Estudo Comparativo das Soluções de eID Móvel para Governo Eletrônico

Glaidson Menegazzo Verzeletti[1,2], Emerson Ribeiro de Mello[2]*, Victor Hugo Barbosa de Oliveira[3], Michelle Silva Wangham[1]

[1]Universidade do Vale do Itajaí (UNIVALI) – SC – Brasil

[2]Instituto Federal de Santa Catarina – SC – Brasil

[3]Universidade de Brasília – DF – Brasil

{glaidson.verzeletti, mello}@ifsc.edu.br,

hugo.victoor77@gmail.com, wangham@univali.br

Abstract. *The Mobile Electronic Identity (Mobile eID) is an important tool to connect citizens and governments securely. Thus, this tool improves citizens' access to electronic government services, as well as to allow a greater interaction of people with public policies and decisions. This article aims to describe and analyze eID solutions described in the literature which have been selected after a systematic review.*

Resumo. *A Identidade Eletrônica Móvel (eID Móvel) é uma importante solução para conectar cidadãos e governos de forma segura. Dessa forma, esta solução melhora o acesso dos cidadãos aos serviços de governo eletrônico, além de permitir uma maior interação das pessoas com as políticas e decisões públicas. Este artigo tem por objetivo descrever e analisar as soluções de identidade eletrônica móvel descritas na literatura e que foram selecionadas após a condução de uma revisão sistemática da literatura.*

1. Introdução

Segundo [ONU 2014], o governo eletrônico constitui-se de uma importante ferramenta para revitalizar a administração pública tanto no nível nacional quanto local. Como estratégia, muitos países indicam a necessidade de oferecer soluções robustas de autenticação do ponto de vista da segurança, que proporcionem mobilidade aos cidadãos e que tenham, preferencialmente, baixo custo. Sendo assim, o desenvolvimento de uma Estratégia Nacional de Gestão de Identidade Eletrônica (GId) é fundamental para a realização de Programas de Governo Eletrônico (e-Gov).

Em [OECD 2011], foi apresentado um estudo sobre as estratégias nacionais de Gid para e-Gov que foram adotadas por alguns países. Constatou-se que tais estratégias se basearam em práticas e regulamentos dos sistemas de identidade convencional existentes. Ou seja, os países presentes no estudo optaram por lançar uma carteira de identidade eletrônica (cartão eID), de forma que a distribuição e entrega dos mesmos para os cidadãos seguisse aquilo que já era feito com as carteiras de identidade convencionais com suporte em papel.

*Bolsista CNPq - 200995/2015-4

O uso de cartão eID aumenta a robustez dos processos de identificação e autenticação do cidadão perante serviços do governo eletrônico, uma vez que esse cartão possui elementos criptográficos e a habilidade de executar algumas pequenas aplicações dentro do próprio ambiente seguro do cartão. A identidade eletrônica móvel (eID móvel) pode ser vista como uma evolução dos cartões eID, tendo em vista que o cidadão poderia fazer uso do seu próprio telefone para acessar de forma segura os serviços de governo eletrônico. Conforme observado por [Ruiz-Martínez et al. 2007], a adoção do eID móvel pode ser motivada pelo crescente uso de serviços de telecomunicações e principalmente pela baixa aceitação das eIDs baseadas em cartão.

Como as soluções de eID Móvel oferecem a possibilidade de autenticação usando a eID a partir do próprio telefone móvel do usuário, o uso do cartão de eID pode ser substituído nos processos de autenticação ou funcionar como complemento às estratégias nacionais de GId. Neste último cenário, as soluções de eID Móvel atuam como tecnologias de inclusão, permitindo que mais pessoas se beneficiem do uso de uma eID para interagir com o governo. Resumidamente, as soluções de eID Móvel tem como potencial aumentar significativamente o fator usabilidade e inclusão digital, sem perder o nível de segurança oferecido pelas soluções baseadas em cartão de eID [Rath et al. 2014].

O objetivo deste artigo é analisar as estratégias e soluções de identidade eletrônica móvel (eId Móvel) presentes na literatura acadêmica. Este artigo descreve os resultados obtidos (trabalhos selecionados) de uma revisão sistemática executada em agosto de 2016 e está organizado da seguinte forma: Na Seção 2, são apresentados os conceitos e características referentes a eID Móvel. A Seção 3 descreve como a revisão sistemática da literatura foi conduzida, bem como a descrição dos trabalhos relacionados. Na Seção 4 é feita a análise dos trabalhos relacionados. Por fim, na Seção 5 são apresentadas as considerações finais e trabalhos futuros.

2. Identidade Eletrônica Móvel (eID Móvel)

A identidade de uma pessoa pode ser descrita como sendo um conjunto de informações pessoais, utilizado a fim de caracterizar corretamente um indivíduo. Essas informações podem se constituir do nome da pessoa, registro biométrico, altura, cor do cabelo, entre outros. Para realizar essa caracterização, a identidade pode também estar associada a outros atributos ligados à pessoa como o nome da mãe, data e local de nascimento. Dependendo do uso e do contexto, a identidade pode ser composta somente por algumas destas informações pessoais [NSTC 2008]. Para [Clauß and Köhntopp 2001], a identidade eletrônica (eID) é criada quando informações pessoais são utilizadas para se caracterizar uma pessoa no meio digital.

Por definição, a identidade eletrônica móvel se refere ao uso da eID através de dispositivos móveis, como telefones inteligentes (*smartphones*) e *tablets*. Segundo [World 2015], eID Móvel é um conjunto formado pela eID do usuário e pelas tecnologias utilizadas para gerenciá-la. Já para [Telia 2016], é como se o cartão de eID estivesse dentro de um telefone móvel.

Durante as últimas décadas, algumas soluções de eID Móvel foram testadas e implementadas em alguns países. Enquanto algumas soluções continuam em uso, outras foram abandonadas ou substituídas. Atualmente, um conjunto heterogêneo de soluções encontra-se em produção, englobando um número crescente e contínuo de diferentes con-

ceitos tecnológicos e implementações [Zefferer and Teufl 2015].

Para [Rath et al. 2014], apesar da diversidade de implementações da eID Móvel, o modelo de confiança advém do uso de algum elemento seguro (*secure hardware element* – SE) presente no dispositivo móvel. Este SE deve possuir a capacidade de armazenar e realizar operações de criptografia. De acordo com esse autor, as implementações atuais de eID Móvel podem ser classificadas em dois tipos de soluções, dependendo da localização do elemento seguro:

- Soluções baseadas em cliente: soluções baseadas neste modelo, normalmente, fazem uso de um cartão SIM (*subscriber identity module*) especial, capaz de armazenar a eID de forma segura e prover operações de criptografia como assinatura de documentos. Tipicamente, o acesso aos dados e funcionalidades deste cartão SIM está protegido por uma senha secreta (*Personal Identification Number* – PIN), proporcionando assim o segundo fator de autenticação.

- Soluções baseadas em servidor: essas soluções utilizam as técnicas de computação em nuvem para implementar um elemento de *hardware* central, como, por exemplo, um Módulo de Hardware Seguro (HSM). Assim, o dispositivo móvel do usuário não armazena os dados da eID e não implementa as funcionalidades de criptografia. Entretanto, o dispositivo móvel participa do processo de autenticação, como um dos componentes obrigatórios. Isto porque este dispositivo é o responsável por acessar a eID no HSM e destravar as funcionalidades de criptografia, o que geralmente é feito com o recebimento de uma senha descartável (*one-time password* – OTP).

Para [Mantoro and Milišić 2010], nos processos de autenticação, as chances de forjar uma identidade devem ser minimizadas, utilizando algum elemento seguro como apresentado acima. É possível utilizar o telefone móvel pessoal para identificar e autenticar o cidadão de forma segura durante o acesso a um provedor de serviço (*Service Provider* – SP) governamental, por exemplo. Por outro lado, conforme apresentado por [Stamp 2011], é recomendável utilizar mais de um fator de autenticação de forma a reforçar a segurança.

Implementar uma solução baseada em cliente ou em servidor depende da infraestrutura e da estratégia nacional de GId para e-Gov adotada em cada país. Como exemplificado por [Zefferer and Teufl 2015], os países Bálticos e Escandinavos passaram a adotar arquiteturas baseadas em cliente, com o uso de cartões SIM como elementos de hardware seguros. A Áustria, por outro lado, preferiu a adoção de uma arquitetura baseada em servidor, utilizando o HSM como hardware seguro.

A popularização e o aumento da adoção de uma solução de eID Móvel pelos governos tem atraído muitas oportunidades de negócios. Empresas privadas começaram a oferecer soluções de eID Móvel prontas para uso, de forma a facilitar a implantação pelos governos. Dentre estas, podem ser citadas as empresas *Valimo Wireless* Ltd[1] e a *Methics Ltd*[2], que oferecem soluções baseadas em cartão SIM; e a ServerBKU[3] e PkBox[4], que

[1] http://www.valimo.com/
[2] http://www.methics.fi/
[3] http://www.valimo.com/
[4] http://www.pksuite.it/eng/pr_pkbox.php

oferecem soluções baseadas no uso de HSM.

Porém, ao abordar a questão identidade eletrônica móvel tanto em soluções oferecidas por empresas privadas quanto públicas, uma preocupação constante se refere à privacidade das pessoas. [Laurido and Feitosa 2015] descrevem privacidade como sendo o direito de cada pessoa de manter e controlar suas informações pessoais, decidindo quem pode ter acesso a elas. Para [Pournajaf et al. 2014], a quebra de privacidade é considerada um problema ao expor atributos sensíveis de uma pessoa como um simples endereço de residência, até informações privadas e particulares como doenças ou estilos de vida.

Como a identidade digital de uma pessoa pode estar atrelada a um conjunto de informações pessoais, conforme afirmado por [Jøsang et al. 2007], o sistema de gestão de identidade desempenha um papel importante na preservação da privacidade. Para [Hansen et al. 2008], há uma grande variedade de princípios e guias que visam estabelecer e manter a privacidade do sistema de gestão de identidade. Os princípios mais amplamente aceitos são as Práticas para Informação Justa (*Fair Information Practice* – FIPs), que foram desenvolvidos na década de 1970.

A OECD[5] publicou um conjunto de diretrizes baseado no FIPs que objetiva garantir a privacidade para a troca de dados pessoais [Hansen et al. 2008]. Em 2013, o conjunto de diretrizes criadas pela OECD foi atualizado, de forma a garantir aderência ao avanço tecnológico dos últimos anos. Ao adotá-lo como guia, um sistema de gestão de identidade passa a operar no modelo centrado no usuário, oferecendo a esse usuário o controle sobre suas informações pessoais [OECD 2013].

De forma geral, a privacidade pode ser entendida como a possibilidade do usuário determinar quais atributos pessoais serão divulgados para os SPs e se concorda com os termos de uso estabelecidos pelo provedor. Segundo os princípios definidos pela OECD, o usuário tem o direito de garantir seu anonimato perante o provedor de serviço, bem como divulgar as informações pessoais que julgar adequadas.

Contudo, apesar de existirem diretrizes para garantir a privacidade dos usuários, quando se trata de soluções de eID Móvel para governo eletrônico, também deve-se considerar que o direito à privacidade deve ser algo previsto em lei.

3. Revisão Sistemática da Literatura

A execução de uma Revisão Sistemática da Literatura (RSL) teve como objetivo principal identificar as publicações relacionadas ao uso da Identidade Eletrônica Móvel (eID Móvel), dentro e fora do contexto de governo eletrônico. [Kitchenham and Charters 2007] propõe quatro passos para conduzir uma revisão sistemática da literatura (RSL): (1) identificação dos recursos (questão de pesquisa, palavras chaves e fontes); (2) seleção dos estudos; (3) extração dos dados e (4) análise dos dados.

Segundo [Kitchenham and Charters 2007], o estabelecimento das questões de pesquisa se constitui a parte mais importante de qualquer revisão sistemática. O processo de revisão visa, portanto, encontrar os estudos candidatos capazes de responder às questões de pesquisa formuladas e a análise destes estudos deverão ser capazes de trazer as respostas esperadas. Para identificar e selecionar estes estudos, foi elaborado e executado

[5]Disponível em http://oecdprivacy.org/.

um protocolo de busca para encontrar nas bases científicas os estudos primários que respondem à seguinte questão: quais soluções de identidade eletrônica móvel (eID Móvel) propostas podem ser aplicadas no contexto de governo eletrônico? Como questão adicional, definiu-se ainda: quais tecnologias estão sendo utilizadas para prover a eID Móvel? Através da análise das publicações, buscou-se analisar as soluções de eID Móvel propostas de forma a identificar como ocorre o armazenamento dos atributos do usuário e como este usuário é identificado pelo provedor de serviço (SP) ao fazer uso do identificador eletrônico (eID).

Na revisão sistemática, executada em agosto de 2016, definiu-se que apenas os estudos publicados na língua inglesa seriam considerados, de acordo com a *string* de busca: ("MOBILEID" OR "MOBILE ID" OR "MOBILE-ID" OR "MOBILE EID" OR "M-ID" OR "MOBILE IDENTIFICATION" OR "MOBILE IDENTITY" OR "IDENTIFICATION ON MOBILE").

O protocolo de busca foi executado considerando as cinco fontes mais relevantes da área, a saber: ACM Digital Library [6], IEEE Explore [7], Science Direct [8], Scopus [9] e SpringerLink [10]. Para extrair a primeira lista de trabalhos, executou-se a string de busca nas fontes citadas, considerando o título e resumo, e utilizou-se como filtro trabalhos publicados nos últimos 10 anos. A Tabela 1 apresenta o total de publicações retornadas de cada uma das cinco bases científicas, o que representou um total de 275 trabalhos.

Tabela 1. Resultados da Execução do Protocolo de Busca e Seleção de Trabalhos

	ACM	IEEEXplorer	ScienceDirect	Scopus	Springer	Total
Resultado da string	25	27	10	52	161	275
Trabalhos lidos	3	6	0	7	2	18
Trabalhos selecionados	2	2	0	3	1	8

Ainda na etapa de seleção dos trabalhos (etapa 2 da RSL), os seguintes procedimentos foram executados para inclusão e exclusão de trabalhos: (1) após verificar o título, autores e filiação, procurou-se identificar os trabalhos repetidos (foi mantido o trabalho mais recente). Trinta e nove (39) trabalhos repetidos foram excluídos da lista; (2) após a leitura do título e do resumo de cada artigo, foram excluídos trabalhos que não tratam exatamente de eID Móvel ou cujos títulos e resumos apresentavam informações conflitantes. Em caso de dúvida, a conclusão do artigo foi analisada. Ainda nesta etapa, trabalhos com até 3 páginas, que caracterizavam resumo estendido e trabalhos sem resumo foram excluídos. Ao final desta etapa 2, duzentos e dezoito trabalhos foram excluídos. Como resultado (3), dezoito artigos foram incluídos na lista de artigos pré-selecionados, pois estes respondiam à questão primária de pesquisa, ou seja, os trabalhos descrevem uma solução para prover eID Móvel e não apenas descrevem o problema (ver Tabela 1). Finalmente, após a leitura completa dos dezoito trabalhos, foram selecionados oito trabalhos que apresentam de forma consistente uma solução para prover eID Móvel. Estes trabalhos estão indicados na Tabela 2.

[6]http://dl.acm.org/
[7]http://ieeexplore.ieee.org/
[8]http://www.sciencedirect.com/
[9]http://link.springer.com/search
[10]http://link.springer.com/

Tabela 2. Resultados da Execução do Protocolo de Busca e Seleção de Trabalhos

Referência	Título	Tipo de Publicação	Fonte
MARTENS (2010)	Electronic identity management in Estonia between market and state governance	Periódico	Springer
EN-NASRY E KETTANI (2011)	Towards an open framework for mobile digital identity management through strong authentication methods	Evento Internacional	Springer
BICAKCI (2014)	Mobile authentication secure against man-in-the-middle attacks	Evento Internacional	IEEE
WU ET AL. (2014)	Research of eID Mobile Identity Authentication Method	Evento Internacional	Springer
KRIMPE (2014)	Mobile ID: Crucial element of m-Government	Evento Internacional	ACM
PRUSA (2015)	E-identity: Basic building block of e-Government	Evento Internacional	IEEE
ZEFFERER E TEUFL (2015)	Leveraging the Adoption of Mobile eID and e-Signature Solutions in Europe	Evento Internacional	Springer
KETTULA (2015)	A novel federated strong mobile signature service: The Finnish case	Periódico	Elsevier

3.1. Descrição dos Trabalhos Selecionados

O trabalho apresentado por [Martens 2010] descreve o Sistema de Gestão de Identidade Eletrônica (*electronic Identity Management System* – eIDMS) da Estônia para o contexto de e-Gov do país. A eID Móvel foi introduzida no governo estoniano em maio de 2007 pela maior operadora móvel (EMT) em cooperação com a SK[11] (Autoridade Certificadora Estoniana). Para poder utilizar a eID Móvel, o usuário precisa trocar o seu cartão SIM por um cartão com capacidade PKI (*Public Key Infrastructure*). Porém, mesmo após realizar a troca do cartão SIM por outro com funcionalidade PKI, o usuário ainda precisa ativar a sua eID Móvel, o que é feito através do cartão de eID.

A PKI adotada na Estônia, prevê o uso de dois pares de certificados digitais para o cidadão: um par utilizado para autenticação e um par utilizado para assinatura eletrônica. Com validade de cinco anos, os dois pares são considerados qualificados, ou seja, são certificados reconhecidos legalmente pelo Ato de Assinatura Digital[12]. Cada uma das chaves privadas possui um código PIN diferente. Os certificados contêm o nome completo do cidadão, seu código pessoal[13] (*Personal Identification Code* – PIC) e um endereço de email reconhecido pelo governo. Entretanto, nenhuma informação biométrica é utilizada.

Em [En-Nasry and El Kettani 2011], os autores propõem um *middleware* para ser integrado em provedores de identidade, de forma a oferecer vários métodos de autenticação para o usuário. Segundo os autores, entre os métodos mais comuns de autenticação dos sistemas de eID Móvel, destacam-se: autenticação baseada em cartão SIM, autenticação baseada em chaves públicas (PKI) e autenticação baseada em senhas descartáveis (*one time password* – OTP).

Independente do mecanismo de eID Móvel adotado, o modelo proposto em [En-Nasry and El Kettani 2011] se baseia em uma camada de software (*middleware*) para

[11]Disponível em https://sk.ee/en/about/.
[12]Disponível em http://www.legaltext.ee/text/en/X30081K4.htm
[13]O PIC é atribuído a todo cidadão do país desde a independência do país em 1992.

integrar todos os métodos de autenticação. Este *middleware* deve ser capaz de gerenciar perfis de usuário e contexto, garantindo que a autenticação possa ocorrer a partir de diversos métodos. Isto significa que o usuário poderá utilizar um, dentre vários métodos, para se autenticar no SP. A proposta prima pela usabilidade, desobrigando o usuário de lembrar exatamente qual o método de autenticação deve utilizar para acessar um serviço *online* protegido.

O protocolo proposto por [Bicakci et al. 2014] tem por objetivo garantir a segurança contra ataques do tipo homem-do-meio (*Man-in-The-Middle* – MITM) em ambientes de autenticação, utilizando soluções tradicionais de eID Móvel. Para os autores, as soluções tradicionais de eID Móvel são as que geram um par de chaves criptográficas assimétricas (pública e privada) para autenticação do usuário, armazenando essas chaves no cartão SIM e protegendo-as com uma senha pessoal (PIN). Contudo, para autenticação no SP com uma eID Móvel, o protocolo proposto leva em consideração o contexto no qual o usuário e o dispositivo estão inseridos. O servidor de assinatura móvel ganha a capacidade de autenticar o usuário, dispensando o uso de uma entidade certificadora (CA). Assume-se também como premissa que o sistema operacional móvel é seguro, portanto o dispositivo móvel deve estar equipado com o ambiente de execução confiável (*Trusted Executed Environment* – TEE).

O método de autenticação em eID Móvel proposto em [Wu et al. 2014], é baseado na utilização da identidade eletrônica em conjunto com a tecnologia NFC (*Near Field Communication*). Os experimentos realizados pelo autor demonstraram que o método proposto pode ser utilizado como uma solução de eID Móvel universal. De forma geral, o método de eID Móvel proposto visa prover a autenticação segura e a privacidade do usuário.

[Krimpe 2014] descreve a implementação da eID Móvel na República do Azerbaijão. Conhecida no país por *Asan Ìmza* ou "Assinatura Simples", a solução de eID Móvel faz parte do projeto de assinatura eletrônica (*e-Signature*) móvel, sendo o principal componente das políticas de e-Gov daquele país. A eID Móvel foi lançada como projeto piloto em 2013 e, oficialmente, entrou em operação no ano de 2014.

A implementação da identidade móvel no Azerbaijão é baseada em uma parceria público-privada (*Public-Private-Partnership* – PPP), realizada com as maiores operadoras de telefonia móvel do país. Um cartão SIM diferenciado, que armazena os certificados digitais pessoais no dispositivo móvel é fornecido ao cidadão. Com base em uma infraestrutura de chave público-privada (PKI), os certificados pessoais emitidos são armazenados no cartão SIM, evitando que a chave privada possa ser copiada. Os certificados também só podem ser destravados com o uso de senhas pessoais (códigos PIN).

O trabalho de [Prusa 2015] trata dos aspectos ligados à confiança relacionada com a eID e sua integração com o governo eletrônico. Foi feita uma discussão sobre os projetos europeus STORK e STORK 2.0 e a integração entre os países da União Europeia, como forma de motivar o avanço da interoperabilidade entre países, especialmente os países da União Africana. O uso da identidade eletrônica é o foco principal da publicação, abordando de forma rápida o uso da eID através de dispositivos móveis e citando superficialmente a Áustria, Estônia e Islândia como países que disponibilizaram a solução de eID Móvel para seus cidadãos.

O trabalho desenvolvido por [Zefferer and Teufl 2015] apresenta uma pesquisa e analisa as soluções de eID Móvel e assinatura eletrônica, adotadas por vários países europeus, com o intuito de servir como referência para outros governos. Na Estônia, a solução de eID Móvel e assinatura eletrônica é conhecida "Mobiil-ID". Nessa solução, os dados do usuário são armazenados no cartão SIM fornecido pelas operadoras de telefonia móvel. Com abordagem semelhante, a solução chamada de "BankID" na Noruega indica também a participação do setor bancário. Outras soluções que seguem a abordagem com uso do cartão SIM também são encontradas na Finlândia e Lituânia, o que demonstra que os Estados Escandinavos e Bálticos estão juntamente com a Áustria, entre os países líderes com relação à adoção da eID Móvel e assinatura eletrônica na Europa.

Com o nome "MobilImza", a Turquia desenvolveu a solução de eID Móvel e assinatura eletrônica, tendo nas operadoras de telefonia móvel Turkcell e Avea os tomadores de decisões centrais. Assim como nos países Escandinavos e Bálticos, a solução da Turquia segue a abordagem de arquitetura baseada em cliente, porém, utilizando um cartão SIM melhorado. Soluções utilizando o cartão SIM foram adotados pela Moldova e Suíça. Na Moldova, a solução foi introduzida em 2012 com a participação das operadoras de telefonia móvel e tendo o governo como entidade certificadora raiz. Na Suíça, com o nome de "Swiss Mobile ID", a solução foi colocada em produção em 2013.

O trabalho de [Kerttula 2015] tem por objetivo descrever questões legais, arquitetura e padrões do serviço de eID Móvel da Finlândia. O serviço é baseado um uma estrutura PKI móvel e na federação de asserções de segurança, usando padrões ETSI MSS[14]. As credencias pessoais de segurança são armazenadas no UICC (*Universal Integrated Circuit Card*) e as operações de criptografia rodam neste SE a prova de violação do operador de telefonia móvel.

Os operadores de telefonia móvel participam ativamente do sistema de eID Móvel naquele país. Com serviço lançado em junho de 2011[15], atualmente, as operadoras TeliaSonera Finland, Elisa e DNA são as responsáveis pela implementação e desenvolvimento da eID Móvel, atuando em cooperação com a FiCom[16]. Entretanto, o sistema é aberto ao ponto de permitir a entrada de novos operadores de telefonia.

Como o modelo faz uso de um elemento seguro (USIM), as chaves RSA podem ser geradas de uma forma simples e segura dentro deste elemento. Da mesma forma, um conjunto de aplicativos (*SIM Application Toolkit* – SAT) é inserido no SE para permitir a assinatura móvel.

4. Análise dos Trabalhos

Na Tabela 3, são apresentadas algumas informações sobre a implementação das soluções de eID Móvel, obtidas na análise dos trabalhos relacionados, a saber (1) os cenários de aplicação da eID Móvel, ou seja, se a solução de eID Móvel foi implementada ou projetada para uso pelos SPs governamentais e SPs privados ou trata-se apenas de um modelo teórico; (2) os países para os quais a solução foi proposta ou implementada; (3) o ano de início da operação (data de lançamento) da solução de eID Móvel; (4) se houve o estabelecimento de parcerias público-privada para desenvolvimento da solução; (5) o tipo de

[14]Disponível em http://www.etsi.org/

[15]Disponível em www.mobiilivarmenne.fi/en/index.html.

[16]Finnish Federation of Communications and Informatics.

elemento seguro adotado pela solução de eID Móvel; e (6) o que é preciso que o cidadão informe para que o processo de autenticação ocorra, como por exemplo, senha numérica, senhas descartáveis (OTP) ou fatores biométricos.

Tabela 3. Comparação dos trabalhos relacionados

Referência	Cenário	País	Ano	PPP	SE	Autenticação
MARTENS (2010)	e-Gov	Estônia	2007	Sim	Cartão SIM	PIN
EN-NASRY E KETTANI (2011)	Teórico	-	-	Sim	Cartão SIM	OTP
BICAKCI (2014)	Teórico	-	-	Sim	C. SIM / TEE	PIN
WU ET AL. (2014)	Teórico	-	-	-	Cartão de eID	PIN
KRIMPE (2014)	e-Gov	Azerbaijão	2014	Sim	Cartão SIM	PIN
PRUSA (2015)	e-Gov	Islândia	2014	Sim	Cartão SIM	PIN
ZEFFERER, TEUFL (2015)	e-Gov	Austria	2010	-	HSM	Senha / OTP
	e-Gov	Noruega	2009	Sim	Cartão SIM	PIN
	e-Gov	Lituânia	2007	Sim	Cartão SIM	PIN
	e-Gov	Turquia	2007	Sim	Cartão SIM	PIN
	e-Gov	Moldova	2012	Sim	Cartão SIM	PIN
	e-Gov	Suíça	2013	Sim	Cartão SIM	PIN
KERTTULA (2015)	e-Gov/Priv	Finlândia	2010	Sim	Cartão USIM	PIN / OTP

Alguns países foram citados em mais de um trabalho relacionado. Assim, foi considerada apenas uma referência (linha) na Tabela, como é o caso da Áustria que aparece nos trabalhos de [Prusa 2015], [Zefferer and Teufl 2015] e [Martens 2010], da Estônia que é descrita nos trabalhos de [Prusa 2015] e [Zefferer and Teufl 2015], e da Finlândia que é citada por [Kerttula 2015] e [Zefferer and Teufl 2015]. Dados incompletos, imprecisos, não informados ou irrelevantes foram deixados intencionalmente sem preenchimento (marcação "-").

Nas publicações de [Martens 2010], [Krimpe 2014] e [Kerttula 2015], apenas um país em cada artigo foi analisado pelos autores, respectivamente, a Estônia, a República do Azerbaijão e a Finlândia. Embora a primeira solução de eID Móvel tenha sido implementada em 2007 (Estônia), observou-se que as implementações posteriores seguem a mesma abordagem, com a adoção do cartão SIM como elemento seguro e utilização da eID tanto pelo governo quanto pelo setor privado.

Os autores [En-Nasry and El Kettani 2011], [Bicakci et al. 2014] e [Wu et al. 2014] optaram por apresentar um modelo teórico de autenticação móvel. [En-Nasry and El Kettani 2011] propõem um protocolo extensível para operar de forma independente em plataformas de autenticação (ex. IdP), de forma que essas plataformas sejam capazes de reconhecer e trabalhar com todos os tipos de autenticação existentes, como biometria, senhas descartáveis, identificação de contexto, entre outras. [Bicakci et al. 2014] apresentam o protocolo "Mobile-ID" utilizando padrões abertos, com uma abordagem que procura mitigar problemas com ataques do tipo homem-no-meio. [Wu et al. 2014] foram os únicos a propor a utilização do *chip* do cartão de eID do cidadão como elemento seguro. Este modelo sugere a utilização do leitor NFC dos dispositivos móveis, que em conjunto com os módulos idealizados, visam promover uma forma segura de autenticação móvel.

Em [Prusa 2015], quatro países são supervisualmente citados: Áustria, Estônia, Islândia e República Tcheca. Destes, a Islândia traz mais informações se destacando com uma das implementações mais recentes de eID Móvel. Por outro lado, o trabalho apresen-

tado por [Zefferer and Teufl 2015] descreve o cenário de eID Móvel em diversos países europeus, dos quais a Áustria se destaca como o único país a apresentar uma solução baseada em servidor.

Permitir a participação de instituições privadas aparenta ser uma prática comum, visto que uma mesma eID pode ser utilizada tanto para autenticação em provedor de serviço governamental tanto quanto o SP privado. Apesar das semelhanças encontradas, a data de implementação varia muito. Países como a Estônia, Lituânia e Turquia implementaram a eID Móvel em 2007; já a Islândia, República do Azerbaijão e Suíça implementaram a solução recentemente.

Ao observar na Tabela 3, o ano de início de operação das soluções, constata-se a afirmação de [Zefferer and Teufl 2015] ao citar que os Estados Escandinavos e Bálticos estão, juntamente com a Áustria, entre os países líderes com relação à adoção da eID Móvel na Europa.

Apesar da maioria das soluções apresentarem parcerias entre governo e iniciativa privada, não foi apresentado pelos trabalhos relacionados o grau de envolvimento do governo ou da iniciativa privada. Ou seja, não foi possível identificar até que ponto o governo dita as regras de negócios e determina quais padrões tecnológicos devem ser seguidos. Da mesma forma, não foi possível determinar como o direito à privacidade é garantido aos cidadãos e usuários das soluções de eID Móvel.

Pela simplicidade de implementação, observa-se que a utilização do cartão SIM como elemento seguro tem sido a solução de eID Móvel mais bem aceita pelos governos. Portanto, considerando a questão de pesquisa elencada como objetivo principal da revisão sistemática, esta solução aparenta ser a mais aderente às políticas de governo eletrônico.

Contudo, considerando a questão adicional de pesquisa, é importante destacar que o HSM também foi citado como solução viável de eID Móvel. Da mesma forma, o trabalho teórico apresentado por [Bicakci et al. 2014], sugere a utilização do TEE como fator complementar à segurança.

De forma geral, conforme apresentado na Tabela 3, como solução baseada no cliente o cartão SIM é identificado como o mais adotado, bem como o HSM é considerado quando o governo pretende adotar uma solução baseada em servidor.

5. Conclusão

Com avanço tecnológico dos dispositivos móveis, as capacidades de *hardware* têm se ampliado e os softwares estão se tornando cada vez mais intuitivos, fazendo destes aparelhos o elemento perfeito para estar junto do usuário em qualquer lugar. Ao combinar elementos seguros de armazenamento e processamento, estes dispositivos passam a permitir que transações *online* seguras possam ser realizadas.

Neste contexto, as soluções de eID Móvel se destacam como soluções viáveis pela usabilidade e pela alta segurança oferecida. No geral, os custos para os cidadãos são relativamente baixos, uma vez que o componente mais caro destas soluções é o dispositivo móvel e normalmente o cidadão já o possui. Além disso, as demais funcionalidades providas por esses dispositivos permitem ao cidadão outras facilidades, que não o uso exclusivo como identificador eletrônico.

Conforme observado no estudo dos trabalhos relacionados, a adoção de soluções de eID Móvel se mostra cada vez mais frequente. Oferecer serviços a uma gama maior de pessoas tem motivado sua adoção por governos, além de ter atraído o interesse de empresas privadas. Trabalhos científicos, em sua maioria, descrevem as soluções já implementadas e prontas para uso. Poucos trabalhos realmente propõem uma solução de eID nova ou oferecem resultados de uma prova de conceito. Mesmo assim, a maioria das soluções foi concebida através da utilização de cartões SIM, justamente pela facilidade de implementação.

Por fim, este estudo demonstrou que as soluções de eID Móvel estão gradativamente sendo adotadas por diferentes países por se constituírem uma grande ferramenta para aumentar a interação dos cidadãos e governos. Em trabalhos futuros, será estudado o cenário de e-Gov no Brasil e será proposto um sistema de eID Móvel que seja aderente à estratégia de GId nacional.

Referências

Bicakci, K., Unal, D., Ascioglu, N., and Adalier, O. (2014). Mobile authentication secure against man-in-the-middle attacks. In *Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2014 2nd IEEE International Conference on*, pages 273–276. IEEE. http://dx.doi.org/10.1109/MobileCloud.2014.43.

Clauß, S. and Köhntopp, M. (2001). Identity management and its support of multilateral security. *Computer Networks*, 37(2):205–219. http://dx.doi.org/10.1016/S1389-1286(01)00217-1.

En-Nasry, B. and El Kettani, M. D. E.-C. (2011). 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*, pages 56–63. Springer. http://dx.doi.org/10.1007/978-3-642-22365-5_8.

Hansen, M., Schwartz, A., and Cooper, A. (2008). Privacy and identity management. *IEEE Security & Privacy*, 6(2):38–45. http://dx.doi.org/10.1109/MSP.2008.41.

Jøsang, A., Zomai, M. A., and Suriadi, S. (2007). Usability and privacy in identity management architectures. In *Proceedings of the fifth Australasian symposium on ACSW frontiers-Volume 68*, pages 143–152. Australian Computer Society, Inc.

Kerttula, E. (2015). A novel federated strong mobile signature service—the finnish case. *Journal of Network and Computer Applications*, 56:101–114. http://dx.doi.org/10.1016/j.jnca.2015.06.007.

Kitchenham, B. and Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE 2007-001, Keele University and Durham University Joint Report.

Krimpe, J. (2014). Mobile id. In *Proceedings of the 2014 Conference on Electronic Governance and Open Society: Challenges in Eurasia*, pages 187–194. ACM. http://dx.doi.org/10.1145/2729104.2729133.

Laurido, J. J. d. V. and Feitosa, E. L. (2015). Segurança em mobile crowd sensing. In *V WGID - Workshop de Gestão de Identidades – XV Simpósio Brasileiro*

em Segurança da Informação e de Sistemas Computacionais - SBSeg, pages 51–92. http://sbseg2015.univali.br/anais/WGID/artigoWGID02.pdf.

Mantoro, T. and Milišić, A. (2010). Smart card authentication for internet applications using nfc enabled phone. In *Information and Communication Technology for the Muslim World (ICT4M), 2010 International Conference on*, pages D13–D18. IEEE. http://dx.doi.org/10.1109/ICT4M.2010.5971895.

Martens, T. (2010). Electronic identity management in estonia between market and state governance. *Identity in the Information Society*, 3(1):213–233. http://dx.doi.org/10.1007/s12394-010-0044-0.

NSTC (2008). Identity management task force report. *Subcomiittee on Biometrics and Identity Management*. https://goo.gl/2iIYOG.

OECD (2011). *National strategies and policies for digital identity management in OECD countries*. OECD Publishing. dx.doi.org/10.1787/5kgdzvn5rfs2-en.

OECD (2013). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. OECD Publishing. https://goo.gl/Y0yxmw.

ONU (2014). *e-Government Survey*. United Nations. https://goo.gl/jccKDV.

Pournajaf, L., Xiong, L., Garcia-Ulloa, D. A., and Sunderam, V. (2014). A survey on privacy in mobile crowd sensing task management. Technical report, Technical Report TR-2014-002, Department of Mathe-matics and Computer Science, Emory University. http://www.mathcs.emory.edu/~lpourna/papers/pournajaf-survey14.pdf.

Prusa, J. (2015). E-identity. In *IST-Africa Conference, 2015*, pages 1–10. IEEE. http://dx.doi.org/10.1109/ISTAFRICA.2015.7190586.

Rath, C., Roth, S., Schallar, M., and Zefferer, T. (2014). A secure and flexible server-based mobile eid and e-signature solution. In *The Eighth International Conference on Digital Society*, pages 7–12. http://dx.doi.org/10.1145/2684103.2684142.

Ruiz-Martínez, A., Sánchez-Martínez, D., Martínez-Montesinos, M., and Gómez-Skarmeta, A. F. (2007). A survey of electronic signature solutions in mobile devices. *Journal of Theoretical and Applied Electronic Commerce Research*, 2(3):94. http://www.jtaer.com/dec2007/ruiz_sanchez_martinez_gomez_p7.pdf.

Stamp, M. (2011). *Information security: principles and practice*. John Wiley & Sons.

Telia (2016). Mobile id. https://www.telia.ee/en/era/muud-teenused/mobiil-id.

World, M. I. (2015). What is mobile id? http://mobileidworld.com/what-is-mobile-id/.

Wu, X., Fan, Y., Zhang, X., and Xu, J. (2014). Research of eid mobile identity authentication method. In *International Conference on Trustworthy Computing and Services*, pages 350–358. Springer. http://dx.doi.org/10.1007/978-3-662-47401-3_46.

Zefferer, T. and Teufl, P. (2015). Leveraging the adoption of mobile eid and e-signature solutions in europe. In *Electronic Government and the Information Systems Perspective*, pages 86–100. Springer. http://dx.doi.org/10.1007/978-3-319-22389-6_7.

