Estudo sobre Self-Sovereign Identity

Pedro Eduardo Garbossa de Almeida[1], **Bruno Bogaz Zarpelão**[1]

[1]Departamento de Computação – Universidade Estadual de Londrina (UEL)
Caixa Postal 10.011 – CEP 86057-970 – Londrina – PR – Brasil

pedro.eduardo1604@uel.br, brunozarpelao@uel.br

Abstract. *In recent decades, centralized authentication has been widely employed in systems and platforms, presenting significant challenges in identity management, since users often lack control over their own data. This phenomenon, coupled with the growing use of various platforms and systems, has contributed to a substantial increase in data leakage incidents, culminating in serious privacy issues. In response to this scenario, there has been an increase in discussions aimed at improving digital identity management practices. In this context, the concept of Self-Sovereign Identity (SSI) stands out as an innovative approach to managing digital identities. This paper aims to carry out an in-depth analysis of SSI, identifying and discussing the fundamental challenges associated with its implementation. In addition, it seeks to demonstrate a concrete example of the application of SSI in a common scenario at the State University of Londrina.*

Resumo. *Nas últimas décadas, a autenticação centralizada tem sido amplamente empregada em sistemas e plataformas, apresentando desafios significativos no gerenciamento de identidades, uma vez que os usuários frequentemente carecem de controle sobre seus próprios dados. Este fenômeno, associado ao crescente uso de diversas plataformas e sistemas, tem contribuído para o aumento substancial de incidentes de vazamento de dados, culminando em sérias questões relacionadas à privacidade. Em resposta a esse cenário, tem-se verificado um aumento nas discussões voltadas para aprimorar as práticas de gestão de identidades digitais. Nesse contexto, destaca-se o conceito de Identidade Auto-Soberana (Self-Sovereign Identity - SSI) como uma abordagem inovadora para a administração de identidades digitais. O presente trabalho propõe-se a realizar uma análise aprofundada do SSI, identificando e discutindo os desafios fundamentais associados à sua implementação. Adicionalmente, busca-se demonstrar um exemplo concreto de aplicação do SSI em um cenário comum na Universidade Estadual de Londrina.*

1. Introdução

A era digital trouxe consigo uma série de avanços e transformações na forma como lidamos com a identidade e os dados pessoais. No entanto, o paradigma atual de autenticação e gestão de identidade frequentemente se baseia em sistemas centralizados, nos quais os usuários cedem o controle de seus dados a terceiros [9].

Neste contexto, surge o conceito de Self Sovereign Identity (SSI), uma abordagem inovadora que visa proporcionar aos usuários o controle total sobre suas próprias identidades digitais. No âmbito do SSI, os usuários detêm o poder de gerenciar e compartilhar

seus dados de forma segura e descentralizada, sem depender de autoridades centrais ou intermediárias [4]. Desse modo, tem-se um dos primeiros desafios na implementação do SSI: a curva de aprendizado. Isso se deve à transferência da responsabilidade pelo gerenciamento de chaves, do provedor centralizado para o usuário. Caso o usuário venha a perder essas chaves, isso resultará na perda irreversível de informações [9].

O presente trabalho propõe explorar e demonstrar uma solução baseada em SSI em um cenário específico dentro da Universidade Estadual de Londrina (UEL). O principal objetivo consiste em identificar e analisar os principais desafios inerentes à implementação do SSI em um contexto real.

Um dos desafios na adoção do SSI é estabelecer uma comunicação confiável entre as entidades responsáveis pela verificação e validação de credenciais digitais [9]. Por isso, serão investigadas tecnologias essenciais para o funcionamento eficiente do SSI, abrangendo a criptografia de dados, a tecnologia blockchain e o uso de identificadores descentralizados. A aplicação dessas ferramentas possibilitará o desenvolvimento de um sistema no qual os usuários poderão compartilhar apenas as informações necessárias para cada contexto específico, preservando sua privacidade e segurança.

2. Fundamentação Teórico-Metodológica e Estado da Arte

2.1. Privacidade

Privacidade é a habilidade que um indivíduo possui de controlar quais informações de si ele deseja ou não expor. Assim, o indivíduo possui a seletividade de determinar quais informações de si poderão ser usadas por terceiros [3].

Atualmente ocorre um ofuscamento das fronteiras da privacidade, e estamos em direção ao amplo acesso à informação. Com isso surge a necessidade de restringir o acesso a alguns dados [8]. Ao utilizar uma mídia social, o usuário coloca nela suas informações, com isso, é montado uma espécie de "portfólio" da sua pessoa. Esse portfólio pode ser trocado ou vendido para outras empresas ou até mesmo para o governo [3].

Devido a tudo isso, discursos sobre direito à privacidade vem tomando o cotidiano, pois uma característica bem presente nos dias de hoje é a exposição. As informações pessoais são cada vez mais acessíveis, tornando essa exposição ainda maior com as redes sociais [3]. A seletividade em compartilhar informações de forma restrita no espaço pessoal, acaba assumindo características diferentes neste ambiente digital. Neste cenário, é proporcionado novas maneiras de expressão, mas ao mesmo tempo, é aberto um caminho para novas formas de violação. Os dados que são compartilhados livremente na internet não podem mais ser totalmente recuperados para a esfera privada, pois o controle desses dados já não pode ser mais garantido [8]. Por isso, torna-se necessário que o usuário volte a ter controle sobre seus dados.

2.2. Gerenciamento de identidade

Com o progresso da era digital, tornou-se indispensável a utilização de plataformas de comércio eletrônico[1], instituições bancárias[2] e demais serviços online. Em decorrência

[1] https://neilpatel.com/br/blog/e-commerce-no-brasil/

[2] https://senhorcontabil.com.br/blog/impactos-do-crescimento-do-numero-de-bancos-dig

disso, observou-se uma ampla disseminação de dados, uma vez que, frequentemente, os usuários são requeridos a efetuar cadastros em cada site visitado [6]. Esses provedores de serviços utilizam mecanismos de autorização, os quais asseguram que apenas usuários autorizados terão acesso e poderão usufruir dos serviços oferecidos. Dessa forma, surgiu a necessidade do emprego de identidades digitais e de um método eficiente para seu gerenciamento [12].

Uma identidade digital é composta pela combinação de subconjuntos de informações, denominados identidades parciais. Alguns desses subconjuntos, como o Cadastro de Pessoa Física (CPF), são capazes de identificar alguém de forma única. A representatividade de uma identidade parcial é contextual e varia de acordo com o ambiente em que está inserida. Por exemplo, em uma instituição educacional, a identidade parcial pode conter informações como número de matrícula, curso e data de nascimento. Em contrapartida, em um ambiente corporativo, essa identidade parcial pode incluir dados como endereço, número de identificação, funções e privilégios específicos de um funcionário [12].

Por sua vez, um sistema de gerenciamento de identidades proporciona ferramentas para administrar essas identidades parciais no ambiente digital. Esse sistema é dotado de funcionalidades que permitem a administração, descoberta e troca de informações, garantindo a identificação de uma entidade e suas informações associadas. Cabe ao sistema decidir quais informações serão compartilhadas com outra entidade. Atualmente, existem quatro modelos de sistemas de gerenciamento de identidades: Tradicional, Federado, Centralizado e Centrado no Usuário [12] e [7].

- O modelo **Tradicional**: amplamente adotado por provedores de serviços, os provedores atuam como fornecedores e administradores de identidades digitais. Nesse formato, os usuários são solicitados a inserir suas informações, recebendo, em troca, uma identificação exclusiva para o provedor específico (como um login), neste modelo não há comunicação entre diferentes provedores. Esse modelo impõe custos significativos aos usuários e os expõe a um risco de segurança considerável, pois, em caso de vazamento de dados, todas as informações fornecidas pelos usuários podem ser comprometidas.
- O modelo **Federado**: surgiu como uma alternativa à inflexibilidade do modelo tradicional, fundamentando-se no compartilhamento de identidades digitais entre diversos provedores de serviços e na ideia de autenticação única. Exemplificando, destacam-se o Google Account[3] e o Microsoft Account[4], que disponibilizam apenas as informações essenciais para os diferentes provedores utilizados. Contudo, a desvantagem desse modelo reside no fato de que os usuários cederem o controle de seus dados a grandes corporações privadas.
- O modelo **Centralizado**: a autenticação de usuários é gerenciada por uma única entidade central, que atua como o ponto de controle para o acesso a sistemas e serviços. Nesse modelo, todas as credenciais e informações de autenticação são mantidas e gerenciadas por esse ponto central, muitas vezes referido como um servidor de autenticação. Dessa forma, nota-se que o risco desse modelo é que, se o servidor de autenticação falhar ou for comprometido, todo o sistema fica em

[3] `https://www.google.com/account/about/`
[4] `https://en.wikipedia.org/wiki/Microsoft_account`

risco.

- O modelo **Centrado no Usuário**: por sua vez, baseia-se na premissa de devolver ao usuário o controle de seus próprios dados. Nesse cenário, o usuário armazena suas identidades digitais em uma espécie de carteira digital, sendo ele mesmo o responsável por liberar as informações solicitadas por um provedor de serviço. Um exemplo de solução que adota esse modelo é o Windows CardSpace[5] que foi descontinuado pela Microsoft.

O modelo de gerenciamento de identidade que tem ganhado destaque nos tempos atuais é o modelo de identidades federadas. Essa abordagem otimiza a troca de informações relacionadas às identidades com base na confiança estabelecida entre as diferentes federações. É amplamente utilizado nos sistemas computacionais, pois o modelo tradicional tornou-se ineficiente e custoso para os usuários, que precisavam gerenciar e fornecer diversas informações em diferentes sistemas e provedores de serviços [12].

Um desafio recorrente associado a essa evolução é a questão da privacidade das informações. Os usuários frequentemente não têm o direito de determinar como e por quanto tempo suas informações serão manipuladas por diversas organizações, o que idealmente deveria ser possível em um cenário mais adequado [12] e [2].

2.3. SSI

Com o aumento significativo nos incidentes de vazamento de identidades digitais, torna-se evidente a ineficácia de alguns métodos existentes de gerenciamento de identidades. Diante desse cenário, observa-se uma crescente busca por abordagens mais seguras, com foco na preservação da privacidade. Nesse contexto, surge a Self-Sovereign Identity (SSI) [9].

Os elementos fundamentais da SSI incluem a ênfase na ampliação do controle do usuário sobre seus dados pessoais e na redução da dependência de serviços oferecidos por grandes corporações, como Google, Microsoft, entre outras, as quais atualmente detêm o controle da maioria das identidades digitais [4]. A SSI pode ser caracterizada por outros atributos [4]:

- O usuário detém o controle de suas identidades digitais;
- O usuário possui acesso absoluto aos seus dados;
- Transparência nos sistemas e algoritmos utilizados;
- Identidades digitais persistentes e portáveis.
- Garantia da proteção dos direitos pessoais.

Há dois componentes que são de extrema relevância no contexto do SSI, são eles: Credenciais Verificáveis (Verifiable Credentials - VCs) e os Identificadores Descentralizados (Decentralized Identifiers - DIDs) [5], os quais serão abordados nas seções 2.4 e 2.5, respectivamente.

[5] `https://en.wikipedia.org/wiki/Windows_CardSpace`

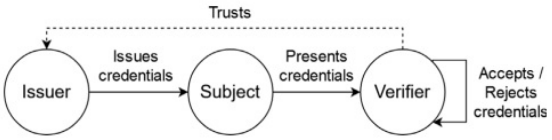

Figura 1. Demonstração do funcionamneto do SSI

A Figura 1 ilustra o processo de funcionamento do SSI e seus componentes. O processo se inicia com uma entidade emissora (*issuer*), que tem a autoridade para emitir e assinar VCs. Essas credenciais são emitidas em nome de um assunto (*subject*), que pode ser uma pessoa, uma organização ou um objeto, dependendo do contexto de uso. O papel do issuer é crucial, pois sua confiabilidade e autenticidade fornecem a base para a validade das credenciais emitidas. Uma vez emitidas, as VCs são atribuídas a um indivíduo (*holder*), que na maioria das vezes é o próprio assunto a quem as credenciais se referem. O holder é responsável por armazenar suas VCs de maneira segura, geralmente em uma carteira digital, e apresentá-las conforme necessário para provar sua identidade, qualificações ou propriedades. Quando um holder deseja acessar serviços ou comprovar uma informação, ele deve apresentar suas VCs a uma entidade verificadora (*verifier*). A função do verifier é examinar as credenciais apresentadas, validar a assinatura digital do issuer para garantir sua autenticidade e, com base nisso, decidir aceitar ou recusar as credenciais. Esta etapa assegura que apenas VCs válidas e emitidas por entidades confiáveis sejam aceitas [5].

Detalhando um exemplo em que se aplica o uso de SSI: após a compra de veículo, uma concessionária atua como o orgão emissor (issuer) ao criar uma credencial verificável (VC) que certifica a compra. Esta credencial contém detalhes importantes sobre o veículo, como descrição, modelo, cor, chassi, etc. Essencialmente, o veículo é o assunto (subject) da credencial, e o comprador é o titular (holder) dessa credencial. O comprador, agora titular da VC, armazena essa credencial de forma segura, em uma carteira digital protegida por criptografia. Quando o titular deseja emplacar o veículo, ele se dirige ao Departamento Estadual de Trânsito (Detran), que neste cenário atua como a entidade verificadora (verifier). Para o procedimento de emplacamento, o titular apresenta a VC emitida pela concessionária. O Detran, então, verifica a autenticidade da credencial, confirmando a validade da assinatura digital da concessionária e as informações contidas na VC.

Uma vez que a credencial é verificada e aceita pelo Detran, o veículo pode ser oficialmente emplacado. Este passo finaliza o processo de transferência de propriedade (no sentido administrativo) e legaliza o veículo para uso em vias públicas, tudo isso facilitado pela troca segura e verificável de informações digitais.

Ultimamente tem-se observado um aumento significativo nas plataformas de SSI [9], entre as quais se destacam o Blockstack [1], uma plataforma open-source de nomeação e armazenamento descentralizado construída com tecnologia Blockchain. A UPort[6] constitui-se como uma framework de SSI baseada na rede blockchain pública da Ethereum. Já a SelfKey[7] é uma outra rede SSI que proporciona aos usuários um

[6] `https://www.uport.me`
[7] `https://selfkey.org`

maior controle sobre seus dados pessoais, garantindo que apenas o mínimo necessário de informações seja compartilhado.

Conforme aumenta-se as discussões sobre SSI, nota-se que há muitos desafios a serem enfrentados, como por exemplo [9]:

- O gerenciamento de chave: nos sistemas tradicionais de gerenciamento de chave, o controle dos dados e chaves são de responsabilidade do provedor, já no SSI, é o usuário que detém suas chaves de acesso, portanto, caso o mesmo perca essas chaves, haverá perda de informações irrecuperáveis.
- Confiabilidade dos dados: os métodos de comunicação entre as entidades, incluindo as credenciais verificáveis trocadas devem ser cuidadosamente designadas. Essas autenticações devem ser feitas através de uma autoridade confiável e fora da rede de blockchain.
- Comercialização: Por ser uma novidade e estar em expansão, algumas entidades podem ficar relutantes quanto a adoção do SSI, por isso podem necessitar de suporte financeiro de algum serviço ou grande corporação para a adoção desta tecnologia.

2.4. Tecnologia VC

Credencial verificável (do inglês *Verifiable Credentials* - VC) pode representar exatamente as mesmas informações de uma credencial física, uma VC faz o uso de assinaturas digitais que provam criptograficamente quem a emitiu [9] e [10]. No contexto físico, uma credencial pode ser definida conforme [10]:

- Informações para Identificação de um Indivíduo: incluem elementos como fotografia, nome e CPF. Esses dados servem para distinguir claramente uma pessoa das demais, garantindo sua identificação de forma precisa e confiável.
- Identificação do Órgão Emissor: refere-se às entidades responsáveis pela emissão de documentos oficiais que validam diversas informações. Exemplos destes órgãos incluem o Instituto de Identificação do Paraná (IIPR) e o Departamento Estadual de Trânsito (Detran). Estes documentos emitidos contêm detalhes que apontam para a origem e a autoridade do órgão que os forneceu, assegurando sua autenticidade e confiabilidade.
- Tipo da Credencial: como Carteira Nacional de Habilitação (CNH), cartão do Sistema Único de Saúde (SUS) ou passaporte, define a natureza e o escopo das informações que ela contém. Cada uma dessas credenciais carrega consigo atributos específicos e serve para comprovar distintas competências ou identificações do portador.
- Atributos do Indivíduo Afirmados pelo Órgão Emissor: constituem elementos essenciais na validação da capacitação e identidade do mesmo. Tais atributos incluem, por exemplo, a categoria da habilitação, o número de identificação e a nacionalidade. Essas informações são conferidas pelo órgão emissor, servindo como meio de certificar as qualificações e a identidade do indivíduo.
- Evidência Relatando Como a Credencial Foi Designada: refere-se à documentação ou informações que atestam o processo pelo qual a credencial foi atribuída ou concedida. Essa evidência fornece detalhes sobre os procedimentos, critérios ou eventos que levaram à emissão da credencial. Como por exemplo, registros de transações, aprovações, verificações ou qualquer outra forma de

documentação que esclareça como a credencial foi concedida. Essa informação é crucial para validar a legitimidade e a autenticidade da credencial, permitindo uma compreensão transparente do processo de designação associado a ela.

- Restrições da Credencial: englobam limitações específicas impostas ao seu uso e validade. Exemplos notáveis incluem o período de validade da credencial e os termos de uso da mesma, que determinam as condições sob as quais a credencial pode ser utilizada. Estas restrições são fundamentais para garantir a aplicação correta e segura das credenciais dentro de seus contextos previstos.

O indivíduo (holder) que detém VC tem a capacidade de gerar Apresentações Verificáveis (do inglês *Verifiable Presentations* - VPs) e compartilhá-las com as entidades verificadoras com o intuito de comprovar efetivamente que possui VC com características específicas. Tanto a VC quanto as VPs podem ser transmitidas de maneira ágil, conferindo-lhes maior conveniência em comparação com suas contrapartes físicas, especialmente ao tentar estabelecer um nível de confiança à distância [10]. Na Figura 2 é ilustrado um exemplo do funcionamento da VC:

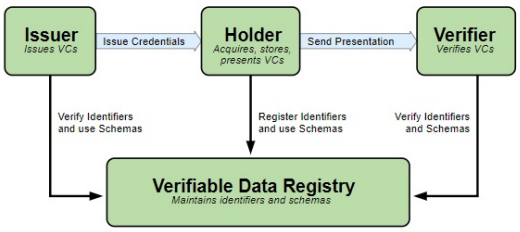

Figura 2. Exemplo de funcionamento do VC

Esclarecendo o fluxograma presente na Figura 2:

- **Holder:** Refere-se a um indivíduo que pode possuir uma ou mais Credenciais Verificáveis (VCs) e gerar VPs para essas credenciais. Exemplos de holders podem incluir estudantes, funcionários e clientes, evidenciando a variedade de contextos nos quais os indivíduos podem ser detentores de VCs, cada uma representando distintas características ou afirmações sobre o titular.
- **Issuer:** Desempenha o papel de atribuir a propriedade sobre um ou mais assuntos (subjects), por meio da criação de VCs e sua subsequente transmissão para um holder. Exemplos ilustrativos dessa atuação incluem a atribuição de propriedade de um veículo a um indivíduo ou a atribuição de um CPF a uma pessoa (neste cenário, o subject da VC faz referência ao holder), entre outras possibilidades. São exemplos de entidades que executam essa função: organizações sem fins lucrativos, corporações e órgãos governamentais. Essas entidades, ao criar e emitir VCs, contribuem para a construção de um sistema que permite a representação confiável de informações sobre indivíduos e entidades em formatos digitais verificáveis. Esse processo apoia a facilitação da troca segura de informações em diversos contextos, destacando a versatilidade e a utilidade dessa abordagem em diferentes setores e organizações.
- **Subject:** É a entidade sobre a qual é exercida propriedade, pode se referir a diferentes objetos ou sujeitos, como animais ou veículos. Em muitas situações, o holder da VC é também o subject, no entanto, em certos casos, essa relação

pode ser distinta. Um exemplo ilustrativo é quando um pai atua como holder, detendo a VC que representa informações sobre uma criança, que é o subject. Nesse cenário, a VC não está diretamente vinculada ao próprio holder, mas sim a um terceiro, destacando a flexibilidade e adaptabilidade desse modelo de gerenciamento de identidades em situações diversas.

- **Verifier:** Responsável por receber uma ou mais VCs, possivelmente dentro de uma Apresentação Verificável (VP) para processamento, é crucial em contextos como equipes de segurança e sites. Essa função envolve a verificação e validação das informações contidas nas VCs, garantindo assim a autenticidade e confiabilidade dos dados apresentados. Em equipes de segurança, a validação das VCs pode ser essencial para garantir a integridade e autorização adequada dos indivíduos. Da mesma forma, em sites, a verificação de VCs pode ser empregada para fortalecer a autenticação dos usuários, promovendo a segurança e confiança nas transações e interações online.
- **Verifiable Data Registry (VDR):** É um sistema ou uma rede que possui como função mediar a criação e a verificação de identificadores, como chaves, esquemas de VCs, chaves públicas do emissor, etc., que são essenciais para o uso de VCs, como por exemplo bancos de dados descentralizados, redes *peer-to-peer*, bancos de dados governamentais ou otras formas de armazenamento confiável. Em resumo, esse sistema mantém identificadores e esquemas, fornecendo uma infraestrutura fundamental para a operação de credenciais digitais.

Após a definição dos termos, o funcionamento da VC é delineado da seguinte maneira: um emissor acessa o VDR e verifica os identificadores, fazendo uso dos esquemas disponíveis. Sua principal função é, então, emitir VCs para o holder. O holder, por sua vez, adquire essas VCs, armazena no VDR e apresenta VPs ao verificador. O verificador, ao receber VCs ou VPs, verifica essas credenciais acessando o VDR e conferindo os identificadores e esquemas pertinentes [10].

2.5. Tecnologia DID

Organizações, provedoras de serviços e indivíduos fazem extenso uso de identificadores únicos em uma variedade significativa de contextos diários. Estes identificadores desempenham o papel fundamental de servir como endereços e meios de comunicação, abrangendo categorias como números de telefone, nomes de usuário, CPF, números de documentos como passaportes, carteiras de habilitação e até identificadores de produtos, como números de série [11].

É importante observar que a grande maioria desses identificadores não está sob nosso controle direto. Frequentemente, esses identificadores são emitidos por autoridades externas que determinam quem ou o que será referenciado por eles e estabelecem as condições sob as quais podem ser revogados[8]. Essa dinâmica ressalta a dependência de entidades externas no que diz respeito à atribuição e gestão desses identificadores essenciais na vida cotidiana [11].

O Identificador Descentralizado (do inglês *Decentralized Identifier* - DID) é uma tecnologia desenvolvida pelo World Wide Web Consortium (W3C) e desempenha um papel fundamental no contexto do SSI [9]. Este novo tipo de identificador viabiliza uma

[8] `https://www.dock.io/post/decentralized-identifiers`

identidade digital verificável e descentralizada, sendo que um DID pode ser atribuído a qualquer entidade, como uma pessoa, uma organização, um modelo de dados, entre outros. A referência associada a um DID é determinada pelo seu controlador [11].

O DID surgiu como uma alternativa aos identificadores centralizados, promovendo o desacoplamento de registros centralizados, provedores de identidade e autoridades de certificação. Seu design permite que o controlador de um DID comprove o controle sobre si mesmo sem depender da autorização de terceiros. Essa comprovação é realizada por meio de assinaturas digitais, que funcionam como prova criptográfica. Em resumo, o DID é um recurso uniforme de identificação (do inglês *Uniform Resource Identifier* - URIs) que associa uma entidade de DID a um documento de DID, possibilitando interações confiáveis envolvendo essa entidade [11].

A Figura 3 mostra os principais componentes da arquitetura DID.

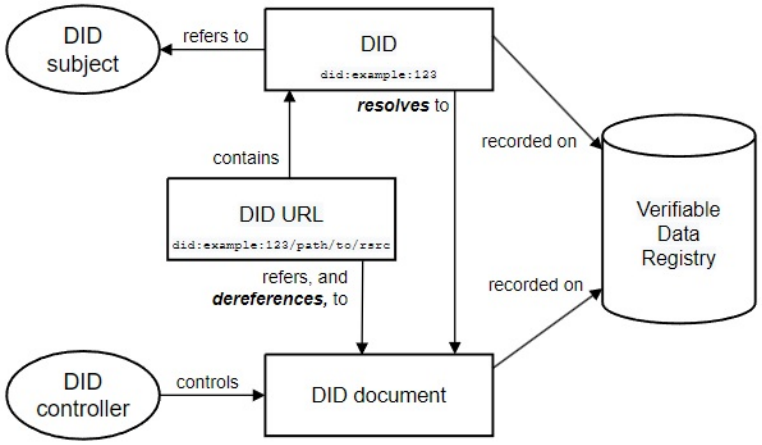

Figura 3. Visão geral da arquitetura DID e a relação dos componentes básicos

Na arquitetura do DID, são identificados seis componentes principais:

- **DID:** É representado por uma cadeia de caracteres (string) simples que consiste em três partes distintas:

    1. Identificador de Esquema DID: Este identificador representa o esquema ao qual o identificador está vinculado. Ela proporciona um contexto para a interpretação do DID.
    2. Identificador do Método DID: Este componente define a metodologia ou o processo específico usado para a criação, resolução e operação do DID.
    3. Identificador do Método Específico: Este componente refere-se a um identificador único e específico associado ao método escolhido, fornecendo informações adicionais sobre a identidade representada.

A Figura 4 mostra um exemplo simples de um DID.

Figura 4. Exemplo simples de um DID

- **DID URL:** Representa uma extensão da sintaxe do DID básico, permitindo a incorporação de outros padrões de URI. Essa extensão possibilita a inclusão de elementos como caminho (path) para localizar recursos específicos associados ao DID.
- **DID Subject:** Refere-se à entidade a que um DID faz referência, sendo possível que essa entidade seja o próprio controlador do DID.
- **DID Controller:** São entidades com a capacidade de modificar um documento DID. Essas entidades podem ser indivíduos ou organizações, e a habilidade de alteração é assegurada pelo uso de chaves criptográficas. Esse mecanismo proporciona uma camada adicional de segurança e controle sobre a gestão dos documentos DID, garantindo que apenas entidades autorizadas possam efetuar alterações nesses registros digitais.
- **DID Verifiable Data Registries (VDR):** São sistemas cuja função principal é intermediar o registro de Identificadores Descentralizados (DIDs). Exemplos desses sistemas incluem bancos de dados descentralizados, redes *peer-to-peer* e outras formas de armazenamento confiável.
- **DID Document:** É um registro que contém informações associadas a um DID. Essas informações geralmente incluem uma chave de criptografia pública ou serviços utilizados para interação com o *DID subject*.

Após a definição desses termos, o funcionamento do DID ocorre da seguinte maneira: o *DID controller* exerce controle sobre um *DID Document*, o qual é referenciado por uma *DID URL*. Este documento é registrado em um *VDR*. A *DID URL*, por sua vez, contém um DID, que faz referência ao *DID subject*. Existe uma resolução que leva ao *DID Document*, o qual também é armazenado em um *VDR*. Esse processo cria uma interconexão entre os elementos essenciais do sistema DID, permitindo a gestão eficiente e segura dessas identidades digitais verificáveis.

3. Objetivos

O presente trabalho tem como objetivo explorar a aplicação do conceito de Self Sovereign Identity (SSI) em um cenário específico dentro da Universidade Estadual de Londrina (UEL), com foco em ceder ao aluno o controle sobre seus dados.

Para isso, será realizada uma revisão bibliográfica buscando as tecnologias disponíveis para se utilizar na implementação de um sistema baseado em SSI. Posteriormente será feito um estudo de caso de uso para a implementação do SSI em um cenário real e com a implementação do sistema feita, busca-se responder às seguintes questões:

- As credenciais digitais têm a capacidade de substituir efetivamente as credenciais físicas utilizadas cotidianamente?

- Quais ferramentas são essenciais para a implementação bem-sucedida de uma solução baseada em SSI?
- Quais são os principais desafios associados à implementação de uma solução fundamentada em SSI?
- Como uma solução baseada em SSI se diferencia de uma solução centralizada?
- Qual é o nível de aceitação por parte dos indivíduos em relação ao uso do SSI?

4. Procedimentos metodológicos/Métodos e técnicas

Na etapa inicial, será realizada uma revisão bibliográfica com foco em SSI e suas tecnologias e padrões, com enfoque específico nos Identificadores Descentralizados (DIDs) e Credenciais Verificáveis (VCs).

Na sequência, será conduzido um estudo de caso de uso para a aplicação do SSI em um cenário comum na UEL. Com o caso de uso definido, será realizado um levantamento das tecnologias, bibliotecas e linguagens de programação a serem empregadas na implementação.

Após a conclusão destas etapas, a fase subsequente compreenderá a implementação do sistema baseado em SSI. Para isso, será utilizado o caso de uso predefinido, assim como as tecnologias previamente selecionadas, e serão realizados testes durante a implementação.

Concluída a implementação, será conduzido um levantamento dos desafios enfrentados ao longo do processo, identificando quais ferramentas se mostraram essenciais para o sucesso da implementação, e analisando as diferenças entre uma solução baseada em SSI e uma solução centralizada.

Dessa forma, será realizada a coleta de opiniões de indivíduos mediante a demonstração de um cenário real no uso de identidades digitais, exemplificando tanto uma solução centralizada quanto uma solução baseada em SSI, visando compreender qual delas é mais aceita pelos usuários de serviços online.

5. Cronograma de Execução

Atividades a serem realizadas:

1. Revisão bibliográfica focada em SSI;
2. Estudo dos padrões de arquitetura do SSI;
3. Estudo da implementação do SSI em um cenário na UEL;
4. Levantamento de tecnologias e linguagens a serem utilizadas;
5. Síntese e redação do TCC parcial;
6. Implementação do SSI em um cenário na UEL;
7. Levantamento dos desafios enfrentados na implementação e redação do TCC completo;

Tabela 1. Cronograma de Execução

	fev	mar	abr	mai	jun	jul	ago	set
Atividade 1	x							
Atividade 2	x	x						
Atividade 3		x	x					
Atividade 4			x					
Atividade 5			x	x				
Atividade 6					x	x	x	
Atividade 7						x	x	x

6. Contribuições e/ou Resultados esperados

Este trabalho tem como objetivo estudar o SSI e suas implicações na privacidade do usuário, bem como os desafios técnicos enfrentados para sua implementação bem-sucedida. Além disso, busca explorar a aplicação do SSI em um cenário real da Universidade Estadual de Londrina.

7. Espaço para assinaturas

Londrina, *4 de março de 2024*.

Aluno

Orientador

Referências

[1] Muneeb Ali, Ryan Shea, Jude Nelson, and Michael J Freedman. Blockstack: A new internet for decentralized applications. *Doylestown, United States*, 2017.

[2] Gergely Alpár, Jaap-Henk Hoepman, and Johanneke Siljee. The identity crisis. security, privacy and usability issues in identity management. *arXiv preprint arXiv:1101.0427*, 2011.

[3] Edvaldo Couto. Educação e redes sociais digitais: privacidade, intimidade inventada e incitação à visibilidade. *Em Aberto*, 28(94), 2015.

[4] Uwe Der, Stefan Jähnichen, and Jan Sürmeli. Self-sovereign identity − opportunities and challenges for the digital revolution. *arXiv preprint arXiv:1712.01767*, 2017.

[5] Damiano Di Francesco Maesa, Andrea Lisi, Paolo Mori, Laura Ricci, and Gianluca Boschi. Self sovereign and blockchain based access control: Supporting attributes privacy with zero knowledge. *Journal of Network and Computer Applications*, 212:103577, 2023.

[6] David P Kormann and Aviel D Rubin. Risks of the passport single signon protocol. *Computer networks*, 33(1-6):51–58, 2000.

[7] Oracle. Identity management. Acessado em 23 de Fevereiro de 2024.

[8] Émilien Vilas Boas Reis and Bruno Torquato de Oliveira Naves. O meio ambiente digital e o direito à privacidade diante do big data. *Veredas do Direito*, 17(37):145–167, 2020.

[9] Reza Soltani, Uyen Trang Nguyen, and Aijun An. A survey of self-sovereign identity ecosystem. *Security and Communication Networks*, 2021:1–26, 2021.

[10] Manu Sporny, Dave Longley, David Chadwick, and Orie Steele. Verifiable credentials data model v2.0. Acessado em 19 de Fevereiro de 2024.

[11] Manu Sporny, Dave Longley, Markus Sabadello, Drummond Reed, Orie Steele, and Christopher Allen. Decentralized identifiers (dids) v1.0. Acessado em 19 de Fevereiro de 2024.

[12] Michelle S Wangham, Emerson Ribeiro de Mello, Davi da Silva Böger, Marlon Guerios, and Joni da Silva Fraga. Gerenciamento de identidades federadas. *Sociedade Brasileira de Computação*, 2010.