DICOMFlowAccess: um modelo de controle de acesso baseado em certificados digitais para prática da telerradiologia

Denys A. B Silva[1], Gustavo H.M.B. Motta[1]

[1]Centro de Informática – Universidade Federal da Paraíba – UFPB, João Pessoa, Brasil

Abstract. *The practice of teleradiology on a global scale will bring countless benefits, mainly to countries with continental dimensions such as Brazil. However, it is known that the solutions already consolidated in radiology departments are modulated to a local context. In a global collaborative network several challenges arise and one of them is the way access control works. This work presents the DICOMFlowAccess. A model of access control based on digital certificates for the practice of teleradiology in a collaborative network with global connectivity.*

Resumo. *A prática da telerradiologia em escala global trará inúmeros benefícios, principalmente, a países de dimensões continentais como o Brasil. Entretanto, sabe-se que as soluções já consolidadas nos departamentos de radiologia estão modeladas para um contexto local. Numa rede colaborativa global, vários desafios surgem e um deles é a atuação do controle de acesso. Este trabalho apresenta o DICOMFlowAccess. Um modelo de controle de acesso baseado em certificados digitais para a prática da telerradiologia em uma rede de colaboração com conectividade global.*

1. Introdução

Apesar do avanço das tecnologias de comunicação e associações entre entidades tornarem-se cada vez mais comuns, com a telerradiologia, não se observa a formação de uma infraestrutura comum na qual entidades de saúde (e.g. hospitais, clínicas, radiologistas) possam associar-se livremente para realização de atividades. Isso porque o *Picture Archiving and Communication Systems* (PACS)[Huang 2011] e o *Digital Imaging and Communications in Medicine* (DICOM)[Pianykh 2012], principais tecnologias dos departamentos de radiologia, foram originalmente concebidas em um contexto de redes locais sob um mesmo domínio de segurança, sendo incapazes, isoladamente, de formarem uma rede colaborativa aberta, compartilhada e com fraco acoplamento para a prática da telerradiologia. Uma rede aberta remete a capacidade de uma infraestrutura integrar um número crescente de entidades (pessoas, organizações ou componentes tecnológicos) e por compartilhada, entende-se que tal infraestrutura é um bem comum, não pertencendo a uma única entidade. O acoplamento fraco significa que uma entidade pertencente a rede não necessita manter uma conexão ativa (síncrona) com nenhuma outra entidade para usufruir dos recursos da rede.

Os benefícios de uma rede de colaboração para prática da telerradiologia com essas características são variados, como emitir laudos mais eficientemente, suprir a necessidade de especialistas em áreas remotas, economia com deslocamento e diminuição da ansiedade dos envolvidos. Um dos desafios para o estabelecimento desta rede é a

eficácia do processo de autenticação e autorização (AA) em adaptar-se ao seu dinamismo. Atualmente existem vários modelos propostos e o *Single Sign On* (autenticação única) é largamente adotado em redes com essas características, entretanto, este modelo possui bases previamente estabelecidas e a necessidade de ao menos um estabelecimento de seção. Características que confrontam a abertura e assincronismo da rede. Inserir essa rede de colaboração sobre computação nas nuvens traz o benefício de uma infraestrutura mínima para seus colaboradores. Entretanto, surge o risco da dependência de um único provedor, confrontando o compartilhamento da rede, associado a questões referentes a segurança dos dados e privacidade dos pacientes.

Diante das limitações identificadas nas atuais soluções de controle de acesso, este trabalho propõe o DICOMFlowAccess (DFA), modelo de controle de acesso para uma rede aberta, compartilhada e fracamente acoplada para o compartilhamento de imagens médicas. Seu funcionamento se baseia em certificados digitais [ICP-BRASIL 2016] e no modelo arquitetural de referência do XACML [OASIS 2017].

As seções seguintes apresentam o contexto em que o DFA está inserido (Seção 2), seu modelo arquitetural (Seção 3), os experimentos realizados (Seção 4) e por fim, conclui-se o trabalho (Seção 5).

2. Contextualização

O DFA foi concebido para fornecer controle de acesso ao DICOMFlow [Araújo 2017], infraestrutura idealizada sobre a base instalada PACS/DICOM dos departamentos de radiologia para o compartilhamento de imagens médicas. A Figura 1 demonstra um cenário de funcionamento do DICOMFlow. Em suma, o funcionamento ocorre da seguinte maneira. **(1)** A imagem é gerada por uma modalidade e armazenada no PACS do HOSPITAL. **(2)** O DICOMFlow monitora a chegada de novos exames e **(3)** inicia uma sequência de troca de mensagens (via e-mail) com o RADIOLOGISTA o notificando que existe um exame disponível para emissão de laudo. **(4)** O RADIOLOGISTA resgata (via HTTPS) a imagem para posteriormente **(5)** emitir o laudo.

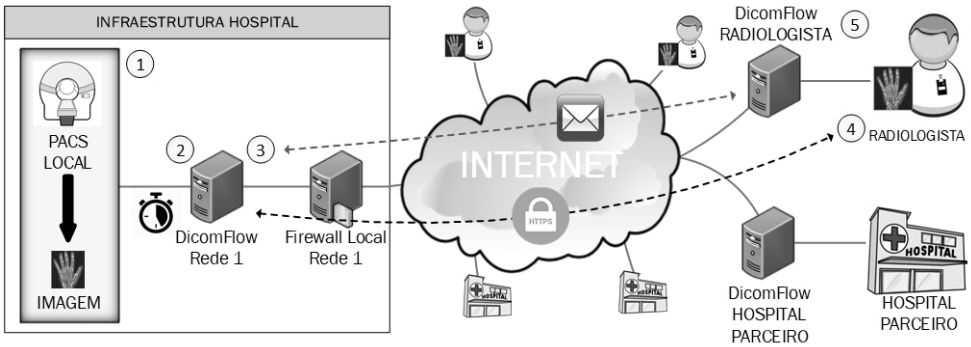

Figura 1: Rede de colaboração proposta pelo DicomFlow.

Durante a troca de mensagens de email, informações de controle são inseridas numa base de dados em HOSPITAL e sempre que o resgate da imagem for solicitado esta base é consultada. Essa forma de controle de acesso limita o crescimento dinâmico da rede, cria a dependência de um provedor de acesso centralizado e não há granularidade. Com a inserção do DFA nessa infraestrutura, esses problemas são sanados. A Figura 2 apresenta uma visão geral do funcionamento da rede proposta pelo DICOMFlow com o DFA inserido e atuando como mecanismo de controle de acesso.

O novo *workflow* se dá da seguinte forma. **(1)** O exame de imagem é gerado por HOSPITAL e, posteriormente, **(2)** transferido para o ARMAZENAMENTO EXTERNO. Em seguida, **(3)** a solicitação de laudo é feita (via email). Ao responder a solicitação, **(4)** o RADIOLOGISTA anexa o seu Certificado Digital de Identidade (CD). De posse desse certificado, o módulo DFA de HOSPITAL **(5)** cria o Certificado Digital de Atributos (CA) associado ao CD enviado anteriormente e o envia para o RADIOLOGISTA. De posse do CA, o RADIOLOGISTA **(6)** faz a solicitação de resgate do exame de imagem (via HTTPS) enviando também seu CD para validação. Caso o DFA valide a requisição de resgate, **(7)** o exame de imagem é transferido e **(8)** o laudo pode ser emitido. O DFA possui duas ações específicas. Emitir e gerenciar os CA's e analisar as solicitações de acesso, informando ao DICOMFlow se o resgate pode ser realizado. É importante reforçar que neste cenário o número de entidades atuantes na rede é crescente.

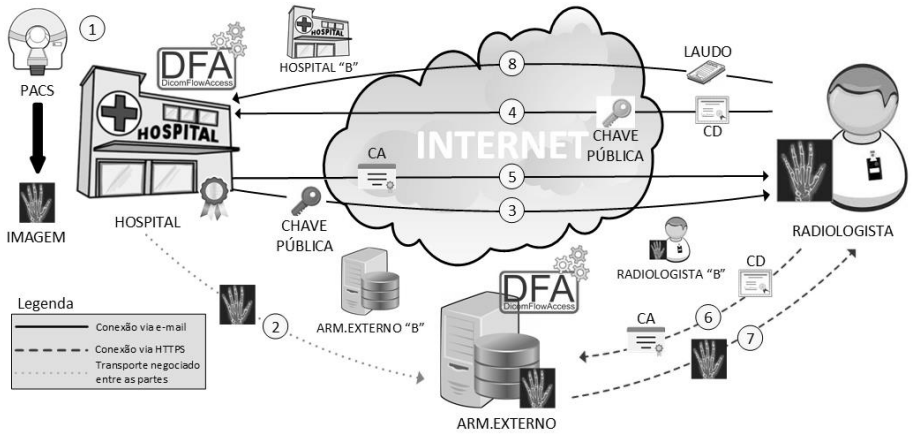

Figura 2: DICOMFlowAccess atuando como mecanismo de controle de acesso

3. Modelo Arquitetural

O modelo arquitetural do DICOMFlowAccess baseou-se no modelo proposto no *eXtensible Access Control Markup Language* (XACML)[OASIS 2017] e é composto por cinco elementos: o PEP (Policy Enforcement Point), responsável por fazer a validação dos certificados; o PDP (Policy Decision Point), que avalia os pedidos de acesso baseando-se nas políticas; o PAP (Policy Administration Point), que armazena e gerencia as políticas; o PIP (Policy Information Point), que mantém informações a respeito dos atributos; e o PRP (Policy Retrieval Point), base de dados em que as políticas são armazenadas. No Certificado de Atributos para uso no DFA, além dos atributos elementares indicados pela ICP-BRASIL, foram criados quatro atributos para prover controle de acesso à rede de colaboração para a telerradiologia proposta por [Araújo 2017], *startDate* e *end*-Date, que determinam a data inicial e final do acesso, *modalityType*, que determina o tipo de exame de imagem que poderá ser obtido e o *dayWeek,* que indica o dia da semana que o acesso poderá ser realizado. Esses dois últimos, são multivalorados. Nesta nova abordagem, a requisição de acesso não será mais tratada pelo DICOMFlow, mas encaminhada ao DFA. A Figura 3 ilustra os módulos e o fluxo interno do DFA.

Este *workflow* ilustra o funcionamento do DFA da entidade ARMAZENAMENTO EXTERNO. **(1)** O DICOMFlow recebe (via HTTPS) a solicitação de acesso a um exame de imagem e encaminha para o PEP os certificados para serem validados. Após esse processo, o **(2)** PEP encaminha os atributos para o PDP analisá-los. Ao certi-

ficar-se que os atributos permitem o acesso ao exame de imagem, **(3)** o PDP consulta o PAP em busca de uma possível sinalização que remeta a negação do acesso. Após essa verificação, **(4)** o PAP indica que ação deve ser executada (aceitar ou negar) e de posse dessa resposta, o **(5)** PDP a informa para o PEP. E finalmente, **(6)** o PEP orienta o DICOMFlow que ação executar, ou seja, se realiza ou não o envio da imagem solicitada.

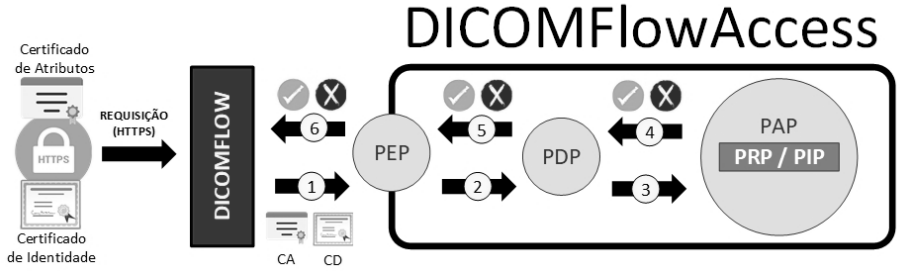

Figura 3: Funcionamento interno do DFA.

4. Experimentos

Os experimentos visaram testar as principais funcionalidades do DFA em um ambiente (virtual) simulando a rede de colaboração para a prática da telerradiologia. Três ações que entendemos serem comuns na rede de colaboração foram simuladas. (A) A criação e envio de forma automática do Certificado de Atributos (CA); (B) Controle de acesso para resgate do exame de imagem utilizando o CA criado no primeiro experimento; e (C) Validação do Certificado de Atributos conforme descrito no [ICP-BRASIL 2016].

5. Conclusão

Os experimentos permitiram observar que o modelo de controle de acesso proposto, o DFA, é tecnicamente viável. O controle às requisições de acesso teve o comportamento esperado e não se observaram anomalias. Em relação aos modelos de autenticação e autorização expostos nesse artigo, o DFA se destaca por não necessitar de conhecimento prévio da entidade que irá solicitar o acesso nem de conexões pré-estabelecidas (persistentes ou não), possibilitando a fácil adaptação a uma rede colaborativa aberta, compartilhada e de fraco acoplamento. Outra característica que reforça essa flexibilidade é que, por utilizar o Certificado de Atributos, o DFA é expansível, podendo adaptar-se a variadas políticas de controle de acesso.

Referências

Araújo, Danilo AB. (2017). DicomFlow: Gateway Assíncrono e Descentralizado para formação de uma Infraestrutura de Informação para distribuição de imagens médicas. [Dissertação de Mestrado] João Pessoa: UFPB.

Huang, HK. (2011). PACS and imaging informatics: basic principles and applications: John Wiley & Sons.

ICP-BRASIL. (2016). DOC-ICP-16. Perfil de uso geral e requisitos para geração e verificação de certificados de atributo na ICP-Brasil. Versão 1.1.

OASIS. 2017. eXtensible Access Control Markup Language (XACML) Version 3.0.

Pianykh, Oleg S. (2012). Digital imaging and communications in medicine (DICOM): a practical introduction and survival guide: Springer Science & Business Media.