A Mobile Identity Management System to Enhance the Brazilian Electronic Government

G. M. Verzeletti, E. R. de Mello, and M. S. Wangham, *Member, IEEE*

***Abstract*—One of the strategies used by governments to enhance eGovernment Programs (eGov) is to define an Electronic Identity Management (IdM) system. Brazil has not yet defined a National Strategy for Identity Management. This work aims to propose a Mobile Identity Management (Mobile eID) System aligned with the Brazilian eGov Program, through a solution that prioritizes security, privacy and usability. As a proof of concept, a prototype was developed in software, which was evaluated through functional test cases and a user satisfaction survey. The results show that it is possible to guarantee the security, privacy and the usability of the Mobile eID through the use of FIDO UAF, TEE and SAML standards.**

***Index Terms*— Electronic Identity, Identity Management, Electronic Government, Mobile Identity**

I. Introdução

Os programas de Governo Eletrônico (e-Gov) tem como princípio a utilização de tecnologias de informação e comunicação (TIC) para democratizar o acesso a informação, ampliar discussões e dinamizar a prestação de serviços públicos com foco na eficiência e eficácia destes serviços [1].

Uma estratégia nacional de gestão de identidade (GId) pode ser definida como o conjunto de procedimentos, normas, leis e sistemas que são utilizados pelos governos para administrar as identidades eletrônicas (eIDs) dos cidadãos. Definir e implementar estratégias nacionais de GId, bem como escolher o formato da eID e definir um sistema de gestão para essas identidades são práticas que colaboram para a concretização do governo eletrônico em um país [2].

O governo brasileiro, até o momento da escrita deste trabalho (agosto de 2017), não definiu sua estratégia nacional de GId. O que existe é uma definição de padrões para interoperabilidade de governo eletrônico, conhecido como arquitetura e-PING, concebidos como estrutura básica para a estratégia de e-Gov no Brasil [3]. Porém, essa arquitetura apenas define um conjunto mínimo de premissas e especificações técnicas para regulamentar o uso das TIC nos serviços de e-Gov, não definindo uma estratégia em si.

Ao longo dos últimos anos, algumas iniciativas do governo surgiram com o propósito de definir uma estratégia nacional de gestão de eID [4]. Dentre estas, destacam-se o projeto para registro de identidade civil (RIC) do Ministério da Justiça [4] e o projeto do documento de identificação nacional (DIN) do Tribunal Superior Eleitoral. Se por um lado o RIC apresenta indícios de descontinuidade [5], por outro o DIN tende a se tornar uma realidade, principalmente após a aprovação do projeto de lei nº 19, em abril de 2017 [6].

O trabalho de Torres *et al.* [7], tem como base o projeto RIC e se propõe a definir uma estratégia nacional de gestão de identidade eletrônica para o governo brasileiro. A estratégia proposta segue o modelo centralizado de gestão de identidade e prevê o uso da eID combinado com diferentes fatores de autenticação, dependendo do nível de garantia de identidade (*Level of Assurance* - LoA) exigido pelo provedor de serviço (SP) a ser acessado pelo usuário. Entre as opções de fatores, para serviços que exigem menores níveis de garantia de identidade, tem-se a utilização do par usuário/senha e também as senhas descartáveis (*One-Time-Password* - OTP). Para serviços que exigem um maior nível de garantia, tem-se a identidade eletrônica móvel (eID Móvel) e o cartão eID. Contudo, esse trabalho apresenta apenas um modelo teórico e não descreve como a eID móvel pode ser implementada.

Enquanto o governo brasileiro busca formas de definir sua estratégia nacional de GId, muitos países estão passando a adotar soluções de eID baseadas em dispositivos móveis (eID Móvel). Grande parte dessa motivação se deve ao crescente uso dos dispositivos móveis e, principalmente, pela baixa aceitação das eIDs baseadas em cartão [8].

Este trabalho propõe um sistema de Gestão de eID Móvel Nacional alinhado à estratégia nacional de e-Gov brasileiro proposta em [7]. O sistema proposto tem como requisitos o uso de mecanismos robustos de autenticação, o cuidado para que a solução não gere custos elevados para o governo ou para o cidadão e que ao mesmo tempo seja simples de usar e implementar. Neste contexto, verificou-se que o padrão aberto e livre de *royalties* FIDO UAF [9], proposto pela FIDO Alliance (*Fast IDentity Online Alliance*), atende todos os requisitos citados. Para verificar a viabilidade da solução proposta, foi desenvolvido um protótipo em *software* chamado de mID-BR, que opera como um agente de usuário para dispositivos móveis, possibilitando criar e utilizar uma eID Móvel para interação com provedores de serviços.

O presente artigo está estruturado da seguinte maneira: na Seção II são introduzidos alguns conceitos sobre as tecnologias adotadas; a Seção III apresenta uma comparação dos trabalhos relacionados; o sistema proposto de Gestão de eID Móvel Nacional é descrito na Seção IV e o protótipo desenvolvido como prova de conceito é apresentado na Seção V; na Seção VI são descritos os resultados obtidos da avaliação do sistema proposto; e, por fim, a Seção VII apresenta a conclusão.

This work was submitted on 13 July 2017.

G. M. Verzeletti, is with the Instituto Federal de Santa Catarina (IFSC), Lages/SC Brazil, and was with the Universidade do Vale do Itajaí (UNIVALI), Itajaí/SC Brasil, (e-mail: glaidson.verzeletti@ifsc.edu.br).

E. R. de Mello, is with the Instituto Federal de Santa Catarina (IFSC), São José/SC Brazil, (e-mail: mello@ifsc.edu.br).

M. S. Wangham, is with the Universidade do Vale do Itajaí (UNIVALI), Itajaí/SC Brazil, (e-mail: wangham@univali.br).

II. Conceitos e Tecnologias Adotadas

Para melhor compreender o sistema proposto, essa seção introduz os conceitos de identidade eletrônica, dos sistemas de gestão de identidade, da identidade eletrônica móvel e do padrão FIDO UAF.

A. Identidade Eletrônica (eID)

A identidade de uma pessoa pode ser definida como sendo um conjunto de informações pessoais, utilizado a fim de caracterizar corretamente um indivíduo. Essas informações podem ser, por exemplo, o nome da pessoa e o registro biométrico. Para realizar essa caracterização, a identidade pode também estar associada a outros atributos ligados à pessoa como o nome da mãe, a data e o local de nascimento. Dependendo do contexto, a identidade pode ser composta somente por algumas destas informações pessoais [10].

A identidade eletrônica (eID) é criada quando informações pessoais são utilizadas para caracterizar uma pessoa no meio digital [11]. A eID pode então ser definida como um conjunto de dados pessoais utilizado para representar uma entidade ou pessoa dentro do contexto eletrônico [12].

Quando uma eID é usada em sistemas eletrônicos, é necessário fazer a gestão desta identidade, de forma que esta possa torna-se confiável. A gestão de identidades pode ser entendida como um conjunto de tecnologias, processos e políticas utilizados que visa garantir a qualidade das informações de uma identidade (identificadores, credenciais e atributos) de forma a possibilitar que essas identidades (e as informações associadas a estas) possam ser usadas por mecanismos de autenticação, autorização, contabilização e auditoria para garantir ao usuário o acesso a um determinado recurso [13]].

B. Sistemas de Gestão de Identidade (SGId)

Um sistema de gestão de identidades consiste na integração de tecnologias, políticas e processos de negócio, resultando em um sistema de autenticação de usuários aliado a um sistema de gestão de atributos [12]. Para compor um sistema de gestão de identidade, é necessário que existam três atores: o usuário, o provedor de identidade (IdP) e o provedor de serviço (SP) [14]. O usuário é a entidade que utiliza uma eID para acessar algum recurso eletrônico disponibilizado em um SP; o IdP é o responsável por gerenciar as eIDs de seus usuários e autenticá-los; e o SP oferece recursos aos usuários, que exige destes uma autenticação para conceder acesso aos recursos requeridos. A forma que um usuário, um IdP e um SP interagem pode caracterizar quatro diferentes modelos de SGId: tradicional, centralizado, federado e centrado no usuário [15].

Ao implantar as estratégias nacionais de GId, os países geralmente seguem uma estratégia baseada em um cartão eletrônico (cartão eID). O cartão eID é dotado de um *smartcard*, em geral de multi-aplicação, que permite, dentro outros possíveis serviços, o armazenamento de atributos para fins de identificação e a execução de protocolos de autenticação presencial ou remota, com provedores de serviços. Normalmente, grande parte das informações impressas no cartão são exatamente as mesmas gravadas no *chip*, o que permite seu uso tanto para identificação presencial quanto eletrônica [16].

C. Identidade Eletrônica Móvel (eID Móvel)

A identidade eletrônica móvel se refere ao uso da eID através de dispositivos móveis, como *smartphones* e *tablets*. As soluções de eID Móvel têm como potencial aumentar o fator usabilidade, sem perder o nível de segurança oferecido pelas soluções baseadas no cartão eID [17].

Nos sistemas de eID Móvel existentes, o modelo de confiança advém do uso de um módulo de *hardware* seguro (*Hardware Security Module* - HSM), instalado no servidor de autenticação, ou do uso de algum elemento seguro (*Secure Element* - SE) presente no dispositivo móvel [17].

Entre os tipos de implementações mais comuns de SE, tem-se: *chipset* SE embarcado diretamente na placa mãe do dispositivo; cartão SIM (*subscriber identity module*) especial para eID; ou TEE (*trusted execution environment*), ambiente de *hardware* isolado onde são armazenados e executados de forma segura aplicativos. O TEE oferece uma flexibilidade maior que o SE, com maior poder de processamento e armazenamento, e oferece um nível semelhante de segurança.

D. Padrão FIDO UAF

O *framework* FIDO UAF [9] foi criado pela *FIDO Alliance* [18] com o objetivo de ser um padrão aberto e livre de *royalties* para permitir autenticação robusta de usuário baseada em criptografia de chave pública [18]. Com o FIDO UAF é possível transpor a autenticação local do usuário em seu dispositivo para serviços online. Logo, o usuário pode ser autenticado por meio de biometria, como impressão digital, reconhecimento de voz e facial, cabendo ao SP confiar que o dispositivo do usuário fez o processo de autenticação corretamente.

Como a confiança entre dispositivos do usuário e SP é intermediada pela *FIDO Alliance*, todo dispositivo usado nesse processo de autenticação precisa ser certificado por ela durante o processo de fabricação. Esse processo envolve alguns requisitos de projeto de *hardware* e *software*, como por exemplo, o armazenamento no TEE da pilha FIDO UAF e dos *softwares* e *hardwares* usados para a autenticação biométrica, embarcados em tempo de manufatura do dispositivo.

As informações sobre todos os dispositivos certificados são fornecidas por um serviço de metadados mantidos pela *FIDO Alliance*. Assim, um SP pode contatar esse serviço de metadados e verificar se o dispositivo que realizou a autenticação de um determinado usuário é um dispositivo certificado e confiável. Características como essas, quando associadas à computação móvel, possibilitam ao padrão FIDO UAF melhorar a usabilidade e minimizar os riscos associados a ataques de espionagens e roubo de informações [19].

III. Trabalhos Relacionados

A seleção dos trabalhos relacionados foi feita após uma revisão sistemática da literatura (RSL), que teve como objetivo identificar as publicações relacionadas ao uso da eID Móvel, dentro e fora do contexto de e-Gov. Os critérios de

inclusão e exclusão de artigos relacionados, bem como a *string* de busca e a análise dos trabalhos, foram publicados em [20].

A Tabela I compara esses trabalhos. A segunda coluna destaca o cenário de aplicação da solução de eID Móvel, indicando se é uma implementação feita pelo governo de algum país ou apenas uma solução teórica proposta pelo autor. Logo na coluna seguinte o nome da respectiva solução é descrito.

TABELA I
TRABALHOS RELACIONADOS

Artigo	Cenário	Nome	SE	3G/4G	PPP
[25]	Estônia	Mobiil-ID	SIM Card	Sim	Sim
[27]	Solução Teórica	Op. Mob. IDM Framework	SIM Card	Sim	Sim
[21]	Solução Teórica	Mobile-ID Protocol	SIM Card TEE	Sim	Sim
[28]	Solução Teórica	Mobile Authentication	eID Card	Não	-
[22]	Azerbaijão	Asan İmza	SIM Card	Sim	Sim
[26]	Islândia	Skilriki Service	SIM Card	Sim	Sim
[24]	Áustria	Mobile Phone Signature	HSM	Não	-
	Noruega	Bank-ID	SIM Card	Sim	Sim
	Lituânia	Lithuanian El. Elet. Signature	SIM Card	Sim	Sim
	Turquia	Mobile Imza	SIM Card	Sim	Sim
	Moldova	Mobile e-ID	SIM Card	Sim	Sim
	Suíça	Swiss Mobile ID	SIM Card	Sim	Sim
[23]	Finlândia	Mobiilivar-menne	USIM Card	Sim	Sim
-	Brasil	mID-BR	TEE	Não	Não

De acordo com as informações referentes ao SE, apenas um trabalho sugeriu o TEE para reforço da segurança [21]. A maioria dos trabalhos adota o cartão SIM como elemento seguro para a eID. Entretanto, as soluções de eID Móvel que se baseiam no cartão SIM, fazem com que cidadão e governo dependam das operadoras de telefonia móvel [22]. Como toda infraestrutura de segurança e autenticação é provida pelas operadoras de telefonia móvel, essa característica exige que o cidadão possua um plano de dados móveis (p.ex. 3G, 4G, etc) [23].

Apesar da maioria das soluções de eID Móvel apresentadas estabelecerem parcerias entre o governo e a iniciativa privada (Parceria Público-Privada - PPP), não foi apresentado nos trabalhos o grau de envolvimento entre eles [24]. Ou seja, não foi possível identificar até que ponto o governo dita as regras de negócios e determina quais padrões tecnológicos devem ser seguidos. No entanto, observa-se que nas soluções com PPP é exigido do cidadão a troca do seu cartão SIM por outro com capacidade criptográfica [25], como foi o caso da Islândia [26]. Como todos os cartões SIM PKI (*Public Key Infrastructure*) oferecidos por essas operadoras possuem alguma tecnologia proprietária embarcada, o custo para a aquisição destes cartões se torna maior para o usuário final.

Em [27], embora os autores também proponham o uso de um cartão SIM, estes abordam a autenticação multi-fatores, sendo que o uso biométrico é citado como increment incremento da segurança. Já [28], propõem o uso de dispositivos móveis equipados com um leitor NFC (*Near Field Communication*) para ler um cartão de eID. No entanto, esses dois trabalhos descrevem apenas modelos teóricos e não apresentam resultados práticos de implementação das soluções propostas.

O mID-BR, proposto neste trabalho, se diferencia das soluções apresentadas, pois não obriga o cidadão a possuir um plano de dados com operadoras de telefonia celular. Propõe a utilização apenas do TEE, já disponível em muitos telefones inteligentes, sem uso do cartão SIM, para oferecer um ambiente de processamento seguro e com proteção de integridade para as informações sensíveis. Faz uso de criptografia de chave pública, conforme definido no protocolo FIDO UAF.

IV. SISTEMA DE GESTÃO DE EID MÓVEL NACIONAL

Esta seção descreve o Sistema de Gestão de eID Móvel proposto para o programa de Governo Eletrônico Brasileiro, que está alinhado aos padrões de interoperabilidade definidos pela arquitetura e-PING e baseado na estratégia nacional Gestão de Identidade (GId) proposta por Torres em [7]

Para garantir a aderência aos padrões recomendados para o programa de e-Gov brasileiro, o sistema proposto adota os seguintes padrões de interoperabilidade definidos no e-PING: TLS (*Transport Layer Security*), para a transferência segura de dados em rede; AES (*Advanced Encryption Standard*), para cifragem simétrica; X.509, para os certificados digitais; SAML (*Security Assertion Markup Language*), para a troca de informações sobre autenticação e autorização; XML (*EXtensible Markup Language*) e JSON (*JavaScript Object Notation*) como padrões para o intercâmbio de dados.

Dentre as características da solução de eID Móvel proposta, destacam-se:

- o uso de um IdP centralizado, conforme definida na estratégia nacional de GId proposta em [7];
- a premissa de que os dispositivos móveis dos usuários foram fabricados com a pilha FIDO UAF e possuem um SE ou TEE;
- o servidor FIDO UAF pode ser configurado para aceitar somente um grupo específico de fabricantes de *hardware*, evitando o uso de dispositivos móveis considerados inseguros pelo governo brasileiro;
- a impressão digital do cidadão é utilizada como fator biométrico para proteger a chave privada gerada no próprio dispositivo móvel;
- o "nome de usuário", cadastrado no IdP, deverá passar por um processo de criptografia antes de ser entregue ao SP, gerando um pseudônimo único por SP; e,
- os certificados digitais utilizados foram emitidos por uma autoridade certificadora (AC) confiável. Assume-se que a AC confiável é a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) [29].

Ao combinar o padrão FIDO UAF com tecnologias presentes no próprio dispositivo móvel do usuário, como o TEE, o sistema proposto visa aumentar a segurança da geração

e do armazenamento das chaves criptográficas utilizadas no protocolo de autenticação. Como o suporte computacional utilizado no sistema é um dispositivo móvel, a capacidade de processamento para as informações sensíveis é maior quando comparada aos elementos seguros tradicionais (cartão SIM).

Com relação aos custos da solução proposta, o usuário terá como gasto a aquisição do próprio dispositivo móvel, algo que também ocorre com todas as demais soluções de eID Móvel. Para o governo, por outro lado, aderir às especificações abertas permite implementar SPs governamentais de baixo custo.

A Fig. 1 apresenta a visão geral do mID-BR e ilustra a integração entre o sistema proposto e a estratégia de GId proposta em [7]. De forma geral, tem-se as seguintes entidades no sistema proposto: o aplicativo mID-BR, o IdP, responsável por identificar o cidadão no meio eletrônico e os SPs, que representam os serviços de governo acessados pelo cidadão e que exigem deste a autenticação, antes de conceder a autorização de acesso. O aplicativo mID-BR, instalado no dispositivo móvel, é constituído de um cliente ativo que interage diretamente com o cliente FIDO disponibilizado pelo fabricante do dispositivo, sendo também responsável pela interação com o usuário, com o IdP e com o SP nas trocas de asserções SAML.

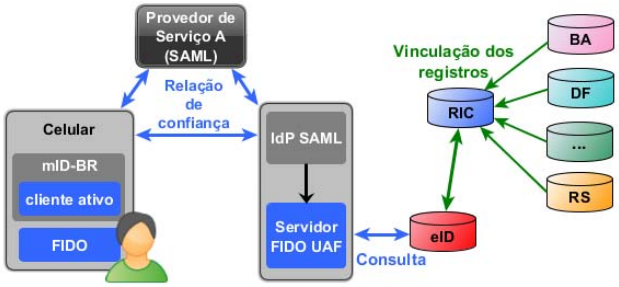

Fig 1. Visão Geral - Sistema de Gestão de eID Móvel

Como representado na Fig. 1, o cidadão, de posse de seu dispositivo móvel certificado pela *FIDO Alliance*, interage com o SP governamental (Provedor de Serviço A) e com o IdP SAML, por meio do aplicativo mID-BR. Como as informações do cidadão estão armazenadas na base de dados RIC e são consultadas pela base eID, para autenticar o usuário e emitir a asserção de atributos do cidadão, o IdP interage diretamente com a base eID para buscar os atributos pessoais do cidadão.

Em complemento ao que foi proposto pela estratégia nacional de GId [7], o IdP implementa o servidor FIDO UAF, mas continua consultando a base de identidades (eID) e a base de atributos do cidadão (RIC) conforme foi definido. No entanto, embora exista uma relação de confiança entre as entidades (ver Fig. 1), os atributos do cidadão só serão encaminhados do IdP ao SP governamental, após a confirmação do usuário por meio de uma tela de consentimento. Essa abordagem caracteriza um modelo de SGId centralizado e centrado no usuário, uma vez que toda interação com um SP inicia obrigatoriamente pela identificação do cidadão junto ao IdP e requer autorização deste para liberar os atributos pessoais.

O sistema proposto contempla quatro etapas: (1) cadastro da eID Móvel na entidade pública responsável pelo registro; (2) registro da eID Móvel nos SPs de e-Gov, para assinar documentos eletrônicos; (3) utilização da eID Móvel para acessar um serviço de e-Gov; e, (4) revogação da eID Móvel.

Na etapa de cadastro da eID Móvel, ilustrada na Fig. 2, o cidadão deve comparecer pessoalmente em uma entidade pública de registro, de posse do seu dispositivo móvel preparado para FIDO e apresentar ao atendente um documento de identificação civil. Ao confirmar a identidade do cidadão, o atendente realiza o cadastro da eID Móvel, processo esse que exige do usuário a instalação do *software* mID-BR e a geração de um novo par de chaves criptográficas assimétricas. O atendente gera um "nome de usuário"', que pode ser um pseudônimo escolhido pelo cidadão, e o associa à chave pública recém gerada no dispositivo móvel do cidadão. Essa associação corresponde à eID Móvel do cidadão, a qual é ligada à base de dados de atributos do governo (base RIC da Fig. 1). Segundo a especificação FIDO, a chave privada permanece gravada apenas no dispositivo móvel do cidadão.

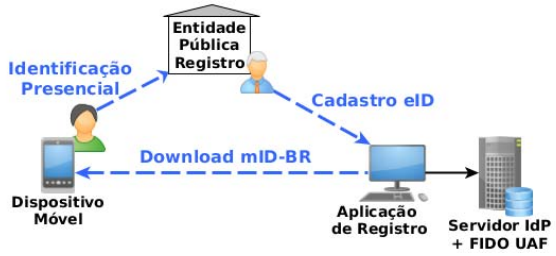

Fig 2. Etapa de Cadastro da eID Móvel

A etapa de registro da eID Móvel nos SPs é prevista para provedores que possuem a funcionalidade de assinatura eletrônica de documentos. Nesse processo, um novo par de chaves criptográficas é gerado no dispositivo móvel do cidadão, logo após o primeiro acesso deste ao serviço. A chave pública é armazenada no SP para confirmar a assinatura de documentos feita pela chave privada correspondente.

Na etapa de utilização da eID Móvel, é previsto que todo acesso a um SP governamental deve, obrigatoriamente, passar pela identificação do cidadão junto ao IdP. No processo de identificação do cidadão junto ao IdP, o mID-BR solicita apenas a impressão digital do cidadão. Após a autenticação, o IdP apresenta ao cidadão a lista de atributos pessoais solicitada pelo SP, por meio de uma tela de consentimento. Somente após concordar com o envio dos atributos, é que o IdP gera a asserção SAML de resposta ao SP.

Por fim, a etapa de revogação da eID Móvel prevê a exclusão da chave pública registrada no IdP e no SP. Após a exclusão da chave, o cidadão não poderá mais se autenticar no IdP e não poderá mais assinar documentos de forma eletrônica. A revogação poderá ocorrer a partir do próprio mID-BR, ou presencialmente, em uma entidade pública de registro. Entretanto, o novo cadastro da eID Móvel exige o comparecimento presencial do cidadão, como descrito na etapa de cadastro.

A. Cenário de Uso

Atualmente, o sistema de votação no Brasil exige que o cidadão compareça presencialmente na zona eleitoral em que ele esteja vinculado, para exercer seu direito ao voto. Para exemplificar o uso da eID Móvel no Brasil, a Fig. 3 apresenta uma situação hipotética de votação eletrônica.

Nesse cenário, o cidadão realiza a votação para presidente, governador ou prefeito, a partir de seu próprio dispositivo móvel pessoal, sem a necessidade de comparecer na zona eleitoral. Para tanto, no dia da votação o cidadão apenas acessará o SP do TSE (Tribunal Superior Eleitoral) para computar seu voto, se identificando com uso da sua eID Móvel e realizando a votação.

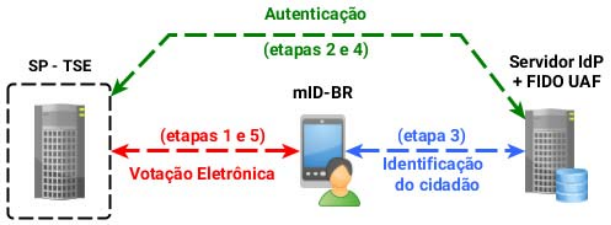

Fig 3. Cenário de Uso - Votação online

Esse processo de votação é feito da seguinte forma:

- **Etapa 1:** O usuário acessa o mID-BR, escolhe o SP do TSE e a opção para registrar seu voto;
- **Etapa 2:** O SP redireciona o usuário ao IdP, para se autenticar (asserção SAML de requisição);
- **Etapa 3:** O usuário se autentica no IdP via mID-BR (identificação do cidadão);
- **Etapa 4:** O IdP informa ao SP que o usuário se autenticou com sucesso (asserção SAML de resposta); e,
- **Etapa 5:** O SP libera o sistema de votação para o usuário registrar seu voto.

Após a votação, o SP se encarregará de disponibilizar publicamente a situação de quitação eleitoral do cidadão.

V. Protótipo Desenvolvido

Com o objetivo de avaliar a funcionalidade, usabilidade e desempenho da solução proposta, foi construído um protótipo em *software*, constituído de um agente de usuário para telefone móvel (mID-BR) e de um módulo de autenticação para o IdP.

A escolha das ferramentas e tecnologias foi baseada, primeiramente, no uso de *software* livre, uma vez que é de entendimento do governo federal que seu uso é uma opção estratégica para reduzir custos e desenvolver o conhecimento no país. Atender as recomendações da arquitetura e-PING foi a segunda preocupação, como forma de buscar a aderência aos padrões de sistemas já em funcionamento no Brasil.

Com relação à hospedagem dos serviços (IdP e SP), foi utilizado o laboratório de experimentação em gestão de identidade da RNP (Rede Nacional de Pesquisa), o GidLab [30].

A. Aplicativo mID-BR

O aplicativo mID-BR (agente do usuário) foi desenvolviddesenvolvido para Android e nos experimentos foi utilizado o celular modelo Nexus 5X da LG, lançado em 2015. Este dispositivo foi escolhido por possuir a versão mais recente do sistema operacional Android no momento, possuir um leitor de impressão digital e estar equipado com a tecnologia TEE.

No entanto, como o Nexus 5X não possui a pilha FIDO UAF embarcada durante a fase de manufatura do telefone, foi necessário fazer uso do aplicativo *Dummy FIDO UAF Client* [31] que implementa o protocolo FIDO UAF, porém não é um aplicativo certificado pela *FIDO Alliance*. Sendo assim, o *Dummy FIDO UAF Client* é adequado para o desenvolvimento do protótipo, uma vez que implementa o padrão FIDO UAF corretamente, porém não seria adequado para um cenário de produção, pois fere o modelo de confiança concebido pela *FIDO Alliance*[1].

A implementação do mID-BR foi feita em duas camadas:

- **1ª camada - cliente ativo:** realiza a comunicação entre SP e IdP, sendo responsável pelo encaminhamento das asserções SAML (requisição e resposta), pela apresentação das mensagens informativas e pela interação com o usuário; e,
- **2ª camada - interface FIDO:** interage com o cliente FIDO do celular, possibilitando o cadastro do usuário através da geração de um par de chaves criptográficas assimétricas. Participa ativamente do processo de autenticação, solicitando e recebendo do cliente FIDO as informações sobre as interações realizadas com o servidor FIDO UAF.

B. Provedor de Identidade - IdP

Para autenticar usuários do sistema de eID Móvel, foi desenvolvido um módulo de autenticação para o *simpleSAMLphp* denominado "authFidoUAF", implementado com base na especificação SAML e definido por meio de uma *Authentication Context Declaration* em XML. Esse módulo possibilitou validar o *token* de autenticação recebido do servidor FIDO UAF, por meio do cliente ativo (mID-BR). Dentre os mecanismos de proteção previstos, encontram-se os seguintes:

- O *token* é invalidado após um tempo pré-definido, contado a partir da sua geração;
- O conteúdo do *token* recebido pelo cliente ativo é invalidado, caso seja diferente do último *token* gerado pelo servidor FIDO UAF para aquele usuário;
- O *token* é invalidado pelo IdP imediatamente após a sua utilização; e,
- Só são aceitos *tokens* gerados a partir da utilização da impressão digital do usuário, muito embora o módulo "authFidoUAF" possa ser reconfigurado para aceitar outro fator de autenticação ou até um conjunto deles.

VI. Resultados

A fase de avaliação do sistema de eID Móvel Nacional proposto foi realizada em duas etapas: na primeira etapa foram

[1] https://fidoalliance.org/mds

executados casos de teste funcionais pelo próprio desenvolvedor e por um testador (aluno de graduação); e, na segunda etapa foi realizada a avaliação de um experimento através de uma pesquisa de satisfação, aplicada à profissionais de tecnologia da informação.

Para a avaliação das funcionalidades do protótipo, casos de testes foram definidos e executados. Além disso, alguns casos de testes avaliaram a segurança da solução. O celular Nexus 5X foi configurado com um perfil de usuário para instalação dos *softwares* e com acesso a Internet através da rede sem fio. Ao todo foram executados sete (7) casos de teste com sucesso, que incluíram desde o cadastro da eID Móvel (ilustrado pelas 3 etapas da Fig. 4), até sua utilização e revogação.

Fig 4. Cadastro da eID Móvel no Aplicativo mID-BR

A execução dos testes de segurança comprovaram que todas as mensagens trocadas entre o mID-BR, o IdP e o SP estavam criptografadas, conforme captura de dados ilustrada na Fig. 5.

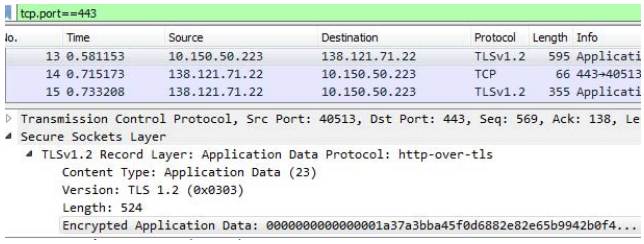

Fig 5. Dados de aplicativo, capturados com o *software wireshark*

Após a avaliação dos casos de teste, foi realizada a segunda etapa de avaliação durante um período de dez dias. Nesse período, foram disponibilizados um roteiro de testes e uma pesquisa de satisfação, que foi respondida por vinte e seis profissionais de TIC. A aplicação dos questionários serviu para avaliar o nível de satisfação dos avaliadores no que tange a utilização do aplicativo mID-BR ao acessar um serviço governamental fictício.

Os resultados obtidos apontam que 96,2% dos avaliadores se sentiram confortáveis durante a realização do experimento (uso do protótipo). Para 69,3% dos avaliadores, realizar presencialmente o cadastro da eID Móvel em uma entidade pública é considerado um fator importante para aumentar a segurança do sistema proposto. Na opinião de 76,9% dos avaliadores, manter armazenada a impressão digital no próprio dispositivo móvel, colabora com a privacidade do usuário. Cerca de 46,2% dos avaliadores preferem combinar mais de um fator para se autenticar em sistemas de e-Gov, porém, outros 46,2% preferem utilizar somente um fator biométrico. Para 84,6% dos avaliadores, a solução de eID Móvel melhora a interação do cidadão com o governo e auxilia na redução da burocracia no país. Cerca de 88,5%, considera que este sistema de eID Móvel proposto contribui mais com a privacidade do usuário do que os sistemas de e-Gov que eles utilizam atualmente.

Os resultados obtidos nos experimentos mostraram que é possível garantir privacidade do cidadão, por meio do sistema de Gestão de eID Móvel proposto. Contudo, observou-se nos experimentos que a usabilidade pode ser afetada quando mensagens de alerta não são compreendidas pelo usuário.

VII. Conclusão

Ao longo dos anos, alguns países tem desenvolvido suas estratégias de GId com base em cartões de identidade civil com *chip* (cartão de eID). Porém, conforme observado em [8] e [32], esses países têm se deparado com a baixa utilização desses cartões nas interações entre cidadãos e serviços de e-Gov. Por outro lado, como as soluções de eID Móvel se apoiam no aumento crescente dos serviços de telefonia móvel e na facilidade de uso, estas tem uma maior aceitação do que as soluções baseadas em cartões.

Pela simplicidade de implementação da eID Móvel e por oferecer proteção contra violação física [33], soluções com cartões SIM têm sido largamente adotadas [24]. Contudo, implementar a eID Móvel utilizando esses cartões tem altos custos para aquisição [24], ao mesmo tempo que gera custos extras com a contratação de um plano de dados móveis [23], visto que o cidadão é identificado via redes de telefonia móvel [33]. Essa dependência, entre governo e operadoras [22], também cria problemas para os SPs governamentais, como a falta de confiança na infraestrutura de autenticação das operadoras de telefonia móvel [25].

Diante desse cenário, com o objetivo de encontrar uma forma de implementar a eID Móvel no Brasil, que contornasse os problemas enfrentados pelas soluções adotadas por outros países, esse artigo apresentou uma proposta de um sistema de gestão de eID Móvel nacional e, como prova de conceito, um protótipo do sistema foi desenvolvido e avaliado. Os resultados obtidos nos experimentos realizados mostram que é possível garantir a segurança e a usabilidade da eID Móvel, por meio dos padrões FIDO UAF, TEE e SAML.

Como trabalho futuro, sugere-se investigar outros protocolos de autenticação seguros e de padrões abertos, comparando esses protocolos com a solução apresentada nesse trabalho que faz uso dos padrões FIDO UAF. Sugere-se ainda investigar as soluções comerciais de eID Móvel, comparando-as com as soluções de padrões abertos, bem como promover testes direcionados de segurança de forma a encontrar possíveis vulnerabilidades dessas soluções.

Referências

[1] ONU, “e-Government Survey,” Economy & Social Affairs, 2014

[2] OECD, *National Strategies and Policies for Digital Identity Management in OECD Countries*. OECD Publishing, 2011.
[3] GOV.BR, "Portaria SLTI/MP nº 92, de 24 de dezembro de 2014." [Online]. Available: http://eping.governoeletronico.gov.br/
[4] J. A. S. Torres, F. Deus, and R. Junior, "Diagnóstico do governo eletrônico brasileiro – uma análise com base no modelo de gerenciamento de identidades e no novo guia de serviços," *XIV SBSEG*, pp. 490–499, 2014.
[5] MJ, "Projeto RIC," 2017. [Online]. Available: http://justica.gov.br/Acesso/governanca/ric
[6] GOV.BR, "Projeto de Lei da Câmara no. 19, de 2017". [Online]. Available: https://www25.senado.leg.br/web/atividade/materias/-/materia/128224
[7] J. A. S. Torres, G. M. Verzeletti, R. Távora, R. T. Sousa, E. R. Mello, and M. S. Wangham, "National strategy of identity management to boost Brazilian electronic government program," in *Computing Conference (CLEI), XLII Latin American*. Valparaíso/Chile: IEEE, 2016, pp. 1–12.
[8] A. Ruiz-Martínez, D. Sanchez-Martínez, M. Martínez-Montesinos, and A. F. Gómez-Skarmeta, "A Survey of Electronic Signature Solutions in Mobile Devices," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 2, no. 3, p. 94, 2007.
[9] S. Srinivas, J. Kemp, and F. Alliance, "FIDO UAF Architectural Overview," 2014.
[10] NSTC, "Identity Management Task Force Report," *Subcomiittee on Biometrics and Identity Management,* 2008. [Online]. Available: https://goo.gl/6tWnVP
[11] S. Clauß and M. Köhntopp, "Identity Management and its Support of Multilateral Security," *Computer Networks*, vol. 37, no. 2, pp. 205–219, 2001. [Online]. Available: https://goo.gl/VLHvcz
[12] M. S. Wangham, E. R. de Mello, D. da Silva Böger, M. Guerios, and J. da Silva Fraga, "Minicursos x simpósio brasileiro de segurança da informação e de sistemas computacionais," *Minicurso-SBSeg 2010-Fortaleza-CE*, pp. 1–52, 2010. [Online]. Available: http://ceseg.inf.ufpr.br/anais/2010/minicursos.html
[13] T. ITU, "Series Y," *Rec. ITU-T Y*, vol. 2720, 2009.
[14] A. Bhargav-Spantzel, J. Camenisch, T. Gross, and D. Sommer, "User centricity," *Journal of Computer Security*, vol. 15, no. 5, pp. 493–527, 2007. [Online]. Available: http://dx.doi.org/10.3233/JCS-2007-15502
[15] A. Jøsang and S. Pope, "User Centric Identity Management," in *Aus-CERT Asia Pacific Information Technology Security Conference.* Citeseer, 2005, p. 77.
[16] I. Naumann and G. Hogben, "Privacy Features of European eID Card Specifications," *Network Security*, vol. 2008, no. 8, pp. 9–13, 2008. [Online]. Available: http://dx.doi.org/10.1016/S1353-4858(08)70097-7
[17] C. Rath, S. Roth, M. Schallar, and T. Zefferer, "A Secure and Flexible Server-Based Mobile eID and e-Signature Solution," in *The Eighth International Conference on Digital Society*, 2014, pp. 7–12.
[18] FIDO Alliance, "About the FIDO Alliance," 2016. [Online]. Available: https://fidoalliance.org/about/overview/
[19] T. Thiemann, "Picking the right path to mobile biometric authentication," *Biometric Technology Today*, vol. 2016, no. 2, pp. 5–8, 2016. [Online]. Available: http://dx.doi.org/10.1016/S0969-4765(16)30034-0
[20] G. M. Verzeletti, E. R. de Mello, V. H. B. de Oliveira, and M. S. Wangham, "Estudo Comparativo das Soluções de eID Móvel para Governo Eletrônico," in *XVI Simposio Brasileiro em Segurança da Informação e de Sistemas Computacionais.* SBSeg, 2016. [Online]. Available: http://sbseg2016.ic.uff.br/pt/files/anais.pdf
[21] K. Bicakci, D. Unal, N. Ascioglu, and O. Adalier, "Mobile Authentication Secure against Man-in-the-Middle Attacks," in *Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2014 2nd IEEE International Conference on*, pp. 273–276, http://dx.doi.org/10.1109/MobileCloud.2014.43
[22] J. Krimpe, "Mobile ID: Crucial element of m-Government," in *Proceedings of the 2014 Conference on Electronic Governance and Open Society: Challenges in Eurasia*. ACM, 2014, pp. 187–194. [Online]. Available: http://dx.doi.org/10.1145/2729104.2729133
[23] E. Kerttula, "A novel federated strong mobile signature service – the Finnish case," Journal of Network and Computer Applications, vol. 56, pp. 101–114, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2015.06.007
[24] T. Zefferer and P. Teufl, "Leveraging the Adoption of Mobile eID and e-Signature Solutions in Europe," in *Electronic Government and the Information Systems Perspective*. Springer, 2015, pp. 86–100. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-22389-6_7
[25] T. Martens, "Electronic identity management in Estonia between market and state governance," *Identity in the Information Society*, vol. 3, no. 1, pp. 213–233, 2010. [Online]. Available: http://dx.doi.org/10.1007/s12394-010-0044-0
[26] J. Prusa, "E-identity: Basic building block of e-Government," in *IST-Africa Conference*. IEEE, 2015, pp. 1–10. [Online]. Available: http://dx.doi.org/10.1109/ISTAFRICA.2015.7190586
[27] B. En-Nasry and M. D. E.-C. El Kettani, "Towards an Open Framework for Mobile Digital Identity Management through Strong Authentication Methods," in *FTRA International Conference on Secure and Trust Computing, Data Management, and Application*. Springer, 2011, pp. 56–63. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-22365-5_8
[28] X. Wu, Y. Fan, X. Zhang, and J. Xu, "Research of eID Mobile Identity Authentication Method," in *International Conference on Trustworthy Computing and Services*. Springer, 2014, pp. 350–358. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-47401-3_46
[29] I. Brasil, "Infraestrutura de Chaves Públicas Brasileira," 2016. [Online]. Available: http://www.iti.gov.br/icp-brasil
[30] M. C. de Souza, E. R. de Mello, and M. S. Wangham, "Gidlab: Laboratório de Experimentação em Gestão de Identidade," 2014. [Online]. Available: https://gidlab.rnp.br
[31] E. R. De Mello, "A dummy FIDO UAF Client suitable to conduct development tests on Android smartphones that are not FIDO Ready," Mar. 2017. [Online]. Available: https://doi.org/10.5281/zenodo.375567
[32] R. G. F. Tavora, J. A. S. Torres, and D. F. R. Fustinoni, "Proposta de um modelo de documento de identidade robusto a fraudes e de baixo custo," in *V WGID - Workshop de Gestão de Identidades – XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. SBSeg, 2015. [Online]. Available: http://sbseg2015.univali.br/anais/WGID/artigoWGID02.pdf
[33] T. van Do, T. Jonvik, I. Jorstad, and T. Van Do, "Better User Protection with Mobile Identity," in *IT Convergence and Security (ICITCS), 2013 International Conference on*. IEEE, 2013, pp. 1–4. [Online]. Available: http://dx.doi.org/10.1109/ICITCS.2013.6717809

Glaidson Menegazzo Verzeletti é Técnico em Eletrônica pela Universidade Tecnológica Federal do Paraná (1999), graduado em Gestão de Tecnologia da Informação pela Universidade do Sul de Santa Catarina (2006), especialista em Rede de Computadores CCNA pela Faculdade Campo Real (2009) e mestre em Computação Aplicada pela Universidade do Vale do Itajaí (2017). Desde 2011 é Analista de Tecnologia da Informação no Instituto Federal de Santa Catarina – IFSC, campus Lages, local em que atuou como coordenador (2012-2015). Tem experiência na área de ciências da computação, com principal ênfase em sistemas distribuídos, rede de computadores e segurança da informação.

Emerson Ribeiro de Mello é Bacharel em Ciências da Computação pela Universidade do Oeste Paulista (2000), mestre (2003) e doutor (2009) em Engenharia Elétrica pela Universidade Federal de Santa Catarina. Foi Diretor de Tecnologia da Informação e Comunicação no Instituto Federal de Santa Catarina - IFSC (2012-2015). Desde 2007 é professor do núcleo de Telecomunicações no IFSC, campus São José. Tem experiência na área de ciências da computação, com ênfase em sistemas distribuídos e, atualmente, desenvolve pesquisa na área de gestão de identidade e sua aplicação na IoT.

Michelle Wangham possui graduação em Engenharia Elétrica pela Universidade Federal do Pará (1998), mestrado e doutorado em Engenharia Elétrica pela Universidade Federal de Santa Catarina (2000, 2004). Em 2016, fez estágio sênior na University of Ottawa, no Canadá. Atualmente, é professora pesquisadora na Universidade do Vale do Itajaí (UNIVALI), no Programa de Mestrado em Computação Aplicada e no curso de Ciência da Computação. Participa como pesquisadora do Grupo de Sistemas Embarcados e Distribuídos (GSED) da UNIVALI. É coordenadora do Comitê Técnico de Gestão de Identidades da RNP e do Laboratório para Experimentação em Gestão de Identidade (GIdLab) financiado pela RNP. Seus principais interesses de pesquisa são em Gestão de Identidades, Segurança na Internet das Coisas e Segurança em Redes Veiculares.