Infraestruturas de confiança para credenciais verificáveis sem blockchain

Shirlei Aparecida de Chaves[1], **Emerson Ribeiro de Mello**[1]

[1]Instituto Federal de Santa Catarina – IFSC

{shirlei.chaves, mello}@ifsc.edu.br

Resumo. *Embora as primeiras implementações de identidade digital descentralizada tenham adotado blockchain, o Registro de Dados Verificável (VDR) é tecnologicamente agnóstico. Este artigo discute duas abordagens de VDR que não dependem de blockchain: a ISO/IEC 18013-5, baseada em Infraestrutura de Chaves Públicas e listas confiáveis, e a proposta da OpenID Federation para ecossistemas de credenciais verificáveis.*

1. Introdução

No modelo de identidade digital descentralizada (IDD) há uma reconfiguração do controle sobre os dados pessoais do usuário, bem como sobre sua apresentação e verificação. Em vez de permanecerem nos provedores de identidade, os quais são consultados a cada acesso a um serviço, esses dados são armazenados, no formato de credenciais verificáveis (VCs, *Verifiable Credentials*), em carteiras digitais (*wallets*), sob controle do usuário.

Embora as VCs sejam protegidas por assinaturas digitais, que permitem comprovar a integridade do conteúdo e a autenticidade da entidade que as produziu, no modelo de IDD ainda há a necessidade do estabelecimento da confiança entre as partes. O verificador precisa determinar se o emissor é confiável e se possui autorização institucional para emitir aquele tipo de credencial. A carteira precisa determinar se o emissor e verificador são confiáveis, bem como o inverso. Dessa forma, além dos mecanismos criptográficos, torna-se necessário um modelo de governança capaz de estabelecer essas relações de confiança e expressar políticas de emissão e verificação [OpenID Foundation 2022].

O Registro de Dados Verificável (VDR, *Verifiable Data Registry*) é a infraestrutura subjacente que permite verificação independente, mediando a criação e a verificação de: (i) identificadores descentralizados (DID); (ii) chaves criptográficas; (iii) esquemas de credenciais verificáveis (definições de tipos de credenciais); (iv) lista de credenciais revogadas; e (v) outros dados relevantes para as operações de verificação [W3C 2024]. Apesar das primeiras soluções de IDD se valerem de *blockchains* (*i.e.* Hyperledger Indy), a definição da VDR pela W3C é tecnologicamente agnóstica. Além de *blockchain*, reconhece como possibilidades: (i) bancos de dados confiáveis; (ii) bancos de dados descentralizados; (iii) bancos de dados governamentais de identificação.

O presente trabalho contribui ao reunir e discutir alternativas à blockchain para a implementação de VDRs, ampliando a discussão sobre o uso de infraestruturas de confiança já consolidadas nesse contexto. Na Seção 2 é apresentada a especificação ISO 18013-5 e como a Infraestrutura de Chave Pública (ICP) desempenha o papel de camada de confiança. Na Seção 3 é feita uma discussão sobre uma proposta de uso da especificação *OpenID Federation* para que essa seja empregada como um VDR federado

para uso em um ecossistema de credenciais verificáveis fundamentado em padrões abertos.

2. Modelo de confiança para credenciais ISO 18013-5

A norma ISO/IEC 18013-5 [ISO/IEC 2021] define o modelo de carteiras digitais de habilitação (*mDL, mobile driver license*) e o formato *mdoc* (*mobile document*), que pode ser utilizado na emissão de documentos digitais verificáveis.

Com um modelo de confiança fundamentado em ICP, a Autoridade Certificadora da Autoridade Emissora (IACA, *Issuing Authority Certification Authority*) atua como âncora de confiança. Dessa forma, as VCs emitidas pelas Autoridades Emissoras podem ser verificadas por meio navegação pela cadeia de certificados até chegar a sua raiz.

A distribuição das âncoras de confiança pode ocorrer de forma bilateral, por canais previamente conhecidos (e.g. página web da autoridade emissora), ou por meio de Listas Confiáveis (*Trusted Lists*). Essas listas agregam certificados de diferentes IACAs e os publicam de forma consolidada, favorecendo a interoperabilidade entre jurisdições e a escalabilidade operacional.

Nos Estados Unidos, a Associação Americana de Administradores de Veículos Motorizados (AAMVA) mantém o Serviço de Confiança Digital (DTS, *Digital Trust Service*), que atua como uma autoridade de confiança para o ecossistema, verificando a legitimidade das autoridades emissoras antes de incluí-las em sua Lista Confiável. No contexto europeu, a regulamentação eIDAS adota lógica semelhante: cada Estado-Membro publica sua lista nacional de provedores de confiança, e a União Europeia agrega essas listas na LOTL (*List of Trusted Lists*) [European Commission 2026].

Como a apresentação prevista na ISO/IEC 18013-5 é presencial (*attended*) e pode ocorrer offline, o leitor da mDL mantém localmente os certificados IACA, obtidos previamente por troca bilateral ou por listas de confiança, possibilitando a validação da autenticidade e da integridade da mDL sem acesso à Internet.

A norma também define mecanismos para vincular, de forma criptográfica, a credencial ao dispositivo no momento de sua emissão. Assim, a credencial passa a estar associada ao par de chaves criptográficas do dispositivo, permitindo que o leitor verifique que ela é apresentada pelo dispositivo legítimo e dificultando ataques de clonagem.

Quanto ao armazenamento das credenciais mdoc/mDL, a norma não especifica uma aplicação de carteira específica. Alguns emissores desenvolveram suas próprias carteiras digitais, como a CA DMV Wallet, utilizada pelo estado da Califórnia. Atualmente, as carteiras digitais nativas dos sistemas operacionais Android e iOS passaram a integrar esse ecossistema, permitindo o provisionamento, o armazenamento e a apresentação de mDLs emitidas por autoridades compatíveis [Google 2026, Apple Inc. 2026].

Em síntese, na abordagem da ISO/IEC 18013-5 o papel de VDR é atendido por uma combinação de ICP, âncoras institucionais e listas confiáveis. O resultado é uma camada de confiança sem necessidade de livros-razão distribuídos.

3. OpenID Federation como base para registro de dados verificável

Na especificação *OpenID Federation* [Hedberg et al. 2026], são definidos mecanismos para a construção de federações multilaterais, em que uma entidade pode participar simul-

taneamente de múltiplas federações e uma federação pode se relacionar com outras, sob um modelo de confiança hierárquico e flexível. Em caráter de rascunho, a especificação *OpenID Federation for Wallet Architectures* [de Marco et al. 2026] descreve como essa abordagem pode ser aplicada à gestão de identidade descentralizada, com base em credenciais verificáveis, identificadores descentralizados, carteiras digitais e VDR.

Nesse contexto, as âncoras de confiança atuam como uma camada comum de confiança entre emissores, verificadores e titulares de credenciais. As transações entre essas partes passam a ser sustentadas por uma terceira parte confiável, responsável por emitir asserções de segurança sobre as entidades participantes, indicando, por exemplo, a conformidade com políticas federativas e a aderência a padrões técnicos. Um exemplo desse mecanismo é a emissão de selos digitais (*trust marks*) para atestar que um emissor está autorizado a emitir um determinado tipo de credencial verificável.

Ao receber uma VC, o verificador precisa estabelecer, no mínimo, dois aspectos: i) a integridade e a autenticidade da credencial, por meio da validação da assinatura digital; e ii) a confiança no emissor da credencial. Para atender ao item i), o método `did:web` é adequado ao emissor de VC, pois permite ao verificador recuperar sua chave pública em uma URL conhecida, como *https://emissor/.well-known/did.json*. Para atender ao item ii), o *endpoint https://emissor/.well-known/openid-federation* disponibiliza asserções e metadados do emissor, permitindo mapear, de forma inequívoca, o identificador criptográfico da entidade à sua respectiva árvore de confiança na federação.

Em relação ao titular da credencial, diferentes estratégias de identificação descentralizada podem ser adotadas. Uma alternativa é o uso de `did:jwk`, no qual o identificador é derivado diretamente de uma chave pública no formato JWK. Nesse caso, a carteira digital demonstra controle sobre a chave privada correspondente durante a apresentação da credencial, sem dependência de um serviço externo de resolução. Conforme proposto em [de Marco et al. 2026], emissor e verificador utilizam a camada de confiança para validar se a carteira digital está vinculada a um provedor de carteira integrante da federação. As interações de emissão e verificação de credenciais utilizam os protocolos OID4VCI [Lodderstedt et al. 2025] e OID4VP [Terbu et al. 2025]. Quanto aos formatos de credenciais, podem ser empregados SD-JWT-VC e W3C VC, compatíveis com mecanismos de revelação seletiva e, portanto, adequados à redução da exposição de dados do titular.

Um cenário para demonstrar a viabilidade da OpenID Federation como registro de dados verificável, sem dependência de livros razão distribuídos, é o de diplomas acadêmicos. Pode-se considerar uma federação em que o Ministério da Educação (MEC) atue como âncora de confiança e emita selos digitais para universidades e institutos, atestando sua autorização para emissão de diplomas como credenciais verificáveis.

Como diplomas acadêmicos são credenciais de longa duração, a dependência de infraestrutura baseada em `did:web` introduz desafios relacionados a integridade dos registros DNS e continuidade operacional em longo prazo, como como desativação de domínios ou extinção de instituições de ensino. A obrigatoriedade do DNSSEC, extensão de segurança do DNS, garante a integridade e a autenticidade dos nomes de domínio. Pode-se ainda imaginar o emprego de mecanismos criptográficos como assinaturas múltiplas ou esquemas de assinatura em limiar ao emitir a VC, nos quais a MEC atua como coassinante e garantidora histórica da chave do emissor.

4. Considerações Finais

Neste trabalho foram apresentadas duas abordagens para a implementação de VDRs que não dependem de blockchain: a ISO/IEC 18013-5, baseada em ICP e listas de confiança; e a proposta OpenID Federation, que segue um modelo federado hierárquico.

A análise evidencia que ambas se apoiam em infraestruturas de confiança já consolidadas, embora apresentem diferentes níveis de maturidade e de escopo. Enquanto a ISO/IEC 18013-5 constitui um modelo normativo estabelecido para documentos móveis e cenários offline, a proposta OIDFed oferece maior flexibilidade para ecossistemas federados, mas ainda depende da consolidação de especificações em desenvolvimento.

Mecanismos de revogação e gerenciamento do status de credenciais, tais como as especificações *Bitstring Status List* [Longley et al. 2025] e *Token Status List* [Looker et al. 2026], integram esse ecossistema, mas demandam uma análise mais aprofundada do que o escopo deste trabalho permite. Como trabalhos futuros, pretende-se acompanhar a evolução técnica e normativa dessas especificações, bem como realizar uma avaliação comparativa das diferentes abordagens, considerando aspectos como interoperabilidade, escalabilidade e mecanismos de revogação.

Referências

Apple Inc. (2026). Identity documents in Apple Wallet security. https://support.apple.com/en-mt/guide/security/secb569bf393/web.

de Marco, G., Hedberg, R., Jones, M. B., and Bradley, J. (2026). Openid federation for wallet architectures 1.0 - draft 05.

European Commission (2026). Information related to data on member states' trusted lists as notified under commission implementing decision (eu) 2015/1505 as amended by commission implementing decision (eu) 2025/2164.

Google (2026). Supported issuers and their iaca certs. https://developers.google.com/wallet/identity/verify/supported-issuers-iaca-certs.

Hedberg, R., Jones, M. B., de Marco, G., Solberg, A. A., Bradley, J., and Dzhuvinov, V. (2026). Openid federation 1.1. https://openid.net/specs/openid-federation-1_1.html.

ISO/IEC (2021). Personal identification – iso-compliant driving licence – part 5: Mobile driving licence (mdl) application. Standard, International Organization for Standardization / International Electrotechnical Commission, Geneva, CH.

Lodderstedt, T., Yasuda, K., Looker, T., and Bastian, P. (2025). Openid for verifiable credential issuance 1.0.

Longley, D., Sporny, M., and Steele, O. (2025). Bitstring status list v1.0. https://www.w3.org/TR/vc-bitstring-status-list/.

Looker, T., Bastian, P., and Bormann, C. (2026). Token status list. https://datatracker.ietf.org/doc/draft-ietf-oauth-status-list/.

OpenID Foundation (2022). Openid for verifiable credentials. Whitepaper.

Terbu, O., Lodderstedt, T., Yasuda, K., Fett, D., and Heenan, J. (2025). Openid for verifiable presentations 1.0.

W3C (2024). Verifiable credentials data model v2.0. W3C Recommendation.