SDM: PROPOSTA DE ARQUITETURA PARA GERENCIAMENTO SEGURO DE CICLO DE VIDA DE DOCUMENTOS

Luís Felipe Feres Santos[1] **(**luisfelipe.fsantos@gmail.com)
Raphael Fogagnoli Tavares[1] (phaelfog@gmail.com)
Eduardo Henrique de Oliveira[1] (adviou@gmail.com)
Renato Lopes e Silva[2] (renatolopesesilva@gmail.com)
Eduardo Hidenori Enari[2] (eduardoenari@gmail.com)
Luis Fernando de Almeida[2] (luis.almeida@unitau.br)
[1]Instituto Nacional de Pesquisas Espaciais, Av. dos Astronautas, 1.758 – S. J. dos Campos – SP – Brasil
[2]UNITAU – Departamento de Informática, Av. Mal. Deodoro, 605, 120100-000, Taubaté – SP – Brasil

Resumo. *Desde muito tempo que há uma preocupação com a segurança das informações que são de alta importância, como por exemplo, documentos de processos, e, para algumas entidades, essas informações em mãos erradas podem causar problemas. Neste sentido, este artigo propõe uma abordagem para controle e gerenciamento de documentos baseada na aplicação de tecnologia smart card, biometria e criptografia. Espera-se proporcionar uma ferramenta para controle seguro ao acesso e inserção das informações em tais documentos.*

Palavras-Chave*: Segurança das informações, Smart card, Biometria, Criptografia.*

1. INTRODUÇÃO

Atualmente, um dos grandes problemas encontrados por empresas e organizações é a falta de segurança no que diz respeito às informações enviadas e à atualização dos documentos que contém as informações. Em alguns casos, a falta de atualização dos documentos se deve ao excesso de trabalho designado a uma pessoa, mas em outros o problema é a não visualização desse arquivo e, também, a falta de segurança aplicada aos documentos que, pela internet, podem ser interceptados ou até mesmo modificados por fraudadores.

Este trabalho apresenta um modelo que vem de encontro com uma necessidade presente nas empresas: prover o controle na segurança de seus dados para que não haja vazamento de informações sigilosas, no que diz respeito a seus próprios dados e, também, de seus clientes. Neste sentido, propõe-se uma arquitetura combinando *smart cards*, biometria, função *hash* e criptografia assimétrica. O foco abordado aqui consiste em um protótipo para gerenciamento do ciclo de vida de um documento - desde sua criação até sua data de expiração, de um modo seguro, possibilitando somente pessoas autorizadas acessar e alterar seu conteúdo.

No restante, este artigo está organizado como segue: a seção 2 aborda os conceitos básicos sobre as tecnologias aplicadas; na seção 3 é apresentado o modelo proposto; a seção 4 demonstra alguns testes realizados; e a seção 5 expõe as considerações finais do modelo proposto.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. Smart Card

Segundo Nicklous et al (2002) um *smart card* pode ser definido como um dispositivo portátil capaz de executar pequenas aplicações e armazenar informações de forma segura, consistindo fisicamente de um pequeno *chip*, com a mesma aparência de um cartão de crédito comum.

Existem três tipos de cartões: com contato, sem contato e híbrido. Neste trabalho foi utilizado um *smart card* com contato, devido, principalmente, seu baixo custo. Dois importantes conceitos referentes a um *smart card* são: *Answer to Reset* (ATR) e *Application Protocol Data Unit* (APDU).

As operações de um *smart card* se iniciam com o envio de um sinal *reset* para o cartão que responde com uma cadeia de *bytes* chamada ATR, que tem até 33 bytes, os quais identificam alguns dados, tais como, o protocolo de transmissão, velocidade de transmissão, entre outros. Além disso, o ATR

contém uma cadeia de bytes denominada *history bytes* que identifica o modelo do cartão e algumas outras características.

Um APDU é uma mensagem que representa um comando ou uma resposta do cartão. A partir dele que é feita a comunicação com o cartão, envio e recebimento de dados e qualquer outro tipo de transação que se deseje realizar. Conforme ilustrado na Tabela 1, cada APDU é dividido em 2 partes: um cabeçalho obrigatório de 4 *bytes*, contendo os *bytes* CLA (Classe da instrução), INS (Instrução), P1 (Parâmetro 1) e P2 (Parâmetro 2), e um corpo opcional, que pode conter os *bytes* LC (quantidade de bytes opcionais que serão enviados), *Data Field* (dados opcionais) e LE (quantidade de *bytes* esperado como resposta).

Tabela 1. Estrutura de um APDU de comando.

Cabeçalho da mensagem				Opcional		
CLA	INS	P1	P1	LC	*Data Field*	LE

Um APDU de resposta, também é dividido em 2 partes, tendo um campo de dados opcional, de tamanho menor ou igual a Le, e dois bytes, SW1 e SW2. Sua estrutura pela Tabela 2.

Tabela 2. Estrutura de um APDU de resposta.

Opcional	Obrigatório	
Data Field	SW1	SW2

2.2. Biometria

Um método muito utilizado para identificação é por meio de senhas. Por exemplo, acessando e-mail, conta bancária e algumas outras aplicações, mais de uma senha pode ser requerida. Por outro lado, também podem ser utilizados smart cards, que permitem o acesso através de uma simples leitura.

O problema desses métodos é que qualquer pessoa pode obter a senha ou o cartão. Desse modo, não há como garantir a total segurança dessas informações. Uma alternativa para este inconveniente é o uso de biometria. O uso de características biológicas tem se mostrado como uma idéia viável, já que cada pessoa possui características diferentes. Por exemplo, não há ninguém com voz igual, ou mesma impressão digital, ou olhos idênticos. Até entre irmãos gêmeos há diferenças.

Com o uso da biometria, os riscos são menores, pois se consegue a autenticidade de uma pessoa, tendo em vista que, por exemplo, ninguém terá uma impressão equivalente a sua.

Como características biométricas, podem ser citadas a íris, a retina, a impressão digital, a voz, o formato de rosto, a geometria da mão, entre outras características que poderão ser usadas no futuro, tais como o DNA e odores do corpo.

Em 2006, o *National Center for State Courts* (NCSC) apresentou um modelo de comparação de sistemas biométricos, onde são comparadas diversas características e comparação dos diferentes tipos de sistema biométrico com base no modelo proposto. A Tabela 3 apresenta o resultado desta comparação.

Tabela 3. Modelo de comparação de sistemas biométricos (Jain, Hong, Pankanti, 2000).

Sistema Biométrico	Verificação	Identificação	Precisão	Confiabilidade	Taxa de erro	Fontes de erro	Falso Positivo	Falso Negativo
Impressão Digital	SIM	SIM	Muito alta	Alta	1 em 500	Sujeira; idade	Extremamente difícil	Extremamente difícil
Reconhecimento da face	SIM	NÃO	Alta	Média	–	Iluminação, idade, óculos, cabelos	Difícil	Fácil
Geometria da mão	SIM	NÃO	Alta	Média	1 em 500	Acidente nas mãos, idade	Muito difícil	Médio
Reconhecimento da Voz	SIM	NÃO	Média	Baixa	1 em 50	ruídos, tempo, resfriados	Médio	Fácil
Reconhecimento da Iris	SIM	SIM	Muito Alta	Alta	1 em 131000	Iluminação deficiente	Muito difícil	Muito difícil
Reconhecimento De Retina	SIM	SIM	Muito Alta	Alta	1 em 10000000	Óculos	Extremamente difícil	Extremamente difícil
Reconhecimento de Assinatura	SIM	NÃO	Média	Baixa	1 em 50	Alterações na assinatura	Médio	Fácil

Neste trabalho foi aplicada a impressão digital devido a facilidade de acesso e menor custo. Consiste em capturar a formação de sulcos na pele dos dedos e das palmas das mãos de uma pessoa. Com relação aos leitores, existem três principais tipos: óptico, que faz uso de um feixe de luz para capturar a impressão digital; capacitivo: que mede a temperatura; e ultra-sônico, que mapeia a impressão digital através de sinais sonoros.

Um sistema biométrico básico necessita que o usuário esteja, previamente, registrado, tendo seu perfil biométrico armazenado em uma base de dados (NBSCP, 2005). Posteriormente, o processo de aquisição, coleta os dados apresentados pelo usuário, e suas características são extraídas para comparação com o perfil armazenado.

2.3. Criptografia

Segundo Moreno, Pereira e Chiaramonte (2005), criptografia pode ser entendida como conjunto de métodos e técnicas para cifrar ou codificar informações legíveis por meio de um algoritmo, convertendo um texto original em um texto ilegível, sendo possível mediante o processo inverso recuperar as informações originais.

A criptografia pré-computacional era formada por um conjunto de métodos de substituição e transposição dos caracteres de uma mensagem que pudessem ser executados manualmente (ou até mesmo mentalmente) pelo emissor e pelo destinatário da mensagem. O surgimento de máquinas especializadas e, posteriormente, dos computadores ocasionou uma significativa evolução das técnicas criptográficas.

Com os avanços da tecnologia e dos estudos na área de criptografia, ela foi dividida em criptografia de chave simétrica e criptografia de chave pública ou criptografia assimétrica.

Criptografia de chave simétrica ou de chave secreta consiste em um algoritmo que utiliza apenas uma chave para cifrar e decifrar a informação. Esta chave é compartilhada entre ambos interlocutores.

O método de criptografia de chave assimétrica ou chave pública utiliza um par de chaves, pública e privada, para realizar as devidas funções. A chave pública é distribuída para todos e a chave privada fica apenas com o dono da chave. O funcionamento dos algoritmos de chaves assimétricas consiste em utilizar a chave pública para cifrar a mensagem e a chave privada para decifrar. Para este tipo de método duas características são consideradas para as chaves: confidencialidade e autenticidade.

2.4. *Hash*

Hash é também conhecido como criptografia de caminho único, pois diferente das cifragens que transformam dados de texto claro em criptograma e depois retorna em texto claro, o hash transforma um texto claro em uma espécie de assinatura representando o fluxo de dados.

O *hash* também pode ser comparado a um selo de segurança, informando qualquer alteração efetuada no arquivo, por menor que seja. Dentre algumas aplicações práticas do hash destacam-se a capacidade de manter a integridade dos dados e a segurança de senhas em banco de dados ou qualquer arquivo de senhas.

3. SDM: *SECURE DOCUMENT MANAGEMENT*

O modelo de controle proposto, denominado *Secure Document Management* (SDM) consiste em um protótipo para controle do ciclo de vida de um documento, o qual sua elaboração consiste na participação de diversos usuários, devidamente autorizados.

Como exemplo, pode-se citar o trâmite de um processo cuja redação depende de diversas pessoas, sendo, às vezes, necessário estabelecer uma ordem de precedência no acesso do documento.

Inicialmente, utilizando um *smart card* devidamente inserido em uma leitora de cartões, um usuário solicita acesso ao sistema por meio de sua senha pessoal. Após validação da senha, o próximo passo consiste na autenticação do usuário por meio de sua biometria a ser comparada com um template contido no cartão. Este processo é descrito na Figura 1.

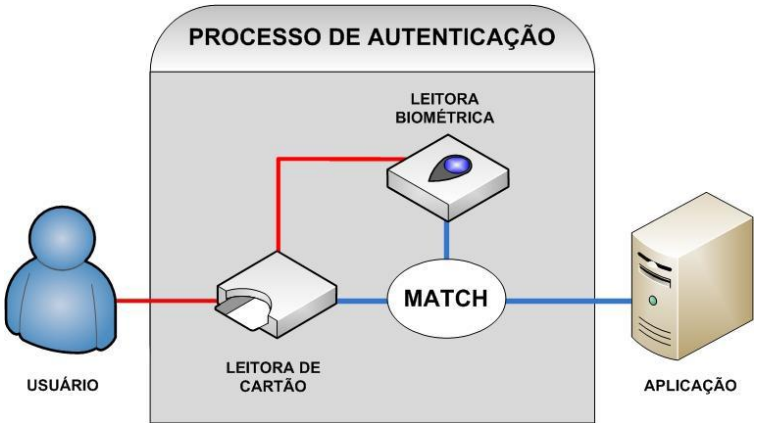

Figura 1. Demonstração do processo de autenticação.

Em seguida, utilizando criptografia de chave assimétrica na assinatura de documentos e simétrica para transferência destes documentos é possível realizar a troca segura de documentos entre entidades. Para validar, que durante o processo de troca não houve interceptação ou alteração do documento enviado, é utilizado um algoritmo hash nomeado MD5, como demonstra a Figura 2.

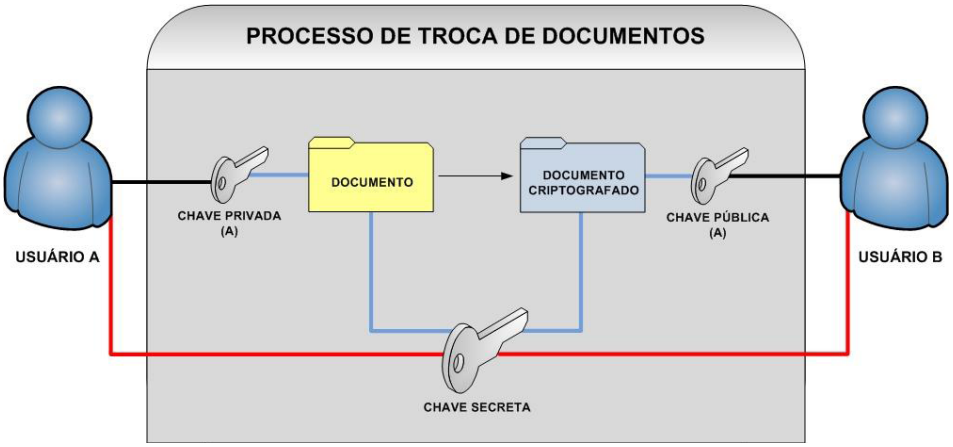

Figura 2. Demonstração do funcionamento do processo de troca de documentos.

3.1. Interface Gráfica e Testesr

Para demonstrar os testes e resultados obtidos serão exibidas, a seguir, imagens do protótipo desenvolvido obtendo sucesso e falha na autenticação biométrica, após a inserção do *smart card* e senha, e também para validar quando o arquivo sofreu alteração ou não, utilizando o algoritmo de *hash*.

A Figura 3 ilustra a falha na autenticação biométrica após inserção do *smart card*, *login* e senha. Já a Figura 4 apresenta um exemplo de sucesso na autenticação biométrica.

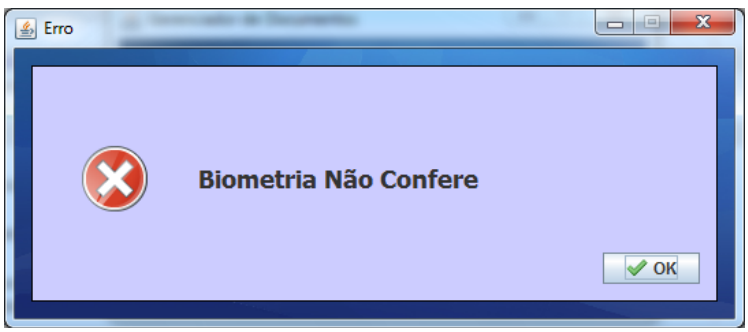

Figura 3. Demonstração da falha na autenticação biométrica após inserção do smart card e do usuário e senha.

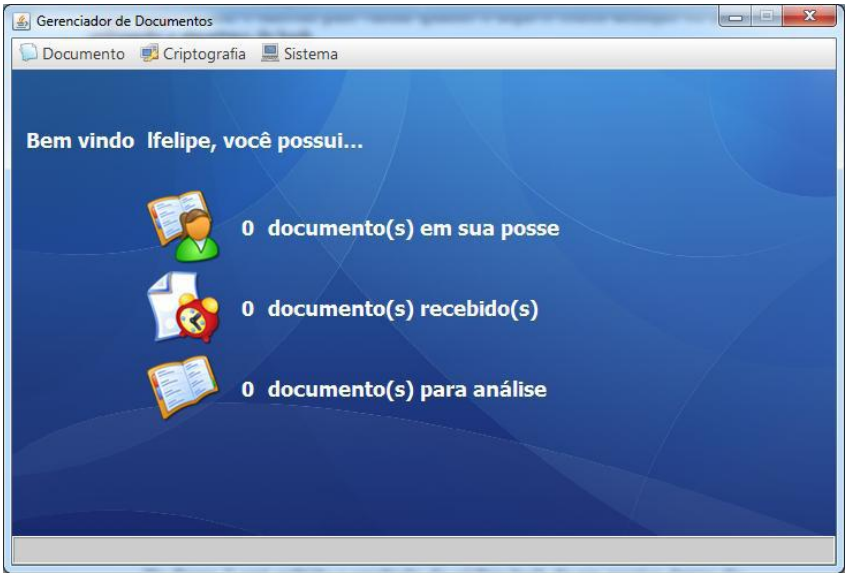

Figura 4. Demonstração de sucesso na autenticação biométrica após inserção do smart card e do usuário e senha.

Na Figura 5 são apresentadas as informações referentes ao resultado do *checksum* de um arquivo dentro do modelo desenvolvido, enquanto que a Figura 6 demonstra o resultado do *checksum* após o arquivo utilizado em questão sofrer alteração.

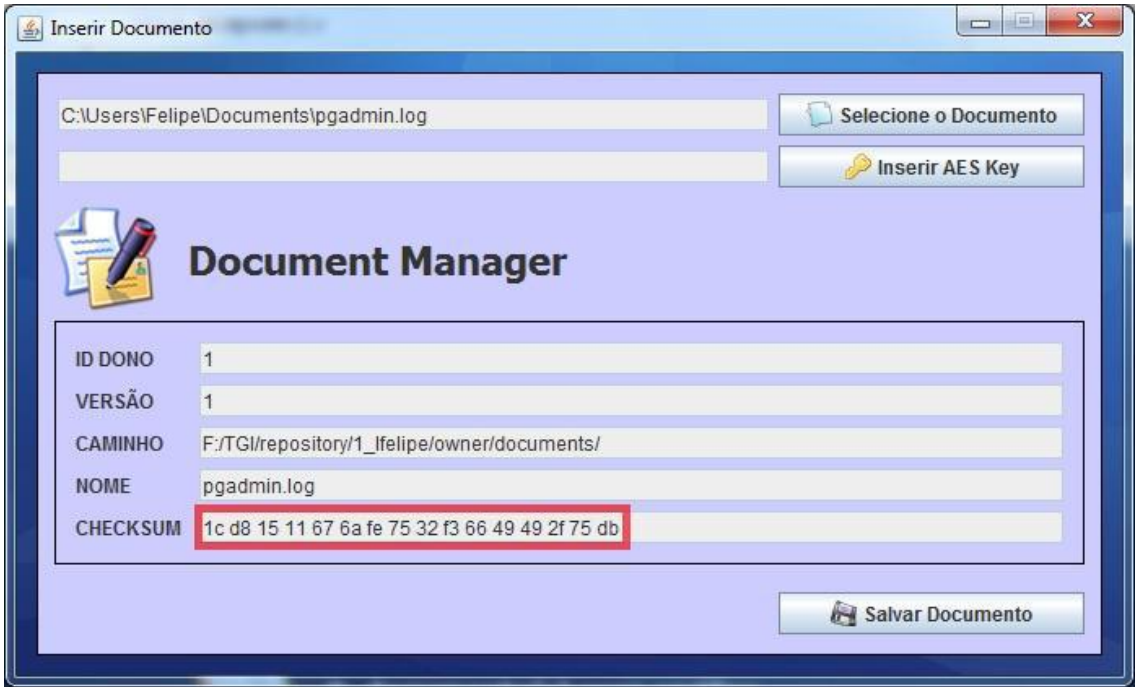

Figura 5. Demonstração do algoritmo hash aplicado a um determinado arquivo dentro do modelo proposto.

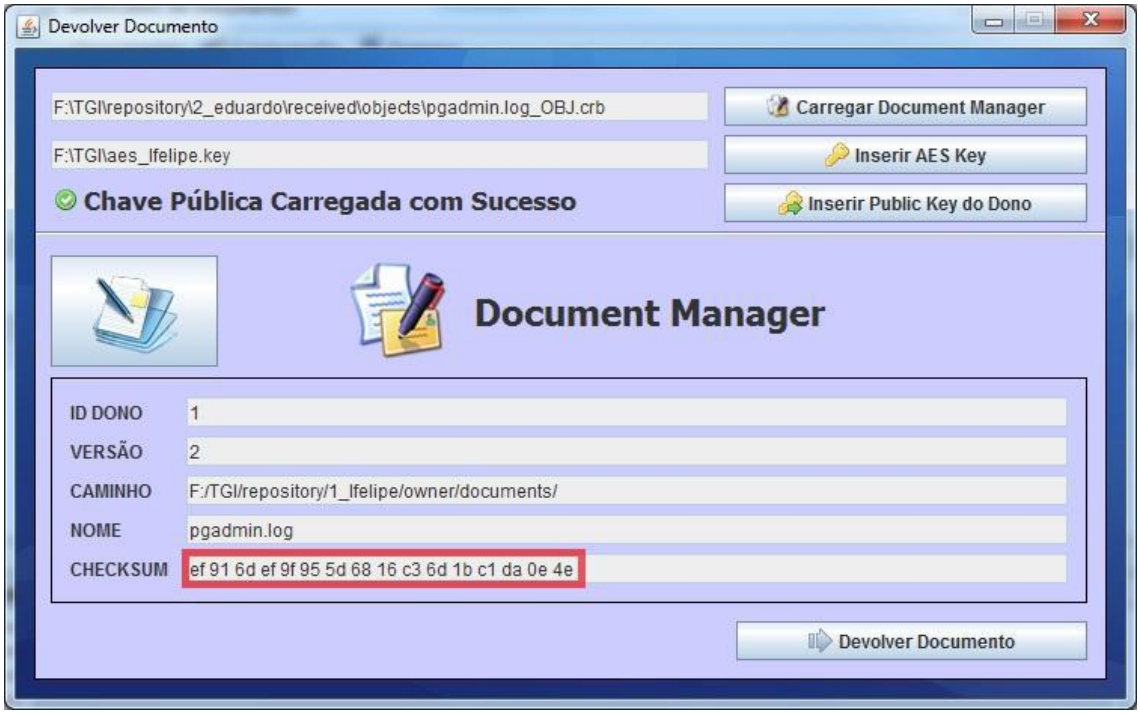

Figura 6. Demonstração do algoritmo hash aplicado arquivo após alteração.

5. CONCLUSÃO

O modelo apresentado neste trabalho propõe uma garantia de que os documentos estão sendo acessados de forma segura e pelas entidades corretas, garantindo, também, assim um maior nível de segurança em relação às informações da entidade que o está utilizando.

Uma das características que se pode citar como inovação é seu funcionamento *online* que permite acesso aos documentos de qualquer lugar que possua conexão com a grande rede. Uma aplicação interessante para este modelo seria o controle do ciclo de vida de processos em cartórios, proporcionando que somente pessoas autorizadas possam acessar determinado processo e, adicionalmente, que se certifique que alguém receba um determinado arquivo.

6. REFERÊNCIAS

Nicklous, M. S., Schack, T., Seliger, F., Hansmann, U., Nicklous, S. M., Schaeck, T. (2002). "Smart Card: application development using Java", Berlim: Springer-Verlag.

Jain, A., Hong, L., Pankanti, S. (2000). Biometric identification, Communications of the ACM , v. 43 , n. 2, pp. 90 – 98.

Moreno, E. D., Pereira, F. D., Chiaramonte, R. B. (2005). "Criptografia em Software e Hardware", Editora Novatec.

NBSP. (2005). "Biometric Technology Application Manual", National Biometric Security Project, v. 1, Biometrics Basics.

Rankl, W. and Effing, W. (2006). "Smart Card Handbook", 3rd ed., Wiley.

DIREITOS AUTORAIS