profil WP kedalam bentuk *Verifiable Credential* (VC). VC selanjutnya akan ditempatkan pada *user storage* (*smartphone* milik WP).
4. WP yang telah memiliki profil WP dalam bentuk VC secara bebas dapat menggunakan VC tersebut untuk berbagai keperluan dengan pihak ketiga. WP bisa mengatur data mana saja yang akan diberikan kepada pihak ketiga, dengan memanfaatkan *crytpo key* yang ada padanya. Misalnya untuk keperluan peminjaman dana di Bank, VC dapat digunakan oleh pihak Bank untuk melakukan proses KYC (*Knowing Your Customer*).
5. Untuk memastikan keabsahan VC, pihak ketiga dapat melakukan validasi VC pada SSI Platform. Untuk keperluan ini akan dibuatkan modul *interface* yang dapat digunakan oleh pihak ketiga.

Berdasarkan cara kerja di atas, maka arsitektur Sistem Identitas dan Profil Wajib Pajak dapat dilihat pada gambar 3.2.



Gambar 3.2. Arsitektur Sistem Identitas dan Profil Wajib Pajak

Tahapan penelitian dapat dilihat pada diagram alir berikut ini :



Gambar 3.3. Diagram Alir Penelitian

Penjelasan tahapan penelitian adalah sebagai berikut :

1. Mempelajari regulasi dan proses bisnis yang ada di DJP terkait identitas dan profil wajib pajak.
2. Mengidentifikasi item-item profil wajib pajak yang bisa dikonversi kedalam bentuk VC (*Verfiable Credential*).
3. Melakukan perancangan dan pengembangan sistem identitas dan profil wajib pajak dengan tahapan sebagai berikut:
    a. Merancang dan mendefinisikan *Verifiable Credential* (VC) sesuai dengan hasil identifikasi item-item profil wajib pajak dan disesuaikan dengan standar W3C (*World Wide Web Consortium*).
    b. Merancang dan mengembangkan Modul Wajib Pajak. Modul ini akan digunakan oleh WP untuk melakukan pendaftaran, pengunduhan VC dan penyerahan VC kepada pihak ketiga.
    c. Merancang dan mengembangkan Modul *Interface* SI DJP yang menjembatani antara SI DJP dan SSI Platform. Tugasnya adalah mengambil dan mengkonversi profil WP kedalam bentuk VC dan megirimkannya ke SSI Platform, yang akan selanjutnya diteruskan ke *user storage* di Modul Wajib Pajak.
    d. Merancang dan mengembangkan Modul *Interface* Pihak Ketiga. Modul ini berupa *service* yang akan digunakan oleh pihak ketiga untuk melakukan validasi VC dari WP.
4. Menentukan SSI Platform yang akan digunakan dalam penelitian, melakukan konfigurasi dan *setting* sehingga bisa berkomunikasi dengan modul-modul yang telah dibuat.
5. Melakukan pengujian dari berbagai aspek, yaitu:
    a. Aspek Keabsahan

        Melakukan uji kualitatif terhadap prototipe untuk mengetahui apakah profil wajib pajak dalam bentuk VC yang dihasilkan oleh sistem ini sesuai dengan ketentuan hak-hak subjek data pribadi yang ada pada Undang-undang Perlindungan Data Pribadi, dan tentunya juga memenuhi ketentuan pasal 34 ayat 1 Undang-undang KUP. Metode yang digunakan adalah kuesioner kepada pihak-pihak pengampu peraturan tersebut.

b. Aspek Keamanan

Melakukan uji kuantitatif terhadap prototipe untuk mengetahui keamanan sistem yang dikembangkan. Pengujian keamanan menggunakan *security tools* yang dapat melakukan pengukuran secara kuantitatif.

c. Aspek Kemudahan Akses

Melakukan uji kualitatif terhadap prototipe untuk mengetahui kemudahan akses informasi profil wajib pajak dan mengukur pengalaman pengguna (*user experience*) baik oleh wajib pajak sendiri maupun pihak ketiga. Metode yang digunakan adalah kuesioner dan wawancara kepada perwakilan wajib pajak dan pihak ketiga (Perbankan dan Penyedia Jasa Aplikasi Perpajakan / PJAP).

3.3. Pendekatan

Pendekatan yang digunakan dalam penelitian adalah sebagai berikut :

1. Melakukan perancangan sistem identitas dan profil wajib pajak.
2. Membuat prototipe hasil rancangan dan mengimplementasikannya pada platform SSI.
3. Melakukan pengujian terhadap prototipe dari berbagai aspek. Pengujian menggunakan meotde kualitatif dan kuantitatif. Metode kualitatif berupa quesioner dan wawancara dengan berbagai pihak (internal DJP, wajib pajak dan pihak ketiga). Sedangkan metode kuantitatif digunakan untuk mengukur tingkat keamanan sistem yang dibuat.
4. Menyimpulkan hasil penelitian.

DAFTAR PUSTAKA

Ahmed, R. , Islam, A., Shatabda, S. and Islam, S. (2022). Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey. *IEEE Access*, 10, pp. 113436 - 113481. doi:https://doi.org/10.1109/ACCESS.2022.3216643.

Cucko, S. and Turkanovic, M. (2021). Decentralized and Self-Sovereign Identity: Systematic Mapping Study. *IEEE Access*, 9, pp.139009–139027. doi:https://doi.org/10.1109/access.2021.3117588.

Dib, O. and Toumi, K. (2020). Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions. *Annals of Emerging Technologies in Computing*, 4(5), pp.19–40. doi:https://doi.org/10.33166/aetic.2020.05.002.

Direktorat Jenderal Pajak. 2021. *Dokumen Kajian Pengembangan Taxpayer Account Management Modul Electronix Taxpayer Account*. DJP. Jakarta.

Liu, Y., He, D., Obaidat, M.S., Kumar, N., Khan, M.K. and Raymond Choo, K.-K. (2020). Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications*, 166, p.102731. doi:https://doi.org/10.1016/j.jnca.2020.102731.

Ngo, T., Dang, T., Huynh, V. and Le, T. (2023). A Systematic Literature Mapping on Using Blockchain Technology in Identity Management. *IEEE Access*, 11, pp. 26004 - 26032. doi:https://doi.org/ 10.1109/ACCESS.2023.3256519

Seyam, H and Habbal, A. (2023). A Systematic Review of Blockchain-based Identity Management Solutions. All Sciences Proceedings. Available at: https://as-proceeding.com/index.php/icras/article/view/712.

Undang-Undang Republik Indonesia Nomor 28 Tahun 2007 *Perubahan Ketiga Atas Undang-Undang Nomor 6 Tahun 1983 Tentang Ketentuan Umum dan Tata Cara Perpajakan.* 11 Juli 2007. Lembaran Negara Republik Indonesia Tahun 2007 Nomor 85. Jakarta.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 *Perlindungan Data Pribadi.* 17 Oktober 2022. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Jakarta.

Tim PSIAP DJP. 2022. *Ringkasan Materi Pelatihan Proses Bisnis Taxpayer Acoount Management* DJP. Jakarta.

www.dock.io. (2023). *Decentralized Identity: The Ultimate Guide 2023*. [online] Available at: https://www.dock.io/post/decentralized-identity.