Plataforma Híbrida de Identidades Auto-Soberanas para Integração Web2–Web3 com Autenticação Federada e Auditoria em Blockchain

Yago de R. dos Santos[1], **Nicollas R. de Oliveira**[1], **Dianne S. V. Medeiros**[1], **Diogo M. F. Mattos**[1]

[1] LabGen/MídiaCom – TET/IC/PPGEET/UFF
Universidade Federal Fluminense (UFF)
Niterói, RJ – Brasil

Abstract. *The increasing digitalization of services heightens the dependence on secure and interoperable digital identities, but the integration of self-sovereign identities into legacy infrastructures still faces challenges. This article proposes the PIDDF, a hybrid platform that connects Web 2 and Web 3 ecosystems by integrating self-sovereign identities with federated authentication based on OpenID Connect. The methodology includes the implementation of a functional prototype with distributed components, such as key management and decentralized identifier registration, the implementation of a blockchain-based audit trail, and the execution of performance and stability experiments in a controlled environment. The results show that PIDDF maintains credential issuance and verification latency in the same order of magnitude as traditional web systems, with variations below 10% under moderate load, while introducing immutable audit trails and separation of identity attributes, indicating the practical feasibility of integrating the platform into Web 2 systems.*

Resumo. *A crescente digitalização de serviços aumenta a dependência de identidades digitais seguras e interoperáveis, mas a integração de identidades auto-soberanas a infraestruturas legadas ainda enfrenta desafios. Este artigo propõe a PIDDF, uma plataforma híbrida que conecta ecossistemas Web 2 e Web 3 ao integrar identidades auto-soberanas com autenticação federada baseada em OpenID Connect. A metodologia inclui a implementação de um protótipo funcional com componentes distribuídos, tais como gestão de chaves e registro de identificadores descentralizados, implementação de cadeia de auditoria em blockchain e a realização de experimentos de desempenho e estabilidade em ambiente controlado. Os resultados mostram que a PIDDF mantém latência de emissão e verificação de credenciais em ordem de grandeza compatível com sistemas Web tradicionais, com variação inferior a 10% sob carga moderada, ao mesmo tempo em que introduz trilhas de auditoria imutáveis e separação de atributos de identidade, indicando a viabilidade prática da integração a sistemas da Web 2.*

1. Introdução

O processo de digitalização de serviços públicos e privados intensifica a dependência de mecanismos de identidade digital para autenticação e controle de acesso em ambientes

online. Modelos centralizados de gestão de identidades, controlados por provedores de serviços ou plataformas privadas, concentram dados pessoais e aumentam riscos de vazamentos, uso indevido e acessos não autorizados [Olivero et al. 2020, Sim et al. 2019], enquanto legislações como GDPR e LGPD impõem requisitos adicionais de tratamento de dados, reforçando a necessidade de alternativas que mitiguem limitações de modelos centralizados ou federados [Naik and Jenkins 2020b].

Soluções baseadas em tecnologias descentralizadas, como *blockchain*, buscam ampliar o controle dos usuários sobre suas identidades digitais [de Rezende dos Santos et al. 2025]. O paradigma de Identidades Auto-Soberanas (*Self-Sovereign Identity* – SSI) permite que indivíduos mantenham posse e gestão de suas credenciais [Mazzocca et al. 2025], mas enfrenta desafios de gestão de chaves, adoção por usuários não técnicos e integração com infraestruturas legadas [Maram et al. 2021], o que limita sua adoção em ambientes baseados em autenticação tradicional.

Este trabalho propõe a PIDDF, uma plataforma para provisionamento descentralizado de Identidades Auto-Soberanas com base em Credenciais Verificáveis (VCs) e Identificadores Descentralizados (DIDs), integrada a autenticação federada e auditoria em *blockchain*. A solução inclui um componente modular de emissão e verificação de VCs, utiliza DIDs gerenciados pela rede Trustbloc Orb [1] e ancora registros de auditoria em uma *blockchain* permissionada Hyperledger Fabric, combinando confiança da SSI com interoperabilidade em ambientes Web 2.

As principais contribuições são: (i) a plataforma PIDDF, de código aberto, para identidades descentralizadas com suporte à autenticação federada; (ii) uma arquitetura baseada no modelo de referência do Trustbloc integrada ao *OpenID Connect* (OIDC); (iii) um módulo de emissão e verificação de VCs integrado ao Trustbloc Orb para registro e resolução de DIDs; e (iv) um mecanismo de gestão segura de chaves baseado no OpenBao, que restringe o acesso às chaves ao usuário autenticado via *tokens*. Essas contribuições aproximam o paradigma de Identidade Auto-Soberana das arquiteturas de autenticação federada consolidadas.

O restante deste artigo está organizado da seguinte forma. A Seção 2 apresenta os principais conceitos sobre Identidades Auto-Soberanas (SSI), Identificadores Descentralizados (DID) e Credenciais Verificáveis (VC). A Seção 3 discute os trabalhos relacionados. A Seção 4 apresenta a arquitetura da solução proposta. A Seção 5 descreve o modelo de ameaças e analisa a sua segurança. A Seção 6 apresenta os resultados experimentais. Por fim, a Seção 7 conclui o trabalho.

2. Identificadores Descentralizados, Credenciais Verificáveis e Identidades Auto-Soberanas

Identificadores Descentralizados (*Decentralized Identifiers* – DIDs) são identificadores de recursos uniformes (*Uniform Resource Identifier* - URIs) únicos usados para identificar entidades digitais e resolver metadados por meio de Documentos DID, conforme o padrão [2] definido pelo World Wide Web Consortium (W3C). Esses identificadores permitem associar a uma identidade digital informações verificáveis, como chaves crip-

[1]Disponível em `https://trustbloc.readthedocs.io`.
[2]Disponível em `https://www.w3.org/TR/did-1.1/`.

tográficas públicas, serviços e referências a documentos ou credenciais, sem depender de registros centralizados, provedores de identidade ou autoridades certificadoras. Estruturalmente, um DID é composto pelo esquema URI, pelo identificador do método e pelo identificador específico do método, combinação que permite localizar o Documento DID associado; a Figura 1 ilustra esses componentes, enquanto o Código 1 mostra um exemplo de Documento DID com uma chave pública de autenticação.

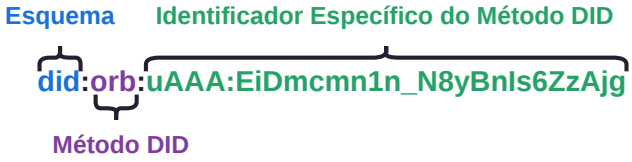


Figura 1. Endereço DID destacando os três componentes utilizados na resolução de um Documento DID: em azul, o esquema do DID; em roxo, o método DID utilizado para sua resolução; por último, em verde, o identificador específico do método.

Código Fonte 1. Exemplo de Documento DID conforme o modelo de dados do W3C.

```
{
"@context": "https://www.w3.org/ns/did/v1.1",
"id": "did:orb:uAAA:EiDmcmn1n_N8yBnIs6ZzAjg",
"authentication": [{
"id": "did:example:123456789abcdefghi#keys-1",
"type": "Multikey",
"controller": "did:orb:uAAA:EiDmcmn1n_N8yBnIs6ZzAjg",
"publicKeyMultibase":
  ↪  "z6MkmM42vxfqZQsv4ehtTjFFxQ4sQKS2w6WR7emozFAn5cxu"
}]
}
```

Credenciais Verificáveis (*Verifiable Credentials* – VCs) são representações digitais de atributos de uma entidade, estruturadas de forma criptograficamente verificável e resistentes à adulteração, conforme o modelo de dados [3] definido pelo *World Wide Web Consortium* (W3C). Esse modelo organiza um ecossistema com três entidades principais: o Emissor, que emite e assina digitalmente a credencial; o Detentor, que armazena e controla seu uso, tipicamente em uma carteira digital; e o Verificador, que valida a credencial apresentada com base na chave pública associada ao identificador do emissor. Durante a apresentação, o Detentor pode compartilhar a VC completa ou apenas partes dela usando Provas de Conhecimento Zero (*Zero-Knowledge Proofs* – ZKP), o que permite comprovar atributos específicos sem divulgar todo o conteúdo, aumentando a segurança e a privacidade pela integridade criptográfica, verificação independente e redução da exposição de dados pessoais. As VCs podem ser representadas em diferentes formatos, sendo o JSON-LD amplamente utilizado em aplicações web, como ilustrado no Código 2, em que a chave *credentialSubject* reúne os atributos da credencial e a chave *proof* contém os dados de assinatura e a DID usada na validação.

[3] Disponível em `https://www.w3.org/TR/vc-data-model-2.0/`.

Código Fonte 2. Exemplo de Credencial Verificável com prova por assinatura

```
{
"type": [
"VerifiableCredential",
"Profile"
],
"issuer": "did:orb:uAAA:EiAr5...",
"credentialSubject": {
"did": "did:orb:uAAA:EiDiP...",
"additionalName": "John Doe",
"email": "johndoe@email.com",
},
"proof": {
"type": "'JsonWebKey2020'",
"verificationMethod": "did:orb:uAAA:EiDiP...#issuer-key-1",
"jws": {
"signature": "vault:v1:MEQCI..."
}
}
}
```

A Identidade Auto-Soberana (*Self-Sovereign Identity* – SSI), por sua vez, é um modelo descentralizado de gestão de identidades em que indivíduos mantêm posse e controle sobre seus dados pessoais por meio de credenciais digitais verificáveis criptograficamente, sem depender de autoridades certificadoras ou provedores centralizados. Esse modelo se organiza em torno do triângulo de confiança composto por Emissor, Detentor e Verificador, ilustrado na Figura 2.

3. Trabalhos Relacionados

Diversos trabalhos recentes investigam o uso de Identidades Auto-Soberanas (SSI) como alternativa aos modelos centralizados de gerenciamento de identidade, abordando principalmente interoperabilidade com sistemas existentes, escalabilidade, privacidade, gerenciamento de confiança e adoção prática em ambientes reais. Em geral, essas propostas exploram a integração de SSI com infraestruturas federadas (SAML e OpenID Connect), o uso de mecanismos criptográficos avançados, como provas de conhecimento zero, arquiteturas específicas para IoT e controle de acesso baseado em atributos, além de análises de desempenho em diferentes tecnologias de registro distribuído. Contudo, poucos trabalhos visam uma solução completa que concilie interoperabilidade com sistemas legados, gestão segura de chaves, auditoria imutável e suporte explícito a ambientes Web 2/Web 3.

Yildiz *et al.* integram credenciais SSI a sistemas federados baseados em SAML em um contexto real de universidades alemãs, permitindo reaproveitar provedores de identidade existentes [Yildiz et al. 2021] . Diferentemente dessa abordagem, que adapta um IdP específico e não avalia segurança ou desempenho, a PIDDF consiste em uma arquitetura interoperável mais geral baseada em OpenID Connect, com componentes de auditoria e gerenciamento de chaves voltados a ambientes híbridos.

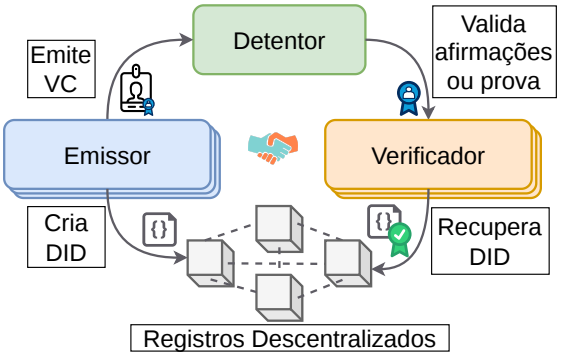


Figura 2. Entidades de confiança das Identidades Auto-Soberanas. O Emissor, em azul, emite uma VC para o Detentor e registra uma DID nos registros descentralizados. O Detentor, ilustrado em verde, pode apresentar a credencial ou apenas uma prova de posse ao Verificador. Por fim, o bloco laranja apresenta o Verificador, que recupera a DID na rede de registros descentralizados para validar a autenticidade da VC.

Grüner *et al.* apresentam um *gateway* modular que integra múltiplas plataformas SSI (uPort [Naik and Jenkins 2020a], Jolocom [Fei et al. 2018]) a aplicações web via OpenID Connect [Grüner et al. 2019]. Enquanto esse trabalho enfatiza a interoperabilidade entre soluções SSI, a proposta PIDDF adiciona mecanismos explícitos de auditoria em *blockchain* e gestão segura de chaves, visando segurança e rastreabilidade.

Lux *et al.* propõem um provedor OpenID Connect descentralizado baseado em DIDs e VCs, permitindo autenticação diretamente com credenciais descentralizadas e eliminando senhas [Lux et al. 2020]. Em contraste, a PIDDF mantém a infraestrutura federada existente e separa autenticação de provisionamento de identidades descentralizadas, favorecendo uma adoção gradual sem substituir os mecanismos de login já implantados.

Outros trabalhos introduzem modelos de identidade descentralizada com foco em segurança, privacidade e gestão de confiança, usando *blockchain*, credenciais duplas e provas de conhecimento zero, especialmente em IoT [Yin et al. 2022, Yin et al. 2025]. Diferentemente dessas propostas, orientadas a cenários específicos e mecanismos de reputação, a PIDDF concentra-se em integração arquitetural com sistemas federados e em componentes práticos de emissão, verificação e auditoria de credenciais em ambientes web corporativos. Há ainda trabalhos que exploram mecanismos criptográficos avançados, tais como árvores de Merkle, provas de conhecimento zero, extensões ao XACML, para autenticação descentralizada e controle de acesso baseado em atributos com SSI [Xie et al. 2025, Maesa et al. 2023]. A PIDDF, contudo, prioriza uma arquitetura interoperável construída sobre padrões amplamente adotados (OIDC, DIDs, VCs, Hyperledger Fabric, OpenBao), buscando integração com sistemas legados em vez de substituir completamente a infraestrutura de chave pública e de autorização existente.

O sistema CanDID torna identidades descentralizadas mais utilizáveis por meio de integração com serviços web, recuperação de chaves e resistência a ataques Sybil [Maram et al. 2021]. Em contraste, a PIDDF foca a interoperabilidade arquitetural com autenticação federada baseada em OpenID Connect, integrando resolução de DIDs, emissão/verificação de VCs e auditoria imutável em uma plataforma coesa.

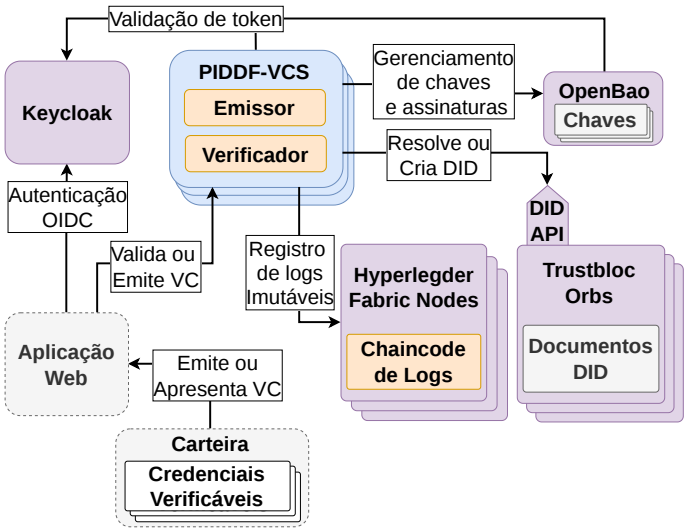


Figura 3. Arquitetura da plataforma PIDDF. Os componentes externos integrados à plataforma são representados em roxo. Em azul está o PIDDF-VCS, componente principal responsável pela emissão e verificação de VCs. Os blocos internos, em laranja, correspondem às implementações próprias da plataforma PIDDF. Em cinza com bordas pontilhadas, estão os módulos independentes não implementados pela PIDDF.

Por fim, Alizadeh *et al.* avaliam desempenho e escalabilidade de abordagens de identidade descentralizada baseadas em DLT, DHT e IPFS, mostrando vantagens potenciais de armazenamento distribuído em certos cenários [Alizadeh et al. 2022]. Diferentemente desse estudo experimental em pequena escala, o PIDDF define uma arquitetura completa de provisionamento de identidades descentralizadas com suporte à autenticação federada e auditoria, pensada para operação em ambientes de produção e integração com infraestruturas web consolidadas.

4. PIDDF: Plataforma de Identidade Digital Distribuída com autenticação Federada

A plataforma PIDDF integra Identidades Auto-Soberanas (SSI) a sistemas tradicionais de gestão de identidade e autenticação federada, preservando as vantagens de segurança e privacidade das SSIs. A Figura 3 apresenta a arquitetura da plataforma, na qual aplicações web se conectam ao módulo PIDDF-VCS, responsável por emitir e verificar Credenciais Verificáveis (VC) por meio de dois submódulos: o Emissor, que coordena criação/recuperação de chaves, criação e resolução de Identificadores Descentralizados (DID) e assinatura das credenciais, e o Verificador, que valida a assinatura da VC usando a chave pública presente no Documento DID correspondente. Essa organização introduz uma camada de intermediação entre aplicações legadas e o ecossistema de identidades descentralizadas, alinhando o fluxo de autenticação federada com a provisão de VCs.

Para simplificar a adoção de SSIs em sistemas legados, a PIDDF abstrai o gerenciamento de chaves usadas na validação de DIDs e VCs por meio da integração ao OpenBao, uma solução de código aberto para armazenamento e distribuição segura de segredos, chaves e certificados. Além da gestão segura de material criptográfico, o OpenBao

integra-se ao protocolo OIDC para autenticação, o que o alinha diretamente aos objetivos de interoperabilidade federada da plataforma PIDDF. Essa combinação permite delegar a complexidade de chaves a um componente especializado, mantendo o foco da plataforma na emissão e verificação de credenciais.

Para validação descentralizada de credenciais, o PIDDF-VCS integra-se ao Trustbloc Orb, que implementa o método DID *did:orb*, baseado no protocolo *Sidetree*, formando uma federação de nós interconectados. Esse método atua como registro verificável e agnóstico ao livro-razão (*ledger*), gerenciando DIDs *off-chain* com opções de transparência e verificação *on-chain*, independentemente da *blockchain* subjacente. Na PIDDF, o módulo PIDDF-VCS realiza as verificações, enquanto as provas de não repúdio são registradas no Hyperledger Fabric como registros de atividades (*logs*) imutáveis em uma árvore de Merkle, garantindo rastreabilidade dos eventos críticos de identidade.

Embora o PIDDF-VCS inclua agentes de emissão e verificação, ambos operam de forma independente, permitindo que uma organização atue apenas como emissora ou apenas como verificadora, conforme a necessidade. Essa separação facilita a escalabilidade horizontal, pois é possível aumentar somente as instâncias de um dos agentes, e reflete o triângulo de confiança em sua forma clássica. Como ilustrado na Figura 3, a aplicação web e a carteira digital integram o ecossistema de identidades descentralizadas, mas estão fora do escopo de implementação da PIDDF, que concentra-se exclusivamente na emissão e verificação de VCs em um ambiente de autenticação federada.

A emissão de uma VC na plataforma PIDDF ocorre da seguinte forma. Inicialmente, o usuário envia seus dados de credencial ao agente emissor do PIDDF-VCS, diretamente ou via aplicação web integrada conforme a arquitetura da Figura 3, e é redirecionado para um autenticador federado compatível com OpenID Connect (OIDC). Após a autenticação, o agente emissor recebe o JWT do usuário e solicita ao OpenBao, que também valida o JWT no sistema de origem, a geração de um BaoToken para executar operações de chave criptográfica, preparando o contexto para a criação da VC.

Com o BaoToken, o agente emissor cria ou recupera três chaves no OpenBao, cada uma associada a uma função específica no ciclo de vida do DID e da VC. A chave de verificação assina a VC e tem sua parte pública registrada no Documento DID, a chave de atualização permite modificar o DID quando necessário e a chave de recuperação atua como mecanismo de restauração das versões do DID em caso de falhas. Em seguida, o agente emissor cria o Documento DID em JSON-LD, incluindo as origens aceitas de tokens para validar VCs associadas ao DID e a chave pública de verificação, adiciona campos de validação derivados do *hash* do conteúdo e das chaves públicas de atualização e recuperação, registra o documento no Trustbloc Orb via API e recebe o endereço DID.

Com o DID criado, o emissor monta o conteúdo completo da VC com base nos dados de credencial do usuário, no endereço do autenticador federado e no DID de validação. A VC é então enviada ao OpenBao para assinatura com a chave privada de verificação, a assinatura é incorporada à credencial, e a VC resultante é entregue ao usuário, enquanto a criação do DID e a assinatura da credencial são registradas como logs imutáveis na *blockchain*. Esse fluxo garante que cada credencial emitida esteja vinculada a um DID resolvível e a chaves gerenciadas de forma segura.

A validação de uma VC inicia-se quando uma aplicação web integrada à PIDDF

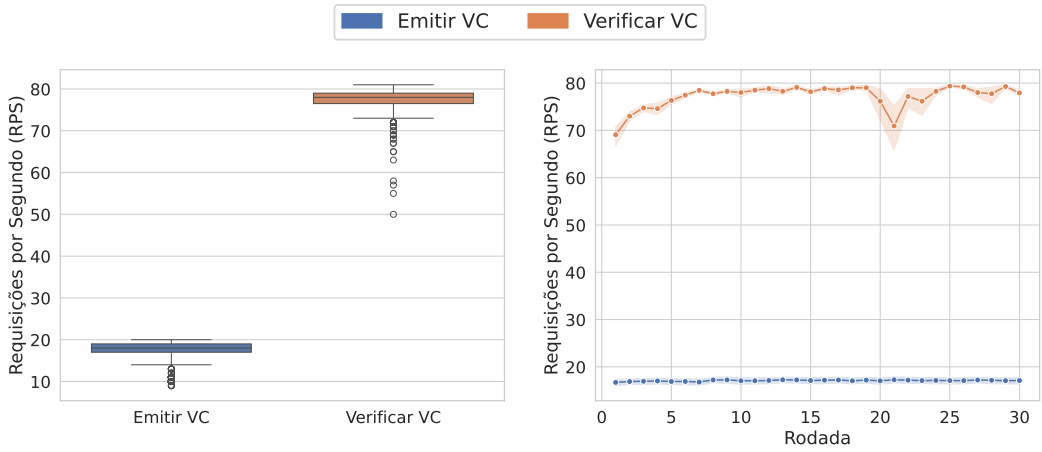
identifica, na própria credencial, o sistema de autenticação federada responsável pela emissão do JWT do usuário. Após autenticar o usuário nesse sistema, a aplicação envia a VC e o JWT para uma instância do agente verificador do PIDDF-VCS, que passa a conduzir o processo de verificação criptográfica, garantindo que apenas sessões autenticadas avancem para a etapa de validação.

O agente verificador valida primeiro o JWT em sua origem, garantindo a autenticidade da sessão federada. Em seguida, a partir da VC, identifica o endereço DID do Documento DID que contém a chave pública usada na verificação da credencial e o resolve no Trustbloc Orb, obtendo o documento correspondente com os endereços autorizados para validação do JWT e a chave pública de verificação da VC. Com essa chave, o agente valida a assinatura da credencial, retorna o resultado à aplicação web, que pode liberar o acesso do usuário e utilizar os dados da VC com garantia de autenticidade, e registra a verificação bem-sucedida como log imutável na *blockchain* para fins de auditoria.

5. Modelo de Ameaças e Análise de Segurança

Este trabalho adota explicitamente um modelo de ameaça baseado em STRIDE para orientar a análise de segurança. Nesse cenário, um provedor OIDC estabelece a sessão do usuário, enquanto os atributos de identidade são representados por Credenciais Verificáveis (VCs) no modelo SSI, e assume-se a presença de adversários capazes de observar, interceptar e modificar comunicações, mas sem acesso às chaves privadas usadas na emissão e assinatura das credenciais; o STRIDE é então usado para classificar ameaças em falsificação, adulteração, repúdio, divulgação de informações, negação de serviço e elevação de privilégio.

No caso de **falsificação de identidade** (*Spoofing*), a combinação de autenticação federada via OIDC com VCs assinadas e vinculadas a Identificadores Descentralizados (DIDs) permite verificar a identidade de usuários e emissores a partir dos Documentos DID, dificultando que atacantes se passem por participantes legítimos. Na adulteração de dados (*Tampering*), assinaturas digitais e a verificação de chaves públicas em Documentos DID impedem que VCs modificadas sejam aceitas, enquanto eventos de emissão e verificação são registrados em *blockchain* Hyperledger Fabric, reforçando integridade e rastreabilidade. Para **não-repúdio** (*Repudiation*), a PIDDF mantém *logs* imutáveis na *blockchain* das operações de emissão e verificação de VCs, fornecendo evidências de ações associadas a DIDs e papeis específicos. Em relação ao **vazamento de informações** (*Information Disclosure*), a separação entre autenticação federada e atributos de identidade mantém os dados sob controle do usuário, que decide quais atributos ou provas derivadas apresentar, reduzindo o armazenamento de dados sensíveis em sistemas tradicionais e a superfície de exposição. No contexto de **negação de serviço** (*Denial of Service*), a proposta mitiga ataques com o uso de infraestrutura distribuída para resolução de DIDs e mecanismos tradicionais de defesa contra DoS nos provedores federados, preservando a disponibilidade dos serviços de identidade. Por fim, na **elevação de privilégio** (*Elevation of Privilege*), a PIDDF foca em autenticidade, integridade, não repúdio e controle de exposição de atributos, delegando às aplicações consumidoras de VCs a definição de políticas de autorização e o mapeamento de atributos para permissões, de modo que a mitigação completa dessa categoria dependa de mecanismos externos à plataforma.



(a) Distribuição do RPS em 30 rodadas. (b) RPS médio ao longo das 30 rodadas.

Figura 4. Requisições por segundo (RPS). (a) A rede é capaz de atender cerca de 18 RPS para emissão de VCs, enquanto o processo de verificação atende aproximadamente quatro vezes mias requisições. (b) O valor médio de RPS ao longo de 30 rodadas é estável em ambos as funções.

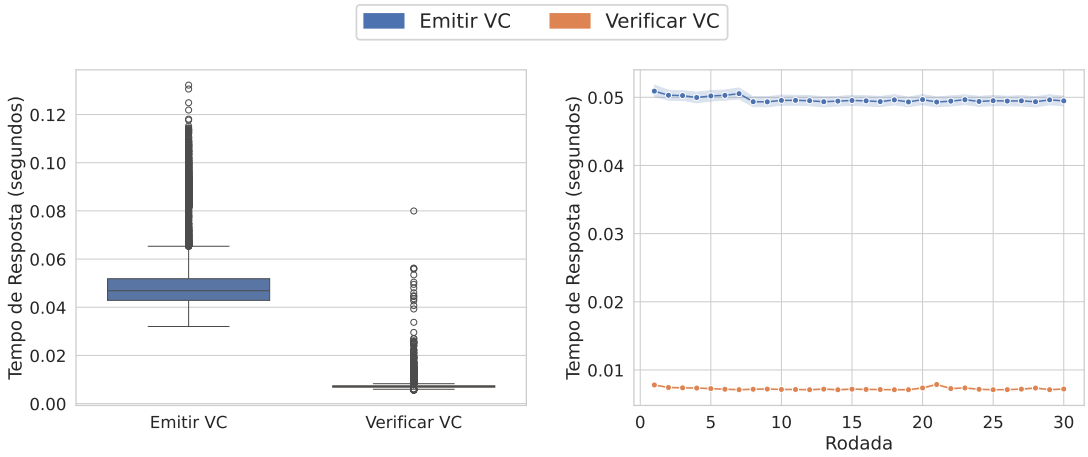
6. Avaliação e Resultados

Para avaliar a viabilidade da plataforma proposta, todos os componentes principais foram executados em *containers* Docker em um computador equipado com 24 GB de RAM, processador Intel Core i7-10510U e sistema operacional Ubuntu 22.04.4. O módulo PIDDF-VCS foi implementado em Python 3 com Flask, expondo uma API REST para emissão e validação de VCs e integrando-se aos demais componentes por meio de APIs REST. O Trustbloc Orb [4] utilizou a rede de testes 1.0.0 configurada com dois nós, o Hyperledger Fabric [5] empregou a rede de testes 2.5 com dois nós *peer*, um nó de ordenação Raft, CAs dedicadas e um único canal no qual um *chaincode* em Go registra *logs* imutáveis em uma Árvore de Merkle, enquanto um módulo em Node.js atuou como *gateway* entre o PIDDF-VCS e o Fabric. Para autenticação foi utilizado o Keycloak 26.1.3, o OpenBao 2.5.1 gerenciou as chaves criptográficas, e todo o código e configurações da plataforma estão disponíveis publicamente no repositório GitHub da PIDDF [6]. Os resultados mostrados nessa seção são valores médios, apresentados com intervalo de confiança de 95%.

O primeiro experimento avaliou o desempenho dos fluxos de emissão e de verificação de VCs em termos de requisições por segundo (RPS), enviando mil requisições sequenciais ao PIDDF-VCS em 30 rodadas, totalizando 30 mil requisições por fluxo. A Figura 4(a) mostra que a emissão atinge em torno de 17–18 RPS, enquanto a verificação alcança aproximadamente 78 RPS, refletindo a maior complexidade e o número de operações criptográficas do fluxo de emissão. A Figura 4(b) indica baixa variação desses valores ao longo das rodadas, o que sugere comportamento estável e previsível da plataforma sob a carga considerada.

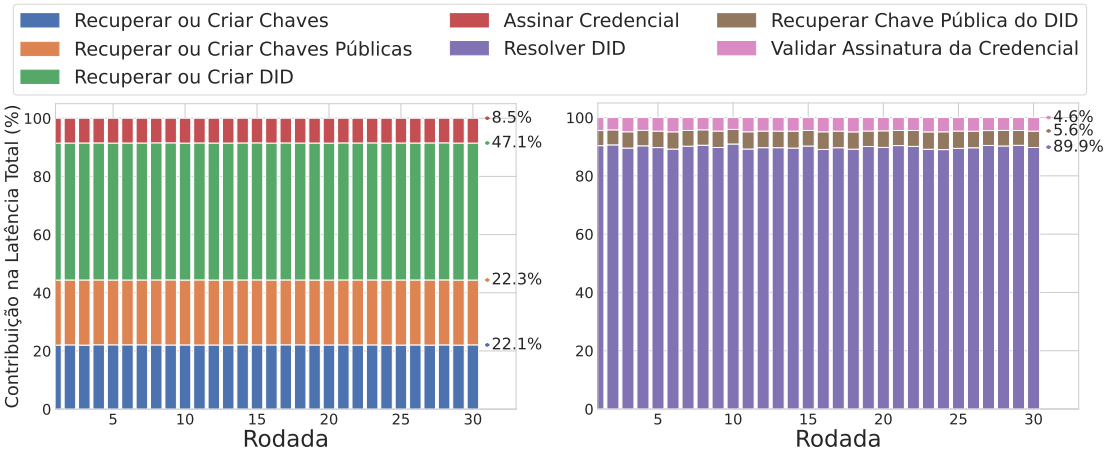
Em seguida, a mesma configuração foi utilizada para avaliar a latência total dos

[4]Disponível em `https://github.com/trustbloc/orb`.
[5]Disponível em `https://hyperledger-fabric.readthedocs.io/en/release-2.5/test_network.html`.
[6]Disponível em `https://github.com/yagorezende/piddf`.



(a) Distribuição do TDR em 30 rodadas. (b) TDR médio ao longo das 30 rodadas.

Figura 5. Tempo de Resposta (TDR). (a) A distribuição do TDR da emissão de VCs é de aproximadamente 0,05 segundos, enquanto a verificação toma apenas 0,01 s. (b) o TDR médio ao longo de 30 rodadas permanece estável e previsível em ambos os fluxos.



(a) Latência medida para emissão da VC. (b) Latência medida para verificação da VC.

Figura 6. Decomposição da latência (*Latency Breakdown*) das etapas de emissão e validação de VCs. (a) A contribuição percentual da latência (CPL) por função na emissão mostra que a etapa Recuperar ou Criar DID representa 47,1% da latência total. (b) Na validação, a etapa Resolver DID é dominante, com 89,9% da latência total. O intervalo de confiança é indicado pelo tamanho do ponto exibido ao lado do valor percentual.

fluxos, medindo o tempo de resposta (TDR) de 30 mil requisições por fluxo. A Figura 5(a) mostra que o TDR de emissão gira em torno de 0,05 s, cerca de cinco vezes maior do que o tempo de verificação, efeito diretamente associado à complexidade adicional da criação da VC e do DID ilustrada na Figura 5. A Figura 5(b) evidencia que a variação do TDR ao longo das rodadas é reduzida, indicando estabilidade e ausência de sinais de degradação de desempenho sob a carga testada.

Por fim, foi realizada uma decomposição da latência (*Latency Breakdown*) para

identificar os principais contribuintes do tempo de execução nos fluxos de emissão e verificação, medindo o tempo gasto em cada função e calculando a contribuição percentual da latência (CPL). Os resultados na Figura 6(a) indicam que, na emissão, cerca de 47,1% da latência está associada à criação ou resolução do DID e aproximadamente 44% a operações envolvendo chaves criptográficas, enquanto na Figura 6(b) a resolução do DID domina o fluxo de verificação com 89,9% da latência total. Em conjunto, essas medições mostram que o desempenho da PIDDF é estável e previsível, que a verificação é significativamente mais leve que a emissão e que a maior parte do custo está vinculada ao gerenciamento de DIDs.

7. Conclusão

Este artigo focou o uso de Identidades Auto-Soberanas para fortalecer o gerenciamento de identidades digitais e propôs a plataforma descentralizada PIDDF, que integra SSI a autenticação federada compatível com OIDC. A análise mostrou que a plataforma, apoiada em Hyperledger Fabric, TrustBloc e OpenBao, oferece segurança, auditabilidade, proteção de privacidade e interoperabilidade com sistemas tradicionais, em consonância com LGPD e GDPR. Nesse contexto, a PIDDF indica que integrar infraestruturas de identidade descentralizada a mecanismos consolidados de autenticação federada é um caminho viável para a adoção prática de identidades auto-soberanas em sistemas digitais. Contudo, a PIDDF ainda apresenta limitações quanto à gestão centralizada de chaves, à restrição atual a credenciais de identidade e à ausência de mecanismos completos de apresentação e revogação de credenciais. Trabalhos futuros incluem integrar carteiras digitais para delegar opcionalmente a gestão de chaves aos usuários, estender o suporte a outros tipos de VCs e incorporar protocolos de apresentação e revogação com técnicas avançadas de preservação de privacidade. Além disso, serão conduzidos testes em ambientes distribuídos em diferentes localidades geográficas, permitindo analisar o comportamento da plataforma sob condições mais próximas às de cenários reais de operação.

Agradecimentos

Este trabalho foi realizado com recursos do CNPq, CAPES, FAPERJ, RNP e INCT ICONIOT. Ferramentas de Inteligência Artificial Generativa, incluindo ChatGPT, Grammarly e Perplexity, foram empregadas na revisão textual deste trabalho.

Referências

Alizadeh, M., Andersson, K., and Schelén, O. (2022). Comparative analysis of decentralized identity approaches. *IEEE Access*, 10:92273–92283.

de Rezende dos Santos, Y., de Oliveira, N. R., Barbosa, G. N. N., Reis, L. H. A., Mendes, A. C. R., de Oliveira, M. T., de Medeiros, D. S. V., and Mattos, D. M. F. (2025). Decentralized security in blockchain-based digital health systems: Self-sovereign identity, access control, and auditing with smart contracts. *Preprint, ResearchSquare*. Posted May 14, 2025; licensed under CC BY 4.0.

Fei, C., Lohkamp, J., Rusu, E., Szawan, K., Wagner, K., and Wittenberg, N. (2018). Jolocom: Self-sovereign and decentralised identity by design. *White paper*.

Grüner, A., Mühle, A., and Meinel, C. (2019). An integration architecture to enable service providers for self-sovereign identity. In *2019 IEEE 18th International Symposium on Network Computing and Applications (NCA)*, pages 1–5. IEEE.

Lux, Z. A., Thatmann, D., Zickau, S., and Beierle, F. (2020). Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 71–78. IEEE.

Maesa, D. D. F., Lisi, A., Mori, P., Ricci, L., and Boschi, G. (2023). Self sovereign and blockchain based access control: Supporting attributes privacy with zero knowledge. *Journal of Network and Computer Applications*, 212:103577.

Maram, D., Malvai, H., Zhang, F., Jean-Louis, N., Frolov, A., Kell, T., Lobban, T., Moy, C., Juels, A., and Miller, A. (2021). Candid: Can-do decentralized identity with legacy compatibility, sybil-resistance, and accountability. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1348–1366. IEEE.

Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., and Conti, M. (2025). A survey on decentralized identifiers and verifiable credentials. *IEEE Communications Surveys & Tutorials*.

Naik, N. and Jenkins, P. (2020a). 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)*, pages 1–7. IEEE.

Naik, N. and Jenkins, P. (2020b). Your identity is yours: Take back control of your identity using gdpr compatible self-sovereign identity. In *2020 7th International Conference on Behavioural and Social Computing (BESC)*, pages 1–6. IEEE.

Olivero, M. A., Bertolino, A., Domínguez-Mayo, F. J., Escalona, M. J., and Matteucci, I. (2020). Digital persona portrayal: Identifying pluridentity vulnerabilities in digital life. *Journal of information security and applications*, 52:102492.

Sim, W. L., Chua, H. N., and Tahir, M. (2019). Blockchain for identity management: The implications to personal data protection. In *2019 IEEE Conference on Application, Information and Network Security (AINS)*, pages 30–35. IEEE.

Xie, T., Gai, K., Yu, J., Zhu, L., and Xiao, B. (2025). Slvc-dida: Signature-less verifiable credential-based issuer-hiding and multi-party authentication for decentralized identity. *arXiv preprint arXiv:2501.11052*.

Yildiz, H., Ritter, C., Nguyen, L. T., Frech, B., Martinez, M. M., and Küpper, A. (2021). Connecting self-sovereign identity with federated and user-centric identities via saml integration. In *2021 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–7. IEEE.

Yin, J., Xiao, Y., Feng, J., Yang, M., Pei, Q., and Yi, X. (2025). Didtrust: Privacy-preserving trust management for decentralized identity. *IEEE Transactions on Dependable and Secure Computing*, 22(3):3105–3120.

Yin, J., Xiao, Y., Pei, Q., Ju, Y., Liu, L., Xiao, M., and Wu, C. (2022). Smartdid: A novel privacy-preserving identity based on blockchain for iot. *IEEE Internet of Things Journal*, 10(8):6718–6732.