UNIVERSIDADE DO VALE DO ITAJAÍ

PROGRAMA DE MESTRADO ACADÊMICO EM COMPUTAÇÃO APLICADA

USO DE IDENTIDADES MÓVEIS EM ESTRATÉGIAS NACIONAIS DE GESTÃO DE IDENTIDADES

RELATÓRIO DE ESTUDO DIRIGIDO

por

Glaidson Menegazzo Verzeletti

Michelle Silva Wangham, Dra.

Orientadora

Itajaí (SC), Julho de 2015

UNIVERSIDADE DO VALE DO ITAJAÍ

PROGRAMA DE MESTRADO ACADÊMICO EM COMPUTAÇÃO APLICADA

USO DE IDENTIDADES MÓVEIS EM ESTRATÉGIAS NACIONAIS DE GESTÃO DE IDENTIDADES

RELATÓRIO DE ESTUDO DIRIGIDO

por

Glaidson Menegazzo Verzeletti

Relatório apresentado como requisito para a aprovação na disciplina Estudo Dirigido I do Curso de Mestrado Acadêmico em Computação Aplicada. Orientador: Michelle Silva Wangham, Dra.

Itajaí (SC), Julho de 2015

SUMÁRIO

LISTA DE ILUSTRAÇÕES

RESUMO

VERZELETTI, Glaidson Menegazzo. **Uso de Identidades Móveis em Estratégias Nacionais de Gestão de Identidades.** Relatório de Estudo Dirigido I – Programa de Mestrado Acadêmico em Computação Aplicada, Universidade do Vale do Itajaí, Itajaí, 2015.

As Identidades Eletrônicas Móveis (eID Móveis) se referem aos atributos dos usuários e às tecnologias de gerenciamento destas identidades, as quais são integrados aos dispositivos móveis do cidadão, possibilitando o consumo de serviços de Governo Eletrônico (e-Gov). Neste contexto, o armazenamento dos atributos do usuário (informações pessoais) precisam ser guardados de forma segura. Para tanto, existem possibilidades de armazenamento em hardware removível, hardware não-removível e software. Utilizando um dos métodos de armazenamento dos atributos do usuário, é possível utilizar o telefone móvel pessoal para identificar e autenticar o cidadão no acesso aos provedores de serviço (SP). Esta abordagem se assemelha às funcionalidades oferecidas pelos cartões inteligentes (*smart cards*), os quais são capazes de armazenar com segurança dados pessoais além de executar aplicações de forma segura. Trazer esta funcionalidade dos *smart cards* ao telefone móvel simplesmente amplia as funções do próprio telefone. Entretanto, quando as funcionalidades dos *smart cards* são transferidas para os dispositivos móveis, as questões de segurança precisam ser muito bem implementadas, uma vez que estes dispositivos têm um histórico pobre quando se fala em segurança. Muitos dos países que implementaram uma estratégia nacional de gestão de identidades buscam implementar a identidade eletrônica (eID) através de dispositivos móveis. Dessa forma, este trabalho visa analisar os conceitos de Identidade Eletrônica Móvel, bem como as estratégias nacionais de gestão de identidade de 5 países (Alemanha, Áustria, Espanha, Estônia e Turquia) e suas implementações de eID Móvel. Para tanto, o trabalho passa pelas fases de conceitos sobre Modelos de Gestão de Identidade Eletrônica (eIDM), definições sobre Identidade Móvel e as tecnologias correlatas. Observa-se no estudo dos países, que cada um deles adota um modelo de eID em dispositivo móvel, normalmente seguindo padrão já existente de gestão de identidades. Como exemplo, podem ser citadas a Alemanha e a Espanha, que adotaram o *eID Card* com *chip* para armazenar os atributos do cidadão e, ao implementar o eID Móvel, optaram por utilizar este cartão, juntamente com a tecnologia NFC para acesso aos SPs.

Palavras-chave: Identidade Móvel, Identidade Eletrônica, Governo Eletrônico

1 INTRODUÇÃO

O desenvolvimento de uma Estratégia Nacional de Gestão de Identidades Eletrônicas (GId) é fundamental para a realização de Programas de Governo Eletrônico (e-Gov) (OECD, 2011). Segundo (United Nations, 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 serviços com processos de autenticação que exijam credenciais robustas de segurança. A adoção de um sistema de GId comum permite harmonizar a gestão de identidades em nível nacional, o que implica em reduzir ou limitar o número de identidades que cada cidadão precisa ter para interagir com os diversos serviços oferecidos pelo Governo.

A cada dois anos o Departamento de Assuntos Econômicos e Sociais da ONU conduz uma pesquisa sobre o desenvolvimento do e-Gov dos 193 Estados membros. O relatório gerado serve como ferramenta para identificar os pontos fortes e desafios dos programas nacionais e para orientar as políticas e estratégias de e-Gov. A publicação também destaca as novas tendências, questões e práticas inovadoras, bem como os desafios e oportunidades de desenvolvimento de e-Gov. O provimento de gestão de identidades é uma das características analisadas na pesquisa da ONU. O número de países que possuem estratégias nacionais cresceu de 52 (em 2012) para 69 países (2014), o que representa 36% do total de países analisados (United Nations, 2014).

Segundo a Organização para Cooperação e Desenvolvimento Econômico (*Organisation for Economic Cooperation and Development* – OECD), vários países já iniciaram alguma ação em relação à gestão de identidades eletrônicas. Segundo a OECD (2011), os países se encontram em diversos estágios em relação ao desenvolvimento e implementação das estratégias nacionais de GId. A partir do desenvolvimento de políticas (definição de leis, planos, ações, etc), os governos conseguem implementar suas estratégias de gestão de identidades.

Um sistema de gestão de identidades (SGId) provê ferramentas para a gestão das identidades em um mundo digital. A gestão de identidades pode ser entendida como o conjunto de processos e tecnologias usados para garantir a identidade de uma entidade, garantir a qualidade das informações de uma identidade (identificadores, credenciais e atributos) e para prover mecanismos de autenticação, autorização, contabilização e auditoria (ITU, 2009). Os SGId são complexos o que possibilita que algumas vulnerabilidades possam ser exploradas. Garantir a segurança sem comprometer a privacidade dos usuários e requisitos de usabilidade e de desempenho é um grande desafio no projeto destes sistemas

e na concepção de uma estrategia nacional de Gerenciamento de Identidades (IdM) (DHAMIJA; DUSSEAULT, 2008).

Conforme apresentado por (BHARGAV-SPANTZEL et al., 2007), um sistema de gestão de identidades é caracterizado pelos seguintes elementos: usuário - aquele que deseja acessar um recurso; identidade - conjunto de atributos de um usuário; provedor de identidade (IdP) - responsável por gerenciar identidades de seus usuários e autenticá-los; provedor de serviços (SP) - oferece recursos aos usuários autorizados, após verificar a autenticidade de sua identidade e após comprovar que a mesma carrega todos os atributos necessários para o acesso. A disposição de cada um destes elementos de um SGId e a forma com que estes interagem entre si caracterizam os modelos de SGId, sendo estes classificados como: tradicional, centralizado, federado e centrado no usuário (JØSANG; POPE, 2005).

- **Modelo tradicional (isolado em silos):** neste modelo, os provedores de identidades e de serviços são agrupados em uma única entidade e cabe a esta fazer a autenticação e controle de acesso de seus usuários sem depender de qualquer outra entidade. O usuário precisa então criar uma identidade diferente para cada provedor que desejar interagir e não existe o compartilhamento de identidades entre diferentes provedores (MELLO et al., 2009). Para uma instituição que hospeda diversos provedores de serviços, tem-se então o desperdício de recursos, uma vez que haverá duplicação dos esforços para manutenção de diferentes contas de um mesmo usuário.
- **Modelo centralizado:** surge como uma solução para as dificuldades apresentadas pelo modelo tradicional. Só existe um provedor de identidades, o qual é responsável por autenticar os usuários, fornecer aos provedores de serviços informações sobre estes, sendo que todos os provedores de serviços devem confiar plenamente nas informações fornecidas por este provedor de identidades. O modelo centralizado fundamentalmente permite o compartilhamento de identidades dos usuários entre os provedores de serviços e permite o uso da autenticação única (*Single Sign-On* – SSO) (BHARGAV-SPANTZEL et al., 2007).
- **Modelo de identidade federada:** está fundamentado sobre a distribuição da tarefa de autenticação dos usuários por múltiplos provedores de identidades, estando estes dispostos em diferentes domínios administrativos. Um domínio administrativo pode representar uma empresa, uma universidade, entre outros, sendo composto por usuários, diversos provedores de serviços e um único provedor de identidades. Conforme citado por Camenisch (2007), a gestão de identidades federadas é uma abordagem para otimizar a troca de informações relacionadas a identidade através de relações de confiança construídas nas federações . Os acordos de confiança estabelecidos entre provedores de identidades garantem que identidades emitidas em um domínio sejam

reconhecidas por provedores de serviços de outros domínios e o conceito de passar pelo processo de autenticação uma única vez durante a sessão (*Single Sign-On*) pode ser garantido, mesmo diante de diferentes domínios.

- **Modelo centrado no usuário:** objetiva dar ao usuário o total controle sobre suas identidades digitais, sendo que as identidades de um usuário são armazenadas em um dispositivo físico que fica em poder do próprio usuário, como por exemplo, um *smartcard* ou mesmo um telefone celular. Os usuários têm a liberdade de escolher os provedores de identidade que irão usar, independentemente dos provedores de serviços que desejam acessar e não precisam revelar informações pessoais aos provedores de serviços, como forma de garantir acesso ao recurso desejado. Neste modelo os IdPs continuam atuando como uma terceira parte confiável na interação entre usuários e SPs, contudo atuam de acordo com os interesses dos usuários e não de acordo com os interesses dos provedores de serviços (JØSANG; POPE, 2005).

A identidade de uma pessoa é composta por uma grande quantidade de informações pessoais que caracteriza essa pessoa em diferentes contextos dos quais essa faz parte (CLAUSS; KÖHNTOPP, 2001). A identidade é composta pela combinação de subconjuntos de identificadores (p.ex. número do CPF) e outras informações (p.ex. sexo), chamados de identidades parciais. Dependendo do contexto e da situação, uma pessoa pode ser representada por uma identidade parcial diferente. A identidade parcial de uma pessoa no contexto de uma universidade pode conter o número da matrícula como identificador e informações como seu nome, data de nascimento e as disciplinas que cursa. No contexto de uma empresa, a identidade pode estar associada com funções, privilégios, direitos e responsabilidades. Cabe salientar que uma mesma informação pessoal pode estar presente em diferentes identidades parciais.

Identidade eletrônica (eID) pode então ser definida como um conjunto de dados que representam uma entidade dentro de um determinado contexto (WANGHAM et al., 2010). No ambiente digital, o número de identidades que uma pessoa pode ter é maior se comparado com o mundo real, já que a Internet permite a interação entre entidades que estão geograficamente distantes. De acordo com a norma ITU-T Y.2720 (2009), uma identidade eletrônica pode consistir de:

- **Identificador:** conjunto de caracteres e símbolos ou qualquer outra forma de dados usados para identificar unicamente uma identidade;
- **Credenciais:** atesta a veracidade da identidade. Exemplo de credenciais incluem certificados digitais X.509 assinados por uma autoridade certificadora, senhas entre outras;

- **Atributos:** um conjunto de dados que descreve as características fundamentais de uma identidade. Como exemplo, o nome completo, o endereço domiciliar, a data de nascimento e papéis (roles).

Segundo a OECD (2011b), a estratégia nacional de GId deve ter como objetivo reduzir ou limitar o número de credenciais digitais que os indivíduos têm de usar em serviços do setor público e privado. Em muitos países, os cidadãos utilizam uma identidade eletrônica nacional única para acesso aos sistemas de governo eletrônico. Os cidadãos que pretendem utilizar os serviços de e-Gov podem acessar uma ampla gama de serviços on-line através de credenciais únicas que permitem que o sistema reconheça o usuário, adeque os serviços às suas necessidades e permita o rastreamento fácil e rápido do estado de transações eletrônicas. O uso de identidade única também é benéfica para o governo na medida em que permite que todas as agências, oferecendo diferentes serviços, disponham de informações confiáveis e seguras sobre os usuários. Isso reduz os trâmites burocráticos, minimiza redundâncias e replicação dentro das agências e agiliza os resultados da prestação de serviços para os cidadãos (United Nations, 2014).

No Brasil, instituído pela lei 9.454 de 1997, o projeto de Registro de Identidade Civil (RIC) foi criado com o objetivo de ser um documento de identificação único, substituindo a tradicional carteira de Identidade, CPF, título de eleitor, carteira nacional de habilitação (CNH), entre outros (MJ, 2015). Até o momento não foi definido o formato do cartão (padrão e tecnologia) RIC, por consequência também não foi definido se este cartão será utilizado para fins de identificação eletrônica. Portanto, o governo brasileiro ainda procura formas para definir a sua estratégia nacional de gestão de identidades para e-Gov. Existe apenas uma definição de padrões de interoperabilidade de sistemas (arquitetura e-PING (BRASIL, 2015)). Dentre estas, destacam-se o uso do SAML como padrão para a troca de informação sobre autenticação e autorização entre domínios, da especificação WS-Security 1.1 para o fornecimento de segurança às mensagens trocadas e WS-Trust 1.4 para a gestão das relações de confianças (intermediação).

De acordo com a OECD (2011), as estratégias nacionais de GId, geralmente adotam uma abordagem semelhante a práticas e regulamentos dos sistemas de identidades em papel (*off-line*). Por exemplo, na pesquisa da OECD, todos os países estudados que lançaram um cartão nacional de identidade eletrônica migraram este de seu cartão nacional em suporte de papel. A natureza voluntária ou obrigatória do cartão, geralmente também segue a mesma natureza do cartão em papel. Países que têm tradição em seus sistemas de registro da população nacional ou que usam identificadores nacionais estão tomando como base estes sistemas em suas estratégias de gestão de eID, por vezes,

ajustando apenas as infraestruturas existentes para a utilização eletrônica (OECD, 2011). Da mesma forma, países que já utilizam sistemas robustos de GId procuram prover a eID através de soluções utilizando identidades eletrônicas móveis, uma vez que estas soluções dispensam o uso de leitores de cartão.

Este estudo dirigido tem como objetivo descrever os conceitos sobre identidade eletrônica móvel (eID Móvel), bem como analisar as estratégias nacionais de gestão de identidades de alguns países e descrever como o modelo de eID Móvel funciona neles. O Capítulo 2 apresenta o conceito da eID Móvel e as principais características técnicas que envolvem o tema. A descrição das estratégias de IdM dos países são apresentadas no Capítulo 3. Por fim, no Capítulo 4, são apresentadas as considerações finais.

2 IDENTIDADE ELETRÔNICA MÓVEL

Dentro do cenário das estratégias nacionais de gestão de identidade, de acordo com Hansen, Schwartz e Cooper (2008), um dos problemas a ser tratado diz respeito à privacidade dos cidadãos. O grau de privacidade por sua vez é determinado pelo nível de interação que um cidadão deseja que suas informações pessoais devem ter perante o contexto no qual a identidade está inserida. Quando a interação do cidadão ocorre com um sistema nacional de gestão de identidades (SGId), a privacidade pode ser vista como a possibilidade deste cidadão determinar quais informações de sua identidade podem ser divulgadas para os provedores de serviços, optando por manter seu anonimato ou divulgando apenas os atributos pessoais que julgar adequado.

Neste contexto, a abordagem de um SGId que contribui com o direito à privacidade são os sistemas centrados no usuário, modelos estes que permitem ao cidadão permanecer fisicamente de posse de seus atributos (FELICIANO et al., 2011). Um dos modelos mais recentes adotados por países desenvolvidos em e-Gov e que implementam o modelo centrado no usuário, é o que se utilizada de um cartão de identidade eletrônica (*smart card*), no qual os atributos do usuário ficam armazenados em um *microchip*, protegidos por mecanismos criptográficos. Entretanto, para fazer uso deste *smart card* é necessário que pelo menos o usuário adquira um leitor de cartão e faça a instalação de um software específico.

Embora o uso do *smart card* seja o método mais aceito para garantir o direito à privacidade dos cidadãos, de um modo geral, esta abordagem de eID trás custos adicionais tanto para os governos ao fazer a emissão dos cartões, quanto para os cidadãos ao adquirirem os leitores de cartão, sem levar em conta o tempo para a confecção do próprio cartão. Para resolver este problema nasceu um novo conceito, o de identidades eletrônicas móveis (eID Móveis), também conhecido *Mobile eID*. As eID Móveis se referem aos atributos do usuários e às tecnologias de gerenciamento destas identidades, os quais são integrados aos dispositivos móveis do cidadão, como *tablets* e *smartphones* por exemplo. O uso de identidades móveis permite que os cidadãos possam consumir serviços, sem que sejam utilizados cartão de identidade eletrônica e com os mesmos benefícios destes, uma vez que todos os elementos (atributos, certificados de criptografia, etc) utilizados pelo cartão também estão disponíveis neste conceito.

De acordo com Krimpe (2014), a identidade móvel provê o uso da identidade eletrônica de forma simples, ao mesmo tempo que oferece um ambiente tão seguro quanto os tradicionais cartões de

banco no acesso aos provedores de serviço. Constitui-se de uma importante ferramenta para conectar cidadãos e governos, permitindo integrar diferentes serviços de forma coerente, uma vez que provê o acesso aos serviços em tempo integral de forma transparente para o usuário e de maneira eficiente.

O armazenamento dos atributos do usuário (informações pessoais) precisam ser guardados de forma segura. Geralmente, o componente que provê este meio de armazenamento em dispositivos móveis é conhecido como "elemento seguro" (*secure element* - SE), o qual normalmente realiza este armazenamento através de mecanismos criptográficos. Para (GUAUS et al., 2008), existem três categorias de SE possíveis: hardware removível, hardware não-removível e software. Portanto, dependendo da categoria o elemento seguro pode ser constituído de um *chip* de memória como um UICC (*Universal Integrated Circuit Card*), um módulo de identificação (*Subscriber Identity Module* -SIM) ou um cartão de memória interno, a exemplo do cartão SD (*Secure Digital*) e microSD. Uma abordagem de software, que também tem sido explorada para armazenamento dos atributos do usuário, é a solução baseada em nuvem. Nesta abordagem, as informações pessoais não ficam armazenadas fisicamente no dispositivo móvel e a infraestrutura funciona de maneira independente do elemento seguro.

Utilizando um dos métodos de armazenamento dos atributos do usuário, é possível utilizar o telefone móvel pessoal para identificar e autenticar o cidadão no acesso aos provedores de serviço governamental. Identificação é o processo de apresentar uma identidade a um sistema ou a uma pessoa. Autenticação visa verificar a identidade de uma pessoa. Desta forma, a identificação é o primeiro passo no processo de autenticação. A autenticação tenta assegurar que o indivíduo é realmente quem ele diz ser. Para Mantoro e Milišić (2010), nos processos de autenticação devem ser minimizadas as chances de se forjar uma identidade. Em geral, existem três formas de um humano se auto-autenticar à uma máquina (STAMP, 2011):

- Algo que você sabe (ex. senha);
- Algo que você tem (ex. *smart card* ou telefone móvel);
- Algo que você é (ex. biometria)

Com a combinação dos métodos acima descritos, a segurança de autenticação é ampliada (MANTORO; MILIŠIĆ, 2010). Muitos sistemas de autenticação estão baseados em autenticação em dois fatores, nos quais dois dos métodos são combinados (STAMP, 2011). Por exemplo, um cartão de pagamento usa autenticação em dois fatores, uma vez que os usuários precisam apresentar o cartão

(algo que você tem) e precisam inserir um PIN[1] (algo que você sabe). Ao inserir o número PIN, o usuário consegue verificar sua própria identidade, o cartão então irá responder utilizando sua chave privada para assinar digitalmente os dados do pagamento (ABBOTT; PRACTICAL, 2002).

Os cartões (*smart cards*) são capazes de armazenar com segurança dados pessoais além de executar aplicações de forma segura. Esta segurança é possível em virtude do uso de elementos criptográficos, previstos desde o design de construção do cartão (BOUDRIGA, 2009). Portanto, com o uso de *smart cards* é possível realizar o processo de identificação e autenticação, além de ser possível armazenar e executar aplicativos. Trazer esta funcionalidade dos *smart cards* ao telefone móvel simplesmente amplia as funções do próprio telefone, muitas vezes sem a necessidade de introduzir novos elementos de hardware (MANTORO; MILIŠIĆ, 2010). Entretanto, quando as funcionalidades dos *smart cards* são transferidas para os dispositivos móveis, as questões de segurança precisam ser muito bem implementadas, uma vez que estes dispositivos têm um histórico pobre quando se fala em segurança (MAYES; EVANS, 2008).

2.1 CARACTERÍSTICAS TÉCNICAS

Dentro do contexto de identidade eletrônica móvel, diversas questões técnicas são abordadas, como o armazenamento seguro dos atributos do cidadão em dispositivos de hardware e software, por exemplo. Nesta seção serão abordados os elementos mais comuns encontrados na literatura a respeito do tema.

2.1.1 Elemento Seguro

O Elemento Seguro (*Secure Element* - SE) é uma combinação de hardware, software, interfaces e protocolos embutidos em um aparelho móvel, os quais habilitam a armazenagem segura de aplicativos e atributos do usuário (REVEILHAC; PASQUET, 2009). Geralmente é utilizado para aplicações que envolvem pagamento, entretanto pode ser usado para todos os tipos de aplicativos que envolvem autenticação e requeiram mecanismos de segurança, como por exemplo o uso como identidade eletrônica móvel (*Mobile eID*) (MANTORO; MILIŠIĆ, 2010). Um SE deve ser gerenciável e ter as seguintes funções: memória segura, funções criptográficas e um ambiente seguro para execução (MADLMAYR et al., 2007). Quando múltiplos aplicativos são armazenados no SE, eles devem ser protegidos uns dos outros e os aplicativos só podem ser gerenciados por partes autorizadas

[1] Número de Identificação Pessoal (do inglês, *Personal Identification Number* é uma senha pessoal, composta por no mínimo 4 dígitos utilizada para acessar algum dado protegido

(MADLMAYR et al., 2007). Dessa forma, o elemento seguro é considerado um componente crítico, uma vez que assegura que as transações *on-line* sejam protegidas de acesso a dados sem autorização (GSMA, 2011).

2.1.2 Elemento Seguro Integrado

O SE integrado é um módulo soldado no telefone móvel, oferecendo o mesmo nível de segurança que o cartão SIM[2] (REVEILHAC; PASQUET, 2009). Como acontece com o SIM, todo aplicativo é armazenado no elemento seguro. O *chip* é integrado dentro do aparelho durante a fase de fabricação e deve ser personalizado depois que o aparelho é entregue ao usuário (EMVCO, 2007). Como o SE é soldado no telefone, ele não pode ser usado em um aparelho diferente. Isto significa que o usuário deverá personalizar seu telefone toda vez que adquirir um aparelho novo. O iPhone 6 é um exemplo de telefone móvel com um SE integrado.

2.1.3 Cartão SIM

O módulo de identificação do assinante, também conhecido por "cartão SIM", armazena os dados do usuário em seu telefone móvel pessoal, sendo utilizado para fins de identificação, autenticação e cifragem de mensagens nas comunicações através de rede de telefonia celular (TSAI; CHANG, 2006). Da mesma forma, o cartão SIM viabiliza também o uso do telefone celular como se fosse um *smart card*. Isto significa que é possível utilizá-lo com diversas aplicações de segurança, como se fosse um cartão de créditos (M'CHIRGUI, 2009; MPFI, 2008). Para MPFI (2008), o risco de sucesso de ataques direcionados à transações financeiras é reduzido com o uso de *smart cards*, por diversas razões:

1. A segurança é o principal requisito empregada na construção de *smart cards*, sendo incorporada desde o design físico e construção do circuito lógico até a escolha dos esquemas de criptografia embutidos.

2. A capacidade de adicionar elementos criptográficos nos *smart cards* permite o armazenamento chaves privadas, o que permite o uso de assinatura digital e encriptação de mensagens dentro do próprio cartão.

[2] O cartão SIM (*SIM Card*), muitas vezes referenciado como cartão GSM-SIM, é um circuito impresso do tipo *smart card* utilizado para identificar, controlar e armazenar dados em telefones celulares com tecnologia GSM (*Global System for Mobile Communications*).

3. A indústria de *smart cards* recebe incentivos para lidar com vulnerabilidades e procurar melhorar constantemente as questões de segurança, uma vez que trabalha com padrões muito específicos, voltados para documentos governamentais ou para cartão de crédito, por exemplo.

4. O uso de *smart card* está associado ao uso de códigos PIN e PUK[3], que limitam as tentativa de acesso, incrementando os fatores de segurança.

2.1.4 Cartão de Circuito Integrado Universal (UICC)

De acordo com Alimi e Pasquet (2009), o Cartão de Circuito Integrado Universal (*Universal Integrated Circuit Card* - UICC) é a próxima geração dos cartões SIM, podendo hospedar múltiplas aplicações simultaneamente. O UICC é compatível com todos os padrões de *smart card* e pode, desta forma, hospedar até aplicações não relacionadas às operadores de telefonia móvel (REVEILHAC; PASQUET, 2009). Existem domínios de segurança separados para cada aplicação, os quais estão baseados no uso de chaves privadas e administradas pelo próprio emissor do aplicativo. Como o sistema operacional no cartão impede que os aplicativos acessem ou compartilhem dados entre si (ALIMI; PASQUET, 2009), o UICC pode ser usado com segurança por vários aplicativos simultaneamente. É possível fazer o gerenciamento remotamente tanto das aplicações quanto dos dados armazenados (MADLMAYR et al., 2007). A tecnologia que permite esse gerenciamento remoto é a *Over-The-Air*[4] (OTA). Trata-se de uma tecnologia que permite atualizações e mudanças no *smart card* sem ter que reemitir os cartões (ALIMI; PASQUET, 2009). De uma forma geral, o SIM tem provado ser uma plataforma padronizada e controlável, a qual tem fornecido serviços com valor agregado sobre uma ampla variedade de aparelhos (MAYES; EVANS, 2008).

2.1.5 Micro SD

O uso do cartão micro SD é uma alternativa viável ao uso do cartão SIM, servindo também como elemento seguro em dispositivos móveis. Apesar da relevância desta solução ter diminuído ao longo dos anos, o uso do micro SD garante a implementação de um *smart card* em telefones celulares. Isto é possível, pois segundo Reveilhac e Pasquet (2009), trata-se de um cartão de memória seguro (*Secure Memory Card*), o que significa que um cartão SD está apto a funcionar como um SE.

[3] A chave de desbloqueio do PIN (do inglês, *PIN Unlock Key*) é uma combinação numérica, composta geralmente por 8 dígitos, utilizada nos casos de bloqueio dos dados do usuário, em consequência à digitação errada do PIN, normalmente por 3 vezes seguidas.

[4] Mais informações em <http://www.gemalto.com/techno/ota>

2.1.6 Solução Baseada em Nuvem

Outra opção que pode assumir o papel do elemento seguro é uma solução baseada na nuvem. O Google recentemente introduziu o *Host Card Emulation* (HCE) para o Android OS[5], oferecendo uma solução baseada na nuvem para ser utilizada ao invés de um SE físico no telefone móvel. Neste caso, o aplicativo é mantido dentro do próprio sistema operacional do telefone móvel o qual é chamado de "host" (PANNIFER DICK CLARK, 2014). Supondo um cenário em que uma pessoa utiliza o dispositivo móvel para realizar um pagamento, com uma solução na nuvem, as credenciais (atributos do usuário) a serem tocadas com o ponto de venda podem ser armazenadas e mantidas pelo próprio provedor de serviço. O aparelho deve se conectar à nuvem utilizando a internet, depois então o aparelho recebe chaves que permitem o uso do aplicativo em um ponto de venda. Estas chaves são fornecidas via uma conexão de internet e, para garantir a segurança, elas são geralmente fornecidas numa quantidade limitada e com um período de validade curto (ALLIANCE, 2014).

2.1.7 NFC

Segundo Alliance (2014), o NFC (*Near Field Communication*) é uma tecnologia de comunicação sem fio de curto alcance (extensão da norma ISO/IEC 14443[6]), utilizada para transferência de dados entre dispositivos móveis. Operando na frequência de 13,56MHz, sobre o padrão ISO/IEC 18000-3[7], oferece velocidade de comunicação entre 106 kbit/s e 424 kbit/s a uma distância teórica de 20 cm, entretanto na prática normalmente utiliza-se uma distância de aproximadamente 4 cm na comunicação entre dispositivos (MILCARZ, 2014).

A tecnologia NFC data de 1983, quando a primeira patente foi atribuída à comunicação por rádio frequência (RFID) para Charles Walton. Em 2004, as empresas Nokia, Sony e Philips se uniram para criar o Fórum NFC[8], que trata-se de uma associação (sem fins lucrativos) para estabelecer o desenvolvimento de uma tecnologia de comunicação sem contato, o NFC (MILCARZ, 2014).

De acordo com Milcarz (2014), o NFC tem dois modos de comunicação possíveis:

- **Modo de comunicação passivo:** Neste modo de comunicação, um dos dispositivos emite o sinal de radiofrequência e o segundo apenas recebe a informação. Por exemplo, um telefone

[5] Site oficial disponível em: <http://www.android.com/>
[6] Padrão de cartão de proximidade, disponível em: <http://www.openpcd.org/ISO14443>
[7] Disponível em: <http://www.iso.org/iso/catalogue_detail.htm?csnumber=53424>
[8] Near Field Communication Forum, disponível em: <http://nfc-forum.org/>

móvel (receptor) lendo uma etiqueta NFC (emissor). A transmissão ocorre quando a frequência emitida pelo receptor induz o emissor a gerar corrente elétrica, devolvendo o sinal em forma de dados.

- **Modo de comunicação ativo:** Neste modo, ambos os dispositivos geram e recebem o sinal de rádio. Um dispositivo desativa seu sinal de rádio frequência (RF) enquanto aguarda pelos dados.

Entretanto, o NFC pode operar de 3 modos diferentes em dispositivos móveis que utilizam o sistema operacional (S.O.) Android (MILCARZ, 2014):

- **Modo de Leitura/Escrita:** O dispositivo móvel pode ler informações de uma etiqueta (tag) NFC, ou enviar informações para serem gravadas na etiqueta.
- **Modo P2P:** No modo de comunicação aos pares (*Peer-to-Peer* - P2P), dois dispositivos operando com a tecnologia NFC trocam informações entre si.
- **Modo de Emulação de Cartão:** Neste modo de operação o dispositivo móvel opera como se fosse um cartão inteligente (*smart card*).

Ao operar no modo de emulação de cartão, o dispositivo móvel pode realizar transações de pagamento ou participar de processos de autenticação *on-line*, como se fosse um *smart card*. De acordo com Reveilhac e Pasquet (2009), a emulação de cartão sem contato segue a normal ISO 14443 e permite que os dados do usuário possam ser armazenados em um elemento seguro.

2.1.8 Emulação de Cartão Baseado em Host

De acordo com Milcarz (2014), a emulação de cartão baseado em host (*Host-based Card Emulation* - HCE), é um método para representar um *smart card* baseado em software. O termo HCE foi criado em 2011 pelos fundadores da SimplyTapp[9], Doug Yeager e Ted Fifelski. Era uma tecnologia dependente do sistema operacional Android da Google, entretanto, somente em 2013 o Android adotou oficialmente o HCE, com a versão 4.4[10] deste sistema operacional (MILCARZ, 2014).

A principal diferença entre a emulação de cartão, modo de operação oferecido pela tecnologia NFC, e a emulação de cartão baseada em host (HCE) do Google, está na forma de armazenamento dos

[9] <https://simplytapp.com/about-simplytapp/>

[10] Versão do Android de codinome KitKat. Maiores informações disponíveis em: <https://www.android.com/versions/kit-kat-4-4/>

dados do usuário. Enquanto a primeira tecnologia depende do elemento seguro, a segunda utiliza o modo de armazenamento baseado em software, que segundo Milcarz (2014) pode ser utilizada uma infraestrutura baseada em nuvem. A figura 1 ilustra as duas tecnologias.

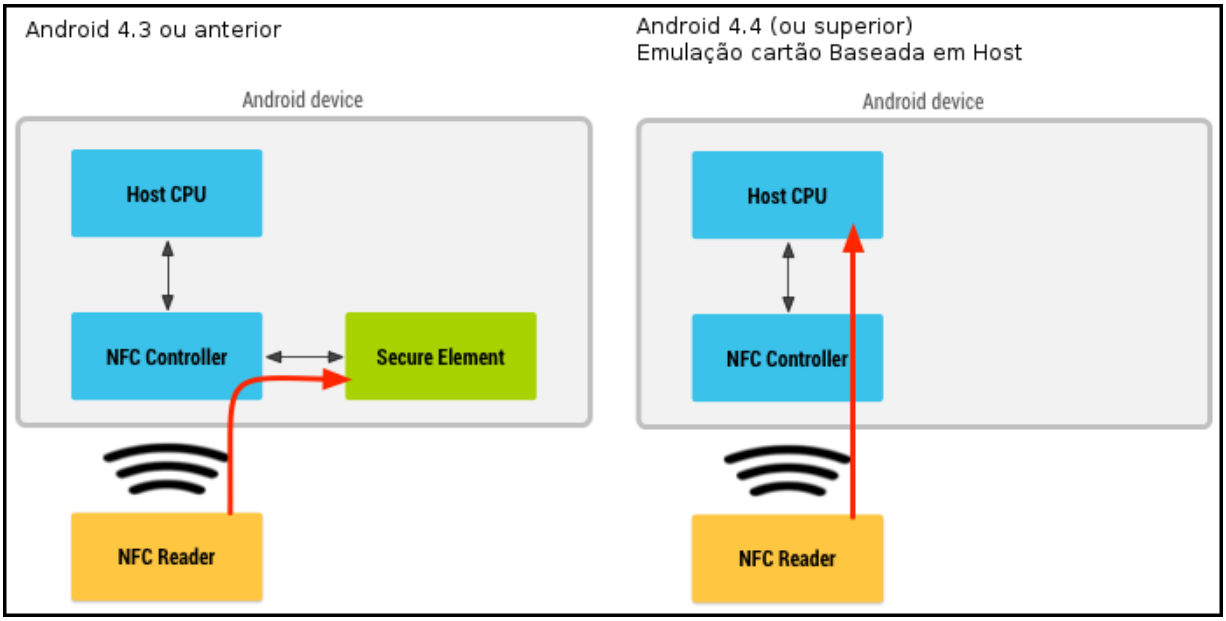

Figura 1: Emulação de Cartão e HCE

De acordo com Alliance (2014), este modo de emulação de cartão permite permite também que os dados sensíveis dos usuários possam ser armazenados em uma infraestrutura baseada em software no próprio telefone do portador. Em outras palavras, operar no modo HCE ou no modo de emulação de cartão habilita o telefone móvel do cidadão a funcionar como uma eID Móvel, podendo ser utilizado por exemplo para autenticação em ambiente de governo eletrônico.

3 ESTRATÉGIAS NACIONAIS

Cada país que implementou alguma estratégia de gestão de identidade para governo eletrônico, o fez em conformidade com leis vigentes, levando em conta questões culturais e sócio-econômicas, particulares de cada lugar. Entretanto, os países mais evoluídos em e-Gov, segundo levantamento da ONU em 2014, demonstram que suas políticas de governo eletrônico bem como as estratégias de eID vem sofrendo alterações ao longo dos anos. Nesta seção serão apresentados alguns países que adotaram o conceito de eID Móvel como uma de suas estratégia de gestão de identidade, bem como será descrito o modelo de eID adotado.

3.1 ALEMANHA

Na Alemanha, o processo de identificação e autenticação eletrônica é feito por meio de um cartão de identificação eletrônico (*eID Card*), que entrou oficialmente em funcionamento no dia primeiro de novembro de 2010. Com o formato de um cartão de crédito, o *eID Card* possui um *microchip* que permite interações tanto com empresas privadas quanto com sistemas *on-line* de e-Gov, servindo também como documento de identidade civil (COMISSION, 2014c).

Para utilizar o *eID Card*, o cidadão deverá adquirir um leitor de *smart card* homologado pelo governo e instalá-lo em seu computador pessoal (INNERN, 2014a), bem como obter o software conhecido como "AusweisApp[1]", disponibilizado pelo Departamento Federal de Segurança da Informação (BSI). Este software foi totalmente reformulado em 2013, sendo disponibilizado em sua nova versão a partir de janeiro de 2014. O desenvolvimento da nova versão focou na usabilidade e na portabilidade, tornando-o mais fácil de usar e permitindo também sua instalação nos sistemas operacionais Android e iOS (SECURITY, 2015).

O novo cartão de identificação civil foi projetado para ser utilizado também na identificação eletrônica do cidadão alemão. O *microchip* incluso no *eID Card* contém todas as funcionalidades necessárias para este uso, entretanto, o portador deste novo cartão deve expressar por escrito sua intenção de utilizar ou não a funcionalidade eletrônica, cabendo à entidade emissora habilitar ou desabilitar o recurso.

Todos os atributos do cidadão gravados no *microchip* do documento de identidade civil são

[1] <https://www.ausweisapp.bund.de/ausweisapp2/>

considerados atributos válidos para uso pela identidade eletrônica. No entanto, as informações pessoais que serão enviadas aos provedores de serviços são apresentadas ao usuário, de forma que este possa aprovar ou não o envio destes dados. A aprovação é feita somente com a digitação do número de identificação pessoal (PIN) e os dados são sempre transmitidos por meio de canais de comunicação criptografados (INNERN, 2014b).

O portador do cartão tem direito por lei de ativar ou desativar a função de identidade eletrônica (eID), através de solicitação por escrito à autoridade emissora. Esta solicitação pode ser feita a qualquer momento durante o período de validade do documento de identidade civil. A excessão é para cidadãos menores de 16 anos, para os quais a função de identificação eletrônica deve obrigatoriamente ser cancelada. Casos de perda ou roubo devem ser comunicados imediatamente à entidade emissora, a qual fará a inclusão deste identificador em uma lista de revogação, replicando esta lista para todos os provedores de serviços (VERBRAUCHERSCHUTZ, 2014).

Cada cidadão pode apenas ter um único *eID Card*, uma vez que ele está vinculado ao documento de identificação civil. O referido eID tem validade igual a do documento de identificação civil (VERBRAUCHERSCHUTZ, 2014), sendo de 10 anos para cidadãos com idade superior a 24 anos e 6 anos de validade para cidadãos com idade inferior a 24 anos (INNERN, 2014c). A emissão é feita pela empresa privada Bundesdruckerei [2], contratada pelo governo em 2010 para produzir os cartões de identificação eletrônica (*eID Card*) em nome do Ministério Federal do Interior (IMC). Os cartões são produzidos de forma centralizada e sob a supervisão do Serviço Federal de Segurança da Informação e da Delegacia da Polícia Criminalista Federal.

Entretanto, a Constituição alemã não permite o uso de um número de identificação único para cada cidadão, por consequência, para que o governo eletrônico possa ser realizado, o cidadão é identificado pelos provedores de serviços a partir de uma combinação de alguns dados pessoais, como por exemplo o nome, sobrenome, data e local de nascimento (COMMUNITIES, 2009b). Cabe ao provedor de identidades a única tarefa de confirmar a identidade do cidadão e fazer o transporte dos atributos do cartão de identidade para o SP.

Partindo desta premissa, o Departamento Federal de Segurança em Tecnologia da Informação (BSI) criou uma série de normas técnicas[3] para os provedores de serviços implantarem seus próprios provedores de identidade, ou *eID-Servers*, como são conhecidos no país.

[2] https://www.bundesdruckerei.de/en

[3] <https://www.bsi.bund.de/ElektronischeAusweiseTR.html>

A norma conhecida como "Orientação Técnica BSI TR-3130[4]" trata especificamente dos requisitos necessários para a operação dos provedores de identidades. Ela descreve a forma com que os IDPs devem ser implementados para que possam estar em conformidade com padrões de comunicação existentes, garantindo que eles operem segundo os requisitos de segurança vigentes. A norma citada está dividida em duas partes:

1ª parte: Especificações funcionais;

2ª parte: Estrutura de segurança para a operação do *eID Server* (IdP).

Por permitir o uso de diversos provedores de identidades e manter os atributos pessoais com o próprio cidadão, a Alemanha estabeleceu como padrão de gestão de identidade o **Modelo Federado e Centrado no Usuário**.

3.1.1 eID Móvel - Alemanha

Em novembro de 2010 o governo da Alemanha iniciou a distribuição do novo cartão de identidade equipado com *microchip* sem contato (POLLER et al., 2012), o que permitiu seu uso para identificação e autenticação nos provedores de serviço. Para que este cartão pudesse ser utilizado como identificador eletrônico, o governo disponibilizou gratuitamente o software "AusweisApp" para ser utilizado como cliente nos computadores (SECURITY, 2015) e o software "MONA" (*Mobile usage of the new German identity card*) para ser utilizado pelos dispositivos móveis (HORSCH JOHANNES BRAUN, 2011). De acordo com CASED (2011), MONA constitui-se de uma aplicação Java ME (*Java Micro Edition*) desenvolvida inicialmente para o telefone celular Nokia 6212, porém facilmente portada para qualquer outro modelo.

A infraestrutura do modelo de gestão de identidade alemã é composta por padrões de comunicação e segurança definidas pelo "German Federal Office for Information Security (BSI)", modelo este que não permite mudanças ou otimizações dos protocolos adotados, uma vez que isto ocasionaria necessidade de modificar também outros elementos, como o próprio provedor de identidades. Portanto, a construção dos módulos da aplicação MONA (*MONACore*, *MONAClient* e *MONALocalClient*) inclui

[4] <https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03130/tr-03130.html>

implementação de protocolos adotados pelo BSI, como por exemplo: PACE/EAC[5], PAOS[6], SOAP[7], e TLS[8] (HORSCH JOHANNES BRAUN, 2011). A figura 2 apresenta a arquitetura do MONA e os protocolos utilizados na comunicação do *eID Card* com o IdP (*eID Server*).

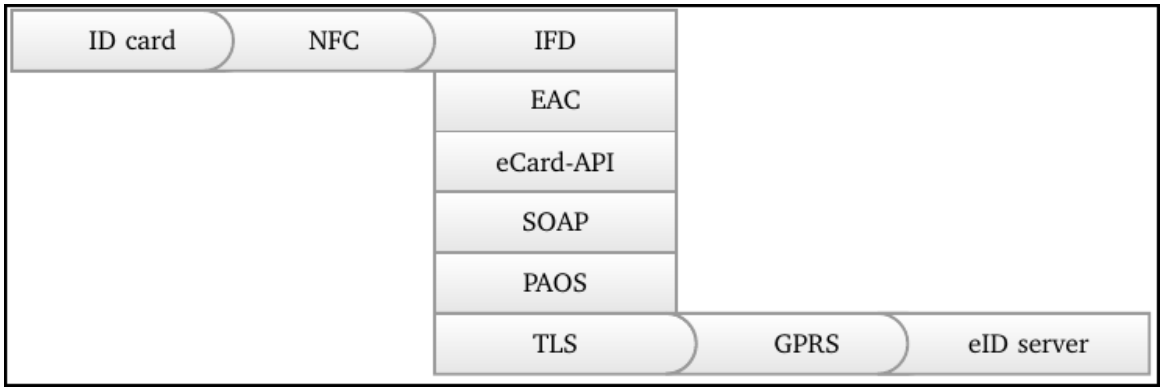

Figura 2: Arquitetura do MONA

A operação tradicional do eID depende de um leitor de cartões, o qual é instalado no computador do cidadão juntamente com o software AusweisApp. De maneira similar, a tecnologia NFC presente em alguns dispositivos móveis, os habilitam a operar como um leitor de cartões sem contato, assim como o aplicativo MONA opera de modo semelhante ao aplicativo para computador (HORSCH JOHANNES BRAUN, 2011). Esta combinação de tecnologias habilita os dispositivos móveis a atuarem no modelo de eIDM alemão, conforme demonstrado pela figura 3, porém fazendo uso dos atributos do cidadão presentes no *eID Card*.

Conforme citado por Horsch Johannes Braun (2011), o MONA foi a primeira solução de eID Móvel oferecida no país. Através desta solução, o cidadão passou a contar com todos os benefícios oferecidos pelo sistema de eID alemão, sem a necessidade de compra dos tradicionais leitores de cartão (HORSCH JOHANNES BRAUN, 2011).

Em 2014, o BSI começou a projetar uma nova versão do AusweisApp que foca na usabilidade e portabilidade. Com esta versão será possível instalá-lo em outros sistemas operacionais, como o Android e o iOS. Com lançamento previsto para o segundo semestre de 2015, se tornará a segunda solução de eID Móvel do país (SECURITY, 2015).

---

5 O PACE (*Password Authenticated Connection Establishment*) e o EAC (*Extended Access Control*) são especificados na TR-03110, disponível em: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/TR-03110_v205_pdf>

6 <http://www.projectliberty.org/liberty/content/download/909/6303/file/liberty-paos-v2.0.pdf>

7 <http://www.w3.org/TR/2000/NOTE-SOAP-20000508>

8 <http://www.ietf.org/rfc/rfc4346.txt>

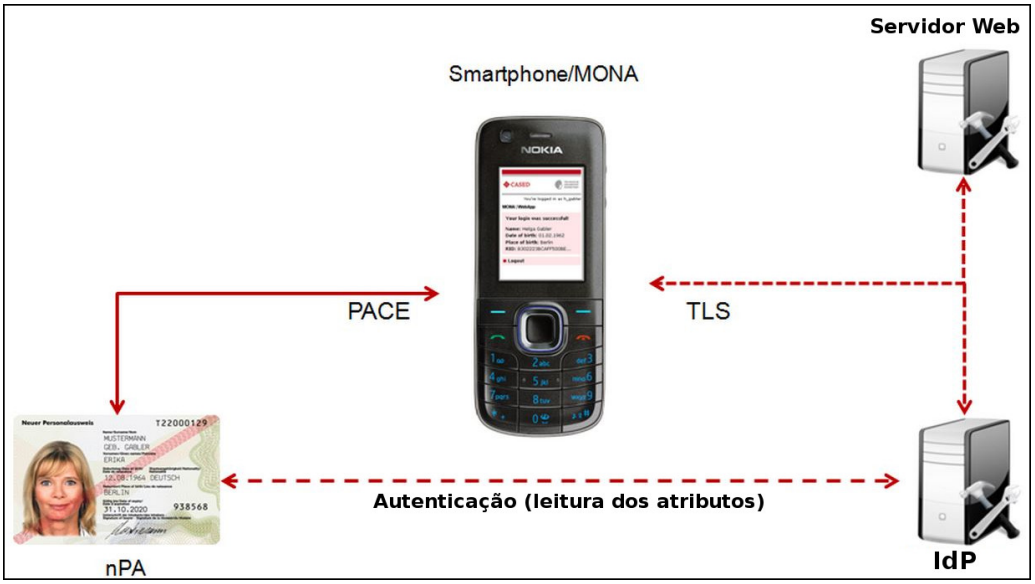

Figura 3: MONA - Cliente eID

3.2 ÁUSTRIA

Na Áustria o Governo Municipal local é o órgão responsável pelo cadastro e emissão dos registros de nascimento e casamento dos cidadãos austríacos. Todos os registros anteriores a 2002 eram feitos em uma Base Local de Registro de Residentes (*Local Resident Registers*[9]), conhecida por LMR. Mas, em março de 2002, o "Registro Central de Residentes[10] (CRR - do inglês *Central Residents Register*)" entrou em operação, de forma que todos os registros de nascimento e casamento das pessoas nascidas no país passaram a ser armazenados em uma base de dados centralizada, criada pelo próprio governo austríaco (COMISSION, 2014a). Como consequência desta base centralizada, passa a ser atribuído a todo cidadão austríaco o Id_{CRR}, que é um identificador único composto por 12 caracteres decimais randômicos (40 bits) (ZWATTENDORFER; TAUBER; ZEFFERER, 2011a).

Ao se criar a identidade eletrônica para o cidadão austríaco é utilizado o identificador civil (Id_{CRR}), garantindo dessa forma, que não haverá mais de um eID para o mesmo cidadão. No entanto, o uso deste Id está sob restrições específicas de proteção de dados, as quais impedem seu uso direto nos processos de governo eletrônico. Neste contexto, a Autoridade de Registro sourcePIN (SRA - *sourcePIN Register Authority*) exerce fundamental papel, sendo responsável por criptografar o Id_{CRR}. Com o processo de criptografia, é gerado um novo número de 128 bits conhecido por sourcePIN que é armazenado em um cartão, denominado "cartão do cidadão" (*citizen card*) (ZWATTENDORFER; TAUBER; ZEFFERER, 2011a).

[9] Em alemão *Lokales Melderegister*
[10] Em alemão *Zentrales Melderegister* (ZMR) - <http://zmr.bmi.gv.at/>

O cartão do cidadão é um conceito de tecnologia neutra que aceita diferentes soluções técnicas, permitindo que o cidadão possa, por exemplo, utilizar uma solução em cartão no formato de *smartcard* e outra como aplicativo no *smartphone* (BüRGERKARTE, 2014). O cartão começou a ser emitido em 2005 pelas operadoras de plano de saúde, para todos os cidadãos austríacos. Em 2007, a empresa pública *Main Association of Social Insurance Organisations*[11] passou a cuidar da emissão destes cartões. Em 2008, foi permitido que a empresa privada A-Trust[12] também se tornasse um emissor de cartões, ampliando os tipos de cartões aceitos. Atualmente, para que possam ser utilizados para autenticação nos SPs, os *smartcards* devem possuir as "funcionalidades de cartão do cidadão", o que efetivamente é feito pelos cartões emitidos pela A-Trust.

De forma a viabilizar o uso do cartão do cidadão, foi criado o "*identity link*". Trata-se de uma estrutura SAML, emitida pela Autoridade de Registro sourcePIN (SRA) e gravada no cartão, e que contém as seguintes informações:

- o sourcePIN,
- o nome do cidadão e sua data de nascimento,
- os dados que ligam o *identity link* ao certificado qualificado do cidadão, e
- a assinatura da SRA.

Entretanto, as leis de proteção de dados[13] proíbem aos SPs públicos ou privados armazenar ou fazer uso direto do sourcePIN. Para contornar esta questão, o governo da Áustria prevê o uso de uma identificação baseada em modelo setorial. Este modelo preserva a privacidade do usuário ao impedir que provedores de serviço possam rastrear as atividades do usuário através de diferentes domínios administrativos. Entende-se por domínio administrativo, o conjunto de SPs disponibilizados pelo mesmo Ministério, Departamento, Secretaria ou Entidade Privada. Na prática cada SP gera um novo código criptografado e exclusivo (160 bits) a partir do sourcePIN, denominado ssPIN (*sector-specific PIN*). Este processo criptográfico garante que não se possa reproduzir o sourcePIN a partir do ssPIN, impedindo assim o rastreamento do usuário entre domínios administrativos diferentes (ZWATTENDORFER; TAUBER; ZEFFERER, 2011a).

Tecnicamente o processo de geração do ssPIN é feito através de dois *middlewares*, um do lado da aplicação do usuário (CCS - *client-side middleware*) e outro acoplado ao provedor de serviços (*open*

[11] <http://www.sozialversicherung.gv.at>
[12] <http://www.a-trust.at>
[13] Lei publicada em 2000, em conformidade com a diretriz de proteção de dados da comunidade europeia 95/46/EC.

source MOA-ID). Ao fazer a requisição de acesso ao SP (passo de identificação), o usuário aciona o MOA-ID, que por sua vez envia instruções ao CCS para leitura do *identity link* do cartão do cidadão, capturando o sourcePIN, o nome e data de nascimento do cidadão. De posse destas informações o MOA-ID calcula o ssPIN. O usuário então recebe uma tela de texto para confirmar o acesso ao SP (processo de autenticação). Uma vez confirmada a intenção de acessar o serviço, o MOA-ID monta em formato SAML uma asserção contendo as informações de identificação do usuário e a transfere para a aplicação on-line (SP), que por sua vez libera o acesso do usuário (ZWATTENDORFER; TAUBER; ZEFFERER, 2011a).

Os Módulos para Aplicação On-line (MOA - *Modules for online applications*) são componentes de software, desenvolvidos pelo governo da Áustria, para auxiliar na implementação das estratégias de governo eletrônico. Algumas de suas funcionalidade incluem: verificação de assinaturas eletrônicas, leitura dos dados de identificação do cartão do cidadão e implementação de funções de segurança (AUSTRIA, 2015).

Desde junho de 2005, o MOA é disponibilizado em software de código aberto e distribuído gratuitamente, o que permite seu desenvolvimento de forma colaborativa e continuada, servindo como uma importante ferramenta de e-Gov para qualquer nação que deseje adotá-lo. O *E-Gov:Labs*[14] é o portal *on-line* disponibilizado pelo governo da Áustria, como um local central de contato entre as pessoas interessadas no software, oferecendo uma visão geral sobre o funcionamento de cada um dos módulos desenvolvidos. O download dos módulos foi disponibilizado na plataforma *Joinup*[15] da Comissão Europeia, a qual constitui-se de uma plataforma criada para assegurar a interoperabilidade entre os países europeus (AUSTRIA, 2015).

Resumidamente, o governo eletrônico na Áustria é baseado em um modelo seguro e com uso do IdP centralizado no governo, modelo este preocupado com questões de privacidade relacionados à autenticação e autorização (ZWATTENDORFER; TAUBER; ZEFFERER, 2011b). Neste modelo a figura principal é o "cartão do cidadão", o qual armazena o identificador civil (Id_{CRR}) em um formato criptografado, denominado sourcePIN. Para garantir a interoperabilidade do modelo, os "Módulos para Aplicação On-line" (MOA) foram adotados, trazendo diversos benefícios, entre eles a facilidade da autenticação única SSO (*Single Sign On*).

[14] <http://egovlabs.gv.at/>
[15] <https://joinup.ec.europa.eu/software/moa-idspss/home>

3.2.1 eID Móvel - Áustria

Preocupada com a adoção de um modelo de gestão de identidade eletrônica que fosse interoperável, a Áustria desenvolveu um novo modelo de cartão do cidadão baseado em telefone móvel (Identidade Eletrônica Móvel), o qual chamou de *Mobile Phone Signature*. Esta solução em eID Móvel foi desenvolvida com o suporte da Comissão Europeia em um grande projeto piloto de interoperabilidade para identidades eletrônicas chamado "Projeto STORK". A solução foi disponibilizada à população no final de 2009, como alternativa ao uso do *smartcard* (COMISSION, 2014a).

As formas de ativação da identidade eletrônica no celular são semelhantes às do *smartcard*. Entretanto, esta forma de uso do cartão do cidadão difere do modo tradicional pelo fato de não requerer a aquisição de um leitor de cartão, o que a torna todo o processo de autenticação ao SP mais simples. Para ativar a funcionalidade de cartão do cidadão, uma das seguintes opções gratuitas podem ser utilizadas pelos cidadãos (BüRGERKARTE, 2014):

- De forma *on-line* no site a A-Trust[16],
- Através do site FinanzOnline[17] do governo,
- Pessoalmente, em um dos 135 locais de registro[18] na Áustria, apresentando documento de identificação com foto, ou
- Através de solicitação por correio com uso de carta registrada.

Como forma de facilitar a adoção das soluções de cartão do cidadão foi criado o portal "www.buergerkarte.at/en", que reúne informações sobre a ativação e uso do *smartcard* e da eID Móvel em um só lugar. Com o principal objetivo de fornecer conteúdo técnico focado em segurança para as autoridades públicas, empresas e cidadãos, este portal foi desenvolvido pela A-SIT[19], uma associação sem fins lucrativos localizada na sede da Polícia Federal em Viena.

3.3 ESPANHA

O Documento de Identidade Civil, conhecido no país por DNI (*Documento Nacional de Indentificación*), foi instituído na Espanha pelo decreto de 2 de março de 1944, e poderia ser emitido

16 <https://www.a-trust.at/e-card/selfdata.aspx>
17 <https://finanzonline.bmf.gv.at/>
18 <http://www.buergerkarte.at/en/registration-authorities.html>
19 www.a-sit.at

para cidadãos maiores de 16 anos. Posteriormente, um novo decreto, de número 196 de fevereiro de 1976, determinou que o DNI deveria ser obrigatoriamente emitido para cidadãos maiores de 14 anos e passaria a contar com uma foto colorida do portador (POLICíA, 2015a).

Em março de 2006 é lançado oficialmente o Documento de Identidade Civil Eletrônico (DNIe), passando a substituir o DNI tradicional (COMISSION, 2014d). Com o formato de um cartão de crédito (*eID Card*), sua emissão é feita de forma centralizada pela Direção Geral da Polícia[20], órgão vinculado ao Ministério do Interior (POLICíA, 2015a). A principal inovação do DNIe em relação ao DNI tradicional é a existência de um *chip* capaz de armazenar as informações com segurança e processá-las internamente. Para incorporar este *chip*, o DNI trocou seu formato tradicional em "papel cartão plastificado" para um cartão de material plástico que tem novas e melhores medidas de segurança (COMMUNITIES, 2009c). O novo cartão fabricado com um material resistente de alta qualidade e durabilidade permitiu a impressão de dados à laser, de forma a impossibilitar a falsificação da impressão (POLICíA, 2015a).

Sendo o DNIe um documento pessoal, ele é utilizado para atestar a identidade bem como os dados pessoais do portador. Dessa forma, ele é valido por um período de tempo após a sua emissão, o qual dependerá da idade do cidadão, conforme segue (POLICíA, 2015a):

- **2 anos:** para crianças menores de 5 anos.
- **5 anos:** para pessoas de até 30 anos.
- **10 anos:** para cidadãos maiores que 30 anos e menores que 70 anos.
- **Permanente:** quando o titular completar 70 anos de idade.

Por ser utilizado também como documento de identidade civil, a emissão do *eID Card* (DNIe) é obrigatória para todo cidadão espanhol maior de 14 anos, entretanto a ativação da funcionalidade eletrônica é voluntária[21] (COMMUNITIES, 2009c). Quando solicitado pela primeira vez, a presença física da pessoa é requerida, bem como a apresentação de uma certidão de nascimento, emitida há no máximo 6 meses pelo Escritório de Registro Civil. Para a renovação, é necessário comparecer pessoalmente a um escritório da Polícia, dentro dos últimos 90 dias de validade do DNIe e apresentar

[20] http://www.policia.es/

[21] O Decreto Real nº 1553/2005, de 23 de Dezembro, que regula a identificação eletrônica, no artigo 9º, parágrafo 2º, estabelece que a ativação do uso do computador (identificação eletrônica do titular e a capacidade de assinar documentos de forma eletrônica) seja voluntária.

os mesmos documentos requeridos na primeira solicitação, além de apresentar o DNIe que está por vencer (POLICíA, 2015a). Na emissão do DNIe, além das informações visíveis impressas à laser, os seguintes dados do portador também são gravados no *chip* (COMMUNITIES, 2009c):

- Detalhes de filiação,
- Imagem digitalizada da foto,
- Imagem digitalizada da assinatura manuscrita,
- Impressões digitais,
- Certificado digital de autenticação e assinatura,
- Certificado digital da autoridade emissora, e
- Códigos "PIN" para cada certificado eletrônico.

Em 19 de setembro de 2014, um conselho de ministros aprovou um acordo para a criação do "Cl@ve[22]", uma nova plataforma para identificação, autorização a assinatura eletrônica a ser utilizada pela Administração Pública. Seu principal objetivo é permitir ao cidadão se identificar mediante a apresentação de chaves combinadas (usuário e senha), sem que para isto precise memorizar credenciais diferentes para cada Provedor de Serviço (PRESIDENCIA, 2014). A implementação da plataforma Cl@ve está sendo feita de forma gradual nos provedores de serviços governamentais, com previsão de disponibilidade do serviço em todos provedores de serviço antes de 1 de Outubro de 2015 (ADMINISTRACIONES, 2014). Com a implementação desta nova plataforma, os cidadãos passam a contar com duas formas de autenticação nos sistemas de e-Gov, uma utilizando o DNIe e outra utilizando a plataforma Cl@ve.

O modelo de gestão do eID adotado com relação ao DNIe é baseado em uma infraestrutura de chave pública privada, para a qual é permitida a participação de entidades públicas e privadas, que atuam como Provedores de Serviço de Certificação (CSP). Para operarem, estes CSPs são homologados pelo governo e, uma vez autorizados, passam a oferecer certificados digitais para os cidadãos, de forma que estes possam interagir com os sistemas de e-Gov (POLICíA, 2015a).

Entretanto, para o DNIe possa ser utilizado, é necessário que os SPs públicos realizem modificações técnicas para aceitarem este *eID Card* como elemento de autenticação e assinatura nos

[22] <http://clave.gob.es/>

processos de comunicação eletrônica com o governo. Diante deste contexto, o Ministério da Fazenda e Administrações Públicas (MINHAP) lançou um serviço chamado "@firma[23]" para atuar como uma espécie de Provedor de Identidades, o qual é responsável unicamente por verificar o estado e validade dos certificados digitais utilizados pelos cidadãos (POLICíA, 2015a).

Resumidamente, o Sistema de Identidade Eletrônica na Espanha, baseado no Documento Nacional de Identidade Eletrônica (DNIe), estabeleceu como modelo de gestão de identidades o Modelo Federado, para o qual o certificado digital de autenticação é o responsável por confirmar a identidade do cidadão. O cidadão tem a opção de escolher qual será seu provedor de certificados, diante de uma lista, composta por diversas entidades públicas e privadas homologadas pelo governo. A figura central deste modelo é a plataforma de validação "@firma" do Ministério da Fazenda e Administrações Públicas, a qual permite verificar o estado e validade dos certificados eletrônicos, utilizados pelos usuários nas transações eletrônicas.

3.3.1 eID Móvel - Espanha

Com o lançamento da versão 3.0 do DNIe em janeiro de 2015, o Ministro do Interior apresenta o novo Documento Nacional de Identidade Eletrônico, adequado ao uso com a tecnologia sem contatos (*Near Field Communication* - NFC) uma vez que este novo *eID Card* possui uma TAG NFC[24], que permite a leitura do cartão bastando apenas aproximá-lo do terminal de leitura (ABC, 2015).

Segundo afirmado por Policía (2015b), a incorporação da tecnologia NFC na nova versão do DNIe possibilita o uso em dispositivos móveis como *smartphones* e *tablets*. Entre os ganhos mais imediatos está a facilidade de acesso aos provedores de serviço, como por exemplo: serviços de email, assinatura de mensagens e entrega de medicamentos, quando existe uma receita eletrônica e o doente não pode ir até a farmácia retirá-la (POLICíA, 2015b). Em outras palavras, o uso da tecnologia NFC no modelo de gestão de identidades permitiu o nascimento da identidade eletrônica móvel no país.

Dentro deste conceito de eID Móvel, foi projetado um *middleware* para a permitir a comunicação entre o dispositivo móvel e o *eID Card*, conhecido por "DNIeDroid". Esta aplicação exige o uso do DNIe para os processos de autenticação nos SPs. Operando em conjunto com plataformas Java, o DNIeDroid oferece uma plataforma de alto nível, podendo operar tanto com sistemas operacionais Android quanto iOS. A figura 4 exemplifica o uso do DNIe, a partir de um dispositivo móvel, no acesso

[23] <http://firmaelectronica.gob.es/>
[24] <http://www.nxp.com/documents/other/R_10014.pdf>

aos provedores de serviço (TARJETAS, 2015).

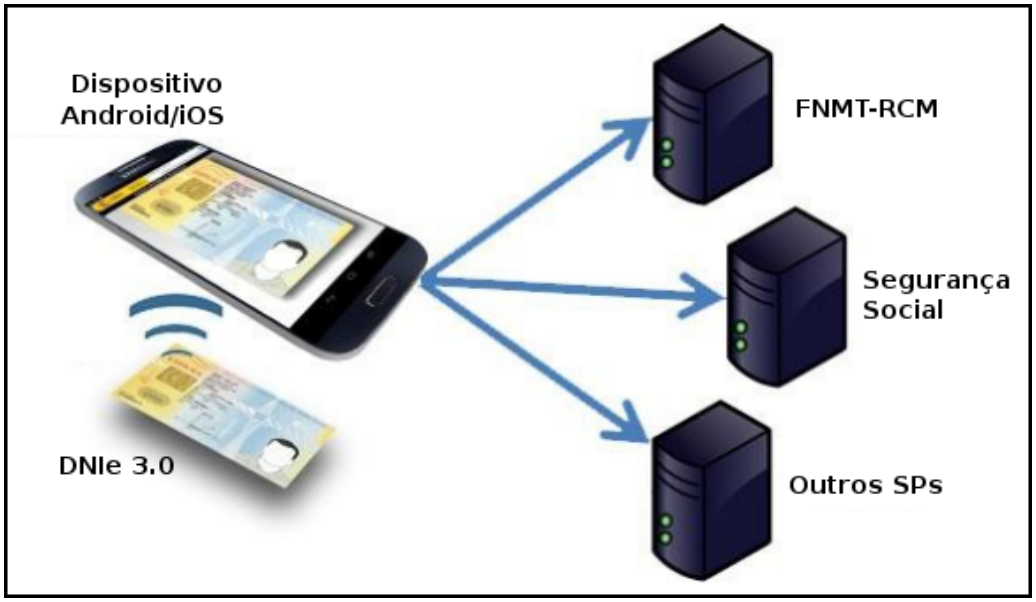

Figura 4: Arquitetura DNIe - Espanha

O uso do DNIe exige do cidadão o uso de uma senha PIN (*Personal Identification Number*) nos processos de autenticação *on-line* e toda comunicação é feita por canais criptografados. Entretanto, somente com o lançamento da versão 3.0 é que foi possível utilizar o fazer uso da identidade eletrônica em dispositivos móveis.

3.4 ESTÔNIA

Para cada novo registro de nascimento emitido na Estônia é gerado um "Número de Registro Civil" único, conhecido por IK (*isikukood*). Fornecido pelo Centro de Registro e Sistemas da Informação da Estônia[25], o IK é utilizado pelos cidadãos no processo de criação do documento de identidade civil (*ID Card*), bem como nas interações com os sistemas de governo eletrônico. Constitui-se de uma sequência de 11 dígitos decimais, formado pela estrutura **GYYMMDDSSSC**:

- **G:** século de nascimento e sexo,
- **YY:** ano,
- **MM:** mês,
- **DD:** dia,

[25] https://ariregister.rik.ee

- **SSS:** número sequencial de nascimento[26],
- **C:** dígito verificador (*checksum*).

O documento de identidade civil estoniano é composto de um cartão de identificação eletrônico (*ID Card*), o qual possui um chip eletrônico que armazena um par de chaves criptográficas utilizadas para assinatura de documentos. Esta característica permitiu o uso deste documento de identidade no processo de votação eletrônica[27] através da Internet, processo este que teve início em 2005 (COMISSION, 2014b). Segundo a lei, todos os cidadãos maiores de 15 anos e residentes estrangeiros são obrigados a ter um cartão de identificação (EU, 2012).

Os primeiros cartões de identificação foram emitidos em 2002 e são atualmente administrados pela Polícia estoniana, conhecida no país por *Politsei- ja Piirivalveamet*. Através de uma parceria entre os setores público e privado, os cartões são emitidos com certificados digitais, os quais garantem a segurança nas transações eletrônicas (ESTONIA, 2003). O uso do *ID Card* é diversificado, servindo como cartão de identificação civil, documento de viagem, cartão bancário, voto eletrônico e provendo acesso aos sistemas *on-line*, sendo também utilizado para visualização de histórico médico do seu portador (desde 2010) (COMISSION, 2014b).

O (*ID Card*) constitui-se do principal elemento no sistema de gerenciamento de identidades para governo eletrônico da Estônia, muito embora existam outras 2 soluções atualmente em uso: o eID Móvel e o Digi-ID. Todas as soluções ligam o usuário ao Número de Registro Civil (IK), garantindo assim a identidade única do cidadão no uso dos sistemas de e-Gov. A adoção de uma solução à outra, dependerá exclusivamente da escolha feita pelo cidadão. Entretanto, a obrigatoriedade de emissão do *ID Card* constitui-se tão somente para a função de Identidade Civil, sendo voluntária a adoção das características do cartão como Identidade Eletrônica. Por este motivo, o cidadão pode solicitar a revogação dos certificados digitais, suspendendo assim as funcionalidades de uso como identificador eletrônico (ESTONIA, 2003).

A solução de cartão de Identidade Digital ou "Digi-ID" constitui-se de um cartão no formato de *smart card*, que tem por finalidade exclusiva a autenticação do usuário nos sistemas *on-line*, bem como para assinar documentos eletronicamente. Este cartão não pode ser utilizado como documento de identificação civil, como é o caso do *ID Card*, tendo seus certificados digitais válidos por 3 anos

[26] Número que demonstra a sequência de nascimentos ocorridos no mesmo dia

[27] A Estônia foi o primeiro país do mundo a implantar o voto através da Internet. Na votação ocorrida em 2007, 30.000 eleitores puderam registrar seu voto e em 2014, mais de 30% dos cidadãos estavam aptos a registrar seu voto pela Internet

apenas, ao contrário do *ID Card* que é de 5 anos. A vantagem do "Digi-ID" é sua emissão imediata, ou seja, ao solicitar o cartão, o cidadão o recebe imediatamente, diferentemente do *ID Card* que demora entre 2 a 4 semanas para ser emitido. Isto permite ao cidadão a continuidade no acesso aos sistemas *on-line*, independentemente da perda, roubo ou dano do *ID Card* (ESTONIA, 2015).

O modelo de Gestão de Identidades adotado no país é centralizado, tendo como elemento central o Centro de Certificação (SK - *AS Sertifitseerimiskeskus*), atuando como emissor dos certificados digitais, ao mesmo tempo que promove a validação dos mesmos através do serviço baseado no OCSP (*Online Certificate Status Protocol*). O OCSP é um sistema cliente-servidor, descrito pela RFC 2560[28], que verifica o certificado do usuário, devolvendo para a aplicação cliente uma das seguintes respostas, as quais servem para autorizar ou não o acesso do usuário (SERTIFITSEERIMISKESKUS, 2014b):

- Certificado válido;
- Certificado não válido;
- Nenhuma informação do certificado. encontrada.

O Centro de Certificação Estoniano, que também é parceiro do projeto STORK, opera emitindo os certificados digitais para as todas soluções de Identidade Eletrônica no país (*ID Card*, eID Móvel e Digi-ID). Este Centro também criou o software básico para uso com o cartão, além de desenvolver o software DigiDoc, o qual provê os seguintes serviços: assinatura digital, validação da assinatura eletrônica e encriptação de dados (STORK, 2014).

Conforme descrito por Sertifitseerimiskeskus (2014a), os termos de uso do Centro de Certificação SK determinam o funcionamento deste provedor em consonância com os requisitos estabelecidos na Lei de Proteção dos Dados Pessoais, garantindo ainda a mudança de comportamento caso a Lei ou a Legislação de Privacidade venham a sofrer alteração. Informa ainda que quaisquer alterações introduzidas nos Princípios de Proteção do Dados serão informados aos usuários, com pelo menos 1 mês de antecedência à mudança.

3.4.1 eID Móvel - Estônia

Em 2007 o serviço de eID Móvel, conhecido no país por *Wireless PKI*, foi iniciado como alternativa ao uso do *ID Card* (COMMUNITIES, 2009a). Este serviço é oferecido através de um

[28] <https://www.ietf.org/rfc/rfc2560.txt>

operador de serviços móveis (EMT[29], Elisa[30], Tele2[31] e Lithuanian[32]) em cooperação com os bancos e o Centro de Certificação[33], o "AS Sertifitseerimiskeskus". Similarmente ao Cartão de Identidade Eletrônico, o eID Móvel passou a oferecer a possibilidade de autenticação nos sites de e-Gov, bem como a de assinar documentos eletronicamente, possuindo inclusive o mesmo valor legal dos documentos assinados manualmente. Esta facilidade foi possível devido ao armazenamento dos certificados digitais pessoais no cartão SIM do celular, os quais são destravados através de uma senha pessoal (PIN) (COMISSION, 2014b).

Tanto a emissão do *ID Card* quanto do *Digi-ID* é feita de forma centralizada pela Polícia Especial da Estônia, chamada de *Police and Border Guard Board*[34] (ESTONIA, 2015). A solicitação deve ser feita pessoalmente, sendo necessário apresentar diversos documentos além de preenchimento do formulário de solicitação (PIIRIVALVEAMET, 2015).

Por outro lado, a emissão do "eID Móvel" inicia com a assinatura de um termo de uso diretamente com a operadora de celular. Após concordar com os termos, o usuário recebe um novo cartão SIM para seu celular, fazendo então a ativação do serviço através de um aplicativo que o liga com a Polícia da Estônia (*Police and Border Guard Board*). Este aplicativo o guia através do processo de ativação, repassando as instruções de forma *on-line* (ESTONIA, 2015).

3.5 TURQUIA

A modernização do sistema de registro civil na Turquia teve seu ápice em 2000 com a introdução do MERNIS[35] (*Central Civil Registration System*), como é conhecido por sua abreviação na Turquia. O MERNIS é um sistema administrado centralmente, que se tornou oficialmente operacional em 2003, permitindo que qualquer mudança no estado do registro civil seja registrada eletronicamente em uma rede segura, rede esta que liga os 966 escritórios distritais de registro civil espalhados pelo país. As informações, mantidas no banco de dados central, são compartilhadas com instituições públicas para fins administrativos. O objetivo principal do sistema é assegurar a atualização e compartilhamento seguro de informações pessoais e, desta forma, aumentar a velocidade e eficiência dos serviços públicos oferecidos aos cidadãos (COMMUNITIES, 2009d).

29 <https://www.emt.ee/en/liitu>
30 <https://www.elisa.ee/>
31 <http://www.tele2.ee/>
32 <http://www.omnitel.lt/klientu_aptarnavimas_telefonu>
33 <https://www.sk.ee/en>
34 Em estoniano *Politsei- ja Piirivalveamet*, responsável por cuidar das fronteiras, monitorar e identificar os cidadãos.
35 <http://www.nvi.gov.tr/English/Mernis_EN,Mernis_En.html>

Conforme NVI (2009), dentre os serviços oferecidos pelo MERNIS podem ser citados:

- Modernização dos serviços de registro civil, mantendo os registros civis na forma eletrônica;
- Atribuição de um único Número de Identidade da República da Turquia[36] para cada cidadão turco; e
- Provisão de intercambio (troca) de dados pessoais *on-line* usando os números de identidade como identificadores;

O projeto do novo de cartão de identidade civil foi elaborado para atender o Plano Estratégico de Ação nº 46 da *Information Society*[37], contemplando o desenvolvimento de um novo Cartão de Identidade Eletrônico dotado de características visuais anti falsificação. Sendo implementado sob a responsabilidade do Ministério do Interior (*Ministry of Interior*) e da Direção Geral do Registro Civil e Nacionalidade (*General Directorate of Civil Registration and Nationality*), este novo *eID Card* possui um *chip* de contato com um sistema operacional desenvolvido pelo *National Research Institute of Electronics and Cryptology*[38] (UEKAE), instituto este afiliado do *Scientific and Technological Research Council of Turkey*[39] (TUBITAK). Além de conter informações pessoais e biométricas (digitais) do portador, pode ser utilizado para fins de identificação e autenticação em sistemas *on-line* (COMMUNITIES, 2009d).

De acordo com NVI (2013), a fase piloto do *eID Card* foi iniciada oficialmente em 2007 com a publicação do *Prime Ministry Circular* nº 2007/16 de 04/07/2007[40] e, de acordo com Office (2015), a última fase foi finalizada em dezembro de 2014 com a emissão de 25 milhões de cartões, os quais deverão ser distribuídos em 2015, atendendo ao Plano Anual[41].

Segundo (MUTLUGÜN; ADALIER, 2009), para a adoção do *eID Card* a Turquia precisou desenvolver um novo sistema para a autenticação eletrônica (*Electronic Authentication System*), o qual é composto por vários componentes, dentre os quais podem ser citados os seguintes:

- **eID Card:** principal componente do sistema, é utilizado para autenticar e identificar o usuário, contendo informações pessoais do portador, bem como o certificado digital.

[36] O *Turkish Republic Identity Number* (TRIN) constitui-se de um identificador único composto por 11 dígitos.
[37] <http://www.nvi.gov.tr/Files/File/Kimlik_Karti/46noluEylem.pdf>
[38] <http://uekae.bilgem.tubitak.gov.tr/en>
[39] <http://www.tubitak.gov.tr/>
[40] <http://www.nvi.gov.tr/Files/File/Kimlik_Karti/2007-16NoluBabakanlkGenelgesi.pdf>
[41] *Council of Ministers' Yearly Plan* para 2015, página 156, do *Official Gazette (Reiterated)* de 1/11/2014. Disponível em <www.resmigazete.gov.tr/eskiler/2014/11/20141101M1-1.pdf>

- **Dispositivo de Acesso ao Cartão:** O CAD (*Card Access Device*) trata-se de um leitor para o *eID Card*, o qual contém um módulo especial de segurança (*Secure Access Module* -SAM) capaz de ler dados biométricos, receber a senha PIN (*Personal Identity Number*) e gerar uma asserção de autenticação. Possui também um tela de LCD colorida que pode mostrar a fotografia digital do portador, salva no *chip* do cartão.
- **Plataforma de Serviços de Segurança:** A SSP (*Security Service Platform*) constitui-se de um conjunto de softwares que conectam o CAD com o provedor de serviços.
- **Serviço de Política de Autenticação:** O APS (*Authentication Policy Server*) constitui-se de uma central de políticas que identifica alguns parâmetros, como por exemplo, o nível de segurança (PIN + Biometria, PIN ou eID Card) e o período de validade da autenticação.

Gradativamente, a partir de 2013[42] o cidadão passou a contar com um terceiro nível de autenticação baseado no *eID Card*, obtendo um nível mais alto de segurança nos processos de identificação e autenticação. Adicionalmente, o cidadão pode combinar o nível de autenticação com uso de um "*token* de acesso", *token* este enviado para o telefone celular pessoal, desde que previamente cadastrado.

3.5.1 eID Móvel - Turquia

Segundo Comission (2015), um sistema de identificação e verificação consite basicamente de um ID de usuário e uma senha (credencais), utilizados em serviços (SPs) de eGov. Muitas vezes estas credenciais de acesso são criadas e mantidas pelos próprios provedores de serviço. Dessa forma, a empresa governamental Turksat[43] (*Turksat Satellite Communication Cable TV and Operation Inc*) está desenvolvendo e oferecendo para os órgãos públicos sistemas para identificação e verificação como assinaturas eletrônicas e assinaturas móveis (*Mobile signature* - MSign).

O Ato de Assinatura Eletrônica nº 5070[44], define os princípios legais e os requisitos técnicos para uso da assinatura digital na Turquia, a qual tem o mesmo impacto legal da assinatura manuscrita (COMISSION, 2015). A Assinatura Móvel é uma forma de usar um dispositivo móvel no lugar de uma assinatura manual, através de um ambiente altamente seguro provido por mecanismos criptográficos (GSMA, 2015).

---

[42] Integração entre o *eID Card* com o Portal do Governo (*e-Government Gateway*) apresentada no *CEBIT Euroasia Exhibition* que ocorreu entre 11 e 13 de setembro de 2013 (COMISSION, 2015)

[43] <http://www.turksat.com.tr/en>

[44] <http://www.lawsturkey.com/law/electronic-signature-law-5070>

Outra empresa que oferece o serviço de assinatura móvel na Turquia é a Turkcell[45]. O serviço é oferecido tanto para empresas privadas quanto públicas (YAPIKREDI, 2015) através de uma aplicação instalada no *SIM Card*. Durante o processo de assinatura de um documento, conforme exemplificado pela figura 5, o cidadão utiliza seu dispositivo móvel para acessar o SP, o qual solicita a assinatura de um documento. A confirmação da assinatura é feita por mensagem SMS trocada entre a entidade certificadora e o cidadão (TURKCELL, 2015).

Figura 5: Assinatura de documento - Turkcell

Toda a infraestrutura de eID Móvel no país se resume ao serviço de assinatura móvel oferecida por empresas de telecomunicações. No entanto, observa-se que o uso da identidade eletrônica é relativamente nova, uma vez que a emissão do *eID Card* só finalizou no final de 2014 (OFFICE, 2015). Portanto, esperam-se grandes avanços no modelo de gestão de identidades na Turquia, bem como no uso da eID Móvel.

[45] <http://www.turkcellteknoloji.com.tr/solutions/simplify-sim-asset-services-management/msign/>

4 CONSIDERAÇÕES FINAIS

Neste trabalho foi realizado um estudo sobre o conceito de Identidade Eletrônica Móvel, além de um levantamento das caraterísticas técnicas relacionadas a este conceito. Foram descritas as estratégias nacionais de gestão de identidade de 5 países (Alemanha, Áustria, Espanha, Estônia e Turquia), bem como uma seção específica foi dedicada à implementação da eID Móvel no respectivo país.

O estudo da eID Móvel demonstrou que um dos aspectos mais importantes se refere à forma de armazenamento dos atributos do cidadão e os mecanismos de segurança envolvidos no processo. Existem muitas soluções de armazenamento destas informações sensíveis, como o armazenamento em nuvem, em cartão SIM, em cartão de circuito integrado universal, entre outros. Cada uma delas depende de uma implementação de software ou hardware, consequentemente cada abordagem trás consigo uma complexidade particular.

Observou-se que países que adotaram o *eID Card* com *chip* sem contato em suas estratégias nacionais de gestão de identidade, naturalmente adotaram a tecnologia NFC em suas estratégias de identidade móvel, como é o exemplo da Alemanha e Espanha. Nesta abordagem, o dispositivo móvel opera de maneira semelhante à um leitor de cartões instalado em um computador pessoal. A Estônia optou pela parceria com empresas privadas de telefonia móvel, oferecendo à seus cidadãos um cartão SIM, o qual armazena tanto os atributos do cidadão quanto certificados digitais pessoais. Por outro lado, a Áustria optou por uma abordagem puramente por software. A Turquia procura consolidar seu modelo de eIDM com a finalização da fase piloto de implantação do *eID Card* em dezembro de 2014, cartões estes que deverão ser distribuídos em 2015. O reflexo desta consolidação se reflete no modelo de eID Móvel no país, onde é oferecido até o momento, a possibilidade de assinatura eletrônica de documentos, uma vez que o acesso aos SPs depende também da adequação destes provedores de serviço.

Por fim, este estudo demonstrou que os países em geral se preocupam com a implantação de um modelo de eID Móvel que seja interoperável. Para tanto, utilizam muitas vezes protocolos e tecnologias conhecidas e amplamente adotadas, como Java, NFC e TLS. Entretanto, observou-se que os aspectos de segurança, como mecanismos criptográficos utilizados na identidade eletrônica móvel, necessitam de pesquisa mais ampla. Tais aspectos criam uma nova demanda de pesquisa e uma grande oportunidade de estudo a ser explorada na dissertação de mestrado.

REFERÊNCIAS

ABBOTT, J.; PRACTICAL, G. **Smart cards: How secure are they**. *GSEC Practical v1*, v. 3, p. 2–18, 2002.

ABC, D. **Así es el nuevo DNI eléctronico 3.0**. 2015. <http://www.abc.es/espana/20150112/abci-electronico-201501121343.html>. Acesso em: 07 agosto de 2015.

ADMINISTRACIONES, I. E. para las. ***Gobierno de España***. 2014. Identidad Electrónica para las Administraciones. <http://clave.gob.es/>.

ALIMI, V.; PASQUET, M. **Post-distribution provisioning and personalization of a payment application on a UICC-based Secure Element**. In: IEEE. *Availability, Reliability and Security, 2009. ARES'09. International Conference on*. [S.l.], 2009. p. 701–705.

ALLIANCE, S. C. **Host Card Emulation (HCE) 101**. 2014. <http://goo.gl/R1GVcH>.

AUSTRIA, F. C. of. ***Modules for Online Applications***. 2015. <https://www.digitales.oesterreich.gv.at/site/6528/default.aspx>.

BHARGAV-SPANTZEL, A. et al. **User centricity: A taxonomy and open issues**. *Journal of Computer Security*, v. 15, n. 5, p. 493–527, 2007. <www.scopus.com>.

BOUDRIGA, N. ***Security of mobile communications***. [S.l.]: CRC Press, 2009.

BRASIL, G. do. **e-PING Padrões de Interoperabilidade de Governo Eletrônico**. *Comitê Executivo de Governo Eletrônico, May*, 2015. <http://goo.gl/6nl68C>.

BüRGERKARTE. ***The Austrian Citizen Card System***. 2014. <https://www.buergerkarte.at>.

CASED, C. for A. S. R. D. ***MONA makes the new personal ID card mobile***. 2011. <http://www.cased.de/en/press/press.html/29>.

CLAUSS, S.; KÖHNTOPP, M. **Identity management and its support of multilateral security**. *Computer Networks*, Elsevier, v. 37, n. 2, p. 205–219, 2001.

COMISSION, E. ***eGovernment in the Austrian***. 2014. EGovernment Factsheets.

COMISSION, E. ***eGovernment in the Estonia***. 2014. EGovernment Factsheets.

COMISSION, E. ***eGovernment in the Germany***. 2014. EGovernment Factsheets.

COMISSION, E. ***eGovernment in the Spain***. 2014. EGovernment Factsheets.

COMISSION, E. ***eGovernment in Turkey***. 2015. EGovernment Factsheets.

COMMUNITIES, E. ***eID Interoperability for PEGS: Update of Country Profiles study - Estonian country profile***. 2009. IDABC European eGovernment Services.

COMMUNITIES, E. ***eID Interoperability for PEGS: Update of Country Profiles study - German country profile***. 2009. IDABC European eGovernment Services.

COMMUNITIES, E. ***eID Interoperability for PEGS: Update of Country Profiles study - Spain country profile***. 2009. IDABC European eGovernment Services.

COMMUNITIES, E. ***eID Interoperability for PEGS: Update of Country Profiles study - Turkish country profile***. 2009. IDABC European eGovernment Services.

DHAMIJA, R.; DUSSEAULT, L. **The seven flaws of identity management: Usability and security challenges**. *Security & Privacy, IEEE*, IEEE, v. 6, n. 2, p. 24–29, 2008.

EMVCO. **EMV Mobile Contactless Payment: Technical Issues and Position Paper**. 2007. <https://goo.gl/NVBnEE>.

ESTONIA, G. of the. ***The Estonian ID Card and Digital Signature Concept - Principles and Solutions***. 2003. <http://www.id.ee/public/The_Estonian_ID_Card_and_Digital_Signature_Concept.pdf>.

ESTONIA, G. of the. ***The Estonian ID***. 2015. <http://www.id.ee/>.

EU, G. ***Data Protection, Consent and Biometric Data in Estonia: requirements and categories***. 2012. <http://www.gencs.eu/news/view/793>.

FELICIANO, G. et al. **Gerência de identidades federadas em nuvens: enfoque na utilização de soluções abertas**. *Minicursos do XI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuidos (SBRC)*, p. 182–231, 2011.

GSMA. **Socio-economic benefits of SIM-based NFC**. booz&co - London, 2011. <http://goo.gl/2HZDY3>.

GSMA. **Mobile Signature**. 2015. <http://www.gsma.com/personaldata/faqs/what-is-a-mobile-signature>. Acesso em: 05 agosto de 2015.

GUAUS, J. et al. **Best Practice for Mobile Financial Services: Enrolment Business Model Analysis**. In: *Mobey Forum Mobile Financial Services Ltd., Helsinki, Finland, Online, June*. [S.l.: s.n.], 2008.

HANSEN, M.; SCHWARTZ, A.; COOPER, A. **Privacy and identity management**. *Security & Privacy, IEEE*, IEEE, v. 6, n. 2, p. 38–45, 2008.

HORSCH JOHANNES BRAUN, A. W. M. ***Mobile eID application for the German identity card***. 2011. Technische Universität Darmstadt. <https://goo.gl/A4mkGk>.

INNERN, B. des. ***Chipkarten-Lesegeräte***. 2014. <http://goo.gl/WMhtZn>.

INNERN, B. des. ***Der Personalausweis***. 2014. <http://goo.gl/41g4JJ>.

INNERN, B. des. ***Gebühren und Gültigkeit***. 2014. <http://goo.gl/3Hc4fy>.

ITU, T. **Series y: Global information infrastructure, internet protocol aspects and next-generation networks**. *Rec. ITU-T Y*, v. 2720, 2009.

JØSANG, A.; POPE, S. **User centric identity management**. In: *AusCERT Asia Pacific Information Technology Security Conference*. [S.l.: s.n.], 2005. p. 77.

KRIMPE, J. **Mobile ID: Crucial element of m-Government**. In: ACM. *Proceedings of the 2014 Conference on Electronic Governance and Open Society: Challenges in Eurasia*. [S.l.], 2014. p. 187–194.

MADLMAYR, G. et al. **The benefit of using SIM application toolkit in the context of near field communication applications**. In: IEEE. *Management of Mobile Business, 2007. ICMB 2007. International Conference on the*. [S.l.], 2007. p. 5–5.

MANTORO, T.; MILIŠIĆ, A. **Smart card authentication for Internet applications using NFC enabled phone**. In: IEEE. *Information and Communication Technology for the Muslim World (ICT4M), 2010 International Conference on*. [S.l.], 2010. p. D13–D18.

MAYES, K.; EVANS, T. **Smart cards for mobile communications**. In: *Smart Cards, Tokens, Security and Applications*. [S.l.]: Springer, 2008. p. 85–113.

MELLO, E. R. d. et al. **Um modelo para confiança dinâmica em ambientes orientados a serviço**. Florianópolis, SC, 2009.

MILCARZ, G. **Mobile Payment using {HCE} and mPoint payment gateway based on {NFC} enabled phones**. 2014.

MJ. **Conselho Nacional de Segurança Pública - CONASP: Recomendação n. 019, de 19 de fevereiro de 2014**. 2015. <http://goo.gl/qxDXyA>.

MPFI. **SIM card report**. 2008. <http://www.mpf.org.in/pdf/general/SIMCard_ReportPPT.pdf>.

MUTLUGÜN, M.; ADALIER, O. **Turkish National Electronic Identity Card**. In: ACM. *Proceedings of the 2nd international conference on Security of information and networks*. [S.l.], 2009. p. 14–18.

M'CHIRGUI, Z. **Dynamics of R&D networked relationships and mergers and acquisitions in the smart card field**. *Research Policy*, Elsevier, v. 38, n. 9, p. 1453–1467, 2009.

NVI. ***The Central Civil Registration System (MERNIS***. 2009. <http://www.nvi.gov.tr/English/Mernis_EN,Mernis_En.html>.

NVI. ***Republic of Identity Card Project***. 2013. <http://www.nvi.gov.tr/Haberler,Bolu_Pilot.html>.

OECD. ***Digital Identity Management: Enabling Innovation and Trust in the Internet Economy***. 2011. OECD Publishing.

OFFICE, I. L. ***Transition to national eID cards***. 2015. <http://www.internationallawoffice.com/newsletters/detail.aspx?r=30667>.

PANNIFER DICK CLARK, D. B. S. **HCE and SIM Secure Element: It's not black and white**. Guildford: Consult Hyperion, 2014. <http://goo.gl/F0VDGH>.

PIIRIVALVEAMET, P. ja. ***Mobile-ID***. 2015. <https://www.politsei.ee/en/teenused/isikut-toendavad-dokumendid/mobiil-id/>.

POLICíA, D. G. de la. ***DNI electrónico***. 2015. Ministerio del Interior. <http://www.dnielectronico.es/>.

POLICíA, G. de Prensa de la Dirección General de la. **El ministro del Interior destaca que el nuevo DNI electrónico 3.0 contribuirá a hacer de España un país más seguro al mejorar la seguridad documental**. 2015. <http://www.policia.es/prensa/20150112_1.html>. Acesso em: 08 agosto de 2015.

POLLER, A. et al. **Electronic identity cards for user authentication—promise and practice**. *IEEE Security & Privacy*, IEEE, n. 1, p. 46–54, 2012.

PRESIDENCIA, M. de la. ***Orden PRE/1838/2014***. 2014. <http://www.boe.es/boe/dias/2014/10/09/pdfs/BOE-A-2014-10264.pdf>.

REVEILHAC, M.; PASQUET, M. **Promising secure element alternatives for NFC technology**. In: IEEE. [S.l.], 2009. p. 75–80.

SECURITY, F. O. for I. ***Neue Software für den Online-Ausweis***. 2015. <https://www.ausweisapp.bund.de/en/startseite/>.

SERTIFITSEERIMISKESKUS, A. ***Principles of Client Data Protection***. 2014. <https://www.sk.ee/en/about/data-protection/>.

SERTIFITSEERIMISKESKUS, A. ***Validity confirmation services***. 2014. <https://sk.ee/en/services/validity-confirmation-services/>.

STAMP, M. ***Information security: principles and practice***. [S.l.]: John Wiley & Sons, 2011.

STORK. ***Estonia: eID card a ten-year success***. 2014. <https://www.eid-stork.eu/index.php?option=com_content&task=view&id=348&Itemid=69>.

TARJETAS, D. de Documentos de I. . ***Descripción Técnica de Aplicaciones Android sobre DNIe v3.0***. 2015. Ministerio del Interior. <http://www.dnielectronico.es/PDFs/Implementacion_NFC_FNMT.pdf>.

TSAI, Y.-R.; CHANG, C.-J. **SIM-based subscriber authentication mechanism for wireless local area networks**. *Computer Communications*, Elsevier, v. 29, n. 10, p. 1744–1753, 2006.

TURKCELL. **MSign**. 2015. <http://goo.gl/zOnS9j>. Acesso em: 07 agosto de 2015.

United Nations. ***e-Government Survey: E-Government for the Future We Want***. 2014. Economy & Social Affairs.

VERBRAUCHERSCHUTZ, B. der Justiz und für. ***Act on Identity Cards and Electronic Identification***. 2014. <http://www.gesetze-im-internet.de/englisch_pauswg/englisch_pauswg.html>.

WANGHAM, M. S. et al. **Minicursos X SBSeg**. In: ____. [S.l.: s.n.], 2010. cap. Gerenciamento de Identidades Federadas, p. 1–52.

YAPIKREDI. **Mobile Signature**. 2015. <http://goo.gl/BYOxHH>. Acesso em: 07 agosto de 2015.

ZWATTENDORFER, B.; TAUBER, A.; ZEFFERER, T. **A privacy-preserving eID based Single Sign-On solution**. In: *NSSÍ1*. [S.l.: s.n.], 2011. p. 295–299.

ZWATTENDORFER, B.; TAUBER, A.; ZEFFERER, T. **A privacy-preserving eID based Single Sign-On solution**. In: IEEE. *Network and System Security (NSS), 2011 5th International Conference on*. [S.l.], 2011. p. 295–299.