PROPOSTA DE UM SISTEMA NACIONAL DE IDENTIFICAÇÃO PESSOAL ÚNICO

Tathinay de Souza Siqueira[1], Brunna Caroline do Carmo Mourão[1], Thatiane Oliveira Rosa[2], Ivo Sócrates Moraes de Oliveira[2]

[1]Graduada em Gestão de TI. E-mail: tatty1000@live.com; brunnacharming@gmail.com.
[2]3Professor(a) do Curso de Gestão de TI e Sistemas de Informação - IFTO. E-mail: thatiane@ifto.edu.br; ivo@ifto.edu.br.

Resumo: Visto o alarmante número de fraudes relacionadas aos documentos de identificação pessoal, este trabalho propõe um modelo para a autenticação de identidade pessoal com tecnologias modernas e de baixo custo. Neste trabalho foram observados critérios essenciais de segurança e de alcance para todas as esferas sociais. Para elaboração desta pesquisa foi realizado um levantamento bibliográfico, para assim definir as propostas que posteriormente foram analisadas. Os resultados consistem em propostas elaboradas a partir de estudos de mecanismos de garantia de autenticidade, análise de dispositivos e aplicações que melhor executarão o processo de identificação.

Palavras–chave: identificação pessoal digital, rfid, sim card, sistema de identificação, smartphone

1 INTRODUÇÃO

Os dados populacionais são significativos itens na tomada de decisão governamental. Erros nestes dados podem gerar déficit nos cofres públicos [IBGE, 2000]. Por isso, o registro civil, título de eleitor, dentre tantos outros documentos de identificação pessoal são de fundamental importância, não apenas para o Estado como para o cidadão, pois sem os tais ele não é ninguém, ou seja, não é reconhecido. Mesmo com tal magnitude os documentos de identificação civil brasileiros são distribuídos em cédulas de papel, podendo ou não serem plastificados, ou em PVC, apresentando geralmente o número de registro geral, data de emissão e UF (Unidade Federativa), data de nascimento, foto e nome, e filiação [Portal Brasil, 2009]. Pela facilidade de falsificação desses documentos não é muito raro acontecerem fraudes relacionadas ao roubo de identidade, onde um indivíduo usurpa de dados pessoais.

O Serasa Experian [Serasa, 2012] identificou as principais operações realizadas com identificação falsa, que são: emissão de cartões de crédito, financiamento de bens eletrônicos, compra de celulares com documentos falsos ou roubados, compra de automóveis, abertura de contas (cartões, cheques, empréstimos pré-aprovados) e abertura de empresas de fachada para aplicação de golpes no mercado. E ainda alerta para o número de tentativas de fraudes detectadas por ano, que gira em torno de 2 milhões; e que a cada 16 segundos o consumidor está sujeito a uma tentativa de fraude. Um dos fatores do número de fraudes ter se estendido muito deve-se a popularização da Internet. Dados levantados pelo CERT (Centro de Estudos, Resposta e

ISSN 2179-5649
VIII JICE©2017

Tratamento de Incidentes de Segurança no Brasil) mostram que dos incidentes de segurança relatados, um total de 1.047.031, em 2014, sendo que 467.621 são relacionados a fraudes, ou seja, um total de 44% dos incidentes.

Com o intuito de facilitar e garantir a segurança da validação dos documentos de identificação pessoal este trabalho busca responder a seguinte pergunta: Quais os mecanismos poderiam ser usados para o processo de validação de documentos de identificação pessoal de forma automatizada e segura? Para responde-la elencou-se como objetivo modelar mecanismos de identificação pessoal, com base em assinatura digital, por meio de GSM-SIM Card e do telefone celular. O SIM Card GSM é um circuito integrado, utilizado em telefones celulares. Nele contém o IMEI, um número de identificação de dispositivos móveis; e a chave de autenticação, que são algoritmos para autenticação da rede e dados do assinante do cartão [ETSI, 1992].

A assinatura digital foi desenvolvida para estancar a lacuna de autenticação e integridade da criptografia e tem como princípio legitimar um documento não modificado no trajeto e garantir a autenticidade de sua origem (GOODRICH e TAMASSIA, 2013). A Lei n. º 290-D/99, 1999, declara que documentos eletrônicos com assinaturas digitais equivalem aos documentos tradicionais de papel com assinatura a punho. Na transmissão de uma mensagem digital a assinatura digital é caracterizada pela adição de um resumo que identifica unicamente a mensagem que será transmitida. O algoritmo padrão da assinatura digital é o *hash*, sendo que em uma transmissão onde qualquer informação é adulterada o valor do *hash* (denominado resumo de mensagem) é alterado e o receptor notificado da ocorrência, se a transmissão não sofre interferências, a identidade do remetente e a integridade do documento são confirmadas (DEITEL, DEITEL e CHOFFNES, 2005) (PEIXINHO, 2013).

O *hash* pode ser utilizado para gerar assinaturas e certificados digitais, para verificar a integridade de arquivos baixados da Internet, como também verificar arquivos armazenados no computador. Maziero (2013) diz que para a função *hash* cumprir esses objetivos deve gerar a mesma saída para a mesma entrada, e saídas diferentes para entradas diferentes, e ainda que que possua espalhamento e sensibilidade, ou seja, uma pequena modificação em trechos dos dados de entrada modifique significante diversas partes do resumo.

Basicamente o SIM Card tem duas finalidades: armazenamento de dados e execução para algoritmos de autenticar identidade [ETSI, 1992]. A especificação GSM 11.14 proporciona

permissões para atualizações dos dados através da rede, sem necessidade de contato. Ferramenta que já é utilizada na Estônia, país reconhecido por ser pioneiro na democracia digital tudo graças a implantação da identificação digital. Sendo uma solução atrativa para a problemática desse trabalho.

2 METODOLOGIA

O método adotado nesta pesquisa foi o estudo de caso relacionando com o sistema de identificação nacional, em que por meio de análises de tecnologias mais recentes analisadas em 2016 são propostas intervenções de melhorias, visando garantir maior segurança e praticidade. Na 1ª fase realizou-se uma pesquisa exploratória dividida em 3 partes: 1ª etapa – objetivou levantar a problematização, que resultou em dados alarmantes sobre fraudes. 2ª etapa – para compreensão dos dados obrigatórios em um documento é que foram analisados os requisitos e as tecnologias permitidas para os mesmos. 3ª etapa – com o intuito de encontrar soluções, averiguou-se soluções aplicadas historicamente em outros países. Na 2ª fase, Desenvolvimento da Proposta, foi alçada as hipóteses de possíveis erros para salientar o quão preciso deve ser os processos para garantir a segurança: 4ª etapa – com o intuito de criar soluções para a problemática foram elencadas especificação a serem abordados pelos mecanismos de autenticação. 5ª etapa – objetivou a familiarização com mecanismos de garantia de autenticidade, com o propósito de selecionar os mais precisos e adaptáveis ao caso. 6ª etapa – com o conhecimento técnico adquirido, concerniu para elaboração dos esboços dos processos. Na 3ª fase, Análise dos Resultados, foi avaliado todo o projeto: 7ª etapa – desenvolvimento da conclusão.

3 RESULTADOS E DISCUSSÕES

Na Estônia, país que possui um dos mais avançados sistemas eletrônicos de governo do mundo, o qual utiliza o e-ID, uma identidade digital. É notório as benfeitorias do uso de um sistema de identificação digital, bem como: segurança, desburocratização, economia tanto para o usuário como para o governo. A identidade digital abriu caminhos para o avanço em diversos seguimentos do governo permitindo, por exemplo, que processo de compra e venda de imóveis seja feito em poucos minutos através da Internet, e até mesmo o voto eleitoral. Para qualquer atividade digital é necessário apenas um computador, Internet e um leitor de *smart-card*, que pode ser

encontrado gratuitamente em centros públicos. A identificação também pode ser feita por SIM-card pelos celulares (E-ESTÔNIA, 2017).

No início a população estoniana não tinha Internet ou dispositivos com os quais usar, o que desprendeu um alto investimento para inserir a tecnologia da informação no cotidiano. Hoje é ofertada Internet de qualidade em praticamente todo território nacional (E-ESTÔNIA, 2017).

Através das análises de sucesso da Estônia e de tecnologias viáveis, identificou-se duas ferramentas de autenticação que se encaixam com a proposta deste trabalho, sendo elas autenticação via Bluetooth® e via RFID. A seguir são apresentados os processos de cada tarefa e demais processos essenciais.

3.1 Cadastro de usuário

Neste processo (Figura 1) é necessário firmar o sistema a uma AC (Autoridade Certificadora) para ser a encarregada do gerenciamento dos certificados e necessidades do sistema. Será necessário o usuário comparecer à AC para convalidar seu cadastro. Na AC o usuário tem seus dados cadastrados e atualizados. Os dados são armazenados no banco de dados do sistema juntamente com o PIN do usuário e então é entregue o SIM Card do usuário; caso este tenha *smartphone* é instalado o aplicativo de identificação pessoal. Concluindo o processo a AC fornece instruções e orientações de uso para o usuário.

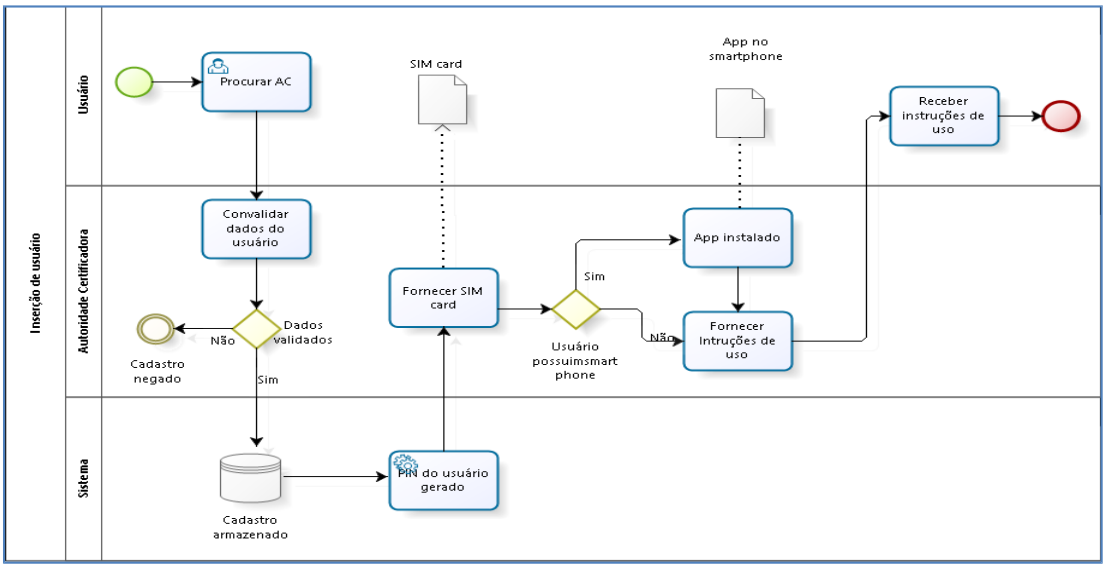

Figura 1 - Cadastro de Usuário

3.2 Autenticação via Bluetooth®

Esta opção foi considerada por ser mais prática em casos onde não é viável o leitor de RFID, não sendo possível ao requerente ter um leitor RFID, é interessante por não depender da Internet para operar, sendo necessário que os usuários apenas tenham o aplicativo instalado. Para esta autenticação é necessário que o requerente e o titular tenham o aplicativo instalado.

Este processo (Figura 2) inicia com o Login nas respectivas aplicações dos requerente e titular, que após a confirmação a aplicação mostra opções de ação: leitor e Gerador de QR Code. Em seguida a aplicação-1 lê o QR Code gerado na aplicação-2, e para confirmar que o titular está ciente do acesso aos seus dados pelo requerente, a aplicação-1 envia uma mensagem de requerimento de código de verificação ao sistema, que envia um SMS para o titular. Este código deve ser inserido na aplicação-1. Com o código confirmado, a aplicação-1 tem as informações do titular e envia SMS ou e-mail com informações sobre o acesso ao banco de dados do sistema e este envia o mesmo SMS para o titular.

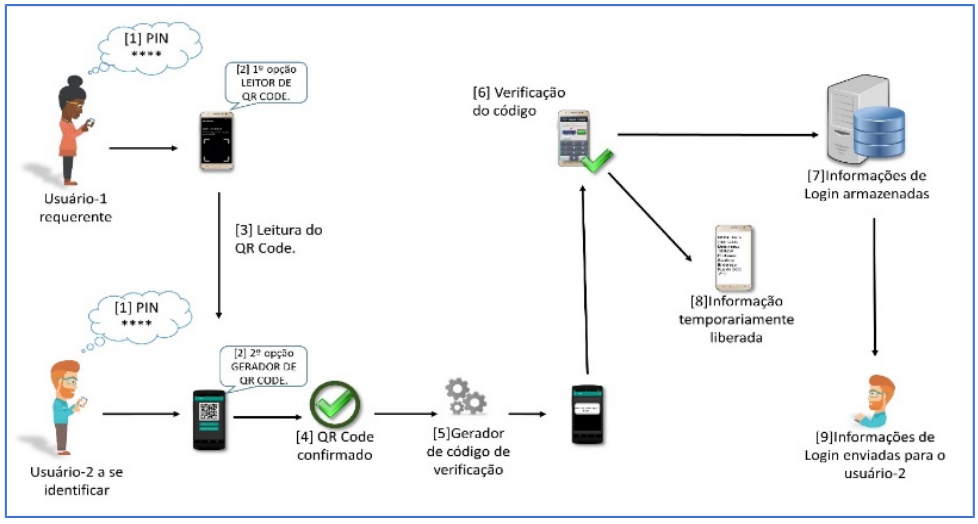

Figura 2 - Autenticação via Bluetooth®

3.3 Autenticação via RFID

RFIDs trata-se de um circuito integrado para armazenar informações e uma antena para transmitir e recebe o sinal, e sua autenticação é feita por leitores ou gravadores separadamente [Goodrich e Tamassia, 2013]. O SIM Card é passado no leitor, o titular digita sua senha, e suas informações são liberadas, e depois de um tempo limite os dados são bloqueados e caso necessário,

a senha deverá ser inserida novamente. E da mesma forma da autenticação via Bluetooth® o armazenamento é feito simultaneamente ao acesso.

Para o processo de autenticação via RFID (Figura 3) basta apenas que o usuário tenha em mãos seu SIM Card de identificação pessoal. A etiqueta é pareada no leitor RFID, o qual faz o requerimento do PIN do usuário, se for inserido corretamente as informações do usuário são liberadas, caso o contrário haverá ainda três chances de inserir o PIN novamente, sendo liberado para nova tentativa após 24h. Depois das informações liberadas o leitor envia as informações do Login para o banco de dados do sistema, o qual envia um SMS ou e-mail com as mesmas informações para o usuário.

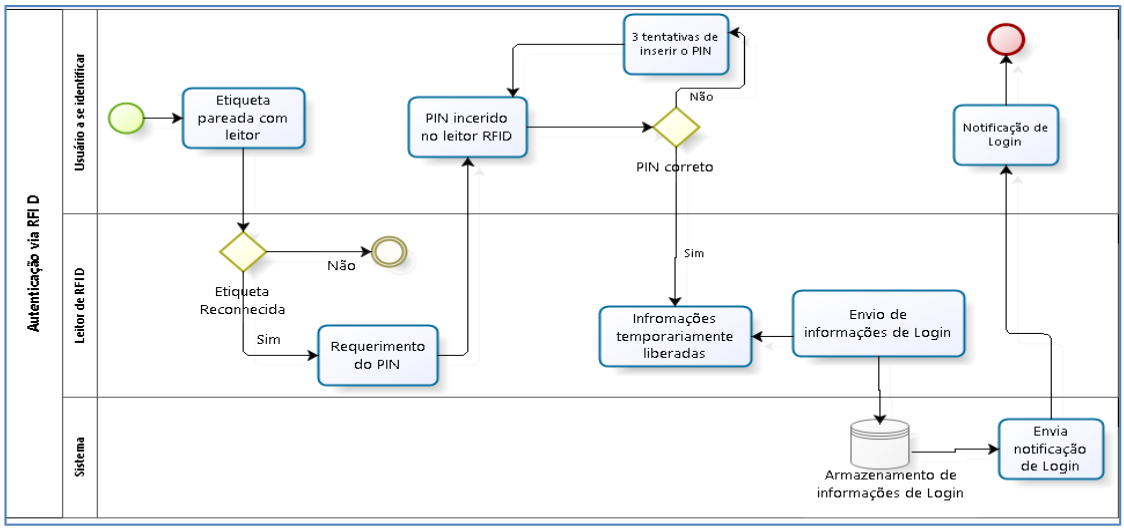

Figura 3 - Autenticação via RFID

3.4 Armazenamento de Login

Seguindo o conceito de segurança, viu-se a necessidade de *backups* de Login, assim quando ocorrer suspeita de Login fraudulento o usuário receberá uma mensagem de alerta via SMS e e-mail e ao constatar atividade fraudulenta o usuário deverá informar a AC para que tome as medidas cabíveis, entre elas fornece outra chave de acesso.

O armazenamento de Login utiliza a tecnologia de serviços de mensagens curtas, por ser uma tecnologia de baixo custo e não depender de conexão banda larga. Após a liberação do acesso que decorre da autenticação, a aplicação gera informações do Login, como: IMEI, data, horário, local e acesso; a aplicação envia um SMS-MO para o servidor; que armazena as informações; e

envia um SMS-MT ou um e-mail, conforme o padrão escolhido pelo usuário; assim o processo finaliza com o usuário recebendo a notificação de Login. A finalidade desse processo é que o usuário tenha ciência que sua conta está sendo acessada, caso este forneça sua senha a terceiros, ou até mesmo em caso da violação do sistema. A seção seguinte apresenta a conclusão deste trabalho, mencionado um breve resumo do que foi abordado para análise dos resultados.

5 CONSIDERAÇÕES FINAIS

Este trabalho foi fundamentado na fragilidade do sistema atual de identificação pessoal. Logo, foram propostas tecnologias que proporcionam segurança e eliminam os conflitos de dados cadastrais de diferentes documentos por meio de uma base de gerenciamento de dados única e a da unificação dos documentos, sendo entregue ao cidadão em um SIM Card GSM. Utilizando caso de sucesso, modelou-se os processos de autenticação, com o intuito de demostrar os resultados das ferramentas de autenticação pesquisadas. A pesquisa focou em buscar ferramentas e métodos de baixo custo e de fácil manuseio.

Com a conclusão de todas as fases da metodologia, notou-se que é possível aplicar um novo método de identificação pessoal pragmático e relativamente mais seguro. Sabe-se, porém, que a aplicação desse novo método implicaria em altos gastos governamentais e mudança cultural, e toda mudança traz um desconforto inicial. No entanto o retorno em segurança e flexibilidade justifica a implantação. Como trabalhos futuros pode-se elencar a análise do impacto da implantação do sistema proposto.

REFERÊNCIAS

DEITEL, H. M.; DEITEL, P. J.; CHOFFNES, D. R. **Sistemas operacionais.** 3º. ed. São Paulo: Pearson Prentice Hall, 2005.

E-ESTONIA. Disponível em: <https://e-estonia.com/>. Acesso em: 24 ago. 17.

ETSI. **Subscriber Identity Modules, Functional Characteristics.** GSM 02.17. 1992.

GOODRICH, M. T.; TAMASSIA, R**. Introdução à segurança de computadores.** Porto Alegre: Bookman, 2013.

IBGE**. Relatório da Divisão de Contabilidade,** 2000. Disponível em: <http://www.ibge.gov.br/home/disseminacao/prestacaodecontas/relatgestao.shtm>. Acesso em: 29 set. 2016.

MAZIERO, C. A. Sistemas operacionais: conceitos e mecanismos. Curitiba: [s.n.], 2013.

PEIXINHO, I. **Introdução a Segurança de Redes.** Rio de Janeiro: RNP - Rede Nacional de Ensino, v. 2.2.0, 2013.

PORTAL BRASIL. **Emissão da Carteira de Identidade (RG) é gratuita em todo País,** 2009. Disponível em: <http://www.brasil.gov.br/cidadania-e-justica/2009/10/emissao-da-carteira-de-identidade-RG-e-gratuita-em-todo-pais>. Acesso em: 29 set. 2016.

SERASA CONSUMIDOR. **A cada 16 segundos uma pessoa é vítima de tentativa de fraude no Brasil,** 2012. Disponível em: <http://www.serasaconsumidor.com.br/a-cada-16-segundos-uma-pessoa-é-vítima-de-tentativa-de-fraude-no-brasil-11>. Acesso em: 28 abr. 2016.