Ministério da Justiça

Termo de Cooperação/Projeto:

Acordo de Cooperação Técnica FUB/CDT e MJ/SE Registro de Identidade Civil – Replanejamento e Novo Projeto Piloto

Documento:

RT Estratégias Nacionais de Gestão de Identidade na Europa.

Data de Emissão:

08/06/2015

Elaborado por:

Universidade de Brasília – UnB
Centro de Apoio ao Desenvolvimento Tecnológico – CDT
Laboratório de Tecnologias da Tomada de Decisão – LATITUDE.UnB

MINISTÉRIO DA JUSTIÇA

José Eduardo Cardozo
Ministro

Marivaldo de Castro Pereira
Secretário Executivo

Helvio Pereira Peixoto
Coordenador Suplente do Comitê Gestor do SINRIC

UNIVERSIDADE DE BRASÍLIA

Ivan Marques Toledo Camargo
Reitor

Paulo Anselmo Ziani Suarez
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA
Ana Maria da Consolação Gomes Lindgren
Andréa Benoliel de Lima
Celso Pereira Salgado
Delluiz Simões de Brito
Elaine Fabiano Tocantins
Fernando Saliba Oliveira
Fernando Teodoro Filho
Guilherme Braz Carneiro
Joaquim de Oliveira Machado
José Alberto Sousa Torres
Marcelo Martins Villar
Raphael Fernandes de Magalhães Pimenta
Rodrigo Borges Nogueira
Rodrigo Gurgel Fernandes Távora
Sara Lais Rahal Lenharo

EQUIPE TÉCNICA
Flávio Elias Gomes de Deus (Pesquisador Sênior)
William Ferreira Giozza (Pesquisador Sênior)
Ademir Agustinho de Rezende Lourenço
Adriana Nunes Pinheiro
Alysson Fernandes de Chantal
Amanda Almeida Paiva
Andréia Campos Santana
Antônio Claudio Pimenta Ribeiro
Carolinne Januária de Souza Martins
Daniela Carina Pena Pascual
Danielle Ramos da Silva
Diogenes Ferreira Reis Fustinoni
Emerson Ribeiro de Mello
Fábio Lúcio Lopes Mendonça
Fábio Mesquita Buiati
Glaidson Menegazzo Verzeletti
Heverson Soares de Brito
Johnatan Santos de Oliveira
José Carneiro da Cunha Oliveira Neto
Kelly Santos de Oliveira Bezerra
Luciano Pereira dos Anjos
Luciene Pereira de Cerqueira Kaipper
Luiz Antônio de Souto Evaristo
Luiz Claudio Ferreira
Marcos Vinicius Vieira da Silva
Marco Schaffer
Pedro Augusto Oliveira de Paula
Roberto Mariano de Oliveira Soares
Sergio Luiz Teixeira Camargo
Soleni Guimarães Alves
Suzane Lais De Freitas
Valério Aymoré Martins
Vera Lopes de Assis
Wladimir Rodrigues da Fonseca

HISTÓRICO DE REVISÕES

Data	Versão	Descrição
08/06/2015	0.1	Versão inicial.

latitude
Laboratório de tecnologias da tomada de decisão

Universidade de Brasília – UnB
Campus Universitário Darcy Ribeiro - FT – ENE – Latitude
CEP 70.910-900 – Brasília-DF
Tel.: +55 61 3107-5597 – Fax: +55 61 3107-5590

SUMÁRIO

1 INTRODUÇÃO

A Secretaria Executiva (SE/MJ), vinculada ao Ministério da Justiça (MJ), é responsável por viabilizar o desenvolvimento e a implantação do Registro de Identidade Civil, instituído pela Lei nº 9.454, de 7 de abril de 1997, regulamentado pelo Decreto nº 7.166, de 5 de maio de 2010.

Atualmente, a República Federativa do Brasil conta com sistema de identificação de seus cidadãos amparado pela Lei nº 7.116, de 29 de agosto de 1983. Essa lei assegura validade nacional às Carteiras de Identidade, ou Cédulas de Identidade; confere também autonomia gerencial às Unidades Federativas no que concerne à expedição e controle dos números de registros gerais emitidos para cada documento. Essa condição de autonomia, ao contrário do que pode parecer, fragiliza o sistema de identificação, já que dá condições ao cidadão de requerer legalmente até 27 (vinte e sete) cédulas de identidades diferentes. Com essa facilidade legal, inúmeras possibilidades fraudulentas se apresentam de maneira silenciosa, pois, na grande maioria dos casos, os Institutos de Identificação das Unidades Federativas não dispõem de protocolos e aparato tecnológico para identificar as duplicações de registro vindas de outros estados, ou até mesmo do seu próprio arquivo datiloscópico. Consoante aos fatos, os Institutos de Identificação não trabalham interativamente para que haja trocas de informações de dados e geração de conhecimento para manuseio inteligente e seguro para individualização do cidadão em prol da sociedade.

Com foco na busca de soluções para tais problemas, o Projeto RIC prevê a administração central dos dados biográficos e biométricos dos cidadãos no Cadastro Nacional de Registro de Identificação Civil (CANRIC) e ABIS (do inglês *Automated Biometric Identification System*), respectivamente. A previsão desse novo modelo sustenta a não duplicação de registros e a consequente identificação unívoca dos cidadãos brasileiros natos e naturalizados. O Projeto RIC, portanto, visa otimizar o sistema de identificação e individualização do cidadão brasileiro nato e naturalizado com vistas a um perfeito funcionamento da gestão de dados da sociedade, agregando valor à cidadania, à gestão administrativa, à simplificação do acesso aos serviços disponíveis ao cidadão e à segurança pública do país.

Nesse contexto, o termo de cooperação entre MJ/SE e FUB/CDT define um

projeto que objetiva identificar, mapear e desenvolver parte dos processos e da infraestrutura tecnológica necessária para viabilizar a implantação do número único de Registro de Identidade Civil – RI\\C no Brasil.

Resultante de um subconjunto das atividades previstas para inicialização da cooperação MJ/SE e FUB/CDT, o presente documento, denominado “RT Estratégias Nacionais de Gestão de Identidade na Europa”, apresenta os resultados da pesquisa desenvolvida sobre governo eletrônico realizada em 8 (oito) países europeus, a saber: Alemanha, Áustria, Dinamarca, Espanha, Estônia, Holanda, Itália e Reino Unido.

A seleção dos países candidatos ao estudo foi feita a partir dos 25 (vinte e cinco) países mais bem colocados no “Índice de Desenvolvimento em Governo Eletrônico - EGDI”, publicado pela ONU em 2014. Após filtrar os países europeus desta seleção, foi realizada uma pesquisa prévia com o intuito de buscar documentações disponíveis sobre governo eletrônico, restritas aos idiomas português, inglês ou espanhol e classificadas pela sua relevância e proximidade com as questões elencadas no relatório anterior (RT 01).

Para cada país europeu citado anteriormente, a presente pesquisa organiza o resultado sistematicamente nos seguintes grupos: Perfil Sociopolítico, Econômico e Governo Eletrônico; Modelo de Organização de Documentos Civis; Identidade Eletrônica; Sistemas de Gestão de eID e Privacidade relacionada a Identidade Eletrônica. Por fim, na Seção 10 é apresentada uma análise comparativa destas nações pesquisadas.

2 ALEMANHA

2.1 Perfil Sociopolítico, Econômico e Governo Eletrônico

2.1.1 Estrutura Sociopolítica

Localizada na Europa Central, a Alemanha faz divisa com países como a Dinamarca, Áustria, Suíça e França, tendo também saída para o mar do Norte e Báltico. Com um território de 357 mil km², possui uma população de 81,8 milhões de habitantes e tem uma densidade demográfica 229ha/km². Apesar de ser o país mais populoso da União Européia tem uma das menores "taxas de fertilidade[1]" do mundo. Em 2004, havia aproximadamente 7 milhões de cidadãos estrangeiros registrados e cerca de 19% dos residentes eram de fora do país ou possuíam ascendência estrangeira. O seu índice de desenvolvimento humano (IDH) é considerado muito alto (0,911) e ocupa a sexta posição do *ranking* da ONU (Programa das Nações Unidas para o Desenvolvimento - PNUD) de 2014[2]. A Alemanha é a maior economia da Europa, a quarta maior do mundo quando é considerado o PIB[3] (Produto Interno Bruto Nominal).

A Alemanha é uma República Federal Parlamentarista, dividida em 16 unidades federativas (estados). É um estado membro das Nações Unidas, do grupo G8, do grupo G20, da OMC (Organização Mundial do Comércio) e ingressou na OTAN (Organização do Tratado do Atlântico Norte) em 1955. Em 1949, após a segunda guerra mundial, foi dividida em dois estados, a Alemanha Ocidental (República Federal da Alemanha) e a Alemanha Oriental (República Democrática Alemã), sendo novamente reunificada em 1990. A Alemanha Ocidental foi um dos membros fundadores da Comunidade Econômica Européia em 1957, que posteriormente se tornou na União Europeia em 1993 (CIA, 2014b).

[1] Relação de filhos por mulher
[2] http://hdr.undp.org/sites/default/files/hdr14-summary-en.pdf
[3] "Report for Selected Countries and Subjects". World Economic Outlook. International Monetary Fund. October 2014

2.1.2 Acesso à Internet

De acordo com *European Comission* (2014), em relação aos índices de acesso à Internet em 2013, as seguintes estatísticas da Alemanha são apresentadas.

- Casas com acesso à Internet: 88%.
- Empresas com acesso à Internet: 98%.
- Casas com acesso por banda larga: 85%.
- Empresas com acesso por banda larga: 86%.
- Indivíduos que fizeram compras pela Internet (últimos 3 meses): 60%.
- Empresas que receberam pedidos de compras *on-line* (último ano): 26%.

Em relação ao número de usuários de Internet, a Alemanha ocupa a sétima posição mundial e possui uma taxa de penetração de 86,78% (percentagem da polução que usa a Internet)[4], o que indica um alto nível de inclusão digital. Em relação ao índice de infraestrutura em telecomunicações (ITT) (United Nations, 2014), a pontuação da Alemanha (0,8038) é muito superior a média europeia (0,6678). Este índice foi obtido a partir dos seguintes componentes (United Nations, 2014).

- Telefone fixo (cada 100 habitantes): 61,23.
- Telefone celular (cada 100 habitantes): 130,02.
- Conexão à Internet Banda Larga (cada 100 habitantes): 33,70.
- Conexão à Internet *Wireless* (cada 100 habitantes): 40,66.

O relatório da ONU de 2014 apresenta um crescimento no uso da Internet de aproximadamente 30% no ano de 2000 para um valor acima de 80% em 2010, o que reflete um investimento alto em infraestrutura de telecomunicações resultando em um crescimento superior a 250% em um intervalo de 10 anos (United Nations, 2014).

2.1.3 *Ranking* de e-Gov da ONU

De acordo com United Nations (2014), classificada com o índice de desenvolvimento de e-Gov de 0,7864 (índice considerado muito alto), a Alemanha passou a ocupar a 21ª posição no *ranking* de governo eletrônico em 2014, caindo

[4] Fonte: http://www.internetlivestats.com/internet-users-by-country/

quatro posições em relação ao *ranking* de 2012. No que se refere ao índice de eParticipação da ONU, a Alemanha está entre os 50 melhores países (26ª posição). O índice de desenvolvimento em e-Gov apresentou as seguintes informações.

• Serviços *On-line*: 0,6693 (média na Europa é de 0,5695).

• Infraestrutura em Telecomunicações: 0,8038 (média na Europa é de 0,6678).

• Capital Humano: 0,8862 (média na Europa é de 0,8434).

2.1.4 Principais Políticas (Leis, atos, decretos, etc)

As principais leis alemãs relacionadas ao desenvolvimento do e-Gov e da gestão de identidades que se destacam são as seguintes.

• **1997:** Lei dos Serviços de Comunicação e Informação, conhecida também como Lei Multimídia. Tem o objetivo de criar condições econômicas favoráveis para os vários usos de dispositivos eletrônicos de informação e comunicação, englobando assinatura eletrônica e serviços de tele-entrega.

• **2005:** Lei do Gerenciamento dos Arquivos Eletrônicos, desenhada para eliminar o uso de papéis no sistema judiciário do país.

• **2007:** Revisão da Lei do Passaporte, regulamentando a segunda geração de passaporte (ePassaporte), prevendo a inclusão de duas impressões digitais do portador no documento eletrônico.

• **2008:** Lei de Reforço de Segurança dos serviços de T.I do governo federal entra em vigor, atribuindo o ”Departamento Federal de Segurança em Tecnologia da Informação” (BSI) como uma parte central no âmbito dos esforços de proteção do governo federal.

• **2009:** Publicação da Lei dos Documentos de Identificação Civil e da Identidade Eletrônica (eID), sendo revisada em 22 de dezembro de 2011. A Lei trata de assuntos como idade para emissão da identificação, validade, revogação, cancelamento, ativação e bloqueio.

• **2011:** Lei para regular o uso do serviço De-Mail. Segundo ela, este serviço de correio eletrônico, diferentemente do modelo convencional, permite por exemplo o envio de documentos confidenciais e mensagens rastreáveis.

• **2013:** Entra em vigor a Lei para promover o governo eletrônico da Alemanha. Entre as facilidades apresentadas está a comunicação com o governo

através de um canal eletrônico exclusivo (De-Mail). Esta Lei incentiva as autoridades a oferecerem aos cidadão e empresas opções para pagamento *on-line* de processos e acesso aos documentos públicos de forma eletrônica. Ao mesmo tempo, estimula o uso do novo cartão de identificação, concedendo aos cidadãos maior agilidade nas interações com o governo.

2.1.5 Cronologia do Desenvolvimento de e-Gov e GId

A seguir, destacam-se alguns marcos importante para o desenvolvimento de e-Gov e sobre a implantação da estratégia nacional de gestão de identidades.

• **1998:** iniciado o projeto *MEDIA@Komm* para promover o desenvolvimento do governo eletrônico, incluindo propostas para tonar o e-GOV mais seguro através do uso de assinatura digital.

• **1998:** é lançado o programa *BundOnline2005* do governo federal, com o objetivo de conceder aos serviços públicos a possibilidade de serem acessados por meio eletrônico até final de 2005. Esta iniciativa faz parte do programa ”Internet para todos - Dez passos para o caminho da Sociedade da Informação”.

• **2001:** lançado o portal *Bund.DE* provendo acesso centralizado aos serviços *on-line* da Administração Federal.

• **2002:** o governo toma decisões que afetam as transações eletrônicas entre empresas e a administração federal, estabelecendo estratégias, padrões e criando condições para as comunicações criptografadas e uso da assinatura digital.

• **2003:** o governo federal inicia ações de e-Gov para diminuir a burocracia, incluindo atrativos para as empresas.

• **2005:** o governo apresenta estratégia para unificar os cartões de identificação[5] existentes em um único cartão eletrônico (*eID Card*). Em novembro deste mesmo ano, a Alemanha inicia a emissão dos novos documentos de viagem, passaportes biométricos chamados de “*ePass*”, os quais passaram a armazenar informações como a fotografia digital do portador em um chip de rádio frequência (RFID).

• **2006:** o governo aplica os princípios do ITIL[6] (*IT Infrastructure Library*) no

[5] Documento de identificação civil, segurança social e de plano de saúde
[6] Um conjunto de ”Boas Práticas” na área de gerenciamento de serviços de tecnologia da informação - http://www.itil.org/

website oficial.

• **2007:** o governo introduz o “Número Único de Identificação” para fins de tributação fiscal, centralizando os dados de identificação no Escritório Central de Impostos do Governo Federal. Em novembro deste mesmo ano, iniciou-se a operação da segunda geração de passaporte (ePassaporte) contendo duas impressões digitais do portador do cartão.

• **2008:** o governo federal adota um regulamento administrativo, abrindo caminho para o uso de um cartão eletrônico (*ID Card* por funcionários públicos e militares. Em julho deste ano, um procedimento legislativo permitiu a inclusão de um certificado digital nos cartões eletrônicos, para ser usado em processos de assinaturas eletrônicas, atendendo dessa forma a lei de assinatura vigente.

• **2009:** o governo adota nova estratégia de banda larga, com objetivo de aumentar a capacidade de conexão das empresas e das residências. Em março, é iniciado projeto piloto da central de atendimento às autoridades do governo, via número telefônico 115, com o objetivo de ser o único telefone de contato com as agências do governo.

• **2010:** em dezembro, iniciou-se o uso de um novo cartão eletrônico (*eID Card*), em um formato de cartão de crédito, que substituiu o cartão de identificação nacional existente.

• **2013:** desde o projeto piloto lançado em 2009, o serviço de contato telefônico 115 é expandido em 2013, passando a atender um total de 340 municipios.

2.2 Modelo de Organização de Documentos Civis

2.2.1 Registro Civil

O registro de nascimento deve ser feito no cartório mais próximo, de preferência na cidade de nascimento do cidadão e em um prazo máximo de 7 dias após o nascimento. O registro é feito mediante pagamento de taxa, apresentação da certidão de casamento dos pais, documento emitido pelo hospital e documento que comprove a identidade dos pais, como carteira de identidade ou passaporte (Stadt Würzbrug, 2014).

Na República Democrática Alemã, existia uma central de registro civil, responsável por emitir um identificador único para os cidadãos. Como parte do tratado

de reunificação, este registro único foi abolido e, atualmente, a constituição Alemã não permite que seja utilizado um número pessoal unificado de identificação para seus cidadãos (European Communities, 2009b).

2.2.2 Identidade Civil

É obrigatório que todos os cidadãos alemães maiores de 16 anos tenham uma carteira de identidade ou um passaporte. Estes documentos são aceitos para comprovação da identidade civil, o que não ocorre com a carteira de motorista.

Desde novembro de 2010, os cidadão passaram a contar com um cartão de identificação eletrônico[7], o qual substituiu a carteira de identidade tradicional. Os dados contidos neste novo documento de identidade são exatamente os mesmos do modelo tradicional (Bundesamt für Sicherheit in der Informationstechnik, 2014b). Ao solicitar esta nova identidade civil, os seguintes dados são impressos no cartão.

1. Sobrenome de família e sobrenome de casado.
2. Primeiro Nome.
3. Grau de Doutor (Dr. ou PhD).
4. Data e local de nascimento.
5. Assinatura.
6. Altura.
7. Foto.
8. Cor dos olhos.
9. Endereço.
10. Nacionalidade.
11. Número de série.

Todos os dados coletados também são armazenados no *microchip,* exceto a altura, cor dos olhos e assinatura. A pedido do titular, informações biométricas também podem ser eletronicamente armazenadas no cartão (Bundesamt für Sicherheit in der Informationstechnik, 2014b).

2.2.3 Relação do Documento de Viagem com a Identidade Civil

[7] Cartão semelhante a um cartão de crédito contendo um *microchip* de rádio frequência.

O passaporte alemão passou por uma transformação em 2005 com a criação do passaporte eletrônico, que inicialmente armazenava apenas alguns dados pessoais e uma imagem facial. Em 2007, este passaporte eletrônico passou a contar com um *microchip* de radio frequência (RFID), possibilitando o armazenamento de mais informações, entre elas, as descritas abaixo (Bundesamt für Sicherheit in der Informationstechnik, 2014c)

- Sobrenome e nome de nascimento.
- Dia e local de nascimento.
- Sexo.
- Altura.
- Cor dos Olhos.
- Local de residência.

Para realizar a emissão do novo documento de identidade civil, normalmente, é solicitada a apresentação do passaporte como um dos documentos necessários, caso o solicitante não possua um cartão de identificação antigo [Bundesministerium des Innern, 2014a].

Tanto o passaporte eletrônico (*ePass*) quanto o cartão de identidade (*eID Card*) possuem um *microchip* de radio frequência para armazenar as informações do portador. Esta característica comum habilita o *eID Card* para ser utilizado como documento de viagem, sendo aceito por diversos países, principalmente por nações pertencentes à comunidade européia (Bundesamt für Sicherheit in der Informationstechnik, 2014a).

2.2.4 Biometria no Sistema de Identidade Civil

A Lei dos Documentos de Identificação Civil e da Identidade Eletrônica (eID)[8] assegura ao cidadão a opção de realizar ou não a coleta da impressão digital para ser armazenada no *microchip* do *eID Card*. Normalmente, é feita a coleta dos dedos indicadores (esquerdo e direito), porém, se não for possível fazer a coleta por algum motivo, é possível substituir estas impressões digitais pelo dedo médio, anelar ou

[8] Sessão 5, parágrafo 9 da Lei dos Documentos de Identificação Civil e da Identidade Eletrônica, disponível em http://goo.gl/NWrE9A.

polegar (Bundesministerium der Justiz und für Verbraucherschutz, 2014).

2.3 Identidade Eletrônica

2.3.1 Uso da Identidade Eletrônica

O processo de identificação e autenticação eletrônica é feito por meio de um cartão de identificação eletrônico (*eID Card*), o qual 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 (European Comission, 2014d).

Para utilizar o *eID Card*, o cidadão deverá adquirir um leitor de *smart card* homologado pelo governo e instalá-lo em seu computador pessoal (Bundesministerium des Innern, 2014c), bem como obter o *software*[9] conhecido como ”AusweisApp”, 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. Esta versão permitirá ao cidadão, a partir de abril de 2015, utilizar a identidade eletrônica através de um telefone móvel, por exemplo (Federal Office for Information Security, 2015a).

O portador do cartão tem direito por lei de ativar ou desativar a função de identidade eletrônica (eID), por meio 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 (Bundesministerium der Justiz und für Verbraucherschutz, 2014).

Cada cidadão pode apenas ter um único identificador eletrônico, uma vez que ele está vinculado ao documento de identificação civil. O referido eID tem validade igual

[9] https://www.ausweisapp.bund.de/ausweisapp2/

a do documento de identificação civil (Bundesministerium der Justiz und für 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 (Bundesministerium des Innern, 2014e).

2.3.2 Cadastro da Identidade Eletrônica

O governo da Alemanha contratou em 2010 a empresa privada Bundesdruckerei[10] 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". Após fazer a solicitação, o cidadão recebe em sua residência o novo cartão de identificação (*eID Cards*), bem como um código de identificação pessoal (PIN), a chave de desbloqueio do PIN (PUK) e uma senha para bloqueio do cartão (Bundesdruckerei GmbH, 2014). O código PIN é composto por 6 dígitos numéricos, o qual deve ser alterado pelo usuário a qualquer momento e por quantas vezes julgar necessário. Após 3 tentativas incorretas de digitação, o PIN é bloqueado, podendo ser desbloqueado pelo código PUK até o limite de 10 vezes. A senha de bloqueio do cartão é utilizada para casos de perda ou roubo do cartão, como forma de garantir que a identidade eletrônica não seja utilizada por pessoas não autorizadas (Bundesministerium des Innern, 2014g).

2.3.3 Atributos da Identidade Eletrônica

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 do 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 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

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

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 (Bundesministerium des Innern, 2014d).

2.3.4 Biometria

A coleta das impressões digitais é realizada em dois dedos, sendo que estas informações são armazenadas no *microship* do novo cartão de identificação eletrônica (*eID Card*) (European Communities, 2009b). Entretanto, conforme citado na Seção 2.4, a coleta é feita de forma voluntária, sendo realizada apenas com o consentimento do cidadão.

2.3.5 Uso de Certificado Digital na Identidade Eletrônica

A diretriz de funcionamento da identidade eletrônica requer o uso de duas infraestruturas de chave pública (PKI)[11], uma para autenticação do *eID Card* (protocolo: Autenticação Passiva), a *Country Signing Certificate Authority* (CSCA) e outra para proteção das digitais biométricas do *eID Card* (protocolo: Terminal de Autenticação), a *Country Verifying Certificate Authority* (CVCA) (Federal Office for Information Security, 2015b). Dentre as autoridades que fazem parte destas infraestruturas estão as seguintes (Bundesministerium des Innern, 2014i).

- Departamento Federal de Segurança em Tecnologia da Informação (BSI): operador da Autoridade Certificadora Raiz (*Root CA*) CSCA e CVCA.
- Escritório Federal de Administração (BVA): atua como operador da autoridade de registro (AR).
- Provedor de Certificado (BerCA): responsável por fornecer os certificados para os provedores de serviços.

O propósito da Autenticação Passiva (PA) é validar a autenticidade e integridade dos dados armazenados no *microchip* do *eID Card*. No processo de fabricação do documento de identificação eletrônico, os dados armazenados no *microchip* são assinados digitalmente através da utilização do certificado *Country Signing Certificate*

[11] Norma técnica BSI-TR-03110, disponível em https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110.html

Authority (CSCA), estando este disponível somente para fabricantes autorizados oficialmente. Este certificado forma a base para a infraestrutura CSCA-PKI, uma hierarquia de certificados que verifica a integridade dos dados de documentos de identidade. Quando a leitura dos dados do *eID Card* ocorre, a Autenticação Passiva verifica a assinatura armazenada no chip e faz o rastreamento até a CSCA, garantindo desta forma que os dados não estejam comprometidos (for Information~Security, 2010).

A Autoridade *Country Verifying Certificate Authority* (CVCA) é responsável pela emissão dos certificados utilizados durante a leitura do *eID Card* pelos Terminais de Autenticação, definindo direitos de leitura individuais, por exemplo, determinando qual informação pode ser lida no documento de identidade eletrônico. Estes certificados são também utilizados para leitura das impressões digitais do portador (for Information~Security, 2010).

O provedor de certificados, conhecido por BerCA, é responsável por fornecer os certificados para os provedores de serviço, emitindo-os em conformidade com a "Lei de Assinatura digital[12]", com a "Portaria de Assinatura[13]" e com as políticas e orientações técnicas emitidas pelo "Serviço Federal de Segurança em Tecnologia da Informação - BSI" (Bundesministerium des Innern, 2014b).

Utilizar certificados digitais, emitidos pelas autoridades mencionadas acima, é obrigatório para que os sistemas de Identificação Eletrônica ocorram de forma segura, uma vez que estes permitem a confiança mútua entre usuários e SPs. Ao conjunto de certificados utilizados no processo autenticação, autorização e troca de informações é dado o nome de "certificados de autorização" (*authorization certificates*), os quais são utilizados antes e durante cada leitura do *eID Card*, determinando quais consultas são permitidas e participando do processo de envio dos dados pessoais do usuário para o provedor de serviço (Bundesministerium des Innern, 2014b).

2.3.6 Obrigatoriedade da Identidade Eletrônica

A Lei de 18 de junho de 2009 sobre Identidade Civil e Identidade Eletrônica, alterada em 22 de dezembro de 2011, afirma que todo cidadão alemão maior que 16 anos é obrigado a ter um documento de identidade civil, a qual terá validade de 6 anos

[12] http://www.gesetze-im-internet.de/sigg_2001/index.html
[13] http://www.gesetze-im-internet.de/sigv_2001/index.html

até o cidadão completar 24 anos, após esta idade o documento de identidade passará a ter validade de 10 anos. Entretanto, esta obrigatoriedade não se aplica à Identidade Eletrônica. Segundo a Lei, todo cidadão maior de 16 anos pode a qualquer momento solicitar por escrito à autoridade competente a desativação da função de identificação eletrônica, cabendo ao fabricante do cartão realizar o procedimento. Casos de cancelamento, perda ou roubo da eID deverão ser comunicados ao administrador da lista de revogação, o qual fará a replicação da lista aos provedores de serviços, evitado problemas de fraude (Bundesministerium der Justiz und für Verbraucherschutz, 2014).

2.4 Sistemas de Gestão de Identidades

2.4.1 Padrão Adotado de Identidade Eletrônica (eID)

A interoperabilidade, no modelo de gestão de identidades alemão, está presente desde a confecção do cartão de identidades até a escolha dos sistemas adotados. Fabricado pela Bundesdruckerei, uma empresa privada contratada pelo governo da Alemanha, o novo *eID Card* segue padrões e normas internacionais como a ISO 14443 (ISO 2009). Quanto aos sistemas, a escolha por tecnologias consolidadas e de código aberto, como por exemplo o SAML, permitiu que o modelo de gestão fosse adaptado facilmente pelas empresas, garantindo dessa forma, o ingresso de entidades privadas para atuarem como provedores de identidade e de serviços.

Diante deste cenário, o governo alemão atua fortemente através do Ministério Federal do Interior (IMC) e do Departamento Federal de Segurança em Tecnologia da Informação (BSI), ditando padrões, homologando provedores (SPs e IdPs) e fiscalizando todas as empresas envolvidas no modelo de GId. Todos os padrões adotados são disponibilizados pelo BSI em formato de ”Normas Técnicas”, os quais servem como modelo de referência para implementação e funcionamento de todos os sistemas, desde provedores de serviços até as infraestruturas de chaves públicas.

2.4.2 Modelo de Gestão de Identidades

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, por exemplo, nome, sobrenome, data e local de

nascimento (European 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[14] para os provedores de serviços implantarem seus próprios provedores de identidade, ou *eID-Servers*, como são conhecidos no país.

A norma conhecida como ”Orientação Técnica BSI TR-3130[15]” 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, a saber.

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**.

2.4.3 Tecnologias de Gestão de Identidades

O modelo alemão de gestão de identidades recebe o nome de eID-Infraestrutura. De acordo com a norma BSI-TR-03130, uma das tecnologias adotadas neste modelo é o SAML (*Security Assertion Markup Language*) (for Information~Security, 2014), uma linguagem consolidada e amplamente utilizada, em especial, em cenários que visam interoperabilidade (entre países). No entanto, esta linguagem não pôde ser aplicada diretamente no eID-Infraestrutura sem passar antes por um processo de adaptação, tendo que se adequar aos padrões de comunicação estabelecidos pelo Departamento Federal de Segurança. A Tabela 1 apresenta algumas regras definidas no modelo SAML e sua regra respectiva no modelo eID-Infraestrutura (for Information~Security, 2014).

[14] https://www.bsi.bund.de/ElektronischeAusweiseTR.html
[15] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03130/tr-03130.html

Tabela 1: Mapeamento de termos da especificação SAML para a eID-Infraestrutura

Usuário	Usuário
Agente Usuário (*User Agent*)	eID-Cliente
Provedor de Serviço (SP)	Provedor de Serviço
Provedor de Identidade (IdP)	Servidor eID

Um dos componentes do modelo eID-Infraestrutura é o eID-Interface, que é constituído de um serviço *web* criado para regular o fluxo de comunicação entre os diferentes atores do modelo de gestão de identidade (IdP, SP e Usuário/Agente de usuário). O eID-Interface é baseado no padrão WSDL[16] (*Web Services Description Language*) e no SOAP[17]. Enquanto o primeiro padrão define o procedimento necessário para que se estabeleça a comunicação em um sistema distribuído, o segundo providencia o transporte dos dados do usuário propriamente dito (for Information~Security, 2014).

2.4.4 Provedores de Identidade Privados

O Departamento Federal de Segurança em Tecnologia da Informação[18] (BSI) é o órgão do governo responsável por auditar, homologar e estabelecer as diretrizes de ingresso dos provedores de identidade privados. Atuando em parceria com o Ministério Federal do Interior[19] (BMI), foi criado o portal do documento de identidade[20] (*Personalausweis Portal*) o qual contém todas as informações necessárias para as entidades privadas que queiram tornar-se um provedor de serviço ou um provedor de identidade.

A possibilidade de ingresso de SPs e IdPs privados na estratégia nacional de gestão de identidades, concede ao cidadão poder de escolha no uso dos sistemas *on-line* de e-Gov. Esta estratégia adotada pelo governo alemão existe desde 2010, com a implantação do novo cartão de identidade eletrônico (European Comission, 2014d).

[16] Especificação desenvolvida pelo W3C (www.w3.org) que permite descrever os *Web Services* segundo um formato XML.
[17] Especificação desenvolvida pelo W3C para garantir a interoperabilidade e intercomunicação entre diferentes sistemas, através da utilização da linguagem XML e do mecanismo de transporte HTTP ou outro como, por exemplo o SMTP
[18] https://www.bsi.bund.de/DE/DasBSI/dasbsi_node.html
[19] http://www.bmi.bund.de/
[20] http://www.personalausweisportal.de/DE/Verwaltung/Diensteanbieterwerden/diensteanbieter_node.html

2.4.5 Padrões de Interoperabilidade

O padrão de interoperabilidade no modelo de gestão de identidades alemão é oferecido pelo uso de certificados emitidos no padrão X.509 pelo provedor de certificados (BerCA) e pelo uso de padrões estabelecidos pelo Departamento Federal de Segurança da Informação (BSI). Estes padrões são ditados com base em protocolos e linguagens amplamente utilizados como o SAML, SOAP e WSDL utilizados, por exemplo, pelo eID-Interface (for Information~Security, 2014).

Coordenando a adesão de novos SPs e IdPs, através de uma sequência de procedimentos obrigatórios, o BSI garante a interoperabilidade destes provedores inseridos no cenário de governo eletrônico alemão. Somente seguindo esta sequência de procedimentos, os provedores de serviços e de identidades conseguem a homologação necessária para poder operar no país (for Information~Security, 2014).

2.4.6 Gestão de Confiança

Toda gestão de confiança adotada na Estratégia Nacional de gestão de identidade eletrônica está baseada nos padrões tecnológicos estabelecidos, nas diretrizes de ingresso de novos provedores (SPs e IdP) e, principalmente, na infraestrutura de chave pública (PKI) descrita na Seção 3.5. É justamente a infraestrutura de chave pública que permite o ingresso de entidades privadas no modelo de e-Gov e que garante a confiança mútua entre governo e entidades externas nas comunicações eletrônicas.

O Departamento Federal de Segurança em Tecnologia da Informação (BSI), órgão do governo federal, é responsável por fazer a gestão das tecnologias utilizadas na Estratégia Nacional de Gestão de Identidades, atuando como operador da federação.

2.4.7 Níveis de Garantia dos Provedores de Identidades

Não existe um padrão de pontuação (ou definição de nível) para os provedores de identidades, de forma a classificá-los segundo algum nível de garantia como o estabelecido pelo NIST[21]. No entanto, o Departamento Federal de Segurança em

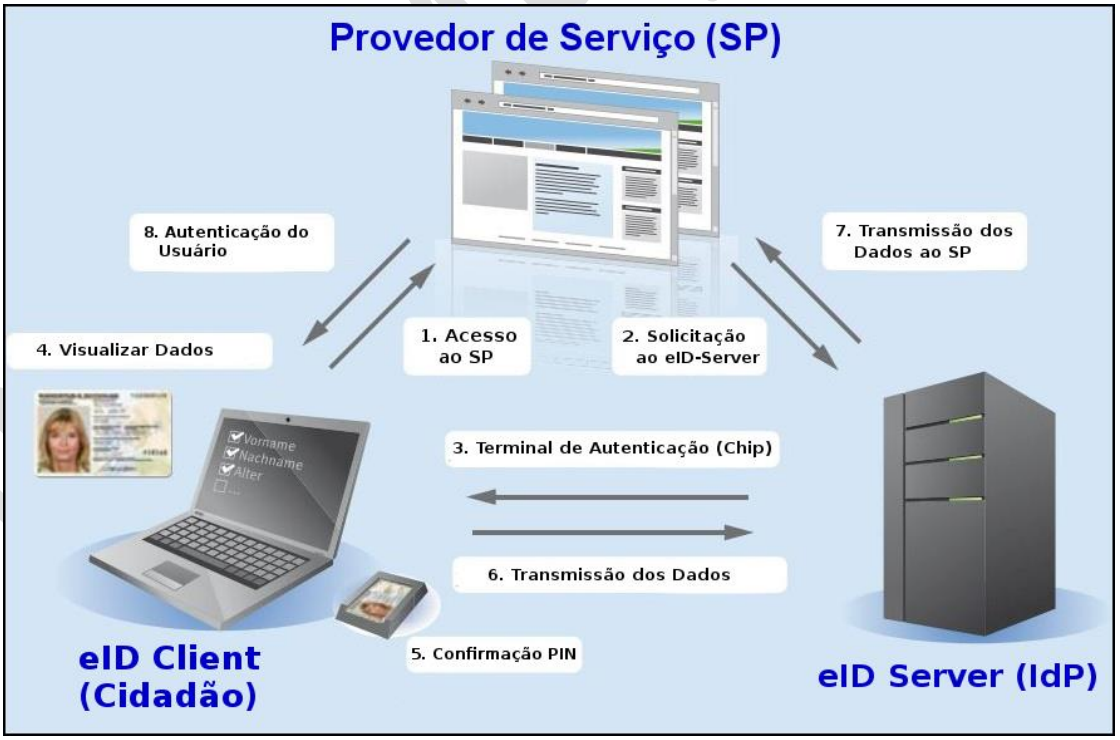
[21] http://www.itl.nist.gov/lab/bulletns/bltnaug04.htm

Tecnologia da Informação (BSI) disponibiliza em seu *website*[22] uma série de normas técnicas para consulta pública. Estas normas ditam padrões e perfis de segurança a serem seguidos por todas entidades que desejarem implementar alguma solução em governo eletrônico na Alemanha.

2.4.8 Mecanismos ou Técnicas de Autenticação

De acordo com Bundesministerium des Innern (2014f), o provedor de identidades é utilizado apenas como mediador no processo de autenticação, uma vez que não possui os atributos do cidadão armazenados em base de dados própria. Em outras palavras, o IdP atua como uma ”terceira parte confiável”, garantindo tanto a autenticidade do usuário quanto do provedor de serviço. A seguir são apresentadas as etapas de autenticação e autorização envolvidas no modelo de e-Gov alemão, exemplificadas pela figura 1.

Figura 1: eID Server - Processo de Autenticação.



1. O titular do cartão acessa o provedor de serviço utilizando seu computador pessoal.

[22] https://www.bsi.bund.de/ElektronischeAusweiseTR.html

2. O SP encaminha a solicitação de autenticação para um provedor de identidade - *eID Server*.

3. É estabelecido um canal seguro entre o *eID Server* e o *eID Client* (*software* cliente) para verificar a autenticidade do usuário.

4. O *eID Client* mostra ao titular quais atributos foram solicitados. O usuário decide quais dados do cartão serão transmitidos.

5. O titular digita o o código PIN do cartão, autorizando dessa forma a transferência dos dados.

6. Os dados de identificação são transmitidos ao *eID Server.*

7. O *eID Server* envia uma resposta de autenticação para o SP, juntamente com os dados autorizados pelo usuário.

8. O SP analisa as informações e decide se a autenticação é considerada bem sucedida. Finalmente, uma resposta ao usuário é apresentada autorizando ou não o acesso ao serviço.

2.5 Privacidade relacionada a Identidade Eletrônica

2.5.1 Uso de Pseudônimos

Dependendo do provedor de serviço acessado, como um fórum ou um *chat*, por exemplo, no qual o cidadão não deseja ser identificado, é permitido o envio de um pseudônimo no lugar do nome e sobrenome do cidadão. Esta medida visa preservar oculta a identidade do cidadão no acesso a alguns serviços (Bundesministerium des Innern, 2014d).

2.5.2 Poder de escolha do Cidadão (eID e provedores de identidades)

O cidadão tem apenas uma única identidade eletrônica, uma vez que ela está vinculada ao cartão de identificação. Uma segunda eID só pode ser emitida com o vencimento do primeiro cartão de identificação civil (Bundesministerium der Justiz und für Verbraucherschutz, 2014). No entanto, a lei assegura ao portador do cartão ativar ou desativar a função de identidade eletrônica a qualquer momento por meio de solicitação por escrito à autoridade emissora (Bundesministerium der Justiz und für Verbraucherschutz, 2014).

Como todos os atributos do cidadão são armazenados no *eID Card* do portador,

não há necessidade de manter estes dados no provedor de identidades. Dessa forma, o IdP realiza um papel importante que é de assegurar a identidade tanto do SP quanto do usuário, fazendo isso com a conferência dos certificados digitais. Devido a esta característica existem diversos IdPs operado no país, sendo instalados a partir de normas técnicas disponíveis para este fim e publicadas pelo BSI. O usuário pode escolher qual utilizar.

2.5.3 Controle de Liberação de Dados Pessoais

O *eID Card* foi projetado para armazenar de forma segura as informações do portador, dados estes só visualizados ou liberados para o provedor de serviços após o aceite do usuário. Esta liberação somente ocorre após a digitação do código PIN, conforme descrito na Seção 4.8. Através do *software* cliente, conhecido por "AusweisApp2" e disponibilizado pelo Departamento Federal de Segurança da Informação (BSI), o usuário pode visualizar os dados armazenados no *microchip* do cartão e interagir com os SPs.

As políticas de privacidade respeitam o princípio de minimização dos dados, que determina o envio do "mínimo de informações pessoais nas transações *on-line*". Estes dados devem realmente fazer algum sentido ao provedor de serviços, de forma que, o SP tenha atributos suficientes para permitir ou não o acesso ao serviço (Bundesministerium des Innern, 2014d). Portanto, o provedor de serviço deverá informar explicitamento ao usuário, quais dados pessoais está solicitando e qual o propósito desta solicitação. O usuário por sua vez, pode permitir ou não o acesso a estas informações (Die Beauftragte der Bundesregierung für Informationstechnik, 2014).

2.5.4 Leis Específicas de Privacidade

A Alemanha possui uma das mais rigorosas leis de proteção de dados da União Europeia, sendo que a primeira Lei é de 1970. Uma revisão em 2002 alinhou a legislação vigente com as diretrizes de proteção de dados pessoais da União Europeia (95/46/EU) (European Comission, 2014d).

2.5.5 Aplicação da Lei de Privacidade

A gestão de uso do identificador eletrônico segue tanto padrões de segurança física[23] ,no que diz respeito ao visual do cartão, quanto padrões para segurança através de comunicações eletrônicas. (Bundesministerium des Innern, 2014h).

A função de identificação eletrônica segue basicamente dois princípios, a saber (Bundesministerium des Innern, 2014h).

1˚ Princípio: segurança dos dados.

2˚ Princípio: minimização dos dados.

O princípio de segurança dos dados segue as seguintes diretrizes.

• O cidadão decide qual SP acessar e deverá ter a opção de confirmar se irá liberar seus dados pessoais ou não.

• Todos provedores de serviço utilizarão certificados emitidos por uma entidade certificadora homologada.

• Antes de cada liberação de atributos, o usuário é informado e pode ou não permitir esta transmissão.

• A aprovação dos dados só ocorre com a digitação do código PIN.

• Os dados são sempre encaminhados por canais de comunicação criptografados.

• A eID só funciona com leitores de cartão, portanto diminui a possibilidade de acesso às informações pessoais do cidadão de outra forma.

• Somente os cidadãos que possuem o cartão e sabem sua senha pessoal podem utilizar a eID.

O princípio da minimização dos dados segue as seguintes diretrizes.

• Só é transmitida as informações realmente necessárias ao provedor de serviços, ou seja, o SP só pode solicitar os dados que realmente precisa.

• Para alguns serviços somente o uso de pseudônimo é necessário, sem fazer uso do nome e sobrenome do usuário.

Estas diretrizes são auditadas pelo Departamento Federal de Segurança da Informação, garantindo que as leis de privacidade sejam realmente aplicadas no país.

23 http://www.personalausweisportal.de/DE/BuergerinnenundBuerger/DerPersonalausweis/Steckbrief/steckbrief_node.html

3 ÁUSTRIA

3.1 Perfil Sociopolítico, Econômico e Governo Eletrônico

3.1.1 Estrutura Sociopolítica

A Áustria é um país com cerca de 8,4 milhões de habitantes. Localizada na Europa Central faz fronteira com países como a Alemanha, Hungria, Eslovênia, Itália e Suíça. A maioria da população fala alemão, muito embora o croata, húngaro e esloveno também sejam considerados idiomas oficiais. O país possui um área de 83.870 km² e uma densidade populacional na ordem de 100 hab/km², possui um PIB nominal *per capita* na ordem de 51.183 dólares, sendo considerado um dos países mais ricos do mundo (vigésimo oitavo em 2013 pelo FMI). O seu Índice de Desenvolvimento Humano (IDH) é considerado muito alto (0,881) e ocupa a 21ª posição do *ranking* da ONU (Programa das Nações Unidas para o Desenvolvimento - PNUD) de 2014[24]. A Áustria aderiu à União Europeia em 1995 e ao Euro como moeda oficial em 1999. É um dos países fundadores da Organização para a Cooperação e Desenvolvimento Econômico (OECD).

O governo é regido por uma democracia representativa parlamentar composta por nove estados federais. A capital Viena é a maior cidade do país com uma população na ordem de 1,6 milhões de pessoas. O chefe de Estado é o Presidente Federal, o qual é eleito por voto popular direto. O presidente do governo federal é o Chanceler Federal, nomeado pelo presidente. Desde 2007, os cidadãos acima dos 16 anos de idade tem direito ao voto, muito embora o voto não seja obrigatório (CIA, 2014a).

3.1.2 Acesso à Internet

De acordo com *European Comission* (2014a), em relação aos índices de acesso à Internet em 2013, as seguintes estatísticas da Áustria são apresentadas.

- Casas com acesso à Internet: 81%.
- Empresas com acesso à Internet: 98%.
- Casas com acesso por banda larga: 80%.
- Empresas com acesso por banda larga: 93%.

[24] http://hdr.undp.org/sites/default/files/hdr14-summary-en.pdf

• Indivíduos que fizeram compras pela Internet (últimos 3 meses): 46%.
• Empresas que receberam pedidos de compras *on-line* (último ano): 16%.

Em relação ao número de usuários de Internet, a Áustria ocupa a 52ª posição mundial, porém possui uma alta taxa de penetração de 83,68% (percentagem da polução com acesso à Internet)[25], o que indica um alto nível de inclusão digital. Em relação ao índice de infraestrutura em telecomunicações (ITT) (United Nations, 2014), a pontuação da Áustria (0,7597) é superior a média europeia (0,6678). Este índice foi obtido a partir dos seguintes componentes (United Nations, 2014).

• Telefone fixo (cada 100 habitantes): 39,49.
• Telefone celular (cada 100 habitantes): 160,54.
• Conexão à Internet Banda Larga (cada 100 habitantes): 25,13.
• Conexão à Internet *Wireless* (cada 100 habitantes): 40,66.

O relatório publicado em *Statistics Austria* (2014) apresenta evolução no uso da Internet pela população de 37% em 2002 para 81% em 2014, o que demonstra crescimento no uso superior a 220% em um intervalo de 12 anos.

3.1.3 *Ranking* de e-Gov da ONU

De acordo com a ONU, classificada com o índice de 0,7912, a Áustria passou a ocupar a 20ª posição no *ranking* de desenvolvimento de governo eletrônico (EGDI) em 2014, subindo uma posição em relação ao ano de 2012. No que se refere ao *ranking* de eParticipação da ONU, a Áustria está entre os 50 melhores países (40º posição). O índice de desenvolvimento em e-Gov apresentou as seguintes informações (United Nations, 2014).

• Serviços Online: 0,7480 (média na Europa é de 0,5695).
• Infraestrutura em Telecomunicações: 0,7597 (média na Europa é de 0,6678).
• Capital Humano: 0,8660 (média na Europa é de 0,8434).

3.1.4 Principais Políticas (Leis, atos, decretos, etc)

As principais leis relacionadas ao desenvolvimento de e-Gov e gestão de

[25] Fonte: http://www.internetlivestats.com/internet-users-by-country/

identidade que se destacam na Áustria são as seguintes.

• **1997:** criada a Lei de Comércio Eletrônico, aplicável a todos os serviços providos via Internet.

• **1999:** criação do Ato de Assinatura Eletrônica, o qual entrou em vigor em 1/1/2000, tornando a Austria o 1º país membro da União Europeia a implementar a Diretiva 1999/93/EC sobre assinaturas eletrônicas. O Ato reconhece legalmente assinaturas eletrônicas que cumprem certos requisitos de segurança e ao mesmo tempo estabelece algum valor legal para assinaturas menos seguras. Este Ato regulamenta as condições para o uso de assinaturas eletrônicas no setor público, bem como o uso de cartões do cidadão.

• **2000:** criação da Lei de Proteção dos Dados, incluindo os direitos fundamentais de privacidade.

• **2001:** criação da Lei Geral dos Processos Administrativos. O artigo 13 trata especificamente de governo eletrônico, regulamentando a comunicação entre cidadãos e autoridades públicas, como por exemplo transmissões feitas por *e-mail* ou formulário *web*.

• **2003:** criada a Lei de Telecomunicações, trazendo para o quadro de Leis Nacionais a regulamentação européia de uso de um *framework* para comunicações eletrônicas.

• **2004:** criação da Lei de e-Gov, a qual se tornou a base legal de todas as políticas de governo eletrônico na Áustria. A comunicação dos cidadãos com o governo, a utilização de cartão eletrônico e o serviço de entrega de documentos eletrônicos às entidades privadas são exemplos de assuntos tratados nesta lei.

• **2008:** entram em vigor as revisões feitas em 2007 das seguintes leis: Governo Eletrônico, Assinatura Digital, Procedimento Administrativo e Serviço de Documentos.

• **2011:** em complemento a Lei Geral dos Processos Administrativos de 2001, no dia primeiro de janeiro de 2011 passa a valer a obrigatoriedade para as autoridades de assinarem eletronicamente documentos públicos, valendo-se de um certificado de segurança qualificado pelo governo.

3.1.5 Cronologia do Desenvolvimento de e-Gov e GId

A seguir, destacam-se alguns marcos importantes para o desenvolvimento de e-

Gov na Áustria bem como a implantação da estratégia nacional de gestão de identidades.

• **1995:** lançada a "Iniciativa da Sociedade da Informação", que trata da criação de um grupo de trabalho composto por 350 especialistas, com a missão de identificar oportunidades e ameaças representadas pelo desenvolvimento da Sociedade da Informação na Áustria.

• **1997:** lançada a versão piloto do portal HELP[26] com o objetivo de auxiliar os cidadãos no uso dos serviços oficiais do governo.

• **2002:** entra em operação a ZMR (Central de Registro dos Residentes), uma base de dados que aloca um número para cada cidadão registrado na Áustria.

• **2004:** implantado o cartão do cidadão (*eCard - citizen card*).

• **2005:** feita a integração do *eCard* com os sistemas bancários, médicos, de educação, entre outros. Este cartão passou a armazenar um certificado digital, o qual possibilita a assinatura eletrônica de documentos.

• **2006:** emitida a primeira versão do passaporte eletrônico (*ePassport*), com a inclusão de dados pessoais do titular e fotografia digitalizada.

• **2009:** lançada a versão do cartão do cidadão para telefones móveis. O serviço desenvolvido a partir do *framework* do projeto STORK[27] promove autenticação e autorização seguras utilizando somente o celular, dispensando o tradicional *eID Card* e o leitor de cartões. Neste mesmo ano, é anunciado que 100% dos serviços públicos serão disponibilizados de forma *online*, permitindo, por exemplo, ao cidadão fazer a emissão da 2ª via de certidões de nascimento e de casamento através da Internet.

• **2012:** contando com uma estrutura de metadados em XML, é lançado neste ano o *Open Government Data Portal* com o objetivo de disponibilizar informações gerais das instituições públicas aos cidadãos. Ainda em 2012, todos os escritórios fiscais passam a oferecer também acesso aos seus aplicativos pela *Internet* e através da versão via celular do *eID Card*. Esta facilidade permitiu aos cidadãos começarem a fazer a entrega do imposto de renda de forma *on-line*.

• **2014:** a partir de janeiro deste ano, as autoridades federais passaram a não aceitar mais faturas emitidas em papel ou enviadas por *e-mail*. Somente faturas

[26] www.help.gv.at
[27] https://www.eid-stork2.eu/

emitidas a partir de formulários *on-line* passaram a serem aceitas.

3.2 Modelo de Organização de Documentos Civis

3.2.1 Registro Civil

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[28]), base de dados conhecida por LMR. Mas, em março de 2002 o "Registro Central de Residentes[29] (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 (European Comission, 2014a).

Apesar da criação da Base de Dados Central (CRR), muitos municípios ainda mantiveram suas bases de dados locais (LMR). Entretanto, por determinação do governo, os municípios que não migraram suas informações para a CRR foram obrigados a manter um sincronismo com esta. Dessa forma, a partir de 2002, passa a existir uma única base de dados central com as informações civis dos cidadãos. Como consequência desta base centralizada, passa a ser atribuído a todo cidadão austríaco o IdCRR, que é um identificador único composto por 12 caracteres decimais randômicos (40 bits) (Zwattendorfer et al., 2011).

3.2.2 Identidade Civil

O documento de identidade civil é emitido no formato de um cartão de plástico semelhante a um cartão de crédito, sendo emitido apenas por solicitação do cidadão, uma vez que sua adesão é voluntária. Muito embora conste na Lei da Polícia de Segurança[30] a emissão não obrigatória, o governo incentiva sua utilização visto que seu formato facilita a identificação do cidadão perante as autoridades oficiais, agências de segurança e setores privados [Govenment of the Austria, 2014a].

A carteira de identidade pode ser emitida pela administração do distrito, mas normalmente é feita em uma delegacia de polícia perante a apresentação de uma foto

[28] Em alemão *Lokales Melderegister*
[29] Em alemão *Zentrales Melderegister* (ZMR) - http://zmr.bmi.gv.at/
[30] http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen Gesetzesnummer=10005792

3x4, de um comprovante de escolaridade, da certidão de nascimento ou casamento e o preenchimento de um formulário de inscrição. Utilizada como um documento de identificação dentro do país, ela não pode ser utilizada como substituto do passaporte. Sua validade está condicionada ao reconhecimento do indivíduo através de sua foto, legibilidade do documento e atualização das informações. A partir do momento em que não é possível identificar o cidadão através da foto ou as informações pessoais estão desatualizadas, uma 2ª via deve ser emitida em substituição à anterior (Govenment of the Austria, 2014a).

3.2.3 Relação do Documento de Viagem com a Identidade Civil

Na Áustria o *Passport Authority* é responsável pela emissão do passaporte para os cidadãos, sendo representado pela Direção do Distrito nas cidades de Leoben[31] e Schwechat[32], e pelo *District Council Office* em Viena[33]. Para a emissão, é obrigatória a apresentação de um documento de identificação com foto, passaporte antigo (se houver), certidão de nascimento ou casamento, foto 35 x 45 mm emitida nos últimos 6 meses, comprovante de escolaridade e pagamento de taxa e emissão (valor de 75,90 Euros). Caso o cidadão não possua uma identificação oficial com foto é aceito o uso da identidade civil de uma testemunha (Govenment of the Austria, 2014c).

A partir de 15 de junho de 2012, menores de 18 anos que realizem viagens internacionais precisam de passaporte próprio. Crianças recém nascidas devem estar presentes no ato da emissão do passaporte para comprovação da identidade. A partir de 15 de junho de 2009, a emissão do passaporte deve ser feita exclusivamente com *chip* eletrônico (*ePassaporte* - criado em 2006), que armazena fotografia e dados pessoais, incluindo impressões digitais de crianças maiores de 12 anos (Govenment of the Austria, 2014b).

3.3 Identidade Eletrônica

3.3.1 Uso da Identidade Eletrônica

A criação do identificador eletrônico é baseada no identificador civil, o IdCRR descrito na seção 2.1, garantindo dessa forma, que não haverá mais de um eID para o

[31] http://www.leoben.at/fileadmin/redakteure/formulare/buergerservice/reisepass.pdf
[32] http://www.schwechat.gv.at/de/serviceleistungen/dokumente/453/Reisepass-mit-Chip
[33] http://www.wien.gv.at/verwaltung/passservice/stellen.html

mesmo cidadão. No entanto, o uso deste Id está sob restrições específicas de proteção de dados, as quais impedem seu uso diretamente nos processos de governo eletrônico. Neste contexto, a Autoridade de Registro sourcePIN (SRA - *sourcePIN Register Authority*) exerce fundamental papel, sendo responsável por criptografar o IdCRR. 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 et al., 2011).

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). De forma a viabilizar o uso desta tecnologia neutra, foi criado o "*identity link*". O *identity link* é uma estrutura SAML, emitida pela Autoridade de Registro sourcePIN (SRA), a qual 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 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 et al., 2011).

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 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 et al., 2011).

3.3.2 Cadastro da Identidade Eletrônica

Como citado na seção 3.1, o conceito chamado de "cartão do cidadão" foi criado para viabilizar o cadastro e uso da identidade eletrônica na Áustria. Ele opera atualmente sob o formato de um cartão de plástico (*smartcard*) ou através de solução em telefone celular (*smartphone*). A atual política de TIC austríaca permite que a identidade eletrônica possa ser ativada em diversos cartões e em diversos telefones celulares, simultaneamente. Isto só é possível porque é utilizado o mesmo identificador (sourcePIN), garantindo portanto a identificação única do usuário, independentemente da quantidade de soluções adotadas pelo mesmo cidadão (Bürgerkarte, 2014).

Os cartões de cidadão em formato de *smartcard* foram emitidos em 2005 pelas operadoras de plano de saúde, para todos os cidadãos austríacos. Em 2007, a empresa pública *Main Association of Social Insurance Organisations*[34] passou a cuidar da emissão destes cartões de saúde. Em 2008, foi permitido que a empresa privada A-Trust[35] também se tornasse um emissor de cartões, ampliando os tipos de cartões aceitos. Atualmente, para que possam ser utilizados para autenticação nos SPs, estes *smartcards* devem possuir as "funcionalidades de cartão do cidadão", o que efetivamente é feito pelos cartões emitidos pela A-Trust.

Dentre os *smartcards* reconhecidos para uso como cartão do cidadão, podem ser cidados os seguintes (European Communities, 2009a).

- Cartão do Plano de Saúde (*e-Card*).
- Cartão de Servidores Públicos,
- Cartão de Estudante.

[34] http://www.sozialversicherung.gv.at
[35] http://www.a-trust.at

• Cartões de Banco.

Para utilizar o cartão do cidadão no formato de *smartcard*, deve-se comprar um leitor de cartão homologado pelo governo, instalar o *software*[36] do leitor, adquirir o *smartcard* e ativar a funcionalidade de cartão do cidadão através de uma das seguintes opções gratuitas (Bürgerkarte, 2014).

• De forma *on-line* no site a A-Trust[37].
• Através do site FinanzOnline[38] do governo.
• Pessoalmente, em um dos 135 locais de registro[39] na Áustria, apresentando documento de identificação com foto, ou por meio de solicitação por correio com uso de carta registrada.

A ativação do cartão do cidadão por meio *on-line* só é possível pois, os leitores de cartão homologados pelo governo, possuem tanto a função de leitura quanto a função de escrita no *chip* do *smartcard* (Bürgerkarte, 2014).

Desde o final de 2009, os cidadãos passaram a fazer uso de uma segunda opção de cartão do cidadão em *MobileID* conhecida como "*Mobile Phone Signature*". 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 (Bürgerkarte, 2014).

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 do *MobileID* 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[40], uma associação sem fins lucrativos localizada na sede da Polícia Federal em Viena.

[36] http://support.gemalto.com/index.php?id=pc_usb_sl
[37] https://www.a-trust.at/e-card/selfdata.aspx
[38] https://finanzonline.bmf.gv.at/
[39] http://www.buergerkarte.at/en/registration-authorities.html
[40] www.a-sit.at

3.3.3 Atributos da Identidade Eletrônica

Quando as funcionalidades do cartão do cidadão são ativadas, conforme os procedimentos descritos na seção 3.2, dois certificados digitais e um *identity link* são gravados no *smartcard* ou no *MobileID*. Conforme citado na referida seção, esta ativação pode ser feita pelo próprio usuário através de aplicações *on-line*, uma vez que o leitor de cartões, por exemplo, permite que informações sejam lidas ou gravadas no *chip* do *smartcard* (European Comission, 2014a).

Os atributos do cidadão, que compõem a identidade eletrônica, são armazenados no cartão do cidadão através do *identity link*, fazendo parte destes atributos as seguintes informações.

- Primeiro Nome.
- Último Sobrenome.
- Data de nascimento.
- Sexo.
- sourcePIN.

A única ligação entre a identidade civil e a identidade eletrônica é encontrada no processo de ativação do cartão do cidadão, caso o cidadão opte pela ativação comparecendo pessoalmente em um dos locais de registro, uma vez que precisa apresentar um documento de identificação com foto. Optando pela ativação presencial, o local de registro realiza a gravação dos certificados digitais e do *identity link* no cartão do usuário.

3.3.4 Biometria

De acordo com European Communities (2009a), nenhum dado biométrico é coletado ou armazenado no cartão do cidadão, tanto na solução em *smartcard* quanto na solução em *MobileID*. Entretanto, seguindo as recomendações feitas pelo *Austrian CIO Office*[41], o cartão do cidadão deve possuir pelo menos um mecanismo de proteção, no que se refere ao acesso dos certificados digitais. Muito embora as recomendações sugiram que este mecanismo de acesso possa ser implementado com

[41] Karlinger G.: " Anforderungen an die BürgerkartenUmgebung nach dem Konzept Bürgerkarte, Spezifikation Version 1.0.0", Chief Information Office Austria, 2002.

o uso de PIN (*personal identification number*) ou com o uso de dados biométricos, a implementação atual utiliza somente o PIN como mecanismo de segurança (British Crown, 2002).

3.3.5 Uso de Certificado Digital na Identidade Eletrônica

De acordo com o *Austrian CIO Office*, é recomendado que o cartão do cidadão possua dois pares de certificados digitais, os quais devem ser emitidos por um Provedor de Serviço de Certificação (CSP - *Certification Service Provider*). Atualmente, a empresa privada A-Trust[42] opera na Áustria como CSP emitindo os seguintes certificados (British Crown, 2002).

1. Assinatura Qualificada: o uso deste certificado é obrigatório para que o cidadão acesse os sistemas de governo eletrônico, apesar de ser recomendada sua aquisição. A emissão do cartão do cidadão é feita juntamente com este certificado digital.
2. Par de chaves adicionais: conhecido também como “assinatura eletrônica simples”, este certificado digital é opcional uma vez que trará funções extras de segurança. Trata-se basicamente de um certificado pessoal utilizado para assinatura e criptografia de documentos.

O termo “Assinatura Qualificada” foi inserido pela EESSI (*(The European Electronic Signature Standardization Initiative)*) e se refere aos certificados digitais que são emitidos em conformidade com as especificações previstas em lei. Como o termo não foi utilizado na diretiva 1999/93/EC[43], ficou a critério de cada país da união européia a adoção do mesmo termo em suas leis, o que foi feito pela grande maioria. No entanto, a Áustria preferiu utilizar o termo “Assinatura Eletrônica Segura” em sua lei de assinaturas[44] e na *signature order*[45] (British Crown, 2002).

3.3.6 Obrigatoriedade da Identidade Eletrônica

[42] https://www.a-trust.at/ATrust/CompanyProfile.aspx
[43] Directive 1999/93/EC of the European Parliament and of the Council of 13. December 1999 on a community framework for electronic signatures.
[44] Austrian signature law: “Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG)”, BGBl. I Nr. 190/1999, BGBl. I Nr. 137/2000, BGBl.
[45] Austrian signature order: “Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV)”, StF: BGBl. II Nr.

De acordo com European Communities (2009a), a adoção do cartão do cidadão é feita de forma voluntária, com exceção de alguns cargos públicos específicos, para os quais é obrigatório o uso de uma identidade eletrônica.

3.4 Sistemas de Gestão de Identidades

3.4.1 Padrão Adotado de Identidade Eletrônica (eID)

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 (*MobileID*), o qual chamou de *Mobile Phone Signature*. Esta solução em *MobileID* 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* que necessita de *hardware* e *software* específicos para o funcionamento (European Comission, 2014a).

O padrão para a ativação do cartão do cidadão (identidade eletrônica), tanto para a solução de *MobileID* quanto para a solução de *smartcard* foi descrito na Seção 3.2.

3.4.2 Modelo de Gestão de Identidades

Desde a criação do *Central Residents Register* (CRR) em 2002, a Áustria passou a contar com uma base central para armazenar os registros civis (nascimento e casamento) dos seus cidadãos, atribuindo a cada um deles um identificar único conhecido por IdCRR.

De acordo com as leis de privacidade vigentes, é permitido o uso do IdCRR somente em sua forma criptografada. Assim, nasce a Autoridade de Registro sourcePIN (SRA - *sourcePIN Register Authority*), vinculada à Autoridade Austríaca de Proteção de Dados[46], com o objetivo de gerar um número único e criptografado gerado a partir do IdCRR, ao qual denominou de "sourcePIN". O sourcePIN então passou a ser armazenado no cartão do cidadão através de uma asserção SAML (*identity link*), de forma que este identificador único pudesse ser utilizado pelos provedores de serviço nos processos de autenticação *on-line*. Neste contexto, a Autoridade de Registro

[46] http://www.dsb.gv.at/DesktopDefault.aspx?alias=dsken

sourcePIN atua como provedor de identidades, caracterizando na Áustria o modelo de gestão de identidades centralizado.

Para viabilizar tecnicamente a interação entre SPs, IdP e usuários através de seus cartões de cidadão (*smartcard* ou *MobileID*), o governo desenvolveu os Módulos para Aplicações *On-line* (MOA - *Modules for Online Applications*), disponibilizando-os gratuitamente em formato *software* de código aberto, tando para uso pelo setor público quanto para uso pelo setor privado (European Communities, 2009a). A seção 4.5 descreve cada um dos módulos disponibilizados pelo governo federal.

3.4.3 Tecnologias de Gestão de Identidades

Segundo E-Government Innovation Center Graz da Austria (2011), os módulos MOA utilizam as versões 1.0 e 2.0 do SAML para a construção de suas asserções. O uso desta tecnologia, além de viabilizar a concepção do modelo de governo eletrônico baseado em políticas de *software* livre, também traz benefícios conhecidos como a autenticação única SSO (*Single Sign On*).

3.4.4 Provedores de Identidade Privados

As políticas de governo eletrônico da Áustria determinam que o “cartão do cidadão” seja um conceito de tecnologia neutra, de forma que possa ser utilizado por diferentes soluções tecnológicas e por segmentos distintos (público e privado) na Áustria. Apesar desta flexibilidade tecnológica e desenvolvimento de aplicações de código aberto pelo governo, não é permitido o ingresso de provedores de identidades privados no modelo adotado pelo país.

3.4.5 Padrões de Interoperabilidade

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 (Federal Chancellery of Austria, 2015).

Desde junho de 2005, os MOA são disponibilizados 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*[47] 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*[48] da Comissão Europeia, a qual constitui-se de uma plataforma criada para assegurar a interoperabilidade entre os países europeus (Federal Chancellery of Austria, 2015).

Atualmente os módulos suportam as seguintes funcionalidades.

- Identificação (MOA-ID).
- Verificação de Assinatura (MOA-SP).
- Servidor de Assinaturas e Validação (MOA-SS).
- Autorização e Representação (MOA-VV).
- *Software* Cliente (MOCCA).
- Assinaturas Oficiais (MOA-AS).
- Entrega (MOA-ZS).

MOA-ID: este módulo é utilizado unicamente para identificar e autenticar o usuário no processo *on-line* de acesso ao provedor de serviço. O módulo MOA-ID atua como um *middleware* instalado no SP, interagindo com outros módulos, como por exemplo, com o MOCCA para calcular o ssPIN (descrito na seção 3.1) e com o MOA-VV para confirmar a veracidade do sourcePIN.

MOA-SP/SS: este módulo agrega todas as funcionalidades necessárias para criar e verificar a assinatura eletrônica e a assinatura qualificada, para tanto, a criação destas assinaturas é suportada por meio de *software* ou módulo de segurança de *hardware*. Todo processo é baseado em mensagens (perguntas e respostas) no padrão XML, através de funções chamadas pelo servidor *web* usando interfaces SOAP[49] ou

[47] http://egovlabs.gv.at/
[48] https://joinup.ec.europa.eu/software/moa-idspss/home
[49] http://www.w3.org/TR/soap/

Java.

MOA-VV: este módulo foi criado para atuar como proxy, permitindo a integração entre diferentes sistemas. A principal função é permitir o uso da última versão do módulo MOA-ID. O MOA-VV faz a comunicação com a *sourcePIN Register Authority* no processo de autenticação e entrega a resposta ao MOA-ID, permitindo assim que o processo de autorização ocorra.

MOCCA: este é o *software* em código aberto utilizado pelo cartão do cidadão. Implementado em Java, a solução independe de sistema operacional, permitindo assim sua fácil portabilidade. Dois modelos de distribuição são suportados: um na forma de *software* instalado no computador do cidadão e outro oferecido pelo provedor de serviço na forma de um *applet*. Essencialmente, este módulo promove a camada de segurança essencial ao funcionamento do cartão do cidadão. Entre as funções oferecidas por este módulo podem ser citadas as seguintes: prover a comunicação entre o leitor de cartões e o computador; ler o *identity link* e calcular o ssPIN; e suportar o uso do PIN (*personal identification number*).

MOA-AS: implementado em Java, suporta tanto as soluções de *smartcard* quanto de *MobileID*. Sua função é a de promover a assinatura de documentos (Assinatura Oficial) eletrônicos no formato PDF.

MOA-ZS: este módulo é responsável pela comunicação com o agente de entrega (*delivery agent*), avaliação do método de entrega (*method of delivery*), criptografia do conteúdo de documentos eletrônicos (se necessário) e disponibilização dos documentos para impressão ou para um serviço de entrega eletrônico (*delivery services*).

Resumidamente, a interoperabilidade ocorre com o uso de padrões amplamente difundidos como o protocolo HTTP para acesso aos provedores de serviços, pelo XMLDsig[50] (XAdES BES) para as assinaturas eletrônicas e pelas especificações e

[50] http://www.w3.org/TR/xmldsig-core/

padrões SAML, XML e Java utilizados pelos Módulos para Aplicações *On-line* (MOA) nos processos de identificação e autenticação (European Communities, 2009a).

3.4.6 Gestão de Confiança

A gestão de confiança na Áustria é baseada na comprovação da identidade do cidadão e nos módulos para aplicação *on-line* (MOA) utilizados pelos provedores de serviço.

Antes de fazer uso da identidade eletrônica, os cidadãos austríacos devem comprovar sua identidade, optar por uma ou mais soluções (*smartcard* ou *MobileID*) e fazer a ativação do cartão do cidadão. Os procedimentos são descritos na seção 3.2. Por outro lado, o uso dos módulos MOA oferecem a camada de segurança necessária nas comunicações *on-line* e comprovam a identidade do cidadão, conforme descrição feita na seção 4.5.

3.4.7 Níveis de Garantia dos Provedores de Identidades

De acordo com European Communities (2009a), o conceito de cartão do cidadão se baseia em assinaturas qualificadas como único nível de segurança entre o usuário e o provedor de serviço. Desta forma, existem apenas dois níveis de garantia: sem identificação ou identificado utilizando o cartão do cidadão.

O provedor de identidades é centralizado no governo, cabendo aos módulos MOA-ID e MOCCA a função de verificar e comprovar a identidade do usuário. Portanto, cabe aos módulos MOA a função de promover o nível de garantia entre os SPs e o IdP governamental.

3.4.8 Mecanismos ou Técnicas de Autenticação

Segundo Slamanig *et al.* (2014), nos processos envolvendo o cartão do cidadão a confiança dos mecanismos de identificação e autenticação são promovidos pelo módulo MOA-ID. A seguir são apresentadas as etapas seguidas pelo MOA-ID, exemplificadas pela figura 2.

1. O cidadão realiza acesso ao SP utilizando seu cartão do cidadão. A aplicação *on-line* inicia o processo de autenticação e aciona o módulo MOA-ID.

2. O MOA-ID lê o *identity link* do cartão do cidadão através do cliente *middleware* (MOCCA) e verifica o sourcePIN. Este é o passo de identificação.

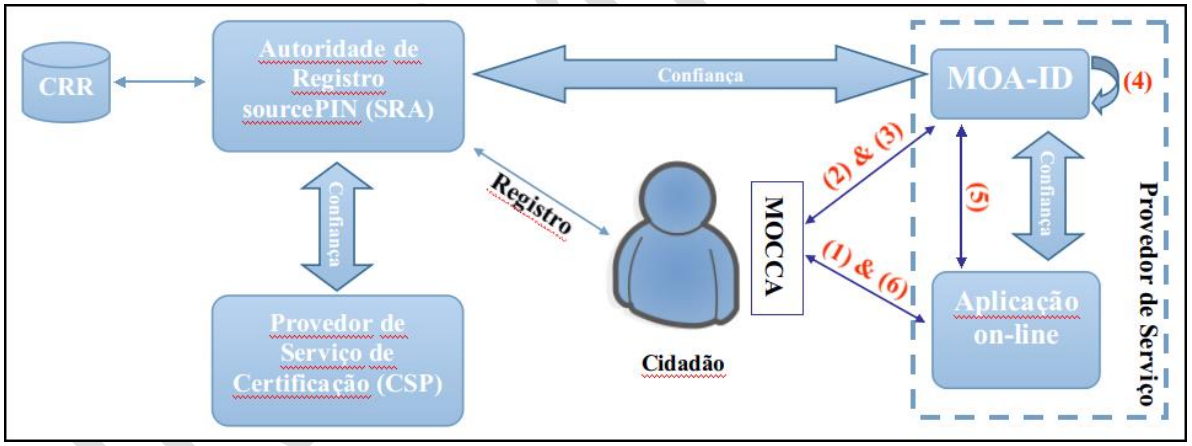
3. O MOA-ID requisita ao cidadão sua assinatura qualificada[51] para prosseguir com o processo de autenticação. Esta assinatura é verificada pelo módulo MOA-ID através de mecanismos de revogação (CRLs, OCSP) oferecidos por um provedor de serviço de certificação (CSP).

4. Para cada domínio em que o provedor de serviço está associado, o MOA-ID utiliza o sourcePIN para calcular um ssPIN exclusivo.

5. Seguindo o padrão SAML, o MOA-ID monta uma estrutura especial (asserção) incluindo o ssPIN e adiciona as informações pessoais do cidadão como nome, sobrenome e data nascimento. Em seguida, esta asserção é transmitida para a aplicação *on-line*.

6. Com base nos dados recebidos, o provedor de serviço libera o uso da aplicação protegida para o cidadão.

Figura 2: MOA-ID - Processo de Identificação e Autenticação



3.5 Privacidade relacionada a Identidade Eletrônica

3.5.1 Uso de Pseudônimos

Para preservar a privacidade do cidadão, é previsto em lei o uso direto do sourcePIN como identificador único para acesso às aplicações *on-line*. A lei de privacidade também determina que as atividades do usuário não devem ser rastreadas

[51] Assinatura Eletrônica Qualificada é um termo legal para assinaturas digitais que satisfazem requisitos específicos de acordo com as diretrizes de assinatura da União Europeia.

entre provedores de serviço de diferentes setores, também chamados de domínios administrativos. Dessa forma, o modelo de eID austríaco implementa um sistema de identificação usando pseudônimos para domínios específicos, também conhecido por ssPIN (*Sector Specific PIN*). As leis de governo eletrônico ainda determinam que o ssPIN só deve trafegar nas transações em forma criptografada (Slamanig *et al*., 2014).

Resumidamente, o ssPIN é único para cada domínio administrativo e nenhum SP consegue recalcular o ssPIN de outro setor, o que impossibilita o rastreamento das atividades dos usuários.

3.5.2 Poder de escolha do Cidadão (eID e provedores de identidades)

O cidadão austríaco pode escolher entre dois modelos implantados do cartão do cidadão: o primeiro utilizando um *eCard* contendo um *chip* eletrônico e o segundo utilizando a função de cartão do cidadão no telefone celular (European Comission, 2014a). Por outro lado, como o modelo de gestão de identidade adotado pelo governo austríaco segue o modelo centralizado, existe apenas um provedor de identidades. Sendo assim, os cidadãos não têm o direito de escolha, devendo apenas aceitar ou não o modelo implantado pelo governo.

3.5.3 Controle de Liberação de Dados Pessoais

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 (E-Government Innovation Center Graz, Austria, 2011). Neste modelo a figura principal é o “cartão do cidadão”, o qual mantém armazenados uma série de atributos conforme descrito na Seção 3.3.

Ao acessar um provedor de serviços, de acordo com Slamanig *et al*. (2014), uma asserção SAML é montada a partir do módulo MOA-ID. Além do ssPIN, esta asserção contém informações pessoais como nome, sobrenome e data de nascimento, cabendo ao usuário a decisão de liberar ou não estas informações ao SP. Após apresentar ao usuário os atributos que está requerendo, o SP aguarda a autorização do mesmo, que é feita com a digitação do número PIN.

3.5.4 Leis Específicas de Privacidade

Em 2000 foi publicada a “Lei de Proteção dos Dados”, em conformidade com a diretriz de proteção de dados da comunidade europeia 95/46/EC. Esta lei inclui os direitos fundamentais de privacidade, no que se refere ao processamento de dados pessoais, direito à correção e remoção de informações pessoais pelo próprio cidadão.

Em 2013 foi lançada a “Estratégia de Cibersegurança Austríaca”, a qual visa proteger as informações e os direitos humanos no mundo virtual. Melhorando a resiliência e segurança da infraestrutura dos serviços disponibilizados, garante a confidencialidade para a sociedade Austríaca nas transações *on-line*.

3.5.5 Aplicação da Lei de Privacidade

A aplicação das leis de privacidade é garantida através dos seguintes mecanismos.

1. Não identificação do usuário: criptografia do número de residente, resultando no sourcePIN.
2. Não rastreabilidade: uso de técnicas criptográficas do sourcePIN, resultando no ssPIN.
3. Controle de liberação dos dados pessoais aos SPs: conforme descrito na Seção 5.3.

4 DINAMARCA

4.1 Perfil Sociopolítico, Econômico e Governo Eletrônico

4.1.1 Estrutura Sociopolítica

A Dinamarca, cuja capital é Copenhague[52], é um país composto por uma grande península (*Jylland*) e cerca de 443 ilhas (76 habitadas) muitas vezes referenciadas como arquipélagos, sendo localizada a sudeste da Suécia e delimitada ao sul pela Alemanha. Possui uma área de 43.094 km² e aproximadamente 5,6 milhões de habitantes, tem uma densidade demográfica na ordem de 130 hab/km², sendo que cerca de 10% da população tem nacionalidade estrangeira, em sua maioria de origem escandinava. A língua oficial é o dinamarquês, possuindo fortes laços históricos e culturais com a Suécia e Noruega.

O país é uma monarquia constitucional com um sistema parlamentar de governo, sendo membro da União Europeia desde 1973. Embora não tenha aderido ao Euro é um dos membros fundadores da Organização do Tratado do Atlântico Norte (OTAN[53]) e da Organização para a Cooperação e Desenvolvimento Econômico (OECD[54]). Divide-se em cinco regiões nas quais se distribuem em 98 municípios. A Groelândia e as ilhas de Faroé integram o Reino da Dinamarca, mas gozam de autonomia, possuindo dois membros cada uma no parlamento dinamarquês.

Com um IDH na ordem de 0,900, possui o mais alto nível de igualdade de riquezas do mundo, sendo considerado em 2011 o país com menor índice de desigualdade social do mundo e classificada em 2013 pelo Índice de Percepção de Corrupção[55] o país menos corrupto do mundo ao lado da Nova Zelândia. O último relatório publicado pelo Índice Global de Paz[56] classificou a Dinamarca como o segundo país mais pacífico do mundo, depois da Islândia.

4.1.2 Acesso à Internet

De acordo com *European Comission* (2014b), em relação aos índices de

[52] 1.636.749 habitantes. 2.561 km²
[53] http://www.nato.int/
[54] http://www.oecd.org/
[55] http://www.transparency.org/cpi2013/infographic
[56] http://www.visionofhumanity.org/#/page/indexes/global-peace-index

acesso à Internet em 2013, as seguintes estatísticas são apresentadas.

- Casas com acesso à Internet: 93%.
- Empresas com acesso à Internet: 99%.
- Casas com acesso por banda larga: 87%.
- Empresas com acesso por banda larga: 97%.
- Indivíduos que fizeram compras pela Internet (últimos 3 meses): 65%.
- Empresas que receberam pedidos de compras *on-line*: 27%.

Em relação ao número de usuários de Internet, a Dinamarca ocupa a 62ª posição mundial, possuindo uma alta taxa de penetração de 96,08% (percentagem da polução com acesso à Internet)[57], o que indica um alto nível de inclusão digital. Em relação ao índice de infraestrutura em telecomunicações (ITT) (United Nations, 2014), a pontuação da Dinamarca (0,8740) é superior a média europeia (0,6678). Este índice foi obtido a partir dos seguintes componentes (United Nations, 2014).

- Telefone fixo (cada 100 habitantes): 43,43.
- Telefone celular (cada 100 habitantes): 117,85.
- Conexão à Internet Banda Larga (cada 100 habitantes): 38,18.
- Conexão à Internet *Wireless* (cada 100 habitantes): 88,00.

4.1.3 *Ranking* de e-Gov da ONU

De acordo com United Nations (2014), classificada com o índice de 0,8162, a Dinamarca passou a ocupar a 16ª posição no *ranking* de governo eletrônico (EGDI), caindo 12 posições em relação ao *ranking* de 2012. O índice de desenvolvimento em e-Gov apresentou as seguintes informações.

- Serviços *On-line*: 0,6614 (média na Europa é de 0,5695).
- Infraestrutura em Telecomunicações: 0,8740 (média na Europa é de 0,6678).
- Capital Humano: 0,9132 (média na Europa é de 0,8434).

4.1.4 Principais Políticas (Leis, atos, decretos, etc)

- **1985:** Lei de Acesso aos Documentos Públicos, permitindo que qualquer cidadão solicite o arquivo de um documento público.

[57] Fonte: http://www.internetlivestats.com/internet-users-by-country/

• **2000:** Ato de Processamento de Dados Pessoais, prevendo a proteção dos dados pessoais e determinando quais dados podem ser disponibilizados publicamente e quais devem permanecer confidenciais.

• **2000:** Ato da Assinatura Eletrônica, no qual o governo estabeleceu um esquema de assinatura digital oficial, segundo a qual todo cidadão recebe um certificado digital pessoal, certificado este emitido pelo *framework* baseado em *software* livre, o OCES ((*Public Certificates for Electronic Services*)), fornecendo segurança suficiente para toda transação com o setor público e privado.

• **2011:** Ato sobre Comunicações Eletrônicas, na qual os provedores de serviço são obrigados a avisar o governo ou órgão competente os casos de violação de dados pessoais.

4.1.5 Cronologia do Desenvolvimento de e-Gov e GId

• **1968:** implantação do sistema de registro civil, como característica os cidadãos passaram a receber um identificador único.

• **1970:** criação de políticas de compartilhamento de recursos de T.I. e implantação do sistema de coleta de impostos para empresas.

• **1970-2000:** criação de políticas para introdução da T.I. no governo.

• **2000:** implantação do Comitê de Administração Digital, visando o uso de XML e assinaturas digitais.

• **2001:** esforços para oferecer serviços governamentais de forma *on-line*. Uso do XML como padrão para o governo.

• **2002:** uso de *Software Open Source* no Governo.

• **2003:** empresa fornece tecnologia de Assinatura Digital para o governo. Primeira versão (rascunho) do *framework* de interoperabilidade do governo eletrônico.

• **2004:** adoção da UBL (Universal Business Language) para *eProcurement*. Neste mesmo ano foi publicada a “Estratégia Nacional de e-Gov 2004 - 2006”.

• **2005:** adoção do SAML 2.0. Pagamentos feitos pelo governo são todos eletrônicos. Nova versão do *eGovernment Interoperability Framework.*

• **2006:** resolução exige o uso de padrões abertos pelo governo. *Web services* nos sistemas de pensão pública e privada.

• **2007:** portal único para serviços públicos. Iniciada a infraestrutura nacional de SOA (Arquitetura Orientada a Serviço) para *eBusiness*, visando interoperabilidade entre governo e empresas.

• **2007:** publicada a Estratégia de e-Gov 2007-2010.

• **2008:** anunciada que a nova geração de Assinatura Digital que seria desenvolvida e implementada pela empresa DanID.

• **2009:** NemHandel[58] é usado por empresas para comunicar com o governo. Esta tecnologia implementa de forma simples (*framework*), o envio de documentos eletrônicos por meio de um canal seguro, a partir do próprio computador do usuário.

• **2010:** troca do tradicional sistema de "usuário/senha" pelo NemID[59], sendo disponibilizado neste mesmo ano para uso com Governo ou Empresas. O NemID, além de constituir-se de credencial única (eID) para acesso à multiplos SPs, agrega a funcionalidade de uso com um cartão de *token*, contendo códigos (*one-time passwords*) para acesso aos sistemas.

• **2011:** estatística publicada apresenta que o NemID é usado por 79% da população. Caixa de correio digital para comunicação com o governo. Por determinação o uso do NemHandel se torna mandatório para comunicação com Governo.

• **2012:** unificação de bases de dados públicas e disponibilização para uso gratuito.

• **2013:** cidadãos (2014) e empresas (2013) DEVEM ter uma caixa de correio digital para comunicar-se com o governo.

• **2014:** início da especificação de um eID público e do novo NemID.

• **2015:** fim do uso de papel.

4.2 Modelo de Organização de Documentos Civis

4.2.1 Registro Civil

O responsável pela emissão das certidões de nascimento é a entidade municipal, a qual faz o cadastro do cidadão no Centro de Registro Pessoal[60] (*CPR register*) dinamarquês, atribuindo a cada pessoa um número CPR (*CPR number*). A

[58] http://www.digst.dk/Servicemenu/English/Digitisation/NemHandel
[59] https://www.nemid.nu/dk-en/
[60] https://cpr.dk

maioria destes municípios também oferece informações e disponibiliza formulários de solicitação da 2ª via em seus *websites* (European Comission, 2014b).

O Centro de Registro Pessoal mantém em base de dados centralizada as seguintes informações de todos os cidadãos: nome, endereço e número de identificação único (número CPR) (European Communities, 2009c).

4.2.2 Identidade Civil

Na Dinamarca, não existe uma única forma de identificar civilmente um cidadão. Pode-se utilizar um conjunto de documentos para identificar o cidadão, entre eles o cartão de segurança social, a carteira de motorista, o passaporte, cartões de banco e em alguns casos é aceito o cartão de saúde do cidadão (European Communities, 2009c).

Opcionalmente, cidadãos maiores de 16 anos podem solicitar o ”Cartão de Identificação” na Dinamarca. Para tanto, é necessário comparecer pessoalmente a administração municipal local, levando consigo uma foto 3x5, o cartão de seguro social, a certidão de nascimento e fazer o recolhimento da taxa correspondente ao serviço de verificação da identidade. No prazo de uma semana o cidadão recebe o Cartão de Identificação com foto em sua residência (Allerød Kommune - Denmark, 2014).

4.2.3 Relação do Documento de Viagem com a Identidade Civil

Não existe uma relação direta entre o passaporte e os demais documentos de identificação civil (licença de motorista, CPR). No entanto, para a emissão de qualquer um dos documentos é necessário provar a identidade como cidadão dinamarquês, o que é feito através do número de registro de cidadão (CPR), devendo o cidadão comparecer pessoalmente na prefeitura de qualquer município. Por outro lado, o passaporte eletrônico é gerado pelo Departamento de Polícia Nacional da Dinamarca, para tanto devem ser informado os dados de identidade do portador (European Comission, 2014b).

4.3 Identidade Eletrônica

4.3.1 Uso da Identidade Eletrônica

Por opção do cidadão, o provedor de identidades permite a utilização de várias

identificações eletrônicas, conhecidas por NemID (eID). O usuário pode optar por utilizar uma identificação para cada serviço que utiliza, por exemplo, uma para transações bancárias, uma para interações com o setor público, uma terceira identidade para interações com o setor privado e assim por diante. Se em dado momento o cidadão portador de múltiplas identidades quiser, ele tem a opção de fazer a fusão dos identificadores, passando a utilizar o mesmo usuário, senha e *token* (cartão de códigos - *one-time passwords*) para todas as interações que passar a fazer após a unificação dos NemIDs (Nets DanID A/S - Finansministeriet, 2014d).

Apesar da adoção do eID ser voluntária, para realizar qualquer transação digital envolvendo o governo ou o setor privado é preciso ter pelo menos um NemID (European Comission, 2014b). De acordo com Nets DanID A/S - Finansministeriet, (2014c), todo cidadão que possuir idade mínima de 15 anos, possuir um número de identificação dinamarquês (CPR) e atender aos requisitos de identificação pode obter um NemID. Mesmo pessoas que não são cidadãos natos, mas que possuem visto de residência ou de estudante, podem obtê-lo. Cidadãos menores de 15 anos podem retirar um NemID somente para uso em transações bancárias, para tanto deverá entrar em contato com o banco para verificar as regras e condições.

4.3.2 Cadastro da Identidade Eletrônica

Em 2008, o governo fez um acordo com um provedor privado, a DanID[61], que pertence à empresa Nets[62], para desenvolver e implementar a próxima geração de assinatura digital na Dinamarca. Desta contratação, nasceu o NemID em maio de 2010 como uma solução de assinatura digital e *login* único para interações do cidadão com serviços bancários, com o setor público e com o setor privado (European Comission, 2014b).

O NemID se constitui de um *login* e senha escolhidos pelo usuário e um cartão de códigos (*token*), que garantem um nível alto de segurança, minimizando os impactos causados por roubo de identidade. De alguma forma, o cidadão é sempre ligado ao seu Número de Registro Nacional (CPR) e ao número de segurança social ao criar sua identidade eletrônica (Nets DanID A/S - Finansministeriet, 2014d).

[61] http://www.danid.dk/
[62] http://www.nets.eu/

4.3.3 Atributos da Identidade Eletrônica

Para realizar o cadastro do NemID o cidadão deve acessar o portal[63] da Agência contratada pelo governo (Nets DanID A/S) e preencher o formulário. Com o número do seguro social, número de telefone móvel e um *e-mail* válido já é possível realizar o cadastro, ou simplesmente informando o número do passaporte ou da carteira de motorista. Ao realizar o cadastro, o cidadão tem a opção de solicitar um cartão de códigos (*tokens*), sendo este requisitado pelos SPs que oferecem um nível maior de segurança nas transações eletrônicas realizadas (Nets DanID A/S - Finansministeriet, 2014d).

Ao realizar o cadastro o cidadão deve concordar com os seguintes termos.

• O portal DanID pode fazer consultas ao CPR para obter o nome e endereço do cidadão.

• O portal DanID pode fornecer aos SPs públicos o número PID (descrito na seção 3.4), o qual faz a ligação entre o certificado digital e o número CPR. Por outro lado, o fornecimento do PID aos SPs privados só ocorre mediante autorização do usuário.

• O DanID pode utilizar os dados pessoais do cidadão (nome, endereço, números de segurança social, endereço de *e-mail* e número de telefone celular) para emissão e gerenciamento de seu certificado digital. Conforme descrito na seção 3.4, esta emissão é feita a partir do *framework* governamental OCES (*Public Certificates for Electronic Services*).

4.3.4 Uso de Certificado Digital na Identidade Eletrônica

Lançado em fevereiro de 2003, a primeira geração de certificados digitais foi desenvolvida pela companhia de telecomunicações TDC, após um processo de licitação que resultou em três vencedores, sendo a TDC escolhida após as negociações. A segunda geração iniciou em 2010, com o lançamento do NemID desenvolvido pela empresa Nets DanID (Nets DanID A/S - Finansministeriet, 2014a).

Para cada NemID criado é emitido um certificado digital, o qual deve ser gerado pelo *framework* OCES[64] (*Public Certificates for Electronic Services*) do Ministério da Ciência, Tecnologia e Inovação. O certificado digital gerado pelo OCES possui um

[63] https://service.nemid.nu/dk-da/bestil_nemid/bestil_med_koerekort_eller_pas
[64] Em dinamarques “Offentlige Certifikater til Elektroniske Services”

número de série que inclui um PID (*person specific identification number*), o qual é responsável por ligar o cidadão ao seu número CPR (European Communities, 2009c).

O uso de certificado digital é intrínseco à solução NemID, sendo fornecido gratuitamente pelo governo através do Nets DanID. Sendo válido até 4 anos, o certificado digital permite ao cidadão a possibilidade de assinar digitalmente formulários eletrônicos, enviar e receber *e-mails* de forma segura e acessar diferentes serviços do governo e empresas privadas incluindo as instituições bancárias (Nets DanID A/S - Finansministeriet, 2014a).

4.3.5 Obrigatoriedade da Identidade Eletrônica

Segundo Nets DanID A/S - Finansministeriet (2014b), toda solução de auto atendimento requer que o cidadão utilize pelo menos um NemID para acessar os recursos digitais. O governo se compromete a dar uma atenção especial a quem não tiver um NemID ou não puder registrá-lo, ao mesmo tempo que isenta o uso do auto atendimento e uso de recursos digitais para quem não puder provar sua identidade em meios eletrônicos, por exemplo, por motivo de deficiência mental ou física, ou por possuir barreiras linguísticas.

4.4 Sistemas de Gestão de Identidades

4.4.1 Padrão Adotado de Identidade Eletrônica (eID)

O cadastrado da eID (NemID) é feito de forma centralizada pela DanID, havendo portanto um padrão único para a confecção da identidade eletrônica na Dinamarca. Para a criação do eID é obrigatória a emissão de um certificado digital pessoal, certificado este que obrigatoriamente deve ser emitido pelo *framework* OCES disponibilizado pelo Ministério da Ciência, Tecnologia e Inovação da Dinamarca (Nets Holding A/S, 2014).

4.4.2 Modelo de Gestão de Identidades

Adotando o modelo centralizado, a gestão da identidade eletrônica é feita pela empresa privada contratada pelo governo (DanID), a qual permite a participação de todos os segmentos de serviços da sociedade, como bancos, empresas privadas e governamentais (European Comission, 2014b).

Utilizando o NemID e sua assinatura digital pessoal, o cidadão pode fazer uso da autenticação única SSO (*Single Sign-On*) (European Communities, 2009c) em mais de 600 serviços disponíveis atualmente na Dinamarca (European Comission, 2014b).

4.4.3 Tecnologias de Gestão de Identidades

De acordo com Nets DanID A/S - Finansministeriet (2014d), as seguintes tecnologias são utilizadas para prover a gestão de identidades.

- SAML 2.0.
- NemID: composto por um *UserID*, senha e um *token* (cartão de códigos - *one-time passwords*).
- Certificados digitais emitidos pelo *framework* governamental (OCES).

4.4.4 Provedores de Identidades Privados

O governo contratou uma empresa privada para atuar como provedor de identidade, oferecendo uma solução de eID (NemID) para uso tanto por provedores de serviço públicos quanto privados. No entanto, existe uma restrição no envio do atributo CPR (número de registro do cidadão) para as empresas privadas, não sendo permitido o envio sem a expressa permissão do usuário (European Comission, 2014b).

4.4.5 Padrões de Interoperabilidade

Especificações consolidadas, como o SAML e o XML, são utilizadas para prover a interoperabilidade entre os SPs e o IdP (European Comission, 2014b). Segundo European Communities (2009c), tecnicamente é possível a um SP de outro país permitir o *login* de um cidadão dinamarquês, desde que o SP suporte o SAML versão 2. Entretanto, esta é uma questão que ainda precisa ser analisada e mapeada, para que de fato a interoperabilidade entre países ocorra.

4.4.6 Mecanismos ou Técnicas de Autenticação

No cadastramento da identidade eletrônica, é solicitado ao usuário somente escolher um *UserID* e uma senha. O cidadão pode optar em fazer uso de um *token* para complementar a segurança no acesso aos SPs. Este *token* constitui-se de um cartão com 148 códigos pré-impressos, ou módulo de *hardware*, que por razões de

segurança não permite que cada código seja utilizado mais de uma vez. O NemID é baseado em uma infraestrutura de chave pública (PKI), significando que para cada NemID criado é emitido um par de certificados digitais, um público e outro privado (Nets DanID A/S - Finansministeriet, 2014d).

4.5 Privacidade relacionada a Identidade Eletrônica

4.5.1 Uso de Pseudônimos

Embora o usuário possa fazer a escolha de um pseudônimo como *login*, o número PID (descrito na seção 3.4) é utilizado pelos SPs públicos para identificar o usuário, fazendo a ligação entre a assinatura digital pessoal e o número CPR. Entretanto, para os provedores de serviço privados a consulta do número PID só ocorre com a permissão do usuário (Nets DanID A/S - Finansministeriet, 2014d).

4.5.2 Poder de escolha do Cidadão (eID e provedores de identidades)

O provedor de identidades é único e privado, contratado pelo governo após processo de licitação e negociação ocorrido em 2008. O cidadão pode voluntariamente adotar o NemID para as interações com os serviços eletrônicos, no entanto se não fizer a adesão, corre o risco de não poder utilizar os serviços eletrônicos disponíveis (Nets DanID A/S - Finansministeriet, 2014d).

4.5.3 Controle de Liberação de Dados Pessoais

Ao optar por criar uma identificação eletrônica (NemID), o cidadão dinamarquês concorda em compartilhar o registro de cidadão (CPR) e o número de segurança social com os provedores de serviços públicos, além de permitir que outras informações como nome, endereço, *e-mail* e número de telefone móvel sejam encaminhadas nestas interações *on-line*. No entanto, suas informações são apenas encaminhadas a um SP privado, caso haja o consentimento do usuário para liberação de seus dados (Nets DanID A/S - Finansministeriet, 2014d).

4.5.4 Leis Específicas de Privacidade

Com a publicação do “Ato de Processamento de Dados Pessoais” em 2000, toda informação pessoal passou a ser tratada de forma diferenciada, de forma que

alguns dados podem ser disponibilizados publicamente e outros devem permanecer confidenciais (European Comission, 2014b).

Neste mesmo ano de 2000, é publicado o “Ato sobre a Assinatura Eletrônica”, no qual o governo estabeleceu um esquema de assinatura digital oficial, segundo a qual todo cidadão recebe um certificado digital pessoal, certificado este emitido pelo *framework* baseado em *software* livre, o OCES ((*Public Certificates for Electronic Services*)), fornecendo segurança suficiente para toda transação com o setor público e privado.

Em 2011, é publicado o “Ato sobre Comunicações Eletrônicas”, no qual os provedores de serviço são obrigados a avisar o governo ou órgão competente os casos de violação de dados pessoais.

4.5.5 Aplicação da Lei de Privacidade

Aplicado pela Agência de Proteção de Dados, todo cidadão passou a contar com o direito de acesso aos registros sobre si próprio (European Comission, 2014b). Por exemplo, se um cidadão quer saber quais informações estão registradas sobre ele no Centro de Registro Pessoal, basta acessar o portal do CPR[65] com seu NemID e solicitar este registro.

[65] https://gws.cpr.dk/cpr-online-gws/selvbetjening.jsp

5 ESPANHA

5.1 Perfil Sociopolítico, Econômico e Governo Eletrônico

5.1.1 Estrutura Sociopolítica

A Espanha é um país situado na Europa Meridional, fazendo fronteira com o Mar Mediterrâneo, França, Oceano Atlântico e Portugal. Conta com uma área de pouco mais de 500 mil km² e população aproximada de 47 milhões. Organiza-se politicamente como uma democracia, formada de um governo parlamentar e uma monarquia constitucional, possuindo portanto, a figura do monarca hereditário na figura de Chefe de Estado (Rei da Espanha). É país membro das Organizações das Nações Unidas (ONU), da União Europeia, da Organização do Atlântico Norte (OTAN), da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e da Organização Mundial do Comércio (OMC).

De acordo com os termos da Constituição de 1978, a Espanha adotou um sistema totalmente descentralizado com 17 Regiões Autônomas (*Comunidades Autónomas*) e duas Cidades Autônomas (Ceuta e Melilla). A constituição estabelece a organização territorial do Estado em municípios, províncias e comunidades autônomas, estas com competência para fazer a gestão de seus próprios interesses, com amplo nível de autonomia contando com poderes legislativos, administrativos e executivos próprios.

5.1.2 Acesso à Internet

De acordo com *European Comission* (2014g), em relação aos índices de acesso à Internet em 2013, as seguintes estatísticas da Espanha são apresentadas.

- Casas com acesso à Internet: 70%.
- Empresas com acesso à Internet: 97%.
- Casas com acesso por banda larga: 69%.
- Empresas com acesso por banda larga: 95%.
- Indivíduos que fizeram compras pela Internet (últimos 3 meses): 23%.

Em relação ao número de usuários de Internet, a Espanha ocupa a décima nona posição mundial e possui uma taxa de penetração de 74,38% (percentagem da polução

com Internet)[66], contando em 2014 com mais de 35 milhões de usuários com acesso à Internet. Em relação ao índice de infraestrutura em telecomunicações (ITT) (United Nations, 2014), a pontuação da Espanha (0,6629) é praticamente igual a média europeia (0,6678). Este índice foi obtido a partir dos seguintes componentes (United Nations, 2014).

- Telefone fixo (cada 100 habitantes): 41,11.
- Telefone celular (cada 100 habitantes): 108,36.
- Conexão à Internet Banda Larga (cada 100 habitantes): 24,26.
- Conexão à Internet *Wireless* (cada 100 habitantes): 53,42.

5.1.3 *Ranking* de eGov da ONU

De acordo com United Nations (2014), classificada com o índice de desenvolvimento de e-Gov de 0,8410, a Espanha passou a ocupar a 12ª posição no *ranking* de governo eletrônico em 2014, subindo onze posições em comparação ao *ranking* de 2012. Em relação ao índice de eParticipação da ONU, a Espanha está entre os 50 melhores países (19ª posição). O índice de desenvolvimento em e-Gov apresentou as seguintes informações.

- Serviços *On-line*: 0,9449 (média na Europa é de 0,5695).
- Infraestrutura em Telecomunicações: 0,6629 (média na Europa é de 0,6678).
- Capital Humano: 0,9152 (média na Europa é de 0,8434).

5.1.4 Principais Políticas (Leis, atos, decretos, etc)

Lei Orgânica 1/1992[67] de 21 de fevereiro sobre a Proteção de Segurança Pública. Alterada pelo Acórdão 341/1993 de 18 de novembro de 1993, pela Lei Orgânica 4/1997 de 04 de agosto, pela Lei 10/1999 de 21 de abril, pela Lei Orgânica 7/2006 de 21 de novembro e da pela Lei Orgânica 3/2013 de 20 de junho.

Diretiva 1995/46/EC, **Diretiva 97/66/CE**, **Diretiva 2002/58/CE**: utilizadas como parâmetro para a Lei de Proteção de Dados Pessoais.

[66] Fonte: http://www.internetlivestats.com/internet-users-by-country/
[67] http://www.interior.gob.es/web/servicios-al-ciudadano/normativa/leyes-organicas/ley-organica-1-1992-de-21-de-febrero

Diretiva 1999/93/EC de 13 de dezembro 1999 do Parlamento Europeu e o Conselho: utilizada como parâmetros para funcionamento do *framework* para assinaturas eletrônicas.

Lei Orgânica 14/1999 de 17 de setembro, regulamentando a assinatura eletrônica qualificada (*eSignature*).

Lei Orgânica 15/1999 de 13 de dezembro[68]: Trata sobre a Proteção de Dados Pessoais e seu processamento.

Diretiva 2001/45/EC: utilizada como parâmetro para a Lei de Proteção de Dados Pessoais.

Lei 59/2003[69] de 19 de dezembro de 2003: o Parlamento aprova a nova lei para assinatura eletrônica, em conformidade com a Diretiva Europeia 1999/93/EC, estabelecendo um *framework* legal para o futuro desenvolvimento do *eID Card* nacional. Modificação feita pela Lei 56/2007 de 28 de dezembro e pela Lei 9/2014 de 9 de maio.

Decreto Real 1553/2005[70] de 23 de dezembro: regula a emissão do documento nacional de identidade e seus certificados de assinatura eletrônica. Alterada pelo Decreto Real 1586/2009 de 16 de outubro e o pelo Decreto Real 869/2013 de 08 de novembro.

Ordem INT/738/2006[71] de 13 de março, pelas quais a declaração de práticas e políticas do Ministério do Interior de certificação é aprovado.

[68] http://www.dnielectronico.es/marco_legal/ley_organica_15_1999.html
[69] http://www.interior.gob.es/web/servicios-al-ciudadano/normativa/leyes-ordinarias/ley-59-2003-de-19-de-diciembre
[70] http://www.interior.gob.es/web/servicios-al-ciudadano/normativa/reales-decretos/real-decreto-1553-2005-de-23-de-diciembre
[71] http://www.interior.gob.es/web/servicios-al-ciudadano/normativa/ordenes-int/orden-int-738-2006-de-13-de-marzo

Lei 11/2007 de 13 de junho: trata do Acesso Eletrônico dos Cidadãos aos Serviços Públicos – LAECSP (*Ley Para el Acceso Electrónico de los Ciudadanos a los Servicios Públicos*).

Decreto Real 4/2010 de 8 de janeiro: regula o uso *Framework* Nacional de Interoperabilidade, em conformidade com a Lei 11/2007.

Lei 19/2013: Determina acesso público, por meios eletrônicos, ao serviços disponibilizados no domínio da justiça.

Lei 19/2013 de 9 de dezembro: Lei para transparência e acesso à informação pública, determinando que toda informação da Administração Central deverá ser disponibilizada publicamento no portal da transparência.

5.1.5 Cronologia do Desenvolvimento de eGov e GId

Set/2001: lançado o portal ”Administration.es”, provendo um portal *on-line* para serviços e informações públicas.

Set/2001: criada a Autoridade de Certificação Pública, conhecida por CERES, a qual foi criada com a finalidade de promover o funcionamento da Infraestrutura de Chave Pública (ICP) na Espanha.

Nov/2002: iniciado o projeto do Documento de Identidade Eletrônica Nacional.

Mai/2003: governo aprova critérios de segurança e padronização para aplicações de T.I. utilizadas na Administração do Estado.

Jul/2003: criada uma nova estrutura inter-ministerial, encarregada de coordenar a implementação de governo eletrônico.

Fev/2004: o Conselho de Ministros aprova a criação e distribuição do novo *eID Card* contendo identificadores biométricos com a intenção de melhorar a segurança nos processos de identificação e autorização.

Jul/2005: o Conselho Superior para e-Gov fornece diretrizes para a adoção de Código Aberto (*Open Source*) nas Agências Públicas.

Mar/2006: o novo Cartão de Identidade Eletrônico (DNIe) é oficialmente

lançado, juntamente com o novo portal “Dnielectronico.ES”.

Mar/2009: Conselho de Ministros aprova um investimento de 14 Milhões, em uma série de ações definidas para incentivar o uso do Cartão de Identidade Eletrônica Nacional e estimular a difusão de serviços digitais confiáveis.

Set/2009: assinado termo de colaboração entre os governos da Espanha e Portugal para validação dos certificados digitais nos dois países.

Out/2009: a Secretaria de Estado de Telecomunicações e Sociedade da Informação (SETSI) anuncia plano de ação para promover o uso do DNIe entre cidadãos e empresas.

Nov/2010: o Instituto Nacional Espanhol de Tecnologia da Comunicação (INTECO) juntamente com uma empresa de consultoria publicam um guia de referência para uso seguro do DNIe na Internet.

Jan/2013: o Alto Conselho de e-Gov anuncia a *Spanish Public Administrations Network* (Red SARA), que se constitui de um projeto estratégico para um serviço de nuvem privado para a administração pública. A “Red SARA” provê a interconexão entre todas as esferas do governo (nacional, regional e local).

Dez/2013: adotada a Estratégia Nacional de Segurança Cibernética, alinhada com a Estratégia de Segurança Nacional de 2013, que inclui a segurança cibernética em suas doze áreas de atuação. A estratégia adotada constitui-se de um documento que trata da proteção do ciberespaço a fim de implementar ações para prevenção, defesa, detecção, resposta e recuperação contra ameaças cibernéticas. Este documento define seis objetivos principais, oito linhas de ação e cria o Conselho Nacional de Segurança Cibernética.

Set/2014: o Conselho de Ministros aprova acordo para a criação do “Cl@ve”, que se constitui de uma nova plataforma para identificação, autorização da assinatura eletrônica a ser utilizada pela Administração Pública.

Jan/2015: O Ministro do Interior apresenta o novo Documento Nacional de Identidade Eletrônico (DNIe), versão 3.0. Entre as inovações de segurança, encontra-se a adoção da assinatura eletrônica do DNIe com a mesma validade legal da assinatura manuscrita. Incorporação da tecnologia sem contatos (NFC), que permite a leitura do cartão bastando apenas aproximá-lo do terminal de leitura.

5.2 Modelo de Organização de Documentos Civis

5.2.1 Registro Civil

Para o sistema legal espanhol o nascimento é um fato muito importante, pois determina o início da personalidade. Sendo assim, todos os nascimentos devem ser registrados no “Escritório de Registro Civil”, dentro do prazo máximo de 30 dias após o nascimento da criança (Ministde Justicia, 2015b).

O Escritório de Registro Civil é uma entidade vinculada ao Ministério da Justiça, o qual é responsável por registrar os fatos relacionados ao estado civil das pessoas. Os fatos a seguir são passíveis de registro: nascimento, casamento, morte e outras modificações judiciais como incapacidade, falência, deveres parentais, guarda e declaração de insolvente (European Communities, 2009e). Especificamente, para realizar o registro de nascimento, é necessário apresentar a Declaração de Nascimento emitida pelo hospital e o documento de identidade dos pais (de Madrid, 2012). O Escritório de Registro Civil por sua vez, armazena as seguintes informações (de Justicia, 2015b).

- Nome e Sobrenome.
- Data, local e hora de nascimento.
- Sexo do bebê.
- Descendência (Nome dos pais).
- Data do registro.
- Número de inscrição único do recém-nascido.

Uma vez feito o registro de nascimento no Escritório de Registro Civil, pode-se solicitar a emissão da Certidão de Nascimento em papel, a qual pode ser fornecida em um dos seguintes formatos, segundo a nomenclatura do pais (de Justicia, 2015a)

1. **Certidão Positiva.**
   - Extrato: resumo das informações relativas ao registro de nascimento.
   - Literal: cópia integral dos dados relativos à identidade e ao fato de nascimento.
2. **Certidão Negativa:** comprovante da existência de cadastro em um

Registro Civil.

3. **Certidão com selo eletrônico:** serve para comprovar a existência dos dados do cidadão na base central de registros, prática esta realizada desde janeiro de 1950.

5.2.2 Identidade Civil

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 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 (Ministerio de la Policía, 2015a).

Em março de 2006 é lançado oficialmente o Documento de Identidade Civil Eletrônico (DNIe), passando a substituir o DNI tradicional (European Comission, 2014g). Com o formato de um cartão de crédito, sua emissão é feita de forma centralizada pela Direção Geral da Polícia[72], órgão vinculado ao Ministério do Interior (Ministerio de la 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 (European Communities, 2009e). 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. Dentre as informações gravadas no corpo do cartão, estão as seguintes (Ministerio de la Policía, 2015a).

- Nome e sobrenome.
- Data e local de nascimento.
- Nacionalidade.
- Sexo.
- Data de validade.
- Data de emissão (DDMMAA).

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

• Número do Documento Nacional de Identidade (nº DNI).
• Primeiro nome dos pais.
• Endereço e cidade de residência.

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 (Ministerio de la 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.

5.2.3 Relação do Documento de Viagem com a Identidade Civil

Para a emissão do documento de viagem é necessário comparecer pessoalmente a uma delegacia de polícia e apresentar o documento nacional de identidade (DNI) e uma foto recente. Em alguns casos, se necessário, será solicitado ao cidadão a apresentação da certidão de nascimento. Este documento de viagem terá a validade de 5 anos para cidadãos menores de 30 anos e 10 para maiores desta idade (Ministerio de la Policía, 2015b).

Entretanto, como o DNIe é construído utilizando as normas ICAO (Ministerio de la Policía, 2015a), este documento de identidade civil poderá ser utilizado como documento de viagem para os países que o aceitarem, o que normalmente ocorre nos países pertencentes à Comunidade Européia.

5.3 Identidade Eletrônica

5.3.1 Uso da Identidade Eletrônica

O documento de identidade eletrônico (*eID Card*) é conhecido na Espanha por DNIe. Por ser utilizado também como documento de identidade civil, sua emissão é obrigatória para todo cidadão espanhol maior de 14 anos, entretanto a ativação da funcionalidade eletrônica é voluntária (veja Seção 3.6) (European Communities,

2009e). 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 os mesmos documentos requeridos na primeira solicitação, além de apresentar o DNIe que está por vencer (Ministerio de la Policía, 2015a).

Em 19 de setembro de 2014, um conselho de ministros aprovou um acordo para a criação do "Cl@ve[73]", 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 (Ministerio de la 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 (para las 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.

5.3.2 Cadastro da Identidade Eletrônica

O Decreto Real 1553/2005[74] de 23 de Dezembro relacionado a emissão do cartão de identidade nacional e seus certificados digitais, confirma que a Diretoria Geral da Polícia[75] é o departamento que deve exercer todas a competências de gerenciamento, direção, organização, desenvolvimento ou administração de todos os assuntos relacionados à emissão ou performance dos cartões de identificação (DNI), incluindo os eletrônicos (DNIe) (European Communities, 2009e). Portanto, de forma centralizada, e de acordo com a legislação vigente, o DNIe poderá ser emitido somente pela Diretoria Geral da Polícia, em qualquer um dos 350 escritórios espalhados em todo o território nacional. Para os cidadãos que não fizeram a ativação da identificação eletrônica no DNIe, ainda existe a possibilidade de se registrarem utilizando a

[73] http://clave.gob.es/
[74] Decreto disponível em http://www.dnielectronico.es/marco_legal/RD_1553_2005.html
[75] Diretoria vinculada ao Ministério do Interior

plataforma Cl@ve. Entre as formas de registro, há a forma presencial através de um "Escritório de Registro[76]" ou pela Internet. Para tanto, o cidadão deverá informar os seguintes dados.

- NIF (*Número de Identificación Fiscal*).
- CVS (*Código Seguro de Verificación*) recebido pelos correios da Agência Tributária.
- Nº do DNIe e data de validade.
- Nº do telefone celular (Operadora Espanhola).
- Endereço de *e-mail*.
- Nº de Conta Corrente como Titular.

5.3.3 Atributos da Identidade Eletrônica

O documento de identidade civil (DNI) e o documento de identidade eletrônico (DNIe) são o mesmo documento, sendo emitidos de forma centralizada pelos escritórios da Polícia. Portanto, além das informações impressas à laser, conforme descrito na Seção 2.2, os seguintes dados do portador são gravados no *chip* (European Communities, 2009e).

- 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.
- Códigos "PIN" para cada certificado eletrônico.

5.3.4 Biometria

Ao fazer a solicitação do documento de identidade (DNIe), são coletadas a impressão digital dos dedos indicadores das duas mãos do cidadão. Se não for possível obter a impressão digital de um dedo indicador ou de ambos, por mutilação ou defeito físico do mesmo, a impressão faltante será substituída pela impressão de outro

[76] Busca por um Escritório de Registro: http://administracion.gob.es/pag_Home/atencionCiudadana/OficinasAtencion.html

dedo, segundo a ordem: dedo médio, anelar, mínimo ou polegar. Se não for possível coletar nenhum deles, deverá ser registado no lugar de apoio o motivo pela qual a impressão digital não foi coletada (Ministerio de la Policía, 2015a).

O DNIe permite a verificação biométrica da identidade de seu portador, embora esta função esteja somente disponível em pontos de acesso controlado. O sistema usa as digitais do usuário para identificá-lo, utilizando o algorítimo *Match on Card* o qual permite que a digital do portador seja comparada com a digital armazenada no próprio *chip* do DNIe (Ministerio de la Policía, 2015a).

5.3.5 Uso de Certificado Digital na Identidade Eletrônica

A emissão da identificação eletrônica está associada com a obtenção de certificados eletrônicos para autenticação e assinatura de documentos, os quais são armazenados no *chip* do DNIe (Ministerio de la Policía, 2015a)

• **Certificado de Autenticação:** tem o propósito de garantir eletronicamente a identidade do cidadão quando o mesmo efetuar uma transação *on-line*. Com este certificado o cidadão poderá provar sua identidade perante qualquer autoridade ou sistema, uma vez que só o portador conhece o código PIN que destrava seu certificado pessoal. Este certificado deve ser usado somente e exclusivamente para sistemas de autenticação (confirmação de identidade) e para acesso seguro a sistemas de informação (por meio de estabelecimento de canais privados e confidenciais com os servidores).

• **Assinatura Qualificada:** este certificado permite aos cidadãos assinarem eletronicamente procedimentos ou documentos, possibilitando a substituição da assinatura manuscrita pela eletrônica[77] nas relações do cidadão com terceiros. Para ter efeito legal e ser aceito eletronicamente, este certificado deverá estar em conformidade com o ETSI[78], a RFC3739[79], a Diretiva Europeia 99/93/CE e com a Lei de Assinatura Eletrônica[80].

[77] (LFE 59/2003 artº 3.4 e 15.2)
[78] http://www.etsi.org/technologies-clusters/technologies/security/certification-authorities-and-other-trust-service-providers
[79] http://www.ietf.org/rfc/rfc3739.txt
[80] Lei de Assinatura Eletrônica nº 59/2003, de 19 de dezembro

Para a operação do cartão de identidade eletrônico (DNIe), foi construída uma Infraestrutura de Chave Pública (ICP), composta por uma hierarquia de duas camadas (Ministerio de la Policía, 2015a)

1. Um primeiro nível onde a Entidade Certificadora Raiz (*AC Raiz*) está localizada, representando um ponto chave de confiança para todos os sistemas. Desta forma, todos os indivíduos, corporações, pessoas públicas ou privadas poderão reconhecer e atestar a identidade do DNIe. Esta AC emite apenas certificados para si mesma e para as AC Subordinadas.

2. Um segundo nível constituído pelas Entidades Certificadoras Subordinadas à Entidade Raiz. Estas CAs emitem os Certificados de Autenticação e Assinatura a serem inseridos no *chip* do DNIe (*eID Card*), podendo participar deste nível tanto empresas públicas quanto privadas.

A Entidade Certificadora de primeiro nível é mantida e controlada pelo FNMT (*Fábrica Nacional de Moneda e Timbre*) através de seu departamento, o CERES (***CER****tificación* ***ES****pañola*). Todo provedor de serviços que deseje oferecer certificados para o DNIe, deverá informar o Ministério de Ciência e Tecnologia (atual Ministério da Industria, Energia e Turismo). O Ministério fará a verificação do provedor de serviço de certificação (CSP), no intuito de comprovar se o provedor está operando em conformidade com a Lei de Assinatura Eletrônica. Sendo comprovada a conformidade, o CSP é incluído na lista dos "Prestadores de Serviço de Certificação e Assinatura Eletrônica[81]" (de Moneda y Timble, 2015).

Segundo a Lei nº 59 de 19 de dezembro de 2003, sobre Assinatura Eletrônica, qualquer empresa pública ou privada pode atuar como Provedor de Serviços de Certificação (CSP), emitindo certificados eletrônicos no padrão "ITU-T X.509" v3[82], os quais são utilizados para identificar uma pessoa física nos processos de transações eletrônicas (Ministerio de la Policía, 2015a).

Dentro do cenário de certificação digital, as seguintes entidades compõem o

[81] Lista de CSPs: https://sedeaplicaciones2.minetur.gob.es/prestadores/
[82] http://www.itu.int/rec/T-REC-X.509

modelo de gerenciamento do *eID Card* (European Communities, 2009e)

• **Escritório Geral de Polícia:** órgão competente que irá emitir e gerenciar o DNIe (*eID card)*.

• **Autoridade que aprova as políticas:** atua como um Comitê executivo da ICP, responsável pela elaboração e atualização das políticas aplicadas à certificação, bem como a homologação das Entidades Certificadoras (CAs Subordinadas).

• **Autoridades Certificadoras (CA)**: composta por uma CA Raiz e CAs Subordinadas.

• **Autoridades de Registro:** constituído por todos os escritórios que emitem o DNIe, estas auxiliam a CA em todos os procedimentos relacionados aos cidadãos, no que diz respeito a sua identificação, registro ou autenticação.

• **Autoridade de Validação (VA):** verificam o estado atual dos certificados usando o OSCP[83]. Atualmente somente o Ministério da Presidência e o FNMT atuam como autoridade de validação em nome do Departamento de Polícia.

• ***Accepting Party:*** qualquer pessoa ou entidade, diferente do portador, que aceita e confia nos certificados contidos no DNIe.

5.3.6 Obrigatoriedade da Identidade Eletrônica

Todo cidadão espanhol maior de 14 anos deve, obrigatoriamente, fazer a solicitação do Documento de Identidade Civil, o qual é conhecido no país por *Documento Nacional de Indentificación* (DNI). Desde março de 2006, este Documento de Identificação passou a ser utilizado também para fins de identificação eletrônica, recebendo a nomenclatura de DNIe (European Communities, 2009e). Muito embora exista a obrigatoriedade na emissão do documento de identificação civil, 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) é voluntária (Ministerio de la Policía, 2015a).

5.4 Sistemas de Gestão de Identidades

5.4.1 Padrão Adotado de Identidade Eletrônica (eID)

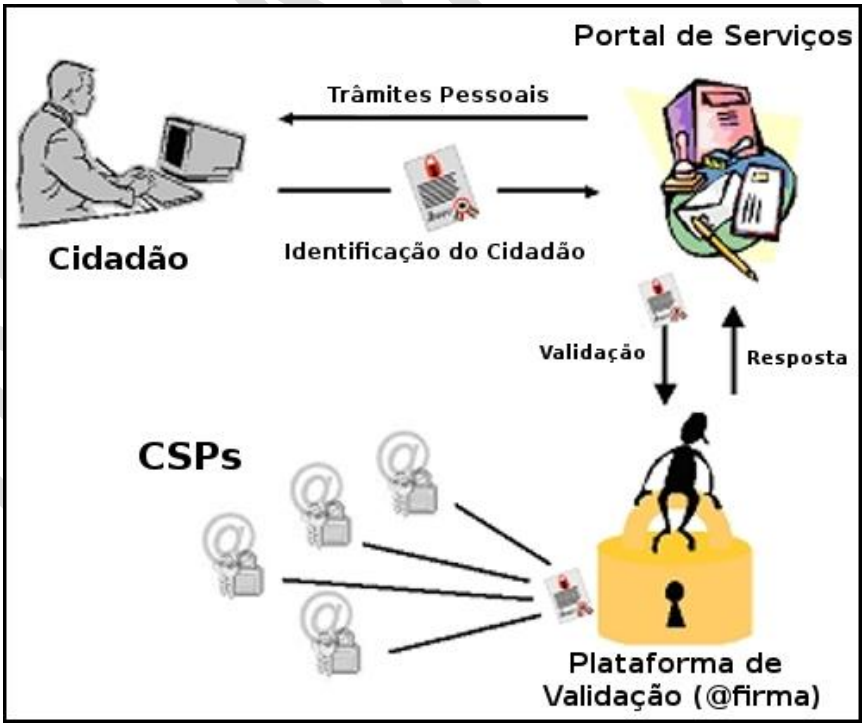
[83] http://ocsp.dnielectronico.es

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, as quais 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.

Por outro lado, a implantação progressiva do DNIe no território nacional, requer uma modificação nos Provedores de Serviço da Administração Pública, de forma a permitir a aceitação deste identificador eletrônico (DNIe) como elemento de autenticação e assinatura nos processos de comunicação eletrônica com o governo.

Diante deste contexto, o Ministério da Fazenda e Administrações Públicas (MINHAP) lançou um serviço chamado "@firma[84]" 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. A Figura 3 ilustra o funcionamento da plataforma @firma (Ministerio de la Policía, 2015a).

Figura 3: Plataforma @firma - Processo de Autenticação



[84] http://firmaelectronica.gob.es/

Em setembro de 2014, um Conselho de Ministros aprovou um acordo para a criação do sistema "Cl@ve", o qual se constitui de uma nova plataforma para identificação, autorização a assinatura eletrônica a ser utilizada pela Administração Pública. O "Cl@ve" complementa os atuais sistemas de acesso que utilizam o DNIe, oferecendo a possibilidade de realizar assinaturas eletrônicas, com certificados pessoais personalizados e armazenados em nuvem.

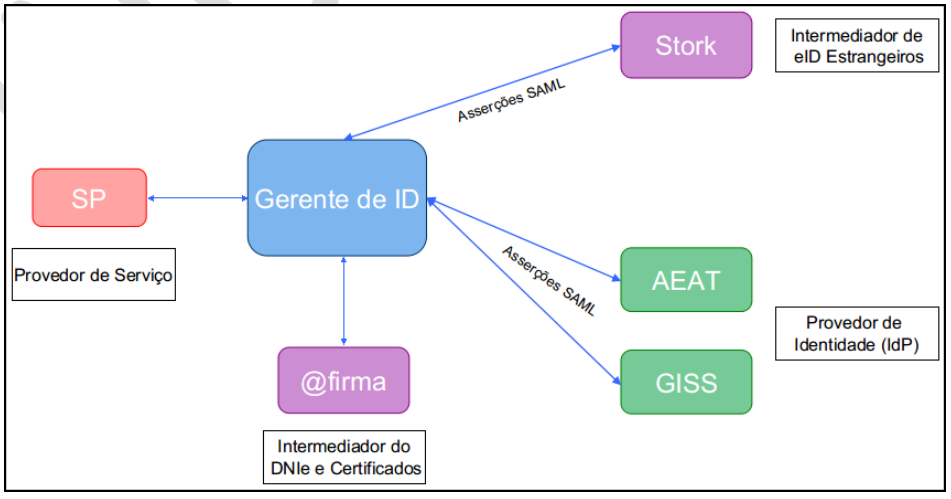
Utilizando um sistema de identificação, baseado em chaves combinadas (usuário e senha) e certificados eletrônicos, o sistema Cl@ve está se inserindo no Sistema de Federação de Identidades Eletrônicas, o qual possui os seguintes elementos.

• Provedor de Serviços (SP): entidades que oferecem serviços públicos por meio eletrônico aos cidadãos e utilizam a plataforma (Cl@ve) para identificação e autenticação dos mesmos.

• Provedores Identificação e Autenticação (IdP): entidades que proporcionam mecanismos de identificação e autenticação dos cidadãos, identificando os mesmos perante os provedores de serviço.

• Gerente de Identificação (*Gateway*): sistema intermediador que possibilita o acesso dos SPs aos diferentes mecanismos de identificação e seleção destes por parte dos usuários.

Figura 4: Plataforma @firma - Infraestrutura



De acordo com este projeto, os provedores de serviço precisam se integrar com o Gerente de Identificação, sendo este último responsável por estabelecer as relações pertinentes com os diferentes sistemas de identificação, incluindo a integração com o provedores do projeto STORK. A Figura 4 ilustra as relações entre os elementos.

5.4.2 Modelo de Gestão de Identidades

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.

O mais recente sistema de Identificação Eletrônico adotado na Espanha, baseado no sistema "Cl@ve" e Coordenado pela Diretoria de Tecnologia da Informação e Comunicação da Administração Geral do Estado, também opera no modelo de Gestão de Identidades Federada, utilizando certificados digitais. Entretanto, diferentemente do DNIe que permite a participação de SPs públicos e privados, o Cl@ve prevê a participação exclusiva de entidades públicas, operando como provedores de serviço.

5.4.3 Tecnologias de Gestão de Identidades

Para a identificação do cidadão, o modelo de gestão de identidades federadas Cl@ve se baseia no padrão SAML, mediante asserções SAML de navegador. Especificamente, o sistema Cl@ve utiliza o perfil SAML 2.0 definido pelo projeto STORK. Este perfil é utilizado tanto nas integrações entre Cl@ve e SP quanto nas interações entre Cl@ve e IdP.

Os provedores de serviços deverão ter a capacidade de criar *tokens* SAML. Para a geração destes *tokens*, os SPs devem fazer a integração com o motor SAML

conhecido por STORKSAMLEngine e com o Serviços de Aplicações Demo (SP-Demo), facilitando desta forma o desenvolvimento dos métodos de necessários para chamar as funções de envio e recebimento de *tokens* (de Estado de Administraciones Públicas, 2015).

5.4.4 Provedores de Identidade Privados

Segundo a Lei nº 59 de 19 de dezembro de 2003, que trata da assinatura digital, é permitida a participação de entidades privadas como provedores de serviço de certificação (CSP). Porém, estes provedores atuam somente no segundo nível, conforme demonstrado na Seção 3.5. Segundo publicado, os seguintes CSPs estão homologados.

- **Provedores Públicos.**

(a) DGP (*Dirección General de la Policía*): http://www.dnielectronico.es/

(b) FNMT-CERES (*Fábrica Nacional de Moneda y Timbre*): http://www.cert.fnmt.es/

(c) CATCert (*Agència Catalana de Certificació*): http://www.catcert.cat

(d) ACCV (*Autoritat de Certificació de la Comunitat Valenciana*): http://www.accv.es/

(e) IZENPE: http://www.izenpe.com/s15-12010/es/

- **Provedores Privados.**

(a) AC Camerfirma: http://www.camerfirma.com/

(b) ANF Autoridad de Certificación: http://www.anf.es/

(c) ANCERT (*Agencia Notarial de Certificación*): http://www.ancert.com/

(d) Firma Profesional: http://www.firmaprofesional.com

(e) ACA (*Autoridad de Certificación de la Abogacía*): http://www.abogacia.es

(f) Banesto: http://ca.banesto.es/

(g) SCR (*Servicio de Certificación de los Registradores*): https://www.registradores.org

Da mesma forma, no modelo de gestão de identidades utilizando o DNIe, é

permitida a participação de provedores de serviço privados, os quais podem ser consultados em http://www.dnielectronico.es/servicios_disponibles/index.html. Na grande maioria, os provedores de serviço privados são compostos por instituições financeiras, por exemplo, bancos.

Por outro lado, o modelo de gestão Cl@ve foi construído para aumentar a usabilidade dos sistemas estatais. Aprovado em setembro de 2014, este modelo prevê que até o final do ano de 2015 todos os órgãos públicos, que operam como provedores de serviço, já tenham se adequado ao uso do novo sistema (para las Administraciones, 2014).

5.4.5 Padrões de Interoperabilidade

A Estratégia Nacional de Gestão de Identidades, baseada no cartão de identidade eletrônico (DNIe), segue padrões internacionalmente conhecidos, como forma de garantir a interoperabilidade da solução. Entre os padrões, estão (Ministerio de la Policía, 2015a)

- ISO 7816, partes 1/2/3/4 (Protocolo de transmissão T=0).
- ISO 14443, partes 1/2/3/4 (Protocolo de transmissão T=CL).
- Estrutura interna de arquivos, segundo o padrão PKCS#15.
- Incorporação de *checksum* criptográfico do tipo MAC, segundo ANSI X9.19 e DES.
- Protocolo de estabelecimento das chaves de sessão baseado no esquema proposto em ISO/IEC 9798, parte 3.
- Cálculo de chaves de sessão segundo o padrão ANSI X9.63.
- Estabelecimento de canais seguros baseados na EN 14890 (versão 2013).

Com relação aos frameworks, existem dois serviços especialmente dedicados à interoperabilidade no contexto de e-Gov, sendo um para nível nacional e outro para nível Europeu (European Communities, 2009e).

- **Esquema Nacional de Interoperabilidade:** compreende um conjunto de critérios e recomendações de segurança, conservação e normatização, que as Administrações Públicas deverão seguir para a tomada de decisões tecnológicas,

garantindo dessa forma a interoperabilidade dos serviços prestados pelos SPs aos cidadãos (Ministerio de la Presidencia, 2010).

• **Projeto Stork:** a Espanha participa deste projeto de aceitação do eID e identificadores similares em serviços de e-Gov de outras Administrações Europeias.

5.4.6 Gestão de Confiança

A gestão de confiança, adotada na Estratégia Nacional de Gestão de Identidade Eletrônica, está baseada nos padrões tecnológicos estabelecidos como uso do SAML e principalmente no ingresso de novos provedores de certificados (CSPs), conforme descrito na Seção 3.5.

A adoção da plataforma de validação "@firma", disponibilizada pelo Ministério da Fazenda e Administrações Públicas, garante um modelo de confiança tanto para os provedores de serviço quanto para os próprios cidadãos, atuando como uma espécie de "terceira parte confiável", validando os certificados digitais utilizados nas transações *on-line*.

5.4.7 Níveis de Garantia dos Provedores de Identidades

Não existe um padrão de pontuação ou definição de nível para os provedores de identidades. Entretanto, toda homologação de um novo provedor de certificados é feita com base na Lei de Assinaturas, garantindo dessa forma, o uso de certificados digitais confiáveis, perante a comprovação da identidade do cidadão.

Conforme citado por European Communities (2009e) de acordo com as políticas estabelecidas, foram determinados 3 níveis de segurança no modelo de autenticação do DNIe, os quais se refletem no "*Framework* Nacional de Segurança". Abaixo são descritos cada um destes níveis.

1. **Nível Básico:** autenticação por conhecimento, que acontece ao se inserir um nome de usuário e uma senha ou um certificado digital.

2. **Nível Médio:** obrigatório o uso de Certificados Eletrônicos Qualificados (QEC), certificados estes emitidos em conformidade com a Lei de Assinatura. É de responsabilidade do administrador do SP permitir métodos de autenticação mais ou menos rígidos. Os certificados deste nível são emitidos de forma *on-line*.

3. **Nível Alto:** da mesma maneira que o nível médio, o uso de Certificados Eletrônicos Qualificados é obrigatório. O que difere este nível dos demais é a forma com que o usuário obtém este certificado, o qual necessariamente deverá ser emitido em um dispositivo físico personalizado e entregue pessoalmente ao cidadão.

5.4.8 Mecanismos ou Técnicas de Autenticação

As funcionalidades do Cartão Nacional de Identidade Eletrônica (DNIe) são complementadas com o suporte oferecido pela Plataforma de Validação multiPKI, que oferece de maneira gratuita o serviço de validação de certificados, o qual é necessário ao funcionamento do governo eletrônico na Espanha (European Communities, 2009e). A Plataforma de Validação multiPKI é conhecida como “Plataforam @fima v.5.0”, validando certificados eletrônicos de autenticação e certificados para assinatura eletrônica (*eSignatures*), emitidos pelas Autoridades Certificadoras do país, incluindo tanto autoridades públicas quanto privadas. A plataforma foi criada utilizando sistemas de código aberto (*open source*) e padrões abertos (*open standards*) (Ministerio de la Policía, 2015a).

Diante deste cenário de e-Gov que opera com uma base de certificados PKI e com o DNIe, é imprescindível que todo serviço (SP e IdP), que opera no modelo de gestão de identidades, se adeque à plataforma @firma. A seguir é descrita a sequência de passos, seguidos pelo usuário, ao acessar um provedor de serviços (público ou privado) (European Communities, 2009e).

1. O cidadão solicita uma uma conexão segura de autenticação ao SP.
2. O SP (Organismo Público ou Entidade Privada) cria uma mensagem autenticada e a envia ao cidadão.
3. O cidadão verifica a validade do certificado de serviço oferecido.
4. O código para a sessão e seu código cifrado é gerado com a chave pública do SP privado ou público.
5. A mensagem para a troca de códigos é construída.
6. O cidadão insere o DNIe no leitor de cartões e, com o certificado de autenticação eletrônica, valida a mensagem para a troca de códigos.

7. O canal privado é estabelecido.
8. O SP verifica a mensagem para abrir a sessão.
9. O SP verifica na Autoridade de Validação o *status* de validação do Certificado de Autenticação do Cidadão.
10. Um canal seguro é estabelecido e o túnel SSL é fechado.

No modelo federado de identidades Cl@ve, para se fazer a integração entre usuários, provedores de serviço e provedores de identidade, é inserido um sistema central, conhecido por “Gerente de Identificação”, cujo papel principal é promover a confiança entre os elementos deste modelo. Para que se estabeleça a relação de confiança entre estes elementos distintos, é adotado o SAML como padrão e as mensagens são trocadas a partir do uso de certificados digitais, garantindo uma transmissão segura em todo o processo de identificação e autenticação (Ministerio de Estado de Administraciones Públicas, 2015).

Neste cenário, com o uso do modelo Cl@ve, o fluxo de interações entre os elementos (usuário, SP e IdP) é descrito abaixo.

1. O cidadão acessa um serviço de administração eletrônica (SP), escolhendo como opção de autenticação o Cl@ve.
2. O cidadão é redireciondo ao Cl@ve, que lhe apresenta uma tela para selecionar o método de identificação que deseja utilizar. As opções de identificação são determinadas pelo SP, que o faz mediante o nível QAA (*nivel de aseguramiento de la calidad de la autenticación*) que espera do IdP.
3. O cidadão seleciona o método de identificação e é redirecionado ao IdP correspondente. Após a autenticar-se com sucesso, o cidadão é redirecionado ao Cl@ve.
4. De forma transparente, sem que seja necessária nenhuma interação, o cidadão é redirecionado ao SP, o qual lhe concede permissão de acesso.

5.5 Privacidade relacionada a Identidade Eletrônica

5.5.1 Uso de Pseudônimos

Utilizando o DNIe, ao solicitar acesso a um provedor de serviço, é exigido do

usuário a comprovação da sua identidade. Isto é feito através da validação do certificado de autenticação, o qual está armazenado no *chip* do cartão de identidade. Entretanto, para se fazer a leitura deste certificado, é solicitado ao usuário que seja inserida uma senha pessoal (PIN), composta por 8 caracteres alfa-numéricos e sensível a letras maiúsculas.

Ao mesmo tempo que, a comprovação da identidade do cidadão é feita através da validação do certificado de autenticação, não é permitido ao usuário fazer uso de pseudônimos. Neste contexto, todas as informações pessoais do usuário, contidas no DNIe, poderão ser utilizadas nas transações *on-line*.

5.5.2 Poder de escolha do Cidadão (eID e provedores de identidades)

O modelo de gestão de identidades na Espanha prevê a participação de entidades públicas ou privadas no fornecimento de certificados digitais de autenticação. Por serem utilizados para acesso aos provedores de serviço, estes certificados operam como uma espécie de provedor de identidades. Portanto, para o cidadão espanhol é permitido a escolha de qual provedor de certificados utilizar.

Com a adoção do Cl@ve em 2014, o modelo de gestão passa gradativamente a operar em um novo sistema, o qual através de um *gateway* central permite ao usuário escolher um, entre vários métodos de autenticação oferecidos. Em outras palavras, o método de autenticação escolhido pelo usuário pode ser, desde o uso do próprio DNIe ou credenciais de acesso (usuários, senha, PIN, SMS), até o uso de certificados digitais.

Portanto, mesmo que o modelo federado Cl@ve venha a se tornar o padrão para todas as comunicações, tanto com o governo quanto com o setor privado, o usuário continuará contando com o poder de escolha sobre qual identificador ou IdP adotar.

5.5.3 Controle de Liberação de Dados Pessoais

Muito embora exista a preocupação do governo com o tratamento dos dados pessoais, a qual está refletida pela Lei Orgânica nº 15 de 13 de dezembro de 1999, não foram encontradas referências técnicas quanto à abordagem “centrada no usuário”. A Lei em questão afirma que os dados pessoais devem ser utilizados de modo lícito,

sendo o provedor de serviços responsável legalmente pelo uso que fizer destas informações. Ao mesmo tempo, a Lei afirma que ao usuário cabe o direito de ser informado caso seus dados pessoais sejam utilizados.

5.5.4 Leis Específicas de Privacidade

Na Espanha, a lei que trata da privacidade é a Lei Orgânica 15/1999 de 13 de dezembro[85], sobre a Proteção de Dados Pessoais (L.O.P.D.). A L.O.P.D. tem por objetivo “garantir e proteger, em tudo que concerne o manuseio de dados pessoais, as liberdades públicas e direitos fundamentais de pessoas físicas e especialmente sua honra e intimidade pessoal e familiar”. Nesta lei estão inclusos 9 princípios sobre a proteção dos dados, a saber.

1. Qualidade dos dados: os dados pessoais tratados não podem ser utilizados para fins incompatíveis com aqueles para os quais os dados foram recolhidos e devem ser armazenados de forma a permitir o exercício do direito de acesso.
2. Direito à informação na coleta de dados: as pessoas às quais os dados pessoais são solicitados, devem ser previamente e explicitamente informadas, de forma precisa e inequívoca.
3. Consentimento do afetado: o tratamento de dados pessoais exige o consentimento expresso da pessoa afetada.
4. Dados especialmente protegidos: nenhum cidadão poderá ser obrigado a fornecer informações sobre sua ideologia, religião ou crença.
5. Dados sobre a saúde: não é permitido o processamento de dados pessoais sobre a saúde das pessoas.
6. A segurança dos dados: os dados pessoais deverão ser armazenados e processados de forma segura a evitar alteração, perda ou acesso não autorizado.
7. Dever de sigilo: os envolvidos em qualquer fase do tratamento de dados pessoais são obrigados a manter a confidencialidade em relação à mesma.
8. Comunicação de dados: os dados pessoais submetidos a terceiros só poderão ser divulgados para fins diretamente relacionados com as funções legítimas do cedente e cessionário, através de consentimento prévio.

[85] http://www.dnielectronico.es/marco_legal/ley_organica_15_1999.html

9. Acesso aos dados por terceiros: caso os dados pessoais sejam utilizados por terceiros, estes também serão legalmente responsáveis pelos dados, devendo seguir todos os princípios citados na L.O.P.D..

5.5.5 Aplicação da Lei de Privacidade

Segundo apresentado pelo *Ministerio de la Policía* (2015a), a Plataforma de Validação "@firma" cumpre as normativas estabelecidas pela Lei Orgânica 15/1999 de 13 de dezembro (Lei Proteção de Dados Pessoais), garantindo o uso correto dos dados de caráter pessoal, principalmente com relação ao princípio de tratamento dos dados por terceiros (Validação), evitando dessa forma o uso indevido.

Por outro lado, a Plataforma de Validação cumpre também as recomendações e boas práticas[86] propostas pelos critérios de Segurança, Normatização e Conservação estipuladas pelo Conselho Superior de Administração Eletrônica. Essa conformidade facilita a adoção de medidas técnicas e organizacionais, de forma a garantir a autenticidade, confidencialidade, integridade, disponibilidade e conservação das informações tratadas e geridas por este sistema.

[86] http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog.html

6 ESTÔNIA

6.1 Perfil Sociopolítico, Econômico e Governo Eletrônico

6.1.1 Estrutura Sociopolítica

Situado na Europa Setentrional, o território da Estônia constituí-se por uma porção continental e um grande arquipélago no mar Báltico. Limita-se ao norte com o golfo da Finlândia, a leste com a Rússia, ao sul com a Letônia e a oeste com o mar Báltico, que o separa da Suécia. Politicamente se organiza como uma República Parlamentarista, tendo um Primeiro Ministro para governar o país, o qual é nomeado pelo Parlamento com indicação do Presidente da República. O Parlamento é formado de 101 deputados, eleitos por voto direto da população, não havendo direito a reeleição. É um país membro da União Europeia desde 1 de maio de 2004 e da OTAN desde 29 de março de 2004.

Com uma área territorial de 45 mil km², pouco superior a Dinamarca, conta com uma população na ordem de 1,3 milhões de habitantes, densidade demografia de 29,7 habitantes por km² e IDH de 0,840. A cidade mais populosa é a capital Tallinn (região de Harju), onde reside aproximadamente 1/3 da população, cerca de 398 mil pessoas. Está dividida desde março de 2013 em 15 regiões, as quais subdividem-se em 226 municípios, sendo 33 urbanos e 193 rurais.

6.1.2 Acesso à Internet

De acordo com *European Comission* (2014c), em relação aos índices de acesso à Internet, as seguintes estatísticas são apresentadas para o ano de 2013.

- Casas com acesso à Internet: 80%.
- Empresas com acesso à Internet: 97%.
- Casas com acesso por banda larga: 77%.
- Empresas com acesso por banda larga: 94%.
- Indivíduos que fizeram compras pela Internet (últimos 3 meses de 2013): 16%.
- Empresas que receberam pedidos de compras *on-line* (2013): 13%.

6.1.3 *Ranking* de e-Gov da ONU

De acordo com *United Nations* (2014), classificada com o índice de 0,818, a Estônia passou a ocupar a 15ª posição no *ranking* de governo eletrônico (EGDI), subindo 5 posições em relação ao de 2012. O índice de desenvolvimento em e-Gov apresentou as seguintes informações.

- Serviços *On-line*: 0,7717.
- Infraestrutura em Telecomunicações: 0,7934.
- Capital Humano: 0,8889.

6.1.4 Principais Políticas (Leis, atos, decretos, etc)

- **1996:** Ato de Proteção aos Dados Pessoais (PDPA) com alterações em 2003 e 2008.
- **1998:** Ato que estabelece as normas gerais sobre coleta, avaliação, preservação e acesso a documentos.
- **2000:** Legislação sobre assinatura digital. Alterada em 2007 e 2010.
- **2001:** Legislação sobre o acesso público de informação do governo, nova versão em 2008. (PIA)
- **2004:** Implementação da diretriz de *eCommerce* estabelecida pela União Europeia (2000/31/CE). Lei de proteção ao consumidor.
- **2008:** Regulamento que estabelece diretrizes de segurança para a proteção dos sistemas que processam dados governamentais.

6.1.5 Cronologia do Desenvolvimento de e-Gov e GId

- **1998:** adoção da primeira estratégia sobre informação eletrônica no país, os "Princípios da Política de Informação Estoniana", complementado por um Plano de Ação da Política de Informação (atualizado em 2001).
- **2000:** lançamento da aplicação *eTaxBoard* que permitiu a declaração de imposto de renda *on-line* aos cidadãos.
- **2000:** decisão ministerial. Em maio deu início à implantação do *Id Card*, um cartão utilizado para fins de Identificação Civil, bem como para Identificação Eletrônica.
- **2001:** com o intuito de garantir comunicação entre os bancos de dados

governamentais, criou-se o sistema *X-Road*.

• **2003:** O Governo da Estônia lança seu portal de *eGovernment* com intuito de reunir todos os serviços de *e-Gov* em um ambiente único.

• **2004:** publicado o plano de Ação da Política de Informação para o período de 2004 a 2006.

• **2005:** lançada uma política nacional de padronização para segurança da informação, com o objetivo de criar um ambiente seguro para empresas e consumidores.

• **2006:** publicação dos padrões estoniano de interoperabilidade (versão 2.0). Neste mesmo ano é lançado um serviço para ajudar os alunos a receberem resultados de exames nacionais por meio eletrônico.

• **2007:** primeiras eleições nacionais do mundo com opção de votação pela Internet. Lançamento de um serviço eletrônico para as autoridades estonianas poderem fazer consultas sobre a renda dos contribuintes de uma determinada área.

• **2007:** início da operação do *Mobile ID*, como alternativa ao uso do *ID Card*.

• **2007:** disponibilizados os primeiros passaportes com dados biométricos gravados no *chip* eletrônico, em conformidade com a Diretriz Europeia 2252/2004/EU.

• **2011:** *Mobile ID* passa a contar com todas as funcionalidades eletrônicas disponíveis no Cartão de Identidade Eletrônico (*ID Card*).

• **2013:** aprovação do chamado *Green Paper*, o qual estabelece diretrizes de serviços públicos, além de elencar e solucionar problemas para serviços de *eGov*. Acordo intergovernamental entre Estônia e Finlândia assinado digitalmente com foco no desenvolvimento de serviços de *e-Gov* entre os dois países.

6.2 Modelo de Organização de Documentos Civis

6.2.1 Registro Civil

Para cada novo registro de nascimento emitido, é gerado um ”Número de Registro Civil” único, conhecido por IK (*isikukood*), o qual é fornecido pelo Centro de Registro e Sistemas da Informação da Estônia[87]. Este número de registro é formado pela estrutura **GYYMMDDSSSC**, que constitui-se de uma sequência de 11 dígitos decimais, tendo o seguinte significado.

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

- **G:** século de nascimento e sexo.
- **YY:** ano.
- **MM:** mês.
- **DD:** dia.
- **SSS:** número sequencial de nascimento[88].
- **C:** dígito verificador (*checksum*).

Este Número de Registro Civil 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 da Estônia.

6.2.2 Identidade Civil

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[89] através da Internet, o qual que teve início em 2005 (European Comission, 2014c). Segundo a lei, todos os cidadãos maiores de 15 anos e residentes estrangeiros são obrigados a ter um cartão de identificação (GENCS 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*. Por meio de uma parceria entre os setores público e privado, os cartões são emitidos com certificados digitais, os quais garantem a segurança nas transações eletrônicas (Govenment of the Estonia, 2003). O uso do *ID Card* é diversificado, servindo tanto como cartão de identificação civil, documento de viagem, cartão bancário, voto eletrônico e provendo acesso aos sistemas *on-line*, quanto utilizado para visualização de histórico médico do seu portador (desde 2010) (European Comission, 2014c).

Além do cartão eletrônico, outros documentos são reconhecidos para comprovar

[88] Número que demonstra a sequência de nascimentos ocorridos no mesmo dia
[89] 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

a identidade civil, a saber (GENCS EU, 2012).

• Passaporte estoniano.

• Passaporte pertencente à União Europeia.

• Documento de viagem para estrangeiros - emitido pelo governo estoniano.

6.2.3 Relação do Documento de Viagem com a Identidade Civil

Segundo *European Comission* (2014c), o cartão de identidade civil (*ID Card*) pode ser usado como passaporte para viagens realizadas dentro da Comunidade Europeia, o que não descarta o passaporte tradicional para viagens realizadas para outros países.

O passaporte tradicional pode ser solicitado em um escritório de serviços, sendo emitido em até 30 dias após a entrega dos seguintes documentos (Politsei- ja Piirivalveamet, 2014b)

• Formulário de solicitação preenchido manualmente, que pode ser enviado por *e-mail* ou pelos correios.

• Cópia do Documento de Identidade.

• Foto colorida 4x5 enviada pelos correios, ou 480x600 *pixels* (JPG) por *e-mail.*

• Comprovante de pagamento da taxa correspondente à emissão do documento.

6.2.4 Biometria no Sistema de Identidade Civil

Em 22 de maio de 2007 foram disponibilizados os primeiros passaportes com dados biométricos gravados no *chip* eletrônico. Esta implementação foi realizada na Estônia para atender a regulamentação 2252/2004/EU estabelecida pela União Europeia (European Comission, 2014c). O governo determina o uso dos dados biométricos do cidadão somente em casos muito específicos previstos em lei, incluindo a lei dos documentos de identidade. São considerados como dados biométricos: imagem facial, impressões digitais, imagem da assinatura e imagem da iris (GENCS EU, 2012).

Para a emissão do passaporte tradicional, a coleta de impressões digitais é obrigatória para cidadãos maiores de 12 anos (Politsei- ja Piirivalveamet, 2014b).

6.3 Identidade Eletrônica

6.3.1 Uso da Identidade Eletrônica

Na Estônia existem 3 soluções para o uso da Identidade Eletrônica: *ID Card*, *Mobile ID* e 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.

O mais importante sistema de eIDM da Estônia é baseado no *ID Card*, um Cartão de Identidade Eletrônico, que tem por objetivo facilitar aos cidadãos e residentes acesso aos sistemas de governo eletrônico do país. A emissão do *ID Card* é obrigatória para todos cidadãos estonianos maiores de 15 anos e para todos os residentes estrangeiros com visto legal de residência, independente da idade. Este cartão tem três funções principais, a saber (European Communities, 2009d).

1. Identificação Civil.
2. Autenticação em sistemas *on-line* com uso de Certificado Digital.
3. Assinatura Digital de documentos.

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 (Govenment of the Estonia, 2003).

Em maio de 2007 o serviço *Mobile ID* (*Wireless PKI*) foi iniciado no país como alternativa ao uso do *ID Card* (European Communities, 2009d). Este serviço é oferecido através de um operador de serviços móveis (EMT[90], Elisa[91], Tele2[92] e Lithuanian[93]) em cooperação com os bancos e o Centro de Certificação[94], o “AS Sertifitseerimiskeskus”. Similarmente ao Cartão de Identidade Eletrônico, o *Mobile ID* passou a oferecer a

[90] https://www.emt.ee/en/liitu
[91] https://www.elisa.ee/
[92] http://www.tele2.ee/
[93] http://www.omnitel.lt/klientu_aptarnavimas_telefonu
[94] https://www.sk.ee/en

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) (European Comission, 2014c).

Finalmente, 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 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* (Govenment of the Estonia, 2015).

6.3.2 Cadastro da Identidade Eletrônica

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*[95], responsável por cuidar das fronteiras, monitorar e identificar os cidadãos (Govenment of the Estonia, 2015).

Todo cidadão maior de 15 anos que deseje um cartão de identificação poderá solicitá-lo pessoalmente em um escritório da Polícia, ou através de correspondência postal, ou por *e-mail*, fornecendo os seguintes documentos (Politsei- ja Piirivalveamet, 2015).

- Formulário de solicitação.
- Cópia do Documento de Identidade.
- Foto colorida 4x5 (impressa) ou 480x600 pixels no formato JPG.
- Comprovante de pagamento da taxa correspondente à emissão do documento.

[95] Em estoniano *Politsei- ja Piirivalveamet*

Aos cidadãos menores de 15 anos que desejem utilizar a identificação eletrônica, a emissão é permitida desde que apresentem também uma cópia do Documento de Identidade de seu representante legal.

Por outro lado, a emissão do “Mobile ID” 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* (Govenment of the Estonia, 2015).

6.3.3 Atributos da Identidade Eletrônica

Conforme citado anteriormente, a criação da Identidade Eletrônica, independentemente da solução adotada pelo cidadão, será administrada de forma centralizada pela Polícia, sendo necessário seguir os procedimentos conforme descrito na Seção 3.2.

Todas as informações disponíveis de forma impressa no *ID Card*, com excessão da foto e da assinatura manuscrita, poderão ser utilizadas como atributo no uso da Identidade Eletrônica (Govenment of the Estonia, 2003). Entre estes atributos, encontram-se os seguintes.

- Nome do Cidadão.
- Data de Nascimento.
- Sexo.
- Naturalidade.
- Identificador de Registro (IK).

Importante citar que atributos complementares poderão ser acessados de forma indireta, como resultado de verificação em um banco de dados mantido pelo governo (Govenment of the Estonia, 2003).

6.3.4 Biometria

Os sistemas de Identidade Eletrônica na Estônia não fazem uso ou coleta de

dados biométricos dos cidadãos (European Communities, 2009d).

6.3.5 Uso de Certificado Digital na Identidade Eletrônica

A SK[96] (em estoniano *AS Sertifitseerimiskeskus*) é um Centro de Certificação, fundado por dois grande bancos (Hansapank e Eesti Ühispank) e por duas companhias de telecomunicações (Eesti Telefon e EMT), constituindo-se atualmente como a única Autoridade Certificadora (CA) na Estônia, a qual é responsável pela emissão dos certificados para autenticação e assinatura digital utilizados nos Documentos de Identidade Nacionais (*ID Card*, *Mobile ID* e Digi-ID). A principal função da SK é assegurar a confiança e integridade dos certificados digitais emitidos, fornecendo garantias legais para esta infraestrutura que opera no país (AS Sertifitseerimiskeskus, 2014a).

Cada *ID Card* emitido contém dois certificados digitais, sendo um para uso em serviços de autenticação e outro com valor legal para assinatura digital de documentos eletrônicos. Estes certificados não possuem restrições de uso, sendo utilizados portanto para todas as formas de comunicação, incluindo comunicações entre duas pessoas, entre organizações, além das próprias interações com o governo (AS Sertifitseerimiskeskus, 2014a). Como possuem uma senha pessoal (PIN) individual, cada certificado (autenticação e assinatura) pode ser utilizado separadamente para acesso aos serviços providos pelo setor público ou privado (Govenment of the Estonia, 2003).

Os certificados contidos no *ID Card* estão ligados ao Código de Identificação Pessoal (IK), operando dessa forma como um identificador único nas transações *on-line* realizadas pelos cidadãos e residentes (European Communities, 2009d).

6.3.6 Obrigatoriedade da Identidade Eletrônica

Conforme citado na Seção 3.1, a emissão do Cartão de Identidade Civil (*ID Card*) é obrigatória. Entretanto, caso não deseje, o usuário pode solicitar a revogação dos certificados digitais inclusos no cartão, abrindo mão das funcionalidades eletrônicas, tendo seus dados removidos de algumas bases de dados. O cidadão que optar por este procedimento não poderá ter acesso aos sistemas de governo eletrônico

[96] https://www.sk.ee

(*e-Gov*) (Govenment of the Estonia, 2003). Por outro lado, o governo não obriga o cidadão a fazer a emissão do *Digi-ID* ou do *Mobile-ID*. Portanto, a adoção da Identidade Eletrônica acaba sendo feita de forma voluntária pelo cidadão (Politsei- ja Piirivalveamet, 2014a).

6.4 Sistemas de Gestão de Identidades

6.4.1 Padrão Adotado de Identidade Eletrônica (eID)

Uma decisão ministerial de maio de 2000 deu início ao *Id Card* na Estônia. Esta decisão impactou na emissão de um Documento de Identidade Civil de caráter obrigatório para os cidadãos maiores de 15 anos e para todos os estrangeiros com residência permanente no país. Um dos requisitos exigidos neste Documento de Identidade é a existência de um *chip* para armazenar informações pessoais do portador, bem como certificados digitais. A funcionalidade oferecida por este *chip* oferece a possibilidade de uso do *Id Card* também como Documento de Identidade Eletrônica. Fisicamente o *Id Card* é confeccionado de acordo com as especificações ICAO[97], permitindo seu uso como documento de viagem (European Communities, 2009d).

O Centro de Certificação Estoniano conhecido como *AS Sertifitseerimiskeskus*, que também é parceiro do projeto STORK, opera emitindo os certificados digitais para as soluções de Identidade Eletrônica no país (*ID Card*, *Mobile ID* 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).

6.4.2 Modelo de Gestão de Identidades

A Estônia adota um modelo centralizado de Gestão de Identidades, 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[98], que verifica o

[97] http://www.icao.int/Security/mrtd/pages/Document9303.aspx
[98] https://www.ietf.org/rfc/rfc2560.txt

certificado do usuário, devolvendo para a aplicação cliente uma das seguintes respostas (AS Sertifitseerimiskeskus, 2014b)

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

Dependendo da resposta retornada pelo SK, o provedor de serviços pode autorizar ou não o acesso do usuário ao serviço requisitado (AS Sertifitseerimiskeskus, 2014b). Neste contexto, pode-se dizer que o Centro de Certificação atua como um provedor de identidades na Estônia.

6.4.3 Tecnologias de Gestão de Identidades

Dentre as tecnologias adotadas pelo governo da Estônia pode ser citado o sistema OCSP, descrito na Seção 4.2, o qual é responsável pela verificação e validação dos Certificados Digitais utilizados na autenticação dos sistemas *on-line* e na assinatura de documentos eletrônicos.

Para a confecção do *ID Card*, são seguidas as especificações ICAO de forma que este cartão possa ser utilizado também como documento de viagem. A Seção 4.1 descreve melhor este padrão adotado.

Outra tecnologia utilizada pelo país é o SAML. Muito embora os documentos e *sites* oficiais não façam referência à adoção desta especificação, conforme citado em Carol Geyer (2008), os sistemas de gestão de identidade que fazem uso do *ID Card* implementam o SAML.

6.4.4 Provedores de Identidade Privados

Embora exista a possibilidade de um provedor de identidades privado atuar no cenário de gestão de identidades da Estônia, até o momento o governo mantém somente o Centro de Certificação - SK oferecendo a infraestrutura necessária para a operação do sistema eID (Govenment of the Estonia, 2003).

6.4.5 Padrões de Interoperabilidade

Atuando em parceria com o projeto STORK, o governo da Estônia procura

desenvolver sistemas que sejam interoperáveis com outros países europeus. Um grande exemplo pode ser citado com o desenvolvimento do *software* DigiDoc, desenhado para suportar uma grande variedade de *smartcards* baseados em certificados digitais que operam com uma infraestrutura PKI. Países como a Áustria, Bélgica e Finlândia demonstram grande compatibilidade com o *ID Card* estoniano (European Communities, 2009d).

6.4.6 Gestão de Confiança

No que se refere à emissão ou ativação do Identificador Eletrônico, toda a gestão é controlada de forma centralizada pela Polícia (*Police and Border Guard Board*) (Govenment of the Estonia, 2015). Entretanto, as soluções de eID dependem diretamente dos certificados digitais para poderem operar, os quais são gerenciados pelo Centro de Certificações (*AS Sertifitseerimiskeskus*), órgão do governo responsável por emitir, validar e revogar tais certificados (Govenment of the Estonia, 2003).

6.4.7 Níveis de Garantia dos Provedores de Identidades

Não há parâmetros para comparação, pois apenas uma empresa atua como provedor de identidade.

6.5 Privacidade relacionada a Identidade Eletrônica

6.5.1 Uso de Pseudônimos

Muito embora alguns provedores de serviço permitam o cadastro de pseudônimos, o uso da certificação digital para autenticação é obrigatória para todo cidadão que deseje realizar alguma transação *on-line*. Por outro lado, toda certificação digital está associada ao portador do cartão de identidade, dessa forma o usuário é sempre identificado pelo SP (Govenment of the Estonia, 2003).

6.5.2 Poder de escolha do Cidadão (eID e provedores de identidades)

Para todo cidadão com residência permanente na Estônia é obrigatória a emissão do *ID Card* para ser utilizado como Documento de Identidade Civil, no entanto, é voluntária a utilização da Identificação Eletrônica provida por este cartão, bem como é voluntária a adoção do *Mobile ID* ou do Digi-ID.

Optando por fazer uso da eID, o cidadão só poderá contar com um provedor de identidades, o *AS Sertifitseerimiskeskus*, muito embora o modelo de gestão de identidades admita o ingresso de provedores privados (Govenment of the Estonia, 2003)

6.5.3 Controle de Liberação de Dados Pessoais

Segundo informado por AS Sertifitseerimiskeskus (2014a), os dados pessoais são encaminhados ao provedor de serviço na seguinte ordem.

1. Nome e Sobrenome do usuário.
2. Código de Registro de Residente ou Data de Nascimento.
3. Informações de contato.
4. Dados referentes à identificação.
5. Informações sobre a emissão do certificado de autenticação.
6. Número e data de validade do documento do cliente ligado aos certificados emitidos.
7. Dados das operações realizadas pelo cliente durante o uso do Serviço (suspensão de certificados, término da suspensão, anulação, renovação de certificados e criação de assinaturas digitais), que são necessários principalmente para se verificar a validade do certificado e a assinatura.

Para o envio e processamento destas informações ao SP, é necessário o consentimento do cliente (AS Sertifitseerimiskeskus, 2014a).

6.5.4 Leis Específicas de Privacidade

Em 19 de julho de 1996 foi publicado o ”Ato de Proteção aos Dados Pessoais” (PDPA). A primeira adequação ocorreu em 2003 com a publicação de novo Ato, adequando o PDPA em conformidade com a Diretriz Europeia nº 95/46/EC, a qual preserva os direitos fundamentais e a liberdade dos indivíduos com o respectivo processamento dos seus dados pessoais. A segunda e última adequação ocorreu em 2008, estendendo os princípios existente no PDPA de forma a aplicá-los no processamento de dados pessoais e dos Números de Registro Civil. Foram também

retiradas as categorias existentes quanto à classificação dos dados (Dados Pessoais não sensíveis), passando para apenas duas categorias (European Comission, 2014c)

1. Dados Pessoais.
2. Dados Pessoais sensíveis.

No dia 1 maio de 1998 foi publicado o Ato que estabelece normas gerais sobre a coleta, avaliação, arquivamento, preservação e acesso a documentos (European Comission, 2014c).

Entra em vigor em 2008 o regulamento sobre “Sistema de medidas de segurança para sistemas de informação”, estabelecendo procedimentos para especificar padrões de segurança organizacional, física e de T.I. para proteger os dados contidos em banco de dados do governo. No entanto, este regulamento não é aplicado à segurança dos sistemas de processamento de informações sigilosas do Estado (European Comission, 2014c).

6.5.5 Aplicação da Lei de Privacidade

Conforme descrito por AS 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.

7 HOLANDA

7.1 Perfil Sociopolítico, Econômico e Governo Eletrônico

7.1.1 Estrutura Sociopolítica

A Holanda está dividida em 12 regiões conhecidas por províncias e administradas cada uma por um governador, também conhecido por comissário do Rei ou da Rainha.

Possuindo um IDH muito elevado (0,915), conta com aproximadamente 17 milhões de habitantes segundo censo realizado em 2013. Com uma área de 41.526 km², tem um densidade demográfica na ordem de 404 habitantes por km², quase 18 vezes maior que o Brasil.

7.1.2 Acesso à Internet

De acordo com *European Comission* (2014f), em relação aos índices de acesso à Internet em 2013, as seguintes estatísticas são apresentadas.

- Casas com acesso à Internet: 95%.
- Empresas com acesso à Internet: 100%.
- Casas com acesso por banda larga: 87%.
- Empresas com acesso por banda larga: 96%.
- Indivíduos que fizeram compras pela Internet (últimos 3 meses): 59%.
- Empresas que receberam pedidos de compras *on-line* (último ano): 13%.

7.1.3 *Ranking* de *e-Gov* da ONU

De acordo com *United Nations* (2014), classificada com o índice de 0,8895, a Holanda passou a ocupar a 5ª posição no *ranking* de governo eletrônico, caindo 3 posições em relação ao de 2012.

Em relação aos serviços *on-line* oferecidos pelo governo, ocupa a 9ª posição no ranking da ONU de 2014 com o índice de 0,9291, mesmo assim é classificado como o 2º país europeu com maior índice de serviços *online*, ficando somente atrás da França.

7.1.4 Principais Políticas (Leis, atos, decretos, etc)

Segundo *European Comission* (2014f), algumas importantes leis foram publicadas com relação ao governo eletrônico, destacando-se as seguintes.

• **31/out/1991:** Legislação sobre o acesso público de informações do governo, modificada em 2005.

• **04/jun/1994:** Lei que estabelece as normas gerais do direito administrativo, com modificação em 2004 na seção sobre o tráfego eletrônico administrativo.

• **01/set/2000:** Legislação sobre proteção de dados pessoais.

• **08/mai/2003:** Legislação sobre assinatura digital.

• **mai/2004:** Lei de comércio eletrônico, implementando a diretriz de *eCommerce* da União Europeia (2000/31/EC).

• **19/mai/2004:** Lei de Telecomunicações, estabelecendo as 5 diretrizes reguladoras para o *framework* de comunicação eletrônica, a qual inclui diretrizes de privacidade e autorização.

• **21/jul/2007:** Lei sobre as disposições gerais de a atribuição, gestão e utilização do número de serviço do cidadão (BSN)

• **27/nov/2008:** Lei de publicação eletrônica, que estabelece a obrigação em disponibilizar de forma *on-line* os documentos oficiais, incluindo diretrizes de privacidade e autorização.

• **21/jun/2011:** Emenda à Lei de Telecomunicações estabelecendo acesso gratuito à Internet.

7.1.5 Cronologia do Desenvolvimento de *e-Gov* e GId

• **Out/1999:** nasce o BSN, também referenciado como CSN (Número de Serviço do Cidadão), como identificador único atribuído a todo cidadão registrado ao nascer.

• **1998:** é iniciado o programa de ações em governo eletrônico da Holanda.

• **Dez/2002:** é iniciado o Programa B4 (Governo Melhor para Cidadãos e Empresas), com o objetivo de resolver problemas sociais, reduzir a burocracia e diminuir os gastos públicos.

• **Jan/2005:** o Serviço de Identificação Digital (DigiD) é lançado, provendo ao cidadão uma solução centralizada de autenticação para acesso aos serviços de *e-Gov*,

baseada em um ID único de usuário.

• **Out/2008:** governo holandês cria mecanismo para permitir a publicação de leis e decisões apenas por meio eletrônico, dispensando a publicação em papel. Autoridades públicas, ministros, empresas e outras organizações passaram a se beneficiar desta nova ferramenta.

• **Jan/2011:** disponibilizado sistema *eRecognition* (lançado em 2010), o qual se constitui de uma infraestrutura de identidade eletrônica para empresas. Esta solução nasceu com a intenção de ser usada para comunicações eletrônicas entre empresas e o governo (B2G), bem como para comunicações entre empresas (B2B).

• **Nov/2013:** contabilizada 100 milhões de transações efetuadas com o DigiD, um crescimento de 33% em relação ao ano de 2012.

• **Dez/2013:** o Ministro da Economia e o Ministro do Interior e das Relações do Reino, anunciam o plano de lançamento do ”eID System” para 2015, que permitirá que as empresas e o governo possam oferecer um meio seguro e confiável de acesso aos serviços eletrônicos. A ideia consiste na utilização de uma identificação eletrônica única para que as pessoas acessem tanto serviços públicos quanto privados, unificando os já existentes sistemas DigiD e o eRecognition em uma única plataforma.

7.2 Modelo de Organização de Documentos Civis

7.2.1 Registro Civil

Dia 1 de outubro de 1994 foi lançado o BSN (número de identificação do cidadão), um identificador único atribuído a todo cidadão holandês nascido a partir desta data. Esta identificação única é gravada na certidão de nascimento e sucessivamente nos demais documentos emitidos para o cidadão, por exemplo, a carteira de motorista, o cartão de identificação e o passaporte.

O governo permite que cidadãos nascidos anteriormente à implantação do sistema façam o cadastro do seu número de identificação de cidadão de forma voluntária, ao contrário das pessoas nascidas após outubro de 1994, para as quais o BSN é obrigatório. Para os cidadãos que não possuem um número BSN o governo considera o número de segurança social e o número fiscal (SoFi Number) como identificadores. Uma vez aderido ao sistema de identificação, automaticamente outros identificadores são substituídos e vinculados ao número BSN, mantendo assim todo o

histório fiscal do cidadão holandes (Govenment of the Netherlands, 2014e).

7.2.2 Identidade Civil

Segundo o *Govenment of the Netherlands* (2014b), os seguintes documentos de identidade são válidos na Holanda.

• Passaporte holandês.

• Passaporte pertencente à União Europeia.

• Documento de viagem de um estrangeiro, desde que emitido por uma autoridade holandesa.

• Carteira de motorista.

7.2.3 Biometria no Sistema de Identidade Civil

Ao solicitar um passaporte holandês ou um documento de identidade, uma das exigências é a coleta das impressões digitais, com excessão das crianças menores de 12 anos que estão isentas. O documento de viagem contém uma imagem da impressão digital a fim de prevenir o roubo de identidade (Govenment of the Netherlands, 2014g).

7.3 Identidade Eletrônica

7.3.1 Uso da Identidade Eletrônica

É permitido o uso de uma identidade eletrônica única, através do uso de um pseudônimo como *login*. Ao cadastrar a identidade eletrônica no portal DigiD[99], o cidadão deve fornecer o BSN (Número de Serviço do Cidadão) como pré-requisito para conseguir sua credencial. O sistema permite a criação de uma segunda credencial, desde que a primeira tenha sido bloqueada ou invalidada (Govenment of the Netherlands, 2014i).

7.3.2 Cadastro da Identidade Eletrônica

O cadastro da identidade eletrônica é feito de forma centralizada no sistema DigiD[100], desenvolvido pelo governo holandês. Para se cadastrar o cidadão deve escolher um usuário e senha, em seguida um código de ativação é enviado ao

[99] https://digid.nl/aanvragen
[100] https://www.digid.nl/en/

endereço residencial, desde que este endereço tenha sido previamente cadastrado na autoridade municipal local (Govenment of the Netherlands, 2014a).

Para os cidadãos holandeses que residem fora do país o governo lançou um serviço de teste do Digid em maio de 2013, de forma a permitir a estes cidadãos o acesso aos sistemas de *e-Gov* de onde estiverem (Govenment of the Netherlands, 2014c).

A identificação eletrônica DigiD expira em 3 anos, se não utilizada pelo cidadão. Porém, um único acesso a qualquer serviço de *e-Gov* é o suficiente para validar as credenciais por mais 3 anos. O sistema automaticamente emite um alerta ao usuário 7 dias antes da credencial expirar (Govenment of the Netherlands, 2014a).

7.3.3 Atributos da Identidade Eletrônica

Ao realizar o cadastro no sistema DigiD[101], o usuário deve informar o número de serviço do cidadão (BSN), a data de nascimento e endereço completo.

Cidadãos que moram fora do país, ao comparecer ao consulado participante do programa de teste, além de fornecer o número BSN devem ter um documento de viagem válido e um número de celular. O processo de ativação da identidade eletrônica é feito no próprio local uma vez que o ”código de ativação” é gerado na mesma hora (Govenment of the Netherlands, 2014c).

A relação que existe entre a eID e o documento de identidade civil é feita através do número de serviço do cidadão, sendo o BSN a chave primária que liga todos os documentos de identificação do cidadão holandês.

7.3.4 Biometria

Um projeto de lei enviado à Câmara dos Deputados em 5 de março de 2012 prevê a criação de um banco de dados biométrico para realizar a coleta de impressões digitais e fotografias digitais, porém somente para residentes estrangeiros (Govenment of the Netherlands, 2014j). A coleta de impressões digitais não está prevista no atual sistema de criação da identidade eletrônica.

[101] https://digid.nl/aanvragen

7.3.5 Uso de Certificado Digital na Identidade Eletrônica

No futuro será implantado o nível alto de segurança através da adoção de um cartão de identidade eletrônica com uso de *chip* (Govenment of the Netherlands, 2014d). Como este nível de segurança ainda não foi implantado, não é citada nenhuma relação entre o uso de certificados digitais e o eID Card do cidadão.

7.3.6 Obrigatoriedade da Identidade Eletrônica

O governo não exige a criação de uma identidade eletrônica, deixando a critério do cidadão a possibilidade de fazer ou não o cadastro. No entanto, todo o acesso aos sistemas de *e-Gov* exigem a utilização de uma eID válida, conforme especificado no termo de uso do DigiD (Govenment of the Netherlands, 2014i).

Mesmo não exigindo a adesão do cidadão, segundo a *European Comission* (2014f), cerca de 9,8 milhões de cidadãos holandeses ativaram sua conta DigiD até 2013, o que representa cerca de 60% da população do país.

7.4 Sistemas de Gestão de Identidades

7.4.1 Padrão Adotado de Identidade Eletrônica (eID)

Segundo OECD (2007), o governo verifica a identidade dos usuários a partir de um único usuário e senha, criados a partir do sistema de autorização da identidade digital holandesa (DigiD). Quando o cidadão cadastra seu eID ele recebe um código de ativação em sua casa, sendo este procedimento o suficiente para garantir a segurança completa em transações com o governo.

7.4.2 Modelo de Gestão de Identidades

O modelo de gestão de identidades adotado na Holanda segue o modelo centralizado, sendo o DigiD o único sistema de autenticação homologado e mantido pelo governo, não sendo permitido às agências participantes desenvolverem seus próprios sistemas de autenticação (OECD, 2007).

7.4.3 Tecnologias de Gestão de Identidades

Em janeiro de 2006 o Ministério Holandês do Interior e das Relações com o Reino criou a organização GBO, que passou a ser conhecida em 2010 pelo nome

LOGIUS[102]. Esta organização foi criada com o objetivo de fornecer soluções relacionadas aos ambiente de tecnologia da informação e comunicação (TIC) para o governo eletrônico holandês, ditando padrões para o intercâmbio de dados e para a segurança da informação (Govenment of the Netherlands, 2014f).

Um dos serviços oferecidos pelo LOGIUS é o DigiD, o qual foi construído tendo como base a especificação SAML 2.0 (Govenment of the Netherlands, 2013).

7.4.4 Provedores de Identidade Privados

A estratégia nacional de eID prevê o uso do DigiD como único provedor de identidades (IdP) para os serviços de *e-Gov*. No entanto, é permitido o uso do DigiD por provedores de serviço privados (SPs), desde que ofereçam serviços de governo eletrônico. No portal principal do DigiD[103] é disponibilizada uma relação completa de SPs que oferecem desde serviços de fundo de pensão e consultoria até serviços relacionados à polícia e seguradoras de saúde.

7.4.5 Padrões de Interoperabilidade

Existe uma preocupação do governo com a interoperabilidade entre os provedores de serviço e o IdP (DigiD), para tanto o Logius publicou um documento para ser seguido pelos desenvolvedores dos SPd, de forma a garantir esta comunicação contínua e segura. O *Govenment of the Netherlands* (2013) constitui como uma espécie de guia de desenvolvimento, o qual supõe conhecimentos prévios do desenvolvedor em SAML 2.0, estando este documento disponível de forma gratuita no portal do Logius.

7.4.6 Gestão de Confiança

Toda gestão do modelo de confiança do governo holandês é feito pela organização LOGIUS. Ela é responsável por ditar os padrões de interoperabilidade para os provedores de serviço, e mantém um roteiro de homologação para SPs que desejam utilizar o DigiD. Após desenvolver a aplicação seguindo os manuais disponíveis, a aplicação é submetida a um ambiente de teste onde várias “listas de verificação” são utilizadas para determinar a maturidade do *software*. Desta forma,

[102] https://www.logius.nl/diensten/
[103] https://www.digid.nl/nl/over-digid/wie-doen-mee/

garante-se que soluções homologadas atendam em 100% os requisitos determinados pelo governo (Govenment of the Netherlands, 2014h).

7.4.7 Níveis de Garantia dos Provedores de Identidades

O DigiD é o único provedor de identidades homologado pelo governo, portanto não existem parâmetros de comparação para determinar o nível de garantia.

7.4.8 Mecanismos ou Técnicas de Autenticação

Para o uso da identidade eletrônica é exigido do usuário apenas um usuário e senha, sendo considerado este nível de segurança como básico. Caso deseje, o cidadão pode ativar a opção de validação de acesso por SMS, passando para o nível médio (Govenment of the Netherlands, 2014d).

7.5 Privacidade relacionada à Identidade Eletrônica

7.5.1 Uso de Pseudônimos

Segundo o *site* do projeto DigiD, o governo aconselha o uso de um usuário e senha que sejam igualmente difíceis de serem vinculados ao usuário (Govenment of the Netherlands, 2014i). O uso de um pseudônimo é altamente recomendado por questões de segurança. A única forma de identificar o usuário é através de seu número BSN, o qual é utilizado para cadastro e também utilizado como atributo na comunicação entre IdP e SPs.

7.5.2 Poder de escolha do Cidadão (eID e provedores de identidades)

O usuário não tem a opção de um segundo provedor de identidades, uma vez que o governo mantém apenas um único IdP (DigiD) homologado. O cidadão tem a liberdade em fazer o cadastro neste IdP de forma voluntária, e uma vez que tenha feito a adesão tem a obrigação em comunicar possíveis fraudes ou roubo de informações, sendo responsável pela sua credencial de acesso.

7.5.3 Controle de Liberação de Dados Pessoais

Segundo o *European Comission* (2014f), a única informação que é enviada do IdP ao SP é o número de cadastro de cidadão (BSN). Legalmente este número é o único permitido para troca de informações entre sistemas, de forma a não expor

diretamente o cidadão e evitar acessos fraudulentos aos serviços públicos.

7.5.4 Leis Específicas de Privacidade

As regras mais importantes para utilização de dados pessoais foram estabelecidas na Lei WBP (Lei de Proteção aos Dados Pessoais) aprovada por unanimidade em 23 de novembro de 1999, entrando em vigor no dia primeiro de setembro de 2001.

8 ITÁLIA

8.1 Perfil Sociopolítico, Econômico e Governo Eletrônico

8.1.1 Estrutura Sociopolítica

Localizada ao sul do continente europeu e contendo algumas ilhas em seu território, com destaque para as duas maiores Sicília e Sardenha, a Itália tem uma área total pouco superior a 301 mil km², fazendo fronteira com França, Áustria, Eslovênia, Suíça, San Marino e Cidade do Vaticano. Em 2013 possuía uma população de quase 61 milhões de habitantes, com densidade demográfica na ordem de 201,7 habitantes por km². Além da capital Roma, outras três cidades possuem mais de um milhão de habitantes: Milão, Nápoles e Turim. Entre as cidades mais importantes do país encontram-se Gênova, Veneza, Florença e Bolonha. O índice de desenvolvimento humano (IDH) da Itália é considerado muito alto (0,872) e a renda *per capita* nominal é da ordem de US$ 35.511,00, sendo considerada em 2010 a oitava maior economia do mundo e a quarta maior da Europa[104]. É membro fundador do G8, da Zona Euro e da OCDE.

A Itália é uma República Parlamentarista, tendo como chefes de Estado o Presidente e Primeiro Ministro, sendo dividida em 110 províncias (*province*) e 8.100 municipalidades (*comuni*). Ao todo são 20 regiões, a saber.

• Cinco regiões possuem um estatuto especial (Friuli-Venezia Giulia, Sardenha, Sicília, Trentino-Alto Ádige, e Vale de Aosta), o que lhes garante mais ampla autonomia para legislar sobre diversas matérias independentes do governo central. Estas cinco regiões são autônomas por fatores culturais, linguísticos e geográficos.

[104] Considerando a renda per capita nominal

Cada região tem um conselho (*consiglio regionale*) eleito e uma junta (*giunta regionale*) comandada por um Presidente.

• As outras quinze regiões possuem um estatuto ordinário e foram estabelecidas nos anos 1970. Após a reforma da constituição de 2001, as competências legislativas das regiões de estatuto ordinário foram ampliadas e os controles estatais foram significativamente reduzidos, como é o caso do comissário do governo central.

8.1.2 Acesso à Internet

De acordo com *European Comission* (2014e), em relação aos índices de acesso à Internet em 2013, as seguintes estatísticas da Itália são apresentadas.

• Casas com acesso à Internet: 69%.
• Empresas com acesso à Internet: 97%.
• Casas com acesso por banda larga: 56%.
• Empresas com acesso por banda larga: 93%.
• Indivíduos que fizeram compras pela Internet (últimos 3 meses): 14%.
• Empresas que receberam pedidos de compras *on-line* (último ano): 8%.

Em relação ao número de usuários de Internet, a Itália ocupa a décima sexta posição mundial e possui uma taxa de penetração de 59.92% (percentagem da polução com Internet)[105], contando em 2014 com mais de 36 milhões de usuários com acesso à Internet. Em relação ao índice de infraestrutura em telecomunicações (ITT) (United Nations, 2014), a pontuação da Itália (0,6747) é praticamente igual a média europeia (0,6678). Este índice foi obtido a partir dos seguintes componentes (United Nations, 2014)

• Telefone fixo (cada 100 habitantes): 35,57.
• Telefone celular (cada 100 habitantes): 159,69.
• Conexão à Internet Banda Larga (cada 100 habitantes): 22,15.
• Conexão à Internet *Wireless* (cada 100 habitantes): 52,15.

O relatório da ONU de 2014 apresenta a Europa com média de 77% em relação

[105] Fonte: http://www.internetlivestats.com/internet-users-by-country/

as casas com acesso à Internet e as Américas com 61%. Esta estatística demonstra que a Itália, apesar de estar com média superior ao continente americano, ainda está a baixo da média Europeia (United Nations, 2014).

8.1.3 *Ranking* de *e-Gov* da ONU

De acordo com *United Nations* (2014), classificada com o índice de desenvolvimento de *e-Gov* de 0,7593, a Itália passou a ocupar a 23ª posição no *ranking* de governo eletrônico em 2014, subindo nove posições em comparação ao de 2012. Em relação ao índice de eParticipação da ONU, a Itália está entre os 50 melhores países (19ª posição). O índice de desenvolvimento em *e-Gov* apresentou as seguintes informações.

- Serviços *On-line*: 0,7480 (média na Europa é de 0,5695).
- Infraestrutura em Telecomunicações: 0,6747 (média na Europa é de 0,6678).
- Capital Humano: 0,8552 (média na Europa é de 0,8434).

8.1.4 Principais Políticas (Leis, atos, decretos, etc)

As principais políticas italianas relacionadas ao desenvolvimento do *e-Gov* e gestão de identidades são as seguintes.

Abr/2002: uma lei (*DPR - Presidential Decree 101/2002*) introduz a possibilidade de um novo procedimento eletrônico para compras públicas. Essa lei também introduz a possibilidade de implementar uma nova ferramenta para compras dentro dos limites da comunidade Européia, o *eMarketplace* (*mercato elettronico*).

2004: com relação ao NSC[106] (*National Service Card*), as fontes mais importantes para a concretização deste cartão são o Decreto nº 117 do Presidente da República de 02/03/2004, e o decreto de 09/12/2004 assinado pelos Ministros das Relações Internas, da Inovação e Tecnologia e das Finanças.

Jan/2004: entra em vigor o ”Código de Proteção dos Dados”, em substituição a Lei de Proteção dos Dados nº 675 de 1996.

Fev/2004: o *Council of Ministers* institui um decreto para a introdução do cartão nacional de serviços (CNS), um *smartcard* para acessar serviços de governo eletrônico.

[106] Em italiano, CNS: *Carta Nazionale dei Servizi*

Mar/2004: divulgado um decreto que garante o mesmo valor legal para cartas registradas e *e-mails* registrados.

Dez/2009: o Decreto nº 177/2009 estabelece a ”DigitPA”, uma nova agência para a Tecnologia da Informação e Comunicação (ICT) na administração pública italiana. A DigitPA substitui o Centro Nacional Italiano para ICT na Administração Pública (CNIPA).

Mai/2010: entra em vigor, em 19 de maio 2010, o decreto do passaporte italiano unificado, baseado na ”*European Union's relative Council Regulation* (EC) nº 2252/2004”. Desta forma, os passaportes emitidos a partir do final junho de 2010 naquele país deveriam conter a imagem digital do rosto do portador, assinatura manuscrita, bem como duas digitais armazenadas em um *microchip*. Os passaportes para crianças menores de 14 deveriam incluir os dados de seus pais.

Set/2011: com a implementação do Decreto lei 150/2009 em 09/2011, se tornou compulsório que os médicos do sistema nacional de saúde (NHS) encaminhem atestados médicos ao Instituto Nacional para Seguridade Social (INPS) via *web*.

Out/2012: aprovado o Decreto de Crescimento *”Growth Decree”*, constituindo outro pacote de medidas urgentes para inovação e crescimento: agenda digital e *”start-ups”*. Pontos principais do decreto, a saber.

- Infraestrutura e serviços digitais.
- Criação de novas empresas de inovação (*start-up companies*).
- Desenvolvimento de instrumentos fiscais para facilitar a implementação de projetos de infraestrutura com capital privado.
- Atração de investimentos estrangeiros.

8.1.5 Cronologia do Desenvolvimento de *e-Gov* e GId

A seguir, destacam-se alguns marcos importantes para o desenvolvimento de *e-Gov* na Itália bem como a implantação da estratégia nacional de gestão de identidades.

1993: criada a Autoridade para Tecnologia da Informação - AIPA.

1995: primeira publicação da política da ”Sociedade da Informação da Itália”. Uma agenda para o desenvolvimento da sociedade da informação, que deveria seguir

os princípios estabelecidos por mecanismos internacionais, como a União Européia e G7.

1997: o fórum da Sociedade da Informação apresenta o documento "Promovendo o Desenvolvimento da Sociedade da Informação: um esquema de referência", que identifica o uso da Tecnologia da Informação e Comunicação nos serviços públicos como prioridade.

2000: este ano é marcado pela aprovação do "Plano de Ação para a Sociedade da Informação" e pela adoção do "Plano de Ação em Governo eletrônico 2000-2002".

Fev/2001: o novo governo indica o Ministro da Inovação e Tecnologia, o qual ganha mais autonomia política e assume a responsabilidade sobre as políticas eletrônicas *ePolicies* do país. Neste mesmo ano o Ministro da Inovação e Tecnologia publica o "Guia 2002 para a Digitalização da Administração Pública", colocando o governo eletrônico como prioridade.

Fev/2002: o Comitê Ministerial para a Sociedade da Informação aprova as diretrizes de 2002 para a digitalização da Administração Pública e endossa 10 objetivos estratégicos de governo eletrônico para serem atingidos até o fim daquela legislatura (2006).

Jun/2002: o portal de *e-Gov* nacional "Italia.gov.it" é divulgado.

Dez/2002: lançado o guia de 2003 para a digitalização da Administração Pública, contendo as prioridades operacionais para aquele ano.

Jun/2003: publicação de relatório recomendando o aumento do uso de "*Software* de Código Aberto" na administração pública.

Jul/2003: a autoridade para T.I. na Administração Pública (AIPA) é substituida por uma nova estrutura, a Agência Nacional Italiana para Administração Digital (CNIPA), responsável pela implementação de planos de *e-Gov* divisados pelo Ministério de Inovação e Tecnologias.

Dez/2003: publicado o guia de 2004 para a digitalização da administração pública, contendo as prioridades operacionais para aquele ano.

Jan/2004: entra em vigor a diretiva ”Transparência Administrativa e Gerenciamento do Fluxo de Documentos”, conhecida como *IT Protocol*, prevendo o gerenciamento e armazenagem de todos os documentos do governo eletronicamente.

Fev/2004: introdução do Cartão Nacional de Serviços (CNS).

Jan/2005: divulgado o guia de 2005 para a digitalização da Administração Pública, contendo as prioridades operacionais para o ano.

Mar/2005: lançado o portal de negocios ”www.impresa.gov.it”.

Dez/2005: divulgado o guia de 2006 para a digitalização da Administração Públicaa, contendo as prioridades operacionais para aquele ano.

Jan/2006: entra em vigência o código de governo eletrônico, contendo regras, obrigações, recomendações e objetivos para criar uma estrutura clara para o desenvolvimento do *e-Gov* nacional.

Abr/2006: entra em vigência o código *Public Procurement Code* com leilões *on-line*, sistema dinâmico de compras, catálogos *on-line*, entre outros.

Jan/2007: o Ministro da Inovação e Reforma, Luigi Nicolais, apresenta o documento “Em direção ao sistema nacional de *eGov*: linhas estratégicas”. No mesmo mês, o órgão italiano de padronização (UNI) publica o padrão nacional “UNI CEI ISO/IEC 26300:2007”, com adoção do Formato de Documento Aberto (ODF).

Fev/2007: o Ministro da Inovação e Reforma assina uma diretiva para a troca de dados entre as entidades públicas, conhecida como *Innovation Directive*. Esta diretiva objetiva dar forte impulso para a informatização dos órgãos públicos e reforçar o código de *e-Gov* que entrou em vigor em 1 janeiro de 2006.

Jun/2007: a cidade de Pavia lança um portal que oferece informações e permite pagamento *on-line* de várias taxas e impostos.

Jul/2007: o uso do *eMarketplace of the Public Administration* (MEPA) no portal de eProcuração *“Acquisti in Rete”* se torna obrigatório para todos os órgãos da

administração pública central ao comprarem produtos e serviços abaixo do valor de 137.000.

Set/2007: o estado Italiano, junto com autoridades locais, adota uma série de medidas para estimular serviços de *e-Gov* a níveis nacional e regional.

Dez/2007: entra em operação "Sistema de Cooperação e Conectividade Pública" (SPC), a nova rede da Administração Pública. Esta rede de banda larga agrupa as administrações públicas centrais, bem como centenas de órgãos públicos italianos pelo mundo.

Jan/2008: como parte de uma nova lei dirigida para melhorar o fluxo de trabalhadores na Itália não pertencentes à Comunidade Europeia, o Ministério de Assuntos Interiores lança um serviço *on-line* que visa checar o *status* da solicitação para empregar trabalhadores de fora da comunidade.

Fev/2008: o Ministério da Reforma e Inovação lança uma consulta *on-line* para que os italianos possam expor suas ideias e propostas de forma a simplificar procedimentos burocráticos.

Mai/2008: a Câmara de Comércio italiana lança um novo portal. O portal traz seus principais bancos de dados para a versão online.

Nov/2008: o Ministério da Administração Pública e Inovação divulga o Plano Estratégico do Governo para Inovação, o qual inclui 60 iniciativas estruturadas em torno das necessidades concretas de ambos governos: locais e central.

Jan/2009: o Primeiro Ministro juntamente com o Ministro da Administração Pública e Inovação apresentam oficialmente o "*eGovernment Plan* 2012". Este plano promove inovação governamental, ampliando serviços *on-line* e reforçando a acessibilidade e transparência da administração pública, de forma a aproximá-la das necessidades dos cidadãos e empresas. O plano consiste em 80 projetos de inovação digital. Cidadãos podem monitorar de forma *on-line* o progresso/status de cada um destes projetos.

Mai/2009: *"Magellano"*, a plataforma de gerenciamento de conhecimento da Administração Pública italiana se torna *on-line*, facilitando o trabalho e colaboração entre autoridades públicas através de um único ponto de acesso ao *expertise* da

Administração Pública Central.

Jun/2009: os cidadãos das províncias de Grosseto e Potenza, ao requisitarem passaporte, passam a receber passaportes biométricos contendo as digitais de ambos os dedos indicadores.

Jun/2009: *"Reti Amiche"*, um projeto que tem a colaboração da administração pública e do setor privado para entregar serviços públicos em ambientes privados (por exemplo bancos), sem custos adicionais para o Estado, começa a ser testado na rede entre cartórios e municipalidades.

Jul/2009: o Ministro da Administração Pública e Inovação e o Reitor da Universidade de L'Aquila assinam um memorando de entendimento para o projeto "Universidade Digital". O memorando é parte do protocolo "Escola e Universidade" pertencente ao plano de *e-Gov* 2012 (*Sector 2-target University*), no qual todas as universidades italianas teriam serviços avançados para alunos, professores e administrativo, desde cobertura completa de Wi-Fi a serviço VoIP em todos os locais, até 2012.

Nov/2009: o Ministro da Administração Pública e Inovação divulga a diretiva nº 8/2009, na qual racionaliza e reduz os *websites* públicos, prevendo o uso do domínio "gov.it".

Fev/2010: aprovada a nova versão do código de governo eletrônico de acordo com o "*e-Gov Plan* 2012".

Abr/2010: anunciado o serviço gratuito *"Posta Elettronica Certificata al Cittadino"*, que oferece aos cidadãos italianos contas de *e-mail* certificadas para comunicação com a Administração Pública.

Mai/2010: passa a operar de modo *on-line* o *The Italian Competence Centre on Open Source*, um consórcio nacional sem fins lucrativos para *software open source* com aplicações em inteligência de negócio (BI), objetivando ajudar o desenvolvimento e adoção de *software open source* na Administração Pública italiana.

Mai/2010: nova versão do portal "Italia.gov.it" é apresentada como uma ferramenta de busca do *eGov*, contendo uma lista de portais públicos.

Mar/2011: novos procedimentos são adotados para o processamento de

dados pessoais contidos em documentos administrativos, mantidos por Administrações Públicas a serem publicados na *web*.

Abr/2011: o Ministro da Administração Pública e Inovação apresenta um novo portal para os cidadãos, possibilitando acesso aos serviços da Administração Pública através de uma única "porta virtual", com serviços rápidos e fáceis de usar.

Nov/2011: o Ministro da Administração Pública e Inovação apresenta a operação "*Open Government, open data and App*". Essa iniciativa é a evolução natural para *web* 2.0 do trabalho que o governo começou 3,5 anos antes. Um novo portal é criado "www.dati.gov.it".

Fev/2012: a província de Savona mostra seu novo *website*, reconstruído com o sistema gerenciador de conteúdo *open source* Drupal[107]. Já em 2007 a província tinha anunciado a migração para a suíte *open source* de escritório *OpenOffice*, listando a migração dos 350 computadores da administração.

Jan/2013: é lançado o novo portal da cidade de Roma, "Roma Digital" (*Rome Digital*), permitindo aos cidadãos encontrarem e acessarem todos os serviços da capital. O portal inclui mais de 50.000 tipos de informação relacionados a transporte, registro municipal, *sites* das instituições, eventos, calendários, entre outros. Também contém informações e notícias para turistas: museus, bibliotecas, localização de prefeituras, departamentos, escolas, áreas de compras e pontos turísticos. O portal está acessível para qualquer dispositivo (*smartphone, tablet, laptop*) através de 700 pontos públicos de acesso *Wi-Fi* em 170 locais pela cidade. A infraestrutura de rede *Wi-Fi* citada, oferece também acesso livre à Internet para pessoas temporariamente em Roma.

Fev/2014: documentos entre as municipalidades, relacionados a assuntos de situação eleitoral e civil, certidões de registro da população e acordos de casamento, devem ser trocados exclusivamente por meios eletrônicos. Estes novos procedimentos foram postos em prática em um decreto proposto pelo Ministro do Interior e co-

[107] http://www.drupal.org

assinado pelo Ministro da Administração Pública. Este decreto implementa as regras dispostas pelo decreto de lei *"Semplifica Italia"*, em acordo com o "Código de Administração Digital" (*Codice dell'Amministrazione Digitale* - CAD), exigindo que o envio dos documentos acima mencionados possam ocorrer somente por inscrições (requerimentos) colaborativos ou por meio do "Correio Eletrônico Certificado".

Mar/2014: a *"Agency for Digital Italy"* lança a agenda nacional para dar mais ênfase na informação pública em 2014. A agenda foi enviada ao Primeiro Ministro para aprovação e subsequente publicação, de acordo com o Código de Administração Digital (artigo 52, parágrafo 6). Comparada com 2013, a agenda teria duração de um ano e daria mais destaque aos dados do governo, contemplando ações relacionadas ao banco de dados de interesse nacional, à utilidade de dados dentro da Administração Pública e ao aumento do interesse em dados abertos (*open data*).

8.2 Modelo de Organização de Documentos Civis

8.2.1 Registro Civil

O registro de nascimento é emitido de forma descentralizada pelo Departamento de Registro de Estado Civil das municipalidades. Obrigatoriamente, cada recém-nascido deve ser registrado na municipalidade onde se verificou o parto ou na cidade de residência dos pais[108] pelo prazo de até 10 dias. Até o 3º dia é permitido que o registro seja feito no hospital ou na instituição de saúde que se realizou o parto. Neste caso, a declaração de nascimento[109] é encaminhada pelo próprio médico ao secretário (oficial escrivão) da municipalidade (Wolters Kluwer Italia e RCS MediaGroup, 2015).

Conforme disposto em lei e de acordo com cada caso previsto, as seguintes pessoas podem encaminhar o registro de nascimento:

- os pais ou um deles;
- um oficial de justiça;
- uma pessoa que tenha sido delegada;
- o médico ;
- uma pessoa que tenha testemunhado o nascimento.

[108] Com prioridade a municipalidade de residência da mãe, caso os pais residam em locais diferentes
[109] A declaração de nascimento deve conter as informações da mãe (pessoais e endereço de residência), nome do hospital, casa de saúde ou qualquer outro local onde ocorreu o nascimento, o dia e hora de nascimento e sexo da criança.

Ao fazer fazer o registro, o secretário da municipalidade deve indicar uma série de atos ou fatos posteriores ao nascimento, conhecidos por anotações. A lei enumera estas anotações em detalhes, sendo as principais as seguintes.

- Comunicações relacionadas com a tutela e proteção.
- Juízos de interdição ou incapacidade.
- Atos que comprovem a existência do casamento, seja religioso ou civil.
- Documentos declarando a nulidade, a dissolução ou extinção dos efeitos civis do matrimônio.
- Atos e medidas para a aquisição, perda, abandono ou reaquisição de cidadania italiana.
- Decisões que declaram ou isentam a filiação.
- Medidas que determinam a alteração ou modificação do nome e sobrenome.
- Os atos de morte.

A emissão dos certificados e extratos de Estado Civil é feita pelo oficial escrivão designado pela municipalidade, sendo ele obrigado a emitir estes documentos para qualquer pessoa que os solicite, com excessão dos casos em que a lei proíbe o acesso, como certidões de nascimento de adotados (Wolters Kluwer Italia e RCS MediaGroup, 2015). Por outro lado, a estratégia nacional de eServiço visa reduzir o uso de certificados entre cidadãos e governo, possibilitando aos cidadãos usarem declarações emitidas por eles mesmos (*autocertificazione*) em substituição às declarações oficiais (European Comission, 2014e).

8.2.2 Identidade Civil

O documento de identidade civil, também conhecido por cartão de identidade, foi introduzido na Itália pelo decreto Real de 18 de Junho de 1931, nº 773[110]. De acordo com o Artigo 3 deste decreto, o prefeito de cada municipalidade tem o dever de emitir documentos de identidade para todos os cidadãos a partir dos 15 anos, se eles o requisitarem (pois este documento não é obrigatório). Um outro Decreto (6 maio 1949, no. 635), declarou no Artigo 288 que o documento de identidade civil deve ser

[110] Disponível em http://www.italgiure.giustizia.it/nir/lexs/1931/lexs_86198.html

considerado um “documento de identificação para a polícia”. Portanto, a principal função do cartão de identidade na Itália é a identificação do portador quando solicitado por lei (European Communities, 2009f).

O documento de identidade civil era emitido somente em papel até o ano de 2005, através do seguinte fluxo de emissão (Enrico Nardelli, 2014)

1. Cidadãos maiores de 15 anos preenchiam e enviavam requerimento do Cartão de Identidade ao prefeito da municipalidade de residência.
2. O prefeito emitia o documento, de acordo com as regras e procedimentos para impressões seguras.
3. O prefeito informava a polícia local (*Questura*) sobre a emissão do documento para fins de controle da própria polícia. Este informe era feito através de envio de um cartão contendo os dados pessoais e fotos do cidadão, adicionados das impressões digitais coletadas voluntariamente.
4. O prefeito informava o Ministério do Interior Local (*Prefettura*), o qual mantinha registro dos números de série dos cartões de identidade entregues às Municipalidades.

Gradativamente a partir de janeiro de 2006, o documento em papel passou a ser substituído pelo cartão de identificação eletrônico, conhecido por EIC[111] (*electronic identity card*). O EIC se constitui de um cartão de plástico ao estilo de cartões de crédito, agregando a funcionalidade de identificador eletrônico (se assim o cidadão solicitar) para acesso aos sistemas de governo eletrônico. Fisicamente, o cartão possui um *microchip* e impressões a laser (*laser band*) para proteção dos dados visíveis.

As principais informações impressas no documento de identidade civil, válidas também até certo ponto para o EIC, são as seguintes (European Communities, 2009f).

- Municipalidade emissora do documento.
- Número do cartão de identidade.
- Nome e sobrenome.
- Data e local de nascimento.
- Número da certidão de nascimento.
- Altura (cm), cor dos olhos e cabelo.

[111] Em italiano - CIE (*carta d’identità elettronica*)

• Algum sinal físico em particular, se houver.
• Foto.
• Endereço da residencia oficial.
• Data de emissão do documento.
• Data de vencimento do documento.
• Cidadania.
• Assinatura manuscrita.
• Indicação de validade do documento no exterior.
• Estado civil (informação opcional).
• Profissão (informação opcional).

Como recurso adicional, o EIC contém o chamado “Código Fiscal”, que é um código de identificação para fins de impostos e seguro social. Os dados do código do cidadão são armazenados no *microchip* e impressos no cartão na *laser band*. O “Código Fiscal” é unicamente atribuído pelo Ministério das Finanças não só para pessoas físicas, mas também para pessoas jurídicas e estrangeiros que precisem ser identificados para propósitos de impostos ou seguro social na Itália. O Ministério das Finanças também é responsável por manter e administrar o registro dos códigos fiscais. O “Código Fiscal” era originalmente um cartão plástico isolado, cujas funções foram incorporadas no cartão de saúde, no NSC (*National Service Card*) e no EIC (European Communities, 2009f).

Cada municipalidade mantém registro de seus residentes e emite cartões de identidade para os mesmos. Sempre que um cidadão solicita a emissão de um novo documento de identidade civil, sua identidade é consultada no registro da municipalidade onde o cidadão reside. A emissão do cartão de identidade em nome das municipalidade também é válida para o EIC. Até a introdução do EIC, não havia armazenamento central dos dados pessoais dos cidadãos. Com a adoção do EIC, um banco de dados central foi montado (INA-SAIA[112]),mas cada registro é criptografado com a chave pública da municipalidade emissora, de forma a preservar a privacidade dos cidadãos. Na prática isto significa que não houve nenhuma mudança real na forma que os dados dos cidadãos são usados (European Communities, 2009f).

[112] INA: *Indice Nazionale delle Anagrafi*. SAIA: *Sistema di Accesso e di Interscambio Anagrafico*.

8.2.3 Relação do Documento de Viagem com a Identidade Civil

Desde 2009 a Itália está gradualmente entrando na fase II da implementação da *European Union's Council Regulation* (EC) nº 2252/2004 de 13 de dezembro de 2004 com relação a "Padronização das características de segurança e biometria nos passaportes e documentos de viagem emitidos pelo Estado Membro". A versão atual do passaporte já contém a imagem facial e digitais do portador. As delegacias de polícia coletam as digitais contidas no documento e as armazenam de modo criptografado no seu microchip invisível. Uma vez que o passaporte é emitido, as digitais são excluídas do arquivo central e mantidas somente no passaporte eletrônico. O novo passaporte é considerado mais seguro com relação à falsificações. Ele se tornou uma ferramenta primária de identificação já que as digitais são únicas. As digitais são coletadas de todos os requerentes ao passaporte maiores de 12 anos. A apresentação dos formulários de solicitação e a entrega do passaporte são feitos nas delegacias de policia locais (European Comission, 2014e).

Segundo *European Comission* (2014e), o novo cartão de identidade (EIC) também pode ser utilizado como documento de viagem dentro da comunidade europeia.

8.2.4 Biometria no Sistema de Identidade Civil

A coleta dos dados biométricos dos cidadãos é feita de forma voluntária, e o dados são armazenados em papel para os documentos de identidades emitidos até janeiro de 2006. A partir desta data, apesar da coleta das impressões digitais continuar sendo feita de forma voluntária, o armazenamento passou a ser feito no *microchip* do cartão de identidade eletrônico (EIC), não sendo possível acessá-las de forma não eletrônica.

A Seção 3.4 tratará dos decretos e leis vigentes na Itália para coleta da impressão digital e uso no novo documento de identidade civil (EIC).

8.3 Identidade Eletrônica

8.3.1 Uso da Identidade Eletrônica

Na Itália os cidadãos podem acessar os serviços públicos *on-line* a partir de dois cartões: o EIC (*electronic identity card* ou CIE - *carta d'identità elettronica*) e o NSC (*National Service Card* ou CNS - *Carta Nazionale dei Servizi*). Conforme descrito na Seção 2.2, o EIC também foi criado para ser o substituto do documento de identificação civil, portanto a partir de sua criação, só é permitido ao cidadão italiano possuir uma única identidade eletrônica, uma vez que o governo permite a emissão de uma única identidade civil. O Artigo 64 código da Administração Digital[113] afirma que o EIC e o NSC são os instrumentos que garantem acesso aos serviços *on-line* oferecidos pelas autoridades públicas quando uma autenticação de usuário é requerida. O acesso a estes serviços pode acontecer também através de outras formas de identificação e autenticação do usuário em base local, mas o acesso pelo EIC deve sempre ser garantido em todo os país por todas as autoridades públicas que fornecem serviços *online*.

O projeto do cartão eletrônico italiano de identidade (EIC) foi lançado em 2001. Após duas fases de teste, o cartão começou a ser lançado pelo país e distribuído aos cidadãos maiores de 15 anos. O cartão eID italiano é um cartão híbrido inteligente que inclui as tecnologias *microchip*, memória ótica (*laser band*) e uma banda ICAO (*machine readable zone*), permitindo que o mesmo possa ser utilizado como documento de viagem. Todos os dados são escritos sem rótulos, o que permite um solução multilíngue onde necessário, por exemplo, nas fronteiras da Itália com França, Eslovênia e Alemanha.

No primeiro lado estão o nome da autoridade emissora do cartão, os dados pessoais do portador (sobrenome, nome, data e local de nascimento, foto e sexo), um número exclusivo de ID do cartão e a banda ICAO. No outro lado estão o endereço e código fiscal do portador, a data de validade do cartão e os dois dispositivos eletrônicos: *microchip* e o *laser band*. No *laser band* estão replicados, em um holograma integrado, os dados pessoais e imagens das digitais do cidadão (não obrigatório) bem como a assinatura holográfica (Mario Gentili, 2001). De acordo com a legislação de proteção de dados, estes dados não são mantidos em nenhum banco de dados central e podem apenas ser divulgados se o portador der sua permissão

[113] *Codice dell'Amministrazione Digitale* disponível em: http://archivio.pubblica.istruzione.it/istanzeonline/allegati/codice_amministrazione_digitale_opuscolo_cnipa_13ii.pdf

inserindo um código PIN. O molde das digitais do portador é armazenado no *microchip* e na memória ótica. O *microchip* possibilita a identificação *on-line* e habilita transações entre cidadãos e provedores, incluindo pagamentos eletrônicos (ePayments) (European Comission, 2014e).

Para habilitar o acesso dos cidadãos a serviços de *e-Gov* com segurança, antes mesmo da disseminação dos cartões de identidade eletrônicos (EIC), o governo italiano também desenvolveu o Cartão Nacional de Serviços (NSC). Ele é um cartão inteligente que permite a identificação *on-line* segura dos cidadãos, sendo usado também para assinar documentos eletrônicos a nível nacional e local devido a sua flexibilidade nos serviços de governo eletrônico (European Communities, 2009f). As principais diferenças do NSC em comparação ao EIC são as seguintes.

• O NSC não contém os elementos de segurança adicionais do EIC, tais como *laser band* e hologramas de segurança.

• O NSC não é aceito como documento de viagem ou como documento de identidade civil.

• O NSC não contém foto e não requer exigências de segurança especias para o suporte plástico.

• A emissão do NSC é feita por uma autoridade privada contratada pela DigitPA[114] e o EIC é emitido por uma autoridade pública.

O NSC foi criado com a única finalidade de prover o acesso aos sistema *on-line* de governo eletrônico. Embora criado antes da existência do cartão de identidade eletrônico (decreto em 2004), devido à correspondência existente entre o NSC e o EIC que garante a interoperabilidade entre as duas soluções, acredita-se que haverá a continuidades de oferta dos mesmos serviços *on-line* após a total adoção do EIC. Importante observar que os cidadãos que solicitarem um novo documento de identidade civil, receberão o cartão de identidade eletrônio (EIC), sendo a estes não mais permitida a obtenção do NSC.

8.3.2 Cadastro da Identidade Eletrônica

Sendo o EIC um documento utilizado tanto para identidade física quanto eletrônica, o cadastramento do cidadão é feito uma única vez, quando ele solicita o

[114] Nova agência de T.I.C italiana criada em 2009, a qual substituiu a CNIPA - *Italian National Centre for ICT in Public Administration*

referido documento à municipalidade (que é a esfera governamental responsável pelas emissões). Portanto, para a emissão do EIC somente é permitida a participação de órgãos públicos. A Seção 2.2 apresenta o fluxo de solicitação do cadastro em mais detalhes.

Por outro lado, com relação ao NSC, a emissão é feita por empresa privada contratada pela DigitPA.

8.3.3 Atributos da Identidade Eletrônica

De acordo com *European Communities* (2009f) , com relação às informações armazenadas no EIC, os seguintes atributos são adicionados ao cartão de identificação eletrônico.

1. Dados que permitem a identificação do portador.
2. O chamado “Código Fiscal”’, que é o código de identificação dos usuários para fins de impostos e seguro social.
3. O endereço do portador.
4. Local de residência.
5. A nacionalidade do portador.
6. A foto do portador.
7. A validade como documento de viagem no exterior.
8. A assinatura do portador.

Estes atributos são impressos no cartão e armazenados tanto no *microchip* quanto no *laser band*. O Artigo 66 do Código da Administração Digital elenca outros dados que podem ser armazenados no EIC, incluindo grupo sanguíneo e dados biométricos, fornecidos somente com o consentimento do portador.

As informações pessoais do portador (incluindo foto) são impressas no cartão e armazenadas no *laser band* e no *microchip*, com o uso de técnicas de criptografia (de forma a permitir a identificação *on-line* e *off-line* do portador). A razão para esta dupla abordagem tecnológica é que, enquanto o *laser band* oferece segurança, já que os dados não podem ser modificados quando houverem tentativas de falsificação, o *microchip* torna identificações *on-line* possíveis e permite transações entre cidadãos e provedores de serviço, armazenando certificados de assinatura digital.

8.3.4 Biometria

O Artigo 66 do Código da Administração Digital afirma que o EIC deve conter, se solicitado pelo portador, dados biométricos do mesmo, com exceção do DNA. As especificações são descritas através do decreto de 08/11/2007. O Artigo 13 deste decreto afirma que a municipalidade é quem obtém os dados biométricos da pessoa que estiver requerendo o EIC: dados biométricos significando foto e impressões digitais. Os moldes das impressões digitais devem ser armazenados no *microchip* do EIC (atualmente não obrigatório nem necessário). Os moldes são na verdade uma representação numérica de elemento biométrico (as digitais de dois dedos) e são usados com o fim de reconhecer a digital original, não sendo possível fazer a reconstrução das impressões digitais a partir destes moldes (European Communities, 2009f).

De acordo com a Lei 06/08/2008, nº 133, todos os leitores de cartões devem estar preparados para trabalhar com as impressões digitais do portador. Isto é necessário, pois os cartões de identidade (EICs) emitidos a partir de 01/01/2010 trazem consigo a possibilidade de armazenamento das impressões digitais do portador (European Communities, 2009f).

8.3.5 Uso de Certificado Digital na Identidade Eletrônica

O EIC é um cartão inteligente baseado em PKI que engloba dois certificados: um para autenticação e outro para assinatura digital. A infraestrutura PKI varia dependendo do projeto, sendo gerenciada por diferentes entidades, dependendo do cartão de identidade eletrônica utilizado. Para o EIC, o certificado pertence diretamente ao Ministério de Assuntos Interiores. Mas com relação à assinatura digital, o Ministério emite certificado apenas para funcionários públicos, os cidadãos, por outro lado, devem escolher um provedor de serviço de certificado na lista do DigitPA (antigo CNIPA) (European Communities, 2009f). Efeitos legais são válidos para documentos assinados digitalmente ou quando o usuário é reconhecido pelo sistema através de seu EIC (certificado de autenticação emitido pelo próprio Ministério) ou NSC (certificado de autenticação emitido por uma CSP italiana credenciada). Para assinar documentos digitalmente, uma assinatura digital se faz necessária, portanto as seguintes questões

devem ser consideradas.

1. O EIC e o NSC podem conter um certificado para assinatura digital.
2. Apenas certificados qualificados emitidos por autoridades certificadoras incluídas na lista oficial do DigitPA são considerados válidos pela lei.

Conforme citado por Gentili (2001) são utilizas chaves de 1024 bits e algorítimo 3-DES[115] para operações de assinatura eletrônica e autenticação de serviços *on-line*.

O procedimento de geração da chave é fundamental na criação do certificado. Este procedimento varia dependendo do esquema de emissão. No caso do EIC, o qual é personalizado e descentralizado nas municipalidades, a solicitação de geração do certificado no padrão PKCS#10[116] é enviada ao CNSD[117] para processamento. No caso do NSC, o qual é personalizado pela própria autoridade que emite o cartão, as seguintes informações são utilizadas para a geração do certificado: dados pessoais do portador (obtidos durante a fase de registro) e a chave pública gerada na fase de personalização (European Communities, 2009f). No caso do certificado gerado pelo Ministério do Interior para o cartão EIC, que é emitido no padrão ”X509 v3” (padrão para infraestrutura de chave pública - PKI), a estrutura é a seguinte.

Version	=	X509v3
Serial	=	Número de série do
Issuer	=	Emissor. Nome Distinto da
Start Date	=	Data da emissão
End Date	=	Data da emissão + 5 anos
Subject	=	Nome Distinto
Public Key	=	Chave pública RSA 1024 bit

Algumas extensões possíveis.

Key Usage	=	Não repúdio

[115] Especificação disponível em: https://tools.ietf.org/html/rfc1851
[116] Especificação disponível em: https://tools.ietf.org/html/rfc2986
[117] O *”Centro Nazionale dei Servizi Demografici”* é uma sub-divisão do Ministério do Interior

Extended Key	=	Autenticação de Cliente
CRL Distribution Point	=	CRL LDAP URL
Personal ID	=	*Hash* da Chave Pública
CA ID	=	Data da emissão + 5 anos

Adicionalmente uma estrutura para o nome distinto (*Distinguished Name*) pode ser utilizada.

Country	=	IT
Organisation	=	*Ministry of Internal the Interior*
Common Name	=	X509v3 + *hash* (dados pessoais)

A estrutura do certificado "EIC X509 v3" apresentada acima mostra que o certificado digital não identifica o portador do cartão EIC (o cidadão), mas o próprio EIC. Isto significa que o processo de identificação não consegue identificar o usuário, entretanto o EIC é reconhecido como um documento válido.

8.3.6 Obrigatoriedade da Identidade Eletrônica

Os primeiros cartões de identidade eletrônicos (EIC) tiveram distribuição limitada. O governo então tomou decisões para "impor" o cartão a partir de 01/01/2006, visando substituir os cartões de identidade de emitidos em papel pelo EIC a partir daquela data. Portanto, quando um cidadão requere um novo cartão de identidade ou a renovação do documento, apenas cartões eletrônicos (teoricamente) são emitidos, em conformidade com a Lei nº 43 de 31/03/2005[118]. Porém, esta medida de "impor" a adoção não foi totalmente respeitada na prática, de forma que muitos cartões de identidade de papel foram emitidos por vários meses após 01/01/2006.

De acordo com o Ministério de Assuntos do Interior, nem todos as municipalidades emitem os EIC uma vez que muitos investimentos localizados foram feitos para a implantação do NSC (European Communities, 2009f). A adoção da identidade eletrônica (EIC ou NSC) é feita de forma voluntária, de acordo com a necessidade de acesso aos sistemas de governo eletrônico ou em casos de renovação da identidade civil.

[118] Disponível em http://www.camera.it/parlam/leggi/05043l.htm

8.4 Sistemas de Gestão de Identidades

8.4.1 Padrão Adotado de Identidade Eletrônica (eID)

Fisicamente o EIC é um cartão “híbrido” feito de policarbonato, que de acordo o Artigo 7 do Decreto 8 de 08/11/2007, é construído respeitando as normas técnicas ISO/IEC 7816-1, 7816-2 e ISO/ID-001. Por seguir estas recomendações técnicas, ele é aceito por outros países da União Europeia (European Communities, 2009f). Segundo *European Communities*, (2009f) o EIC apresenta outras características, a saber.

• Esquema para o circuito de emissão do EIC, Roma, 22 de dezembro de 1999.

• Processo de autenticação *online*, Roma, 22 de Dezembro de 1999.

• Grupo de trabalho do EIC, AIPA (agora CNIPA)/associações de fornecedores.

• Projeto do CNSD, Roma, dezembro de 2002, Ministério de Assuntos do Interior/Universidade de Rome Tor Vergata.

• ISO/IEC 9594-8:2001 para o formato dos certificados digitais, extensões e políticas.

• ISO/IEC 10118-3:1998 para a função *hash* SHA-1.

• ISO/IEC 11694-1-2-3-4 Anexo A e Anexo B para *laser band*.

• ISO/IEC 7816-1-2-3-4-5-6-7-8-9 para o cartão inteligente.

• PKCS11 para interface com cartões inteligentes.

• Anexo Técnico do Acordo de 13 maio de 2003 entre o governo e fabricantes de *microchips*.

• Comitê técnico de restrito do EIC, trabalhos sobre o *microchip*, 21de abril de 2006.

• ICAO, documento 9303, parte 3.

• *Council* da União Europeia, “A” item note 15000/05, *Hague Programme*.

• EU *Regulation* 2252/2004.

8.4.2 Modelo de Gestão de Identidades

De acordo com DigitPA (2011), a Itália adota o modelo de gestão de identidades federado para o EIC, no qual cada municipalidade é responsável por armazenar os atributos dos cidadãos, para os quais é emitido um documento de

identidade civil/eletrônico.

Com relação aos serviços fornecidos pelas autoridades públicas, estes podem ser divididos em dois grupos descritos a seguir (European Communities, 2009f).

1. Serviços locais: são organizados e fornecidos com autonomia total pelas autoridades locais. Toda vez que o SP local quiser acessar os atributos do cidadão, obrigatoriamente haverá a participação do munícipio. Se atributos delicados (que firam a privacidade do cidadão) forem solicitados, o portador do cartão EIC deverá consentir com a liberação das informações.
2. Serviços Nacionais: frenquentemente requerem acesso aos atributos do cidadão, portanto sempre haverá a participação das municipalidades nas interações. Nenhuma autoridade pública da administração central, por exemplo, o Ministério de Assuntos do Interior tem permissão de acessar diretamente os atributos do cidadão, participar do processo de autenticação ou rastrear as atividade do usuário.

8.4.3 Tecnologias de Gestão de Identidades

O modelo de gestão de identidades da Itália, apoiado no uso do EIC, é inspirado nas normas amplamente adotadas como o SAML versão 2 (SAML-Core, SAML-Techov) e WS-Security, contando também com a experiência tecnológica de nações estrangeiras [E-auth_USGov]. Todo o esforço que as regiões estão fazendo em prol da gestão de identidades federadas está documentado na “força tarefa INF-3” do projeto ICAR[119] (DigitPA, 2011).

8.4.4 Provedores de Identidade Privados

No atual modelo de gestão de identidades federado, não é permitida a participação de provedores de identidade privados para o uso do EIC. Toda gestão de identidades eletrônicas é provida pela esfera pública, sendo o DigitPA o órgão responsável (European Communities, 2009f).

8.4.5 Padrões de Interoperabilidade

No modelo adotado pela Itália de gestão de identidades federadas, no qual a

[119] Disponível na página 88 do documento: http://archivio.cnipa.gov.it/site/_files/cnipa_minig_16_ok_b.pdf

administração do EIC é feita de forma descentralizada nas municipalidades, a interoperabilidade pode ser analisada em duas perspectivas diferentes: interoperabilidade interna e internacional (ou externa) (European Communities, 2009f).

A interoperabilidade em nível internacional segue o padrão europeu, de forma que se consiga a comunicação entre os sistemas da Itália com os da Comunidade Europeia. Entretanto, este modelo para o EIC não está muito desenvolvido. Basicamente, até o momento o EIC não é interoperável com sistemas de outros países (European Communities, 2009f).

Em nível interno, a abordagem feita permite interoperabilidade total com outros projetos de identificação eletrônica, por exemplo, o CNS. A padronização na confecção dos cartões de identidade eletrônica permite que diferentes fornecedores possam oferecer seus cartões à Administração Pública, de forma que, cartões de fornecedores diferentes possam coexistir no cenário de gestão de identidades da Itália (European Communities, 2009f). Tecnicamente, com relação a autenticação, as regras promulgadas pelo Ministério de Assuntos do Interior afirmam que a estrutura do certificado de autenticação do EIC deve possuir as seguintes características (European Communities, 2009f).

• O “Código Fiscal” do portador deve ser inserido no campo “*Common Name of the Subject* (DN)”. Este campo é público para garantir a interoperabilidade com o NSC.

• O código de identificação do *microchip*, separado do Código Fiscal através dos caracteres “...” (ponto, ASCII 0x2E) é inserido no campo “*Common Name of the Subject*” (DN).

• O identificador do cartão (*ID Carta*) é criptografado com a chave emitida e gerenciada pelo Ministério de Assuntos do Interior (base 64) e é inserido no campo DNQ (dnQualifier) do “Subject” (DN).

• O campo “*emailAddress*” do atributo X509v3 “*Issuer Alternative Name*” é preenchido com o endereço “support@backbone.cnsd.interno.it”.

• O valor do *hash*, calculado a partir dos dados pessois (base 64), é iserido no campo “serialNumber” do “Subject” (DN).

8.4.6 Níveis de Garantia dos Provedores de Identidades

O modelo de gestão de identidades para o EIC, apesar de federado, é baseado puramente em uma solução governamental, tendo no DigitPA o principal responsável pela gestão dos provedores de identidade (municipais). Sendo assim, todo controle de níveis de garantia é mantido pelo governo, não sendo liberadas as informações publicamente.

8.4.7 Mecanismos ou Técnicas de Autenticação

O processo de autenticação com a utilização do EIC é feito com o protocolo SSLv3 e o mecanismo desafio/resposta (Mario Gentili, 2001).

O uso do protocolo SSLv3 permite uma conexão segura entre o servidor *web* do provedor de serviços, o EIC e o provedor de identidades. O SP oferece funções de *software* para ler o certificado EIC e conferir os dados pessoais do usuário. Após extrair os dados pessoais do "*microchip*", o aplicativo calcula a função "*hash*" e liga o resultado com as informações "*Common Name*" do certificado. O protocolo SSL tem a vantagem de usar o EIC com um navegador de Internet sem a necessidade de instalação de "*softwares* adicionais".

A autenticação "desafio/resposta" é baseada na assinatura (resposta) de um desafio (*random string*) gerada pelo SP e enviada ao cliente. O SP verifica a resposta usando a chave pública do EIC contida no certificado digital e liga o resultado com o desafio original. Este mecanismo simples tem a desvantagem de não ter memória, portanto para comunicações sem conexão, ele deve ser repetido cada vez que for necessário verificar a identidade do portador do cartão. O *software* usado para a implementação desafio/resposta pode ser fornecido com um *Plug-in applet* ou *ActiveX*. Para permitir uma solução *open market* usando PKI para o componente do mecanismo desafio/resposta, o formato da resposta deve ser assinado no padrão PKCS#7.

8.5 Privacidade relacionada a Identidade Eletrônica

8.5.1 Uso de Pseudônimos

Conforme demonstrado na Seção 3.5, o cidadão tem garantido seu direto à privacidade com relação à identificação, uma vez que o certificado digital não identifica o portador do cartão EIC, mas o próprio EIC. Na prática isto significa que não é

necessário o uso de pseudônimos para garantir a privacidade do usuário.

8.5.2 Poder de escolha do Cidadão (eID e provedores de identidades)

Como já mencionado anteriormente, na Itália existem dois cartões de identidade eletrônica dignos de menção: EIC e NSC. Cada um desses sistemas tem alvos e objetivos específicos, no entanto muitas de suas funcionalidades são comuns entre si, sendo abaixo resumidas (European Communities, 2009f).

• EIC: basicamente disponível a todos os cidadãos. No entanto, não está muito claro quem está autorizado a obtê-lo. O cartão de identidade de papel tradicional é emitido para cidadãos e estrangeiros que residem na Itália, mas no caso do EIC, não se sabe ao certo se os estrangeiros residentes naquele país estão habilitados a tê-lo. Aparentemente existem práticas divergentes entre as municipalidades, de forma que, as autoridades de Padua emitem o EIC somente para cidadãos italianos[120], enquanto que em Bologna a administração local também emite o EIC para cidadãos estrangeiros se eles nasceram na Itália[121].

• NSC: criado com objetivo de ser disponibilizado de forma regional. Na Lombardia, por exemplo, todos os residentes são alvo do NSC.

Com relação à autenticação, o EIC visa servir tanto como identificação *on-line* quanto *off-line*. O NSC foi criado somente para autenticação *on-line* e não é um cartão de identidade válido. A razão para isto é que o NSC objetiva ser um instrumento ”temporário” antes que o EIC seja distribuído para toda a população. Em outras palavras, o desenvolvimento do plano de *e-Gov* requer a disponibilidade de uma autenticação *on-line* extensa em todo o país. Por esta razão, o processo de disseminação do EIC é ”ajudado” pela adoção do NSC. O NSC tem o objetivo de habilitar o uso dos serviços fornecidos pelo EIC, mesmo entre usuários que ainda não tenham o EIC [European Communities, 2009f]. O fato de algumas regiões, principalmente a Lombardia, terem investido muitos recursos financeiros e de capital humano na implementação e distribuição do NSC, não torna realista uma mudança

[120] Referência disponível em: http://www.padovanet.it/dettaglio.jsp?tassid=1529 id=6519
[121] Referência disponível em: http://urp.comune.bologna.it/WebCity/WebCity.nsf/5cf59f3096f4e560c125669f0058bcc2/5e38c30e967b905541256af1003116ba?OpenDocument

dramática do sistema de gestão de identidades em favor do EIC. Pode-se prever então que os dois modelos de identidade eletrônica irão coexistir por algum tempo, de forma que o acesso a muitos serviços seria possível com o uso de qualquer uma das duas soluções (European Communities, 2009f). Resumidamente, a adoção da identidade eletrônica é feita de forma voluntária e teoricamente haveria apenas a opção de utilização do EIC, mas na prática, dependendo da região, o cidadão tem apenas o NSC disponível como opção de eID.

8.5.3 Controle de Liberação de Dados Pessoais

A Seção 4.2 apresenta que ao usuário só é permitido consentir com o envio dos dados, caso estes venham a ferir as questões de privacidade citadas em lei. Caso contrário, todos os demais dados disponíveis no cartão de identidade eletrônica são passíveis de serem utilizadas pelos provedores de serviço.

8.5.4 Leis Específicas de Privacidade

Em 1º de janeiro de 2004 entra em vigor o “Código de Proteção dos Dados”, em substituição a Lei de Proteção dos Dados nº 675 de 1996. Este código complementa e consolida as questões de privacidade do país, introduzindo importantes inovações em conformidade com a “Diretriz de Proteção de Dados” nº 95/46/EC e com a “Diretriz sobre Privacidade e Comunicação Eletrônica” nº 2002/58/EC, ambas da comunidade europeia. A última alteração foi feita em 4 de novembro de 2010.

Basicamente, o código tem como objetivo fortalecer os direitos de proteção de dados dos indivíduos, permitindo-lhes exercer seus direitos e instigar processos com mais facilidade.

8.5.5 Aplicação da Lei de Privacidade

Como o cartão de identidade eletrônica principal da Itália, o EIC começou a ser emitido a partir de janeiro de 2006 e o código de proteção dos dados já estava vigente desde 2004, reconhece-se que havia amparo legal para a concepção de um modelo de gestão de identidades no momento da emissão do EIC. Na prática, este amparo legal é demonstrado através da implementação de mecanismos, como o criptográfico, como medidas adotadas pelo governo de forma a garantir que as diretrizes de privacidade

fossem efetivamente aplicadas neste modelo.

9 REINO UNIDO

9.1 Perfil Sociopolítico, Econômico e Governo Eletrônico

9.1.1 Estrutura Sociopolítica

O Reino Unido é uma união política entre Escócia, Inglaterra, Irlanda do Norte e País de Gales. Trata-se da mais antiga monarquia constitucional da Europa, tendo a rainha como chefe do estado. O governo é regido por um sistema parlamentar, sendo o poder legislativo dividido entre a Câmara dos Comuns e a Câmara dos Lordes. O poder executivo é comandado pelo primeiro ministro e geralmente se escolhe o líder do maior partido político dentro da Câmara dos Comuns para ocupar o cargo. Com uma recente e ampla reforma política, houve a descentralização do poder através do estabelecimento de um Parlamento e Executivo na Escócia, uma assembleia legislativa local no País de Gales e na Inglaterra houve uma descentralização do poder até o nível regional.

No censo realizado em 2013, constatou-se que o Reino Unido possuía 63.896.071 de habitantes e com uma densidade demográfica de 261 habitantes por km². Com um índice de desenvolvimento humano (IDH) de 0,892, o Reino Unido ocupa da 14ª posição mundial.

9.1.2 Acesso à Internet

De acordo com *European Comission* (2014h), em 2013 o Reino Unido possuía os seguintes índices de acesso à Internet.

- Casas com acesso à Internet: 88%.
- Casas com acesso à Internet via banda larga: 87%.
- Empresas com acesso à Internet: 96%.
- Empresas com acesso à Internet via banda larga: 95%.
- Indivíduos que fizeram compras pela Internet nos últimos 3 meses: 71%.
- Empresas que receberam pedidos de compras *on-line* no último ano: 19%.

9.1.3 *Ranking* de *e-Gov* da ONU

Desde 2001 a ONU vem fazendo um levantamento sobre o desenvolvimento do

serviço de governo eletrônico para os cidadãos dos seus países membros. A partir de 2008 começou a publicar relatórios bienais para ilustrar as estratégias de sucesso, práticas pioneiras visando a reforma administrativa e o desenvolvimento sustentável. Para tal criou um *framework* conceitual para o índice de desenvolvimento de governo eletrônico (*E-Government Development Index* – EGDI), que é composto por três subíndices: serviços *on-line*; infraestrutura de telecomunicações; e recursos humanos.

Em 2008 os países estavam investindo recursos na criação de portais *web* com o intuito de serem somente informativos, disponibilizando políticas, leis e outros arquivos. Em 2010 constatou-se a oferta de serviços mais avançados, melhor acesso a informação e uma melhor interação dos cidadãos com o governo.

Em 2012 notou-se que os governos começaram a investir em soluções para integrar com o setor privado, e até mesmo para integrar serviços de diferentes agências do próprio governo com o intuito de garantir a escalabilidade e sustentabilidade da solução. Em 2014 o relatório mostrou os países agrupados de acordo com seus índices EGDI, sendo que valores maiores que 0.75 indicam um índice muito alto, entre 0.5 e 0.75 um índice alto, entre 0.25 e 0.5 um índice médio e menor que 0.5 um índice baixo.

O Reino Unido em 2008 estava na 10ª posição, em 2010 na 4ª posição, em 2012 na 3ª posição e em 2014 caiu para a 8ª posição. Ao longo dos anos o Reino Unido veio investindo em iniciativas para reduzir os custos iniciais de implantação ao mesmo tempo que aumentava seus impactos para os cidadãos. Desde de 2012 que o Reino Unido adotou a estratégia de “Digital por padrão”, o que vem guiando as mudanças no serviços *on-line* para torná-los mais convenientes para seus cidadãos.

9.1.4 Principais Políticas (Leis, atos, decretos, etc)

Desde 1998 o governo do Reino Unido está publicando leis, atos e suas regulamentações para conseguir atender sua principal estratégia de *e-GOV* que é “Digital por padrão”. Abaixo, alguns dos principais atos e regulamentações organizados cronologicamente.

1998

-Ato sobre proteção de dados.

Define as regras impostas as organizações privadas e públicas sobre como lidar

com as informações pessoais, sejam estas em papel ou digitais.

2000

- Ato de liberdade de acesso à informação.

Objetiva garantir o acesso à informação mantida pelos órgãos do governo.

- Legislação sobre assinatura eletrônica.

Cria um *framework* para uso de assinaturas eletrônicas pelos setores público e privado.

- Ato sobre comunicação eletrônica.

Objetiva prover confiança na comunicação eletrônica por meio de um *framework* de comércio eletrônico entre os setores público e privado.

2002

- Regulamentações dos atos sobre assinatura eletrônica e comércio eletrônico.

2003

- Regulamentação sobre privacidade e outros elementos chave para o *framework* de Comunicação Eletrônica, o que inclui a diretiva de acesso, diretiva de autorização e a diretiva de serviço universal.

2006

- Regulamentação sobre contratos públicos voltada para permitir que o processos de procuração ocorram de forma eletrônica.

9.1.5 Cronologia do Desenvolvimento de *e-Gov* e GId

Dez/2000

É lançado o portal de serviços públicos ukonline.gov.uk, promovendo um ponto único de acesso aos serviços públicos *online*.

Nov/2002

Iniciada a “Estratégia Nacional para *e-Gov* Local”, a qual forneceu um *framework Municipal* voltado para permitir a interligação de serviços municipais a outros serviços

públicos.

Dez/2006

O Portal do governo “Direct.Gov.UK” inicia oferta de serviço para dispositivos móveis.

Out/2012

O portal “Gov.uk” surgiu para substituir todos os demais portais *web* do setor público até 2014, o que incluiu o “Direct.Gov.UK”, sendo este agora um ponto único para cidadãos terem acesso a serviços e informações do governo.

Dez/2012

Programa de garantia de identidade (IDAP) é um serviço para que cidadãos possam provar sua identidade quando forem interagir com serviços de *e-Gov*.

9.2 Modelo de Organização de Documentos Civis

9.2.1 Registro Civil

As certidões de nascimento são emitidas pelo escritório de registro local, sendo o registro feito de maneira *on-line*. O pedido de segunda via pode ser feito através do portal do governo Gov.UK. Existem regras distintas para Irlanda do Norte e Escócia.

9.2.2 Identidade Civil

A última vez que o Reino Unido emitiu carteiras de identidade civil de forma obrigatória para seus cidadãos foi durante a segunda guerra mundial. Após a guerra, a sociedade se mostrou contrária a ter um sistema de identificação com receio de ferir suas liberdades. Em 2006 o parlamento britânico publicou um ato criando a Carteira de Identidade Nacional, um documento de identidade civil que também servia como um documento de viagem para os demais países da comunidade Europeia.

A carteira de identidade nacional é um cartão plástico que contém uma foto, nome, data de nascimento, nacionalidade, situação sobre imigração. Um *chip* eletrônico armazena informações biométricas, como até 10 impressões digitais, registro da face e da iris.

Na eleição geral de 2010 uma nova coalizão política Conservador/Democrática Liberal anunciou a destruição do Registro Nacional de Identidade e invalidou todas as

carteiras de identidade emitidas. A organização Liberdade dos Direitos Humanos do Reino Unido se opôs às carteiras de identidade e o Registro Nacional de Identidade, devido a:

• não serem efetivas no combate a criminalidade e imigração ilegal, como o governo havia indicado;

• não serem justas, pois teriam aumentado a desigualdade entre cidadãos britânicos e imigrantes;

• serem caras, pois até novembro de 2008 estimasse que o governo britânico gastou 5 bilhões de libras esterlinas;

• serem intrusivas, pois guardam uma grande quantidade de informações pessoais dos cidadãos, as quais poderiam ser compartilhadas entre muitas agências do governo.

Atualmente carteiras de habilitação emitidas a partir de 1998 e passaportes (documentos de viagens) são os únicos aceitos como documentos de identificação no Reino Unido.

9.2.3 Relação do Documento de Viagem com a Identidade Civil

Até janeiro de 2011 a carteira de identidade nacional, criada pelo ato de 2006, era reconhecida como documento de viagem oficial em toda a comunidade europeia. Atualmente o somente o passaporte biométrico cumpre o papel de documento de viagem no Reino Unido.

9.3 Identidade Eletrônica

9.3.1 Uso da Identidade Eletrônica

A identidade eletrônica pode ser usada no portal de serviços de governo eletrônico. O governo do Reino Unido possui contrato com empresas para que atuem como provedores de identidades para seus cidadãos. Atualmente tem-se cinco provedores registrados: Digidentity, Experian, Mydex, the Post Office e Verizon, contudo espera-se ter mais no futuro. O cidadão tem a liberdade de escolher um ou mais destes provedores, bem como determinar se não quer mais usar um determinar

provedor de identidade.

Os motivos que levaram o governo a terceirizar o serviço de provimento de identidade foram:

• liberdade de escolha para o cidadão;

• não existência de uma base de identidade centralizada, desta forma cada provedor de identidade fica como responsável por garantir a privacidade de seus usuários e garante que cada serviço dos diferentes departamentos do governo só tenha acesso aos dados que realmente necessite;

• a não existência de ponto único de falha, pois não existe um único serviço que mantém todos os dados dos usuários;

• desenvolvimento do mercado interno, dando liberdade aos provedores de identidade para criar serviços que atendam as normas;

• fazer uso de toda tecnologia disponível, uma vez que empresas especializadas possuem a velocidade necessária para acompanhar as mudanças constantes na tecnologia e métodos para verificação de identidades.

9.3.2 Atributos da Identidade Eletrônica

O Reino Unido segue um modelo federado com diversos provedores de identidade mantidos por instituições privadas. As identidades eletrônicas digitais armazenam informações biográficas, contudo não existe uma carteira física. Os serviços de autenticação, providos por estes IdPs, são os responsáveis por garantir outras informações de uma pessoa através do cruzamento de dados com outras fontes de informação. Desta forma, os IdPs conseguem provar para os SPs interessados que uma pessoa é quem diz ser e também consegue prover outros atributos sobre esta pessoa.

9.3.3 Biometria

Desde janeiro de 2011 as carteiras de identidades físicas não são mais consideradas válidas, sendo assim no Reino Unido não existe mais o armazenamento de dados biométricos em documentos emitidos pelo governo para cidadãos Britânicos. Porém, a biometria é ainda armazenada nos cartões de autorização de residência no

Reino Unido para cidadãos de países que não fazem parte da União Europeia. Estes dados biométricos não ficam armazenados no Registro Nacional de Identidade.

9.3.4 Obrigatoriedade

A criação de uma identidade eletrônica não é obrigatória, tanto que o governo permite que o cidadão escolha seu provedor de identidade dentro os diversos provedores privados homologados.

9.4 Sistemas de Gestão de Identidades

9.4.1 Modelo de Gestão de Identidades

O Programa de Garantia de Identidade (*Identity Assurance Programme* – IDAP) faz parte do programa de Governo Digital do Reino Unido e visa o desenvolvimento de padrões para garantir a oferta de serviços de governo eletrônico. Foi escolhido o modelo federado de gestão de identidade e os provedores de identidades são empresas privadas, cabendo o governo atuar somente como provedor de serviços.

9.4.2 Tecnologias de Gestão de Identidades

O serviço concentrador para garantia de identidade (*Identity Assurance Hub Service*) possui dois perfis SAML: perfil de atributos e perfil SAML2.0. Estes perfis descrevem os metódos usados e as regras aplicadas para o processo de autenticação do ponto de vista dos provedores de identidade, provedores de serviços e serviços correlatos. Sendo assim, todos os serviços que fizerem uso do serviço concentrador para garantia de identidade devem seguir estas especificações SAML (Cabinet Office and Government Digital Service, 2012).

9.4.3 Níveis de Garantia dos Provedores de Identidades

Provedores de Identidade devem executar diversas verificações quando estiverem validando a identidade um usuário. A amplitude destas validações é determinada pelo nível de garantia exigido pelo provedor de serviço que o usuário deseja acessar, podendo ser LoA2 ou LoA3. Atualmente todos os provedores de serviços exigem a LoA2. Existe um guia de boas práticas (nº43) para os provedores de

identidade sobre os níveis de garantia, que leva em consideração: a amplitude de provas; a força das provas; os processos de validação e verificação realizada; e um histórico de atividade do usuário.

9.4.4 Leis Específicas de Privacidade

Em 1998 foi publicado o ato para proteção de dados pessoais. O ato lista regras obrigatórias para todas organizações (pública, privada, sem fins lucrativos, etc.) que mantém ou processam dados pessoais, estejam estes em papel ou em formato eletrônico. O ato apresenta 8 princípios que indicam como todos os dados devem ser: tratados de forma justa e lícita; obtidos e usados somente para um uso específico e legal; obter dados relevantes, adequados e não excessivos; devem ser precisos e quando necessários mantidos atualizados; manter somente o período que for necessário; processar de acordo com os direitos individuais; manter seguros; e somente transferir para países que possam garantir a proteção adequada.

10 Comparação e Análise dos Países

10.1 Perfil Sociopolítico e Econômico

O estudo do perfil sociopolítico e econômico dos países analisados apresenta questões relevantes no intuito de entender melhor as políticas de *e-Gov* adotadas. Nações que se preocuparam no passado com questões de ordem social, apresentando na atualidade altos índices de IDH, certamente poderão direcionar maiores investimentos financeiros para outras áreas da sociedade, melhorando, por exemplo, a infraestrutura de telecomunicações, investimentos estes que refletem diretamente nos índices de governo eletrônico do país.

A tabela 2 mostra os países europeus analisados, apresentando a similaridade entre eles com relação ao índice de desenvolvimento humano (IDH), bem como grandes diferenças em termos de quantidade populacional e territorial.

Tabela 2: Perfil Sociopolítico, Econômico

	Governo (regime)	Área mil km²	População milhões hab	Densidade hab/km²	IDH
Alemanha	República Federal Parlamentarista	357	81,7	229	0,911
Áustria	República Federal Parlamentarista	83,9	8,4	100	0,881
Dinamarca	Monarquia Constitucional	43	5,6	129	0,900
Espanha	Monarquia Constitucional / Democracia Parlamentarista	504	47,3	90	0,869
Estônia	República Parlamentarista	45	1,3	29	0,840
Holanda	Monarquia Constitucional	41,5	16,8	405,6	0,915
Itália	República Parlamentarista	301	60,3	200,12	0,872
Reino Unido	República Federal Parlamentarista	244,8	63,2	255,6	0,892

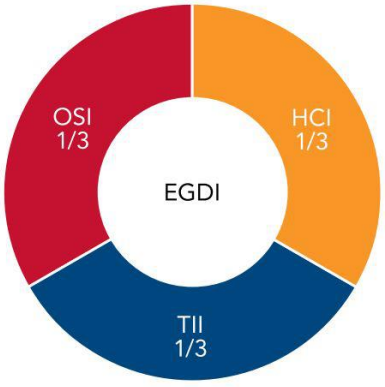
Este estudo apresentou características importantes com relação à administração política dos países. A Holanda, apresentando uma divisão em 12 regiões, cada qual administrada por um governador (vinculado ao Rei), se destaca como o país de maior índice de desenvolvimento de governo eletrônico. Por outro lado, a Alemanha com um dos menores índices de *e-Gov* entre as nações pesquisadas, demonstra grande preocupação com a questão de privacidade dos seus cidadãos, se destacando como o país europeu mais focado na criação de leis que garantam a liberdade e anonimato de seus cidadãos, quando o assunto é a interação eletrônica com o governo.

10.2 Governo Eletrônico

O Departamento de Assuntos Econômicos e Sociais da ONU realiza a cada dois anos uma pesquisa para identificar os pontos fortes, desafios e tendências sobre o desenvolvimento de governos eletrônicos dos 193 Estados membros (United Nations, 2014). Desta pesquisa é feita a pontuação de cada país, chegando-se ao Índice de Desenvolvimento de *e-Gov* (EGDI), no qual os países são apresentados em ordem de classificação. Este índice é gerado a partir de uma nota obtida de outros 3 índices, conforme segue abaixo e representado pela Figura 5.

- Índice de Serviços *Online* (OSI).
- Índice de Infraestrutura de Telecomunicações (TII).
- Índice de Capital Humano (HCI).

Figura 5: EGDI - Índice de Desenvolvimento de *e-Gov*



O cálculo do Índice de Serviços *Online* (OSI) leva em consideração diversos aspectos, entre eles os descritos abaixo.

1. Entrega Multicanal (*web*, *e-mail*, sms, media social, etc.).
2. Barreira Digital (acesso à Internet, linguagem acessível à população, etc.).
3. Aumento do uso dos sistemas.
4. Políticas de Governo Aberto.
5. Participação da população.

Para a confecção do Índice de Infraestrutura em Telecomunicações (TII), cinco pontos são analisados englobando basicamente o acesso à Internet e uso de telefonia móvel e fixa. O Índice de Capital Humano (HCI) é obtido, por exemplo, através da pontuação em renda *per capita*, média de idade dos cidadãos na escola e percentagem de adultos na escola.

Tabela 3: Governo Eletrônico

	Rank 2014	*Rank* 2012	EGDI	ePartic	Serviço *on-line*	Infra Teleco
Alemanha	21	17	0,7864	0,7059	0,6693	0,8038
Áustria	20	21	0,7912	0,6275	0,7480	0,7597
Dinamarca	16	4	0,8162	0,5490	0,6614	0,8740
Espanha	12	23	0,8410	0,7843	0,9449	0,6629
Estônia	15	20	0,8180	0,7647	0,7717	0,7934
Holanda	5	2	0,8897	1,0000	0,9291	0,8175
Itália	23	32	0,7593	0,7843	0,7480	0,6747
Reino Unido	8	3	0,8695	0,9608	0,8976	0,8574

A tabela 3 apresenta os índices de governo eletrônico EGDI, OSI e TII das nações pesquisadas, bem como o Índice de Participação dos cidadãos (*eParticipation*). Este último índice tem o propósito de mesurar o uso das ferramentas *on-line*, utilizadas para promover a interação entre cidadão e o governo.

10.3 Identidade Eletrônica

Com relação ao estudo da Identidade Eletrônica, algumas das características pesquisadas são apresentadas na Tabela 4, as quais são descritas abaixo.

1. **Id Único:** algumas nações optam por uma política de governo eletrônico dotada de diversas soluções (*eID Card*, *MobileId*, certificados digitais, etc.), sendo o cidadão identificado através de um identificador único por todos os provedores de serviços. Um exemplo desta política é ilustrada pelo governo da Estônica, onde um identificador (ID) composto por 11 caracteres identifica o usuário em todas as transações *on-line*. Por outro lado, na Áustria o ID é criptografado de forma que, para cada SP acessado pelo usuário, o identificador apresenta o caráter de exclusividade, significando que nenhum SP poderá rastrear as atividades do usuário. Na prática, esta característica se reflete como se existissem diversos identificadores (pseudônimos) para o mesmo usuário.

2. **Cadastro Obrigatório:** reflete a imposição do governo, no sentido de obrigar o cidadão a criar sua identidade eletrônica. Para a grande maioria dos países é obrigatório utilizar um eID para acesso aos SPs, no entanto, a adesão é voluntária, cabendo ao cidadão optar por criar esta identidade.

3. **Cadastro Centralizado:** algumas nações centralizam o cadastro da Identidade Eletrônica em apenas um órgão, seja público ou privado. Exemplificando, a Espanha centraliza a emissão do DNIe na Direção Geral da Polícia, enquanto no Reino Unido, o cidadão pode escolher entre diversos IdPs privados.

4. **Relação do Documento de Identidade Civil com o eID:** ao se criar o eID, alguns países obrigam o cidadão a fornecer ou apresentar um documento de identidade civil. Em outras nações, como é o caso da Itália, o EIC (*electronic identity card*), utilizado como documento de identidade civil, é o próprio cartão de identidade eletrônica utilizado nas interações com o governo. Nestes casos a relação é direta, ou seja, o Documento de Identidade Civil é utilizado ou constitui-se do próprio eID.

5. **Coleta Biométrica:** a biometria é representada como a coleta de impressões digitais, iris, face, olhos, entre outros. Algumas nações obrigam o cidadão a fornecer estes dados biométricos, como ocorre na Espanha, que obriga o cidadão a fornecer as impressões digitais no momento da criação do documento de identidade

civil, documento este também utilizado como eID.

6. **Uso de Certificados Digitais:** as políticas de governo eletrônico normalmente diferenciam os certificados digitais em Certificados de Autenticação e Assinatura Qualificada. Os primeiros são utilizados para acesso aos SPs e o segundo para assinar documentos. A Tabela 4 representa a recomendação ou obrigatoriedade em utilizar certificados para acesso aos provedores de serviço.

Tabela 4: Comparativo Identidade Eletrônica

	Id Único	Cadastro Obrigatório	Cadastro Centralizado	Rel. com Doc. Civil	Coleta Biometrica	Uso Certif. Digital
Alemanha	Não	Não	Não	Sim	Voluntária	Obrigatório
Áustria	Não	Não	Não	Sim	Não	Recomendad
Dinamarca	Não	Não	Não	Não	-	Obrigatório
Espanha	Sim	Não	Sim	Sim	Obrigatória	Obrigatório
Estônia	Sim	Não	Sim	Sim	Não	Obrigatório
Holanda	Sim	Não	Sim	Não	Não	Não
Itália	Não	Não	Não	Sim	Voluntária	Obrigatório
Reino Unido	Não	Não	Não	Não	Não	-

10.4 Sistemas de Gestão de Identidades

A adoção do modelo de Gestão de Identidades não segue um padrão propriamente dito. A pequisa realizada com os países europeus demonstra que, os fatores que levam um país preterir um modelo a outro depende de diversos fatores, entre eles podem ser citados os seguintes.

- Questões culturais.
- Existência de Leis.
- Investimentos financeiros e de pessoal qualificado.
- Regime político (democracia, monarquia, etc.).
- Autonomia das divisões políticas (regiões).
- Contratação de empresas privadas.
- Cobertura da infraestrutura de telecomunicações (Internet e Telefone).
- Confiança nos escritórios públicos locais.

Entretanto, quando confrontados os países, como é feito na Tabela 5, observa-se que para estas nações europeias duas características são marcantes, a saber.

1. Adoção de padrões consolidados e de código aberto.
2. Trabalho conjunto dos governos para criação de políticas e diretrizes comuns.

A primeira característica demonstra a preocupação dos governos em criar sistemas nos quais a robustez da solução e a interoperabilidade estejam presentes. Mesmo países que iniciaram soluções de identificação eletrônica, como a Espanha por exemplo, sem ter grandes preocupações no início com os padrões utilizados pelos provedores de serviço, aos poucos adotam o SAML como padrão de comunicação entre clientes, IdPs e SPs.

Com relação a segunda característica, o grande exemplo do trabalho comum destes países é a criação de diretrizes conjuntas como a Diretiva nº 1999/93/EC, que trata dos parâmetros para funcionamento do *Framework* Legal para Assinaturas Eletrônicas, ou a Diretiva nº 95/46/EU que estabelece regras de Proteção dos Dados Pessoais. Estas diretrizes de operação e boas práticas acabam refletindo a maneira com que a nação escreve suas próprias leis ou modela seus sistemas de informação.

Tabela 5: Comparativo SGId

	Modelo IdM	SAML	IdP	STORK 2.0
Alemanha	Federado e Centrado no Usuário	Sim	Privado	Não
Áustria	Centralizado	Sim	Governo	Membro
Dinamarca	Centralizado	Sim	Privado	Membro
Espanha	Federado	Sim	Gov/Priv	Membro
Estônia	Centralizado	-	Governo	Membro
Holanda	Centralizado	Sim	Governo	Membro
Itália	Federado e Centrado no Usuário	Sim	Gov/Priv	Membro
Reino Unido	Centralizado	Sim	Privado	Membro

Por fim, um trabalho que vem ganhando espaço e destaque na comunidade europeia é o “Projeto Stork” (*Secure identity across borders linKed*). Encontrando-se na

versão 2.0, é um projeto que visa facilitar a criação de um sistema único de identificação e autenticação eletrônica interoperável e sustentável para a Europa, para os cidadãos e para as empresas. A ideia desta iniciativa é garantir uma convergência de estratégias e soluções privadas e públicas, a nível nacional e comunitário, para um acesso seguro e facilitado a serviços transfronteiriços, recorrendo a credenciais de identificação.

10.5 Privacidade relacionada a Identidade Eletrônica

A criação de leis é uma das principais formas de garantir a privacidade dos cidadão. Um grande exemplo é dado pela Alemanha ao criar leis específicas de privacidade e incorporá-las nos sistemas de governo eletrônico do país. A aplicação destas leis é levada tão a sério que alguns provedores de serviço permitem o uso de pseudônimos, como forma de garantir o anonimato dos usuários.

A Tabela 6 demonstra que a criação de leis específicas de privacidade é uma preocupação de todos os países pesquisados, bem como a aplicação destas leis no sistemas de *e-Gov*.

Tabela 6: Privacidade

	Pseudônimo	Solução única eID	Escolha IdP	Leis Privacidade	Aplicação Lei Priv.
Alemanha	Si	Sim	Sim	Sim	Sim
Áustria	Si	Não	Não	Sim	Sim
Dinamarca	Si	Sim	Não	Sim	Sim
Espanha	Nã	Não	Sim	Sim	Sim
Estônia	Nã	Não	Não	Sim	-
Holanda	Si	Sim	Não	Sim	-
Itália	Nã	Não	Sim	Sim	Sim
Reino Unido	-	Não	Sim	Sim	

Outro aspecto que depende das políticas adotadas para cada nação é a possibilidade de escolha do IdP. Se por um lado o Reino Unido preferiu fazer uma licitação e contratar somente provedores de identidades privados, concedendo aos cidadãos poder de escolha, a Itália por outro lado procura promover o sistema de eID governamental como principal solução no país, muito embora exista uma segunda solução no país mantida por empresa privada.

A tabela 6 demonstra que a existência de diversas soluções, como uso simultâneo do MobileID e eiD Card por exemplo, é uma realidade em alguns países, como é o caso da Áustria. Escolher qual IdP o cidadão poderá utilizar para se autenticar também é uma característica que depende das políticas de governo adotada.

Como citado, cada país implementa as politicas que refletem melhor cada realidade local. Entretanto, criar leis de privacidade, adotar soluções de código aberto e melhorar a vida do cidadão com investimentos em governo eletrônico é uma realidade cada vez mais presente nos países europeus.

11 CONCLUSÃO

Por meio de um trabalho coordenado e interdependente entre as equipes da SE e da Universidade de Brasília, as atividades de elaboração deste RT foram planejadas, discutidas, executadas e documentadas.

O presente relatório teve como propósito analisar as características e estratégias nacionais de Gestão de Identidades de oito (8) países europeus: Alemanha, Áustria, Dinamarca, Espanha, Estônia, Holanda, Itália e Reino Unido. Esta análise foi feita com base nas vinte e oito (28) questões elencadas no Relatório 01, as quais estão subdivididas nas seguintes categorias.

1. Perfil Sociopolítico e Econômico e o Governo Eletrônico.
2. Modelo de Organização de Documentos Civis.
3. Identidade Eletrônica.
4. Sistemas de Gestão de eID.
5. Privacidade relacionada a Identidade Eletrônica.

É notória a preocupação dos países analisados com questões relacionadas à existência de Leis, Atos e Decretos, enfim, à existência de base jurídica relacionada ao tratamento de dados e privacidade, questões estas que se constituem de alicerce legal para o nascimento das soluções de T.I.C. voltadas aos sistemas de eIDM. Particularmente com relação ao Modelo de Gestão de Identidade adotado pelos países, este guarda estreita relação com a cultura da nação, ou seja, para um país extremamente preocupado com a privacidade como a Alemanha, os sistemas são desenvolvidos para garantir ao máximo o anonimato ou, no caso do Reino Unido, a população prefere confiar em Provedores de Identidade privados a confiar em um IdP governamental. De uma forma ou de outra, sempre está presente a parceria público privada quando se trata de governo eletrônico, seja simplesmente para confeccionar os cartões de identidade eletrônicos, seja na atuação como provedores de serviço, identidade ou de certificados digitais.

Os países em questão demonstram grande progresso no desenvolvimento de soluções voltadas à Gestão de Identidades para *e-Gov*, inclusive com tal maturidade que, em geral, a solução de governo eletrônico em uso já se encontra em sua segunda

ou terceira edição. Estudando o histórico dos países, observa-se que esta característica é marcante uma vez que sempre houve continuidade nos investimentos e ações acerca das soluções e padrões a serem seguidos. Mesmo em países que optaram por terceirizar parte dos serviços, os padrões de interoperabilidade sempre partem do governo. Exemplos desses padrões podem ser observados no Reino Unido com o Programa de Garantia de Identidade (*Identity Assurance Programme* – IDAP), ou na Alemanha com a publicação das Normas Técnicas pelo Departamento Federal de Segurança em Tecnologia da Informação (BSI), os quais ditam os requisitos a serem seguidos pelos elementos que compõe o cenário de Governo Eletrônico do país.

Resumidamente, conforme observado por essa pesquisa, a base para construção do governo eletrônico está no investimento continuado na capacitação de profissionais, infraestrutura de telecomunicação, criação e manutenção de leis, disponibilização de sistemas *on-line* e no uso de tecnologias e especificações consolidadas no mercado, como o SAML e ICAO por exemplo.

As atividades envolvidas nesta etapa observaram formalmente a execução dos passos da metodologia elencada para gestão do projeto, PMI/PMBoK. A equipe da UnB considera que teve acesso a todas as informações necessárias à boa condução dos trabalhos e que a disponibilização dessas informações pela equipe da SE, assim como as atividades conjuntas de análise e discussão, levou a etapa do projeto a bom termo.

12 Questões sobre Gestão de Identidade

Na **Categoria 1 (Perfil Sociopolítico e Econômico e o Governo Eletrônico)**, as seguintes questões de pesquisa serão investigadas no estudo de cada país.

1. Qual o perfil sociopolítico e econômico do país? Indique a população, o território, a densidade demográfica, o índice de desenvolvimento humano, o sistema político e s organização política administrativa.
2. Quais os índices de acesso à Internet do país?
3. Qual a posição no *rank* da ONU de desenvolvimento de *e-Gov* nos anos de 2012 e 2014 (EGDI)? Qual a posição do país no *rank* que avalia o grau de participação dos cidadãos nas aplicações de *e-Gov* e no *rank* de serviços on-line oferecidos pelo governo?
4. Quais as principais políticas (leis, atos, decretos, etc.) de *e-Gov* do país?
5. Qual a cronologia do desenvolvimento de *eGov* e GId do país?

Na **Categoria 2 (Modelo de Organização de Documentos Civis)**, as seguintes questões de pesquisa serão investigadas no estudo de cada país.

1. Como é feito o registro de nascimento, casamento e óbito pela nação? Este registro é feito de forma centralizada por uma única entidade credenciada? O registro é feito exclusivamente por órgãos do governo ou há a participação de entidades privadas? Este documento pode ser eletrônico?
2. Em relação ao sistema de identificação civil, há um documento de identidade civil *adhoc offline*? Quem o emite e como é realizado o processo de criação do documento de identidade civil (centralizado ou distribuído)? Este documento é obrigatório? Qual a relação do documento de identidade com outros documentos civis?
3. Existe alguma relação entre o documento de viagem e o documento civil?
4. Nos sistemas de identificação civil, é coletada algum tipo de biometria (p.ex impressões digitais)? Que tipo de dados biométricos são coletados? Como é feito o armazenamento destas informações (*smartcard*, banco de dados do governos e/ou em papel)?

Na **Categoria 3 (Identidade eletrônica)**, as seguintes questões de pesquisa

serão investigadas no estudo de cada país.

1. O cidadão pode ter mais de uma identidade eletrônica ou é permitido o uso de apenas uma única identidade eletrônica?
2. As políticas de *e-Gov* determinam que o cadastro seja feito de forma centralizada em uma única organização ou permite que o registro seja feito de forma descentralizada? Existe a participação de entidades privadas neste cadastro?
3. Quais informações são levadas em consideração para se criar a identidade eletrônica do cidadão? Existe alguma relação da eID com documentos de identidade civil?
4. Exite algum processo de coleta de dados biométricos dos cidadãos? Se sim, que tipo de dados biométricos são coletados e como é feita coleta? Como é feito o armazenamento destas informações (*smartcard*, banco de dados do governos e/ou em papel)?
5. A identidade eletrônica possui certificado digital? Se sim, é opcional ou obrigatório? O governo exige o uso de certificados digitais pelos seus cidadãos para o acesso de sistemas de *e-Gov*? Como é feita a gestão deste certificado digital pessoal?
6. O cidadão é obrigado a criar sua identidade eletrônica ou o governo permite a adesão voluntária?

Na **Categoria 4 (Sistemas de Gestão de eID)**, as seguintes questões de pesquisa serão investigadas no estudo de cada país.

1. Existe um padrão de eID no país ou existe uma busca por um padrão de eID que seja interoperável e usado por diversos países?
2. Qual modelo de gestão de eID é adotado no país e quais os motivos para esta escolha?
3. Quais tecnologias de GId são utilizadas na Estratégia Nacional de GId?
4. Provedores de Identidade privados podem atuar em conjunto com o governo para autenticar usuários de serviços *e-Gov*? Provedores de serviços privados podem fazer uso do SGId usado na Estratégia Nacional de eID?
5. Quais padrões de interoperabilidade são utilizados na Estratégia Nacional?
6. Qual o modelo de gestão de confiança (*Trust Framework*) adotado na Estratégia Nacional de GId?

7. Existem mecanismos legais e/ou especificações técnicas sobre o uso de níveis de garantia (LoA - *Level of Assurance*) para os provedores de identidade?

8. Quais mecanismos/técnicas de autenticação são utilizados no(s) provedore(s) de identidade(s)?

Na **Categoria 5 (Privacidade relacionada a Identidade Eletrônica)**, as seguintes questões de pesquisa serão investigadas no estudo de cada país.

1. O cidadão pode fazer uso de pseudônimos para acesso aos sistemas do governo? Quais são os dados que estão associados ao usuário? Como é formado o identificador (caso haja uma identidade nacional única)? De alguma forma o identificador pode identificar o cidadão?

2. O cidadão pode escolher qual identidade eletrônica ou provedor de identidade deseja usar?

3. Existe alguma forma de o cidadão poder controlar os dados pessoais que são encaminhados ao provedor de serviço (SP) - abordagem centrada no usuário? Existe alguma preocupação do SP ou do IdP em informar ao usuário qual informação pessoal está sendo enviada?

4. Existem leis específicas para proteção da privacidade?

5. Existem mecanismos nos SGId que aplicam a lei?

REFERÊNCIAS

[Allerød Kommune - Denmark, 2014] Allerød Kommune - Denmark (2014). Billedlegitimati- onskort. http://www.alleroed.dk/Borger/Familie_Born_Unge/Unge/Billedlegitimation.aspx .

[AS Sertifitseerimiskeskus, 2014a] AS Sertifitseerimiskeskus (2014a). Principles of Client Data Protection. https://www.sk.ee/en/about/data-protection/.

[AS Sertifitseerimiskeskus, 2014b] AS Sertifitseerimiskeskus (2014b). Validity confirmation services. https://sk.ee/en/services/validity-confirmation-services/.

[British Crown, 2002] British Crown (2002). Security Architecture of the Austrian Citizen Card Concept. IEEE Computer Society.

[Bundesamt für Sicherheit in der Informationstechnik, 2014a] Bundesamt für Sicherheit in der Informationstechnik (2014a). Der elektronische Reisepass - ePass. https://www.bsi. bund.de/DE/Themen/ElektronischeAusweise/ePass/epass_node.html.

[Bundesamt für Sicherheit in der Informationstechnik, 2014b] Bundesamt für Sicherheit in der Informationstechnik (2014b). Elektronische Ausweise. https://www.bsi.bund.de/DE/ Themen/ElektronischeAusweise/elektronischeausweise_node.html.

[Bundesamt für Sicherheit in der Informationstechnik, 2014c] Bundesamt für Sicherheit in der Informationstechnik (2014c). Sicheres Reisedokument. https://www.bsi.bund.de/ DE/Themen/ElektronischeAusweise/Personalausweis/Funktionen/Funktionen_node.html.

[Bundesdruckerei GmbH, 2014] Bundesdruckerei GmbH (2014). ID Card. https://www. bundesdruckerei.de/en/714-new-german-id-card.

[Bundesministerium der Justiz und für Verbraucherschutz, 2014] Bundesministerium der Justiz und für Verbraucherschutz (2014). Act on

Identity Cards and Electronic Identification. http://www.gesetze-im-internet.de/englisch_pauswg/englisch_pauswg.html.

[Bundesministerium des Innern, 2014a] Bundesministerium des Innern (2014a). Be- antragung. http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/ Der-Personalausweis/Beantragung/beantragung_node.html.

[Bundesministerium des Innern, 2014b] Bundesministerium des Innern (2014b). Berechti- gungszertifikate. http://www.personalausweisportal.de/DE/Wirtschaft/Technik/eID-Server/ eID-Server_node.html.

[Bundesministerium des Innern, 2014c] Bundesministerium des Innern (2014c). Chipkarten- Lesegeräte. http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/ Online-Ausweisen/Das-brauche-ich/Kartenlesegeraete/Kartenlesegeraete_node.html.

[Bundesministerium des Innern, 2014d] Bundesministerium des Innern (2014d). Der Personalausweis. http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/ Der-Personalausweis/der-personalausweis_node.html.

[Bundesministerium des Innern, 2014e] Bundesministerium des Innern (2014e). Gebüh- ren und Gültigkeit. http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/ Der-Personalausweis/Gebuehren/gebuehren_node.html.

[Bundesministerium des Innern, 2014f] Bundesministerium des Innern (2014f). Online-Ausweisen. http://www.personalausweisportal.de/DE/Wirtschaft/Technik/ Online-Ausweisen/Online-Ausweisen_node.html.

[Bundesministerium des Innern, 2014g] Bundesministerium des Innern (2014g). PIN, PUK und Sperrkennwort. http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/ Online-Ausweisen/Das-brauche-ich/Pin-Puk-Sperrkennwort/Pin-Puk-Sperrkennwort. html.

[Bundesministerium des Innern, 2014h] Bundesministerium des Innern (2014h). Sicherheit und Datenschutz. http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Sicherheit-und-Datenschutz/Sicherheit-und-Datenschutz-node.html.

[Bundesministerium des Innern, 2014i] Bundesministerium des Innern (2014i). Technik. http://www.personalausweisportal.de/DE/Wirtschaft/Technik/Technik_node.html.

[Bürgerkarte, 2014] Bürgerkarte (2014). The Austrian Citizen Card System. https://www. buergerkarte.at.

[Cabinet Office and Government Digital Service, 2012] Cabinet Office and Government Di- gital Service (2012). Identity assurance: delivering trusted transactions. https://www.gov. uk/government/collections/identity-assurance-enabling-trusted-transactions.

[Carol Geyer, 2008] Carol Geyer (2008). List of organizations using SAML. http://saml.xml. org/wiki/list-of-organizations-using-saml.

[CIA, 2014a] CIA, C. I. A. (2014a). The world factbook - europe:: Austria. [Online; acessado 07-Dezembro-2014].

[CIA, 2014b] CIA, C. I. A. (2014b). The world factbook - europe:: Germany. [Online; acessado 04-Dezembro-2014].

[de Estado de Administraciones Públicas, 2015] de Estado de Administraciones Públicas, S. (2015). Cl@ve: Identidad electrónica para las administraciones. Ministerio de Hacienda y Administraciones Públicas. http://administracionelectronica.gob.es/ctt/clave/infoadicional.

[de Justicia, 2015a] de Justicia, M. (2015a). Certificado/certificación de nacimiento. Ministe- rio de Justicia. http://goo.gl/BOQC4B.

[de Justicia, 2015b] de Justicia, M. (2015b). Inscripción de nacimiento. Ministerio de Justicia. http://goo.gl/Xodr2p.

[de la Policía, 2015a] de la Policía, D. G. (2015a). Dni electrónico. Ministerio del Interior. http://www.dnielectronico.es/.

[de la Policía, 2015b] de la Policía, D. G. (2015b). Pasaporte ordinario. Ministerio del Interior. http://www.policia.es/documentacion/docu_esp/pasaporte/clases_pas.html.

[de Madrid, 2012] de Madrid, A. (2012). Inscripción de nacimiento. Ayuntamiento de Madrid. http://goo.gl/fyFqKW.

[de Moneda y Timble, 2015] de Moneda y Timble, F. N. (2015). Ceres - certificación es- pañola. Fábrica Nacional de Moneda y Timble. http://www.cert.fnmt.es/.

[Die Beauftragte der Bundesregierung für Informationstechnik, 2014] Die Beauftragte der Bundesregierung für Informationstechnik (2014). Der neue Personalausweis. http://www.cio.bund.de/Web/DE/Innovative-Vorhaben/Neuer-Personalausweis/neuer_ personalausweis_node.html.

[DigitPA, 2011] DigitPA (2011). MODELLO DI GESTIONE FEDERATA DELLE IDENTITÀ DIGITALI (GFID). http://www.agid.gov.it/sites/default/files/documentazione/ spcoop-modellogfid_v1.5.1.pdf.

[E-Government Innovation Center Graz, Austria, 2011] E-Government Innovation Center Graz, Austria (2011). A Privacy-Preserving eID based Single Sign-On Solution. IEEE Computer Society.

[Enrico Nardelli, 2014] Enrico Nardelli (2014). The italian Electronic Identity Card: overall architecture and first phase of deployment. https://danishbiometrics.files.wordpress.com/ 2009/08/italian-eic-porvoo5-13may04.pdf.

[European Comission, 2014a] European Comission (2014a). eGovernment in the Austrian. eGovernment Factsheets.

[European Comission, 2014b] European Comission (2014b). eGovernment in the Denmark. eGovernment Factsheets.

[European Comission, 2014c] European Comission (2014c). eGovernment in the Estonia. eGovernment Factsheets.

[European Comission, 2014d] European Comission (2014d). eGovernment in the Germany. eGovernment Factsheets.

[European Comission, 2014e] European Comission (2014e). eGovernment in the Italy. eGo- vernment Factsheets.

[European Comission, 2014f] European Comission (2014f). eGovernment in the Nether- lands. eGovernment Factsheets.

[European Comission, 2014g] European Comission (2014g). eGovernment in the Spain. eGovernment Factsheets.

[European Comission, 2014h] European Comission (2014h). eGovernment in the U.K. eGo- vernment Factsheets.

[European Communities, 2009a] European Communities (2009a). eID Interoperability for PEGS: Update of Country Profiles study - Austrian country profile. IDABC European eGovernment Services.

[European Communities, 2009b] European Communities (2009b). eID Interoperability for PEGS: Update of Country Profiles study - Danish country profile. IDABC European eGovernment Services.

[European Communities, 2009c] European Communities (2009c). eID Interoperability for PEGS: Update of Country Profiles study - Estonian country profile. IDABC European eGovernment Services.

[European Communities, 2009d] European Communities (2009d). eID Interoperability for PEGS: Update of Country Profiles study - German country profile. IDABC European eGovernment Services.

[European Communities, 2009e] European Communities (2009e). eID Interoperability for PEGS: Update of Country Profiles study - Italian country profile. IDABC European eGo- vernment Services.

[European Communities, 2009f] European Communities (2009f). eID Interoperability for PEGS: Update of Country Profiles study - Spain country profile. IDABC European eGo- vernment Services.

[Federal Chancellery of Austria, 2015] Federal Chancellery of Austria (2015). Modules for
Online Applications. https://www.digitales.oesterreich.gv.at/site/6528/default.aspx.

[Federal Office for Information Security, 2015a] Federal Office for Information Security (2015a). Neue Software für den Online-Ausweis. https://www.ausweisapp.bund.de/ startseite/.

[Federal Office for Information Security, 2015b] Federal Office for Information Security (2015b). Security mechanisms in electronic ID documents. https://www.bsi.bund.de/EN/ Topics/ElectrIDDocuments/SecurityMechanisms/securPKI/securitymechanismsPKI .html.

[for Information Security, 2010] for Information Security, F. O. (2010). Innovations for an eid architecture in germany. Federal Office for Information Security. http://goo.gl/nAJhWa.

[for Information Security, 2014] for Information Security, F. O. (2014). Technical guideline eid-server - part 1: Functional specification. Federal Office for Information Security. http://goo.gl/4ayMaK.

[GENCS EU, 2012] GENCS EU (2012). Data Protection, Consent and Biometric Data in Estonia: requirements and categories. http://www.gencs.eu/news/view/793.

[Govenment of the Austria, 2014a] Govenment of the Austria (2014a). Allgemeines zum Identitätsausweis. https://www.help.gv.at/Portal.Node/hlpd/public/content/54/Seite.540600. html.

[Govenment of the Austria, 2014b] Govenment of the Austria (2014b). Reisepass – Min- derjährige unter 18 Jahren. https://www.help.gv.at/Portal.Node/hlpd/public/content/2/Seite. 020450.html.

[Govenment of the Austria, 2014c] Govenment of the Austria (2014c). Reisepass – Passpfli- cht, Einreisebestimmungen usw. https://www.help.gv.at/Portal.Node/hlpd/public/content/2/ Seite.020950.html.

[Govenment of the Estonia, 2003] Govenment of the Estonia (2003). The Estonian ID Card and Digital Signature Concept - Principles and Solutions. http://www.id.ee/public/The_ Estonian_ID_Card_and_Digital_Signature_Concept.pdf.

[Govenment of the Estonia, 2015] Govenment of the Estonia (2015). The Estonian ID. http: //www.id.ee/.

[Govenment of the Netherlands, 2013] Govenment of the Netherlands (2013). Koppelvlaks- pecificatie DigiD SAML - Authenticatie. https://www.logius.nl/fileadmin/logius/ns/diensten/ digid/koppelvlakspecificaties/Koppelvlakspecificatie_SAML_DigiD4_v3.0_definitief.pd

f.

[Govenment of the Netherlands, 2014a] Govenment of the Netherlands (2014a). About Di- giD. https://www.digid.nl/en/about-digid/.

[Govenment of the Netherlands, 2014b] Govenment of the Netherlands (2014b). Com- pulsory identification. http://www.government.nl/issues/identification-documents/ compulsory-identification.

[Govenment of the Netherlands, 2014c] Govenment of the Netherlands (2014c). DigiD - Security levels. https://www.digid.nl/en/about-digid/levels-of-authentication/.

[Govenment of the Netherlands, 2014d] Govenment of the Netherlands (2014d). DigiD for Dutch people living abroad. https://www.digid.nl/en/about-digid/digid-via-balieuitgifte/.

[Govenment of the Netherlands, 2014e] Govenment of the Netherlands (2014e). Identifica- tion documents - The Citizen Service Number (BSN). http://www.government.nl/issues/ identification-documents/the-citizen-service-number.

[Govenment of the Netherlands, 2014f] Govenment of the Netherlands (2014f). Logius. http: //www.logius.nl/english.

[Govenment of the Netherlands, 2014g] Govenment of the Netherlands (2014g). Pass- ports, identity cards and Dutch nationality certificates. http://www.government.nl/issues/ identification-documents/passports-identity-cards-and-dutch-nationality-certificates.

[Govenment of the Netherlands, 2014h] Govenment of the Netherlands (2014h). Stappen- plan aansluiten op DigiD. https://www.logius.nl/ondersteuning/digid/#c8438.

[Govenment of the Netherlands, 2014i] Govenment of the Netherlands (2014i). Terms and Conditions of Use DigiD. https://www.digid.nl/en/terms-and-conditions/.

[Govenment of the Netherlands, 2014j] Govenment of the Netherlands (2014j). Use of bio- metric data of foreign nationals. http://www.government.nl/issues/identification-documents/ use-of-biometric-data-of-foreign-nationals.

[Mario Gentili, 2001] Mario Gentili (2001). Italian Electronic Identity Card: principle

and architecture. http://www.dia.uniroma3.it/~vldbproc/072_629.pdf.

[Ministerio de la Presidencia, 2010] Ministerio de la Presidencia (2010). Real Decreto 4/2010. http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1331.pdf.

[Ministerio de la Presidencia, 2014] Ministerio de la Presidencia (2014). Orden PRE/1838/2014. http://www.boe.es/boe/dias/2014/10/09/pdfs/BOE-A-2014-10264.pdf.

[Nets DanID A/S - Finansministeriet, 2014a] Nets DanID A/S - Finansministeriet (2014a). Digital signatur. https://www.nemid.nu/dk-da/om_nemid/hvad_er_nemid/digital_signatur/.

[Nets DanID A/S - Finansministeriet, 2014b] Nets DanID A/S - Finansministeriet (2014b). Er NemID obligatorisk? https://www.nemid.nu/dk-da/om_nemid/er_nemid_obligatorisk/.

[Nets DanID A/S - Finansministeriet, 2014c] Nets DanID A/S - Finansministeriet (2014c). Hvem kan få NemID? https://www.nemid.nu/dk-da/om_nemid/hvem_kan_faa_nemid/.

[Nets DanID A/S - Finansministeriet, 2014d] Nets DanID A/S - Finansministeriet (2014d). NemID. https://www.nemid.nu/.

[Nets Holding A/S, 2014] Nets Holding A/S (2014). Nets. http://www.nets.eu/.

[OECD, 2007] OECD (2007). OECD e-Government Studies - NETHERLANDS. OECD Publishing.

[para las Administraciones, 2014] para las Administraciones, I. E. (2014). Gobierno de es- paña. Identidad Electrónica para las Administraciones. http://clave.gob.es/.

[Politsei- ja Piirivalveamet, 2014a] Politsei- ja Piirivalveamet (2014a). Digi-ID. http://www. politsei.ee/en/teenused/isikut-toendavad-dokumendid/digi-id/.

[Politsei- ja Piirivalveamet, 2014b] Politsei- ja Piirivalveamet (2014b). Estonian ci- tizen's passport. http://www.politsei.ee/en/teenused/isikut-

toendavad-dokumendid/ eesti-kodaniku-pass/.

[Politsei- ja Piirivalveamet, 2015] Politsei- ja Piirivalveamet (2015). Mobile-ID. https://www. politsei.ee/en/teenused/isikut-toendavad-dokumendid/mobiil-id/.

[Slamanig et al., 2014] Slamanig, D., Stranacher, K., and Zwattendorfer, B. (2014). User- centric identity as a service-architecture for eids with selective attribute disclosure. In Proceedings of the 19th ACM symposium on Access control models and technologies, pages 153–164. ACM.

[Stadt Würzbrug, 2014] Stadt Würzbrug (2014). Informationsblatt zur Anzeige einer Geburt. http://www.wuerzburg.de/m_31031.

[Statistics Austria, 2014] Statistics Austria (2014). Persons with Internet usage 2002 to 2014. http://www.statistik.at/web_en/statistics/information_society/ict_usage_in_ households/041019.html.

[STORK, 2014] STORK (2014). Estonia: eID card a ten-year success. https://www.eid-stork. eu/index.php?option=com_content&task=view&id=348&Itemid=69.

[United Nations, 2014] United Nations (2014). e-Government Survey: E-Government for the Future We Want. Economy & Social Affairs.

[Wolters Kluwer Italia e RCS MediaGroup, 2015] Wolters Kluwer Italia e RCS Me- diaGroup (2015). Atto di nascita, dichiarazioni, certificati ed estratti. http: //www.dirittierisposte.it/Schede/Persone/Nascita-morte-e-certificati/atto_di_nascita_ dichiarazioni_certificati_ed_estratti_id1118282_art.aspx.

[Zwattendorfer et al., 2011] Zwattendorfer, B., Tauber, A., and Zefferer, T. (2011). A privacy- preserving eid based single sign-on solution. In NSS'11, pages 295–299.

Universidade de Brasília – UnB

Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

www.unb.br – www.cdt.unb.br – www.latitude.eng.br