Identificação Eletrônica do Registro Civil do Brasil

Brendon Vicente R. Silva[1], **Frederico Schardong**[1,2], **Luis Carlos Vendramin Junior**[3], **Ricardo F. Custódio**[1]

[1]Laboratório de Segurança em Computação (LabSEC)
Universidade Federal de Santa Catarina (UFSC)

[2]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS)

[3]Operador Nacional do Sistema Eletrônico de Registros Públicos (ONSERP)

Resumo. *Este artigo apresenta a Identificação do Registro Civil (IdRC), um provedor de identidade eletrônica integrado as bases de dados biográficos do cidadão brasileiro, por meio dos registros públicos tais como nascimento, casamento e óbito efetuados pelos Oficiais de Registro Civil de Pessoas Naturais. Por usar dados primários, a IdRC se diferencia de outros provedores de identidade eletrônica, podendo fornecer para provedores de serviço, mediante autorização do usuário, atributos primordiais, prova de vida e outros.*

1. Introdução

A importância da identidade eletrônica é emergente na sociedade, tendo em vista a crescente digitalização das interações humanas. Tarefas e serviços que até então eram feitos exclusivamente no mundo físico são gradativamente transportados para o âmbito virtual. Nesse sentido, é possível observar uma movimentação tecnológica global de digitalização e padronização de identidades eletrônicas, a fim de oficializar o reconhecimento digital de cidadãos em um contexto legal [Council of European Union 2014, Grassi et al. 2017].

Um dos grandes desafios nesse cenário diz respeito à maneira de coletar, assegurar e principalmente verificar a autenticidade de informações do usuário, de forma que se possa afirmar com precisão a veracidade de seus dados. É possível, por exemplo, requerer a documentação física de uma pessoa para atestar sua identidade, de maneira similar ao processo de autenticação feito no mundo real. Mas, embora essa solução atenue os problemas citados, ela ainda não os resolve. Documentos físicos podem ser fraudados, precisam ser cadastrados manualmente e podem não refletir os dados mais atualizados.

Dessa forma, a busca por uma identidade eletrônica que reflita e agregue os registros públicos dos cidadãos brasileiros de maneira integral resultou na criação da Identificação do Registro Civil (IdRC)[1]: uma identidade eletrônica que, por ser conectada à base de dados primária da nação, garante uma vasta gama de informações de seus usuários. Esses dados são verificados, assegurados e constantemente atualizados (conforme Art. 106 e 107 da lei Nº 6.015 [Brasil 1973]) por uma entidade governamental, sem que seja necessária sua administração por parte do proprietário da identidade.

O presente trabalho foi realizado com apoio do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS).

[1]`https://idrc.registrocivil.org.br/`

Neste artigo serão descritas e embasadas as escolhas arquiteturais e técnicas da IdRC, esclarecendo suas características e funcionamento, bem como passos futuros. O restante deste trabalho é organizado da seguinte maneira: a Seção 2 apresenta fatores de autenticação disponíveis; a Seção 3 apresenta os níveis de garantia e o ciclo de vida de identidades; então a Seção 4 explica como a integração com provedores de serviço acontece; e, por fim, a Seção 5 conclui o artigo apontando trabalhos futuros.

2. Fatores de Autenticação

Fatores de autenticação podem ser descritos como métodos ou técnicas utilizados para garantir que o usuário é quem diz ser, ou seja, garantir que o usuário é o dono da identidade eletrônica que está tentando utilizar. Tipicamente três categorias de fatores de autenticação são descritas pela literatura [Grassi et al. 2017]: (i) algo que você sabe (conhecimento); (ii) algo que você possui (posse); e (iii) algo que você é (intrínseco).

A IdRC atualmente conta com cinco fatores de autenticação distribuídos nas três categorias mencionadas acima. Conhecimento: (i) senha; e (ii) questionário sobre informações biográficas intergeracionais. Posse: (iii) *Time-based One Time Password* (TOTP) enviado por *e-mail* ou SMS, bem como apresentado em aplicativos (*e.g.*, Google Authenticator e FreeOTP); e (iv) WebAuthN [Hodges et al. 2021]. Por fim, o fator intrínseco é (v) biometria facial. A biometria consulta múltiplas fontes governamentais para avaliar a veracidade das informações coletadas. Estes fatores de autenticação compõem, em conjunto com outros parâmetros, os níveis de garantia da IdRC.

3. Nível de Garantia e Ciclo de Vida

O nível de garantia (ou *Level of Assurance* (LoA)) de uma identidade é um conceito que reflete a precisão de que o portador de uma identidade é quem as informações contidas nela descrevem [Grassi et al. 2017]. É importante observar que os atributos biográficos de uma IdRC independem de LoA, pois são definidos pelos dados primários de cada cidadão. Tendo como base modelos de LoA internacionais, como os estabelecidos pelo governo dos EUA (NIST-SP 800-63-3) [Grassi et al. 2017] e pela União Europeia (eIDAS) [Council of European Union 2014], e casos de usos nacionais, como o sistema de identidade Gov.br [MGISP 2021], a IdRC propõe três níveis de garantia: baixo, substancial e alto. O LoA baixo implica baixa certeza de que o portador da IdRC é de fato seu dono (esse é o nível padrão das identidades). O LoA substancial carrega maior confiabilidade. Para que uma identidade tenha este nível, é necessário que a autenticação por biometria facial ou certificado ICP-Brasil tenha sido usado, pelo menos uma vez, nos últimos 12 meses. Por fim, o LoA alto significa que o cidadão compareceu presencialmente a uma serventia de registro civil de pessoas naturais, para a realização de coleta biométrica facial e definição de fatores de autenticação; esse nível de garantia confere, no sistema, o mais alto grau de certeza de que o portador da IdRC é quem os dados descreve.

O ciclo de vida da IdRC inicia no nascimento de uma pessoa. O registro de nascimento em uma serventia de registro civil de pessoas naturais implica na criação de uma IdRC para o recém-nascido. Todos os brasileiros nascidos antes da implantação da IdRC já tiveram suas identidades criadas no sistema. Ou seja, o primeiro acesso de um cidadão à sua IdRC, que só é permitido para usuários a partir de dezesseis anos, consiste em obter a posse de sua identidade. Tal processo pode acontecer nas dependências de uma serven-

tia de registro civil de pessoas naturais, o que implica no LoA alto da identidade, ou de maneira *online* pelo próprio usuário, o que limita o LoA para substancial.

O primeiro acesso *online* inicia com o indivíduo informando seu Cadastro de Pessoa Física (CPF), seguido pela resolução de um desafio para garantir que um ser humano está usando o sistema. Então é submetido à captura de biometria facial, o que exige que o processo esteja sendo feito em um dispositivo com câmera e que requisitos mínimos de qualidade de imagem e luminosidade ambiente sejam satisfeitos. Caso a biometria seja capturada e validada com sucesso, em todos os bancos biométricos governamentais disponíveis em que o cidadão tenha registro, a IdRC terá seu LoA elevado à substancial e o usuário poderá seguir para o registro dos fatores de autenticação. Em casos de falha da captura, o usuário poderá seguir o processo submetendo um documento oficial com foto. Como último recurso, se algum erro ocorrer durante a submissão, um questionário intergeracional será feito. Se a captura de documento ou o questionário forem concluídos com sucesso, o LoA será definido como baixo, e o indivíduo seguirá para o registro de fatores de autenticação. Esse registro inicia com a definição de uma senha. Nenhuma política de senha é imposta. Então é facultado ao usuário que: (i) registre número de telefone para envio de OTP; (ii) registre endereço de e-mail para envio de OTP; (iii) escaneie QR code para OTP offline; e (iv) registre um ou mais dispositivos para WebAuthN.

Durante o ciclo de vida da IdRC é possível que seu LoA seja elevado ou rebaixado. A mudança de LoA de uma identidade de baixo para substancial está associada ao uso de biometria facial ou certificado ICP-Brasil. Esta elevação pode acontecer automaticamente, caso um provedor de serviço solicite uma IdRC autenticada com dois fatores e o usuário opte pela biometria facial ou certificado ICP-Brasil. Estas opções são sempre apresentadas em conjunto com os fatores de autenticação que o usuário cadastrou no primeiro acesso ou *a posteriori*. A outra forma de elevação acontece quando um provedor de serviço exige LoA mínimo substancial e a IdRC do usuário realizando a autenticação é baixo. Neste caso somente serão apresentados os dois fatores associados com a elevação de LoA de baixo para substancial e o usuário deve, obrigatoriamente, concluir o processo de autenticação com um dos dois. A elevação de substancial para alto somente acontece mediante ao comparecimento presencial à uma serventia de registro civil de pessoas naturais, com a apresentação de documentos e coleta de biometria.

Um usuário pode, por outro lado, ter o LoA de sua identidade rebaixado de alto para substancial caso passe mais que 1 ano sem utilizar biometria facial. De forma semelhante, pode ser rebaixado de substancial para baixo se passar mais que 1 ano sem usar um fator de autenticação associado ao nível substancial. Em caso de óbito, detectado através da integração com a base de dados do Registro Civil do Brasil, o acesso à identidade eletrônica é automaticamente revogado e os *tokens* de acesso concedidos a provedores de serviço são invalidados.

Quando o proprietário da identidade é incapaz de usar sua senha para ter acesso à IdRC, é possível recorrer à recuperação de senha. Esse processo permite que usuários de categoria baixa e substancial possam redefinir suas credenciais de acesso, utilizando outros fatores de autenticação pré-cadastrados. Em caso de identidades com LoA alto ou que não tenham outros métodos de autenticação disponíveis, é necessário o comparecimento a uma serventia de registro civil de pessoas naturais para que seja realizado esse processo.

4. Integração com Provedores de Serviço

A IdRC permite que aplicações conectem-se ao sistema com a finalidade de identificar, autenticar e obter atributos de usuários. A integração entre IdRC e provedores de serviço, *i.e.*, clientes, acontece via os protocolos *OpenID Connect* [Sakimura et al. 2014] e *OAuth 2.0* [Hardt 2012]. Os clientes ligados à IdRC são adicionados ao sistema por um administrador e recebem uma *string* de identificação única e um *token* de acesso.

Aplicações podem requisitar à IdRC a identificação e autenticação de um usuário, especificando o LoA mínimo. É possível, ainda, que o cliente especifique qual segundo fator de autenticação deve ser utilizado. Por fim, atributos do usuário, como data, cidade e UF de nascimento, nome, telefone, e-mail, filiação (informação de pais e avós) e sexo podem ser solicitados. O usuário então autoriza ou não o compartilhamento dos mesmos.

5. Conclusão e Trabalhos Futuros

A Identificação do Registro Civil é um provedor de identidade e de atributos robusto, por ser vinculada diretamente à fonte de dados primária do cidadão brasileiro. A garantia de que o óbito implica na impossibilidade de utilizar a IdRC traz ganhos significativos para provedores de serviço, que não precisam se preocupar com prova de vida dos usuários. Além disso, ao exigir validação presencial para obtenção de LoA alto, a IdRC trás um nível de garantia superior a outros provedores, sem impor um fardo excessivo ao usuário, pois todos os municípios possuem uma serventia de registro civil de pessoas naturais.

Como trabalhos futuros espera-se a implementação de novos protocolos, como o *OpenID Connect for Identity Assurance* [Lodderstedt et al. 2022] e o *Financial-grade API Security Profile* [Sakimura et al. 2021]. Também estuda-se a possibilidade de emissão de credenciais verificáveis para usuários que desejam permanecer no paradigma de identidade auto-soberana [Schardong and Custódio 2022].

Referências

Brasil (1973). Lei nº 6.015, de 31 de dezembro de 1973. *Diário Oficial*.

Council of European Union (2014). Regulation no 910/2014 of the european parliament.

Grassi, P., Garcia, M., and Fenton, J. (2017). Digital identity guidelines. Technical Report SP 800-63-3, NIST, Gaithersburg, MD.

Hardt, D. (2012). The OAuth 2.0 Authorization Framework. RFC 6749.

Hodges, J., Jones, J., Jones, M. B., Kumar, A., and Lundberg, E. (2021). Web authentication: An api for accessing public key credentials level 2. *World Wide Web Consortium*.

Lodderstedt, T., Fett, D., Haine, M., Pulido, A., Lehmann, K., and Koiwai, K. (2022). Openid connect for identity assurance 1.0.

MGISP (2021). Conta gov.br. Disponível em `https://www.gov.br/governodigital/pt-br/conta-gov-br`. Acessado em 24/07/2023.

Sakimura, N., Bradley, J., and Jay, E. (2021). Financial-grade api security profile 1.0.

Sakimura, N., Bradley, J., Jones, M., De Medeiros, B., and Mortimore, C. (2014). Openid connect core 1.0. *The OpenID Foundation*.

Schardong, F. and Custódio, R. (2022). Self-sovereign identity: a systematic review, mapping and taxonomy. *Sensors*, 22(15):5641.