Comitê Gestor da Internet no Brasil

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

Contribuição do CGI.br à Tomada de Subsídios sobre o Guia Orientativo “Mecanismos de Aferição de Idade"

1. Contexto

Ao longo de sua atuação, o Comitê Gestor da Internet no Brasil (CGI.br) tem exercido um papel central na articulação do diálogo multissetorial e na construção de entendimentos voltados ao aprimoramento das políticas públicas e dos marcos regulatórios relacionados à governança da Internet no Brasil. Essa atuação resultou em contribuições significativas para o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), o Estatuto Digital da Criança e do Adolescente – ECA Digital (Lei nº 15.211/2025) e a tomada de subsídios para o Guia Orientativo “Fornecedores de Produtos ou Serviços de Tecnologia da Informação”.

Reconhecemos e valorizamos a iniciativa da Agência Nacional de Proteção de Dados (ANPD) de realizar a Tomada de Subsídios referente ao **Guia Orientativo “Mecanismos de Aferição de Idade”**. Essa consulta representa uma medida relevante para apoiar a implementação das disposições do ECA Digital, ampliar a participação da sociedade no processo regulatório e proporcionar maior segurança jurídica aos agentes sujeitos à regulação. Além disso, a Tomada de Subsídios constitui uma oportunidade para que representantes da sociedade civil, da comunidade científica e tecnológica e do setor privado apresentem contribuições que auxiliem na elaboração de orientações baseadas em fundamentos técnicos, proporcionais e adequadas à diversidade do ecossistema digital brasileiro.

O Núcleo de Informação e Coordenação do Ponto BR (NIC.br), braço executivo do CGI.br, através de seu Centro de Estudos sobre Tecnologias Web (Ceweb.br) e como *host* do capítulo brasileiro do *World Wide Web Consortium* (W3C), vem acompanhando e estudando o desenvolvimento e aplicações de credenciais verificáveis. No contexto global de transformação digital cresce a necessidade de soluções seguras e interoperáveis para a comprovação automática de informações no ambiente online. As credenciais verificáveis permitem que declarações de atributos como identidade, diplomas, comprovantes de renda, propriedade de imóveis, habilitação para dirigir, registros de vacinação ou idade sejam emitidas por instituições confiáveis e apresentados digitalmente, com garantia criptográfica, preservação da privacidade e revelação seletiva de dados. Essas características contribuem para a agilidade da burocracia, o aumento da eficiência na prestação de serviços e o fortalecimento da confiança na economia digital.

No Brasil, o ECA Digital destaca-se como uma aplicação relevante dessa tecnologia ao estabelecer a necessidade de mecanismos eficazes de verificação de

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

idade para a proteção de crianças e adolescentes no ambiente online. As credenciais verificáveis oferecem uma solução precisa e respeitosa à privacidade, permitindo comprovar a maioridade ou a faixa etária sem a exposição de dados pessoais desnecessários, reduzindo os riscos de vazamento de informações e promovendo maior segurança jurídica e tecnológica para plataformas digitais e seus usuários.

Com o objetivo de contribuir com o tema, em novembro de 2025, o CGI.br produziu a *Contribuição do CGI.br à Consulta Pública – Aferição de Idade na Internet Brasileira do Ministério da Justiça e Segurança Pública*[1]. O documento prevê **sete recomendações para a aferição de idade** prevista no ECA digital, dentre as quais: (1) Proporcionalidade e necessidade, propondo que soluções de aferição de idade sejam aplicadas conforme o risco da atividade, evitando exigências excessivas para ambientes de baixo risco; (2) Privacidade e Proteção de Dados, prevendo que a implementação siga rigorosamente os princípios da Lei Geral de Proteção de Dados (LGPD), tais como minimização da coleta e vedação ao uso secundário das informações; (3) Inclusão e não discriminação, de forma que os mecanismos sejam acessíveis a todos, considerando-se que crianças e adolescentes em situação de vulnerabilidade, que não possuam documentos e dispositivos próprios, possuam alternativas; (4) Segurança Técnica, de forma a adotar padrões elevados que previnam fraudes, vazamentos e outros incidentes; (5) Não fragmentação, preservando o caráter global e aberto da Internet; (6) Interoperabilidade e padrões abertos, evitando a dependência de tecnologias proprietárias e concentração de mercado; (7) Transparência e auditabilidade, garantindo a transparência, responsabilidade e prestação de contas e direito a contestação por ações e resultados.

Aproveitando a experiência acumulada no Ceweb.br | NIC.br | CGI.br, este documento traz contribuições para o tema de “mecanismos de aferição de idade” com especial enfoque técnico, em credenciais verificáveis e em seu uso para aferição de idade. O CGI.br agradece a oportunidade de participar desta Tomada de Subsídios e reafirma seu compromisso em contribuir para uma implementação do ECA Digital que seja pautada por fundamentos técnicos, proporcionalidade e respeito ao princípio da proteção integral, em consonância com os direitos fundamentais de crianças e adolescentes. Nesse contexto, o Comitê coloca-se à disposição para colaborar com a ANPD na realização de debates técnicos, na promoção de ações de capacitação, no compartilhamento de evidências e boas práticas e na elaboração de orientações e instrumentos regulatórios que fortaleçam a proteção de crianças e adolescentes e favoreçam a construção de ambientes digitais mais seguros, inclusivos e compatíveis com seu desenvolvimento.

[1] COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Contribuição do CGI.br à consulta pública: aferição de idade na internet brasileira do Ministério da Justiça e Segurança Pública**. [S.l.]: CGI.br, [s.d.]. Disponível em: https://cgi.br/publicacao/contribuicao-do-cgi-br-a-consulta-publica-afericao-de-idade-na-internet-brasileira-do-ministerio-da-justica-e-seguranca-publica/. Acesso em: 13 jul. 2026.

Comitê Gestor da Internet no Brasil

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

2. Contribuições ao Guia

2.1. Enquadramento de credenciais verificáveis como Verificação de idade

Na seção "I. ASPECTOS GERAIS" do Guia Orientativo "Mecanismos de Aferição de Idade", a Figura 1 apresenta a taxonomia dos mecanismos de aferição de idade. **Dada a importância das credenciais verificáveis no contexto da aferição de idade, recomendamos que ela conste na figura**, sob a categoria a qual ela corresponde, que é de "verificação de idade". Tal enquadramento pressupõe a adoção das melhores práticas para a emissão de credenciais verificáveis, conforme exposto na seção 2.7 deste documento. O destaque das credenciais verificáveis dentre os mecanismos de verificação de idade deve ajudar a esclarecer as questões que levantamos a seguir.

2.2. Esclarecimentos técnicos sobre credenciais verificáveis

2.2.1. O significado de "verificável"

No tópico "Credenciais Verificáveis" da seção IV. REQUISITOS ESPECÍFICOS, o termo "verificável" é descrito como uma referência "*à possibilidade de a autenticidade e a integridade de uma credencial (...) ser recebida e validada por uma 'parte verificadora', por meio de suas próprias regras de negócio*". Essa redação dá a impressão de que o diferencial das credenciais verificáveis frente a outras formas de aferição de idade seria que ela permitiria uma validação arbitrária da autenticidade e integridade da credencial pelo produto/serviço de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles. Entretanto, esse sentido é incorreto e decorre de uma interpretação equivocada da própria fonte citada para tal definição[2].

Segundo tal referência:

> *O termo "verificável" nos termos "credencial verificável" e "apresentação verificável" refere-se à característica de uma credencial ou apresentação de poder ser verificada por um verificador, conforme definido neste documento. A verificabilidade de uma credencial não implica a veracidade das declarações nela codificadas. Em vez disso, ao estabelecer a autenticidade e a atualidade de uma credencial verificável ou apresentação verificável, um verificador valida*

[2] WORLD WIDE WEB CONSORTIUM (W3C). **What is a Verifiable Credential**. In: *Verifiable Credentials Data Model 2.0*. [S.l.]: W3C, [s.d.]. Disponível em: https://www.w3.org/TR/vc-data-model-2.0/#what-is-a-verifiable-credential

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

> *as declarações incluídas utilizando suas próprias regras de negócio antes de confiar nelas.*[3]

Vemos que o termo "verificável" refere-se à possibilidade da credencial ser verificada nos termos apresentados pela referência; e verificação significa, segundo ela[4]:

> *Avaliar se uma credencial verificável ou uma apresentação verificável constitui uma declaração autêntica e atual do emissor ou do apresentador, respectivamente. Isso inclui verificar se a credencial ou a apresentação está em conformidade com a especificação, se o mecanismo de segurança é atendido e se, quando aplicável, a verificação de status é bem-sucedida. A verificação de uma credencial não implica a avaliação da veracidade das declarações nela codificadas.*[5]

Concluímos que **"verificável" significa que é possível checar de maneira automatizada, por computadores: a conformidade da credencial com a especificação técnica; o status da credencial, se aplicável; e, mais importante, que a prova criptográfica de integridade da informação e de autenticidade da emissão é válida**.

A confusão feita no Guia Orientativo ocorre porque a referência alerta, logo após à definição de "verificável", que a verificação de uma credencial apenas garante que sua informação foi realmente produzida pelo seu emissor e que não foi adulterada *a posteriori*. Ela não garante, entretanto, que a informação que nela consta é verdadeira. A veracidade da informação depende de quão confiável é o emissor da credencial para atestar as informações em questão, e esse julgamento depende de critérios alheios à especificação técnica das credenciais verificáveis, critérios estes que são chamados pela referência de "regras de negócio do verificador".

2.2.2. Provas de conhecimento zero, revelação seletiva de informação e rastreabilidade

O Guia Orientativo menciona e recomenda em diversas passagens o uso de provas de conhecimento zero (*Zero-Knowledge Proofs*, ZKP):

> "*Existem meios técnicos que permitem que apenas a data de nascimento ou a idade sejam coletados, ou que compartilham informações de forma anonimizada ou pseudonimizada, como prova de conhecimento zero ou tokens, sem vinculação direta a nomes ou cadastros associados à determinada pessoa.*" (p. 6, 2° parágrafo);

[3] Tradução própria.
[4] WORLD WIDE WEB CONSORTIUM (W3C). **Verifiable Credentials Data Model 2.0**. [S.l.]: W3C, [s.d.]. Disponível em: https://www.w3.org/TR/vc-data-model-2.0/#dfn-verify
[5] Tradução própria.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

> "*Essas tecnologias permitem que um usuário comprove um atributo específico, por exemplo 'é maior de idade', a partir de uma credencial emitida por fonte fidedigna, sem que o serviço receba ou retenha informações adicionais, como data de nascimento completa, número de documento ou outros dados identificáveis.*"; (Quadro de dica da p. 29)
>
> "(...) *deve-se privilegiar o uso de provas de conhecimento zero (Zero-Knowledge Proof - ZKP) ou mecanismos equivalentes que permitam a verificação da idade sem revelação do dado pessoal relacionado.*"; (p. 43)

Tal recomendação é correta, dado que ZKPs permitem atestar predicados sem disponibilização de outras informações. Entretanto, a redação do guia pode dar a impressão de que a vantagem das ZKPs se limitaria à capacidade de relevar algumas das declarações (*claims*) presentes na credencial enquanto mantém as demais ocultas. Essa característica, em específico, também pode ser obtida com outros métodos mais simples como o de revelação seletiva disponível em padrões como o SD-JWT[6], do *Internet Engineering Task Force* (IETF), ou através da produção de credenciais com apenas a informação necessária para aferição de idade (e.g., ser maior de 18 anos).

Entretanto, ZKPs trazem outras vantagens, como evitar a rastreabilidade (*linkability*) presente nos métodos mais simples mencionados. A rastreabilidade acontece porque a assinatura digital, apresentada para confirmar a integridade e autenticidade da credencial, é única, de maneira que pode ser utilizada para acompanhar os acessos de um determinado usuário a sites e aplicativos toda vez que ele apresenta sua credencial. Já tecnologias como as assinaturas BBS[7] permitem a geração de ZKPs que demonstram a autenticidade e integridade das declarações da credencial sem revelar a assinatura digital do emissor, impedindo o rastreamento dos usuários. Embora a revelação seletiva do SD-JWT evite o fornecimento de outras declarações presentes na credencial, ela não evita o fornecimento de outras informações em sentido mais amplo, pois fornece a assinatura digital do emissor. Tal limitação do SD-JWT e de outros padrões que permitem revelação seletiva pode ser contornada com a emissão de múltiplas cópias de uma credencial que são descartadas após a apresentação, cada uma com uma assinatura digital diferente[8].

Para preservar a privacidade e evitar que se criem novos mecanismos de monitoramento online de usuários, **sugerimos que o Guia Orientativo recomende a adoção de tecnologias que não possibilitem o rastreamento (*linkability*) dos**

[6] INTERNET ENGINEERING TASK FORCE (IETF). **RFC 9901**. [S.l.]: IETF, [s.d.]. Disponível em: https://datatracker.ietf.org/doc/rfc9901/

[7] WORLD WIDE WEB CONSORTIUM (W3C). **Data Integrity BBS Cryptosuites v1.0**. [S.l.]: W3C, [s.d.]. Disponível em: https://www.w3.org/TR/vc-di-bbs/

[8] Seção "10.1. Unlinkability", INTERNET ENGINEERING TASK FORCE (IETF). **RFC 9901**. [S.l.]: IETF, [s.d.]. Disponível em: https://datatracker.ietf.org/doc/rfc9901/

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

usuários. Para além da revelação seletiva, essa é uma característica das provas de conhecimento zero que aconselhamos ressaltar.

Com base no exposto, sugerimos a seguinte modificação no quadro de dica da página 29:

> (...) *Entre essas abordagens estão mecanismos baseados em credenciais verificáveis e técnicas criptográficas de revelação seletiva e prova de conhecimento zero (Zero-Knowledge Proof – ZKP).*
>
> *Essas tecnologias permitem que um usuário comprove um atributo específico, por exemplo 'é maior de idade', a partir de uma credencial emitida por fonte fidedigna, sem que o serviço receba ou retenha informações adicionais, como data de nascimento completa, número de documento ou outros dados identificáveis. Provas de conhecimento zero possuem a vantagem adicional de não possibilitarem o rastreamento (linkability) dos usuários via apresentação de atributos únicos e fixos, tal qual a assinatura digital de uma credencial. Dessa forma, a verificação ocorre com exposição mínima de dados pessoais e do comportamento dos usuários, contribuindo para a observância dos princípios de minimização de dados e proteção da privacidade desde a concepção.*

E, na página 43:

> (...) *deve-se privilegiar o uso de provas de conhecimento zero (Zero-Knowledge Proof - ZKP) ou mecanismos equivalentes que permitam a verificação da idade sem revelação do dado pessoal relacionado e que não possibilitem o rastreamento (linkability) dos usuários.*

2.2.3. Checagem do status de validade da credencial

No tópico "Credenciais Verificáveis" da seção IV. REQUISITOS ESPECÍFICOS, está presente a seguinte frase: "*Cabe destacar ainda a necessidade de a credencial ter seu status de validade checado a cada apresentação pelo usuário.* Credenciais, de maneira geral, podem, de fato, ser revogadas. O exemplo mais corriqueiro disso é o da carteira nacional de habilitação (CNH), que pode ser suspensa antes da sua validade em razão do acúmulo de um certo número de pontos. Entretanto, os fatos que poderiam invalidar uma credencial de maioridade são menos evidentes.

Antes de aprofundar esse tema, cumpre diferenciar três processos que podem ser referidos como "checagem de validade" de uma credencial. O primeiro é a

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

verificação da integridade das informações e autenticidade da emissão da credencial através da prova criptográfica. Esse processo deve ser sempre executado para qualquer tipo de credencial. Segundo, caso a credencial possua um campo de validade (e.g., `validUntil`)[9], a data nele especificada pode ser consultada para sabermos se a credencial permanece dentro da validade estipulada pelo emissor no momento da emissão. Destacamos que esses dois processos são feitos isoladamente pelo verificador e independem de qualquer contato entre este e o emissor da credencial.

Terceiro, a credencial pode ser suspensa ou revogada antes da data de validade nela especificada, tal qual no exemplo da CNH. Nesse caso, a checagem de se isso ocorreu é comumente denominado de checagem de status.[10] Para esse processo, há necessidade de troca de informações entre emissor e verificador. A frase do Guia Orientativo destacada nesta seção parece tratar deste caso.

Está claro que um indivíduo, uma vez com idade igual ou superior a 18 anos, jamais terá sua condição de maior de idade revogada. No caso de uma credencial que ateste que um indivíduo pertence a uma determinada faixa etária, a existência de uma data de validade pré-estipulada poderia servir para invalidar a credencial antes do indivíduo mudar de faixa, tornando a checagem de status desnecessária. Portanto, a necessidade de checar o status de validade da credencial de idade ou maioridade a cada apresentação não é tão óbvia. Dado que essa checagem requer troca de informação entre emissor e verificador (troca antes desnecessária) e de mais processamento por ambos, **recomendamos que seja esclarecido as situações que poderiam levar à revogação ou suspensão de tais credenciais.**

Um possível motivador para a checagem de status de uma credencial seria a sua emissão com dados falsos ou incorretos. Entretanto, tais casos devem ser exceção e não ensejam, necessariamente, checagem de status a cada apresentação de todas as credenciais.

2.2.4. Armazenamento de credenciais em *cookies* de navegadores Web

O segundo parágrafo presente na página 44 do Guia Orientativo começa com a frase:

> "*Uma vez emitida e assinada digitalmente pelo emissor, a credencial verificável pode ser armazenada no próprio dispositivo do usuário – o portador, como em carteiras digitais ou em cookies de navegadores web.*"

[9] WORLD WIDE WEB CONSORTIUM (W3C). **Validity period**. In: *Verifiable Credentials Data Model 2.0*. [S.l.]: W3C, [s.d.]. Disponível em: https://www.w3.org/TR/vc-data-model-2.0/#validity-period
[10] WORLD WIDE WEB CONSORTIUM (W3C). **Bitstring Status List**. [S.l.]: W3C, [s.d.]. Disponível em: https://www.w3.org/TR/vc-bitstring-status-list/

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

Entretanto, desconhecemos referências técnicas que sugiram o armazenamento de credenciais verificáveis, tal qual descritas pelo W3C[11], em *cookies* de navegadores Web. Ao contrário, *cookies* seriam contra-indicados para o armazenamento de credenciais verificáveis por alguns motivos:

1. Os *cookies* são vinculados a domínios específicos e são acessíveis apenas pelo domínio que os definiu. Essa característica contraria o objetivo de uma credencial verificável de ser apresentável a qualquer verificador (no caso do navegador Web, a qualquer domínio).
2. O armazenamento de credenciais verificáveis deve ser feito de maneira segura, utilizando criptografia para garantir que as informações nelas presentes não sejam coletadas por pessoas não autorizadas. Porém, cookies podem ser facilmente inspecionados por qualquer pessoa que tenha acesso ao navegador em questão.
3. Espera-se que o detentor ou portador (*holder*) de credenciais verificáveis tenha controle sobre quando suas credenciais são apresentadas a verificadores. Entretanto, em requisições HTTP, *cookies* são enviados automaticamente ao domínio que os definiu. Dessa forma, a utilização de *cookies* para o armazenamento de credenciais verificáveis elimina a autonomia do portador sobre seus dados.
4. *Cookies* possuem limite de tamanho de 4KB. Credenciais verificáveis, entretanto, podem ser maiores que isso.

Algumas das limitações acima podem ser superadas com uso adaptado dos *cookies* e do navegador. Por exemplo, as informações armazenadas nos *cookies* podem ser criptografadas pelo domínio que os criou, atenuando o problema do item 2, e as informações de uma credencial podem ser dispersas em múltiplos *cookies*, reduzindo a limitação apresentada no item 4. Além disso, é possível utilizar outros armazenamentos do navegador, como o *cache*, para se transmitir informação entre domínios, numa estratégia conhecida como *supercookie*[12]. Entretanto, *cookies* certamente não foram desenhados para o armazenamento de credenciais verificáveis e não são o meio adequado para tal.

É possível que tal passagem do Guia Orientativo esteja se referindo ao uso de JSON Web Tokens (JWTs) em sistemas de Single Sign-On (SSO) ou de identidade federada, por exemplo, tal qual o OpenID Connect[13]. JWTs podem conter informações assinadas digitalmente e ser utilizados como um formato para credenciais verificáveis[14]. Além disso, sistemas de SSO ou de identidade federada com JWTs podem ser utilizados para realizar verificação de idade. Entretanto, apesar das

[11] WORLD WIDE WEB CONSORTIUM (W3C). **Verifiable Credentials Overview**. [S.l.]: W3C, [s.d.]. Disponível em: https://www.w3.org/TR/vc-overview/

[12] MOZILLA. **Mozilla explains: cookies and supercookies**. [S.l.]: Mozilla, [s.d.]. Disponível em: https://blog.mozilla.org/en/internet-culture/mozilla-explains-cookies-and-supercookies/

[13] OPENID FOUNDATION. **How OpenID Connect works**. [S.l.]: OpenID, [s.d.]. Disponível em: https://openid.net/developers/how-connect-works/

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

semelhanças com o sistema de credenciais verificáveis descrito pelo W3C, a distribuição de papéis e o local de armazenamento das credenciais são diferentes.

No sistema de credenciais verificáveis existem dois papéis que, tipicamente, são independentes: o emissor (*issuer*) e o detentor/portador (*holder*) da credencial. Enquanto o primeiro é a autoridade responsável por emitir a credencial e atestar as informações nela presentes, o segundo é quem armazena e apresenta a credencial a terceiros. Ademais, nesse sistema, a credencial fica armazenada no dispositivo do usuário, em um aplicativo de carteira digital ou *software* similar. Já no caso do SSO ou identidade federada, o provedor de identidade ou credenciais tipicamente acumula ambas as funções de emissor e armazenador, além de centralizar em seus servidores as credenciais de todos os usuários. Nesse sistema, o JWT que é enviado pelo provedor de identidade ou credenciais ao terceiro é uma confirmação de maioridade temporária e destinada especificamente ao terceiro em questão, tendo uma função similar à de apresentação verificável (*verifiable presentation*)[15] do ecossistema de Credenciais Verificáveis do W3C. A Tabela 1 resume algumas diferenças entre as duas arquiteturas.

A partir da discussão apresentada, **sugerimos um maior esclarecimento das tecnologias referenciadas sob o guarda-chuva "credenciais verificáveis" e termos associados**, tais como tokens etários, com explicitação dos seus significados e das distintas variações e possibilidades de implementação. Adicionalmente, recomendamos a citação de referências que definam tais termos.

	Credenciais Verificáveis	**Identidade Federada / SSO**
Estilo de verificação de atributos	"Apresente um documento"	"Ligue para a autoridade"
Nome dado ao produto/serviço de TI que quer comprovar a idade de um usuário	Verificador (*Verifier*)	Cliente (*Relying Party*)
Nome dado à autoridade responsável por atestar a identidade ou outros atributos do usuário	Emissor (*Issuer*)	Provedor de identidade (*Identity Provider*)

[14] INTERNET ENGINEERING TASK FORCE (IETF). **OAuth Selective Disclosure JWT for Verifiable Credentials (draft)**. [S.l.]: IETF, [s.d.]. Disponível em: https://www.ietf.org/archive/id/draft-ietf-oauth-sd-jwt-vc-00.html

[15] WORLD WIDE WEB CONSORTIUM (W3C). **Verifiable Presentations**. In: *Verifiable Credentials Data Model 2.0*. [S.l.]: W3C, [s.d.]. Disponível em: https://www.w3.org/TR/vc-data-model-2.0/#verifiable-presentations

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

Produto/serviço de TI precisa, previamente, estabelecer relação com a autoridade?	Não, não há acesso a um serviço, apenas consulta à credencial.	Sim, o cliente precisa estar registrado junto ao provedor de identidade.
Local de armazenamento da identidade/atributos dos usuários	Num repositório de credenciais (e.g. carteira digital) no dispositivo do usuário	Nos servidores do provedor de identidade.
Quando a autoridade é contactada por um produto/serviço de TI?	Apenas se/quando o verificador quiser checar o status da credencial.	Sempre que o usuário precisar autenticar no produto/serviço.
A autoridade precisa estar online no momento da verificação?	Não, a autoridade apenas emite a credencial e a envia ao usuário.	Sim, o provedor de identidade é a autoridade.
A autoridade sabe quais produtos/serviços estão sendo acessados pelo usuário?	Não, a apresentação da credencial é feita pela carteira digital do usuário.	Sim, sempre que o usuário precisar autenticar.
Como um site pode evitar repetir autenticação de um usuário?	Armazenando um *cookie* no navegador do usuário	Armazenando um *cookie* no navegador do usuário
Produto de TI (e.g. app) pode autenticar o usuário offline?	Sim, o app verifica as informações da credencial com a chave pública da autoridade.	Não, o cliente precisa contactar o provedor de identidade.
Há necessidade de um software instalado no dispositivo do usuário?	Sim, um repositório de credenciais ou carteira digital.	Não, a troca de informações é feita entre provedor de identidade e cliente.
O repositório de credenciais sabe quais produtos/serviços estão sendo acessados pelo usuário?	Sim, sempre que o usuário precisar apresentar uma credencial.	Não se aplica, não há necessidade desse tipo de software.

Tabela 1: Comparação entre sistema de credenciais verificáveis e identidade federada / SSO.

2.3. Definição de tokens etários

O termo “token etário” é mencionado diversas vezes no Guia Orientativo. Por exemplo:

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

> "*A utilização de tokens etários reduz significativamente a exposição de dados pessoais e limita a circulação de informações sensíveis entre diferentes sistemas.*" (p. 6);
>
> "*Nesse processo de verificação de idade, há a possibilidade de se recorrer a intermediários confiáveis que emitem tokens de idade (age tokens) para os usuários se autenticarem, conferindo maior segurança aos seus dados pessoais.*" (nota de rodapé 22, p. 18);
>
> "*O sistema operacional, já configurado com o perfil de criança sob supervisão parental, envia automaticamente um sinal de idade (token etário) informando que o usuário possui entre 12 e 14 anos*" (exemplo na p. 20);
>
> "*Entre os exemplos de tecnologias que podem contribuir para esse objetivo estão soluções baseadas em intermediários confiáveis, credenciais verificáveis ou tokens criptográficos.*" (p. 36); e
>
> "*Para esse fim, recomenda-se a adoção de arquiteturas baseadas em tokenização ou credenciais digitais, nas quais o resultado da aferição etária seja representado por um sinal de idade ou token criptográfico que indique apenas se o usuário atende ao requisito etário exigido pelo serviço ou produto.* (p. 39).

Entretanto, não há, no Guia Orientativo, uma definição do que significa "token etário". Conforme seção anterior, sugerimos que essa definição seja incluída.

Uma definição de token criptográfico (*age tokens*) é apresentada na publicação "Radar Tecnológico n° 5: mecanismos de aferição de idade" da ANPD[16], p. 32:

> "*É uma espécie de credencial digital, emitida e assinada por uma entidade de confiança, que serve para comprovar um atributo específico de uma pessoa sem expor seus dados completos. Esse modelo é descrito em normas internacionais de padronização (ISO/IEC, 2025; W3C, 2025) e em estudos recentes na Austrália (Australia, 2025b) e na União Europeia (Comissão Europeia, 2025a). No contexto da aferição de idade, o token não carrega dados como nome, CPF ou data de nascimento. Em vez disso, ele contém apenas a informação necessária, por exemplo ser 'maior de 13 anos' ou 'entre 16 e 18 anos' ou ainda 'maior de 18 anos'. Essa credencial é protegida por criptografia, o que garante sua autenticidade e impede falsificações.*"

Segundo a publicação, tokens etários possuem diversas das características de credenciais verificáveis: eles são emitidos e assinados por uma entidade de

[16] AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Radar Tecnológico n. 5: mecanismos de aferição de idade**. Brasília: ANPD, [s.d.]. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-5-mecanismos-de-afericao-de-idade.pdf

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

confiança; eles são descritos em normas como o *Verifiable Credentials Data Model v2.0* do W3C[17]; e são credenciais protegidas por criptografia, o que garante sua autenticidade e impede falsificações.

A seguir, publicação afirma que tokens etários seguem as seguintes etapas principais, que também são as etapas seguidas pelas credenciais verificáveis: a emissão do token é feito por uma organização de confiança após comprovação de idade pelo usuário; o token é armazenado pelo usuário em carteiras digitais ou outro tipo de *software* instalado em seu dispositivo; quando requisitado, o usuário apresenta o token, que é validado pela chave pública do emissor.

Por fim, a publicação afirma que os tokens etários têm seu uso regido por um modelo de duplo-cego, no qual quem emite a credencial não sabe em qual serviço ela será apresentada e o serviço que o recebe não consegue identificar o usuário. "*Em outras palavras, o emissor não rastreia o comportamento do usuário, e o receptor não tem acesso à sua identidade, ficando restrito à informação binária de que o requisito etário foi atendido.*" (Radar Tecnológico n° 5, p. 33). Esse padrão de uso também se encaixa nas credenciais verificáveis. A própria publicação menciona que "*a estrutura do duplo-cego aparece nos padrões do W3C*", se referindo ao *Verifiable Credentials Data Model v2.0*. Conclui-se, portanto, que tokens etários seriam credenciais verificáveis com a especificidade de conterem apenas a informação necessária para a verificação etária.

Entretanto, ao contrário do termo "credenciais verificáveis", que é mais bem estabelecido e preciso, o termo "token etário" não possui uma definição clara em referências para além do Radar Tecnológico n° 5. O termo pode ser usado, por exemplo, para se referir a um serviço de verificação de idade que segue uma arquitetura de SSO ou identidade federada, diferente da arquitetura de credenciais verificáveis, tal qual mencionado na seção anterior. Exemplo disso é o serviço provido pela empresa Yoti[18]. **Frente a possível confusão entre os mecanismos de credenciais verificáveis e de SSO ou identidade federada, e considerando que estes últimos podem ser possíveis soluções para a aferição etária online, recomendamos que eles sejam apresentados, descritos e diferenciados das credenciais verificáveis, acompanhados da especificação de seus requisitos específicos**.

[17] WORLD WIDE WEB CONSORTIUM (W3C). **Verifiable Credentials Data Model 2.0**. [S.l.]: W3C, [s.d.]. Disponível em: https://www.w3.org/TR/vc-data-model-2.0/
[18] YOTI. **Age token**. [S.l.]: Yoti, [s.d.]. Disponível em: https://developers.yoti.com/age-verification/age-token

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

2.4. Relação entre confiabilidade e proteção à privacidade

2.4.1. O entendimento presente no Guia Orientativo

Ao longo do Guia Orientativo, parece estar presente, implicitamente, uma suposição de que existiria um *trade-off* entre proteção à privacidade e acurácia/robustez/confiabilidade, como se essas qualidades estivessem dispostas em uma escala unidimensional, na qual o aumento de uma qualidade (e.g., acurácia/robustez/confiabilidade) necessariamente implicasse numa redução da outra (e.g., proteção à privacidade). Essa suposição é representada na Figura 1.

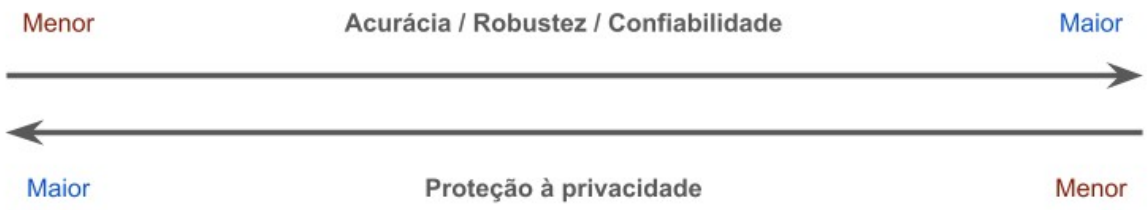

Figura 1: compreensão equivocada da relação entre proteção à privacidade e acurácia/ robustez/confiabilidade.

Exemplo de onde essa suposição parece presente é o segundo parágrafo visível na página 7 do referido documento (na seção I. ASPECTOS GERAIS), que diz "*(...) o Decreto prevê o uso de soluções de verificação de idade em contextos que podem ser considerados de maior risco*", e em seguida afirma que a verificação de idade pode também ser utilizada em casos de dúvida surgidas da adoção de outros mecanismos de aferição de idade. Dessa forma, o texto parece dizer que os mecanismos padrão de aferição de idade para contextos de baixo risco seriam outros que não a verificação de idade e que a verificação de idade seria apenas adotada em caso de necessidade, como se dela decorresse, necessariamente, algo negativo.

Outro trecho do documento onde a suposição de *trade-off* entre privacidade e confiabilidade parece estar presente é na seção III. REQUISITOS GERAIS, quando é tratado o tema da proporcionalidade. No terceiro parágrafo presente na página 16, o texto diz que o requisito da proporcionalidade "*impõe aos fornecedores o dever de buscar equilíbrio entre, de um lado, a acurácia, a robustez e a confiabilidade exigidas em um determinado contexto e, de outro, a probabilidade e a gravidade dos efeitos adversos que a própria solução de aferição de idade pode gerar sobre direitos dos usuários, em especial sobre a privacidade e a proteção de dados pessoais.*" Ao tratar da relação entre acurácia, robustez e confiabilidade, de um lado, e a privacidade e proteção de dados pessoais, de outro, como relação de equilíbrio, o documento parece indicar a existência de um *trade-off*.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

Na mesma seção, essa concepção de *trade-off* também fica implícita no trecho do quinto parágrafo da página 17: "*O racional é que mecanismos de aferição etária com um grau maior de impacto à privacidade, à proteção de dados pessoais, à segurança, à saúde e ao bem-estar de crianças e adolescentes devem ser reservados para contextos de risco elevado no ambiente digital. Por outro lado, mecanismos com menor nível de impacto deve* [sic] *ser priorizados em cenários de baixo risco. Essa abordagem busca equilibrar a proteção de crianças e adolescentes no ambiente digital com os direitos à privacidade e à proteção de dados pessoais.*" Ao colocar que mecanismos de menor impacto à privacidade devem ser priorizados em cenários de baixo risco, dá-se a impressão que mecanismos com maior impacto à privacidade são necessários em cenários de alto risco.

Por fim, a ideia de *trade-off* pode ser apreendida do terceiro *bullet point* da página 24. Esse item recomenda que fornecedores de produtos ou serviços "*avaliem a proporcionalidade entre os riscos do produto ou serviço e os riscos decorrentes do mecanismo de aferição de idade a ser implementado*", como se produtos com maior risco exigissem soluções de aferição de idade mais confiáveis e, necessariamente, com mais riscos.

Entretanto, a realidade é que as qualidades de acurácia/robustez/confiabilidade e proteção à privacidade são independentes e ortogonais, mais adequadamente representadas na Figura 2. Isso significa, como corretamente aponta o documento em outros trechos, que existem soluções que combinam alta proteção à privacidade com alta acurácia, robustez e confiabilidade: as credenciais verificáveis e tecnologias associadas. **Ao atenderem simultaneamente a esses dois requisitos, as credenciais verificáveis mostram-se atualmente a solução tecnicamente mais adequada para todos os tipos de produtos e serviços**, quaisquer que sejam seus riscos.

A Figura 2 também sugere uma especificação mais clara e precisa das recomendações ou obrigações de cada produto/serviço de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles em relação a adoção de mecanismos de aferição de idade. **Para produtos/serviços de alto risco, são exigidos mecanismos de aferição de idade com alta confiabilidade. Para produtos/serviços de baixo risco, são exigidos mecanismos de aferição de idade com alta proteção à privacidade.** Cumpridos esses quesitos, recomenda-se a busca pela melhor solução em relação a outra dimensão, isto é: para serviços de alto risco, as opções de mecanismos seriam aquelas com alta confiabilidade, como já foi dito; e dentre essas opções, as com maior proteção à privacidade seriam preferíveis. Já entre serviços de menor risco, as opções de mecanismos seriam aquelas com alta proteção à privacidade; e dentre essas opções, as com maior confiabilidade seriam preferíveis frente às demais. **Novamente concluímos que a solução de credenciais verificáveis, se disponível, é tecnicamente mais adequada para todos os produtos/serviços.**

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

Figura 2: Relação entre proteção à privacidade (eixo horizontal) e acurácia/robustez/confiabilidade (eixo vertical). Diferentes métodos de aferição de idade são distribuídos no diagrama de maneira aproximada, como recurso ilustrativo. As linhas tracejadas verde e rosa indicam as características que devem ser priorizadas nas soluções de aferição de idade para produtos ou serviços de baixo e alto risco, respectivamente.

2.4.2. Modificações propostas ao Guia Orientativo

Com base no exposto acima, entendemos que não faria sentido sugerir a complementação de um método de estimativa ou inferência com credenciais verificáveis, tal qual feito no segundo parágrafo da página 7 do Guia Orientativo, dado que os primeiros métodos são tanto menos confiáveis quanto menos seguros em relação à privacidade do que o último. **Havendo a disponibilidade da adoção de credenciais verificáveis, essas devem ser utilizadas no lugar dos demais**

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

mecanismos de aferição de idade. Apresentamos a seguir uma nova redação do referido parágrafo que reflete o entendimento acima:

> *Por isso, o Decreto prevê o uso de soluções de verificação de idade (isto é, de alto grau de confiabilidade) em contextos que podem ser considerados de maior risco, como serviços que oferecem acesso a conteúdo pornográfico (art. 16, § 1o), redes sociais que disponibilizam conteúdos, serviços ou produtos proibidos (art. 19, II) e jogos eletrônicos com caixas de recompensa (art. 23). ~~A verificação de idade também pode ser utilizada~~ Mecanismos de verificação de idade com menor proteção à privacidade, tais como a verificação documental, também podem ser utilizados para complementar análises efetuadas por estimativa e inferência, ou até mesmo fornecer evidências adicionais sempre que necessário, especialmente quando o resultado da aferição não é conclusivo. Igualmente, ~~um mecanismo de verificação de idade poderá ser utilizado~~ tais mecanismos poderão ser utilizados em casos de contestação do resultado inicial pelo usuário ou quando houver divergência entre a aferição de idade realizada pelo fornecedor de tecnologia da informação e o sinal de idade enviado pela loja de aplicações de internet ou sistema operacional. Em qualquer caso, havendo a disponibilidade de verificação de idade via mecanismos que combinam confiabilidade com alta proteção à privacidade, tais como credenciais verificáveis, esta será preferível no lugar dos demais mecanismos.*

Em consonância com o exposto, sugerimos que a entrada na coluna “Aferição de idade” da linha “Fornecedor de conteúdo, produto ou serviço proibido (art. 15)” da Tabela 1 seja alterada *para:*

> *“Mecanismos eficazes de verificação de idade, independentemente do sinal de idade recebido, com preferência para credenciais verificáveis e tecnologias análogas.*

”

Na seção III. REQUISITOS GERAIS, sugerimos que seu terceiro parágrafo seja alterado para:

> *Este requisito orienta a aplicação dos demais parâmetros previstos no Decreto, na medida em que impõe aos fornecedores o dever de ~~buscar equilíbrio entre, de um lado,~~ otimizar, em conjunto, a acurácia, a robustez e a confiabilidade exigidas em*

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

> *um determinado contexto ~~e, de outro,~~ com a probabilidade e a proteção contra efeitos adversos que a própria solução de aferição de idade pode gerar sobre direitos dos usuários, em especial sobre a privacidade e a proteção de dados pessoais.*

Além disso, no último parágrafo da página 16, recomendamos a complementação do trecho para:

> Nesse sentido, o relatório do Ministério da Justiça e Segurança Pública (MJSP) "Mecanismos de aferição de idade" registra convergência multissetorial quanto à preferência por soluções que "minimizam a exposição de dados", tais como as credenciais verificáveis [...]

Ainda na seção III. REQUISITOS GERAIS, recomendamos a seguinte redação para o quinto parágrafo presente na página 17:

> (...) O racional é que mecanismos de aferição etária com um grau maior de impacto à privacidade, à proteção de dados pessoais, à segurança, à saúde e ao bem-estar de crianças e adolescentes devem ser reservados para contextos de risco elevado no ambiente digital, quando mecanismos confiáveis com menor grau de impacto estiverem indisponíveis. Por outro lado, mecanismos com menor nível de impacto devem ser priorizados em cenários de baixo risco. Essa abordagem busca equilibrar a proteção de crianças e adolescentes no ambiente digital com os direitos à privacidade e à proteção de dados pessoais.

Já na coluna "Exemplos de medidas de mitigação" da linha "Riscos advindos da verificação etária" da Tabela 4, sugerimos o seguinte conteúdo:

> "*Adotar mecanismos de aferição com menor grau de impacto à privacidade, desde que atendam aos graus mínimos de acurácia, robustez e confiabilidade e nas hipóteses permitidas, tais como o de credenciais verificáveis.*"

E, no terceiro *bullet point* da página 24:

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

"Avaliem ~~a proporcionalidade entre~~ em conjunto os riscos do produto ou serviço e com os riscos decorrentes do mecanismo de aferição de idade a ser implementado;"

2.5. Inclusão e não discriminação com métodos alternativos a credenciais verificáveis

Conforme apresentado na seção anterior, do ponto de vista da acurácia/robustez/confiabilidade, da segurança e da proteção à privacidade, as credenciais verificáveis são o mecanismo de aferição de idade preferível em qualquer contexto. Nesse sentido, se disponíveis, elas devem sempre ser ofertadas aos usuários como a maneira padrão de aferição de idade.

Ocorre que, para ser realizável, a verificação de idade com credenciais verificáveis requer que o usuário possua uma credencial verificável que possa ser utilizada para verificação de idade, mas nem todas as pessoas se enquadram nessa situação. Podem existir, por exemplo, pessoas que não possuem conta no gov.br de nível suficiente para a emissão de credenciais, que não realizaram essa emissão, e que não têm acesso a meios alternativos legítimos de emissão de credenciais. Isso torna relevante os demais mecanismos de aferição de idade mesmo no cenário no qual a verificação de idade através de credenciais verificáveis está disponível: **os demais mecanismos servem como alternativas de verificação que possam garantir a inclusão e a não discriminação**, embora às custas da confiabilidade, segurança e proteção à privacidade.

Assim, o modelo de aferição de idade com múltiplas camadas, quando conta com credenciais verificáveis em uma das camadas, não tem por objetivo garantir maior confiabilidade (dado que as credenciais verificáveis são o mecanismo mais confiável de aferição de idade), mas sim maior inclusão e não discriminação. Nesse sentido, propomos a **complementação** do segundo parágrafo presente na página 17 com a frase:

Ademais, métodos isolados de aferição etária podem ser incapazes de garantir inclusão e não discriminação, uma vez que nem todas as pessoas podem estar aptas a realizar a aferição através de um determinado método. Essa visão privilegia o requisito da proporcionalidade e possibilita que a aferição de idade seja estruturada com a utilização sucessiva de diferentes mecanismos, aplicados progressivamente conforme a capacidade do usuário de realizar a aferição ou conforme o grau de incerteza do resultado obtido em etapas anteriores. (...)

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

2.6. Interoperabilidade

Na página 35 do Guia Orientativo, dentro da seção III. REQUISITOS GERAIS, é iniciada uma subseção sobre interoperabilidade. De maneira geral, a subseção trata das bases legais para a interoperabilidade e menciona algumas de suas vantagens, mas não especifica em detalhe como ela é atingida. Entretanto, acreditamos que essa possa ser uma informação útil dentro do Guia Orientativo.

Nesse sentido, **sugerimos esclarecer que a interoperabilidade é perseguida com a adoção de padrões de interface e protocolos de comunicação entre sistemas que sejam amplamente adotados**, seja porque definidos por organizações de padronização – como a Associação Brasileira de Normas Técnicas (ABNT), *International Organization for Standardization* (ISO), IETF, W3C e *OpenID Foundation* –, seja por que utilizados pela maioria dos provedores de um determinados serviço ou por instituições de grande peso. No caso das credenciais verificáveis, recomenda-se a adoção de padrões como OpenID4VCI[19], W3C VCDM[20], SD-JWT VC[21], ISO mDoc[22], OpenID4VP[23], W3C DC API[24], HTTP[25], IETF Status List[26] e/ou W3C Bitstring Status List[27].

Ademais, **recomendamos, sempre que possível, que os padrões adotados pelas implementações dos mecanismos de aferição de idade sejam padrões abertos**, isto é, que sejam publicamente disponíveis, que possam ser implementados por qualquer pessoa ou organização, sem discriminação, e que seja livre de *royalties* (ou seja, de implementação gratuita). Padrões abertos eregem menos barreiras para a criação de soluções tecnológicas, facilitam a entrada de novos participantes e possibilitam o surgimento de um ecossistema mais diverso, robusto e volumoso, beneficiando todos os envolvidos através de seu efeito de rede.

[19] OPENID FOUNDATION. **OpenID for Verifiable Credential Issuance 1.0**. [S.l.]: OpenID, [s.d.]. Disponível em: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
[20] WORLD WIDE WEB CONSORTIUM (W3C). **Verifiable Credentials Data Model 2.0**. [S.l.]: W3C, [s.d.]. Disponível em: https://www.w3.org/TR/vc-data-model-2.0/
[21] INTERNET ENGINEERING TASK FORCE (IETF). **OAuth Selective Disclosure JWT for Verifiable Credentials (draft)**. [S.l.]: IETF, [s.d.]. Disponível em: https://www.ietf.org/archive/id/draft-ietf-oauth-sd-jwt-vc-00.html
[22] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 18013-5: Mobile driving licence (mDL)**. Genebra: ISO, [s.d.]. Disponível em: https://www.iso.org/standard/69084.html
[23] OPENID FOUNDATION. **OpenID for Verifiable Presentations 1.0**. [S.l.]: OpenID, [s.d.]. Disponível em: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
[24] WORLD WIDE WEB CONSORTIUM (W3C). **Digital Credentials**. [S.l.]: W3C, [s.d.]. Disponível em: https://www.w3.org/TR/digital-credentials/
[25] INTERNET ENGINEERING TASK FORCE (IETF). **RFC 9110: HTTP Semantics**. [S.l.]: IETF, [s.d.]. Disponível em: https://www.rfc-editor.org/info/rfc9110/
[26] INTERNET ENGINEERING TASK FORCE (IETF). **OAuth Status List (draft)**. [S.l.]: IETF, [s.d.]. Disponível em: https://datatracker.ietf.org/doc/draft-ietf-oauth-status-list/
[27] WORLD WIDE WEB CONSORTIUM (W3C). **Bitstring Status List**. [S.l.]: W3C, [s.d.]. Disponível em: https://www.w3.org/TR/vc-bitstring-status-list/

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

Por fim, destacamos que os parágrafos sexto e sétimo da página 36, ainda na subseção sobre interoperabilidade, na realidade tratam de privacidade. Recomendamos que eles sejam suprimidos ou transferidos para a seção apropriada do Guia.

2.7. Definição de parâmetros para sinais de idade, verificação de idade como serviço e emissão de credenciais

Em diversos trechos do Guia Orientativo são colocadas a possibilidade de produtos/serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles realizarem a aferição de idade através de sinais de idade fornecidos por lojas de aplicações ou sistemas operacionais, verificação de idade como serviço ou por credenciais verificáveis. Cumpre ressaltar que a confiabilidade desses sistemas depende de como a idade é inicialmente aferida pelos fornecedores desses serviços ou emissores das credenciais. Entretanto, o Guia Orientativo não aborda essa questão, a não ser de forma sucinta a respeito da verificação de idade como serviço na nota de rodapé 22. Dessa forma, **recomendamos a definição de parâmetros para: (1) a produção de sinais de idade por lojas de aplicações ou sistemas operacionais; (2) a verificação de idade que será posteriormente ofertada como serviço; e (3) a emissão de credenciais verificáveis**.

Como as aferições iniciais de idade feitas por lojas de aplicações, sistemas operacionais e prestadores de serviço de verificação de idade, que posteriormente serão oferecidas a terceiros, são aferições tais quais as demais descritas no Guia Orientativo, a elas cabem, preliminarmente, as mesmas orientações gerais e específicas feitas no Guia. Entretanto, por se tratarem de serviços que, a princípio, serão utilizados em larga escala por muitos atores, inclusive em contextos de alto risco, tal qual explicitado pela Tabela 3 do Guia Orientativo, a eles cabe o rigor máximo em termos de acurácia/robustez/confiabilidade, segurança e proteção à privacidade.

Em outras palavras, dada a recomendação do uso de sinais de idade ou de verificação de idade como serviço em todos os contextos, não teria sentido que esses mecanismos terceirizados tivessem qualidades inferiores aos demais mecanismos sugeridos. Isto é, o uso de sinais de idade ou de verificação de idade como serviço não podem servir para validar a aplicação de métodos inferiores aos exigidos para cada contexto. Dessa forma, **recomendamos que a aferição inicial de idade feita por lojas de aplicações, sistemas operacionais e prestadores de serviço de verificação de idade seja realizada utilizando credenciais verificáveis**.

De maneira similar, a acurácia/robustez/confiabilidade das próprias credenciais verificáveis está vinculada a quem é seu emissor e ao método utilizado

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

para atestar as informações nela inscritas. A fim de garantir tais qualidades, recomendamos que a emissão das credenciais seja feita a partir de documentos ou bases oficiais do governo. Além de terem grau máximo de confiabilidade dentre os mecanismos possíveis de aferição de idade, documentos e bases oficiais possuem validade jurídica e são a referência legal basilar para comprovação de informações, de maneira que seu uso na emissão de credenciais traz maior segurança jurídica para o sistema.

Do ponto de vista da acurácia/robustez/confiabilidade e da proteção à privacidade, a emissão de credenciais verificáveis por entidades privadas a partir de documentos oficiais introduz um ponto a mais de risco no sistema se comparado com a emissão direta pelo poder público. A verificação de idade inicial, necessária para emissão da credencial, ainda seria uma verificação documental sujeita aos riscos discutidos no próprio Guia Orientativo, página 41, tais como adulteração dos documentos e armazenamento, retenção, vazamento e uso indevido de dados.

A Figura 3 ilustra tal comparação. No processo de emissão, transmissão e apresentação de credenciais verificáveis, cada novo ator e nova transação introduz um novo ponto de risco para a acurácia/robustez/confiabilidade e privacidade. Na situação B, por exemplo, os documentos digitais ou em papel, emitidos pelo poder público, podem ser adulterados antes de serem entregues ao emissor privado, e o emissor privado pode ter os documentos vazados ou utilizar os documentos de maneira indevida, adicionando mais riscos aos já existentes na situação A.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

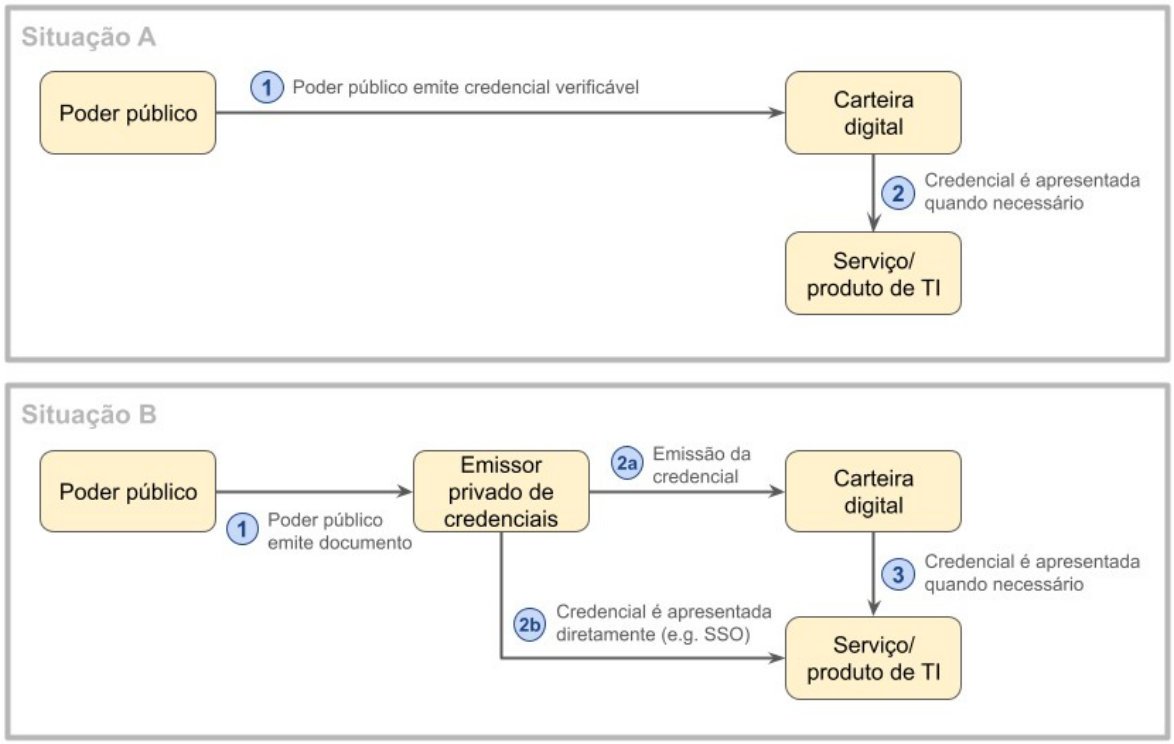

Figura 3: Fluxo e atores da emissão e uso de credenciais verificáveis nas situações em que a emissão é feita pelo governo (A) e por terceiros (B). O fluxo 2b representa a possibilidade do emissor privado cumprir o papel de emissor e armazenador das credenciais e prestar o serviço terceirizado de verificação de idade em um sistema de identidade federada ou *Single Sign-On* (SSO), tal qual descrito na seção 2.2.4 deste documento.

Dessa forma, **sugerimos que a emissão de credenciais seja feita diretamente e exclusivamente pelo poder público e que seja conferido a tais credenciais uso preferencial**. A emissão de credenciais verificáveis através de intermediários e sua utilização devem ser reservadas a situações especiais, visando a inclusão e não discriminação, se necessário, tal qual descrito na seção 2.5 deste documento.

Em consonância com o exposto, cumpre salientar que as recomendações de uso de credenciais verificáveis feitas nas seções anteriores pressupõem elas terem sido emitidas de maneira acurada, robusta, confiável, segura e com respeito à privacidade, tal qual aqui especificado.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

2.8. Dispositivos compartilhados e autenticação do usuário em carteiras digitais

Dentro da seção IV. REQUISITOS ESPECÍFICOS, a subseção sobre Credenciais Verificáveis estabelece alguns requisitos para as carteiras digitais e outros repositórios que armazenariam as credenciais. Frente ao difundido uso compartilhado de dispositivos nas famílias brasileiras, no qual crianças e adolescentes têm acesso ao dispositivo desbloqueado dos pais ou responsáveis, cabe considerar a recomendação, em certos contextos, da carteira digital realizar a autenticação do usuário – via senha ou biometria – antes dela apresentar uma credencial de maioridade a algum site ou aplicativo. Isso ajudaria a impedir que crianças e adolescentes acessem conteúdos proibidos através de dispositivos compartilhados.

O Comitê Gestor da Internet no Brasil agradece, mais uma vez, a oportunidade de contribuir tecnicamente com o tema, tendo em vista a necessidade em desenvolver mecanismos de aferição de idade que sejam tecnicamente pertinentes, além de compatíveis com o princípio da proteção integral da criança e do adolescente.

Ficamos à disposição para quaisquer esclarecimentos e novas colaborações.