Análise de viabilidade de implantação de sistema de autenticação híbrido baseado em Identidades Digitais Federadas e Identidades Digitais Descentralizadas

Raquel Pereira Leite[1] **Marco Aurélio Amaral Henriques**[1]

[1]Faculdade de Engenharia Elétrica e de Computação
Universidade Estadual de Campinas (Unicamp)
13083-852 – Campinas, SP, Brasil

r243687@dac.unicamp.br maah@unicamp.br

Abstract. *With the goal of making the user the absolute and exclusive owner of its personal data, new models of digital identity management have emerged, based on the Decentralized ID concept and stimulated by the advent of blockchains. This project is concerned with finding out the real benefits and costs of a digital identity system based on decentralized identities. To this end, it proposes to evaluate a smooth transition between federated and decentralized identity management models, based on the use of a hybrid authentication system that combines the two models. Thus, it is possible to learn more about the risks, advantages, and disadvantages of one form of authentication over the other.*

Resumo. *Com objetivo de tornar o usuário dono absoluto e exclusivo de seus dados pessoais, novos modelos de gestão de identidades digitais emergiram, baseados no conceito de Identidades Descentralizadas (DID - Decentralized ID) e estimulados pelo advento das blockchains. O presente trabalho busca entender os reais benefícios e custos de um sistema de identidade digital baseado em identidades descentralizadas. Para isso, propõe-se a avaliar uma transição suave entre os modelos de gestão de identidades federadas e descentralizadas, baseada no uso de um sistema de autenticação híbrido que combina os dois modelos. Assim, é possível conhecer melhor os riscos, vantagens e desvantagens de uma forma de autenticação em relação à outra.*

1. Introdução

A capacidade de provar que uma entidade é quem ela alega ser é fundamental para as interações na sociedade, seja no mundo físico, seja no mundo virtual. Com a crescente transição dos processos de trabalho e de serviços para o contexto virtual, tornou-se necessário que as identidades digitais - a forma como nos apresentamos nos diversos canais digitais em que participamos - sejam autenticadas de maneira confiável. Atualmente, porém, a grande maioria das identidades (e os dados relacionados a elas) não está sob controle dos usuários em si. Elas são mantidas por autoridades externas que decidem a quem ou a que elas se referem, a quem podem ser entregues e quando podem ser revogadas [Reed et al. 2021]. Tal centralização, além de ser o alvo de hackers e de compartilhamento indevido de informações [Schardong and Custódio 2021], dificulta que o usuário tenha real propriedade de seus dados pessoais.

Com o objetivo de melhor entender os custos e benefícios existentes em um sistema de identidade digital descentralizada e as eventuais dificuldades de se migrar de um sistema de identidades federadas para outro descentralizado, este trabalho escolheu uma plataforma de suporte a identidades descentralizadas chamada Jolocom como ferramenta básica de implementação. Assim, nas seções que seguem teremos uma discussão do assunto sob a ótica de trabalhos relacionados; estudo dos conceitos de identidade autossoberana, identidade descentralizada e credenciais verificáveis; seleção da plataforma de apoio à solução SSI; instalação e configuração de um ambiente de testes para a implementação de uma solução SSI na plataforma escolhida; realização de testes com a plataforma criada e a proposta de um sistema híbrido para facilitar a transição entre os modelos federado e descentralizado de autenticação.

2. Trabalhos Relacionados

Desde o advento da Internet, os modelos de identidade digital evoluíram significativamente, de tal forma que essa evolução pode ser dividida em quatro etapas: identidade centralizada, identidade federada, identidade centrada no usuário e identidade autossoberana [Allen 2016]. O primeiro estágio (identidade centralizada), caracterizado pelo prestador de serviço fornecer os identificadores e credenciais aos clientes que desejam acessar seus serviços, é o menos conveniente no âmbito da usabilidade: há uma grande carga imposta ao usuário, que precisa gerenciar uma identidade digital para cada novo serviço que deseja acessar. Além disso, os dados do usuário são centralizados no provedor do serviço e o usuário não tem controle sobre eles. O segundo estágio (identidade federada, onde cada domínio de identidade consiste em um único provedor de identidade e em um ou mais provedores de serviços [Ferdous et al. 2019]), apesar de ter diminuído a carga sobre o usuário, ainda tem os problemas sérios do primeiro, que são a concentração de dados do usuário nos provedores federados e a falta de controle do usuário sobre seus dados. Com o terceiro estágio (identidade centrada no usuário), continuaram os esforços para que a experiência do usuário fosse melhor e houvesse uma maior descentralização das informações e da confiança. Nesse estágio, representado tipicamente pela proposta OpenID [Allen 2016], a ideia era passar o papel do provedor de identidade para o próprio usuário, dando-lhe mais controle sobre a autenticação. Entretanto ele deveria criar, configurar e manter um sistema OpenID para isso, algo inviável na maioria dos casos. Isso levou os grandes provedores de serviços na Internet (*Google, Facebook, Apple* etc) a oferecerem o serviço de Provedor de Identidade para seus clientes (alguns deles baseados exatamente no OpenID). Portanto, esse modelo centrado no usuário se tornou similar ao das identidades federadas, não descentralizando de fato a gestão de identidades e nem colocando o usuário no controle de seus dados. Começaram a surgir então, propostas mais concretas e viáveis para que uma identidade digital ficasse totalmente sob o controle de seu dono: as identidades autossoberanas.

Com a ideia de se dar um maior controle ao usuário sobre sua identidade digital, consolidou-se o termo Identidade Autossoberana (SSI - *Self-Sovereign Identity*) no quarto estágio. O conceito principal da SSI, uma forma de identidade descentralizada (DID - *Decentralized ID*), é o de os indivíduos serem soberanos sobre seus "eus" digitais e, portanto, terem o controle de seus dados [Schardong and Custódio 2021]. Essa ideia diferencia fundamentalmente a SSI dos modelos de identidade anteriores, nos quais os indivíduos eram vistos apenas como usuários. As DIDs são desenvolvidas de modo a es-

tarem desacopladas de quaisquer registradores centralizados, provedores de identidades e autoridades certificadoras, também sendo resistentes a adulterações. O detentor da DID deve ser capaz de provar o controle de sua identidade utilizando métodos criptográficos (ou demais técnicas de verificação) sem depender de terceiros. Além disso, podem ser feitas alegações sobre uma DID em forma de Credenciais Verificáveis.

Fomentando o quarto estágio, o surgimento da tecnologia blockchain tem trazido novas perspectivas para o estudo de implementação de DIDs, de forma que certas propriedades das *blockchains* coincidem com algumas das propriedades desejáveis em uma DID [Ferdous et al. 2019]. *Blockchains* públicas, por exemplo, fornecem um domínio descentralizado e fora do controle de um agente único. Os dados armazenados nas *blockchains* estão sempre disponíveis quando necessários, de modo que as transações feitas são imutáveis, isto é, elas não podem ser alteradas ou deletadas. O proprietário dos dados armazenados em uma *blockchain* tem controle total sobre como e quando tais dados serão compartilhados com outros usuários. Um controle mais fino sobre os dados de identidade que são liberados a terceiros pode ser exercido por contratos inteligentes em *blockchains* que suportam este tipo de contratos, como a *blockchain Ethereum*. Com a viabilização e popularização das soluções SSI, novas propostas de sistemas de gestão de identidades descentralizadas têm surgido, dentre elas: uPort/Serto [Naik and Jenkins 2020], Jolocom [Fei et al. 2019], Sovrin Foundation [Reed et al. 2021] e DIF - Digital Identity Foundation (plataforma ION) [Buchner et al. 2021].

Como não se tem ainda muita experiência acumulada com DIDs, há várias questões relacionadas à melhor forma de implementá-las, considerando, entre outros aspectos, o processo de transição do modelo de gestão de identidades federadas, bastante usado atualmente na academia. Neste sentido, faz-se necessário buscar um maior conhecimento sobre DIDs e sobre maneiras de transitar de um modelo para outro. Assim, o presente trabalho procura estender outro trabalho com objetivos similares realizado por Wolff e Henriques [Wolff and Henriques 2021] e compreender melhor os detalhes da implantação e configuração de um sistema DID baseado em *blockchain*, a fim de comparar as formas de gestão de identidades federada e distribuída sob o ponto de vista do usuário, buscando validar a hipótese de que é possível prover uma transição simples de um modelo federado para o descentralizado.

3. A tecnologia DID e Identidades Autossoberanas

Para avaliar a transição entre os modelos de gestão de identidades federadas e descentralizadas, é primeiramente necessário entender os conceitos de identidade autossoberana, identidade descentralizada e credenciais verificáveis. De acordo com a normativa do W3C (*World Wide Web Consortium*), que desenvolveu um padrão para identificadores descentralizados, as DIDs são projetadas para permitir que indivíduos e organizações gerem seus próprios identificadores usando sistemas nos quais confiam. A DID deve ser resolvível para um documento DID, que contém informações referentes a materiais criptográficos, métodos de verificação e terminais de serviços que permitem ao controlador de uma DID provar o seu controle [Reed et al. 2021]. Uma DID associa um sujeito ao documento DID, permitindo interações confiáveis com esse sujeito. Deve-se ressaltar que somente o controlador pode fazer alterações no documento DID, através de um conjunto de chaves criptográficas em seu nome usadas pelo *software*. Na Figura 1, tem-se o exemplo de uma DID, que pode ser vista como uma simples string de texto.

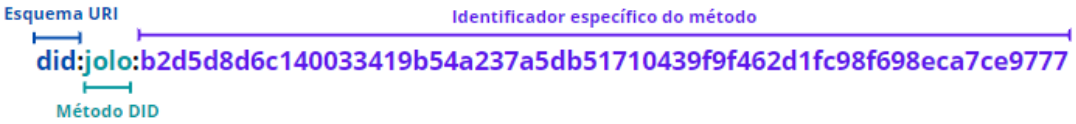

Figura 1. Exemplo de uma DID e seus respectivos campos.

Explicitando as partes formadoras de uma DID, tem-se: (i) Identificador do esquema URI (*Uniform Resource Identifier*): identifica que a interação pertence a identificadores descentralizados, permanecendo a mesma independente da implementação; (ii) Identificador do método DID: protocolo que determina onde ou como encontrar a DID (no exemplo explicitado, o método DID refere-se à solução Jolocom); (iii) Identificador específico do método: valor alfanumérico que resolve o DID para o documento DID (semelhante à resolução de um *link* para uma página em um servidor *web*).

A identidade descentralizada permite que as entidades provem o controle de suas próprias identidades, através da autenticação com provas criptográficas (como assinaturas digitais localizadas em seus respectivos documentos DID). Para que as DIDs sejam resolvidas em documentos DID, é necessário que elas sejam registradas em um sistema ou rede subjacente de algum tipo, que forneça um registro de dados verificáveis. Independentemente da tecnologia específica usada, qualquer sistema que ofereça suporte ao registro de DIDs e ao retorno de dados necessários para produzir documentos DID é chamado de registro de dados verificáveis.

A Figura 2 mostra um exemplo de um documento DID no formato JSON (*JavaScript Object Notation*), seguindo a normativa do W3C (neste caso, o documento DID é referente à identidade da Figura 1). Nota-se que um documento DID contém informações associadas à DID, tais como formas de autenticar criptograficamente um controlador DID. Porém, é importante destacar que o documento DID não contém informações pessoais sobre o sujeito, pois elas vêm por meio das Credenciais Verificáveis [Sporny et al. 2021].


```
{
 "@context": [
  "https://www.w3.org/ns/did/v1",
  "https://w3id.org/security/suites/ed25519-2020/v1"
 ]
 "id": "did:jolo:b2d5d8d6c140033419b54a237a5db51710439f9f462d1fc98f698eca7ce9777",
 "authentication": [{

  "id": "did:jolo:b2d5d8d6c140033419b54a237a5db51710439f9f462d1fc98f698eca7ce9777#keys-1",
  "type": "Ed25519VerificationKey2021",
  "controller": "did:jolo:b2d5d8d6c140033419b54a237a5db51710439f9f462d1fc98f698eca7ce9777",
  "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
 }]
}
```


Figura 2. Trecho do documento DID referente à identidade descentralizada criada e exposta na Figura 1 (adaptado de [Sporny et al. 2021]).

No âmbito das SSIs, qualquer afirmação relativa a um assunto é chamada de alegação; de modo que um conjunto de uma ou mais alegações feitas por uma entidade, independente do assunto, é uma credencial. Se a credencial está associada a um método

de revogação e possui material criptográfico que garante sua integridade e identificação, então se trata de uma Credencial Verificável (CV). Nos sistemas SSI, as entidades emitem CVs aos usuários, que escolhem as alegações que desejam compartilhar.

Com a possibilidade de escolha da alegação a ser compartilhada, o provedor de serviços não precisa tomar conhecimento de todas as informações da identidade do usuário, mas somente da alegação necessária ao acesso do serviço. Por exemplo, caso seja necessário que o usuário prove sua maioridade para acessar certo serviço, constrói-se uma Apresentação Verificável (*Verifiable Presentation* - VP) no contexto das SSIs, alegando-se que: a credencial foi emitida por um terceiro confiável, que tal credencial atesta a maioridade do detentor e que a credencial não foi revogada [Schardong and Custódio 2021].

4. O Protocolo Jolocom

A solução de identidade Jolocom visa ser um protocolo universal, leve e de código aberto para identidade digital descentralizada e gerenciamento de direitos de acesso [Fei et al. 2019]. Atualmente, o protocolo expõe as seguintes funcionalidades básicas de gerenciamento de identidade: geração de uma identidade global única, descentralizada e permanente; derivação de identidades a partir de uma identidade mestre para modelar com precisão diferentes personas de usuário e/ou dispositivos de IoT de provisionamento; associação de credenciais verificáveis de terceiros com a identidade do usuário escolhida e definição de um conjunto de tokens de interação padrão que podem ser usados para modelar qualquer identidade ou interação relacionada à credencial [Fei et al. 2019].

O protocolo Jolocom segue as especificações básicas propostas pela normativa W3C referentes a Identificadores Descentralizados [Reed et al. 2021] e Credenciais Verificáveis [Manu et al. 2021]. Visando ser *collision-resistant*, a solução de identidade Jolocom permite que os usuários provem que um dado identificador é pertencente a um específico detentor através das interações com tal identificador. Para tal, cria-se uma DID única, processo que reduz-se essencialmente à geração de um par de chaves público-privada e à geração de um DID e seu correspondente documento DID (contendo metadados, tais como chaves públicas utilizadas na autenticação, encriptação e recuperação da identidade).

Com a criação da DID, deve-se ancorá-la, de modo que outros usuários da rede encontrem o identificador descentralizado utilizando o processo de resolução definido na especificação do método DID. Através do *Jolocom DID Method Specification*, utiliza-se o IPFS (Sistema de Arquivos Interplanetário - *InterPlanetary File System*) como camada CAS (Armazenamento Endereçado por Conteúdo - *Content Addressable Storage*) descentralizada para documentos DID. Um *smart contract* (implantado por meio do *execution environment* da *Ethereum*) fornece um mapeamento de uma DID para um endereço *hash* IPFS do documento DID correspondente. Assim, a rede de teste *Rinkeby* atua como uma camada de confiança para resolver uma DID para um documento DID (de modo que apenas uma DID e uma referência ao seu documento DID são armazenados na *blockchain Ethereum*). O documento DID é armazenado no IPFS, onde se encontram as credenciais públicas. Mesmo que o protocolo esteja atualmente implementado na *blockchain Ethereum* de testes (*Rinkeby Testnet*), a equipe do projeto Jolocom afirma que a solução DID já foi implantada com sucesso utilizando outras tecnologias para certos casos de uso [Fei et al. 2019].

Propondo utilizar diversas tecnologias para oferecer um ambiente de suporte à gestão das identidades descentralizadas, a solução Jolocom desenvolveu um aplicativo móvel chamado *Jolocom SmartWallet*, que permite realizar o gerenciamento da identidade de forma mais pessoal (privada), visual e amigável. Dessa forma, o protocolo Jolocom utiliza vários componentes e tecnologias para oferecer suporte a um sistema de gerenciamento de identidade descentralizado, permitindo o estudo e avaliação de como é feito o fluxo de comunicação entre agentes com esta solução descentralizada. Nas próximas seções, serão apresentados a implementação e os resultados dos testes realizados com essa plataforma.

5. Implementação da plataforma de testes

Para a análise da implementação da solução descentralizada Jolocom, foi necessário preparar um ambiente de testes que permitisse a realização dos fluxos de comunicação entre identidades descentralizadas por meio da troca de Credenciais Verificáveis. A criação do ambiente de testes tomou como base o estudo realizado por Wolff e Henriques [Wolff and Henriques 2021]. Para implementar a plataforma de testes, foi utilizado o Jolocom-SDK (*Jolocom Software Development Kit*[1]), um conjunto de ferramentas para o gerenciamento de agentes SSI e suas interações, seguindo a normativa W3C para DIDs e Credenciais Verificáveis.

O Jolocom-SDK requer um módulo de armazenamento para a persistência dos dados (i.e. Documentos DID, Credenciais Verificáveis, chaves criptográficas etc.) geradas e coletadas durante as diversas interações e etapas das comunicações entre SSIs. Foi implementado, portanto, um *back-end* de armazenamento (carteira digital) em banco de dados SQLite3 para persistir os dados e armazenar credenciais verificáveis.

Para a realização dos testes de fluxo de comunicação, dois agentes foram criados localmente, sendo eles o servidor e o cliente. A criação e a reutilização de um agente de armazenamento podem ser feitas por meio de uma senha ou de um mnemônico BIP39 (*Bitcoin Improvement Proposal*[2]). Ambos os agentes foram criados com uma DID aleatória e foram carregados mediante apresentação de senha a partir do agente de armazenamento. Usando esse *back-end* de armazenamento, cada agente mantém localmente uma carteira criptografada (contendo as chaves da identidade) e o documento DID (permitindo que a identidade seja utilizada em momentos posteriores).

No ambiente de testes implementado, o agente servidor representa um provedor de serviço capaz de emitir e verificar credenciais verificáveis (ou seja, o servidor atua como um provedor de serviços e um provedor de Credenciais Verificáveis a depender do fluxo de comunicação testado no momento). O agente cliente, por sua vez, representa um usuário interessado em possuir credenciais e acessar algum serviço fornecido pelo agente servidor. A plataforma de testes foi instalada em um ambiente Node.js em uma máquina de testes local. Tendo em vista que o Jolocom-SDK só é compatível com versões do Node.js anteriores à 15, foi utilizada a versão 14.19.3.

As mensagens são codificadas em *JSON Web Token* (JWT) [Jones et al. 2015] e transmitidas pela rede através de requisições HTTP. Para uma melhor compreensão do

[1] `https://github.com/jolocom/jolocom-sdk`
[2] `https://pub.dev/documentation/bip39/latest/`

conteúdo de cada uma, foi utilizada a técnica "*man-in-the-middle*", que intercepta todas as mensagens que cada agente recebe e envia. O estabelecimento de um canal de comunicação bidirecional foi realizado via a tecnologia *WebSockets*[3] e, para a criação de requisições HTTP, utilizou-se a plataforma Postman[4].

Os testes realizados com os dois agentes sendo executados em uma única máquina de testes permitiram um conhecimento mais aprofundado sobre o fluxo de comunicação dos mesmos a partir da solução descentralizada Jolocom, conforme descrito mais adiante. Em seguida foi configurado um novo agente cliente usando o aplicativo móvel *Jolocom SmartWallet* e, assim, foi possível avaliar um caso prático mais viável e mais próximo da realidade das identidades autossoberanas.

Os fluxos de interações comuns entre agentes do Jolocom-SDK - descritos na documentação do protocolo Jolocom [Fei et al. 2019] - podem ser englobados em dois casos principais: (i) emissão e recebimento de credenciais verificáveis e (ii) solicitação, fornecimento e verificação de credenciais verificáveis. Os agentes foram implementados para tais fluxos, de modo que foi possível associar informações a esses agentes em forma de credenciais verificáveis personalizadas, que atestam a posse de um *e-mail*.

6. Fluxos de comunicação na plataforma de testes

6.1. Fluxo de emissão de credenciais verificáveis

O primeiro fluxo de comunicação implementado foi o fluxo de emissão e recebimento de credenciais verificáveis. Na primeira implementação, ambos os agentes servidor e cliente têm suas identidades descentralizadas (seguindo o formato exposto na Figura 1) instanciadas na máquina de testes local. Iniciando o fluxo de emissão, exposto de maneira simplificada na Figura 3, o usuário - no primeiro passo - acessa a URL (*Uniform Resource Locator*) do servidor, que atua como um emissor de credenciais verificáveis, por meio de uma requisição HTTP GET.

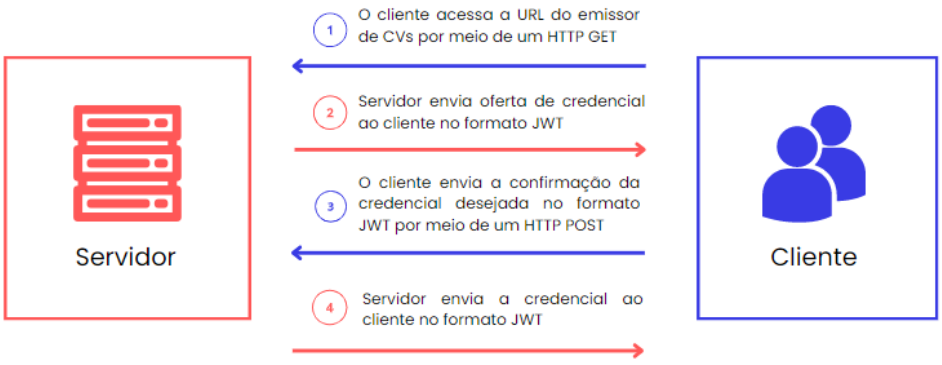

Figura 3. Fluxo de emissão e recebimento de credenciais verificáveis da plataforma de testes, com agentes cliente e servidor locais.

Com a requisição HTTP GET realizada pelo cliente - que deseja possuir a CV emitida pelo servidor - o emissor envia uma oferta de credencial. Tal oferta, codificada em

[3] https://developer.mozilla.org/pt-BR/docs/Web/API/WebSocket
[4] https://www.postman.com/

um JWT, possui os tipos de credenciais que o servidor pode emitir. A oferta de credencial gerada no passo 2 é exposta na Figura 4, bem como sua decodificação feita por meio da ferramenta *online* JWT.IO[5].

Na mensagem decodificada (Figura 4(b)), cujas seções *Header* (que contém informações sobre o tipo de token e a assinatura utilizada) e *Verify Signature* (incluindo o método de codificação utilizado) foram suprimidas, a seção de dados revela informações importantes sobre a oferta de credencial. O campo "*callbackURL*" contém a URL para qual a mensagem deve ser respondida e o campo "*offeredCredentials*" contém informações referentes ao tipo de credencial que pode ser emitida, seguida da DID do respectivo emissor. Ao final do JWT decodificado, há mais alguns metadados, como, por exemplo: (i) o campo "*typ*", que contém informações sobre o tipo do *token* (uma oferta de credencial); (ii) o campo "*iat*", que corresponde ao horário em que a mensagem foi emitida; (iii) o campo "*exp*", referente ao horário de expiração da mensagem; (iv) o campo "*jti*", que corresponde ao identificador único do JWT e (v) o campo "*iss*", que contém a DID do criador da mensagem (que, no caso, é o agente servidor emissor de CVs).

Ao receber a oferta de credencial, o agente cliente deve decodificar o JWT, verificar sua autenticidade com o apoio da blockchain e, em seguida, criar e enviar uma resposta contendo os tipos de credenciais desejadas. Essa mensagem - muito semelhante àquela exposta na Figura 4 (sendo do tipo "*credentialOfferResponse*", cujo *issuer* é o agente cliente) - é enviada no passo 3 por meio de uma requisição HTTP do tipo POST do cliente para o emissor de credenciais. Ao receber a resposta com as credenciais desejadas, o servidor também realiza a verificação da mensagem por meio da *blockchain* e gera as credenciais solicitadas, enviando-as para o usuário no passo 4. Após isso, o agente cliente armazena as credenciais emitidas localmente.

Figura 4. (a) *Json Web Token* referente à oferta de credencial do tipo e-mail e (b) decodificação do campo de dados (porção sublinhada no JWT).

Para o caso em que o agente cliente corresponda à carteira digital no dispositivo móvel, o usuário deve instalar em seu dispositivo móvel o aplicativo *Jolocom*

[5]https://jwt.io/

SmartWallet. A instalação pode ser feita em dispositivos Android[6] e iOS[7]. Ao inicializar, o aplicativo criará uma identidade autossoberana baseada em DIDs de acordo com um mnemônico BIP39 que será gerado durante a primeira inicialização. O aplicativo oferecerá recursos para interpretar códigos QR, armazenar e compartilhar credenciais verificáveis [Wolff and Henriques 2021].

O processo do fluxo de solicitação e emissão das credenciais para este caso (com a presença da carteira digital no dispositivo móvel) está exposto na Figura 5. A primeira requisição HTTP GET (com o navegador acessando o servidor do emissor de CVs), no passo 1, estabelece uma conexão *WebSocket* entre o navegador e o emissor de credenciais na plataforma de testes [Wolff and Henriques 2021]. A conexão *WebSocket*, demonstrada no passo 2, facilita o envio de mensagens de maneira bidirecional entre o navegador e o emissor de credenciais. O passo 3 é análogo ao passo 2 do caso anterior (Figura 3), de modo que o JWT contendo as credenciais ofertadas é renderizado pelo navegador em um QR Code. Assim, permite-se que o agente cliente escaneie o código QR (passo 4) e decodifique o JWT, criando a resposta com as credenciais desejadas após a verificação da mensagem recebida por meio da *blockchain*. Deve-se enfatizar que a autenticidade de todas as mensagens resultantes da interação entre os agentes são verificadas com apoio da *blockchain* a cada interação.

A resposta criada pelo agente cliente na carteira digital contendo as credenciais solicitadas é codificada em JWT e enviada, por meio de uma requisição HTTP POST, para o emissor de credenciais (passo 5). O servidor emissor então recebe a resposta e realiza a decodificação da mesma, também verificando sua validade. Com isso, o emissor de CVs gera as credenciais solicitadas, codificando-as em um JWT, renderizado em um QR Code, enviando-as ao navegador. Por fim, a carteira digital do dispositivo móvel do agente cliente escaneia o código QR e armazena as credenciais emitidas.

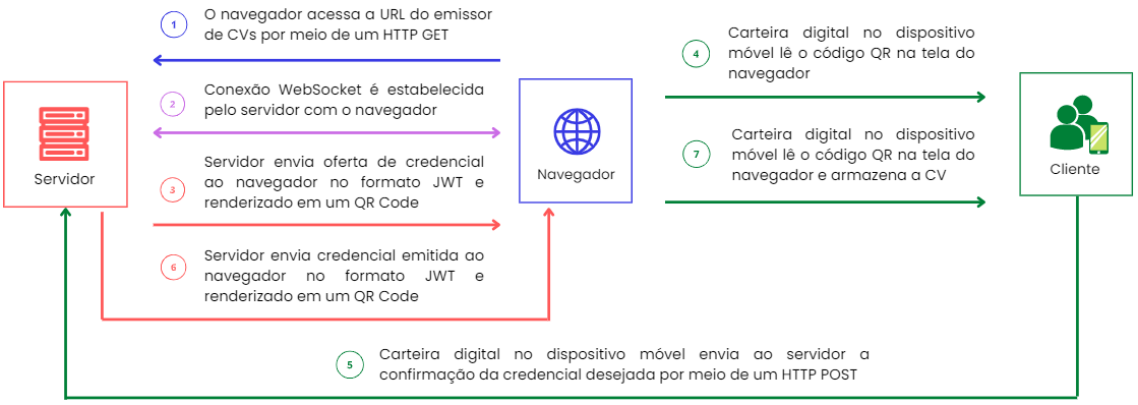

Figura 5. Fluxo de emissão e recebimento de credenciais verificáveis da plataforma de testes, com agente cliente em aplicativo móvel *Jolocom SmartWallet*.

6.2. Fluxo de verificação de credenciais

O segundo fluxo de comunicação implementado foi o fluxo de solicitação, fornecimento e verificação de credenciais verificáveis. A implementação deste fluxo é muito semelhante

[6] https://play.google.com/store/apps/details?id=com.jolocomwallet
[7] https://apps.apple.com/us/app/jolocom-smartwallet/id1223869062

à anterior, havendo agora um provedor de serviços (SP) como servidor que solicita a apresentação de uma credencial para que o agente cliente acesse seus serviços. Assim como exposto na seção anterior, dois casos foram simulados: o agente cliente na máquina de testes (Figura 6), bem como o agente cliente sendo representado pela carteira digital no dispositivo móvel (Figura 7). Como o fluxo do segundo abarca todas as situações do primeiro, diferenciando apenas no redirecionamento para a carteira digital, o discutiremos em detalhes.

Em ambos os casos, o agente cliente - que já possui uma identidade descentralizada e uma credencial verificável instanciada (seja em seu dispositivo móvel, seja localmente na máquina de testes) - realiza uma requisição HTTP GET na URL do SP. No caso da Figura 7, essa requisição ocorre a partir de um navegador. Após a requisição, o segundo passo para o caso do agente cliente no celular é o estabelecimento de uma conexão *WebSocket* entre o provedor de serviço e o navegador. A solicitação de credencial então é gerada por parte do SP e transmitida para o navegador no passo 3 (ou diretamente para o usuário, no passo 2 da Figura 6), contendo informações codificadas em um *token* JWT (referentes ao tipo de credencial exigida), que será renderizada em um código QR pelo navegador.

No passo 4 da Figura 7, a aplicação móvel escaneia o código QR, decodifica o JWT, verifica sua autenticidade a partir da *blockchain* e cria uma resposta contendo as credenciais exigidas para o acesso ao serviço. Esta resposta é também codificada em JWT e enviada por meio de uma requisição para o SP por meio de uma requisição POST do dispositivo móvel para a plataforma de testes (passo 5). Recebendo a resposta, o SP decodifica o *token*, verifica sua autenticidade com apoio da *blockchain*. Caso o agente cliente tenha as credenciais necessárias e validadas, o usuário é autenticado e tem acesso ao serviço solicitado (passo 6).

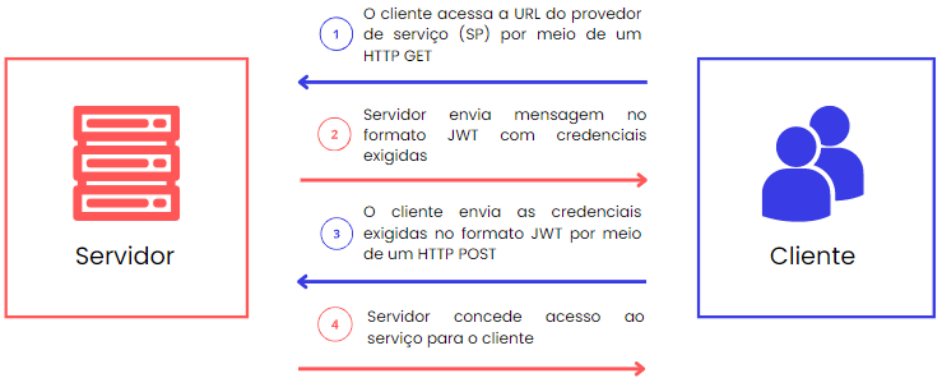

Figura 6. Fluxo de solicitação, fornecimento e verificação de credenciais verificáveis da plataforma de testes.

7. Proposta de um sistema de autenticação híbrido

O modelo de gestão de identidades federadas é muito popular atualmente. Nele, cada domínio de identidade tem um único provedor de identidade (o qual chamaremos de IdP, responsável por armazenar e compartilhar dados da identidade de um usuário com diferentes domínios) e diversos provedores de serviços (ou SPs, responsáveis por fornecer serviços online a um usuário com base em seu perfil conforme recebido do IdP)

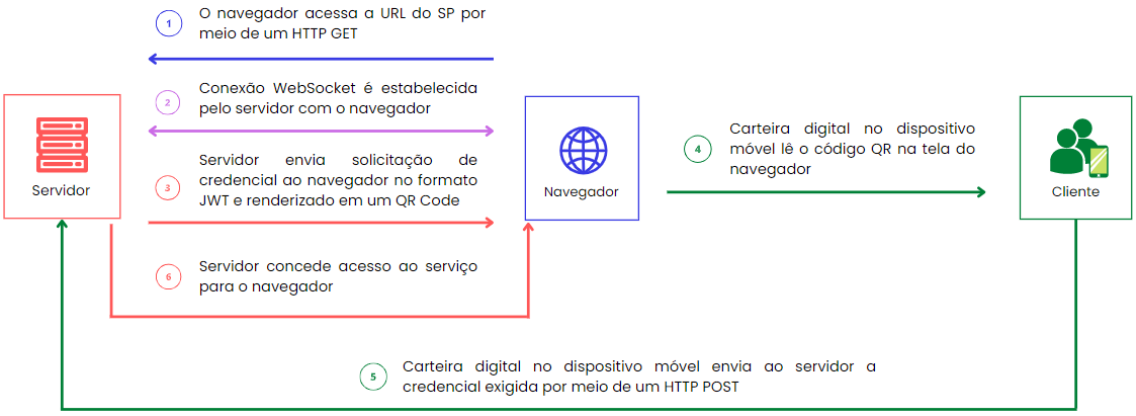

Figura 7. Fluxo de solicitação, fornecimento e verificação de credenciais verificáveis da plataforma de testes, com agente local criado por meio do aplicativo móvel *Jolocom SmartWallet*.

[Ferdous et al. 2019]. Nesse contexto, portanto, os usuários poderiam estar registrados em apenas um IdP para acessar os mais diversos serviços disponíveis na *web*. Por outro lado, os SPs devem reconhecer e serem reconhecidos pelos IdPs ou federações de IdPs desejados para trabalhar com usuários identificados e autenticados, de modo que uma relação de confiança é necessária entre IdPs e SPs. Como exemplo de soluções que provêem o gerenciamento de identidades federadas, destaca-se o *Shibboleth*[8] e o *Microsoft CardSpace* [Bertocci et al. 2007]. Usando a tecnologia *Shibboleth*, a Rede Nacional de Ensino e Pesquisa - RNP estruturou uma federação de identidades entre as universidades e instituições de pesquisa brasileiras chamada CAFe - Comunidade Acadêmica Federada[9], a qual conta hoje com quase 300 instituições (IdPs) que dão acesso a mais de 70 provedores de serviços (SPs) no Brasil e no exterior.

Como o modelo de gestão de identidades federadas fomenta concentração de dados do usuário nos IdPs federados e não provê um controle maior do usuário sobre seus dados, seria interessante poder avaliar os benefícios que a implementação de um sistema de gestão de identidades baseado em SSI traria para as instituições e seus usuários, como na federação CAFe, por exemplo. No entanto, em um sistema que está beneficiando um grande número de usuários, como na CAFe, não é possível realizar uma transição imediata de um modelo de gestão para outro. Um processo de transição desse porte teria de ser implementado gradualmente durante uma janela de tempo razoável (talvez em alguns anos) e exigiria uma coexistência de duas formas de autenticação e de compartilhamento de credenciais.

Nossa proposta de implementação do modelo de identidade descentralizada é a seguinte: o sistema federado continua o mesmo até que todos os provedores de identidade tenham se preparado para SSIs. As instituições que aderirem ao novo modelo SSI deveriam implementar um novo fluxo de autenticação baseado em protocolos SSI. Tal proposta tornou-se mais simples a partir da versão 4 do IdP *Shibboleth*, que permite a construção de estratégias mais sofisticadas de autenticação utilizando fluxos de autenticação externos ao IdP. Desse modo, ao acessar um serviço via navegador, o usuário seria redirecionado ao

[8] https://shibboleth.atlassian.net/wiki/spaces
[9] https://www.rnp.br/servicos/cafe

IdP de sua instituição, que lhe apresentaria duas opções de se autenticar: via *login*/senha tradicional ou via credenciais verificáveis de SSI armazenadas em seu dispositivo móvel. Após a autenticação, de um modo ou de outro, o IdP prepararia e enviaria asserções SAML para o SP, sem que esse precisasse saber que a autenticação foi feita via SSI.

Usando um fluxo externo de autenticação para implementar SSI, o IdP solicita ao agente de verificação de credenciais do Jolocom que faça a solicitação e validação de credenciais do usuário conforme descrito anteriormente. Se a autenticação for bem sucedida, as informações básicas do usuário solicitadas pelo SP devem ser passadas da wallet do usuário para o IdP e deste (via asserções SAML) para o SP. Nesse método, deve-se salientar que uma vez que o controle é transferido para o mecanismo externo, o IdP não tem controle sobre o que acontece e terá que confiar em qualquer informação passada de volta pelo Jolocom. Assim, torna-se viável um sistema de autenticação híbrido, facilitando uma transição suave entre os modelos. De maneira mais detalhada, o fluxo de autenticação híbrido com os protocolos SSI e Shibboleth pode ser resumido nos seguintes passos: (i) O fluxo inicia-se com o usuário solicitando o acesso a um serviço qualquer; (i) O provedor de serviço encaminhará o usuário para um IdP; (iii) O IdP disponibilizará duas formas de autenticação: o esquema usual login/senha e a autenticação via solução descentralizada (no caso, implementada por meio da plataforma Jolocom); (iv) Com o usuário escolhendo a autenticação SSI pelo navegador, o IdP redireciona o fluxo de autenticação para um servidor externo com o serviço Jolocom de verificação de credenciais; (v) O navegador conecta-se ao servidor Jolocom para se autenticar; (vi) O Servidor Jolocom envia ao navegador uma mensagem codificada em JWT solicitando as CVs necessárias para o acesso ao serviço; (vii) A mensagem é transformada em um QR Code que o usuário escaneia com sua carteira digital (Jolocom Smart Wallet); (viii) se estiver de acordo, o usuário autorizao o envio das CVs solicitadas para o servidor Jolocom; (ix) O Servidor Jolocom verifica a autenticidade das CVs e, caso válidas, repassa as mesmas ao IdP para que este possa criar as asserções SAML; (x) O IdP envia as CVs no padrão Shibboleth ao navegador, que as redireciona para o provedor de serviços e (xi) O SP recebe as credenciais do navegador, verifica sua autencidade e concede ao usuário o acesso ao serviço.

Uma alternativa ao esquema acima baseado em fluxo customizado é a implantação de um IdP extra em cada instituição, focado na autenticação com SSI via fluxo externo único. Por ser de implementação mais simples, temos feito testes com esse tipo de IdP, que tem fluxo de autenticação externo com um sistema de SSI Jolocom e se comunica via asserções SAML com os SPs. A implementação do fluxo externo no IdP Shibboleth usado na federação CAFe está sendo feita com o apoio do GIdLab - Laboratório de Experimentação em Gestão de Identidades da RNP, mas até o momento desta publicação, devido a algumas dificuldades técnicas encontradas ao tentar compatibilizar as diferentes tecnologias adotadas, não foi possível viabilizar o fluxo externo no IdP para comunicação com um servidor Jolocom. Acreditamos que tais dificuldades não são insuperáveis e poderão ser resolvidas em breve.

Mesmo com a implantação de IdPs compatíveis por um lado com a autenticação via DID e por outro com um protocolo já amplamente utilizado (Shibboleth), ainda restam vários desafios a serem vencidos. Dentre eles, destacam-se a transferência para o usuário da responsabilidade pela gestão de sua identidade, a necessidade de interfaces humano-computador que facilitem essa gestão para os usuários sem grande familiaridade com

sistemas mais complexos e os novos custos que deverão surgir para a implantação de uma blockchain privada (permissionada) ou para o pagamento de taxas de transações em blockchains públicas consolidadas. A implantação de IdPs híbridos irá permitir uma avaliação profunda desses desafios sem interromper os serviços providos pela federação atualmente.

8. Conclusões e trabalhos futuros

Diante dos problemas trazidos pela centralização de informações de identidades digitais, tais como compartilhamento indevido de dados pessoais e falta de autonomia por parte dos usuários no tratamento de suas próprias informações, diversos modelos de gestão de identidades digitais evoluíram e foi nesse cenário que emergiram novas ideias baseadas em Identidades Descentralizadas (DID - *Decentralized ID*) e Credenciais Verificáveis (CV), com o objetivo de dar ao usuário mais controle sobre seus dados pessoais. Possuindo ferramentas que implementam uma solução descentralizada eficiente, a plataforma Jolocom foi utilizada para testes do fluxo de comunicação entre agentes no contexto SSI. Tais testes permitiram conhecer e avaliar melhor todos os detalhes envolvidos na implementação de um sistema SSI e assim dar um embasamento melhor para a discussão de implementações em larga escala desse modelo. Foi proposto um modelo de autenticação híbrido para IdPs de sistemas federados baseados em Shibboleth (como o da Federação CAFe) de forma a permitir tanto uma avaliação mais detalhada do modelo descentralizado como uma eventual adoção gradual desse novo modelo na federação. Foi possível constatar que haverá uma maior complexidade para os usuários na gestão de suas identidades, em troca da maior autonomia nessa gestão, mas não está claro ainda quantos desses usuários estarão de fato dispostos a assumir esta carga. Vai ser preciso conhecer melhor a relação custo/benefício dessa transição.

Em relação a trabalhos futuros, é preciso concluir os testes de implementação de um fluxo de autenticação externo no IdP *Shibboleth*, de forma a melhor avaliar o sistema híbrido de autenticação. Além disso, é necessário um aprofundamento do estudo sobre a usabilidade da solução SSI - tendo em vista a carga de gerenciamento das identidades digitais no usuário - e sobre a efetividade das âncoras de confiança em uso e baseadas, majoritariamente, em *blockchains*. Por fim, é importante avaliar os custos da utilização de blockchains em soluções SSI. Em *blockchains* comerciais, o processo de ancoragem das DIDs pode ser inviável economicamente. Porém, em *blockchains* de baixo custo, como a que o *CT-Blockchain* está propondo construir em nível nacional sob a coordenação da RNP, tal uso seria mais plausível. Essas e outras questões - como a alternativa KERI (*Key Event Receipt Infrastructure*)[10], desenvolvida pela Jolocom - devem ser estudadas e comparadas para se ter uma ideia mais precisa da viabilidade prática das propostas de adoção de identidade descentralizada.

Referências

Allen, C. (2016). *"The Path to Self-Sovereign Identity"*. Life with Alacrity, http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html, April.

[10]`https://jolocom.io/blog/how-keri-tackles-the-problem-of-trust/`

Bertocci, V., Serack, G., and Baker, C. (2007). *"Understanding Windows Cardspace: an introduction to the concepts and challenges of digital identities"*. Pearson Education.

Buchner, D., Steele, O., and Ronda, T. (2021). *"Sidetree v1.0.0 - DIF Ratified Specification"*. Technical Report, Decentralized Identity Foundation. https://identity.foundation/sidetree/spec/. March.

Fei, C., Lohkamp, J., Rusu, E., Szawan, K., K., W., and Wittenberg, N. (2019). *"Jolocom Whitepaper"*. https://jolocom.io/wp-content/uploads/2019/12/Jolocom-Whitepaper-v2.1-A-Decentralized-Open-Source-Solution-for-Digital-Identity-and-Access-Management.pdf. March.

Ferdous, M., Chowdhury, F., and Alassafi, M. (2019). *"In Search of Self-Sovereign Identity Leveraging Blockchain Technology"*. IEEE Access, vol. 7, pp. 103059-103079. doi: 10.1109/ACCESS.2019.2931173.

Jones, M., Bradley, J., and Sakimura, N. (2015). *"JSON Web Token (JWT)"*. Internet Engineering Task Force (IETF). ISSN: 2070-1721 (No. rfc7519). datatracker.ietf.org/doc/html/rfc7519. May.

Naik, N. and Jenkins, P. (2020). *"uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain"*. In 2020 IEEE International Symposium on Systems Engineering (ISSE) (pp. 1-7). IEEE. October.

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., and Sabadello, M. (2021). *"Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations"*. W3C Working Draft.

Schardong, F. and Custódio, R. (2021). *"Self-Sovereign Identity: A Systematic Map and Review"*. ACM Comput. Surv. 1, 1, Article 1.

Sporny, M., Longley, D., Chadwick, D., Reed, D., Steele, O., and Allen, C. (2021). *"Verifiable Credentials Data Model 1.0"*. W3C - World Wide Web Consortium. https://w3c.github.io/vc-data-model/. July.

Wolff, B. and Henriques, M. (2021). *"Estudo experimental sobre Gestão de Identidades Autossoberanas para avaliação de riscos e oportunidades de adoção pela RNP"*. Anais do XXI SBSeg - Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, WGID - Workshop de Gestão de Identidades Digitais.