UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

Programa de Pós-Graduação em Ciência, Tecnologia e Inovação

Dissertação de Mestrado

Esquemas de Assinaturas Digitais: o uso de criptografia assimétrica como um método técnico para autenticidade e não-repúdio em emissão de laudos médicos remotos para PACS

Natanael de Freitas Neto

Natal, dezembro de 2017

Universidade Federal do Rio Grande do Norte - UFRN
Sistema de Bibliotecas - SISBI
Catalogação de Publicação na Fonte. UFRN - Biblioteca Central Zila Mamede

Freitas Neto, Natanael.
Esquemas de assinaturas digitais: o uso de criptografia assimétrica como um método técnico para autenticidade e não-repúdio em emissão de laudos médicos remotos para PACS / Natanael de Freitas Neto. - 2018.
14 f.: il.

Dissertação (mestrado) - Universidade Federal do Rio Grande do Norte, Ciência e Tecnologia, Ciência, Tecnologia e Inovação. Natal, RN, 2018.
Orientador: Prof. Dr. Hélio Roberto Hékis.

1. Criptografia - Dissertação. 2. Assinatura Digital - Dissertação. 3. Telessaude - Dissertação. I. Hékis, Hélio Roberto. II. Título.

RN/UF/BCZM CDU 004.056.55

Elaborado por FERNANDA DE MEDEIROS FERREIRA AQUINO - CRB-15/301

Esquemas de Assinaturas Digitais: o uso de criptografia assimétrica como um método técnico para autenticidade e não-repúdio em emissão de laudos médicos remotos para PACS

Natanael de Freitas Neto

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência, Tecnologia e Inovação da Universidade Federal do Rio Grande do Norte, como parte dos requisitos para obtenção do título de Mestre em Ciência, Tecnologia e Inovação

Orientador: Prof. Dr. Hélio Roberto Hékis

Comissão Examinadora

Prof. Dr. Hélio Roberto Hékis

Profa. Dra. Karilany Dantas Coutinho

Prof. Dr. Custódio Leopoldino de Brito Guerra Neto

Prof. Dr. João Paulo Queiroz dos Santos

Natal, dezembro de 2017

Abstract

Paper documents are being replace in different areas every day and, for any activity that requires authenticity, these new digital forms need to assure the same guaranties as the physical document does, i.e., authorship, authenticity, chronological evidence and integrity. In this article we shall analyze a viable use of available technologies to solve this evidenced issue. In medical reports for image exams, the use of a Picture Archive Communications System (PACS) allow the medical reports to be emitted remotely but it alone does not guarantee any of the security measurements for non-repudiation. The results presented in this article were obtained from an Integrative Literature Review and make evidence that the digital signatures model, based on asymmetric cryptography, could help solve this issue if a solution implementation does not change the installed DICOM/PACS environment and if it makes possible for an easy emitter check without the possibility of repudiation, within the local legislation.

Resumo

Os documentos em papel estão sendo substituídos em diferentes áreas todos os dias e, para qualquer atividade que exija autenticidade, essas novas formas digitais precisam assegurar as mesmas garantias que o documento físico, isto é, autoria, autenticidade, evidências cronológicas e integridade. Neste artigo é analisada uma viável utilização das tecnologias disponíveis a fim de solucionar-se o evidenciado problema. Em laudos médicos para exames de imagem, o uso de um Sistema de Comunicações de Arquivo de Imagem (PACS) permite que os laudos médicos sejam emitidos de forma remota, mas, por si só, não garantem nenhuma medida de segurança para não-repúdio. Os resultados apresentados neste artigo foram obtidos a partir de uma Revisão Integrativa de Literatura a evidenciam que o modelo de assinaturas digitais, baseados em criptografia assimétrica, poderia ajudar a resolver esta dificuldade, caso a implementação de uma solução não alterasse o ambiente DICOM/PACS já instalado e possibilitasse uma verificação do emissor facilmente, sem a possibilidade de repúdio, dentro da legislação local.

Agradeço a todos os professores pelos conselhos que recebi durante a pesquisa e que foram de fundamental importância para sua conclusão. Agradeço, também, a minha esposa pelo carinho, pela felicidade dos dias bons e compreensão dos dias ruins. Agradeço, por fim, a minha família por sempre estar ao meu lado, em especial minhas avós Edna, que sempre foi e será parte importante da minha vida e da pessoa que me tornei, e Maria, que mesmo não podendo estar presente nesse dia, sempre acreditou que eu teria força para tornar realidade todos os meus sonhos.

Dedico este trabalho a todos que utilizam o conhecimento científico como elemento modificador da sociedade e de comportamentos.

Tabela de Conteúdo

Introdução

As últimas décadas foram marcadas por uma explosão no uso da ciência da computação como meio de reduzir o consumo de papel, aumentar a produtividade e automatizar processos. No campo da emissão de laudos médicos não é diferente e, como resultado, o fluxo de documentos associados à atividade começou a migrar do meio físico para o digital. No entanto, a substituição de documentos em papel por documentos digitais em qualquer área exige que sejam oferecidas garantias equivalentes às do papel, ou seja, autoria, autenticidade, evidência cronológica (ADAMS, CAIN, et al., 2001) e integridade (WERLANG, 2014). Somado a isso, no caso dos laudos médicos, ainda existem requisitos funcionais a fim de garantir acesso restrito às informações e a vinculação entre o exame médico e seu laudo.

Tais garantias podem ser firmadas em um ambiente eletrônico se o uso associado de assinaturas digitais e do protocolo DICOM (DICOM STANDARD, 2018) puder ser feito. Os sistemas de informação geralmente são as maneiras mais fáceis e seguras de associar dados e têm um forte impacto na qualidade do gerenciamento e na satisfação do usuário dos serviços de saúde. Diferentes soluções tecnológicas adaptadas à saúde estão sendo utilizadas, possibilitando o desenvolvimento de sistemas de apoio à tomada de decisão. Os hospitais públicos brasileiros já arquivam uma variedade de exames por meio de um Sistema de Arquivo e Comunicação de Imagens - PACS, permitindo acesso remoto a exames médicos.

Devido às décadas de PACS como um sistema de arquivo médico padrão, há um número enorme de exames disponíveis e remotamente acessíveis, o que abre a possibilidade de que, através da aplicação de ferramentas computacionais, várias soluções possam ser desenvolvidas para as numerosas dificuldades presentes na saúde pública, como a falta de uma distribuição igualitária de médicos por habitantes em diferentes regiões.

Fundamentação Teórica (Científico-Tecnológica)

Os hospitais públicos brasileiros que possuem equipamentos médicos possuem uma grande diversidade de tipos de exames, já padronizados, via protocolo DICOM, pela NEMA (DICOM PS3.3 2017d - Information Object Definitions [Patients], topic C.7.3.1.1.1 Modality, 2017).

A estrutura dos sistemas disponíveis para arquivar imagem de exames, PACS, e o protocolo padronizado para a associação de dados às imagens médicas, DICOM, permite um ambiente de desenvolvimento barato e seguro para novos recursos nesse modelo. Assim, para adicionar a capacidade de não-repúdio dos dados assinados ao formato de imagem DICOM, que é baseado na especificação ACR-NEMA (ACR-NEMA, 1989), um procedimento padronizado deve ser seguido. Sendo que especificação ACR-NEMA adiciona um cabeçalho de arquivo e várias *tags* privadas pré-definidas disponíveis ao arquivo (BIDGOOD e HORII, 1992).

A estrutura comum para adicionar quaisquer dados personalizados em arquivos formatados DICOM é feita por atributos de arquivo chamados *tags* que devem ser desenvolvidos de forma a evitar conflitos com elementos privados documentados por qualquer fabricante de dispositivo na Declaração de Conformidade DICOM.

Uma *tag* DICOM usual é composta de um grupo de dois *bytes*, como *g* para um *bit* e um elemento de dois bytes, como *e* para um bit:

$$(gggg, eeee)$$

A documentação de Elementos de Dados Privados do NEMA (DICOM PS3.5 2013 - Data Structures and Encoding, topic C.7.8 Private Data Element [Data Set], 2017) define quatro regras para evitar conflitos com elementos de dados privados que podem ser retomados como:

1. Os Elementos de Dados do Criador Privado numerados $(gggg, 0010 - 00FF)$, em que $gggg$ é um número ímpar, devem ser usados para reservar um bloco de elementos com o número do grupo $gggg$ para uso por um implementador individual. O implementador deve inserir um código de identificação no primeiro elemento não atribuído desta série para reservar um bloco de elementos privados (DICOM PS3.5 2013 - Data Structures and Encoding, topic C.7.8.1 Private Data Element Tags [Data Set], 2017).

2. O Elemento de Dados do Criador Privado $(gggg, eeee)$ identifica o implementador, até que Elemento de dados do criador particular $(gggg, FFFF)$ identifique os elementos de reserva do implementador $(gggg, FF00 - 00FF)$ (DICOM PS3.5 2013 - Data Structures and Encoding, topic C.7.8.1 Private Data Element Tags [Data Set], 2017).

3. Codificadores de Elementos de Dados Privados devem ser capazes de atribuir dinamicamente dados privados a quaisquer blocos não reservados dentro do grupo Particular e especificar essa atribuição através dos blocos Elementos de Dados do Criador Particular correspondentes (DICOM PS3.5 2013 - Data Structures and Encoding, topic C.7.8.1 Private Data Element Tags [Data Set], 2017).

4. Elementos com as *tags* $(0001, eeee)$, $(0003, eeee)$, $(0005, eeee)$ e $(0007, eeee)$ não devem ser utilizados (DICOM PS3.5 2013 - Data Structures and Encoding, topic C.7.8.1 Private Data Element Tags [Data Set], 2017).

Essas *tags* são uma forma engenhosa de adicionar novos conteúdos, como, por exemplo, laudos médicos e seus mecanismos de validação, autenticação, segurança e não-repúdio, à estrutura PACS disponível em qualquer instalação médica comum, através dos blocos privados não reservados do protocolo DICOM. Então, para satisfazer que esses atributos de segurança possam não apenas serem adicionados, mas verificados posteriormente, um esquema de assinatura digital é a melhor prática de desenvolvimento a ser adotada.

Assinaturas são usadas como prova de autoria e autenticidade por séculos, onde os indivíduos registram seus nomes em documentos e mensagens. Para incorporar esses atributos a um documento digital é necessário um mecanismo que tenha validade técnica e legal a fim de garantir o não-repúdio dos documentos após assinados.

O principal processo utilizado na comunicação moderna para autenticidade e validação é a criptografia assimétrica. Ele é usado desde cartões de crédito, garantindo que apenas o proprietário do cartão possa utiliza-lo, até aplicações em criptomoedas,

ajudando a gerenciar todas as negociações de carteiras virtuais e as identidades de seus proprietários. Tudo possível devido à distribuição de chaves públicas.

A distribuição de chaves era um grande problema para comunicações seguras até novembro de 1976, quando Whitfield Diffie e Martin Hellman inventaram a criptografia de chave pública em seu artigo "*New Directions in Cryptography*" (DIFFIE e HELLMAN, 1976) e em particular o esquema de assinatura digital (LYSYANSKAYA, 2002). Com o uso de um desses esquemas, um remetente pode enviar uma mensagem assinada simplesmente aplicando uma chave secreta à mensagem, isto é, criptografando-a. Quando o destinatário recebe a mensagem, é possível verificar a assinatura, aplicando na mensagem criptografada uma segunda chave publicamente acessível (BATTEN, 2012).

Nos esquemas de assinatura digital, cada usuário possui uma identidade, representada por sua chave pública, ou seja, uma sequência de bits disponíveis para todos (LYSYANSKAYA, 2002). Estes esquemas existem se, e somente se, houver transformações unidirecionais (ROMPEL, 1990). A criptografia assimétrica consiste precisamente em uma transformação unidirecional, através de um par de funções computacionalmente eficientes e não viáveis para a inversão (LYSYANSKAYA, 2002).

Para o par de funções:

$$E_k(M) \rightarrow m$$

$$D_k(m) \rightarrow M$$

O *M* maior representa a mensagem de texto simples e o *m* menor representa o texto cifrado. Essas equações representam funções facilmente computáveis para uma dada chave *k*. Ao mesmo tempo, não é computacionalmente possível obter *k*, mesmo sob *M* ou *m*. Não é uma tarefa fácil obter uma das mensagens, possuindo a outra, sem também possuir o valor de *k* (DIFFIE; DIFFIE; HELLMAN, 1976; RIVEST; SHAMIR; ADLEMAN, 1978).

O primeiro esquema de assinatura digital foi construído por Rivest, Shamir e Adleman no documento que também propôs o primeiro sistema de criptografia de chave pública (RIVEST, SHAMIR e ADLEMAN, 1978). Seu esquema de assinatura é baseado em uma suposição que eles introduziram, chamada "suposição RSA".

O processo matemático para o método de criptografia de chave pública consiste em:

$$m = E(M) = M^e * \ mod\ n$$

$$M = D(m) = m^d * \ mod\ n$$

Onde *M* representa a mensagem de texto simples no texto cifrado, *n* é o produto de dois números primos ($n = p * q$), e é um número entre 3 e *n*-1, e *e* também deve ser primo relativo a *p*-1 e *q*-1 e *d* devem ser calculados pela expressão:

$$M = D(m) = m^d * \ mod\ n$$

Assim, a chave privada é dada por n e d, e a chave pública é dada por n e e. A suposição RSA afirma que: mesmo com um valor de e próximo ou igual a 3, a transformação pode ser considerada unidirecional, sendo que ter o resultado de numerosos fatores, n, e a mensagem criptografada m, ainda é inviável em termos computacionais obter um par M e e cuja mensagem m é igual a $M^e * mod\ n$ (RIVEST; SHAMIR; ADLEMAN, 1978).

Por enquanto, a suposição RSA é dada como uma suposição criptográfica padrão (LYSYANSKAYA, 2002).

Objetivos

Neste trabalho analisamos um uso viável de tecnologias disponíveis para resolver o problema de não ter um mecanismo, associado ao formato de arquivo DICOM, que garanta, de maneira confiável, um atributo de não-repúdio para dados registrados em arquivos de dados privados do formato DICOM.

Esses métodos podem permitir que a emissão remota de relatórios médicos para imagens de exames seja incorporada ao conjunto de funcionalidades já presentes para o protocolo DICOM e seus sistemas de arquivamento.

O avanço na segurança, autenticação e autoria da inserção de dados nos arquivos DICOM poderia permitir que a responsabilidade pelos dados fosse atribuída ao seu emissor com um atributo técnico e legal de não repúdio e afastar a possibilidade de técnicos, médicos, médicos residentes e outros profissionais que possam ter acesso ao banco de dados ou aos arquivos DICOM em acessar ou editar seus dados sem prévia permissão.

Metodologia

A Portaria de Políticas Públicas de Saúde Pública nº 2564/2011, redefine o Programa da Rede Nacional de Telessaúde (MINISTÉRIO DA SAÚDE BRASILEIRO, 2011). Assim, é possível que médicos de regiões com altos índices de profissionais por habitante, enviem remotamente, por meio da internet, exames de imagens médicas de usuários dos sistemas públicos de saúde (pacientes) em regiões onde esses mesmos profissionais são escassos.

Para destacar os estudos e tecnologias relevantes sobre o tema, a Revisão Integrativa de Literatura foi o método utilizado, estabelecendo critérios para inclusão e exclusão de estudos e tecnologias; pesquisa na literatura; categorização; avaliação dos estudos e tecnologias incluídos na revisão integrativa; interpretação de resultados; apresentação da revisão e síntese dos conhecimentos adquiridos.

A escala de tempo para a pesquisa adotada foi a partir da data do primeiro esquema de assinatura digital já proposto, em 1978 (RIVEST; SHAMIR; ADLEMAN, 1978), até os dias atuais (2018). Os critérios gerais para incluir estudos e tecnologias foram:

- Abordar as questões de segurança dos dados envolvidos;
- Uso exclusivo de tecnologias de código aberto;
- Recuperação fácil do conteúdo após ser garantido;

- A implementação de um esquema de assinaturas digitais não interfere com o sistema PACS / DICOM;

Para obter um resultado confiável e opiniões e experiências diferentes sobre as tecnologias e conhecimentos envolvidos, os seis principais bancos de dados de artigos foram considerados de grande valor para as áreas envolvidas:

- *DSpace@MIT: MIT Open Access Articles;*
- *Harvard Dash: Digital Access to Scholarship at Harvard;*
- *Elsevier Scopus database;*
- *Google Scholar repository;*
- *IEEE Xplore Digital Library*
- *CAPES Periodical repository.*

Além disso, a questão norteadora para a revisão foi a implantação de novas tecnologias de informação e comunicação no contexto de relatórios médicos, de acordo com os sistemas de imagens médicas, ou seja, Arquivo de Imagens e Sistemas de Comunicação - PACS.

Tecnologia Desenvolvida

Os principais estudos e tecnologias encontrados referem-se ao uso de métodos de criptografia. Existem basicamente duas categorias de criptografia, dependendo do tipo de chaves de segurança usadas para criptografar e descriptografar os dados. Estas são as técnicas de criptografia simétrica e assimétrica (THAKUR e KUMAR, 2011).

Principalmente, as evidências na literatura mostram o uso de mecanismos de criptografia assimétrica como a técnica confiável para proteger a comunicação, restringir o acesso à informação e gerar e verificar assinaturas digitais seguras (RIVEST; SHAMIR; ADLEMAN, 1978; LYSYANSKAYA, 2002; THAKUR e KUMAR, 2011), WERLANG, FC, 2014). Isso acontece porque os métodos criptográficos simétricos têm um problema, não importa o quão fortes eles sejam, cada par que trocará mensagens precisaria de um par de chaves e à medida que o número de pares aumentasse, o número de pares de chaves necessários aumentaria indefinidamente (KAPOOR, PANDYA e S. SHERIF, 2011).

Além disso, seria necessário um mecanismo para gerenciar e distribuir as chaves secretas para cada um dos pontos que podem estar em locais geograficamente difíceis de acessar, bem como rotas inseguras para o tráfego, como o acesso público à Internet. Problemas não evidenciados no método criptográfico assimétrico (RIVEST, R. L. 1990; LYSYANSKAYA, 2002).

No desenvolvimento de softwares comumente associados a um ambiente PACS, o uso de grupos privados é amplamente adotado como uma fonte de solução de problemas locais que o protocolo padronizado geralmente não consegue.

Esses resultados levam à conclusão de que os sistemas de informação representam um grande impacto na qualidade do gerenciamento, cuidado e satisfação dos usuários (pacientes) do sistema público de saúde e, mesmo quando observados em diferentes estágios de implementação, o desenvolvimento de soluções de tecnologia da informação

adaptadas à saúde. gradualmente utilizado e permite o desenvolvimento de métodos para comparar práticas, trocar informações, apoiar sistemas para a tomada de decisões e facilitar o acesso aos processos educacionais.

No caso de um sistema de validação de emissor de relatórios médicos remotos, o benefício ocorre tanto para áreas com baixa concentração de profissionais por habitantes, com uma solução relativamente barata para profissionais que terão um aumento na oferta de trabalho sem a necessidade de se deslocar para outras regiões, que muitas vezes são profissionalmente pouco atraentes.

Discussão dos Resultados

A implementação de esquemas de assinaturas digitais em arquivos formatados em DICOM incorporado ao Programa Nacional de Telessaúde, permite ao médico de saúde recuperar arquivos DICOM, visualizar a imagem do exame, emitir o relatório e assiná-lo digitalmente. Todo o processo executado em um fluxo de trabalho de oferta e demanda.

O acúmulo de informações digitais publicamente acessíveis, como arquivos DICOM anônimos, permite que instituições e empresas utilizem o banco de dados para o desenvolvimento de algoritmos de inteligência artificial e aprendizado de máquina como mecanismos avançados de tomada de decisão para o diagnóstico médico.

Com uma grande quantidade de dados de exames de imagem, relatórios médicos devidamente anonimizados e relacionados, técnicas de inclinação da máquina e diferentes algoritmos inteligentes podem ser usados para encontrar correlações, permitindo a previsão de possíveis doenças, auxiliando médicos a precisarem melhor o diagnóstico e um início de tratamento mais precoce para o usuário do sistema de saúde (paciente) o que reduz a possibilidade de sequelas de tratamento.

Referências

ACR-NEMA Committee. Digital imaging and communications. ACR-NEMA standards publication No. 300-1988. Washington, DC: National Electrical Manufacturers Association, 1989; iii.

ADAMS, C. et al. Internet X.509 Public Key Infrastructure Time-Stamp. [S.l.]. 2001.

BATTEN, L. M. Public Key Cryptography: Applications and Attacks. Melbourne: IEEE Press, 2012. p. 2-131.

BIDGOOD, W. D. Jr; HORII, S. C. Introduction to the ACR-NEMA DICOM Standard; DOI: 10.1148/radiographics.12.2.1561424; Radiographics; p. 345-355; March 1992.

BRAZILIAN MINISTRY OF HEALTH, Minister's Cabinet. Administrative Rule No. 2.546. October 27, 2011.

DICOM STANDARD. Digital Imaging and Communication in Medicine. History. DICOM Standard 2018. Available at: < https://www.dicomstandard.org/history/>

DIFFIE, W.; HELLMAN, M. New Directions in Cryptography, v. T-22, n. 6, p. 644-654, November 1976.

NEMA. DICOM PS3.3 2017d - Information Object Definitions [Patients], topic C.7.3.1.1.1 Modality. [S.l.]. 2017. Available at: <http://dicom.nema.org/medical/dicom/2017d/output/chtml/part03/sect_7.3.html >

NEMA. DICOM PS3.5 2013 - Data Structures and Encoding [Data Set], chapter 5, topic C.7.8 Private Data Element, 2017. Available at: <http://dicom.nema.org/dicom/2013/output/chtml/part05/sect_7.8.html>

NEMA. DICOM PS3.5 2013 - Data Structures and Encoding [Data Set], chapter 5, topic C.7.8.1 Private Data Element Tags, 2017. Available at: <http://dicom.nema.org/dicom/2013/output/chtml/part05/sect_7.8.html#sect_7.8.1>

DIFFIE, W.; DIFFIE, W.; HELLMAN, M. E. New Directions in Cryptography. IEEE Transactions on Information Theory, v. 22, n. 6, p. 644–654, 1976.

LYSYANSKAYA, A. Signature Schemes and Applications to Cryptographic Protocol Design. [S.l.]: Massachusetts Institute of Technology, 2002.

NEMA. About the National Electrical Manufacturers Association. [S.l.]. 2017.

RIVEST, R. L. Cryptology. In: LEEUWEN, J. V. Handbook of Theoretical Computer Science. Cambridge: Elsevier, 1990. p. 717-755. Available at: <http://people.csail.mit.edu/rivest/Rivest-Cryptography.pdf>.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Programming Techniques, 21, n. 2, February 1978. p. 120-126. MIT Laboratory for Computer Science and Department of Mathematics.

ROMPEL, J. One-way functions are necessary and sufficient for secure, Baltimore, 1990. p. 387-394.

WERLANG, F. C. *Assinatura Digital com Reconhecimento de Firma: um modelo de assinatura digital centrado no usuário*. Florianópolis. 2014.