DOI: 10.5748/19CONTECSI/COM/ESD/7036

PLATAFORMA DE IDENTIDADE DIGITAL AUTOSSOBERANA: ARQUITETURA, DESAFIOS NA IMPLEMENTAÇÃO E RESULTADOS DE TESTE PILOTO

Elder Bruno Evaristo Correa ; https://orcid.org/0000-0002-4031-6857
Centro de Pesquisa e Desenvolvimento em Telecomunicações - CPQD

Mateus Sousa ; https://orcid.org/0000-0002-9518-0010
Centro de Pesquisa e Desenvolvimento em Telecomunicações - CPQD

Jose Reynaldo Formigoni Filho ; https://orcid.org/0000-0001-5128-6609
Centro de Pesquisa e Desenvolvimento em Telecomunicações - CPQD

Fernando Marino ; https://orcid.org/0000-0002-3860-2467
Centro de Pesquisa e Desenvolvimento em Telecomunicações - CPQD

SELF-SOVEREIGN DIGITAL IDENTITY PLATFORM: ARCHITECTURE, IMPLEMENTATION CHALLENGES AND PILOT TEST RESULTS

ABSTRACT: The Internet evolution to a fully decentralized environment has shed light over the outdated model of identity silos, which brings an illusion of privacy for the users. In this paper, we present a new generation of digital identity systems called Self-Sovereign Identity (SSI), describes the architecture of the SSI platform developed by (Hidden for submission), which is based on microservices and uses blockchain to register decentralized identifiers, data schemas and public cryptographic keys. The results of a pilot test and the challenges associated with its implementation and evolution of the platform's roadmap are also presented.
Keywords: Digital Identity, Blockchain, Segurança, Privacy,

PLATAFORMA DE IDENTIDADE DIGITAL AUTOSSOBERANA: ARQUITETURA, DESAFIOS NA IMPLEMENTAÇÃO E RESULTADOS DE TESTE PILOTO

RESUMO: A evolução da Internet para um ambiente cada vez mais descentralizado jogou luz sobre o modelo defasado de silos de identidades, que traz uma falsa ilusão de privacidade para os usuários. Neste artigo, é apresentado uma nova geração de sistemas de identidade digital denominada identidade digital autossoberana ou Self-sovereign Identity (SSI), descreve a arquitetura de uma plataforma SSI desenvolvida (Ocultado para submissão), baseada em microsserviços, que utiliza blockchain para registrar identificadores e chaves criptográficas públicas. São apresentados também os resultados de um teste piloto e os desafios associados à implementação e evolução da plataforma.
Palavras-chave: Identidade digital, Blockchain, Segurança, Privacidade

1 INTRODUÇÃO

A identificação digital segura de pessoas, organizações ou coisas, é um pilar fundamental da transformação digital dos diversos setores da economia. O atual gerenciamento de identidades na Internet conta com o que o foi chamado, há mais de uma década, de uma "colcha de retalhos de identidades únicas" [Cameron 2005], compreendendo vários tipos de sistemas de gerenciamento de identidade que são restritos a domínios específicos e não interagem entre si [Nakamura 2019].

Nos sistemas de gerenciamento de identidade, sejam eles centralizados ou federados, os provedores fornecem aos usuários vários identificadores digitais e meios de identificação além de forçarem usuários a confiarem em seus sistemas [Mühle et al., 2018; Grüner et al., 2019].

SSI é uma nova geração de sistemas de identidade digital que aborda o conceito emergente de identidade descentralizada no qual entidades, por exemplo, indivíduos, organizações e coisas, gerenciam sua identidade digital [Xu et al. 2020] sem dependência de qualquer autoridade externa. Dessa forma, é eliminado o único ponto de falha, ao mesmo tempo em que aumenta a confiança, privacidade, segurança [Terzi et al. 2020] dentre outras propriedades, tais como transparência, persistência, interoperabilidade.

Os sistemas de SSI também permitem comprovar as etapas de uma jornada de coisas físicas e digitais em uma cadeia de suprimentos. Por exemplo, eles podem eliminar as preocupações de privacidade e identificação relacionadas aos dados do paciente em sistemas digitais de saúde e podem estabelecer confiança nas transações de valor e na comunicação com parceiros, clientes e reguladores nos ecossistemas de negócios [Zwitter et al. 2020]. Os sistemas de SSI também podem permitir o surgimento de novos modelos de negócios, como os esquemas de seguro de identidade [Wang e De Filippi, 2020].

Apesar de seus potenciais benefícios, a transformação dos processos existentes e a orquestração dos ecossistemas da nova identidade digital carregam vários desafios, como a fragmentação do mercado de SSI, padrões e regulamentações que ainda estão em amadurecimento, a imaturidade da tecnologia, e os desafios relacionados à governança [Wang e De Filippi, 2020] [Prewett et al., 2020].

Desde 2019, o (Ocultado para submissão) vem trabalhando com SSI, não só desenvolvendo componentes, mas também participando de comunidades de desenvolvimento como a Hyperledger Foundation e a Decentralized Identity Foundation (DIF). Após o desenvolvimento de vários componentes que compõem o núcleo de um sistema SSI, decidiu-se pelo desenvolvimento de uma plataforma de SSI, cuja arquitetura e resultados de um teste piloto será apresentada no presente artigo.

Na Seção 2 são apresentadas as iniciativas e trabalhos acadêmicos relevantes relacionados com SSI. A Seção 3 descreve as principais características e elementos que compõem a SSI. Na Seção 4, descreve-se o modelo conceitual e a arquitetura da plataforma SSI desenvolvida em desenvolvimento no (Ocultado para submissão). A Seção 5 apresenta o ambiente do teste piloto realizado com resultados encontrados e discussões acerca de pontos relevantes e por fim a Seção 6, expondo as considerações finais e trabalhos futuros, levando em consideração assuntos relevantes que norteiam o futuro do piloto.

2 TRABALHOS RELACIONADOS

Recentemente a comunidade acadêmica, juntamente com grandes empresas e governos, começaram a explorar o paradigma SSI de forma aprofundada. A partir disso, novos trabalhos e projetos foram desenvolvidos para as mais diversas áreas (e.g. economia, agricultura, humanitário, etc). Nesta seção são apresentados alguns desses trabalhos.

O projeto eIDas (Lips et al., 2020) pode ser definido como um dos mais notórios, tendo em vista sua robustez tanto em escalabilidade quanto em padronização. O mesmo foi implantado nos países pertencentes à União Europeia com o intuito de prover confiança no sistema de transações online do mercado único europeu. O sistema permite que cada membro tenha autonomia para implementar sua própria versão, todavia, há uma regulamentação que impõe limitações visando manter a interoperabilidade e transparência do ambiente.

No trabalho de [Grech 2021], é abordado um estudo da viabilidade de SSI aplicado à educação. Nesse contexto, os autores trazem uma discussão sobre possíveis desafios frente à validação das credenciais além das fronteiras, bem como os problemas inerentes, tais como governança, dimensões legais, questões técnicas sobre implementação e semântica das informações.

No estudo de caso apresentado em [Gravity 2022], o conceito de SSI foi aplicado em cenário de ajuda humanitária com o objetivo de ajudar refugiados a conseguirem emprego através da identidade digital. Devido a situação de fuga de regiões de conflitos ou imigração ilegal, muitos dos refugiados não conseguem alocação devido a falta de prova de educação ou vínculos empregatícios passados. A solução proposta faz uso da plataforma de identidade descentralizada da Gravity onde usuários criam credenciais verificáveis que podem ser apresentadas aos futuros empregadores.

O European Self-Sovereign Identity Framework Lab (eSSIF-Lab), tem como objetivo prover um ecossistema que possibilite a governos, empresas que pensam num ambiente de desenvolvimento, experimentação, validação e especificação (Kubach, M., & Roßnagel, H. (2021)). O eSSIF-Lab prevê um ambiente que seja dividido em categorias, atrelando conceitos de governanças que possam ser desenvolvidos em 3 categorias básicas como Governos e empresas, população e ecossistemas jurídicos.

Para gerenciar todas essas categorias o eSSIF-Lab se concentra na gerência e administração das políticas de controle dos dados (informações, aplicações, e etc.) relevantes que permeiam os processos entres as categorias que o projeto europeu classifica.

O governo alemão vem trabalhando no projeto IDunion, que tem como objetivo usar identidades autossoberanas (SSI) para lançar uma rede de produção e implementar mais de quarenta aplicativos de identidade, um ecossistema aberto e seguro para identidade descentralizada. A intenção é dar aos usuários a opção de decidir quando e com quem desejam compartilhar seus dados (Kudra, A. (2022)). Nos próximos três anos, a IDunion testará casos de uso específicos em áreas de Berlim e Colônia para integrar a tecnologia SSI na vida cotidiana. Ao fazer isso, a IDunion está se concentrando em uma solução que pode ser usada em toda a Alemanha e em toda a Europa.

Outra iniciativa é o projeto do banco espanhol Santander, que, em parceria com outras nove empresas na Espanha, criou uma solução de verificação de identidade digital baseada em blockchain. O projeto, denominado Dalin, funciona com emissores de credenciais que certificam e validam a identidade digital dos usuários, que podem ter controle sobre seus dados pessoais, e estarão acessíveis a qualquer momento por meio de um aplicativo móvel. Eles poderão decidir com quem desejam compartilhar seus dados (Santander, 2020).

De acordo com os trabalhos citados acima, é notável como o gerenciamento de identidades digitais vem se modificando constantemente conforme a internet e suas tecnologias vão avançando, ganhando maior importância e criticalidade. Dessa forma, tomando esse cenário como base que este trabalho avança, mostrando ser uma opção de gerenciamento de identidade que pode ser adaptado para contexto diversos, seja a nível empresarial ou acadêmico.

3 IDENTIDADE DIGITAL AUTOSSOBERANA

As primeiras referências sobre SSI datam de 2012, porém as primeiras iniciativas de desenvolvimento ocorreram a partir de 2015 (Reed 2021). Infelizmente não existe um consenso sobre a definição de SSI. Pode-se dizer que SSI é um conjunto de princípios sobre como o controle de identidade e dos dados pessoais deve funcionar nas redes digitais (Allen 2016).

Do ponto de vista tecnológico, pode-se dizer que SSI é um conjunto de tecnologias que se baseiam em conceitos de gerenciamento de identidade, computação distribuída, distributed ledger technology (DLT), para a maior parte das soluções implementadas, e criptografia. Esses conceitos centrais foram estabelecidos ao longo de décadas. A novidade é como eles são reunidos para criar um novo modelo de gerenciamento de identidade digital.

Embora a SSI esteja muito relacionada com a identidade de pessoas, e suas necessidades individuais de segurança, privacidade e controle de dados pessoais, o modelo se aplica às organizações e coisas. Na verdade, se aplica a qualquer coisa que precise de identidade segura na internet.

Os modelos baseados em SSI são considerados a camada de identidade da Internet, e possuem as seguintes características (Sovrin 2018): (i) ausência de uma autoridade central, (ii) uso de blockchain como forma de registro para a maioria das soluções atualmente implantadas, (iii) usuário fazendo a gestão dos próprios dados, (iv) elevados níveis de segurança e privacidade, (v) uso de mecanismos de governança para garantir a confiança entre os membros da rede e (vi) conformidade com as leis gerais de proteção de dados, como por exemplo o Regulamento Geral de Proteção de Dados (GDPR) e a lei brasileira de proteção de dados pessoais (LGPD), enfatizando que os dados pessoais não são colocados na rede blockchain.

Um sistema baseado em SSI é constituído pelos seguintes componentes básicos (Reed 2021):

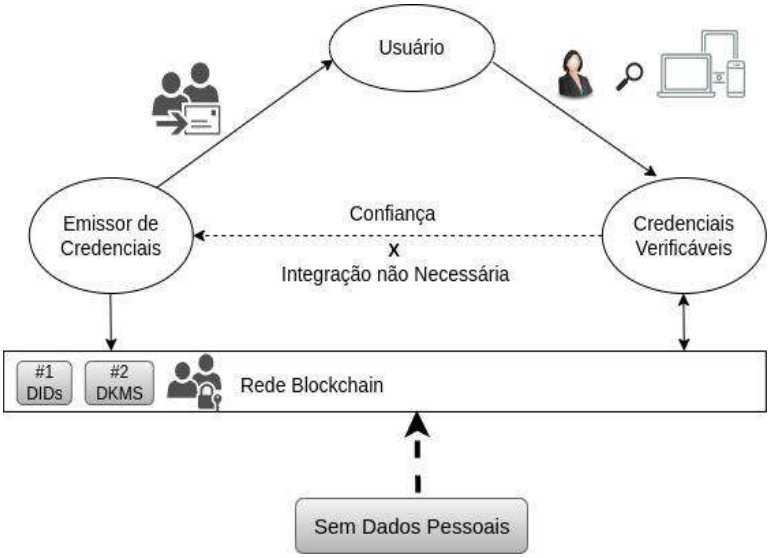
- Credencial verificável (VCs): trata-se de um conceito chave de um sistema SSI e é a representação digital de credenciais físicas, tais como uma Carteira Nacional de Habilitação (CNH), Registro Geral de Identidade (RG), diploma e certificados, dentre outros exemplos. De acordo com a definição do W3C, a credencial verificável pode representar todas as mesmas informações que uma credencial física representa. A adição de tecnologias, tais como assinaturas digitais, torna as credenciais verificáveis menos vulneráveis e mais confiáveis do que suas credenciais físicas (W3C 2022). Geralmente, a identidade digital de um usuário de um sistema SSI será composta por um conjunto de credenciais verificáveis;
- Carteira digital: uma carteira digital consiste em software que permite que o usuário gere, armazene, gerencie e proteja chaves criptográficas, credenciais verificáveis, identificadores descentralizados (DIDs) e outros dados privados confidenciais. As carteiras podem ser instaladas em diferentes dispositivos, tais como smartphones e notebooks;

- Agente digital: é um módulo de software que gerencia as interações da carteira com os demais atores do sistema, ou seja, os emissores e verificadores de credenciais. Um agente digital é para uma carteira digital o que um sistema operacional é para um computador ou smartphone;
- Identificador Descentralizado (DIDs): no nível mais básico, um identificador descentralizado (DiD) é simplesmente um novo tipo de identificador global, não muito diferente das URLs. DiDs são considerados como uma nova camada de identidade digital descentralizada semelhante ao que é a infraestrutura de chave pública (PKI) para a Internet. Os DIDs são a contrapartida criptográfica das credenciais verificáveis (VCs) e juntos são considerados os pilares da padronização SSI. Eles foram projetados para serem controlados por seu proprietário, sem qualquer meio centralizado, como uma certificação de autoridade (W3C 2021);
- Registro de dados verificáveis: local onde são registrados DIDs, chaves públicas e *schemas* de dados das credenciais verificáveis. Pode ser uma blockchain, como por exemplo a Hyperledger Indy (Nakamura 2019) ou outras formas de registros dos dados.

Conforme mostrado na Figura 1, um sistema SSI pode ser representado pelo triângulo da confiança, que é composto pelos seguintes atores:

- Emissor: na sua maioria, são organizações como agências governamentais emitindo documentos oficiais (CNH, RG, etc), instituições financeiras, universidades emitindo diplomas e outros certificados, corporações emitindo credenciais de empregos. Vale destacar que um indivíduo ou até mesmo dispositivos podem ser emissores, por exemplo, um sensor devidamente equipado pode emitir uma credencial assinada digitalmente sobre a uma leitura (Reed 2021).
- Usuário: são indivíduos, pessoas ou coisas que detêm as credenciais nas suas carteiras digitais e que apresentam comprovantes oriundos de credenciais, quando solicitados pelos verificadores;
- Verificador de credenciais: são aqueles que solicitam credenciais digitais, para realizar alguma ação, por exemplo, liberar o acesso ao serviço digital após verificar a autenticidade, que pode ocorrer em uma blockchain.

Figura 1 - Triângulo da Confiança do Metassistema SSI



Fonte: Elaboração Própria (2021)

A confiança trazida pelo triângulo representado na Figura 1 é reforçada por uma estrutura de governança, também denominada de *framework* de governança, encarregada de especificar as políticas e procedimentos que os emissores devem seguir para emitir uma credencial. Em alguns casos a estrutura de governança específica os termos e condições com os quais os titulares devem concordar em obter credenciais — ou com os quais os verificadores devem concordar em verificar as credenciais. As estruturas de governança também podem especificar modelos de negócios para troca de credenciais, políticas de responsabilidade, seguro e outros requisitos legais e comerciais (Reed, 2021).

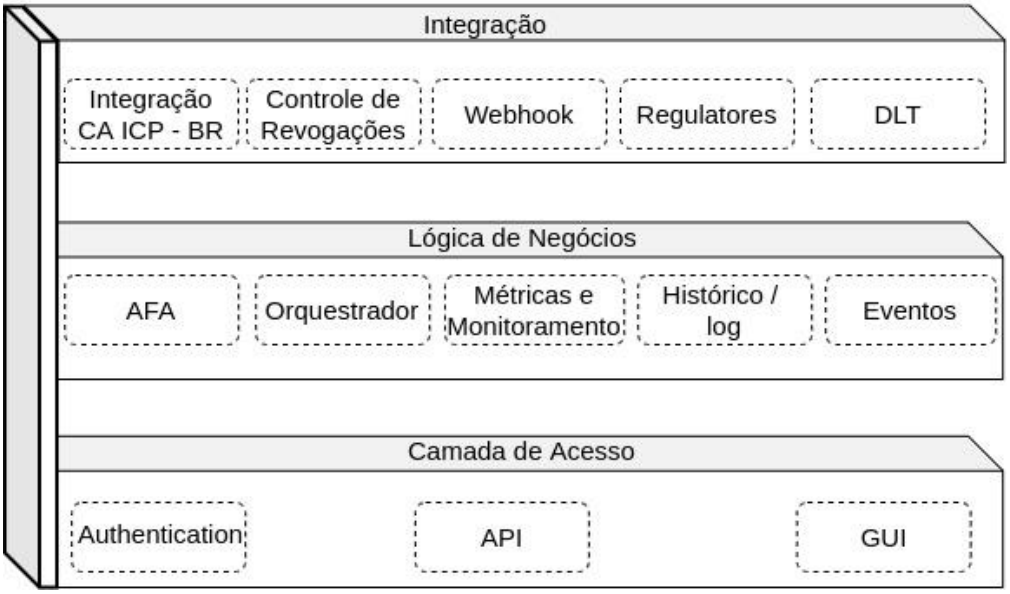
4 ARQUITETURA DA PLATAFORMA

O (Ocultado para submissão) desenvolveu componentes para uma plataforma de SSI optando por uma arquitetura baseada em microsserviços, seguindo os padrões e boas práticas determinadas pelo W3C, IETF e DIF. O desenvolvimento utilizou como base vários componentes de código aberto da Hyperledger Foundation, tais como as bibliotecas Aries e Ursa e a rede Hyperledger Indy.

4.1. MODELO CONCEITUAL

A fim de facilitar o entendimento conceitual de uma solução SSI, foi desenvolvido pelo (Ocultado para submissão) um modelo conceitual em quatro camadas, conforme mostrado na Figura 2.

Figura 2: Camadas de microsserviços que constituem o modelo conceitual de solução SSI.



Fonte: Elaboração Própria (2021)

Segue uma descrição de cada camada:

- Camada de Acesso: é considerada o principal recurso de integração com aplicações clientes, é por meio dela que as soluções citadas acima realizam seus acessos e integração com as principais funcionalidades desenvolvidas na solução. Ela é responsável por prover uma API para integração de aplicações clientes, podendo se ressaltar – mas não se limitando – à aplicações clientes, como aplicações web para clientes e administração, além de sistemas legados.
- Camada de lógica e regras de negócio: camada dos componentes que implementam as funcionalidades da solução de SSI para a criação e gerenciamento de agentes verificadores, agentes emissores, definição de credencial e configurações necessárias

para os participantes, tais como configuração de rede, de emissão de credencial, verificação de credencial e registro aplicações de domínio do cliente.

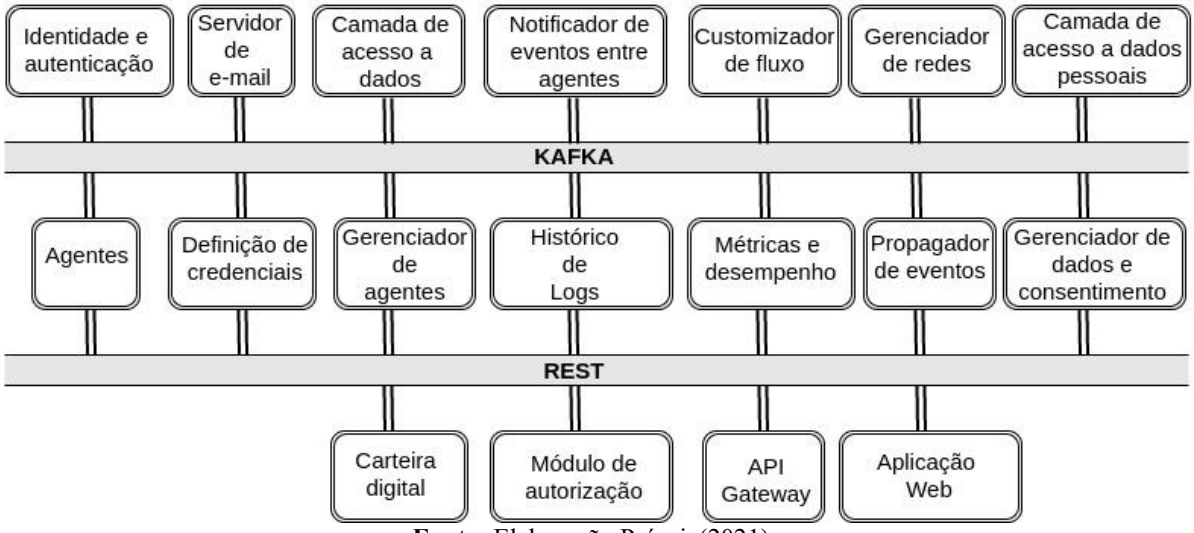
- Camada de integração: camada dos componentes que realizam integração aos serviços necessários da plataforma de SSI, como por exemplo serviços de cloud, billing e antifraude. Além disso, são responsáveis por integrar a solução a serviços de banco de dados e redes DLTs.

Camada de segurança: camada dos componentes de segurança da informação, garantindo à plataforma alta disponibilidade, confiabilidade e também confidencialidade dos dados e informações por ela trafegados.

4.2 ARQUITETURA DA PLATAFORMA

Conforme mostra a Figura 3, a solução utiliza uma arquitetura baseada em microsserviços, implementada na nuvem, objetivando atender os requisitos de escalabilidade, alto desempenho e alta disponibilidade. Além disso, para a correta integração entre os componentes e também um bom desempenho das requisições entre os microsserviços, foi projetada a implantação de um sistema de mensageiria utilizando a ferramenta Apache Kafka (Apache).

Figura 3: Arquitetura detalhada dos microsserviços que baseiam a Solução SSI



Fonte: Elaboração Própria(2021)

A plataforma possui funcionalidades para gerenciamento de Agents - com a finalidade para operação de credenciais verificáveis— e fornece os seguintes recursos:
Criação de Cloud Agents;

- APIs para integração com os Cloud Agents;
- Mecanismos para mensageria de eventos entre agentes;
- Aplicações clientes facultativas para administração dos agentes (tanto mobile quanto web);
- Sistema de antifraude para detecção de fraude em transações realizadas pela identidade dos usuários.

Muito tem se debatido e testado no âmbito do usuário, como a criação de carteiras digitais, usabilidade para consentimento e gerenciamento de seus dados, mas o mesmo não pode ser dito para os outros dois atores - emissores e verificadores - que geralmente são compostos por organizações e, ao invés de manusearem uma aplicação móvel, no formato de uma carteira, possuem aplicações implantadas em nuvens que automatizam processos e tomam decisões.

Além da necessidade de criar componentes úteis para os atores corporativos do sistema de DID, os desenvolvimentos do (Ocultado para submissão) até aqui foram baseados em agentes em nuvem, que se mostrou efetivo quanto à segurança, versatilidade e persistência das informações, ainda que em casos de sinistros, tais como perda ou roubo do dispositivo. Além disso, ao prover um agente em nuvem, a criação de um agente "multiplataforma" para o gerenciamento da identidade descentralizada das pessoas torna-se mais simples e natural. Por isso, conceitualmente, a abordagem de "DIDaaS" – identidade digital autossoberana como Serviço – pode ser utilizada também para pessoas físicas.

5 PILOTO NO (Ocultado para submissão)

Desde meados de 2019, o (Ocultado para submissão) vem desenvolvendo protótipos, produtos mínimos viáveis e pilotos para diferentes setores da economia, tais como o agronegócio, saúde, educação, governo e setor financeiro.

Em meados de 2019, o (Ocultado para submissão) desenvolveu no Laboratório de inovação Financeira do Banco Central (LIFT) uma identidade digital autossoberana para o setor financeiro denominada FinID (Marino, 2020). No LIFT de 2020, o (Ocultado para submissão), juntamente com mais duas entidades relevantes do setor financeiro, desenvolveu um protótipo de sistema de gestão de identidade e consentimento de compartilhamento de dados para a segunda fase do Open Banking, o qual utilizava o FinID (Formigoni 2021) e uma rede blockchain de propósito genérico.

Ainda em 2020, foi desenvolvido um piloto, juntamente com a Secretaria de Governo Digital (SGD) do Ministério da Economia, com o objetivo de se utilizar uma credencial verificável para acesso ao portal Gov.br, sem a necessidade de o cidadão utilizar o tradicional login com usuário e senha. O processo de cadastro para a emissão de credencial foi feito utilizando a base do TSE, a partir de dados biográficos e biométricos enviados pelo cidadão. De posse da credencial emitida pela SGD, e armazenada na carteira digital, o cidadão poderia escolher a opção de acesso via SSI. Um QR Code era então apresentado ao cidadão e, após a leitura pelo seu smartphone, a credencial era enviada e o acesso liberado.

Na esteira do piloto realizado com a SGD, surgiu a possibilidade de realizar piloto semelhante dentro do próprio (Ocultado para submissão), mas ao invés de utilizar o Ministério da Economia como emissor e a base do TSE para o processo de checagem de dados e informações durante o processo de registro do usuário, optou-se por utilizar o próprio (Ocultado para submissão) como emissor e utilizando face match como base de coleta das informações para a verificação do ID.

5.1 DESCRIÇÃO GERAL

O piloto do (Ocultado para submissão) teve como objetivo a emissão de Credencial Verificável (VC) para os funcionários da Fundação para que estes pudessem utilizá-las no acesso a sistemas corporativos, por exemplo o Jira, sem a necessidade de realizar um login tradicional. A autenticação por meio da Credencial Verificável foi opcional, isto é, o funcionário poderia continuar a se autenticar utilizando-se do usuário e senha. A autenticação com a Credencial Verificável como uma opção foi parte do estudo deste laboratório, objetivando medir a adesão voluntária da autenticação por meio de VC.

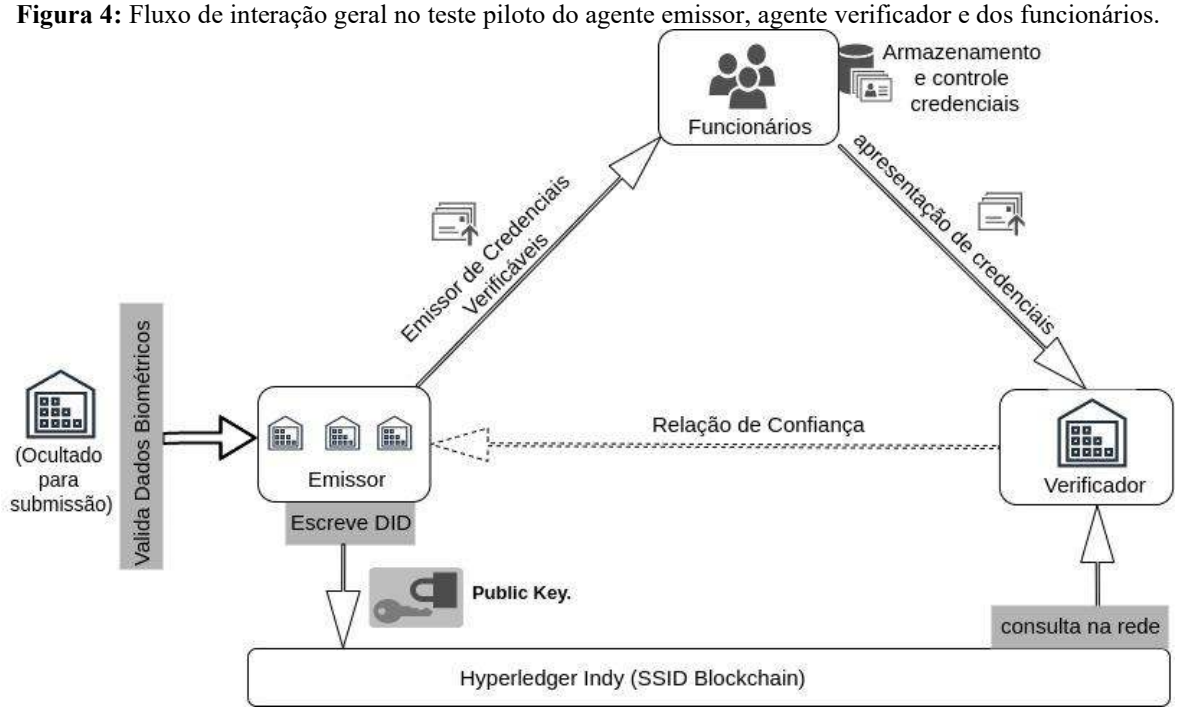
Outro objeto do piloto foi avaliar a usabilidade do processo de registro do funcionário através de validação, tanto da sua biometria e como também das informações biográficas que compõem a sua credencial verificável. É importante ressaltar que, apesar do (Ocultado para submissão) já ter executado um processo de cadastro do seu funcionário no momento da contratação, esse novo processo foi realizado a fim de se analisar a taxa de abandono

durante o registro, aproximando-se assim ao comportamento que deverá ocorrer com as carteiras digitais com o público em geral.

5.2 VISÃO GERAL

A visão geral do piloto está representada na Figura 4, que ilustra as interações dos funcionários (Ocultado para submissão) e plataforma SSI, utilizando como caso de uso o login único dos funcionários aos serviços dos sistemas corporativos do (Ocultado para submissão).

Figura 4: Fluxo de interação geral no teste piloto do agente emissor, agente verificador e dos funcionários.



Fonte: Elaboração Própria (2021)

A solução é centrada no funcionário que, em linhas gerais, fará a instalação do aplicativo (Ocultado para submissão) iD em seu dispositivo móvel para, então, se comunicar diretamente com o agente emissor do (Ocultado para submissão).

Por sua vez, o agente emissor do (Ocultado para submissão) irá registrar na blockchain um identificador descentralizado único (aqui chamado de DID) e público. O DID é criado por meio da assinatura digital da chave privada do proponente,ou seja, o (Ocultado para submissão). Após esse processo, uma conexão criptografada segura entre o agente móvel do funcionário e o agente emissor do (Ocultado para submissão) é criado por meio de DID privados cujo hash sejam derivados de suas chaves privadas, para isto, utiliza-se como base o protocolo DIDComm. Com a conexão criada, o colaborador solicitará a emissão de sua identidade digital, onde:

- A identidade digital é formada por um conjunto de credenciais eletrônicas (aqui chamada de (Ocultado para submissão) iD;
- O colaborador realiza a captura de uma selfie e fotografa sua CNH usando a câmera fotográfica do smartphone e as envia com alguns dados pessoais para serem autenticadas junto ao (Ocultado para submissão);

- A credencial (Ocultado para submissão) iD é emitida pelo agente do (Ocultado para submissão) a partir do resultado da análise biométrica realizada pela base de dados do (Ocultado para submissão);
- Compatível com GDPR e LGPD, os dados pessoais do colaborador não são armazenados pela solução.

Após emissão da (Ocultado para submissão) iD, a credencial será utilizada por um serviço de autenticação e validação de identidade a fim de prover o acesso único aos serviços dos sistemas corporativos relacionados ao perfil do funcionário.

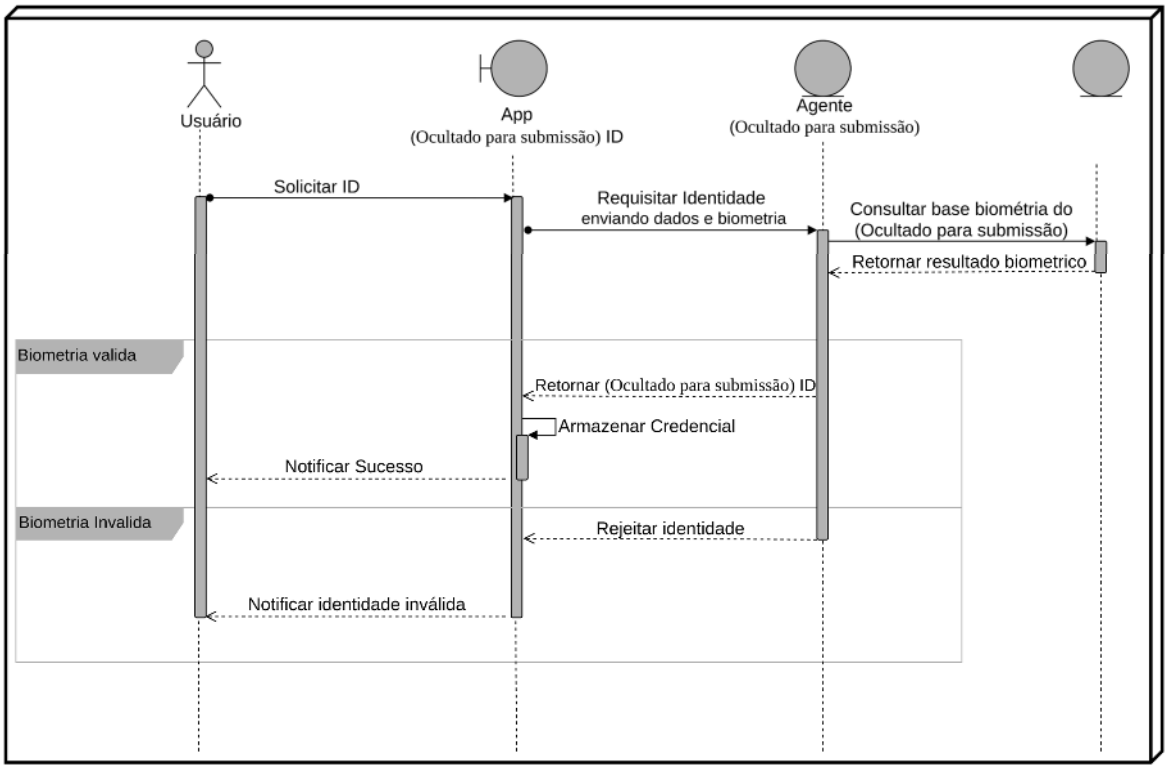
5.3 FLUXO DE FUNCIONAMENTO

Os principais fluxos de funcionamento da solução são: (i) emissão da credencial e (ii) autenticação e validação da identidade do funcionário, os quais são descritos a seguir.

A. Emissão da credencial

O processo de emissão da credencial do (Ocultado para submissão) iD consiste nas etapas e fluxos referentes a criação da conexão segura via DIDComm entre os agentes do funcionário e do (Ocultado para submissão), verificação biométrica e o face match com a CNH do funcionário junto às bases do (Ocultado para submissão) e, por fim, a emissão da credencial do (Ocultado para submissão) iD pelo agente do (Ocultado para submissão). Esse processo pode ser visualizado no diagrama de sequência da Figura 5.

Figura 5 - Diagrama de emissão da credencial do colaborador.



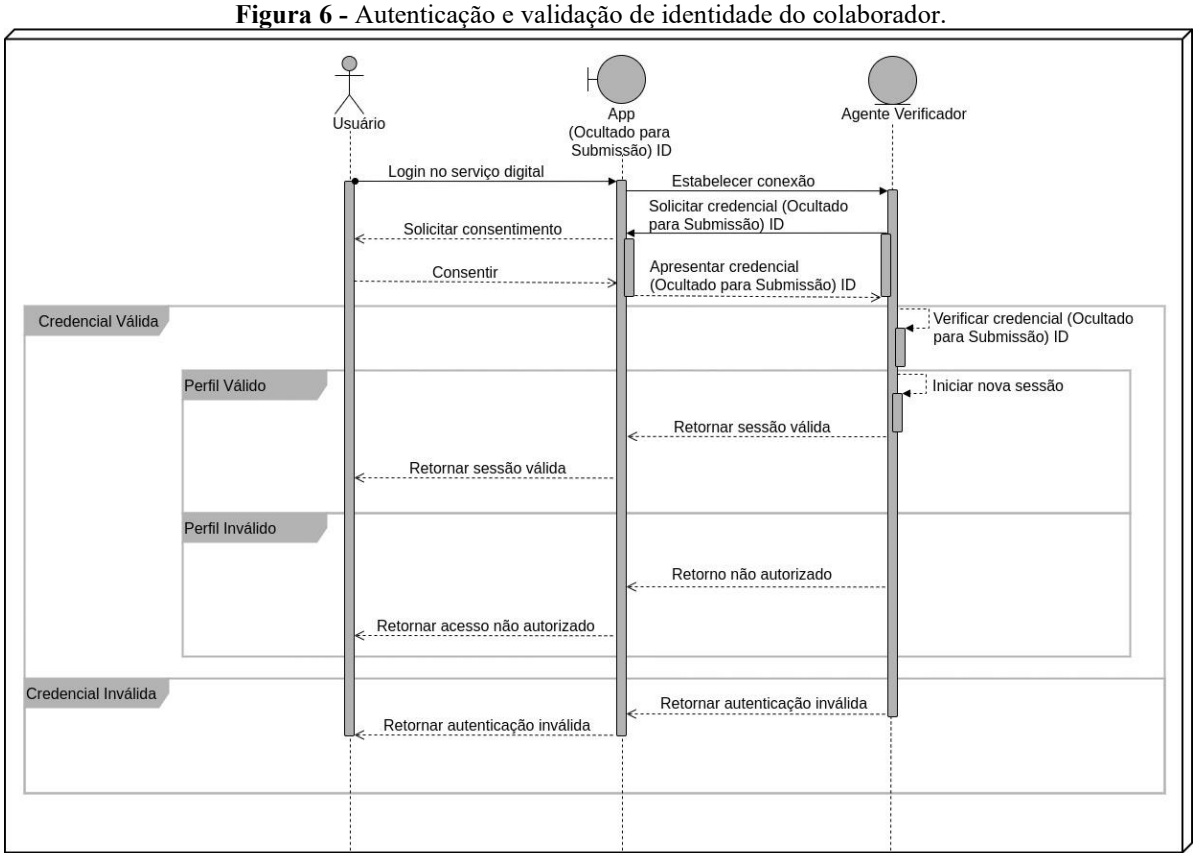
Fonte: Elaboração Própria (2022)

B. Autenticação e validação da identidade do funcionário

O cenário de verificação da credencial consiste em dar a opção ao funcionário de, ao invés de se autenticar utilizando as credenciais corporativas baseadas em usuário e senha, se

autenticar por meio da carteira digital do dispositivo móvel ao ler um código qr-code que inicia um processo de autenticação através de verificação de Credencial Verificável, a credencial (Ocultado para submissão) iD. Esse processo pode ser visualizado no diagrama de sequência da Figura 6.

Figura 6 - Autenticação e validação de identidade do colaborador.



Fonte: Elaboração própria(2022)

5.4 RESULTADOS OBTIDOS

Após a execução do piloto com 172 downloads do aplicativo da carteira digital SSI (Ocultado para submissão) iD, foi possível analisar o comportamento dos funcionários do (Ocultado para submissão), permitindo, assim, vislumbrar uma possível utilização na produção de uma aplicação de Identidade Digital Descentralizada. Portanto, resultados interessantes foram obtidos, como por exemplo a taxa de abandono durante o processo de registro da VC (Ocultado para submissão) iD, isto é, a quantidade de funcionários que simplesmente abandonaram o processo de registro após a solicitação da aplicação para a realização da coleta de imagens de autorretrato e da Carteira Nacional de Habilitação, uma vez que do total de 172 funcionários que iniciaram o processo de registro, apenas 65 concluíram o processo e obtiveram assim a VC (Ocultado para submissão) iD.

Portanto, apenas 37,8% dos funcionários que participaram voluntariamente do piloto receberam uma credencial. Ao analisar alguns pontos relacionados ao teste do piloto, chegamos algumas conclusões como:

- Que para se finalizar o processo de verificação e emissão da carteira digital do portador é de suma importante a finalização de todo o processo de autenticação, para que assim o registro do usuário seja validado;
- Através da finalização de todo o processo é possível a emissão de uma credencial de um e-mail ou número telefônico validado(s) por código via e-mail ou ainda SMS;

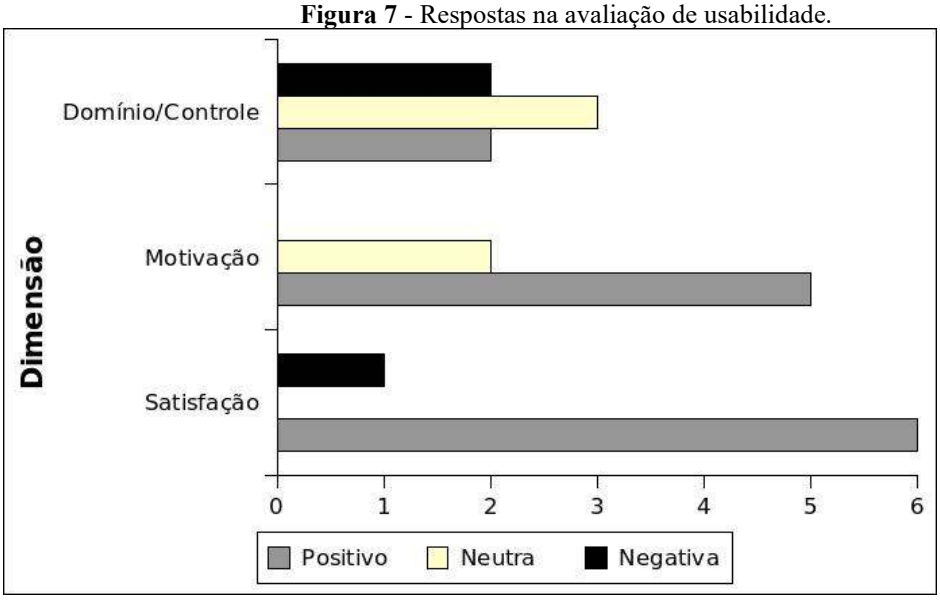
- Posteriormente a esse passo, pode-se disponibilizar credenciais mais complexas de acordo com regimes de autenticação mais robustos para que o processo seja finalizado.

Avançando na avaliação do projeto piloto, foi possível coletar algumas informações relacionadas à usabilidade, como as voltadas a frequência de uso, que está atrelado a dificuldade ou não no cadastro e na autenticação. Levamos em conta etapas como a captura da face match tanto de documentos como CNH e captura do rosto.

Outra caracteŕsitca avaliada tem relação com a opinião exposta pelos usuários de acordo com o teste no ambiente real, essa característica está atrelada a opnião de como o usuário avaliou o teste, nisso foi proposto respostas classificadas em positiva, neutra e negativa.

Na Figura 7 é destacada a avaliação de usabilidade da aplicação. A partir dos resultados obtidos, é possível afirmar que a maior parte dos usuários não tiveram dificuldades ao utilizarem a aplicação. Todavia, no quesito "domínio/controle" os usuários relataram uma posição neutra, o que está será averiguado em novas avaliações.

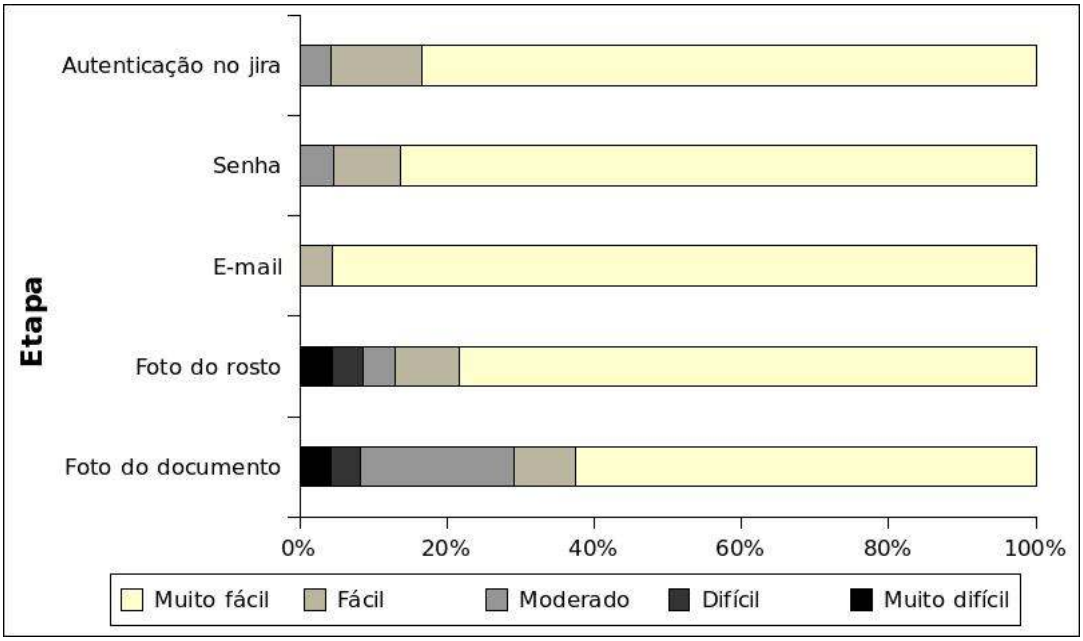
Figura 7 - Respostas na avaliação de usabilidade.



Fonte: Elaboração própria (2022)

Já na Figura 8 é apresentada a classificação das funções de cadastro e autenticação pelos usuários. De acordo com o gráfico pode-se ver que cerca de 80% dos usuários acharam o processo bastante simples e intuitivo.

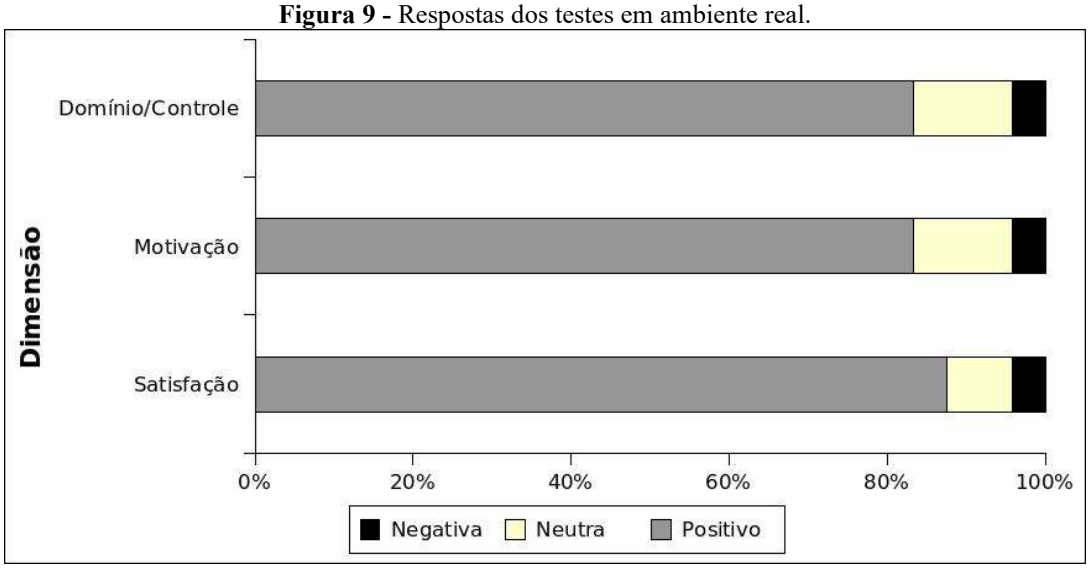
Figura 8 - Dificuldade percebida no cadastro e na autenticação.



Fonte: Elaboração própria (2022)

Por fim, na Figura 9 está representando os resultados relacionados aos testes em ambiente de produção. É possível afirmar que os usuários mantiveram uma opinião positiva acerca da utilização da aplicação.

Figura 9 - Respostas dos testes em ambiente real.



Fonte: Elaboração própria (2022)

Além dos resultados observados acerca da experiência dos funcionários da fundação com a metatecnologia de SSI, também foram gerados resultados tecnológicos significativos. Tais como: a criação de uma carteira digital de documentos móvel compatível com o sistema operacional móvel Android, e a implantação e customização de um agente institucional emissor para a própria Fundação (Ocultado para submissão). Tal agente foi registrado com o papel de emissor na rede pública-permissionada de identidade digital descentralizada, a Sovrin.

Além disso, outro resultado relevante foi a integração com serviços para consultas de dados biométricos e biográficos provenientes da base do (Ocultado para submissão), culminando com um processo de onboarding confiável, cujo o resultado é a emissão da Credencial Verificável do (Ocultado para submissão) iD, dando, portanto, um registro reutilizável para autenticação sem senha e também para criação de novos cadastros em sistemas corporativos digitais para ao funcionário do (Ocultado para submissão).

Por fim, outro resultado obtido foi a implementação de um agente verificador genérico de credencial, que de forma conjunta com plugins de interoperabilidade - também desenvolvidos para este piloto - permitiram com que sistemas legados que já utilizam protocolos de identificação pudessem facilmente se integrar com a solução de SSI. Inicialmente, o protocolo objeto da interoperabilidade foi o OAuth 2.0 e, posteriormente, também foi abarcado o protocolo SAML 2.

6 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

O presente artigo apresentou uma visão geral do que é um sistema SSI, seus principais componentes, assim como a arquitetura da plataforma SSI desenvolvida pelo (Ocultado para submissão). Também foram apresentados os desafios encontrados no desenvolvimento da plataforma e os resultados encontrados na realização de um teste piloto feito no (Ocultado para submissão).

Atualmente, existem várias iniciativas de desenvolvimento de sistemas SSI, conforme apresentado no item 2. Pode-se afirmar que tanto a tecnologia quanto os modelos de negócio associados à SSI ainda não atingiram a sua maturidade. Do ponto de vista tecnológico destacam-se os desafios da interoperabilidade, padronização das credenciais verificáveis e a possibilidade de adoção do sistema de armazenamento de registros único.

No roadmap evolutivo da plataforma também será necessário considerar desafios associados ao desempenho e escalabilidade para que o sistema possa suportar dezenas de milhões de carteiras. Em relação à carteira digital, será necessário considerar novos requisitos de segurança, melhor usabilidade, assim como a interoperabilidade entre carteiras SSI e a possibilidade de uma fusão de carteiras de criptomoeda, incluindo as Central Bank Digital Currency e as carteiras SSI.

Outra questão de extrema relevância é a convergência dos sistemas SSI com os sistemas centralizados baseados em PKI. Várias iniciativas em desenvolvimento contemplam a convergência destes sistemas. O próprio (Ocultado para submissão) desenvolveu uma solução no setor de saúde onde a carteira digital do médico está associada à ICP Brasil e a do paciente à plataforma SSI. Vale salientar a iniciativa da União Europeia de iniciar discussões sobre a convergência do sistema centralizado eIDAS (electronic IDentification, Authentication and trust Services) com SSI. Para disponibilizar o eIDAS como uma estrutura de confiança no ecossistema SSI, a Comissão Europeia está desenvolvendo o projeto SSI eIDAS Bridge.

Como trabalhos futuros é possível verificar a necessidade do desenvolvimento de formas que visem embarcar sistemas biométricos, que contam com vários processos distintos na carteira digital, que visem a extração de templates, com a intenção de aumentar o tempo de geração e armazenamento no momento do cadastro para economizar tempo de processamento e comparações futuras, algumas dessas possibilidades estão atreladas ao desenvolvimento de novas linhas de integrações que visem a principalmente a interoperabilidade e novas formas de registros, como por exemplo.

O projeto OpenWallet Foundation foca em fornecer ou emitir credenciais padronizadas, ou seja, a ideia se concentra a construção de um mecanismo de software de código aberto que outras organizações e empresas possam aproveitar para desenvolver suas

próprias carteiras digitais e que tenha como objetivo alcançar a paridade de recursos com as melhores carteiras disponíveis.

Dentro do contexto de identidade descentralizada é importante entender os processos de governança, que está atrelado ao conceito de trust registry. Onde um registro de confiança é uma lista aprovada de emissores e verificadores autorizados a emitir/verificar determinadas credenciais em um ecossistema de credenciais verificável. Os registros de confiança são criados e mantidos pela autoridade governante de um ecossistema, que geralmente é o provedor do ecossistema.

Outro Cenário bastante interessante é o conceito de Internet of Trusted Things, ou seja, a relação de identidade descentralizada digital (IDD) com internet das coisas (IoT), para oferecer mais segurança, privacidade e confiabilidade aos processos de autenticação, controle de identidade e de rastreabilidade dos objetos, bem como à auditoria de transações realizadas no universo de Internet das coisas, onde a premissa básica é entender os fatores básicos para aumentar a confiança no ecossistema IoT é a identificação digital segura e isso vale para pessoas e coisas fatores básicos para aumentar a confiança no ecossistema IoT é a identificação digital segura e isso vale para pessoas e coisas.

Portanto, há muito trabalho ainda a ser feito pelas diferentes comunidades envolvidas com o desenvolvimento do ecossistema SSI. A maturidade tecnológica não atingiu a sua plenitude e muitos componentes ainda estão sendo desenvolvidos para o core das soluções e também para as carteiras digitais. Entidades como a DIF, Hyperledger Foundation e W3C têm desempenhado um papel importante no fomento das discussões de padronização e interoperabilidade, assim como no desenvolvimento de novos componentes de código aberto.

7 AGRADECIMENTOS

Os autores reconhecem o apoio financeiro dado a este trabalho pelo (ocultado para submissão), mais especificamente, através dos projetos (ocultado para submissão), finalizado em novembro de 2021 e o projeto (ocultado para submissão), iniciado em dezembro de 2021. Este documento reflete apenas as opiniões dos autores e as Agências não são responsáveis por qualquer uso que possa ser feito das informações nele contidas.

8 REFERÊNCIAS

Allen, Christopher. “The Path to Self-Sovereign Identity.” *Lifewithalacrity.com*, 26 Apr. 2016,www.lifewithalacrity.com/2016/04/the-path-to-self-sovereereign-identity.html. Acessado 13 abril 2022.

“Apache Kafka.” Apache Kafka, 29 July 2022, kafka.apache.org/documentation/. Acessado 13 abril 2022.

Cameron, Kim, et al. The Laws of Identity Problem Statement a Patchwork of Identity One-Offs. 5 Nov. 2005.

Chong, S., Vikram, K., & Myers, A. C. (2007, August). SIF: Enforcing Confidentiality and Integrity in Web Applications. In USENIX Security Symposium (pp. 1-16).

Formigoni Filho, J. R., Marino, F. C. H., Marion, S. H., Almeida, A. R., Ribeiro, S. L., de Oliveira, C. A., & Sevilla, P. A. (2020). RegConID–Gestão do Registro de Consentimento e Identidade no Open Banking. Revista LIFT papers, 3(3).

Grüner, A., Mühle, A., Gayvoronskaya, T., & Meinel, C. (2019, March). A comparative analysis of trust requirements in decentralized identity management. In International Conference on Advanced Information Networking and Applications (pp. 200-213). Springer, Cham.

Loffreto, and Devon. What Is "Sovereign Source Authority"? 15 Feb. 2012, www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html. Acessado 14 Maio 2022.

Marino, F., et al. "V. 2 N. 2 (2019): LIFT Papers - 2° Edição | Revista LIFT Papers." Revista.liftlab.com.br, 2020, revista.liftlab.com.br/lift/issue/view/15/27. Acessado 12 Maio 2022.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. Computer Science Review, 30, 80-86.

Naik, N., & Jenkins, P. (2020, August). Self-Sovereign Identity Specifications: Govern your identity through your digital wallet using blockchain technology. In 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud) (pp. 90-95). IEEE.

Nakamura, E. T., Marino, F. C. H., Formigoni Filho, J. R., Ribeiro, S. L., & de Oliveira, V. P. (2019). Identidade Digital Descentralizada: Conceitos, aplicações, iniciativas, plataforma de desenvolvimento e implementação de caso de uso. Sociedade Brasileira de Computação.

Prewett, K. W., Prescott, G. L., & Phillips, K. (2020). Blockchain adoption is inevitable—Barriers and risks remain. Journal of Corporate accounting & finance, 31(2), 21-28.

Reed, Drummond, Preukschat, Alex (2021). "Self-Sovereign Identity: Decentralized Digital Identity and VCs". Manning Publications, version 10.

Young, I. K. Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials.

Sovrin Foudation. Sovrin TM : A Protocol and Token for Self- Sovereign Identity and Decentralized Trust a White Paper from the Sovrin Foundation. 2018.

Terzi, S., Savvaidis, C., Votis, K., Tzovaras, D., & Stamelos, I. (2020, November). Securing emission data of smart vehicles with blockchain and self-sovereign identities. In 2020 IEEE International Conference on Blockchain (Blockchain) (pp. 462-469). IEEE.

Xu, J., Xue, K., Tian, H., Hong, J., Wei, D. S., & Hong, P. (2020). An identity management and authentication scheme based on redactable blockchain for mobile networks. IEEE Transactions on Vehicular Technology, 69(6), 6688-6698.

W3C. "Decentralized Identifiers (DIDs) V1.0." W3.org, 20 July 2021, www.w3.org/TR/did-core/#introduction. Acessado 10 Abril 2022.

W#C. “Verifiable Credentials Data Model 1.1.” W3.org, 19 Nov. 2019, www.w3.org/TR/vc-data-model/. Acessado 10 Abril. 2022.

Wang, F., & De Filippi, P. (2020). Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. Frontiers in Blockchain, 28.

Windley, Phil. “Multi-Source and Self-Sovereign Identity.” Www.windley.com, 2018, www.windley.com/archives/2018/09/multi-source_and_self-sovereign_identity.shtml. Acessado 12 Abril 2022.

Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. Information and Organization, 29(2), 105-117.

Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital identity and the blockchain: universal identity management and the concept of the “Self-Sovereign” individual. Frontiers in Blockchain, 3, 26.

Grech, A., Sood, I., & Ariño, L. (2021). Blockchain, self-sovereign identity and digital credentials: promise versus praxis in education. Frontiers in Blockchain, 4, 616779.

Gravity. (2022). https://www.gravity.earth/. Gravity Earth. https://www.gravity.earth/.

Lips, S., Bharosa, N., & Draheim, D. (2020, November). eIDAS implementation challenges: the case of Estonia and the Netherlands. In International conference on electronic governance and open society: challenges in Eurasia (pp. 75-89). Springer, Cham.
Kubach, M., & Roßnagel, H. (2021). A lightweight trust management infrastructure for self-sovereign identity. Open Identity Summit 2021.

Kudra, A. (2022). Self-Sovereign Identity (SSI) in Deutschland. Datenschutz und Datensicherheit-DuD, 46(1), 22-26.

Santander. (2020). Ten Spanish companies join forces to promote digital identity using blockchain technology.