Universidade Federal de Santa Catarina

Ciências da Computação

Luca Fachini Campelli

DESENVOLVIMENTO DE UM APLICAÇÃO PARA COLETA DE DADOS E EMISSÃO DE PASSAPORTES ELETRÔNICOS NA PLATAFORMA JAVACARD

Florianópolis/SC
2018

Luca Fachini Campelli

DESENVOLVIMENTO DE UM APLICAÇÃO PARA COLETA DE DADOS E EMISSÃO DE PASSAPORTES ELETRÔNICOS NA PLATAFORMA JAVACARD

Trabalho de Conclusão de Curso para a graduação no curso de Ciências da Computação UFSC

Florianópolis, 2018

Resumo

Com a preocupação com a segurança em todas as áreas, a identificação correta e segura das credenciais de uma pessoa se torna de extrema importância. A necessidade de vários documentos diferentes para as mais variadas funções faz surgir vários problemas, desde falsificação e roubo, até simples desorganização e perda. O maior exemplo da necessidade dos mais variados documentos é em viagens internacionais. Nelas são necessárias diversas etapas até que se confirme a identidade do viajante afim de evitar falsificações, e outros tipos de ameaça, sendo o mais importante dos documentos o passaporte.

O intuito deste trabalho é criar uma infra-estrutura para emissão de passaportes eletrônicos na plataforma Javacard, baseado no padrão ICAO 9303 [10], tendo em mente a segurança das informações. O sistema de emissão deverá prover um aplicativo que colete as informações do usuário, e crie um passaporte eletrônico dentro de uma das 5 possibilidades existentes e descritas no trabalho de conclusão de curso citado [12]. Este cartão deve possuir todas as informações de identificação da pessoa, juntamente com informações biométricas. O projeto será efetuado juntamente com o LabSec (Laboratório de Segurança Computacional da UFSC) e o professor responsável, com a utilização da biblioteca JMRTD [9], que será adaptada para os fins deste projeto, e projetos anteriores do LabSec que servirão de base para desenvolvimento do produto final.

Palavras-chave: Javacard, Passaporte,JMRTD, Segurança, Passaporte-Eletrônico, e-Passport

Abstract

With the increasing importance over security, the correct identification of a person's credentials becomes increasingly as important. The need for various documents for diferent uses brings many problems to the surface, ranging from falsification to disorganization and loss. The greatest example being international travels, where various stages are required util the identity of an individual is confirmed, to prevent any kind of threat. The most important of these documents being the passport.

This paper aims to create an infra-structure for the issuance of electronic passports on the JavaCard platform, based on the ICAO 9303 standard [10], with information security in mind. The issuance system should provide an application that collects user information, and creates an electronic passport in one of 5 existing possibilities described on the cited end-term project [12]. This passport should posess all required user information, along with biometrics. This project will be done together with LabSec (UFSC's Computational Security Lab) and it's responsable professor, utilizing the JMRTD library [9], that shall be adapted for this project's purposes, along with prior projects from the lab, that will serve as a basis for the developing of the final product.

Key-Words: Javacard, Passaport,JMRTD, Security, Electronic-Passport, e-Passport

Sumário

Figuras

1 Introdução

Com o aumento do compartilhamento de dados entre instituições de um mesmo grupo, a necessidade de segurança aumenta conforme o tamanho do grupo aumenta e a necessidade de confirmar a identidade de um usuário, para que não haja abuso dos recursos nem acesso irrestito aos dados se torna cada vez mais importante. Assim, cada vez mais cresce a quantidade de documentos necessários para que se confirme a identidade do usuário, como CPF, RG, CNH, Passaporte, e biometrias digitais que todos ficam armazenados em documentos físicos e separados, aumentando a quantidade de itens que uma pessoa tem que carregar, e aumentando o tempo para resgatar estas informações e conferir com o usuário.

Este trabalho visa o desenvolvimento de um sistema que controle a emissão de passaportes universitários eletrônicos baseado no padrão ICAO 9303, na plataforma Javacard [1]. Este sistema deverá englobar todas as necessidade documentais para a identificação correta e segura do usuário, para agilizar processos de identificação biométrica. Ele deve coletar os dados do usuário como digitais, assinatura digitalizada, nome, e dados de identidade para a criação de um cartão Javacard eletrônico seguro, dentro dos vários modelos possíveis. Para tal serão utilizadas técnicas de criptografia para assegurar uma comunicação segura com o cartão, e seu funcionamento adequado.

2 Objetivos

O objetivo principal deste projeto é a criação do sistema de coleta de dados, e emissão do cartão, onde os dados sejam armazenados dentro do cartão para que depois possam ser extraídos e validados em qualquer tipo de máquina que possua este sistema.

Os objetivos específicos se dão por:

1.Coleta dos dados básicos do usuário[10][12]
2.Coleta da foto do usuário e extração dos dados faciais da foto[4][10].
3.Coleta dos dados biométricos como digital e íris.
4.Ter o cartão preenchido e funcional.
5.Ter o programa que colete os dados do usuário de forma rápida e fácil.

Ao final do projeto espera-se ter concluído a criação de um sistema que colete os dados do usuário, armazenando-os no banco de dados, e que emita o cartão conforme as especificações ditadas no padrão ICAO9303

3 Conceitos Básicos

3.1 O que é segurança computacional? [[13] - cap 1]

Segurança computacional engloba todas as áres de pesquisa relacionadas a manter algum tipo de informação segura, seja ela uma senha, listas de cadastros, um banco de dados, documentos ou uma receita de bolo. As pesquisas relacionadas a segurança computacional, trabalham para proteger estas informaçõe de pessoas que as poderiam utilizar para maus fins, seja impedindo que elas sejam obtidas ou entendidas por outras pessoas, ou garantindo que uma informação não foi alterada antes de ser entregue ao destinatário. As próximas seções deste documento explicam certos campos desta área que serão tratados.

3.2 Criptografia Simétrica e Assimétrica [[13] -parte 1 - parte 2]

É possível cifrar a informação para que apenas quem possua a chave da cifra possa acessa-la. O ato de embaralhar o significado da mensagem se chama cifrar, e o inverso, decifrar. Para tal, utiliza-se algum tipo de algoritmo que, em conjunto com uma chave, seja capaz de mascarar a informação original e que seja reversível, para que com o uso da chave, se possa desfazer a criptografia e acessar o conteúdo original da mensagem. Nesta área existem dois tipos de protocolos para cifrar mensagens: a criptografia Simétrica e a Assimétrica.

Na criptografia simétrica, uma única chave é utilizada por ambas as partes, para cifrar e decifrar a mensagem. Na criptografia assimétrica, são utilizadas duas chaves distintas, uma pública e uma privada. Ambas podem ser usadas para cifrar, porém o que uma cifrar, somente poderá ser decifrado pela outra. Devido às dificuldades de se utilizar este protocolo ele é mais utilizado para certificações digitais.

3.3 Função Hash - SHA [[13] - cap 11 - pg313]

Esta função é amplamente utilizada para garantia de consistência tanto em criptografia quanto em várias outras áreas. Esta função funciona embaralhando os bits de uma mensagem à um ponto que seja impossível inverter o processo. Ela aceita uma mensagem de qualquer tamanho, porém sempre retornará uma cadeia de bytes de tamanho fixo, não importando qual seja a entrada. Porém a maior característica desta função está no fato de que para duas entradas distintas x e y quaisquer, o resultado da função sempre será diferente para os dois. Desta forma, é possível se checar a integridade de uma mensagem, aplicando a função hash sobre ela antes de ser enviada, e depois de recebida, e comparando as saídas, pois se a mensagem foi alterada, por menor que seja a alteração, os dois resultados da função serão completamente diferentes. O algoritmo mais utilizado para esta função é o SHA 2 - Secure Hash Algorithm 2(Algoritmo de Hash Seguro 2), projetado pela NSA, e possui seis versões diferentes, onde a mudança principal está no número de bits que eles retornam: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.

3.4 Assinaturas Digitais[[13] - cap 13.1 - pg 395]

A confiança entre duas partes de uma troca de mensagens pode não ser suficiente para que informação sensível seja transferida. Uma parte "A" pode forjar uma mensagem alegando ter sido enviada pela parte "B", ou "B" pode simplesmente negar ter enviado qualquer mensagem, mesmo que o tenha. Desta forma, um meio de proteger âmbas as partes contra fraude mútua são as assinaturas digitais. Uma assinatura digital consiste normalmente da própria mensagem "M", passada pela função hash e cifrada com a chave privada do remetente, concatenada ao fim da mensagem. Ao ser recebida esta assinatura pode ser verificada, removendo-a da mensagem, decifrando-a com a chave pública do remetente e comparando-a com a hash da mensagem recebida. Sendo assim duas afirmações podem ser concluídas: apenas o remetente pode ter enviado a mensagem, pois apenas a sua chave privada pode ser decifrada com sua chave pública, e a mensagem não foi alterada durante seu trajeto, pois as hash's coicidem.

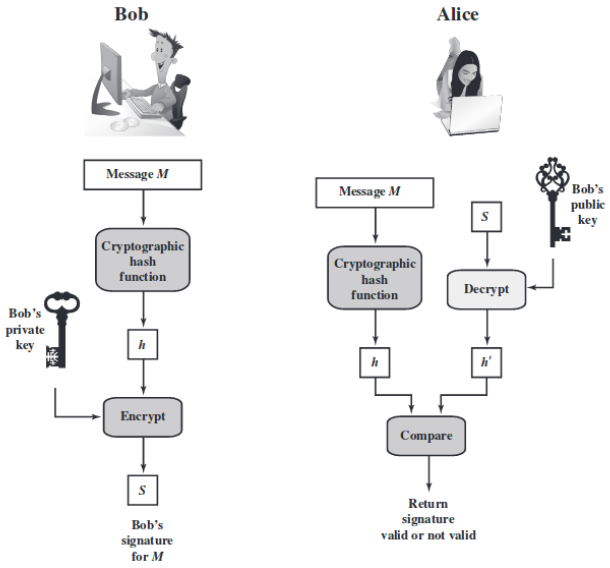

Figure 1: Descrição simplificada do funcionamento de uma assinatura digital.

3.5 Certificados Digitais[[13] - cap 14.4 - pg 435]

Certificados digitais são documentos eletrônicos que garantem a autenticidade de um certo elemento. Este que pode ser uma entidade, um site da internet ou um terminal de cartões. Um certificado é composto de algumas informações da entidade, a chave pública da entidade, e uma assinatura digital sobre o certificado. Dependendo do tipo de certificado, esta assinatura adicionada ao final do documento é cifrada ou com a chave privada de quem o criou, denominado de certificado auto-assinado, ou com a chave privada de uma autoridade certificadora (CA - Certificate Authority).

4 O Documento ICAO 9303[10]

O documento ICAO 9303 é o documento emitido que regulamenta passaportes eletrônicos, e é o padrão utilizado para toda formatação de passaportes eletrônicos. ICAO é uma sigla para "International Civil Aviation Organization", que é uma agência especializada das Nações Unidas. Foi estabelecida em 1944 para gerenciar a admnistração e governância da Convenção de Aviação Civil Internacional (Convenção de Chicago).

O documento é escrito em 12 partes, cada uma descreve um aspecto sobre como um passaporte eletrônico deve ser desenvolvido, a primeira parte dando uma introdução sobre o as características de um passaporte eletrônico, e definindo siglas e acrônimos para os documentos seguintes.

A segunda parte da especificações sobre a segurança física do cartão, desde o design interno, quanto a produção, transporte e criação do cartão.

A terceira parte especifica as características sobre a apresentação de todos os tipos de passaporte, como fonte, linguagem, campos de preenchimento e representação das informações.

A quarta parte específica como os dados para passaportes legíveis por máquina, que possuem forma de livreto como são hoje, mostrando dimensões e formatos dos campos, também chamado de tipo TD3.

A quinta parte especifica como deve ser o layout dos dados para passaportes do tipo cartão plástico impresso, chamado TD1. Este cartão possui uma zona legível por máquina (MRZ), que possui os dados básicos de seu portador, formatados para mais fácil leitura humana e por máquina, impresso em seu exterior junto com todas as outras informações no verso, e uma imagem do portador.

A sexta parte se assemelha à quinta, pois descreve as características de cartões do tipo TD2, que possuem de diferente do tipo TD1 apenas suas dimensões, tendo todas as informações necessárias em um lado do cartão, permitindo informações opcionais serem adicionadas ao verso.

A sétima parte se refere à vistos legíveis por máquina. Estes se assemelham aos tipos de passaportes TD1 e TD2, porém possuem as informações referentes aos vistos.

A oitava parte não foi preenchida ainda, e é mantida reservada para uso futuro.

A nona parte fala sobre como se deve dispor das informações biométricas do portador do passaporte, formatos e dados, tomando como principal a identificação facial da pessoa, e como identificações secundárias as digitais e íris.

A décima parte especifica a estrutura logica de dados (LDS) do cartão, e como se deve armazenar os dados biométricos dentro do cartão.

A décima primeira parte especifica como funcionam os protocolos de segurança necessários à comunicação do cartão e obtenção dos dados biométricos para verificação da identidade da pessoa.

Por último a décima segunda parte especifica o funcionamento de todas as assinaturas digitais necessárias à certificação do cartão via chaves públicas, e sua infra-estrutura.

5 História do Passaporte Eletrônico

Quando começaram a ser utilizados, os passaportes funcionavam apenas por meio físico, na forma de uma caderneta, com todas as informações sendo verificadas manualmente, comparando as informações com o sistema. Isto acarreta em uma passagem mais lenta pelo controle e abre muitas brechas para erros e falsificações passarem pelos vigías. Várias formas de prevenir falsificações como marcas d'água, padrões de impressão e manufatura do papel foram utilizadas, porém a inovação mais impactante e discutida foi a inserção de um chip dentro do passaporte. Embora várias informações possam ainda ser verificadas visualmente, mais ainda podem ser verificadas por meio eletrônico com o chip interno do passaporte, e mais rapidamente, diminuindo o risco de fraude. Este chip pode guardar as informações biométricas do dono, junto com as informações visuais, e ainda mais importante, possuindo diversos protocolos de segurança para garantir a autenticidade dos dados conferidos.

6 Trabalhos Correlatos

O método de criação de um passaporte é extremamente burocrático[2]. O modelo de passaporte que normalmente possuímos é o tipo TD3 descrito no documento ICAO[10],e exigem o preenchimento de formulários e a manufatura da caderneta com chip como parte de sua emissão. Os chips vem programados da fábrica e todos obedecem o padrão descrito no documento ICAO[7]. Diver-

sos softwares existem para a leitura de passportes e em sua maioria se utilizam da biblioteca JMRTD[9] como base para seu funcionamento, poucos utilizam outras bibliotecas de código fechado, como o software de leitura de chips NFC da empresa InnoValor[3], mas não foi possível encontrar o software utilizado por aeroportos para a verificação de passaportes. Apenas um software foi encontrado que efetivamente recolha dados e emita um passaporte sendo este uma versão antiga da biblioteca JMRTD que possuía um aplicativo standalone para emissão e leitura de passaportes eletrônicos, este que foi descontinuado da versão 0.4.9 para a versão 0.5, mantendo o pacote apenas como uma biblioteca.

7 Javacard[1]

O Javacard é um cartão eletrônico que possui dois componentes principais, Um chip de contato e um processador interno. Este chip de contato se faz presente do lado externo do cartão, da mesma forma que cartões de crédito ou débito modernos, e cuida da comunicação do cartão com a leitora. O processador interno funciona como um computador, ele roda um sistema operacional Java, o que torna este cartão um Javacard. Ele também possui uma memória interna capaz de armazenar dados. O que diferencia este cartão de cartões de crédito por exemplo, é o fato de o cartão possuir um máquina virtual Java (JVM) instalada. A JVM faz possível o cartão possuir aplicativos em sua memória, e dependendo do programa que os acessar, pode escolher qual deles executar. Estes aplicativos conversam com o terminal por meio de mensagens, chamadas APDU's, que são em sua maioria padronizadas em alguns formatos específicos. O Chip de contato fornece energia e faz a comunicação entre a leitora ou terminal e o processador. Estes cartões possuem diversos mecanismos de segurança embutidos na própria JVM, os aplicativos rodam isolados uns dos outros, portanto os dados de um aplicativo nunca poderão serem lidos por outro. Os cartões também suportam funções de criptografia, que dependem dos aplicativos para serem utilizadas.

8 O aplicativo e sua estrutura lógica de dados

A biblioteca JMRTD possui consigo um aplicativo a ser instalado e executado no cartão para o funcionamento da biblioteca[12]. Este aplicativo foi feito juntamente com a biblioteca no padrão ICAO9303, portanto ele pode ser lido inclusive por outras bibliotecas que implementem o padrão. Este aplictivo tem como função armazenar todas as informações referentes a um passaporte, e portanto possui uma estrutura de dados lógica interna descrita pelo padrão ICAO9303:

DG 1 — Informação da Zona Legível por Máquina
DG 2 — Características Faciais (Foto)
DG 3 — Informações de identificação adicionais (Digitais)*
DG 4 — Informações de identificação adicionais (Iris)*
DG 5 — Fotografia impressa na frente do cartão*
DG 6 — Reservado para uso futuro*
DG 7 — Assinatura escrita digitalizada*
DG 8 — Características de dados* **
DG 9 — Características estruturais* **
DG 10 — Características substanciais*
DG 11 — Detalhes pessoais adicionais*
DG 12 — Detalhes do documento adicionais*
DG 13 — Detalhes opcionais*
DG 14 — Informações da chave pública para Autenticação Passiva***
DG 15 — Informações da chave pública para Autenticação Ativa***
DG 16 — Pessoas para contato*

* - Opcional
** - Ainda não definido, estrutura geral que acomoda qualquer tipo de dados
*** - Condicional, apenas se suportado

Além destes existem mais dois arquivos que não armazenam dados do usuário mas sim dados do cartão, estes são: COM e SOD.

O arquivo COM, ou Arquivo de Cabeçalho e de Presença de Grupos de Dados, possui a

função de armazenar a presença dos arquivos de dados, ou seja, quais arquivos estão presentes no cartão, e informações de versionamento do sistema de arquivos do cartão.

O arquivo SOD, ou Document Security Object - Objeto de Segurança do Documento, possui a função de armazenar o resultado da função hash de cada arquivo, ou seja, no processo de emissão do cartão, cada arquivo é passado também pela função hash, e seu resultado é armazenado dentro do arquivo SOD. Ele também armazena todas as informações de segurança do cartão como os algoritmos utilizados para a função hash e criptografia. O cartão possui também uma zona que é ilegível por meios externos, informações sensíveis a criptografia como chaves privadas são armazenadas ali na sua criação, e depois só podem ser lidas pelo próprio cartão.

9 As bibliotecas utilizadas

O sistema principal será desenvolvido na linguagem de programação Java, porém algumas das bibliotecas escolhidas foram escritas na linguagem de programação C ou C++ exigindo a utilização da Interface Nativa Java (JNI) para sua utilização.

JMRTD[9]

Java Machine Readable Travel Documents: é uma biblioteca para a criação, edição, e aferição de passaportes eletônicos escrita na linguagem de programação Java. Ela foi desenvolvida juntamente com a biblioteca Scuba, que a complementa. Ela possui a capacidade de criar, e editar novos passaportes, além que resgatar as informações de um passaporte pronto.

SCUBA[15]

Smart Card Utilities for Better Access: é uma biblioteca para a comunicação com cartões eletrônicos da plataforma javacard, escrita na linguagem de programação Java. Ela faz a ponte entre o JMRTD e o javacard possuindo a capacidade de transmitir mensagens e prover a comunicação com os cartões.

STASM[6]

Active Shape Models with STASM: é uma biblioteca de reconhecimento facial escrita na linguagem de progrmação C++. Ela se utiliza de modelos de formas para reconhecer um rosto em uma foto e retirar os pontos de referência do rosto para que depois seja feito o reconhecimento da pessoa, fazendo uso da biblioteca Open-CV. Possui a maioria dos pontos de reconhecimento parecida com o padrão ISO[4], e foi escolhida por ser de fácil utilização e possuir uma extensa documentação com exemplos mínimos disponíveis, facilitando a sua compreensão, além de ser complementar à biblioteca Open-CV.

LIBFPRINT[5]

É uma biblioteca de coleção e verificação de digitais biométricas escrita na linguagem de programação C. Ela provê funções para se coletar uma digital e guardá-la como uma imagem, e depois extrair as minutas desta imagem para que se compare com uma digital recém tirada. Foi escolhida por ter uma documentação extensa, exemplos mínimos e ter sido recomendada pelo orientador deste projeto.

OPEN-CV[14]

Open Source Computer Vision Library: é uma biblioteca para manipulação de imagens e visão computacional escrita na linguagem de programação C++ e Java. Ela possui funcionalidades para conversão de imagens, e acessar a câmera do dispositivo para tirar fotos ou videos. Ela também provê visão computacional, permitindo identificar formas e rostos na imagem. A biblioteca Stasm amplia a funcionalidade para rostos, detectando mais pontos de interesse no rosto da pessoa, e foi escolhida por ser a mais bem recomendada biblioteca de manipulação de imagens e visão computacional, com relação a sua utilização.

EJBCA[11]

Open Source PKI Certificate Authority: é uma biblioteca para criação e manejo de certificados digitais auto-assinados escrita na linguagem de programação Java. É necessária para o funcionamento da biblioteca JMRTD, para criação dos certificados verificáveis por cartão (CVC), necessários para a execução dos protocolos de segurança do cartão.

BOUNCYCASTLE[8]

Bouncy Castle Security Provider: é um provedor de segurança, uma biblioteca que possui funções criptograficas e de geração e acordo de chaves para criptografia escrita na linguagem de programação Java. Toda a segurança da biblioteca do JMRTD é feita com ele, portanto por motivos de compatibilidade foi-se utilizado o bouncycastle como provedor para o sistema final.

10 Metodologia - Reescrever?

O projeto será executado tendo como base o aplicativo JMRTD[9], que engloba uma API Java e um Applet, onde juntos já permitem o armazenamento de informações no cartão, e o projeto: IDEdu: Proposta de um Cartão de Identificação Acadêmico[12] baseado no padrão ICAO 9303[10], para que seja criado um aplicativo que emita os passaportes, e que possa ser expandido caso haja a necessidade, para englobar mais documentos e não só o passaporte.

Será feita uma extensa pesquisa sobre os documentos ICAO 9303[10], e a documentação da biblioteca JMRTD para se iniciar o projeto.

O programa será desenvolvido com a linguagem de programação Java, utilizando o sistema JNI para a integração de bibliotecas que existem somente em C e C++, e as bibliotecas JMRTD, como a biblioteca principal para a construção do cartão, BouncyCastle[8] e EJBCA[11] como provedores de segurança e certificação, libfprint[5] para a coleta das digitais biométricas, Stasm[6] para o reconhecimento facial, e OpenCV[14] para processamento de imagem.

Utilizando uma parte do código da versão 0.4.9 da biblioteca JMRTD, é possível enviar informações para o cartão, desta forma pode-se fácilmente coletar e enviar as informações à respeito do MRZ. A biblioteca OpenCV será usada para o processamento da foto da pessoa, e possui funções para tirar a foto com a camera da máquina. Com a biblioteca Stasm, se pode retirar os pontos faciais da pessoa, e depois tratá-los para se adequarem ao padrão ICAO. Foi necessário utilizar a API nativa do java para integrar as bibliotecas Stasm e libfprint ao projeto, pois elas existem apenas em C. Com a biblioteca libfprint foi possível a extração da digital para sua inserção.

10.1 Os protocolos de segurança

Para o acesso as informações do cartão diversos protocolos de segurança devem ser efetuados para garantir a troca segura de mensagens entre o terminal e o cartão, e ter a certeza de que o terminal e o cartão não foram adulterados de alguma maneira. Todos os protocolos estão completamente descritos no documento ICAO 9303 parte 11

BAC - Basic Access Control - Controle de Acesso Básico

Antes de fazer qualquer tipo de operação no cartão, deve-se efetuar este protocolo. Ele utiliza as informações do número do documento, data de nascimento e de validade do cartão para criar chaves simétricas seguras para a troca de mensagens entre o terminal e o cartão criando assim um canal seguro de comunicação. Esta informação estará impressa na frente do cartão, e portanto a execução com sucesso deste protocolo não só garante um canal de comunicação seguro, mas também confirma que as informações impressas batem com as armazenadas no cartão.

PA - Passive Authentication - Autenticação Passiva

Este protocolo faz uso dos arquivos COM e SOD para seu funcionamento. O arquivo SOD armazena a hash de cada Grupo de Dados presente no cartão, e o arquivo COM indica sua presença. Desta forma o protocolo se inicia verificando se para cada arquivo cuja presença esteja indicada em COM, incluindo o arquivo COM, se sua hash coincide com a hash armazenada em SOD. Se todas coincidirem então nenhum arquivo foi alterado desde a fabricação do cartão.

O segundo passo consiste em utilizar o certificado de assinatura encontrado no SOD, construindo uma corrente de certificação até um certificado assinado por uma CA reconhecida, e garantindo que cada certificado da corrente seja válido. Passados por estes dois passos então se pode confirmar que os dados do cartão são válidos e não foram alterados.

AA - Active Authentication - Autenticação Ativa

Este protocolo deve ser feito após o PA, pois ele confirma que o SOD foi lido de um cartão com um chip válido. Ele consiste em uma troca de mensagens de desafio-resposta onde a aplicação envia

uma mensagem ao cartão e este responde com esta mensagem cifrada pela chave privada do cartão. A aplicação então decifra utilizando a chave pública armazenada no arquivo DG15 e, caso a resposta coincida com a mensagem enviada, então o chip não foi adulterado, já que a chave privada interna do cartão é o par da chave pública gravada no arquivo DG15.

EAC - Extended Access Control - Controle de Acesso Extendido

Este protocolo deve ser feito após o BAC e é necessário para se obter acesso as biometrias adicionais do cartão. Ele consiste em autenticar o terminal para o cartão, e o cartão para o terminal em duas etapas, Utilizando-se de um par de chaves assimétrico com curvas elípticas. Ao término do protocolo um canal de comunicação de maior segurança entre o cartão e o terminal é gerado, e o acesso às biometrias adicionais é liberado.

11

12 Referências

[1] Zhiqun CHEN. *Java Card^{TM} Technology for Smart Cards : architecture and programmer's guide*. Addison-Wesley, England, UK, 2000.

[2] HomeOffice. How your passport is made – exclusive behind-the-scenes footage. `https://www.youtube.com/watch?v=Ha5VPXZ3ILs`. Accessed: 26-06-2018.

[3] InnoValor. Readid. `https://www.readid.com/`. Accessed: 26-06-2018.

[4] ISO/IEC. Iso/iec 19794-5 biometrics. https://www.iso.org/standard/50867.html. Accessed: 23-05-2018.

[5] LibFPrint. Libfprint. `https://www.freedesktop.org/wiki/Software/fprint/libfprint/`. Accessed: 13-04-2018.

[6] S. Milborrow and F.Nicolls. Active shape models with sift descriptors and mars. *VISAPP*, 2014. Accessed: 13-04-2018.

[7] U.S. Department of State. Policy podcast: Making a passport. `https://www.youtube.com/watch?v=1XIjbJ4GvEQ`. Accessed: 26-06-2018.

[8] The Legion of the Bouncy Castle. Bouncy castle. `http://www.bouncycastle.org/java.html`. Accessed: 13-04-2018.

[9] Martin OOSTDIJK. Jmrtd. `https://www.jmrtd.org`. Accessed: 13-04-2018.

[10] International Civil Aviation Organization. Icao 9303: Machine readable travel documents. `https://www.icao.int/publications/pages/publication.aspx?docnum=9303`. Accessed: 13-04-2018.

[11] PrimeKey. Ejbca open source pki certificate authority. `https://www.ejbca.org`. Accessed: 13-04-2018.

[12] Felipe SASSO. Idedu: Proposta de um cartão de identificação acadêmico baseado no padrão icao 9303. `https://docs.google.com/document/d/15Jd3IzxCOFT7Vi-mvTHSbRyRPQeikQoldCGfVxTFUMU/edit`. Accessed: 31-07-2017.

[13] William STALLINS. *Criptography and Network Security Principles and Practice*. Prentice Hall, ?, 2014.

[14] OpenCV Team. Opencv library. `https://opencv.org/`. Accessed: 13-04-2018.

[15] SCUBA Team. Smart card utilities for better access, project scuba. `http://scuba.sourceforge.net`. Accessed: 13-04-2018.