BraZKIL: um Framework híbrido para verificação de maioridade via SSI, DID/VC e Divulgação Seletiva em conformidade com o ECA Digital

Otávio Alves Gomes[1], **Carlos Frederico Marcelo da Cunha Cavalcanti**[1]

[1]Departamento de Ciência da Computação (DECOM)
Universidade Federal de Ouro Preto (UFOP) - Ouro Preto, MG - Brasil

otavio.gomes@aluno.ufop.edu.br, cfmcc@ufop.edu.br

Resumo. *A entrada em vigor do ECA Digital exige mecanismos confiáveis de verificação de idade, enquanto a LGPD restringe a coleta excessiva de dados pessoais. Este trabalho propõe o BraZKIL, uma arquitetura híbrida de verificação de maioridade baseada em identidade autossoberana, identificadores descentralizados, credenciais verificáveis e divulgação seletiva. A arquitetura separa a validação inicial, apoiada em uma fonte autoritativa, das comprovações posteriores realizadas por uma credencial reutilizável sob controle do titular. Foi implementada uma prova de conceito com SD-JWT VC, serviços locais, uma carteira digital de código aberto e integração ao ambiente de demonstração do Datavalid. Os resultados indicam a viabilidade funcional do fluxo e permitem que o verificador receba apenas a afirmação de maioridade, sem acesso a CPF, biometria, data de nascimento ou aos demais dados utilizados na validação inicial.*

Abstract. *The ECA Digital requires reliable age-verification mechanisms, while the LGPD limits excessive collection and processing of personal data. This paper presents BraZKIL, a hybrid age-verification architecture based on self-sovereign identity, decentralized identifiers, verifiable credentials, and selective disclosure. The architecture separates the initial validation, supported by an authoritative source, from subsequent proofs performed with a reusable credential controlled by the holder. A proof of concept was implemented using SD-JWT VC, local services, an open-source digital wallet, and integration with the Datavalid demonstration environment. The results provide preliminary evidence of the functional feasibility of the flow and allow the verifier to receive only the adulthood claim, without accessing the CPF, biometric data, date of birth, or other data used during the initial validation.*

1. Introdução

A Lei n.º 15.211/2025, conhecida como ECA Digital [Brasil 2026], tornou a verificação confiável de idade um requisito relevante para plataformas digitais no Brasil. Ao vedar mecanismos exclusivamente declaratórios em situações de acesso a conteúdos, produtos ou serviços destinados ao público adulto, a norma exige soluções eficazes de aferição etária. Simultaneamente, esses mecanismos devem observar os princípios da Lei Geral de Proteção de Dados (LGPD) [Brasil 2018], especialmente finalidade, necessidade, segurança e minimização do tratamento de dados.

Essa combinação normativa cria uma tensão técnica. A autodeclaração apresenta baixa exposição de dados, mas é facilmente contornável. Em contrapartida, métodos baseados no envio recorrente de documentos, biometria facial ou consultas cadastrais podem aumentar a confiabilidade, mas também ampliam a circulação de dados pessoais, criam repositórios fragmentados e elevam a superfície de ataque. Mecanismos mal projetados ainda podem favorecer rastreamento, vigilância e erosão do anonimato online [Moreira et al. 2023]. O desafio, portanto, consiste em comprovar a maioridade sem expor desnecessariamente CPF, documento, data de nascimento, biometria ou outros atributos identificadores.

Tecnologias associadas à identidade autossoberana (*Self-Sovereign Identity*, SSI) [Kuhn et al. 2018], como identificadores descentralizados (*Decentralized Identifiers*, DIDs) [Sporny et al. 2022], credenciais verificáveis (*Verifiable Credentials*, VCs) [Sporny et al. 2025] e mecanismos de divulgação seletiva, oferecem uma alternativa para esse problema. Elas permitem que uma entidade confiável ateste atributos armazenados sob controle do titular e posteriormente apresentados a diferentes verificadores, sem a revelação de todos os dados utilizados durante a emissão.

Soluções internacionais fornecem padrões e componentes reutilizáveis, mas sua aplicação no Brasil exige adaptações institucionais e regulatórias. Iniciativas como a *European Digital Identity Wallet* foram concebidas sob o arcabouço do eIDAS 2.0, com modelos próprios de governança e credenciamento. No Brasil, a validação de identidade permanece fortemente apoiada em bases governamentais e serviços acessíveis por API, como o Datavalid e o ecossistema gov.br. Assim, o problema não consiste em substituir as soluções internacionais, mas em integrar seus padrões a fontes oficiais e a um modelo de confiança compatível com o ECA Digital e a LGPD.

Este trabalho propõe o BraZKIL (*Brazilian Zero-Knowledge Identity Layer*), uma arquitetura híbrida que separa a validação inicial da comprovação recorrente da maioridade. Na primeira etapa, uma fonte autoritativa fornece evidências cadastrais e biométricas, a partir das quais um emissor aplica sua política de aceitação e produz uma credencial de maioridade. Nas interações posteriores, a carteira do titular apresenta seletivamente apenas a afirmação etária necessária, utilizando formatos e protocolos interoperáveis, como SD-JWT VC, OID4VCI e OID4VP [Lodderstedt et al. 2024, Terbu et al. 2023].

Uma prova de conceito com dados sintéticos reproduz, em ambiente controlado, os módulos de validação, emissão, armazenamento, apresentação seletiva, verificação e revogação. A implementação permite avaliar preliminarmente o funcionamento do fluxo e os dados expostos aos diferentes participantes. Os detalhes da integração com o serviço de validação e da avaliação experimental são apresentados na Seção 5.

1.1. Contribuições

A contribuição do trabalho não está na criação de uma nova primitiva criptográfica, mas na integração de padrões existentes em uma arquitetura de confiança voltada ao contexto brasileiro. Especificamente, o artigo apresenta:

- uma arquitetura híbrida que separa a validação inicial por fonte autoritativa da comprovação recorrente da maioridade por credenciais verificáveis;
- um modelo de confiança que articula fonte de validação, emissor, titular, verificador e registro de confiança e status;

- um fluxo baseado em DIDs, VCs, SD-JWT VC, OID4VCI e OID4VP, no qual o serviço final recebe a afirmação etária sem obter os dados pessoais utilizados na emissão;
- uma análise comparativa com trabalhos acadêmicos e soluções institucionais, acompanhada de uma PoC que avalia preliminarmente o fluxo funcional e a minimização da exposição de dados.

2. Fundamentação teórica e tecnológica

2.1. SSI, DIDs e credenciais verificáveis

A identidade autossoberana (*Self-Sovereign Identity*, SSI) amplia o controle do titular sobre suas credenciais digitais e reduz a necessidade de consultar uma autoridade central em cada interação [Kuhn et al. 2018]. Identificadores descentralizados (*Decentralized Identifiers*, DIDs) são identificadores resolvíveis cujos documentos podem conter chaves públicas, métodos de verificação e pontos de serviço [Sporny et al. 2022]. Um DID, entretanto, não estabelece confiança por si só, que depende de mecanismos de credenciamento e governança.

Credenciais verificáveis (*Verifiable Credentials*, VCs) permitem que um emissor ateste afirmações sobre um titular no modelo *issuer–holder–verifier* [Sporny et al. 2025]. A assinatura comprova a integridade e a origem da credencial, enquanto sua aceitação também depende da confiança no emissor, da validade temporal e do estado de suspensão ou revogação. No BraZKIL, a VC representa a condição de maioridade sem transportar ao serviço final os dados pessoais utilizados durante a validação.

2.2. Divulgação seletiva e provas de conhecimento zero

A divulgação seletiva permite apresentar apenas os atributos necessários a uma interação. Provas de conhecimento zero (*Zero-Knowledge Proofs*, ZKPs) podem demonstrar um predicado sobre um valor oculto, como verificar que uma data de nascimento satisfaz determinado limiar etário sem revelá-la.

O SD-JWT, por sua vez, protege atributos por meio de *disclosures*, valores aleatórios e resumos criptográficos. O titular revela somente os *disclosures* necessários, cuja integridade é conferida em relação ao token assinado [Yasuda et al. 2024].

A PoC utiliza SD-JWT VC e uma afirmação previamente calculada, representada por `age_over_18`. Portanto, não executa uma prova de predicado em sentido criptográfico estrito. A preservação de privacidade decorre da não divulgação dos demais atributos, sem eliminar riscos de correlação associados a identificadores persistentes ou metadados.

2.3. OID4VCI e OID4VP

O *OpenID for Verifiable Credential Issuance* (OID4VCI) define fluxos de emissão de credenciais para carteiras, enquanto o *OpenID for Verifiable Presentations* (OID4VP) padroniza solicitações e apresentações dirigidas a verificadores [Lodderstedt et al. 2024, Terbu et al. 2023].

Esses protocolos não determinam quais emissores são confiáveis nem quais políticas regulatórias devem ser aplicadas; essas decisões pertencem ao modelo de confiança do BraZKIL. Quando suportado pelo formato adotado, o vínculo ao titular pode exigir a

Figura 1. Relação entre os fundamentos tecnológicos utilizados no BraZKIL.

demonstração de posse da chave associada à credencial, combinando desafio, audiência e validade temporal.

A Figura 1 sintetiza a relação entre os componentes tecnológicos adotados no BraZKIL.

3. Estado da arte e trabalhos relacionados

A pesquisa sobre verificação de identidade e de atributos com preservação de privacidade tem evoluído de protocolos criptográficos isolados para arquiteturas que combinam identidade autossoberana, credenciais verificáveis, registros de confiança e mecanismos de divulgação seletiva. Essas propostas diferem quanto ao modelo de confiança, às propriedades criptográficas oferecidas e às dependências institucionais necessárias para sua implantação.

Hoang et al. [Hoang et al. 2024] propõem o *zkSSI*, um *framework* que combina SSI, VCs e *zk-SNARKs*. A solução permite que verificadores expressem condições sobre atributos mantidos em sigilo, possibilitando a avaliação criptográfica de predicados sem a revelação dos valores subjacentes. O trabalho demonstra a viabilidade de integrar provas de conhecimento zero a ecossistemas de identidade autossoberana, embora permaneça orientado a um cenário genérico de identidade descentralizada.

Maurya et al. [Maurya et al. 2025] apresentam uma arquitetura descentralizada de verificação de identidade que combina credenciais verificáveis, provas de conhecimento zero e um *issuer trust registry* mantido por contratos inteligentes. O registro permite que verificadores identifiquem emissores reconhecidos e avaliem credenciais utilizadas em diferentes domínios. A proposta reforça a importância de articular mecanismos criptográficos com uma camada explícita de governança e confiança.

No contexto específico da verificação de idade, Scheffler e Liu [Scheffler and Liu 2025] analisam diferentes arquiteturas de aferição etária sob a perspectiva da privacidade. Os autores destacam que abordagens baseadas no envio direto de documentos ou biometria aos serviços finais ampliam a exposição de dados, enquanto modelos apoiados em entidades confiáveis e evidências criptográficas permitem separar a verificação inicial da comprovação posterior do atributo.

Esses trabalhos demonstram a maturidade de tecnologias capazes de comprovar atributos com exposição reduzida de dados. Entretanto, não tratam diretamente da articulação entre essas tecnologias, as fontes oficiais brasileiras de validação e os requisitos estabelecidos pelo ECA Digital e pela LGPD. O BraZKIL não propõe uma nova primitiva criptográfica. Sua contribuição está na definição de uma arquitetura de integração e confiança que separa a validação inicial da comprovação recorrente da maioridade e adapta padrões existentes ao contexto institucional brasileiro.

No âmbito aplicado, diferentes soluções e iniciativas de identidade digital ofere-

cem componentes que podem ser reutilizados ou adaptados ao problema da verificação etária.

Self Protocol. O Self Protocol [Self Labs 2024] é uma solução de identidade digital com preservação de privacidade que utiliza documentos eletrônicos compatíveis com NFC, como passaportes, para produzir evidências criptográficas sobre atributos do titular. Essa abordagem reduz a necessidade de o serviço final receber diretamente os dados documentais. Entretanto, o fluxo documentado depende da disponibilidade de documento compatível e de componentes específicos do ecossistema Self. No contexto brasileiro, essa dependência pode restringir a cobertura do mecanismo. O BraZKIL considera, alternativamente, uma validação inicial remota por fonte autoritativa acessível por API, sem exigir leitura NFC no fluxo proposto.

Privado ID. O Privado ID [Privado ID 2024], anteriormente denominado Polygon ID, fornece uma infraestrutura de identidade baseada no protocolo *iden3* e em circuitos *zk-SNARK*. A solução permite a emissão e a apresentação de credenciais com provas sobre atributos, incluindo condições etárias, e oferece mecanismos de verificação *on-chain* e *off-chain*. Sua adoção no cenário brasileiro, contudo, exige a definição de emissores reconhecidos, políticas de governança e integração com fontes oficiais de validação. O BraZKIL trata explicitamente dessa integração e não vincula sua arquitetura, em princípio, a uma infraestrutura blockchain específica.

EUDI Wallet. A *European Digital Identity Wallet* (EUDI Wallet) constitui uma referência institucional para carteiras digitais, apresentação seletiva e interoperabilidade [European Commission 2025]. Sua arquitetura foi desenvolvida sob o regulamento eIDAS 2.0 e depende de modelos europeus de governança, credenciamento de emissores e infraestrutura de confiança. Seus padrões e princípios são reutilizáveis, mas sua adoção no Brasil requer adaptações regulatórias e institucionais. O BraZKIL busca aproveitar esses padrões interoperáveis, articulando-os com as fontes de validação e as normas brasileiras.

A Tabela 1 sintetiza as principais características das abordagens analisadas e o posicionamento arquitetural do BraZKIL. A comparação não pretende afirmar a inviabilidade das soluções existentes, mas identificar as adaptações necessárias para sua aplicação ao contexto considerado neste trabalho.

Em conjunto, os trabalhos acadêmicos e as soluções aplicadas demonstram que credenciais verificáveis, registros de confiança, divulgação seletiva e provas criptográficas constituem mecanismos viáveis para reduzir a exposição de dados em processos de verificação de atributos. O diferencial do BraZKIL não está na criação desses mecanismos, mas em sua organização em uma arquitetura voltada ao contexto brasileiro, na qual uma fonte autoritativa apoia a validação inicial e os serviços posteriores recebem apenas a evidência necessária à decisão de acesso.

A PoC apresentada neste trabalho utiliza SD-JWT VC para divulgar seletivamente uma afirmação de maioridade previamente calculada. Portanto, ela não oferece as mesmas

Tabela 1. Comparação entre trabalhos e soluções relacionados ao BraZKIL.

Abordagem	Principal contribuição	Aspecto não contemplado diretamente	Adaptação no BraZKIL
zkSSI	Integra SSI, VCs e provas de conhecimento zero para avaliação de condições sobre atributos ocultos.	Arquitetura genérica, sem integração com fontes oficiais ou requisitos regulatórios brasileiros.	Adota SSI e VCs em um fluxo voltado à verificação etária brasileira; a PoC utiliza SD-JWT VC, e não *zk-SNARKs*.
Maurya et al.	Combina VCs, ZK e um registro de confiança de emissores mantido por contratos inteligentes.	Não trata especificamente da verificação de idade nem da governança institucional brasileira.	Incorpora uma camada de confiança e status, ancorada em emissores e fontes autoritativas reconhecidas.
Self Protocol	Produz evidências de atributos a partir de documentos eletrônicos compatíveis com NFC.	Depende, no fluxo considerado, de documentos compatíveis e de componentes específicos do ecossistema.	Propõe validação inicial remota por fonte autoritativa e integração com carteiras compatíveis com os padrões adotados.
Privado ID	Oferece infraestrutura ZK-SSI para emissão e comprovação criptográfica de atributos.	Exige definição de governança, emissores reconhecidos e integração com fontes oficiais brasileiras.	Propõe um fluxo institucional integrado à validação estatal, sem vinculação arquitetural obrigatória a uma blockchain específica.
EUDI Wallet	Referência institucional em governança, interoperabilidade e apresentação seletiva.	Seu modelo de confiança e credenciamento está associado ao arcabouço europeu eIDAS 2.0.	Reutiliza princípios e protocolos interoperáveis, adaptando o modelo de confiança ao ECA Digital, à LGPD e à infraestrutura brasileira.

propriedades de uma prova de predicado baseada em conhecimento zero, como as utilizadas pelo zkSSI ou pelo Privado ID. Essa escolha reduz a complexidade da implementação preliminar, mas também delimita suas propriedades criptográficas.

4. Arquitetura do modelo BraZKIL

O BraZKIL (*Brazilian Zero-Knowledge Identity Layer*) é uma arquitetura híbrida para verificação de maioridade. A validação inicial da identidade e da condição etária é apoiada por uma fonte autoritativa, enquanto as comprovações posteriores são realizadas por meio de credenciais verificáveis e divulgação seletiva. O objetivo é separar a validação forte da utilização recorrente do atributo, reduzindo a necessidade de reenviar documentos, CPF, biometria ou dados cadastrais a cada serviço acessado.

A arquitetura organiza-se em duas camadas principais. Na camada de validação e emissão, uma fonte autoritativa fornece evidências cadastrais e biométricas, e o Middleware BraZKIL aplica uma política de aceitação e atua como emissor. Na camada de posse e apresentação, a carteira do titular armazena a credencial e produz apresentações em resposta às solicitações dos verificadores.

Um registro de confiança e status complementa essas camadas, publicando identificadores, chaves públicas, emissores autorizados e informações sobre suspensão ou revogação. O registro não verifica a apresentação em nome do serviço final; ele fornece

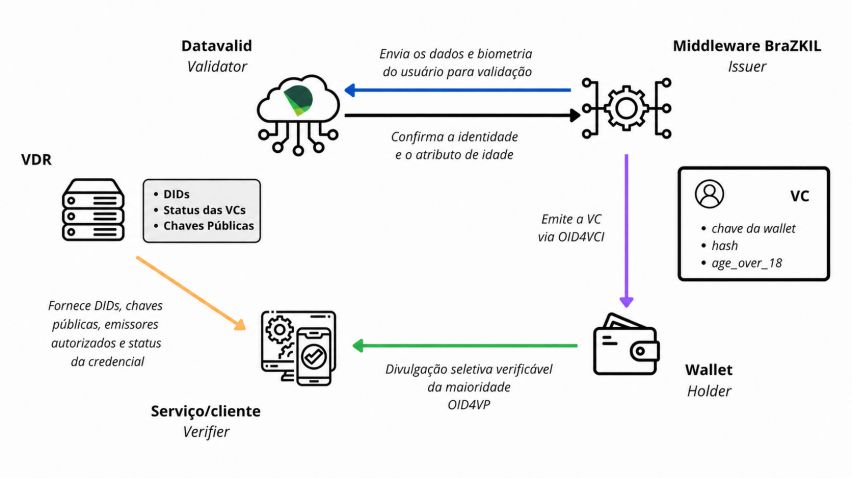

Figura 2. Modelo de confiança e fluxo principal do BraZKIL para verificação de maioridade no contexto do ECA Digital.

elementos para que o próprio verificador avalie a origem, a integridade, a validade e o estado da credencial.

Embora o Datavalid seja utilizado como referência de fonte autoritativa no cenário brasileiro considerado, a arquitetura não depende exclusivamente desse serviço. Outras fontes oficiais ou entidades autorizadas podem desempenhar função equivalente, desde que produzam evidências adequadas à política de emissão.

4.1. Atores e artefatos principais

O BraZKIL estende o modelo *issuer–holder–verifier* das credenciais verificáveis [Sporny et al. 2025] com uma fonte externa de validação e uma camada explícita de confiança e status. Seus componentes principais são:

- **fonte autoritativa**: fornece evidências cadastrais e, quando aplicável, biométricas para a decisão de emissão;
- **Middleware BraZKIL**: atua como emissor (*Issuer*), aplica a política de aceitação e produz a credencial de maioridade;
- **titular**: atua como *Holder*, controla a carteira e o material criptográfico associado à credencial;
- **serviço digital**: atua como *Verifier*, solicita e verifica a apresentação da condição de maioridade;
- **registro de confiança e status**: publica DIDs, chaves públicas, emissores autorizados e informações de suspensão ou revogação.

Os principais artefatos do fluxo são as evidências produzidas na validação, o DID e o *DID Document* do emissor, a credencial verificável de maioridade, os metadados de validade e status, a *Credential Offer* do OID4VCI e a *Presentation Request* do OID4VP [Sporny et al. 2022, Sporny et al. 2025, Lodderstedt et al. 2024, Terbu et al. 2023].

4.2. Validação inicial e emissão da credencial

Na etapa inicial, o titular solicita ao Middleware BraZKIL a emissão de uma credencial de maioridade. O Middleware coleta os dados necessários e consulta uma

fonte autoritativa. Na instanciação brasileira considerada, o Datavalid é adotado como referência por oferecer modalidades de validação cadastral e biométrica por API [Serviço Federal de Processamento de Dados (SERPRO) 2024].

A comunicação entre o Middleware e a fonte de validação deve ocorrer por canal autenticado e protegido. A resposta pode conter confirmações cadastrais, índices de similaridade ou resultados biométricos, conforme a modalidade de consulta utilizada. Essas evidências não constituem, isoladamente, uma decisão de emissão.

Cabe ao Middleware aplicar uma política de aceitação previamente definida. Essa política pode considerar a coerência dos dados cadastrais, o resultado da validação biométrica, os limiares configurados e a idade calculada a partir da data de nascimento validada. A credencial somente é emitida quando os critérios estabelecidos forem atendidos.

A credencial contém a afirmação etária necessária, representada na PoC pelo atributo `age_over_18`, além de metadados como emissor, período de validade, mecanismo de consulta de status e, quando adotado, material de vinculação ao titular. Documento bruto, CPF, imagem facial, data de nascimento e resposta completa da fonte de validação não integram a apresentação enviada ao serviço final.

Para fins de auditoria, os registros do emissor podem indicar que a emissão foi fundamentada em uma fonte autoritativa, sem incorporar os dados pessoais utilizados na validação. A confiança institucional no emissor pode ser reforçada por políticas de credenciamento, registros de emissores autorizados ou certificados institucionais, inclusive mecanismos associados à ICP-Brasil.

4.3. Emissão para a carteira e vinculação ao titular

Após a decisão de emissão, o Middleware disponibiliza a credencial à carteira por meio de um fluxo compatível com OID4VCI [Lodderstedt et al. 2024]. A oferta pode ser entregue por QR Code, *deep link* ou URI, permitindo que a carteira identifique o emissor, obtenha seus metadados e solicite a credencial.

O BraZKIL é projetado para reduzir o acoplamento a uma carteira específica. A interoperabilidade, contudo, depende da compatibilidade concreta quanto ao perfil do OID4VCI, ao formato SD-JWT VC, aos algoritmos criptográficos e aos mecanismos de vinculação adotados. Portanto, não se presume que qualquer carteira existente possa participar do fluxo sem configuração ou adaptação.

A carteira armazena a credencial, protege suas chaves privadas, acompanha validade e status e produz apresentações em resposta aos verificadores. Para reduzir o risco de transferência ou reutilização indevida, a arquitetura prevê a vinculação da credencial a uma chave controlada pela carteira.

Em uma implementação baseada em SD-JWT VC, essa vinculação pode ser representada pelo parâmetro de confirmação `cnf`, associado à chave pública do titular. Durante a apresentação, a carteira pode demonstrar a posse da chave privada correspondente por meio de um token de vinculação contendo um desafio não reutilizável (*nonce*), a audiência do verificador e informações temporais.

O verificador deve conferir a assinatura do token, sua correspondência com a chave indicada na credencial, o desafio, a audiência e a validade temporal. Esses me-

canismos constituem requisitos da arquitetura; a Seção 5 delimita quais deles foram efetivamente implementados e avaliados na PoC.

A prova de posse da chave não garante, isoladamente, a presença física ou a identidade civil contínua do titular. A proteção também depende da segurança do dispositivo, do armazenamento das chaves e dos mecanismos locais de autenticação da carteira.

4.4. Apresentação seletiva e verificação

Quando um serviço exige comprovação de maioridade, ele envia à carteira uma solicitação de apresentação compatível com OID4VP [Terbu et al. 2023]. A solicitação identifica o atributo necessário, a audiência e, quando o perfil adotado utilizar vinculação ao titular, um desafio de frescor.

A carteira seleciona uma credencial compatível e produz uma apresentação seletiva. Na instanciação baseada em SD-JWT VC, revela-se o *disclosure* correspondente ao atributo `age_over_18`, mantendo os demais atributos protegidos.

Ao receber a apresentação, o verificador valida a assinatura e a integridade da credencial, obtém a chave pública e os metadados do emissor e aplica sua política de confiança. Também verifica a validade temporal e o estado de suspensão ou revogação da credencial. Quando houver vinculação ao titular, confere ainda o desafio, a audiência e a prova de posse da chave associada. Por fim, verifica se a apresentação contém somente os atributos necessários à decisão de acesso.

O registro de confiança e status fornece parte das informações utilizadas nesse processo, como chaves públicas, emissores autorizados e estado das credenciais. A decisão de aceitar ou rejeitar a apresentação, contudo, permanece sob responsabilidade do serviço verificador.

4.5. Fluxo integrado e minimização de dados

O fluxo integrado do BraZKIL inicia-se quando o titular solicita ao Middleware a emissão de uma credencial de maioridade. O Middleware coleta os dados necessários e consulta a fonte autoritativa por canal autenticado e protegido. As evidências retornadas são avaliadas segundo a política de emissão e, quando os critérios definidos são atendidos, o Middleware produz a credencial verificável.

A credencial é então disponibilizada à carteira por meio de um fluxo compatível com OID4VCI. A carteira armazena a credencial, protege o material criptográfico associado e, quando solicitado por um serviço, produz uma apresentação seletiva por meio do OID4VP. Na implementação baseada em SD-JWT VC, essa apresentação revela apenas o atributo `age_over_18`, mantendo os demais atributos protegidos.

Ao receber a apresentação, o verificador avalia a assinatura, a identidade e a autorização do emissor, a validade temporal e o estado da credencial. Quando o perfil adotado incluir vinculação ao titular, também são verificados o desafio, a audiência e a prova de posse da chave associada antes da decisão de acesso.

Essa separação limita os dados cadastrais e biométricos à etapa de validação e emissão. Sua retenção deve observar a finalidade e o período estritamente necessários, conforme a política do emissor e os requisitos legais aplicáveis. Nas interações posteri-

ores, o serviço final recebe a afirmação etária e os metadados necessários à verificação, sem acesso direto a CPF, documento, imagem facial ou data de nascimento.

A arquitetura reduz, portanto, a circulação de dados identificadores entre diferentes serviços. Essa propriedade, entretanto, não elimina riscos relacionados a metadados de rede, correlação entre apresentações, comprometimento da carteira ou políticas excessivas de solicitação de atributos.

4.6. Status, expiração e revogação

A credencial de maioridade não deve ser tratada como permanente. Sua validade pode ser limitada por expiração, rotação de chaves, suspeita de fraude, comprometimento da carteira ou perda de confiança no emissor. Por isso, pode incluir metadados como `validFrom`, `validUntil` e `credentialStatus` [Sporny et al. 2025].

O BraZKIL diferencia suspensão e revogação. A suspensão representa uma interrupção temporária, enquanto a revogação indica o cancelamento definitivo. Em ambos os casos, o estado deve ser consultável pelo verificador antes da aceitação da apresentação.

A arquitetura pode empregar listas agregadas de status publicadas em um registro verificável. Esse modelo evita consultas diretas ao emissor a cada apresentação e pode reduzir a correlação entre usos da credencial. O período de atualização das listas e o comportamento diante de indisponibilidade devem ser definidos pela política de risco do verificador.

5. Prova de conceito e avaliação preliminar

Para avaliar preliminarmente a viabilidade funcional do BraZKIL, foi desenvolvida uma prova de conceito com execução em ambiente controlado. A implementação reproduz os principais componentes da arquitetura: módulo de validação, emissor de credenciais, carteira do titular, verificador e registro de status. Seu objetivo é demonstrar o fluxo de validação, emissão, armazenamento, apresentação seletiva, verificação e revogação de uma credencial de maioridade.

A PoC foi implementada em Python 3.12, utilizando as bibliotecas cryptography 44.0.0, python-jose 3.3.0, httpx 0.28.1, FastAPI 0.115.6 e SQLAlchemy 2.0.36. As latências foram medidas com `time.perf_counter()`, em execuções sequenciais e sem etapa de aquecimento. O intervalo cronometrado compreendeu exclusivamente a operação avaliada, excluindo a inicialização dos componentes e a preparação prévia dos dados.

Os componentes de emissão, carteira e verificação foram implementados como serviços locais, com integração a uma carteira de código aberto da walt.id, versão `v0.22` [walt.id 2026]. A credencial utiliza o formato SD-JWT VC, no qual os atributos protegidos são representados por *disclosures*, valores aleatórios e resumos criptográficos. Durante a apresentação, a carteira revela apenas a afirmação `age_over_18`, mantendo CPF, nome, data de nascimento e demais atributos fora da informação enviada ao serviço final.

A vinculação ao titular foi implementada pelo campo `cnf` da credencial e por um *Key Binding JWT* assinado pela carteira. O token inclui o desafio, a audiência e a informação temporal, permitindo ao verificador confirmar a posse da chave associada à credencial e reduzir o risco de repetição da apresentação.

Os resumos criptográficos são calculados com SHA-256, enquanto a credencial é assinada com ES256, baseado em ECDSA sobre a curva P-256. Esses algoritmos foram adotados por sua disponibilidade nas bibliotecas e nos formatos utilizados pela PoC. Eles não oferecem resistência pós-quântica, propriedade que permanece fora do escopo desta avaliação.

A implementação foi organizada em módulos correspondentes às funções de validação, emissão, armazenamento, apresentação, verificação e consulta de status. Os dados utilizados no fluxo de credencial e de status são sintéticos e empregados apenas para testes e benchmarking inicial. Já a etapa de validação realiza chamadas reais ao ambiente de demonstração do Datavalid, que disponibiliza interface REST API para testes. Como esse ambiente aceita apenas um conjunto reduzido de perfis de exemplo, limitando-se a cinco perfis distintos, os dados de entrada precisaram ser definidos de acordo com essas restrições. Assim, a PoC não representa uma integração produtiva com bases governamentais nem contempla todos os controles operacionais necessários a um serviço em produção.

Tabela 2. Resultados da PoC BraZKIL.

Operação avaliada	**Evidência observada**	**Resultado**
Validação integrada	O módulo de validação processa dados cadastrais, condição etária e escore biométrico retornado para os perfis de demonstração.	Executado
Emissão da credencial	Issuer gera credencial SD-JWT com atributos pessoais protegidos por *salt* e hash.	Executado
Armazenamento na carteira	Wallet armazena credencial e disclosures localmente.	Executado
Apresentação seletiva	Wallet revela apenas `age_over_18`, mantendo CPF, nome e data de nascimento ocultos.	Executado
Verificação da apresentação	Verifier valida assinatura, desafio de frescor, holder binding e status da credencial.	Executado
Revogação	Credencial marcada como revogada no VDR simulado é rejeitada em apresentação posterior.	Executado
Minimização de dados	Verifier recebe somente o atributo necessário à decisão de acesso.	Confirmada

A Tabela 2 resume os fluxos funcionais avaliados. Os resultados indicam que a PoC reproduz as etapas centrais da arquitetura, incluindo emissão da credencial, armazenamento na carteira, apresentação seletiva, verificação e tratamento de revogação. Em particular, o fluxo de apresentação permite que o verificador receba a afirmação etária necessária à decisão de acesso sem obter os dados pessoais utilizados durante a validação inicial.

Além da avaliação funcional, foram realizadas medições preliminares das principais operações do fluxo. Essas medições possuem caráter exploratório e foram conduzidas no ambiente de desenvolvimento local. Seu objetivo é registrar a ordem de grandeza observada na implementação, não estimar o desempenho de uma implantação pública ou de produção. As medições foram executadas em um computador portátil com processador Intel Core i5-12450HX, 8 GB de RAM, armazenamento SSD e sistema operacional Linux.

Na operação de validação, o intervalo medido corresponde ao *round-trip* HTTP

completo entre o módulo local e a API do ambiente de demonstração do Datavalid, incluindo o envio da requisição e o recebimento da resposta. As 50 medições reutilizaram os cinco perfis disponibilizados pelo ambiente de demonstração.

Tabela 3. Latências da PoC BraZKIL.

Operação	Média (ms)	Desvio (ms)	N
Validação do Datavalid via API	8.29	4.46	50
Emissão da credencial SD-JWT	4.86	0.96	1000
Geração da apresentação seletiva	3.50	0.88	1000
Verificação da apresentação	4.52	1.01	1000
Consulta de status/revogação	1.69	0.10	1000

A Tabela 3 apresenta os tempos observados nas operações avaliadas. Os valores incluem custos próprios da implementação utilizada e podem ser influenciados por serialização, bibliotecas, sistema operacional, instrumentação e comunicação entre componentes. Por esse motivo, devem ser interpretados apenas como indicação preliminar do comportamento da PoC no ambiente avaliado. Eles não permitem inferir desempenho em redes públicas, dispositivos móveis, carteiras de terceiros ou cenários com carga concorrente.

A PoC apresenta limitações relevantes. A execução utiliza dados sintéticos e componentes em ambiente controlado, sem representar requisitos completos de disponibilidade, escalabilidade, proteção de chaves, segurança da captura biométrica ou governança de emissores. A avaliação também não demonstra interoperabilidade universal com carteiras digitais nem resistência a todos os ataques considerados no modelo de ameaças. Esses aspectos exigem experimentos adicionais em ambientes próximos de produção.

6. Análise de segurança

A segurança do BraZKIL deve ser analisada em duas fases. Na primeira, dados cadastrais e biométricos são processados para validar a identidade e a condição etária do titular antes da emissão da credencial. Na segunda, a credencial é utilizada para apresentar seletivamente a afirmação de maioridade a diferentes serviços. Esta seção delimita o modelo de ameaças, relaciona as mitigações previstas pela arquitetura e reconhece os riscos que permanecem fora de seu controle direto.

6.1. Modelo de ameaças e mitigações

Considera-se um adversário capaz de fornecer dados falsos ou manipular a captura biométrica durante a validação inicial; interceptar ou reutilizar apresentações; comprometer a carteira ou obter acesso à chave privada do titular; apresentar credenciais expiradas, suspensas ou revogadas; operar como verificador malicioso, solicitando atributos excessivos; ou correlacionar apresentações realizadas em diferentes serviços.

Também são considerados ataques na borda de captura biométrica, incluindo fotografias, vídeos, *deepfakes*, câmeras virtuais e outras formas de ataque de apresentação. Para delimitar o modelo, assume-se que os algoritmos criptográficos utilizados permanecem seguros, que a fonte autoritativa e sua base de dados não foram comprometidas e que a comunicação entre os componentes ocorre por canais autenticados e protegidos.

Tabela 4. Ameaças, mitigações previstas e riscos residuais no BraZKIL.

Ameaça e impacto	Mitigação prevista	Risco residual
Fraude na validação inicial: emissão indevida da credencial.	Validação cadastral e biométrica por fonte autoritativa e política de aceitação aplicada pelo emissor.	Ataques à captura, falhas de detecção de vivacidade ou comprometimento do dispositivo.
Emissor comprometido: emissão fraudulenta ou uso indevido de chaves.	Registro de emissores autorizados, auditoria, proteção e rotação de chaves e revogação de credenciais.	O emissor permanece um componente crítico e depende de controles operacionais.
Carteira comprometida: uso indevido da credencial ou extração da chave.	Vinculação à chave da carteira, armazenamento protegido, autenticação local e suspensão ou revogação.	A segurança depende do dispositivo, da proteção da chave e da resistência a *malware*.
Repetição de apresentação: reutilização de uma apresentação capturada.	Uso de *nonce*, audiência, validade temporal e prova de posse da chave vinculada.	Falhas no controle dos desafios podem permitir reutilização indevida.
Credencial inválida: aceitação de credencial expirada, suspensa ou revogada.	Verificação de `validUntil`, `credentialStatus` e listas agregadas de status.	A decisão depende da atualização do registro e da consulta pelo verificador.
Coleta excessiva: exposição desnecessária de dados pessoais.	Apresentação seletiva de `age_over_18`, sem CPF, documento, biometria ou data de nascimento.	Um verificador pode exigir atributos adicionais como condição de acesso.
Correlação: rastreamento entre serviços ou interações.	Redução de identificadores persistentes, ausência de consulta recorrente ao emissor e divulgação mínima.	O SD-JWT não garante não correlação; metadados e identificadores ainda podem associar diferentes usos.

As mitigações apresentadas na Tabela 4 pertencem ao modelo arquitetural do BraZKIL. A Seção 5 delimita quais mecanismos foram efetivamente implementados e exercitados na prova de conceito. Em particular, vinculação ao titular, desafio de frescor, autenticação local da carteira e listas agregadas de status dependem do perfil e da implementação adotados.

6.2. Discussão

As mitigações do BraZKIL atuam em camadas. Na emissão, a confiabilidade da credencial decorre da combinação entre a fonte autoritativa, a política de aceitação do emissor e a verificabilidade de suas chaves e metadados. Essa camada pode ser reforçada por registros de emissores autorizados, auditoria, rotação de chaves e, quando aplicável, certificados institucionais associados à ICP-Brasil.

Na apresentação, DIDs e credenciais verificáveis permitem verificar a origem e a integridade da credencial, enquanto OID4VCI e OID4VP padronizam os fluxos de emissão e apresentação [Lodderstedt et al. 2024, Terbu et al. 2023]. Esses protocolos, entretanto, não determinam por si sós se um emissor é confiável nem impedem o uso de uma

credencial cuja chave privada tenha sido comprometida.

Na PoC, a minimização de dados é realizada com SD-JWT VC, revelando apenas a afirmação etária necessária à decisão de acesso [Yasuda et al. 2024]. Diferentemente de uma prova de predicado baseada em conhecimento zero, o SD-JWT não calcula a condição etária sobre uma data de nascimento oculta. A privacidade decorre principalmente da não divulgação dos atributos protegidos e da separação entre a validação inicial e as apresentações posteriores.

A vinculação à chave da carteira e o uso de desafios de frescor podem reduzir os riscos de transferência e repetição indevidas. Contudo, a prova de posse de uma chave não comprova, isoladamente, a presença física ou a identidade civil contínua do titular. Um dispositivo desbloqueado, uma chave comprometida ou o compartilhamento voluntário da carteira ainda podem permitir o uso da credencial por terceiros.

Permanecem, portanto, riscos relacionados ao comprometimento do emissor ou da carteira, à indisponibilidade ou desatualização do registro de status, à correlação por metadados e à adoção de políticas excessivas pelos verificadores. O BraZKIL reduz a circulação de dados pessoais e biométricos, mas sua efetividade depende da combinação entre mecanismos criptográficos, governança institucional, segurança dos dispositivos e controles operacionais.

7. Conclusão e trabalhos futuros

Este trabalho apresentou o BraZKIL, uma arquitetura híbrida para verificação de maioridade no contexto brasileiro. A proposta separa a validação inicial, apoiada em uma fonte autoritativa, das comprovações posteriores realizadas por credenciais verificáveis e divulgação seletiva. Dessa forma, o serviço final recebe apenas a afirmação etária necessária, sem acesso direto a CPF, documento, data de nascimento ou biometria.

A contribuição central está na integração de padrões de identidade descentralizada, protocolos OpenID e fontes oficiais de validação em um modelo de confiança orientado ao ECA Digital e à minimização prevista pela LGPD. A PoC integrou serviços locais, uma carteira de código aberto e o ambiente de demonstração do Datavalid, exercitando emissão, armazenamento, apresentação seletiva, vinculação ao titular, verificação e revogação. Os resultados fornecem evidência preliminar da viabilidade funcional e da redução dos dados expostos ao verificador.

A implementação utiliza SD-JWT VC para divulgar uma afirmação de maioridade previamente calculada, não equivalendo a uma prova de predicado baseada em conhecimento zero. Os resultados também não permitem concluir sobre escalabilidade, conformidade jurídica integral ou interoperabilidade universal. Como trabalhos futuros, serão avaliados ambientes próximos de produção, resistência a repetição e correlação, modelos de governança e provas de conhecimento zero para predicados etários.

Declaração de uso de IA

Ferramentas de inteligência artificial foram utilizadas apenas como apoio à revisão textual, organização e formatação. Todo o conteúdo, análise, interpretação e responsabilidade científica são de responsabilidade exclusiva dos autores.

Referências

Brasil (2018). Lei n. 13.709, de 14 de agosto de 2018: Lei geral de proteção de dados pessoais (LGPD). Diário Oficial da União.

Brasil (2026). Lei n. 15.211, de 2025: ECA digital – proteção de crianças e adolescentes no ambiente digital. Diário Oficial da União. Vigência a partir de 17 mar. 2026.

European Commission (2025). Use case manual: Age verification. Technical report, European Commission. Manual de caso de uso da EU Digital Identity Wallet. Acessado em: 10 maio 2026.

Hoang, A.-T., Ileri, C. U., Sanders, W., and Schulte, S. (2024). zkssi: A zero-knowledge-based self-sovereign identity framework. In *2024 IEEE International Conference on Blockchain (Blockchain)*, pages 276–285.

Kuhn, D. R., Sporny, D., Longley, M., and Allen, C. (2018). The inevitable rise of self-sovereign identity. Technical report, Sovrin Foundation.

Lodderstedt, T., Yasuda, K., and Looker, T. (2024). OpenID for verifiable credential issuance. OpenID Foundation Specification. Acessado em: 28 abr. 2026.

Maurya, U. K., S, L., and Kumar, K. V. (2025). Decentralized identity verification using zero-knowledge proofs: A privacy-preserving authentication framework. In *2025 2nd International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF)*.

Moreira, A. L. D., Razzolini Filho, E., and Adrião, M. C. (2023). Vigilância do fluxo informacional e privacidade no ambiente digital. *RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação*, 21(00):e023012.

Privado ID (2024). Introduction to privado ID (formerly polygon ID). Documentação oficial. Acessado em: 28 abr. 2026.

Scheffler, S. and Liu, S. (2025). Exploring privacy in ID-based age verification architectures. IAB/W3C Workshop on Age-Based Restrictions on Content Access. Workshop paper. Acessado em: 11 maio 2026.

Self Labs (2024). Self Protocol: technical documentation. Self Labs Developer Documentation. Acessado em: 28 abr. 2026.

Serviço Federal de Processamento de Dados (SERPRO) (2024). Datavalid: documentação da api de validação biométrica e cadastral. SERPRO API Center. Acessado em: 28 abr. 2026.

Sporny, M., Guy, A., Sabadello, M., and Reed, D. (2022). Decentralized identifiers (DIDs) v1.0. W3c recommendation, W3C.

Sporny, M., Longley, D., Chadwick, D., et al. (2025). Verifiable credentials data model v2.0. W3c recommendation, W3C.

Terbu, O., Lodderstedt, T., Yasuda, K., Lemmon, A., and Looker, T. (2023). OpenID for verifiable presentations. OpenID Foundation Specification, Draft 16. Acessado em: 28 abr. 2026.

walt.id (2026). walt.id documentation. Acesso em: 3 ago. 2026.

Yasuda, K., Lodderstedt, T., et al. (2024). Sd-jwt-based verifiable credentials (sd-jwt vc). https://www.ietf.org/archive/id/draft-ietf-oauth-sd-jwt-vc-04.html.