**UNIVERSIDADE FEDERAL DA PARAÍBA**

**CENTRO DE INFORMÁTICA**

*PPGI - PROGRAMA DE PÓS GRADUAÇÃO EM INFORMÁTICA*


**DENYS ALEXANDRE BARBOZA DA SILVA**

# DICOMFLOWACCESS: CONTROLE DE ACESSO PARA COMPARTILHAMENTO DE IMAGENS MÉDICAS EM AMBIENTE ABERTO E DISTRIBUÍDO

11 de abril de 2019

João Pessoa - Paraíba

**UNIVERSIDADE FEDERAL DA PARAÍBA**

**CENTRO DE INFORMÁTICA**

*PPGI - PROGRAMA DE PÓS GRADUAÇÃO EM INFORMÁTICA*


# DICOMFLOWACCESS: CONTROLE DE ACESSO PARA COMPARTILHAMENTO DE IMAGENS MÉDICAS EM AMBIENTE ABERTO E DISTRIBUÍDO

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática da Universidade Federal da Paraíba como parte dos requisitos para obtenção do título de Mestre em Informática.

Orientador: Prof. Dr. Gustavo H. M. B. Motta

11 de abril de 2019

João Pessoa - Paraíba

**Catalogação na publicação**
**Seção de Catalogação e Classificação**

S586d Silva, Denys Alexandre Barboza da.
DICOMFlowAccess: Controle de acesso para compartilhamento de imagens médicas em ambiente aberto e distribuído. / Denys Alexandre Barboza da Silva. - João Pessoa, 2019.
114 f. : il.

Orientação: Gustavo Henrique Matos Bezerra Motta.
Dissertação (Mestrado) - UFPB/PPGI.

1. Controle de Acesso. 2. Telerradiologia. 3. DICOM. 4. PACS. 5. DICOMFlow. I. Motta, Gustavo Henrique Matos Bezerra. II. Título.

UFPB/BC

**FOLHA DE APROVAÇÃO**

**DENYS ALEXANDRE BARBOZA DA SILVA**

# DICOMFLOWACCESS: CONTROLE DE ACESSO PARA COMPARTILHAMENTO DE IMAGENS MÉDICAS EM AMBIENTE ABERTO E DISTRIBUÍDO

Aprovado em _____ de _____ de _____.

Banca Examinadora:

_____

Prof. Dr. Gustavo H. M. B. Motta – CI/UFPB

Orientador

_____

Prof. Dr. Ed Porto Bezerra – CI/UFPB

_____

Prof. Dr. Fernando Menezes Matos – CI/UFPB

_____

Prof. Dr. Carlos Eduardo da Silva - IMD/UFRN

"Me dá prazer, ou pelo menos paz, realizar minhas tarefas."

LANGDON, Robert; *Inferno*; 2013.

# AGRADECIMENTOS

À meu Pai do Céu, que sempre me conduziu.

À Dona Carminha, minha mãe. A pessoa mais extraordinária que conheço.

Aos meus irmãos, Danilo e Daniel. Sempre presentes.

À minha companheira de vida, Alécia. Sempre sendo minha base forte e motivadora.

Ao Professor Gustavo. Pessoa brilhante e orientador extraordinário.

Aos professores do Programa de Pós-Graduação em Informática (PPGI), por todos os ensinamentos trocados durante o mestrado.

Aos colegas de trabalho do Laboratório de Arquitetura e Sistemas de Software (LARQSS), pela parceria formada.

Às minhas gatinhas de estimação, Majú e Judith. Companheiras nas madrugadas de estudo e escrita desta dissertação.

Do fundo de minha alma, muito obrigado.

# Sumário

# Lista de Figuras

# Lista de Tabelas

# Lista de Abreviações e Siglas

| | |
|---|---|
| ABAC | Attribute-Based Access Control, 22 |
| AC | Autoridade Certificadora, 27 |
| ACT | Autoridade Certificadora de Tempo, 27 |
| API | Application Programming Interface, 41 |
| AR | Autoridade de Registro, 27 |
| ASN.1 | Abstract Syntax Notation One, 63 |
| AWS | Amazon Web Services, 40 |
| CA | Certificado Digital de Atributos, 17 |
| CAA | Certificado de Atributos Autônomo, 33 |
| CAV | Certificado de Atributos Vínculado, 33 |
| CBIS | Congresso Brasileiro de Informática em Saúde, 96 |
| CD | Certificado Digital de Identidade, 17 |
| CFM | Conselho Federal de Medicina, 27 |
| CR | Computed Radiography, 61 |
| CT | Computed Tomography, 61 |
| DAC | Discretionary Access Control, 22 |
| DFA | DICOMFlowAccess, 15 |
| DICOM | Digital Imaging and Communications in Medicine, 12 |
| DIMEDAC | Distributed Medical Database Access Control, 50 |
| EEA | Entidade Emissora de Atributos, 32 |
| FTP | File Transfer Protocol, 18 |
| GDE | Gestão de Documentos Eletrônicos, 32 |
| HIS | Health Information Technology, 12 |
| HIT | Health Information Technology, 12 |
| HTTP | Hypertext Transfer Protocol, 18 |
| HTTPS | Hyper Text Transfer Protocol Secure, 39 |
| IANA | Internet Assigned Numbers Authority, 59 |
| ICP-Brasil | Infraestrutura de Chaves Públicas Brasileira, 52 |
| II | Infraestrutura de Informação, 10 |
| JCA | Java Cryptography Architecture, 41 |
| JDK | Java SE Development Kit, 41 |

LARQSS Laboratório de Arquitetura e Sistemas de Software, 19
LCR Lista de Certificados Revogados, 32

MAC Mandatory Access Control, 22
MR Magnetic Resonance, 61

OCSP Online Certificate Status Protocol, 41
OID Object Identifier, 59
OrBAC Organization Based Access Control Model, 49
OV Organizações Virtuais, 15

PACS Picture Archiving and Communication System, 12
PAP Policy Administration Point, 34
PDP Policy Decision Point, 34
PEP Policy Enforcement Point, 34
PGCA Política Geral de Controle de Acesso, 68
PIP Policy Information Point, 34
PKI Public Key Infrastructure, 27
PRA Permission Role Assignment, 49
PRP Policy Retrieval Point, 34

RBAC Role-Based Access Control, 22
REST Representational State Transfer, 40
RFC Request for Comments, 59
RIS Radiology Information System, 12

SBSeg Simpósio Brasileiro em Segurança da Informação de Sistemas Computacionais, 96
SSH Secure Shell, 18

TI Tecnologia da Informação, 18

URA User Role Assignment, 49
US Ultrasound, 61

VM Virtual Machine, 79

XACML eXtensible Access Control Markup Language, 52

# RESUMO

SILVA, Denys A. B. da. **DICOMFlowAccess: Controle de Acesso para compartilhamento de imagens médicas em ambiente aberto e distribuído**. 2019. 115f. Dissertação (Mestrado em Informática) - Programa de Pós-Graduação em Informática, Universidade Federal da Paraíba, João Pessoa, 2019.

A necessidade de associações entre entidades das mais diversas áreas de atuação para o compartilhamento de informações torna-se cada vez mais comum. Assim também acontece com a telerradiologia, vertente da telemedicina que utiliza a tecnologia da informação para emissão de diagnóstico a distância através do compartilhamento de imagens médicas. Entretanto, a infraestrutura (PACS/DICOM) existente nos departamentos de radiologia é bem consolidada em um ambiente de rede local, necessitando de adaptações para atuar em um contexto global de comunicação que utiliza a Internet como infraestrutura de interconexão entre entidades. Uma dessas adaptações é a atuação do controle de acesso às informações compartilhadas entre as entidades associadas. Observou-se limitações nas atuais propostas de controle de acesso para gerir a autenticação e autorização de informações compartilhadas em uma rede globalmente aberta e distribuída, limitando-as para atuarem numa rede com essas características. O objetivo desse trabalho foi elaborar o DICOMFlowAccess, um modelo de controle de acesso para uma rede colaborativa aberta e distribuída para a prática da telerradiologia. Para tanto, foi utilizado o Certificado Digital de Atributos especificado pela ICP-Brasil e outras tecnologias já consolidadas na Internet, como o certificado digital de identidade, a infraestrutura de e-mail e protocolos de transmissão de conteúdo. Experimentos em ambiente virtual simulando uma rede colaborativa entre entidades distintas, atestaram a sua viabilidade técnica e operacional. Concluiu-se, que o DICOMFlowAccess obteve sucesso em prover controle de acesso aos exames de imagens médicas compartilhados numa rede colaborativa aberta e distribuída, em um contexto global de comunicação, formada por entidades distintas e que utilizam a Internet como meio de interconexão.

**Palavras-Chave:** Controle de Acesso, Telerradiologia, DICOM, PACS, DICOMFlow.

# ABSTRACT

SILVA, Denys A. B. da. **DICOMFlowAccess: Access Control for sharing medical images in open and distributed environment**. 2019. 115p. Dissertação (Mestrado em Informática) - Programa de Pós-Graduação em Informática, Universidade Federal da Paraíba, João Pessoa, 2019.

The need for associations between entities from the most diverse areas for information sharing becomes increasingly common. Thus also it happens with the teleradiology, a telemedicine component that uses information technology to issue remote diagnostics through the sharing of medical images. However, the infrastructure (PACS / DICOM) in radiology departments is well consolidated in a local network environment, requiring adaptations to act in a global communication context that uses the Internet as an interconnection infrastructure between entities. One of these adaptations is the performance of access control to information shared between associated entities. Limitations were observed in current access control proposals to manage the authentication and authorization of shared information in a globally open and distributed network, limiting them to operate in a network with these characteristics. The objective of this work was to elaborate the DICOMFlowAccess, an access control model for an open and distributed collaborative network for the practice of teleradiology. For this purpose, the Digital Certificate of Attributes specified by ICP-Brazil and other technologies already consolidated in the Internet was used, as digital certificate of identity, email infrastructure and content transmission protocols. Experiments in a virtual environment simulating a collaborative network between distinct entities, attest to its technical and operational feasibility. It was concluded that DICOMFlowAccess was successful in providing access control to shared medical image exams in an open and distributed collaborative network in a global context of communication formed by distinct entities that use the Internet as a means of interconnection.

**Keywords:** Access Control, Teleradiology, DICOM, PACS, DICOMFlow.

# CAPÍTULO 1

# INTRODUÇÃO

Este capítulo introduz os desafios para estabelecer controle de acesso para uma infraestrutura assíncrona, escalável e descentralizada para o compartilhamento de imagens médicas utilizando a Internet. São apresentadas as motivações que levaram à sua elaboração, os objetivos almejados, assim como as justificativas e benefícios para tais objetivos. Ao final deste capítulo, também é apresentada a estrutura deste documento.

## 1.1 Contextualização

Com o alcance da comunicação cada vez mais global, a troca de informações entre organizações é cada vez mais comum e a Internet é o principal meio de comunicação para que isto aconteça. A Internet é um ambiente que possui características de uma Infraestrutura de Informação (II) (EDWARDS et al., 2007; BOWKER et al., 2009; HANSETH; LYYTINEN, 2010), pois, (1) é aberta, isto é, organizações podem associar-se livremente para realizar troca de informações digitais, (2) é um ambiente amplamente distribuído e descentralizado (fisicamente e logicamente), pois está presente em diversos dispositivos e localidades sem possuir uma entidade centralizadora que detenha direitos administrativos, tecnológicos ou legais sobre ela e (3) novos serviços e negócios podem surgir a partir dela.

O uso de imagens é amplamente difundido atualmente e está presente nas mais diversas áreas. Na medicina para a realização de exames e produção de laudos, no planejamento estratégico de um governo para a construção de novas estradas ou por empresas ligadas ao agronegócio poderem identificar a melhor localização para iniciar o cultivo da soja. O que estas imagem possuem em comum é que diferente das imagens que existem em redes sociais ou portais de notícias, elas geram um grande volume de dados e possuem informações críticas que na maioria das situações devem ser preservadas de acessos não autorizados. Principalmente, as obtidas através de exames de imagens médicas, pois, possuem informações sensíveis de pacientes e que devem ser preservadas de acessos que não tenham sido previamente autorizados.

Transportar essas imagens entre parceiros tem sido um grande desafio que motiva empresas de tecnologia e a comunidade científica na pesquisa de soluções para atender tal demanda, particularmente na telerradiologia (MUN et al., 2005; BENJAMIN et al., 2010), que é uma das áreas de telemedicina que utiliza tecnologias da informação (e.g. computadores, aplicativos, meios de comunicação) com o objetivo de permitir o diagnóstico a distância através do envio de imagens médicas. Neste contexto, o fator crítico é a distância (CFM-2.107/14, 2014). Um dos resultados dessa parceria foi o estabelecimento do padrão de Comunicação de Imagens Digitais em Medicina (do inglês, *Digital Imaging and Communications in Medicine* - DICOM) (DICOM, 2017), que estabelece uma linguagem comum entre equipamentos, mesmo que de marcas diferentes, para o tratamento, armazenamento e transmissão de imagens médicas. O DICOM é suportado pelo Sistema de Comunicação e Arquivamento de Imagens (do inglês, *Picture Archiving and Communication Systems* - PACS), que é um conjunto de tecnologias, como computadores, periféricos e aplicativos que se conectam às modalidades (e.g. equipamento para raio-x, ultra-som, ressonância magnética) para obtenção do exame de imagem médica (HUANG, 2011).

Entretanto, o conjunto de tecnologias PACS/DICOM é parte de um ambiente mais complexo para serviços em saúde, denominado Tecnologia da Informação em Saúde (do inglês, Health Information Technology - HIT). O HIT abrange toda a tecnologia aplicada em saúde

e suporta sistemas de gerenciamento de informações relacionadas a médicos, pacientes, exames, fornecedores e parceiros. Essa infraestrutura para prática dos cuidados da saúde é modular e outros subsistemas podem coexistir. A exemplo do Sistema de Informação Hospitalar (do inglês, Hospital Information System - HIS) e o Sistema de Informação Radiológica (do inglês, Radiology Information System - RIS). O PACS/DICOM atua diretamente com o RIS. A Figura 1 apresenta o *workflow* para a prática telerradiológica e nela (destacado em vermelho) podemos visualizar em que fase do processo a infraestrutura PACS/DICOM está posicionada.

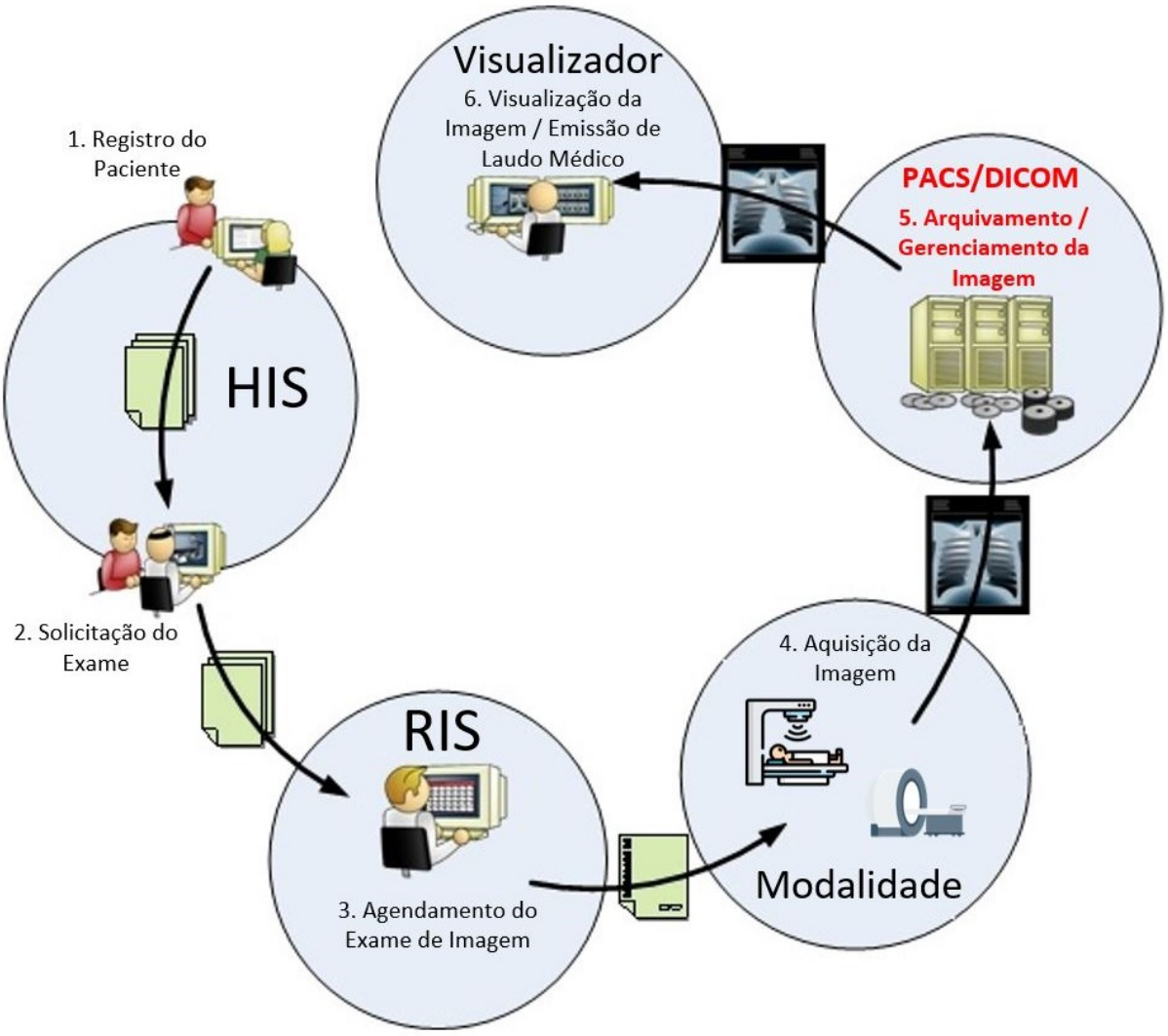



Figura 1: Etapas de um *workflow* radiológico.
Fonte: Adaptada do Google Images

Atualmente existe uma demanda crescente pelo compartilhamento de imagens médicas

para fins de emissão de laudos, estudos ou investigações. Tais imagens podem ser repassadas para pesquisadores ou estudantes com a finalidade de desenvolver melhores tratamentos e prestação de serviços de saúde com maior qualidade (RAY et al., 2016). O compartilhamento de informações entre profissionais de saúde situados em locais geograficamente distantes um do outro tem o potencial de gerar efetivamente grande economia de tempo e recursos, além de trazer melhorias na eficácia clínica. Contudo, apesar do avanço das tecnologias para transmissão de dados, a infraestrutura PACS/DICOM foi projetada entre as décadas de 80 e 90, período em que as redes locais ainda estavam se estabelecendo (HUANG, 2011).

Esse modelo é amplamente consolidado quando a comunicação acontece em uma rede local ou até mesmo em um único domínio de segurança, mesmo que fisicamente distribuído. Entretanto, apresenta algumas dificuldades quando o contexto global de comunicação se torna necessário, como a falta de padronização no envio das imagens médicas, na emissão dos laudos, na solicitação de uma segunda opinião, em como será feito o controle de acesso nas informações compartilhadas ou qual o melhor meio de transmissão. Diante desses obstáculos sociotécnicos, criam-se, mesmo que involuntariamente, grandes forças para romper o contexto da comunicação local para a comunicação global (MOTTA, 2014). O protocolo DICOM também é capaz de prover implementações personalizadas dos sistemas PACS, possibilitando uma customização do modelo aplicado em cada departamento para atender as necessidades locais, entretanto, diante das características de cada implementação, construir uma infraestrutura que possibilite a interoperabilidade desses departamento torna-se um grande desafio.

O DICOMFlow (ARAUJO, 2017) é um *gateway* para prover essa interligação entre entidades de saúde (e.g. hospitais, clínicas) a fim de criar uma infraestrutura capaz de tornar possível a interoperabilidade entre departamentos de telerradiologia. Mas como relatado pelo próprio autor, apresenta algumas limitações para prover um controle de acesso com granularidade fina e escalabilidade. Vários outros estudos existem com propostas para solucionar essa lacuna, não necessariamente para a prática da telerradiologia. Alguns deles serão apresentados e discutidos no Capítulo 2, na Seção de Trabalhos Relacionados.

## 1.2 Motivação

A telerradiologia está estabelecendo rapidamente sua presença como uma solução eficaz para o problema de provisão de serviços radiológicos em locais remotos (TIE; KOCZWARA, 2004). Embora tenham surgidos avanços significativos ao longo dos anos com a parceria academia-indústria somada a evolução nas tecnologias de comunicação, não se observa uma infraestrutura capaz de prover uma comunicação global entre entidades de saúde (MOTTA, 2014). Considerando as características singulares da telerradiologia, como o acesso remoto podendo ser simultâneo, originando-se em múltiplos locais e o compartilhamento de informações médicas, os dados compartilhados (exames de imagens médicas, prontuários eletrônicos e laudos) são sensíveis, pois carregam informações que devem ser mantidas fora do acesso de pessoas não autorizadas. Diante disto, a atuação eficiente do mecanismo de controle de acesso nesta infraestrutura é primordial para o êxito de sua implementação.

Com o advento das Organizações Virtuais (OV)(VILLARRUBIA et al., 2017; CHILD, 2015), a forma de estabelecer associações entre entidades utilizando a Internet como meio de interconexão ganha uma nova dinâmica (FRANCO et al., 2018; DU; EL-GAFY, 2012). Tais associações podem ser estabelecidas de forma espontânea e sua duração passa a ser acordada entre as partes envolvidas. Podendo durar anos ou o tempo necessário para realizar uma simples atividade. Necessariamente, OV são criadas para que as entidades associadas possam fazer a troca de informações entre si com a finalidade de executar alguma atividade. Um exemplo do estabelecimento de uma OV é quando acontece algum desastre natural e entidades como departamento de polícia, defesa civil, corpo de bombeiros ou organizações sociais, se mobilizam, associam-se, e trocam informações a respeito do desastre. E, nessas associações, a atuação do mecanismo de controle de acesso as informações compartilhadas é de vital importância para a segurança dos dados.

Contudo, no âmbito da telerradiologia e da dinâmica das associações na rede colaborativa como propomos, surgem duas particularidades. (1) Enquanto o conceito de Organizações Virtuais estabelece um modelo de associações entre entidades distintas (DU; EL-GAFY, 2012), nossa proposta vai um pouco mais além e visa estabelecer associações entre os mem-

bros dessas entidades de forma independente da infraestrutura de suas entidades de origem. No exemplo da OV criada para atuar diante de um desastre natural, quando, por exemplo, um policial vai trocar informações com um bombeiro, ambos devem fazer uso da infraestrutura de suas entidades para comunicar-se e do estabelecimento da associação entre elas. O que nós pretendemos com esse trabalho é retirar a dependência da infraestrutura da entidade associada e criar associações diretas entre pessoas, que no nosso cenário, são os médicos radiologistas e os dados compartilhados são exames de imagens médicas e laudos especializados. De fato, o que se propõe nesse trabalho é a criação de uma Organização Virtual, não entre entidades, e sim entre pessoas. (2) Outro aspecto relevante para nossa proposta, e ponto central deste trabalho, é definir o funcionamento do mecanismo de controle de acesso das informações compartilhadas. Visto que, as propostas pesquisadas de soluções para prover controle de acesso numa infraestrutura semelhante a aqui idealizada, apresentaram limitações em atender os pré-requisitos estabelecidos para as funcionalidades do mecanismo de controle de acesso numa rede colaborativa aberta e distribuída para a prática da telerradiologia. Detalharemos essas propostas futuramente.

## 1.3 Objetivos

Este trabalho objetiva desenvolver e validar o DICOMFlowAccess (DFA), um modelo de controle de acesso que não necessita de conexões ativas para seu funcionamento, independe de uma entidade centralizadora para validação de solicitações de acesso e baseia-se em atributos para analisar solicitações de acesso a imagens médicas compartilhadas.

Para que o objetivo geral seja alcançado, foi efetuada uma subdivisão com objetivos mais específicos, apresentados a seguir:

**Objetivo1.** Possibilitar que o originador do exame de imagem médica tenha controle sobre seu acesso, mesmo que já compartilhado e revogando acessos previamente autorizados quando necessário.

**Objetivo2.** Proporcionar a liberdade de acesso de forma segura à imagem desejada, deste que autorizado pelo originador e independente de disponibilidade do mesmo.

**Objetivo3.** Atender a escalabilidade de uma infraestrutura para o compartilhamento de imagens médicas em ambiente aberto e distribuído.

**Objetivo4.** Ser independente de uma base de dados centralizada para armazenar informações[1] de usuários para fins de autenticação e autorização de acesso.

**Objetivo5.** Testar o controle de acesso no DICOMFlow (ARAUJO, 2017), arquitetura que contempla as características necessárias na formação de uma infraestrutura aberta e distribuída para a pratica da telerradiologia, a fim de atestar sua eficácia.

O termo "escalabilidade", utilizado no Objetivo 3, em um ambiente computacional pode possuir múltiplas interpretações: como a capacidade de aumento no número de requisições em um servidor WEB ou a quantidade de nós que uma infraestrutura de balanceamento de carga pode possuir. Enquanto o entendimento comum de escalabilidade remete a questões tecnológicas associadas a desempenho ou disponibilidade, o ambiente em que este modelo de controle de acesso se propõe a atuar é a infraestrutura proposta pelo DICOMFlow (ARAUJO, 2017) para prática da telerradiologia. No ambiente proposto, entidades de saúde e possíveis parceiros podem associar-se livremente para realizar atividades e seu crescimento é indeterminado, livre de escala, ou seja, novos nós podem agregar-se a essa rede de colaboração para proverem imagens médicas, emitirem laudos, compartilharem uma segunda opinião de um laudo e demais atividades associadas a telerradiologia.

O DICOMFlowAccess (DFA) propõe-se a ser um modelo de controle de acesso escalável que atende o crescimento da rede de colaboração criada pelo DICOMFlow para a prática da telerradilogia ou, com os devidos ajustes, atuar em outros tipos de rede colaborativas que possuam características semelhantes as existentes na infraestrutura criada pelo DICOMFlow.

[1]Conforme descrito em (AMARAL, 2016), existe uma diferença entre "dado" e "informação". O **dado** é um registo que não foi contextualizado e inicialmente não faz sentido algum. Enquanto **informação** é um registro (dado) que foi contextualizado ou interpretado e passa a ter um significado. No âmbito deste trabalho, qualquer registro, seja ele eletrônico ou não, mesmo que não contextualizado, será referenciado como **informação**.

## 1.4 Justificativa

Os desafios para tornar a prática de telerradiologia um serviço dentro de uma II agrega um conjunto de benefícios, seja para pacientes e seus familiares, profissionais especializados ou investidores (DRNASIN et al., 2009). Criar uma infraestrutura de informação para a prática da telerradiologia exige que vários requisitos (técnicos e legais) sejam contemplados. O controle de acesso é um deles. A maneira de implementar o controle de acesso que propomos independe de uma conexão ativa entre entidades ou de uma base de dados centralizada. Isto é possível principalmente pela utilização de certificados digitais (Certificado Digital de Identidade (CD) e Certificado Digital de Atributos (CA)), que por si só já fazem a identificação e liberação de acesso caso as políticas implementadas sejam atendidas. Detalhes desses certificados (e outras tecnologias que fazem parte de nossa solução ) são apresentados no Capítulo 2 e como eles são criados e utilizados em nossa solução será apresentado do Capítulo 3.

Com o modelo proposto, parcerias podem ser formadas e outros tipos de serviços para dar suporte a telerradiologia podem emergir na II, como o processamento ou armazenamento de imagens por instituições externas ao hospital ou clínica que geram o exame de imagem. O acesso ao exame de imagem funcionará como o mecanismo de *voucher*, onde o originador da imagem, ou entidade autorizada por ele, fornece um certificado de atributos para o requerente indicando o local aonde a imagem está armazenada e de posse deste certificado o requerente usará o seu certificado digital para atestar sua identidade e o certificado de atributos para autorizar seu acesso ao exame requerido. No processo de controle de acesso, o certificado digital será usado para o procedimento de autenticação e o certificado de atributos para o de autorização.

Desta forma, não é necessária uma conexão ativa entre o originador do exame de imagem e a entidade que pretende obtê-lo. Outra possibilidade é a necessidade do originador da imagem querer revogar um direito de acesso. Nesta situação, basta revogar o certificado de atributos que foi emitido para o requerente e o mecanismo de controle de acesso fará a identificação que o certificado foi revogado pelo emissor. Todo o transporte do exame da imagem pode ser realizado utilizando HTTP, FTP ou SSH, serviços já consolidados na atual

estrutura da Internet.

Os benefícios com o surgimento de uma II para a prática da telerradiologia são muitos, como o alcance a áreas que não possuem recursos mínimos (médicos especializados ou um infraestrutura de Tecnologia da Informação (TI)) ou geograficamente mais dispersas, tornar mais atrativo os investimentos, agilidade dos laudos e avanço nas pesquisas de novos tratamentos para as enfermidades.

## 1.5 Metodologia

Como mostrado anteriormente, vários aspectos são necessários para a implementação do controle de acesso em uma infraestrutura da informação. Este trabalho usará as abordagens investigativas e experimentais para a proposta e desenvolvimento de uma solução aplicável.

Durante as investigações por tecnologias e trabalhos relacionados foram pesquisadas propostas de controle de acesso que fazem a utilização de certificados digitais para prover formas de autenticação e autorização e/ou que busquem atuar em uma estrutura aberta e distribuída, não necessariamente para a prática da telerradiologia, mas que atue em uma infraestrutura similar a que já descrevemos. Os experimentos foram divididos em duas etapas. (1) Atestar a viabilidade técnica de nossa solução com a finalidade de constatar que é possível criar um controle de acesso baseado em certificados digitais e (2) mostrar que nossa solução é escalável e descentralizada para atuar em um ambiente aberto e distribuído como a Internet, em particular para a da prática da telerradiologia, utilizando a II proposta pelo DICOMFlow em (ARAUJO, 2017). Os experimentos que visam testar as funcionalidades do DICOMFlowAccess foram realizados em ambiente virtual que simula a rede de colaboração para a prática da telerradiologia como propomos. Os pormenores da rede para a prática da telerradiologia em ambiente global e as tecnologias utilizadas para a criação do ambiente virtual que simula esta rede serão apresentadas futuramente neste trabalho nos capítulos três e quatro, respectivamente.

As questões de pesquisas deste trabalho objetivam buscar por propostas de Controle de

Acesso para dados compartilhados em Organizações Virtuais. Algumas dessas questões de pesquisa foram elaboradas baseando-se nos conceitos de Infraestrutura de Informação. E outras estão relacionadas as particularidades de nossa pequisa.

1. O mecanismo/modelo de controle de acesso proposto é capaz de permitir associações dinâmicas entre entidades?

2. O mecanismo/modelo de controle de acesso é independente de base de dados centralizada?

3. O mecanismo/modelo de controle de acesso é independente do estabelecimento de sessões?

4. O mecanismo/modelo de controle de acesso proposto é capaz de permitir controle aos dados, mesmo que já compartilhados?

5. O mecanismo/modelo de controle de acesso proposto é capaz de atender prováveis particularidades entre membros associados?

6. O mecanismo/modelo de controle de acesso proposto usa certificados digitais?

7. O mecanismo/modelo de controle de acesso proposto possui ligação com cuidados em saúde?

O DICOMFlowAccess foi desenvolvido no Laboratório de Arquitetura e Sistemas de Software (LARQSS), no Campus IV da Universidade Federal da Paraíba. A equipe que irá conduzir o desenvolvimento é composta por 2 (dois) analistas de sistemas e 1 (um) administrador de redes de computadores. Todos são membros da equipe que atua no LARQSS. Os mecanismos de busca por documentações que irão auxiliar na pesquisa serão os seguintes:

- IEEEXplore[2];
- Science Direct[3];
- PubMed[4];

[2]http://www.ieeexplore.ieee.org
[3]http://www.sciencedirect.com
[4]https://www.ncbi.nlm.nih.gov/pubmed/

- Google Scholar[5].

O acesso irrestrito a essas plataformas de busca utilizando a rede de dados da Universidade Federal da Paraíba foi o que motivou a escolha dos mecanismos acima.

## 1.6 Estrutura da Dissertação

Os próximos capítulos deste trabalho estão divididos conforme a estrutura abaixo.

**Capítulo 2:** Serão apresentados os conceitos e tecnologias utilizadas para o desenvolvimento de nossa solução e a apresentação de alguns trabalhos correlatos. A análise dos pontos positivos e negativos de cada trabalho relacionado também é feita.

**Capítulo 3:** Apresenta o DICOMFlowAccess de uma forma mais minuciosa.

**Capítulo 4:** Descreve os experimentos utilizados para a validação da nossa proposta.

**Capítulo 5:** Conclui o trabalho, discute os resultados dos experimentos e apresenta possíveis trabalhos futuros.

[5]https://scholar.google.com.br/

# CAPÍTULO 2

# FUNDAMENTAÇÃO TEÓRICA E TRABALHOS RELACIONADOS

Este capítulo tem a finalidade de expor conceitos e tecnologias que formaram a base para a construção de um controle de acesso capaz de atender as necessidades de uma infraestrutura distribuída não só em seus aspectos físicos (e.g. servidores, bases de dados ou serviços), mas em seu aspecto lógico, onde não existe uma centralização, ou seja, um único responsável pelas informações de usuários (e.g. login e senha) para fins de validação no controle de acesso a um determinado recurso (e.g. arquivo, impressora, serviço). Inicialmente (Seção 2.1), será feita uma explanação acerca do conceito de controle de acesso e alguns modelos já propostos que servirão de base para a construção do nosso modelo. Na sequência (Seção 2.2 e 2.3), serão apresentas as principais tecnologias utilizadas para a construção do controle de acesso proposto e, em seguida (Seção 2.4), serão discutidos trabalhos relacionados a nossa pesquisa. Por fim, serão feitas as considerações finais.

## 2.1 Controle de acesso

O controle de acesso é uma ferramenta utilizada na proteção de determinado recurso e existe desde os primórdios da humanidade. Desde o bater palmas em frente a uma residência e fazer o reconhecimento da voz de quem chama até o uso da íris para atestar a identidade de uma pessoa. Apesar disto, algo é imutável mesmo com todos esses séculos de utilização: o controle de acesso tem duas necessidades básicas, (1) saber se **"você é quem você afirma ser"** e (2) saber **"o que você quer fazer"** (SANDHU; SAMARATI, 1994; SAMARATI; VIMERCATI, 2000; BUTLER et al., 2000). E essas necessidades criaram dois processos que dão sustentação ao conceito de controle de acesso, (1) autenticação, que faz a verificação de identidade do solicitante respondendo a pergunta "você é quem você afirma ser?"e (2) autorização, processo que ocorre após a autenticação e, baseado em regras de acesso, determina se o solicitante tem permissão para acessar um recurso, respondendo a pergunta "o que você quer fazer?". Na Figura 2 podemos visualizar com mais clareza essas etapa.

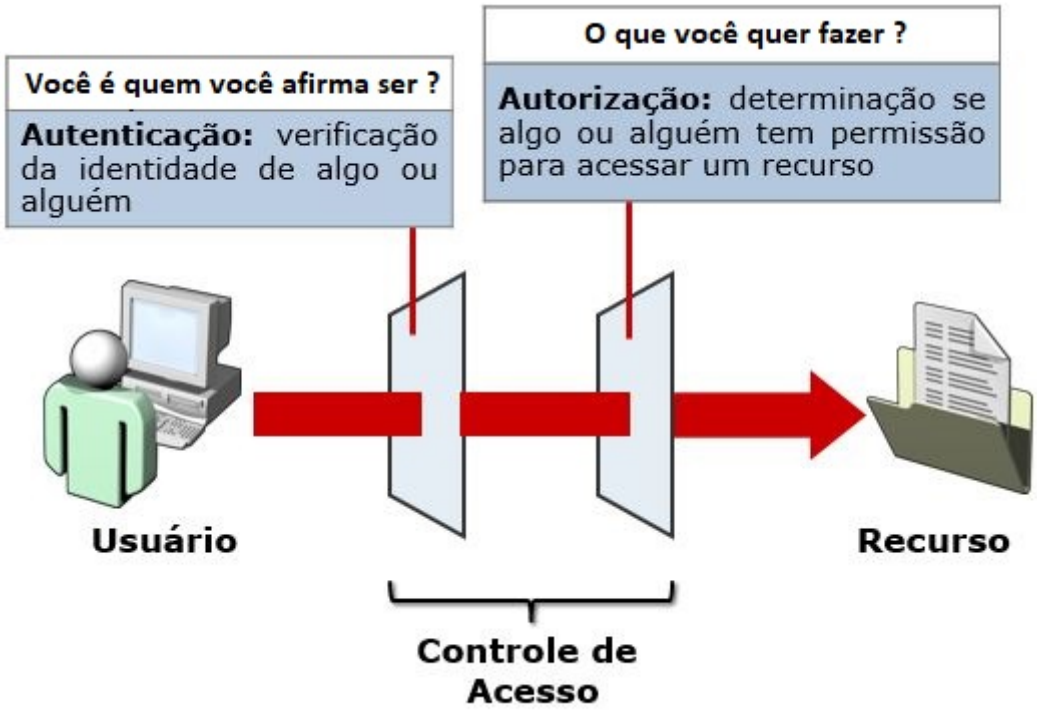



Figura 2: Etapas de um controle de acesso
Fonte: Próprio autor

O controle de acesso está posicionado entre o usuário que faz a solicitação e o recurso solicitado. Através de suas políticas de controle de acesso, ele faz o tratamento da requisição

e toma a decisão de permitir ou não o acesso ao recurso solicitado. Regras de acesso são as políticas que envolvem o uso de um determinado recurso, utilizando o exemplo do ato de "bater palmas", um pai pode orientar um filho a só abrir a porta para sua mãe. Está é a regra de acesso criada, caso outra pessoa solicite entrada na casa o filho irá aplicar a regra imposta pelo pai e não abrirá a porta, ou a regra de acesso poderia ser "não abra a porta para ninguém antes das 18h:00", regra que já utiliza o fator tempo, ou "só abra para alguém da família", que implementa um conceito de grupo. Como podemos observar, existem várias aplicações para o controle de acesso e em consequência disso vários modelos foram criados ao longo dos anos, sendo que alguns desses modelos dão sustentação para a criação de nossa solução e serão apresentados na seção a seguir.

## 2.2 Modelos de Controle de Acesso

Começando com a matriz de acesso de Lampson no final da década de 1960, foram propostas dezenas de modelos de controle de acesso. Apenas três alcançaram sucesso na prática e permitiram variações para a criação de novos modelos: Controle de Acesso Discricionário (do inglês Discretionary Access Control - DAC) (SANDHU; SAMARATI, 1994), Controle de Acesso Obrigatório (do inglês Mandatory Access Control - MAC) (SANDHU, 1993) e Controle de Acesso Baseado em Papéis (do inglês Role-Based Access Control - RBAC) (FERRAIOLO et al., 2001). Enquanto o DAC e o MAC surgiram no início da década de 1970, o RBAC demorou mais para desenvolver bases sólidas (JIN et al., 2012). Uma das variações desses modelos é o Controle de Acesso Baseado em Atributos (do inglês, Attribute-Based Access Control - ABAC), poderosa ferramenta que permite maior granularidade nas regras de controle de acesso e é recurso essencial para nossa solução. Nas subseções a seguir discutiremos a respeito dos modelos acima citados.

### 2.2.1 DAC - Discretionary Access Control

O modelo de Controle de Acesso Discricionário é um modelo no qual todo usuário, ou programa atuando em seu nome, tem a permissão de especificar qual será o tipo de acesso que outros usuários terão em recursos ou informações de sua propriedade (SAMARATI; VIMERCATI, 2000).

Políticas discricionárias aplicam o controle de acesso baseando-se na identificação do usuário e em um grupo de regras que determinam quem poderá e como poderá acessar um determinado recurso. Um exemplo de aplicação de um modelo discricionário está presente no sistema de arquivos do Linux, na qual as permissões são atribuídas a um usuário ou grupo de usuários com os modos de acessos *r (read), w (write) e x (execute)*.

### 2.2.2 MAC - Mandatory Access Control

O modelo de Controle de Acesso Mandatório faz a restrição de todos os acessos ao sistema baseando-se em regras obrigatórias que são impostas por uma autoridade central (SAMARATI; VIMERCATI, 2000). Os usuários que são proprietários de um objeto do sistema não conseguem realizar quaisquer alterações nas permissões que sejam contrárias as regras impostas pelo administrador do sistema. A forma mais comum de política mandatória é a segurança multinível, que é baseada na classificação de todos os usuários e objetos do sistema, rotulando-os com um nível de segurança (OSBORN, 1997). Os níveis comuns de classificação no sentido *top-down* são: Top Secret, Secret, Confidential, Restricted, Official, Unclassified, Clearance e Compartmented Information.

O modelo MAC associa cada usuário e objeto (e.g arquivo) do sistema a um nível de classificação, apenas quando os níveis são equivalentes ou superior é que o acesso é feito. Por exemplo, um usuário é classificado no nível *secret*, então ele poderá acessar qualquer recurso que seja classificado como *secret* e como todos os outros níveis abaixo de *secret*. Essa abordagem é centralizada e apenas quem administra o sistema é quem poderá alterar as permissões de usuários e objetos. Mesmo que um usuário tenha total controle sobre um determinado objeto, a alteração da política de acesso a esse objeto só poderá ser feita pelo administrador. Esse modelo de controle de acesso é comumente utilizada em informações militares.

### 2.2.3 RBAC - Role-Based Access Control

O modelo de Controle de Acesso Baseado em Papéis teve sua discussão iniciada na década de 1990 e ganhou rapidamente aceitação por parte do mercado. Emergiu como uma das principais tecnologias para gerência e controle em sistemas de larga escala em grandes corporações (SAMARATI; VIMERCATI, 2000). O ponto central do RBAC é que a gestão de controle de acesso é baseada em papéis existentes dentro de uma organização e aos usuários são designados esses papéis, com esse modelo o papel desempenhado por determinado usuário é determinante para o acesso a um recurso e não somente a sua identidade.

A principal vantagem sobre o modelo DAC é que no RBAC as permissões são dadas aos papéis, que comumente possui uma quantidade bem inferior a de usuários, já em relação ao modelo MAC a vantagem está em ser mais flexível, já que no MAC todo objeto deve ser rotulado com uma classificação e a alteração desse rótulo só poderá ser feita por uma entidade central, tornado-o um modelo de difícil aplicação em ambiente comercial.

A relação entre usuário-papel é de muitos-para-muitos, onde um usuário pode fazer parte de vários papéis e um papel pode ser atribuído a vários usuários. Um exemplo que sistema que utiliza o modelo RBAC é o Active Directory da Microsoft.

### 2.2.4 ABAC - Attribute-Based Access Control

O modelo de Controle de Acesso Baseado em Atributo define um paradigma de controle de acesso pelo qual os direitos de acesso são concedidos aos usuários através do uso de políticas que combinam atributos. As políticas podem usar qualquer tipo de atributos (atributos de usuário, atributos de recursos, objetos, atributos de ambiente etc.). Este modelo suporta lógica booleana em que as regras contêm instruções *"if"* e *"then"* sobre quem está fazendo a solicitação, o recurso e a ação. Por exemplo: **SE** o solicitante é um gerente, **E** está acessando entre às 14h:00 e 19h:00 **E** está no endereço IP 200.123.123.123, **ENTÃO** permita o acesso de leitura / gravação a dados estratégicos.

Ao contrário do RBAC, que emprega funções pré-definidas que possuem um conjunto

específico de privilégios associados a eles e aos quais os usuários são atribuídos, a diferença principal com o ABAC é o conceito de políticas que expressam um conjunto de regras booleanas complexas que podem avaliar muitos atributos diferentes. Os valores dos atributos podem ser multivalorados ou atômicos (HU et al., 2013). O modelo de controle de acesso proposto nesse trabalho e que será apresentado no Capítulo 3 utiliza este tipo de funcionalidade para gerenciar acessos. Na próxima seção serão introduzidos os conceitos relacionados com Certificação Digital.

## 2.3 Certificação Digital

Nesta seção serão apresentados um conjunto de tecnologias que darão suporte a implementação da segurança da informação durante as transações existentes em nossa solução.

### 2.3.1 Infraestrutura de Chaves Públicas do Brasil - ICP-Brasil

Uma Infraestrutura de Chave Pública (do inglês, Public Key Infrastructure - PKI) é a base dos quatro principais elementos da segurança digital: autenticação, integridade, confidencialidade e não repúdio. É formada por um conjunto de recursos humanos, físicos, virtuais, e procedimentais necessários para prover a criação, manutenção, validação e revogação de certificados digitais (CD) (ADAMS; LLOYD, 2003). A estrutura de uma ICP é hierárquica e possui várias entidades, semelhante a uma estrutura de árvore de dados, onde um nó primário, Autoridade Certificado Raiz (AC-Raiz), deriva nós secundários, as Autoridades Certificadoras (AC) e outros componentes básicos que são descritos a seguir.

1. **Autoridade Certificadora Raiz (AC-Raiz):** É a autoridade inicial em toda cadeia de certificação. É quem executa as políticas de certificados e as normas técnicas e operacionais que são aprovadas pelo comitê gestor da ICP-Brasil. A sua função é emitir, expedir, gerenciar, revogar e distribuir os certificados das autoridades certificadores que estão posicionadas a um nível imediatamente subsequente ao seu.

2. **Autoridade Certificadora (AC):** entidade pública ou privada que é subordinada à hierarquia da ICP-Brasil, que assim como a AC-Raiz é responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais.

3. **Autoridade de Registro (AR):** é responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC, tem por objetivo o recebimento, a validação, o encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.

4. **Autoridade Certificadora de Tempo (ACT):** é uma entidade na qual os usuários de serviços de Carimbo do Tempo confiam para emissão dos mesmos. A ACT tem a responsabilidade geral pelo fornecimento do Carimbo do Tempo, conjunto de atributos fornecidos pela parte confiável do tempo que, associado a uma assinatura digital, confere provar a sua existência em determinado período.

A hierarquia da ICP-Brasil é complexa e passa por constante modificações a medida que novas entidades vão se credenciando. Uma visualização completa da hierarquia atual da ICP-Brasil pode ser encontrada em http://www.iti.gov.br/images/repositorio/autoridades-certificadoras/estrutura_completa.pdf. Na Figura 3 é possível visualizar de forma resumida a hierarquia da ICP-Brasil.

O processo de emissão do Certificado Digital de Identidade da ICP-Brasil é iniciado pelo solicitante escolhendo uma entre as Autoridades Certificadoras (AC) vinculadas a ICP-Brasil. Neste momento, o tipo de certificado (A1 ou A3, pessoa física ou jurídica) é escolhido e o solicitante deve pessoalmente ir até uma Autoridade de Registro (AR) para apresentar os documentos necessários indicados pela AC para a emissão do certificado. Esse processo é denominado de avaliação presencial e será agendado diretamente pela AR. Após o processo de validação dos documentos apresentados, o certificado solicitado será emitido. Este é o processo para se obter um certificado válido na ICP-Brasil.

Contudo, existe outro mecanismo para se obter um certificado digital de identidade. É a criação de um certificado auto-assinado, em que uma entidade cria seu certificado para uso em suas aplicações. O processo de assinar documentos, por exemplo, funcionará sem maiores problemas, entretanto, este certificado ou documentos por ele assinados, não terão validade jurídica, pois, a entidade que o gerou não participa da hierarquia da ICP-Brasil.

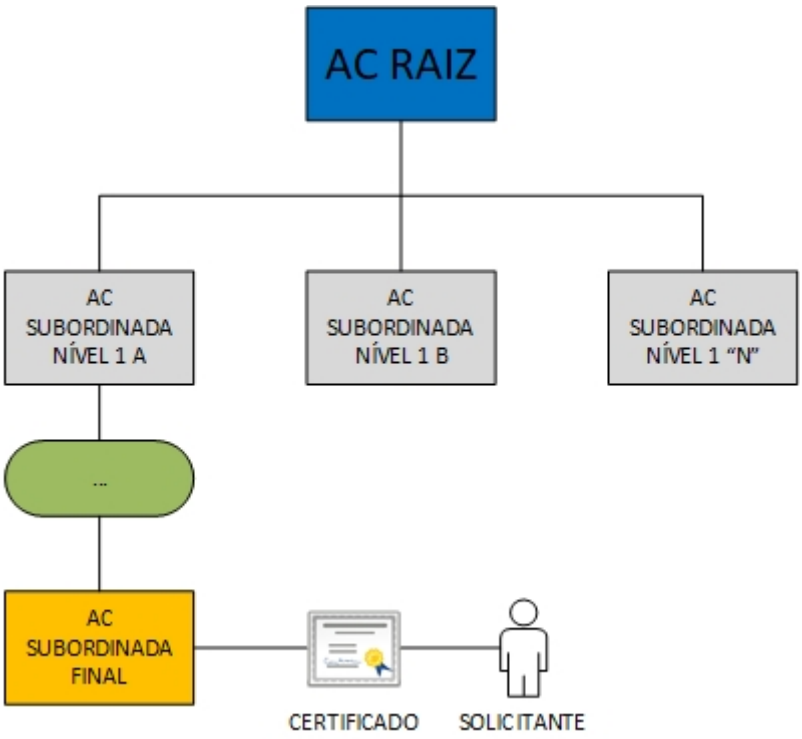



Figura 3: Versão resumida da hierarquia da ICP-Brasil
Fonte: Próprio autor.

Esse tipo de certificado é muito útil para validação de soluções como a que propomos e, inicialmente, será utilizado na elaboração do DFA.

O Conselho Federal de Medicina (CFM) é uma Autoridade Certificadora da ICP-Brasil e através da RESOLUÇÃO CFM Nº 1.821/2007 (CFM-1.821/07, 2007) determinou que ele será a entidade responsável pela distribuição dos CRM-Digital para os médicos interessados em utilizarem essa tecnologia. Na implementação em outros países, deve-se observar qual a orientação de seus Conselhos de Medicina para o utilização de certificados digitais. Essa é uma medida direcionada para a validade jurídica da solução, visto que não há restrições técnicas quanto a entidade emissora dos certificados utilizados.

### 2.3.2 Criptografia

Conforme dito em (NAKAMURA; GEUS, 2007) e (STALLINGS, 2008), a criptografia é a ciência que estuda como manter o processo de troca de mensagens entre entidades mais seguro e tem importância cada vez maior dentro das organizações. O ato de criptografar passa

por duas etapas, a **cifragem** (*encryption*), que é o o processo para disfarçar a mensagem original, o texto claro (*plaintext*), de tal modo que sua informação é escondida em uma mensagem como texto cifrado (*ciphertext*), enquanto a **decifragem** (*decryption*) é o processo de trazer o texto cifrado ao seu estado de texto claro.

Esses processos (cifragem e decifragem) usam algoritmos com funções que transformam os textos claros, que são entendíveis a interpretação humana, em texto cifrados, que são inteligíveis ao homem e cuja decifragem é computacionalmente difícil sem o conhecimento de um segredo específico, a chave.

#### 2.3.2.1 Tipos de Criptografia

Os algoritmos modernos usam uma chave para controlar o ato de cifrar e decifrar e a forma de utilização dessa chave é que determina qual o tipo de criptografia aplicado. A seguir descrevemos os dois principais mecanismos aplicados atualmente.

1. **Criptografia com chave simétrica:** Algoritmos de chave simétrica são algoritmos para criptografia que usam uma mesma chave criptográfica para cifragem de texto puro e decifragem de texto cifrado. A chave, na prática, representa um segredo compartilhado entre duas ou mais partes que pode ser usado para manter uma ligação de informação privada. Na Figura 4 pode-se observar o funcionamento deste tipo de utilização das chaves.

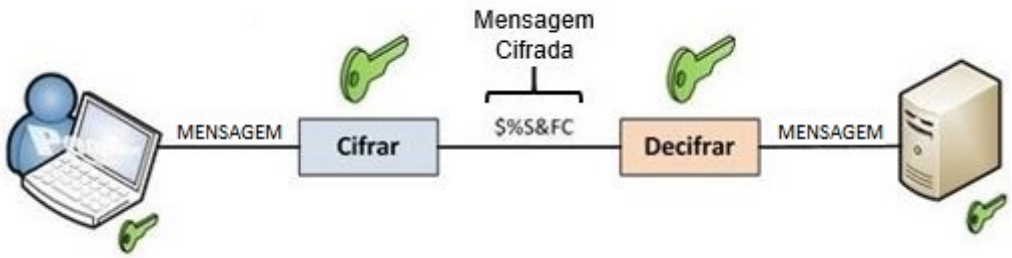



Figura 4: Criptografia Simétrica
Fonte: Adaptada do Google Images

2. **Criptografia com chave assimétrica:** A criptografia assimétrica, também conhecida por criptografia de chave pública, é baseada no uso de pares de chaves. As duas chaves

são relacionadas através de um processo matemático que usa funções unidirecionais para a codificação da informação. Uma chave, chamada chave pública, é usada para codificar, enquanto a outra, chamada chave privada, é usada para descodificar. Uma mensagem codificada com uma chave pública só pode ser decifrada pela outra chave, a privada, com a qual está relacionada. Na Figura 5 podemos observar a utilização do par de chaves para prover uma comunicação criptografada.

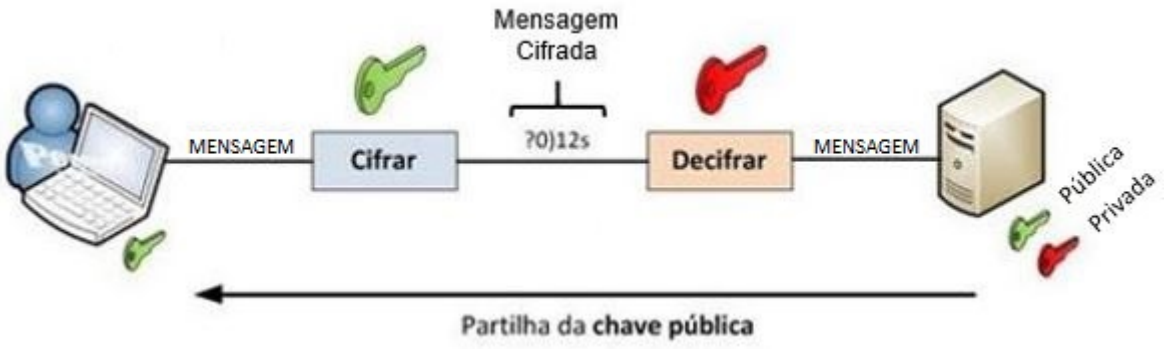



Figura 5: Criptografia Simétrica
Fonte: Adaptada do Google Images

#### 2.3.2.2 Resumo Criptográfico

Resumo Criptográfico, também conhecido como *hash* ou função *hash* tem a finalidade de reduzir um fluxo de dados de tamanho variável em um fluxo de dados de tamanho fixo através de funções matemáticas reversíveis (STALLINGS, 2008). Funções *hash* são largamente utilizadas na busca por elementos em bases de dados, na verificação da integridade de arquivos obtidos na Internet ou no armazenamento e/ou transferência de senhas.

A função *hash* pode ser utilizada no envio de um documento digital por exemplo. Antes de enviar o documento, o emissor gera o *hash* e o envia para o destinatário e, posteriormente, envia o documento propriamente dito. Após receber este documento, o destinatário gera novamente o *hash* e faz a comparação com o *hash* enviado anteriormente pelo emissor. Caso os valores sejam iguais, isso significa que o conteúdo do documento não sofreu alterações, caso contrário, houve alteração ou perda de dados.

#### 2.3.2.3 Assinatura Digital

A Assinatura Digital é uma tecnologia que serve para assinar qualquer documento eletrônico. Tem validade jurídica inquestionável e equivale a uma assinatura de próprio punho. É uma tecnologia que utiliza a criptografia assimétrica e vincula um certificado digital ao documento eletrônico que está sendo assinado pelo signatário. Assim, dá garantias de integridade e autenticidade. Normalmente é utilizada em conjunto com o resumo criptográfico que foi apresentado na subseção anterior. Como assinar grandes volumes de dados torna o processo lento e inviável, o resumo criptográfico (*hash*) de uma mensagem é gerado e posteriormente assinado com a chave privada do emissor, desta forma a assinatura digital garante a autenticidade da mensagem e o resumo criptográfico a integridade dos dados. A Figura 6 ilustra de forma simplificada o processo de assinatura digital do resumo criptográfico de uma informação.

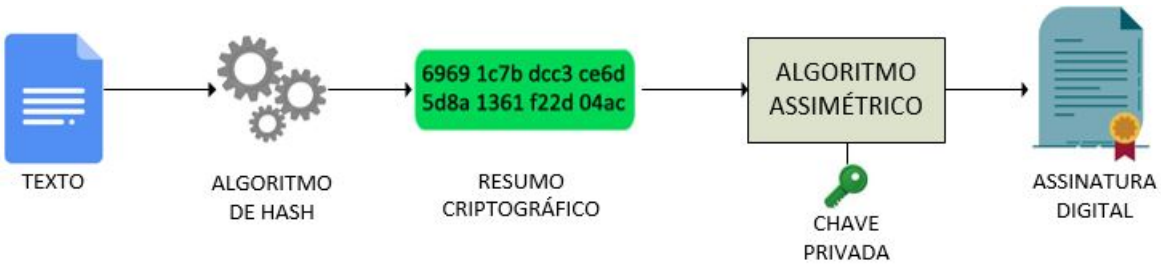



Figura 6: Fluxo simplificado de assinatura digital
Fonte: Próprio autor

O processo para verificação de uma assinatura digital é feito utilizando somente a chave pública que está associada a chave privada utilizada para cifrar o texto. Desta forma, garantindo a autenticidade da assinatura, computando o resumo criptográfico que foi recebido e comparando-o com o que foi assinado é possível fazer a checagem da integridade da mensagem. Conforme descrito em (NAKAMURA; GEUS, 2007), o algoritmo de assinatura digital é aplicado sobre a assinatura digital, o que resulta no resumo da mensagem, que é exatamente o processo inverso realizado na assinatura. O algoritmo de *hash* é aplicado na mensagem original, que também resulta no resumo da mensagem. No caso de os dois resumos da mensagem gerados serem iguais, isso significa que a assinatura é válida, pois a chave pública do remetente foi utilizada e ela é correspondente à chave privada utilizada. Caso os

dois resumos sejam diferentes, significa que a assinatura é inválida, pois chaves pública e privada não são equivalentes.

### 2.3.3 Certificado Digital de Identidade

Na prática, o certificado digital ICP-Brasil funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora, que seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (e.g. pessoa, processo, dispositivo) a um par de chaves criptográficas.

O certificado digital da ICP-Brasil, além de personificar o cidadão em toda a Internet, garante, por força da legislação atual, validade jurídica aos atos praticados com o seu uso. A certificação digital é uma ferramenta que permite que aplicações como comércio eletrônico, assinatura de contratos digitais, operações bancárias virtuais, iniciativas de governo eletrônico, entre outras, sejam realizadas. São transações feitas de forma virtual, ou seja, sem a presença física do interessado, mas que demandam identificação clara da pessoa que a está realizando pela internet.

No Brasil, o Conselho Federal de Medicina (CFM) publicou a RESOLUÇÃO CFM nº 1.983/2012 (CFM-1.983/12, 2012) que trata da utilização do Certificado Digital de Identidade, para que progressivamente seja adotado como recurso de identificação de um médico. Ele não é obrigatório, mas para a utilização de nossa solução, o radiologista deverá possuir um Certificado Digital de Identidade válido emitido pelo CFM. A criação do Certificado Digital de Identidade não é uma tarefa cabível à nossa solução, considera-se que o radiologista que irá receber a demanda para emissão de laudo possua um Certificado Digital de Identidade fornecido pelo Conselho Federal de Medicina.

### 2.3.4 Certificado Digital de Atributos

O Certificado Digital de Atributos (CA) é uma ferramenta disponibilizada pela ICP-Brasil que fornece facilidades em termos de segurança e interoperabilidade na gestão de documentos eletrônicos (GDE), inserindo não só segurança no âmbito técnico, mas principalmente, no jurídico. A principal diferença entre o Certificado Digital de Identidade (CD) e o Certificado Digital de Atributos é que o CD tem por finalidade permitir a identificação de uma pessoa/empresa e assinar documentos eletrônicos, já o CA tem a finalidade de qualificar uma pessoa/empresa dentro de uma organização. Outra diferença importante entre o CA e o CD é que normalmente o CD tem um período de validade de meses ou anos. Já o CA pode ter seu período de validades medido em horas, pois normalmente o controle de validade de um CA é feito internamente em uma instituição (MAVRIDIS et al., 2001). O CA pode ser utilizado para as mais diversas finalidades:

- na identificação de profissionais pertencentes a uma determinada categoria;
- na identificação de cargos de funcionários e servidores em empresas e órgãos públicos;
- restrição de acesso em aplicações;
- delegação de poderes, similar a uma procuração.

O formato do Certificado de Atributo segue o padrão X.509, adotado pela ICP-Brasil na emissão de certificados de pessoa física, jurídica e de equipamentos. Todo CA deve ser emitido por uma Entidade Emissora de Atributos (EEA), que pode ser interna ou externa (terceirizada) a organização que deseje utilizar essa tecnologia. As obrigações de uma EEA são:

- ser responsável pelo ciclo de vida do certificado emitido;
- possuir um CD (tipo A3 ou A4, pessoa jurídica) para que este possa assinar os CA emitidos;
- manter e disponibilizar uma Lista de Certificados Revogados (LCR)

Um CA pode ser vinculado a um CD no momento de sua criação. Caso exista a vinculação, a entidade que será titular do CA deverá enviar para a EEA emissora o seu Certificado

Digital de Identidade. Este, por sua vez, irá adicionar dados do CD do titular na CA emitido. Esta forma de emissão de CA é chamada de **Certificado de Atributos Vinculado - (CAV)**. No momento da solicitação de acesso aos recursos desejados o titular do CA deverá disponibilizar o seu CD para validação. Esse modelo é o utilizado no DICOMFlowAccess (DFA). Também existe a possibilidade de não ser necessário vincular um CD ao CA emitido. No momento da solicitação de acesso ao recurso, basta que o CA emitido esteja na validade e possua uma assinatura digital válida. Esta forma de criação de CA é denominada de **Certificado de Atributos Autônomo (CAA)**.

Quaisquer informações que estejam sob a gestão de uma EEA, a respeito de um cidadão ou de uma empresa são passíveis de serem incluídas num Certificado de Atributos, desde que a EEA seja a gestora e responsável legal pela informação a estar contida no CA. Outros detalhes relacionados a criação e uso de um Certificado Digital de Atributos são disponibilizados em dois documentos publicados pela ICP-Brasil: (ICP-BRASIL, 2012), que contém uma visão geral do uso do CA; e (ICP-BRASIL, 2016), que apresenta os detalhes técnicos necessários para criação e uso dos certificados de atributos.

## 2.4 eXtensible Access Control Markup Language - XACML

O eXtensible Access Control Markup Language é um padrão apresentado pela (OASIS, 2017) que define uma linguagem para políticas de controle de acesso descritas em XML. O XACML, em sua essência, é um controle de acesso baseado em atributos, em que atributos associados a um usuário são transportados em XML e utilizados na decisão de conceder ou negar acesso a um recurso. A proposta apresentada se divide em duas vertentes: (1) criar um protocolo para gerar e transportar os atributos de uma solicitação de acesso em XML e (2) propor uma arquitetura referência para receber e analisar as requisições de acessos com a finalidade de retornar uma permissão ou negação a solicitação.

Sua arquitetura de referência é formada por 5 elementos: o PEP (Policy Enforcement Point), o PDP (Policy Decision Point), o PAP (Policy Administration Point ), PIP (Policy Information Point) e o PRP (Policy Retrieval Point). O posicionamento de cada um deles na

arquitetura pode ser observado na Figura 7 e suas funções são descritas, de forma resumida, posteriormente.

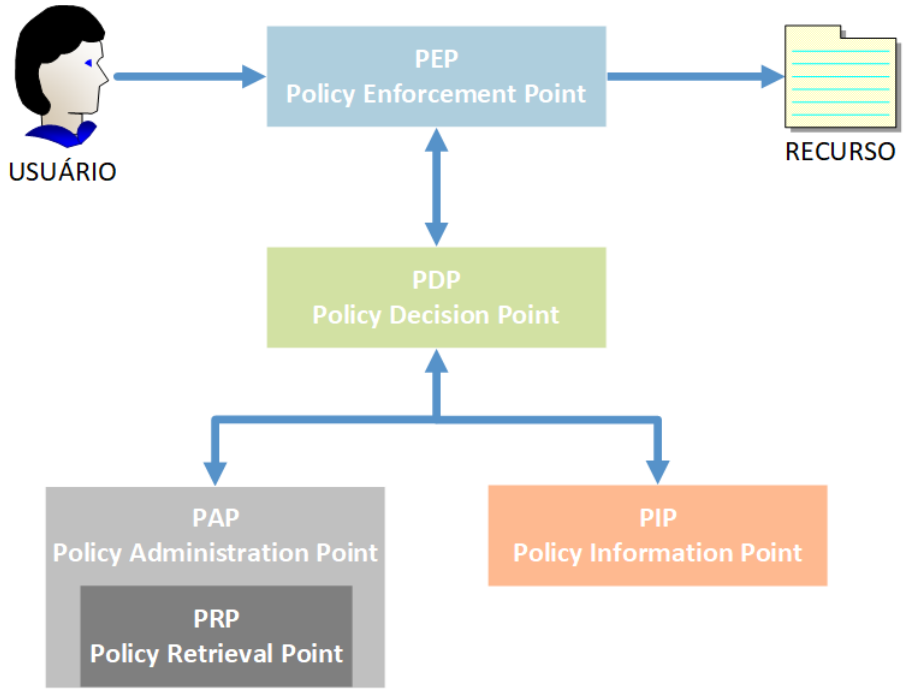



Figura 7: Arquitetura de referência do XACML
Fonte: Adaptada de (OASIS, 2017)

- PEP: faz a interceptação da solicitação de acesso de um usuário a um recurso, envia essa solicitação para o PDP, aguarda e aplica a decisão recebida.
- PDP: avalia os pedidos de acesso baseando-se nas políticas de autorização antes de emitir decisões de acesso.
- PAP: armazena e gerencia as políticas de autorização de acesso.
- PIP: mantém informações a respeito dos atributos existentes.
- PRP: base de dados ou sistema de arquivos em que as políticas de autorização de acesso XACML são armazenadas. Esse módulo está embutido no PAP.

O fluxo de ações até chegar a decisão acerca da solicitação de acesso é descrito abaixo:

1. Um usuário envia uma solicitação de acesso a um recurso que é interceptada pelo PEP;

2. O PEP converte a solicitação do pedido em um pedido de autorização XACML e a envia para PDP;

3. O PDP avalia o pedido de autorização de acordo com as políticas nele configuradas. Tais políticas são adquiridas através do PIP e são gerenciadas pelo PAP. Caso algum atributo não tenha sido gerado corretamente pelo PEP, o PIP será acionado para recuperar valores e informações a respeito dos atributos;

4. O PDP obtém a decisão (permite / nega / não aplicável / indeterminado) e retorna para o PEP;

5. O PEP aplica a decisão informada pelo PDP.

Imaginemos o seguinte cenário: o usuário "médico_a", deseja "ler" o exame de imagem "mamografia_b". Essa requisição irá ser recebida pelo PEP que, suprimindo algumas informações contidas como dados do *plugin* utilizado, irá gerar uma solictação de acesso no formato XACML com a estrutura apresentada na Figura 8.

Pode-se perceber em destaque os tipos de atributos e seus valores. Essas serão as informações utilizadas pelo PDP para a tomada de decisão sobre a solicitação enviada após consultar as políticas de acesso ao recurso solicitado que são gerenciadas pelo PAP. Uma implementação similar ao RBAC também pode ser feita utilizando o XACML e o conceito de controle de acesso baseado em papéis ser utilizado na implementação.

Contudo, dentro de uma organização, os atributos utilizados no controle de acesso aos recursos podem ser customizados para atender as necessidades internas. Causando dificuldades na operabilidade entre instituições distintas. Sendo assim, devido a possibilidade desta customização, geralmente, específica em cada organização, é imperativa a necessidade de uma padronização para criar-se um controle de acesso que atue em escala global de comunicação, principalmente, em circunstâncias em que associações entre entidades são criadas livremente e dinamicamente. Outra característica deste modelo e que certamente é um limitador para uma comunicação aberta e distribuída é a necessidade de uma base centralizada de políticas. Existem estudos (LEE; LUEDEMANN, 2007; ALZAHRANI et al., 2010; NGO

```
...
<xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">medico_a</xacml3:AttributeValue>
<xacml3:AttributeDesignator
AttributeId="user-ID"
DataType="http://www.w3.org/2001/XMLSchema#string"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
MustBePresent="false"
/>
...
<xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ler</xacml3:AttributeValue>
<xacml3:AttributeDesignator
AttributeId="action-ID"
DataType="http://www.w3.org/2001/XMLSchema#string"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
MustBePresent="false"
/>
...
<xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">mamografia_b</xacml3:AttributeValue>
<xacml3:AttributeDesignator
AttributeId="resource-TYPE"
DataType="http://www.w3.org/2001/XMLSchema#string"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
MustBePresent="false"
/>
...
```

Figura 8: Exemplo de requisição de acesso XACML
Fonte: Próprio autor.

et al., 2012) propondo o compartilhamento e sincronização destas políticas, entretanto, isso não é relevante para a nossa proposta, visto que, queremos proporcionar a liberdade para que qualquer entidade provedora de recurso na rede de colaboração como propomos, possa implementar a sua própria política de acesso. Observa-se que no momento que o PEP repassa o XACML gerado para o PDP, este, por sua vez, tem que consultar uma base de dados (PAP, PIP e PRP) para validar a requisição. Com isso, a proposta apresenta um modelo vinculado a necessidade do conhecimento prévio de entidades, atributos ou políticas. Não adaptando-se facilmente a demanda de escalabilidade e dinamicidade da infraestrutura idealizada para a prática da telerradiologia.

Contudo, a arquitetura de referência proposta mostra-se flexível, por exemplo, cada elemento pode ser posicionado em um ambiente computacional diferente, o que possibilita um

ajuste fino nas regras de segurança em cada uma deles. Como uma das possibilidades com a implementação do DICOMFlowAccess é o surgimento de parcerias entre entidades de saúde e empresas provedoras de serviços de armazenamento, o PAP é um elemento com características que tornará a administração dessas possíveis parcerias mais flexível e eficiente. Em nosso cenário existe a necessidade de fornecer algum tipo de controle para os parceiros das entidades de saúde (e.g. fornecedores de armazenamento externo) e o PAP é o elemento utilizado para exercer essa função. Detalhes de como a arquitetura de referência do XACML foi adaptada para atender as necessidades do DFA e de como será implementada, são apresentados no Capítulo 3.

## 2.5 DICOMFlow

Proposto em (ARAUJO, 2017), o DICOMFlow é um *gateway* assíncrono e descentralizado para auxiliar o compartilhamento de imagens médicas entre entidades de saúde que praticam a telerradiologia e desejam formar uma rede de colaboração para emissão de laudos médicos utilizando exames de imagens. Foi desenvolvido para operar em conjunto com a consolidada infraestrutura telerradiológica PACS/DICOM, que, como dito anteriormente, é uma infraestrutura que apresenta limitações para operar em um ambiente computacional fora do escopo de uma rede local. Esta é a limitação que o DICOMFlow se propõe a sanar, ser um *gateway* para auxiliar a base instalada para telerradiologia PACS/DICOM transpor o contexto de uma rede local para o contexto global, atuando na comunicação entre a infraestrutura telerradiológica com a Internet, posicionando-se na borda da infraestrutura telerradiológica sem causar interferência no fluxo de trabalho já existente internamente.

Em suma, suas atividades são duas: (1) analisar as atualizações de exames de imagens médicas e, comunicando-se com outros módulos do DICOMFlow previamente configurados em outra infraestrutura PACS/DICOM, (2) fazer a transferência dos exames de imagens quando necessário. A Figura 9 mostra o posicionamento dos módulos DICOMFlow em uma rede de colaboração formada entre dois hospitais (HOSPITAL e HOSPITAL PARCEIRO) e um RADIOLOGISTA externo. É importante reforçar que essa rede de colaboração pode ter a adesão de novos membros de forma indeterminada. Entidades de armazenamento externo

de imagens ou de processamento dessas imagens podem aderir a essa rede colaborativa formando parcerias, desde que possuam um módulo do DICOMFlow ativo em suas estruturas computacionais.

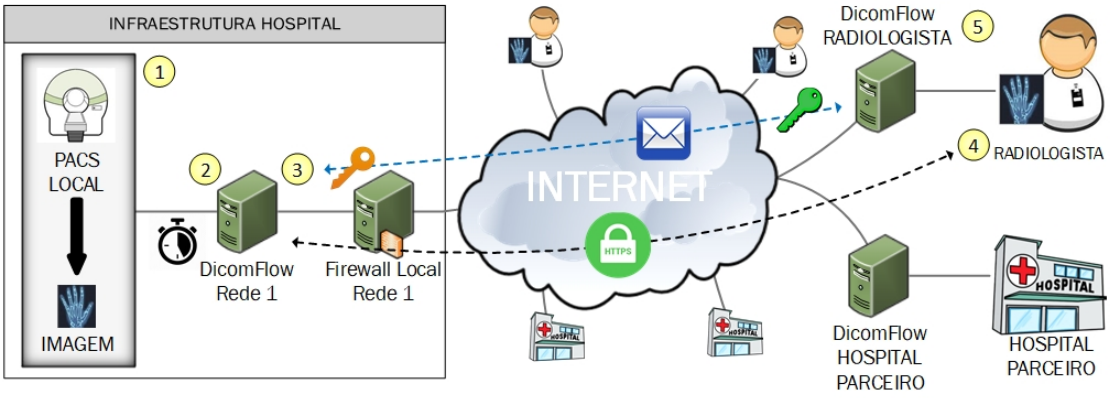



Figura 9: DICOMFlow atuando na borda da infraestrutura PACS/DICOM
Fonte: Adaptado de (ARAUJO, 2017)

Os passos até a obtenção do laudo por HOSPITAL são os seguintes:

- Passo 1: O exame de imagem é gerado por uma modalidade e armazenado na infraestrutura PACS/DICOM do HOSPITAL;
- Passo 2: Em uma periodicidade pré-estabelecida, o DICOMFlow monitora a infraestrutura PACS/DICOM local afim de identificar novos exames de imagens que necessitem, inicialmente de laudo médico. Entretanto, outros serviços podem emergir na rede de colaboração para prática da telerradiologia.
- Passo 3: O DICOMFlow, via email, inicia uma série de troca de chaves públicas com a entidade escolhida para emissão de laudo. Neste cenário, esta entidade é o RADIOLOGISTA, mas poderia ser o HOSPITAL PARCEIRO ou qualquer outra entidade participante da rede de colaboração. Após a troca de chaves, uma mensagem de email criptografada contendo dados de controle e segurança é enviada para o RADIOLOGISTA. Ao fazer esta solicitação de laudo, uma tripla associação é criada e armazenada em uma base de dados local para fins de controle de acesso. Essa associação contém o **ID da mensagem**, a **URL** para obter o exame e o **email** do RADIOLOGISTA solicitado. Na Figura 10, pode-se observar essas informações. O email está descriptografado para tornar as informações legíveis. Em vermelho estão os dados

de controle de acesso, em azul o tipo de serviço solicitado e em verde os dados para obtenção do exame, contendo a URL para resgate da imagem e as credenciais.

- Passo 4: De posse da solicitação, utilizando seu módulo do DICOMFlow, o RADIOLOGISTA pode obter a imagem utilizando HTTPS, após ter sido previamente autenticado e autorizado. Os dados de controle são enviados juntos dessa solicitação e analisados pelo módulo DICOMFlow existente em HOSPITAL. Caso os dados de controle dessa solicitação sejam equivalentes aos previamente gerados e armazenados no Passo 3, o exame de imagem é obtido fazendo o *download* via HTTPS;

- Passo 5: Após a obtenção do exame de imagem, o RADIOLOGISTA pode emitir o laudo solicitado por HOSPITAL.

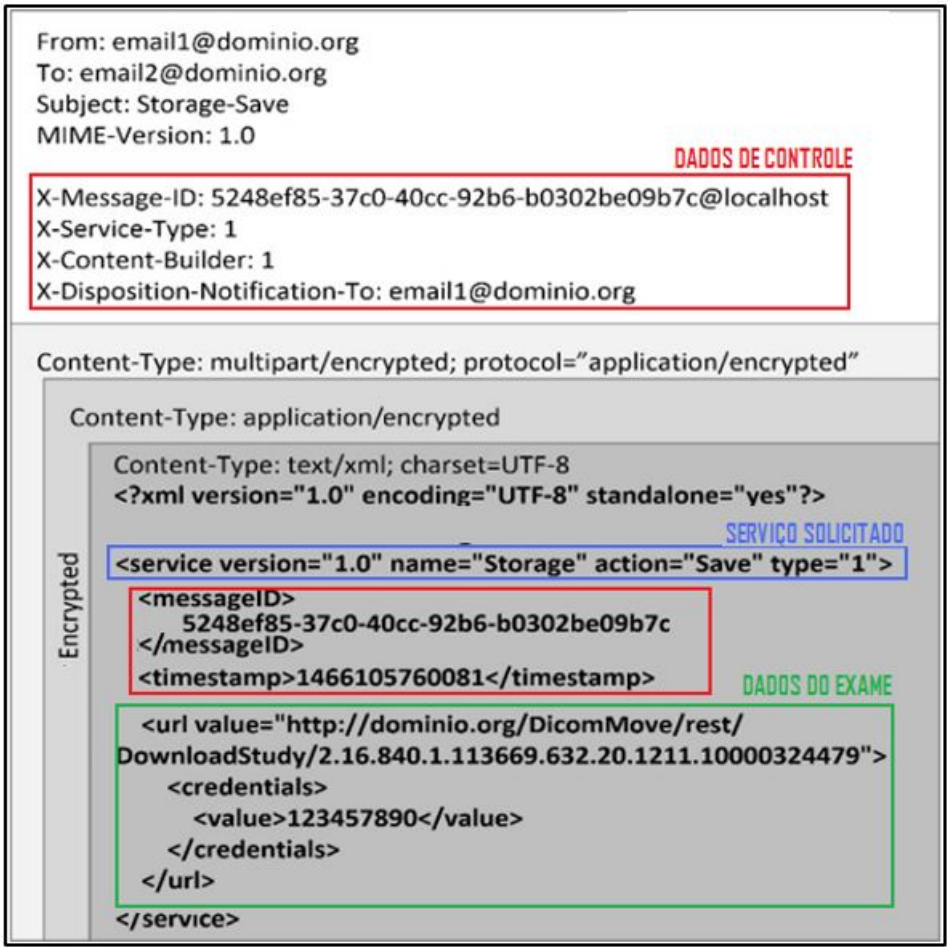



Figura 10: Mensagem DICOMFlow com a solicitação de laudo e dados de controle.
Fonte: Retirado de (ARAUJO, 2017)

No geral, o processo de controle de acesso é dividido em duas etapas: a autenticação e a autorização (BENANTAR, 2006). No DICOMFlow, a etapa de autenticação é feita usando o Amazon Web Services (AWS) para autenticação com Representational State Transfer (REST) (AMAZON, 2017). E a etapa de autorização é feita pela base de dados centralizada. Criada durante a troca de emails com a solicitação de laudos e os certificados digitais das entidades envolvidas.

Algumas características positivas desta solução são a (1) assincronia para obtenção do exame de imagem, pois o RADIOLOGISTA escolhe o momento que julgar oportuno para obter o exame de imagem já que no email não é transportada os exames de imagens e sim os metadados com informações de como obtê-la e (2) não ser necessária uma conexão ativa e persistente, como a utilização de autenticação através de login e senha, entre o RADIOLOGISTA e HOSPITAL, isto é possível por causa dos dados de controle existentes na mensagem de solicitação de laudo.

Entretanto, a criação de uma base de dados centralizada limita uma série de possibilidades de crescimento da rede colaborativa criada, como a formação de parcerias para armazenamento externo ou emissão de laudo terceirizado. Imaginemos o seguinte cenário: O HOSPITAL não quer armazenar as imagens geradas pelas suas modalidades em sua infraestrutura PACS/DICOM, seja por motivos técnicos ou financeiros para manter uma infraestrutura de armazenamento de dados. Ele decide formar parceria com uma empresa de armazenamento externo e passará a informar aos parceiros que o resgate dos exames de imagens deverá ser feito neste parceiro que fornece este serviço de armazenamento externo dos exames de imagens. Desta forma, haverá a necessidade de compartilhar a base de dados e mantê-la sincronizada ou disponível para consulta para que possa ser feita a validação das credenciais dos radiologias ou parceiros do HOSPITAL no momento do resgate do exame de imagem.

Esta situação não é desejada, pois, torna o processo mais oneroso na medida que novas entidades começam a aderir a rede colaborativa. Outra limitação no atual modelo é a falta de granularidade no controle de acesso, atualmente, não é possível especificar dias ou horários para obtenção de imagens ou tipos de exames de imagens (e.g. tomografia computadorizada,

ressonância magnética, mamografia ) que pedem ser obtidos. Essas limitações, tando a centralização da base de dados quanto a falta de granularidade nas opções de controle de acesso, são superadas com a implantação do DFA.

## 2.6 Bouncy Castle Crypto APIs

The Legion of the Bouncy Castle é uma iniciativa (*open source*) criada na Austrália que desenvolve um provedor de criptografia compatível com o Java Cryptography Architecture (JCA). Esta Interface de Programação de Aplicativos (do ingles, Application Programming Interface (API)) possui inúmeros recursos fundamentais para o desenvolvimento de nossa solução, visto que, nativamente, o Java SE Development Kit (JDK) atual não fornece suporte a implementação de Certificados de Atributos.

Alguns dos recursos existentes nesta API que serão utilizados neste trabalho são: provedor de criptografia JCA, bibliotecas ASN.1 e S\MIME, para criação do certificado e envio de email, respectivamente. Também serão utilizados os recursos de emissão de certificados X.509, listas de certificados revogados e os arquivos PKCS#12. E as funções de Online Certificate Status Protocol (OCSP) para verificação online do *status* do certificado em sua entidade emissora. A versão mais atual da API até o desenvolvimento deste trabalho é a 1.59 e pode ser obtida em https://www.bouncycastle.org/java.html.

## 2.7 Trabalhos relacionados

Nesta seção são discutidos os trabalhos relacionados a nossa pesquisa que desempenharam relevância para a problemática que orbita o funcionamento do controle de acesso a recursos compartilhados em ambientes abertos e distribuídos. Em suma, a Subseção 2.7.1 apresenta os critérios de investigação dos trabalhos relacionados e a Subseção 2.7.2 apresenta as principais características dessas propostas e as discute.

### 2.7.1 Critérios utilizados na investigação

Baseando-se nos conceitos de Infraestrutura da Informação (HANSETH; LYYTINEN, 2010) e nas particularidades de nossa área de pesquisa, identificou-se que o controle de acesso em uma rede colaborativa globalmente distribuídas deve conter algumas características. Abaixo, apresentamos e discutimos as principais delas.

1. **Permitir associações dinâmicas entre entidades:** isto remete ao funcionamento aberto da infraestrutura proposta. Entidades podem livremente associar-se sem a dependência de uma análise prévia de uma entidade administrativa. Essas associações podem ser duradouras ou não.

2. **Ser independente de base de dados centralizada:** não conter uma entidade central responsável pelas informações relacionadas os questões de autenticação e autorização de solicitação de acesso aos recursos compartilhados.

3. **Ser independente do estabelecimento de sessões:** permitir que os membros associados possam acessar, remotamente, os recursos compartilhados a qualquer momento. Não existindo a necessidade do estabelecimento de uma sessão em tempo real.

4. **Permitir controle de acesso aos dados, mesmo que já compartilhados:** a proposta deve permitir que o responsável pelo recurso compartilhado, no nosso cenário é o originador dos exames de imagens médicas, possa ter controle sobre quem tem permissões para acessá-lo, mesmo que já compartilhados.

5. **Atender prováveis particularidades entre membros associados:** eventualmente, políticas distintas de controle de acesso possam surgir. O mecanismo de controle de acesso deve ser flexível o suficiente para atender a essas particularidades entre associações.

6. **Fazer uso de certificados digitais:** está não é uma questão explícita nos conceitos de controle de acesso em uma Infraestrutura da Informação (II). Porém, por questões de projeto, visto que o DICOMFlowAccess pretende aprimorar o uso de certificados digitais na infraestrutura do DICOMFlow, é desejável que a solução pesquisada também utilize esse recurso.

7. **Possuir ligação com cuidados em saúde:** assim como o item anterior, esta característica não está vinculada aos conceitos de um II. Entretanto é desejável que, de alguma forma, as propostas de controle de acesso estejam direcionadas às informações utilizadas nas tecnologias ligadas aos cuidados em saúde, como exame imagens médicas, laudos ou prontuários.

A busca por trabalhos que ajudaram na concepção do DICOMFlowAccess foi norteada por essas características. Na subseção seguinte são apresentadas as propostas estudas, analisando seus aspectos positivos e negativos.

### 2.7.2 Análise crítica das propostas estudadas.

O objetivo desta subseção é apresentar propostas com potencial agregador para auxiliar na concepção do DICOMFlowAccess. Aqui é feita uma análise crítica de suas características, padrões e tecnologias utilizadas. O foco foi buscar por propostas que resolvam a problemática do funcionamento do mecanismo de controle de acesso em ambientes similares aos criados pela formação de organizações virtuais. Em particular, associações criadas para a prática da telerradiologia.

#### 2.7.2.1 Task-Based Access Control for Virtual Organizations

A proposta apresentada em (PERIORELLIS; PARASTATIDIS, 2004) propõe um *middleware* que trata as questões de confiança, segurança e gerenciamento durante a colaboração virtual entre empresas. O projeto visa fornecer uma tecnologia para apoiar a criação, operação e dissolução de organizações virtuais. Os autores propõem ampliar as ideias do RBAC somado aos serviços WEB existentes e emergentes como uma plataforma de implementação.

Na primeira parte do artigo vários conceitos como papéis, permissões e obrigações dentro de um ambiente composto por componentes autônomos que são reunidos para formar uma Organização Virtual. Os autores descrevem três caminhos serem seguidos para o estabelecimento de associações seguras entre entidades. (1) Implementação de políticas de controle de acesso que protegerão os ativos de cada parte contra o uso não autorizado, permitindo o compartilhamento. (2) Detalhamento da arquitetura de sistemas confiáveis como forma de

aumentar a confiança por meio da confiabilidade do sistema e (3) Investigação da formação de zonas de confiança. Desenvolvendo regras às quais todos os participantes do sistema aderem.

Na segunda parte do trabalho os autores descrevem como a confiança é estabelecida entre entidades e cita duas possibilidades comumente utilizadas. A confiança baseada em histórico (experiências transacionais passadas com alguém) e a confiança baseada em contexto (estar dentro de uma zona de confiança ou um limite de regras e regulamentos). Reforçam também que em ambientes altamente dinâmicos, como organizações virtuais, as partes podem não ter a oportunidade de criar um histórico de transações. Na terceira parte do artigo é descrito alguns conceitos, já apresentado neste trabalho, acerca do papel do controle de acesso.

Por fim, os autores apresentam a solução. Uma estrutura baseada em relação de confiança estabelecida baseando-se no contexto que utiliza troca de mensagens XML para determinar se o solicitante tem permissão suficiente para executar operações ou acessar recursos. Também é citado que outros níveis de verificação de identidade do solicitante podem ser solicitado usando metodologias existentes. A solução usa conceitos de sistemas distribuídos para o tratamento de transações. O conceito de esferas de controle e o conceito de ações atômicas coordenadas. A proposta define as associações como *projetos* e que cada projeto possuem tarefas. Associadas a estas tarefas estão as regras de controle. Um exemplo de projeto pode ser visto na Figura 11.

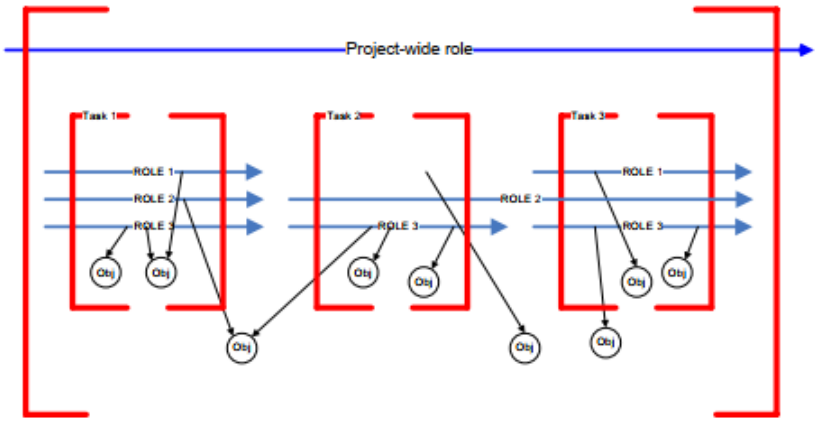



Figura 11: Exemplo de projeto proposto em (PERIORELLIS; PARASTATIDIS, 2004).
Fonte: Retirado de (PERIORELLIS; PARASTATIDIS, 2004)

A linha de tempo maior, representa todas as tarefas que estão vinculadas os projeto. Dentro do projeto, existem as tarefas individuais com suas regras (políticas) e objetivos (documentos ou serviços). Cada entidade envolvida na formação da organizações social para a realização de um determinado projeto, possui suas políticas locais que determinam parâmetros para o estabelecimento das associações. O nível de granularidade proposto permite monitorar as ações de cada tarefa em tempo real. Caso uma determinada entidade achar que deve negar as ações de cada tarefa, independente de já iniciada, ela pode fazê-lo.

Na Seção 6.2 do documento, os autores esclarecem alguns pontos relacionados a segurança. Dentre eles, que aspectos ligados a autenticação devem ser implementados separadamente. Uma combinação de tecnologias são sugeridas, como o WS-Security, WS-Trust, WS-Federation, SAML e XACML. Posteriormente a essa seção, os autores concluem o trabalho alegando que a solução apresentada é mais eficiente que modelos tradicionalmente conhecidos como o RBAC para atuar no contexto de organizações virtuais.

**Análise da Proposta**

A proposta de (PERIORELLIS; PARASTATIDIS, 2004) detalha como deve ser feita a autorização de acesso a recurso compartilhados em organizações virtuais e segundo os autores, nesse aspecto ela é bem sucedida. Entretanto, algumas questões fundamentais não ficam claras ou não são contempladas pela solução. A primeira é a respeito do estabelecimento da organização virtual. Os autores sugerem um conjunto de tecnologias para exercer essa função. A segunda é a respeito das questões associadas a autenticação de acesso. Os autores optaram por não atuarem nas ações associadas a essa etapa do controle de acesso. Focando apenas nas ações relacionadas a autorização. E por último, aspectos associados a segurança não são discutidos. Deixando as possibilidades como certificados X.509 como sugestão.

Apesar de interessante a implementação de tarefas e as políticas de segurança estarem direcionadas a elas. Diferente das políticas tradicionais, que estão direcionadas a recursos e usuários. A solução apresentada, isoladamente, é carente de questões mais complexas para atuar numa infraestrutura aberta e distribuída para a prática da telerradiologia numa rede colaborativa de alcance global.

#### 2.7.2.2 A Trust-based Access Control Model for Virtual Organizations

Em (LIN et al., 2006), os autores iniciam a proposta alegando que é normal organizações virtuais utilizarem o mecanismo de controle de acesso baseado em funções e expõem algumas das limitações desse modelo em atuar fora de seu domínio de segurança.

Os autores introduzem o funcionamento do modelo de controle de acesso proposto. Um controle de acesso baseado em confiança. E nele são instituídas três premissas para o estabelecimento de confiança. O primeiro nível, pode ser estabelecido quando um usuário, por exemplo, apresenta seu certificados digital de identidade. O segundo nível, os autores mostram que relações de confiança podem ser estabelecidas através de julgamentos subjetivos individuais entre as partes. Mesmo que a parte A confie na parte B, isso não significa que a parta B passe a ser confiável para outras partes. Cada parte tem seu próprio julgamento em relação a outras partes. E por último, o terceiro nível. Nele os autores descrevem que uma relação de confiança tem apenas uma direção, ou seja, se a parte A confia na parte B, não significa que o parte B confia em A.

O modelo descreve que as relações de confiança são niveladas e são previstas situações em que as relações de confiança podem ser alteras. Por exemplo, a parta A confia na parte B para compartilhar documentos classificados como "secretos". no entanto, a parte A não confia na parte B quanto ao compartilhamento de documentos classificados como "ultra secretos". Os autores propõem um modelo matemático para classificar o nível da relação estabelecida. Basicamente este modelo calcula o número de interações que acontecem entre partes em um determinado espaço de tempo. Quanto mais interações, mas alta a classificação da relação de confiança. Sendo reforçado que, assim como na vida real, uma relação de confiança é mais fácil de destruir que estabelecer.

Na proposta é definida três categorias de partes de uma organização virtual. (1) *User*, um usuário, que possui atributos associados a ele e que pode acessar recursos e serviços. (2) *Group*, que é um conjunto de usuários, possui atributos e um líder. E *vrooms*, que é um *workspace* que mantém grupos, recursos e serviços associados para um objetivos específico. Uma *vroom* também possui atributos de identidade e um proprietário. A protótipo de me-

canismo que implementa o modelo proposto é baseado em Shibboleth, portanto mais duas partes adicionais precisam ser introduzidas. A primeira é o *identity provider*, que mantém, verifica e atesta atributos de usuários. E a segunda é o *service provider*, que oferece serviços a usuários pertencentes a um *identity provider*. Uma tabela com as possibilidades de relacionamentos é apresentada abaixo na Figura 12, que mostra as possibilidades de relações de confiança entre as partes, em que "x" significa que a confiança é possível. Nela, é definida que as partes da coluna confiam nas partes da linha.

| | **user** | **group** | **vroom** | **IdP*** | **SP*** |
|---|---|---|---|---|---|
| **user** | x | x | x | | x |
| **group** | x | x | x | | x |
| **vroom** | x | x | x | x | x |
| **IdP*** | | | x | | x |
| **SP*** | x | x | x | x | |

Figura 12: Possíveis relações de confiança propostas em (LIN et al., 2006).
Fonte: Retirado de (LIN et al., 2006)

A classificação no nível de acesso entre as entidades vai no nível 0 até o 5. aonde o nível 0 não possui acesso ao recurso solicitado e o nível 5 tem controle gerencial sobre o recurso. Já as políticas são escritas em XML e, segundo os autores, flexíveis o suficiente para atender a grande número de situações durante o compartilhamento de recursos e serviços nas associações estabelecidas.

**Análise da Proposta**

Apesar da interessante possibilidade de relacionamento direto entre usuários e políticas de acesso flexíveis, a proposta apresentada em (LIN et al., 2006) contém algumas limitações para que possa atuar como controle de acesso na rede colaborativa como idealizamos. Uma das limitações é a necessidade da presença de um provedor de identidade. Esta característica implica que o conhecimento prévio de um determinado usuário é necessário para que ele possa associar-se a outros. Tal característica impacta diretamente na formação de associações dinâmicas. Outro aspecto negativo da solução é o *score* estabelecido para a classificação da solução, não ficou claro no texto, qual o real impacto disso nos níveis de acessos permitidos, entretanto o histórico das interações para o estabelecimento das organizações virtuais, deno-

minadas *vrooms* pelos autores, é um aspecto negativo para o cenário que idealizamos. Pois, médicos radiologistas que nunca mantiveram contato profissional antes devem ter a possibilidade de relacionamentos sem a possibilidade de "penalidade"por nunca terem estabelecido uma relação profissional antes.

#### 2.7.2.3 Access Control Model for Inter-organizational Grid Virtual Organizations

Na abordagem apresentada em (NASSER et al., 2005), os autores propõem um Modelo de Controle de Acesso Baseado em Organização (do inglês, Organization Based Access Control Model - OrBAC), um modelo, que segundos os autores, é capaz de establecer e gerenciar organizações virtuais de forma dinâmica. Neste trabalho o conceito de *grid computacional* é induzido a ser compreendido como uma organização virtual, aonde surgem os conceitos de usuários, recursos, comunicação multi-domínio e contextos.

No ambiente de grade ou organização virtual, cada parceiro possui recursos que são colocados em comum para serem compartilhados pela comunidade. A necessidade, segundo os autores, é de um modelo de controle de acesso que indique: quem pode fazer, o que e em qual contexto. O modelo de controle de acesso OrBAC é proposto para modelar uma política de segurança que não está restrita a permissões estáticas e inclui regras contextuais relacionadas a permissões, proibições e obrigações.

Existem oito conjuntos básicos de entidades: *Org* (organização: um grupo organizado de sujeitos, desempenhando algum papel dentro do grupo), *S* (um conjunto de sujeitos), *A* (um conjunto de ações), *O* (um conjunto de objetos), *R* (um conjunto de funções), *a* (um conjunto de atividades), *V* (um conjunto de visualizações) e *C* (um conjunto de contextos). O OrBAC considera que Org $\subseteq$ S, S $\subseteq$ 0. Qualquer entidade pode ter atributos, por exemplo, se S é um sujeito, então o nome (S), endereço (S) representa o nome e o endereço do sujeito S. O OrBAC também define relações entre esses conjuntos.

Para gerenciar as conexões entre membros do *grid* estabelecido, os autores propuseram um módulo de administração do ORBAC, o AdOrBAC. Dois módulos gerenciais estão presentes no AdOrBAC, o módulo de Atribuição de Função do Usuário (do inglês, User Role

Assignment - URA) e o de Atribuição de Função de Permissão (do inglês, Permission Role Assignment - PRA). O primeiro é usado para determinar quem tem permissão para atribuir um usuário a uma função e em quais condições. Ele é composto por três objetos: *Subject, Role e Org*. Já o segundo módulo é responsável pelas políticas de acesso e é composto por cinco objetos: *Issuer, Grentee, privilege, target e Context*. Estes atributos servem para identificar uma requisição dentro de uma organização virtual estabelecida.

**Análise da Proposta**

Apesar da proposta apresenta em (NASSER et al., 2005) ser eficiente nas questões relacionadas a estabelecimento de organizações virtuais e revogação de acesso. Não fica claro se o OrBAC atuará como um *gateway* para interligar entidades distintas. Já o AdOrBAC é um módulo administrativo que está disponível em cada organização. Mas essa não é uma característica impeditiva para a implantação do OrBAC como solução pra uma rede de colaboração para a prática da telerradiologia como propomos. Dois aspectos chamam a atenção na solução. (1) Para que um usuário possa acessar os recursos e serviços ofertados nas associações, ele é obrigado a estar posicionado logicamente atrás da infraestrutura de sua entidade. Pois, o OrBAC não fornece a capacidade de estabelecer associações entre usuário. Somente são estabelecidas associações entre entidades. (2) Os atributos existentes para estabelecer um critério de acesso são estáticos. Tornando assim difícil a adaptação do modelo em situações que fogem o previsto por ele. Entretanto, na seção relacionada aos trabalhos futuros, os autores citam algumas dessas limitações e que futuramente irão tentar contorná-las.

#### 2.7.2.4 Access-rule certificates for secure distributed healthcare applications over the Internet

Em (MAVRIDIS et al., 2002), os autores enfatizam o uso de certificados digitais para controle de acesso na Internet. Citam que os certificados de identidade e de atributos são tipos comuns e já utilizados tanto na indústria quanto na academia. Como novidade, eles propõem a criação de um terceiro certificado, o certificado de regra de acesso. Os autores enaltecem o alcance da comunicação através da Internet, entretanto, destacam o grande desafio de utilizá-la de forma confiável para o compartilhamento de informações, principalmente, as que transportam dados clínicos de pacientes.

Eles destacam a necessidades de políticas de controle de acesso descentralizadas, pois, o ambiente idealizado por eles é distribuído geograficamente e possui múltiplos domínios de segurança. É proposto a delegação de controle de políticas descentralizado. Aonde uma administrador de segurança global fornece as políticas básicas e administradores de segurança regional pode implementar alguma regra de segurança para atender a uma necessidade específica. Desde que essa regra específica não sobreponha uma regra global.

Então ao autores apresentam o Controle de Acesso à Base de Dados Médica Distribuída (do inglês, Distributed Medical Database Access Control - DIMEDAC). Os autores afirmar que há um volume significativo de médicos, enfermeiros e estudando realizando rotação em diferentes departamentos e clínicas. O que torna a identificação e autorização de usuários onerosa. Então o DIMEDAC para a identificação de usuários através do local em que a requisição de acesso é feita. Para tal, são definidos três locais de usuários. (1) Site, que pode ser uma estação de trabalho a partir da qual um usuário efetua *login* no sistema. (2) Administrative Domain, que é a identificação da organização ou conjunto de organizações que o usuário seja membro e (3) living space, que faz referência ao contexto envolvido da solicitação de acesso, como ser um médico externo da instituição ou parentes de um paciente. Situações que os autores classificam como "necessidades temporárias".

A arquitetura operacional proposta é dividida em três fases diferentes. **(1)** A Propagação das Políticas é o processo que os mecanismos de controle entre diferentes níveis de domínios administrativos tornam-se capazes de herdar as políticas de domínios administrativos superiores. O certificado utilizado para executar esse processo é o Access-Rule Certificate. Sua esturura é similar a existente nos demais certificados utilizados na solução. **(2)** A Definição de Credenciais de Segurança é o processo que todo usuário deve executar. Ele é responsável por fornecer o Certificado de Identidade e Certificado de Atributos que iram identificar o usuário na infraestrutura proposta e apresentar as permissões deste usuário, respectivamente. A Figura 13 mostra os passos apresentados pelos autores para chegar até a obtenção dos certificados.

Na proposta, a obtenção dos certificados passa por duas estapas. A primeira etapa (Passos

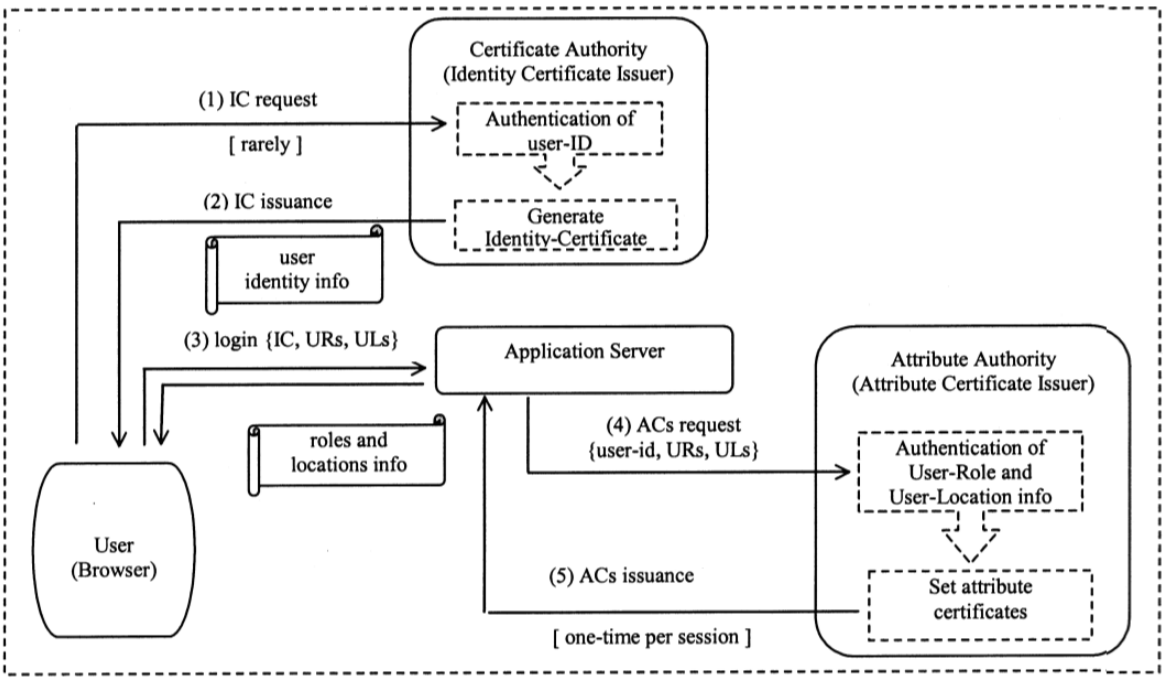



Figura 13: Etapas para obtenção dos certificados apresentadas em (MAVRIDIS et al., 2002). Fonte: Retirado de (MAVRIDIS et al., 2002).

1 e 2), o usuário obtém o Certificado de Identidade fornecido por uma autoridade certificadora local. A segunda etapa (Passos 3, 4 e 5), mostra as ações necessárias para o obtenção do Certificado de Atributos.

Por fim, **(3)** é feito o Processamento do Pedido de Acesso. Um usuário faz a solicitação de acesso via *browser* e os certificados de identidade e atributos transportam as informações necessárias para a autenticação e autorização de acesso. Uma validação é feita com as regras que acesso que foram aplicadas utilizando o Certificado de Regras de Acesso.

Os autores concluem que o DIMEDAC se mostrou eficiente em controlar pedidos de acessos em aplicativos de saúde distribuídos pela Internet. Reforçam que os certificados de identidade são certificados digitais de longa duração baseados em identidade com mecanismos de revogação e são usados para identificação e autenticação do usuário. Já os os certificados de atributos emergentes são propostos a serem certificados de curta duração, sem mecanismos de revogação, e devem ser usados para passar informações de controle de acesso baseadas em função de usuário e localização. Por fim, reforçam o terceiro tipo de certificado,

o certificado de regras de acesso. Que distribui as políticas de acesso para os mecanismos de controle de acesso,

**Análise da Proposta**

A utilização de certificados digitais para validação das informações de usuários é útil para compor uma solução de controle de acesso nesta e em outras soluções. Na proposta, existem algumas limitações para auxiliar o compartilhamento de informação médicas em ambiente aberto e distribuído. (1) Ela foi projetada para atuar em um único domínio de segurança ou em uma federação de domínios; (2) existe a centralização de autoridades certificadoras e, aparentemente, isso não ficou claro na proposta, não fazem parte de uma cadeia de certificação como a ICP-Brasil. Fato que invalida o certificado em um ambiente global; (3) o curto prazo de validade do certificado de atributos, sendo similar a um token de acesso; e (4) a dependência de uma conexão com a entidade emissora dos certificados no momento do acesso ao recurso solicitado para ser realizada as validações e análise dos atributos. Além desses aspectos que dificultam a aplicação deste modelo em um ambiente aberto e distribuído, não foi relatado pelos autores se a solução atua em conjunto com a infraestrutura PACS/DICOM presente nos departamentos de radiologia.

#### 2.7.2.5 ACROSS: A generic framework for attribute-based access control with distributed policies for virtual organizations

Em (SILVA et al., 2018), é proposto um *framework* genérico e extensível com autenticação e autorização para organizações virtuais com suporte a federação de identidade e recursos de controle de acesso. No âmbito deste artigo, o conceito de organização virtual tem o mesmo significado que entidades, que usamos neste artigo para referenciar uma instituição ativa num cenário global e um conjunto de organizações virtuais é o que denominamos federação.

Na base da solução apresentada orbita o conceito de SSO (Single sign-on) utilizando SAML (Secure Assertion Markup Language), que é um conjunto de especificações baseado em XML para a troca de informações (atributos) de um usuário. Algumas adaptações são implementadas (módulos) para suportar diferentes tecnologias de autenticação e ser independente dos recursos tecnológicos na formação de federações. A Figura 14 ilustra resumi-

damente uma estrutura SSO.

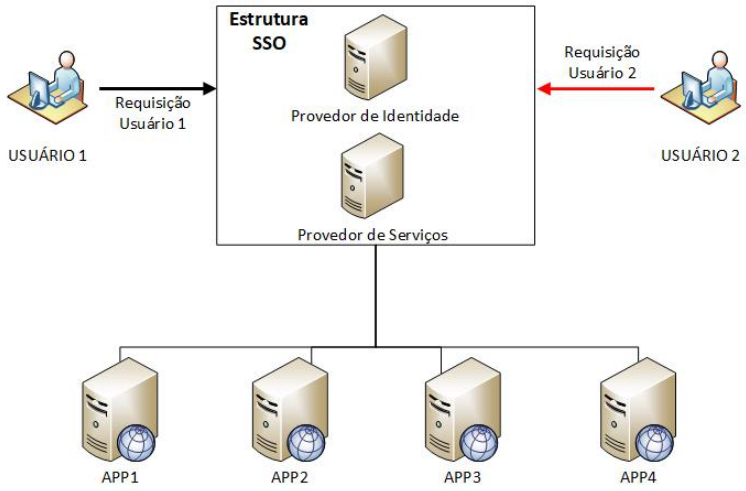



Figura 14: Funcionamento de uma estrutura SSO.
Fonte: Próprio autor.

Pode-se observar dois módulos principais, o Provedor de Identidades, que mantém, por exemplo, uma base de dados LDAP com informações de usuários para fins de autenticação e o Provedor de Serviços, que cria associações com aplicações distribuídas formando uma relação de confiança entre uma determinada aplicação e o provedor SSO. Quando um usuário faz a autenticação no provedor de SSO, através da relação de confiança pré estabelecida, ele poderá usufruir dos recursos das aplicações externas vinculadas ao Provedor de Serviços.

Os autores apresentam algumas soluções já propostas para prover autenticação em ambiente compartilhado, o VOMS[1] (Virtual Organization Membership Service), CAS[2] (Community Authorization Service), PREMIS[3] (PrivilEge and Role Management Infrastructure Standard) e Akenti[4]. Discutindo suas características e pontuando algumas limitações, que são similares as já pontuas neste trabalho, como base de dados centralizada, baseados dependência de conexão ativa, baseadas em funções e outras.

O ACRROS propõe a criação de módulos para a implantação de políticas (locais e glo-

[1]https://italiangrid.github.io/voms/
[2]https://www.apereo.org/projects/cas
[3]http://www.openpermis.info/
[4]https://dst.lbl.gov/ACSSoftware/Akenti/

bais) em cada organização virtual e para auxiliar na conexão com tecnologias heterogêneas de autenticação. Como pode ser visto na Figura 15.

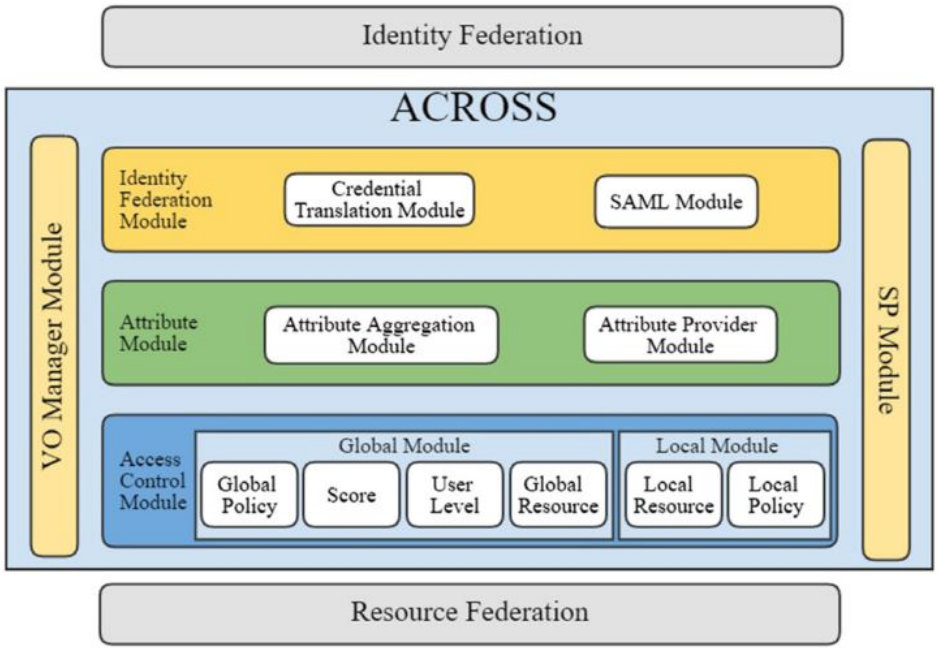



Figura 15: Arquitetura da solução ACROSS
Fonte: (SILVA et al., 2018)

O primeiro módulo criado é o *Identity Federation Module*, que junto com seus submódulos (*SAML Module* e *Credential Translation Module*), é o responsável por manter comunicação com a Federação de Identidade na qual deseja-se comunicação. O segundo módulo é o *Attribute Module*, que possui dois submódulos (*Attribute Provider* e *Attribute Aggregation Module*). Ele é o responsável por alinhar os atributos fornecidos pela Federação de Identidade com os atributos existentes na organização virtual. O terceiro módulo é o *Access Control Module*, responsável por implementar o suporte ao RBAC, ABAC, a distribuição das políticas implementadas e o suporte ao XACML. Possui dois submódulos: o *Global Module* e o *Local Module*. Os administradores utilizam esses submódulos para implementarem políticas de como os usuários podem acessar recursos externos (globais) e os recursos internos (locais). Outros dois módulos são inseridos na arquitetura, o *SP Module*, responsável por fornecer uma interface de usuário para os outros módulos ACRROS e o módulo *VO Manager*, que fornece uma interface de gerenciamento para o administrador de uma organização virtual.

**Análise da Proposta**

Em sua essência, o ACROSS implementa SAML para prover interconexão entre organizações virtuais. É uma ferramenta capaz de trabalhar com os principais modelos de controle de acesso (ABAC e RBAC) e provê suporte ao XACML que, como discutido anteriormente, é um padrão com muita aceitação, tando da academia quanto da indústria, para prover um controle de acesso baseado em atributos. Sua modularidade o torna muito adaptável para trabalhar com várias tecnologias de controle de acesso.

Entretanto, apresenta duas características que tornam sua operação em ambiente aberto e distribuído limitada. A primeira, é uma limitação presente na proposta do SSO, que depende de uma conexão estabelecida com a entidade de origem do usuário, ou seu provedor de identidade. E a segunda, é a necessidade de uma base de dados com usuários e atributos associados a ele que deverá estar disponível no momento do acesso para formação da credencial do usuário. Soluções semelhantes também são propostas em (YUAN; TONG, 2005), (SHEN; HONG, 2006) e (ALSHEHRI; RAJ, 2013). Este último, apresenta um outro modelo de controle de acesso denomidado de BiLayer Access Control (BLAC), que consiste em duas camadas de controle. A primeira, relacionada aos atributos associados ao solicitante. E a segunda, relacionada as políticas de segurança associadas ao objeto solicitado. Entretanto, assim como as demais propostas apresentadas, não apresenta solução para contornar o problema da base de dados, seja de usuários, atributos ou políticas, centralizada.

Caso um usuário queira acessar um determinado recurso pertencente a outro membro da rede colaborativa, ou conjunto de organizações virtuais, como se referem os autores, e essa criação de credencial não estiver disponível, o acesso não será realizado, ou seja, é uma proposta dependente de conexões pré-estabelecidas para seu funcionamento. Um outro aspecto é a necessidade de gerenciamento de informações de contas de usuários, grupos e atributos, que são necessários para a implementação do modelo RBAC. A proposta do DICOMFlowAccess independe de conexões ativas com o gestor de identidade e criação de credencial para qualificar um usuário, pois, todas essas informações estão armazenadas em certificados digitais de atributos e de identidade. Na seção seguinte, faremos as considerações finais deste capítulo e nela iremos comparar nossa proposta de controle de acesso com

as apresentadas nos trabalhos relacionados.

### 2.7.3 Considerações Finais

Foram apresentadas nestes capítulo as tecnologias que, concatenadas, deram sustentação a proposta de controle de acesso DICOMFlowAccess (DFA). Algumas delas já são bem estabelecidas, como a certificação digital e os protocolos de comunicação da Internet, como o HTTPS e email. Outras tecnologias ainda estão se estabelecendo, como o Certificado Digital de Atributos e o DICOMFlow. Também foi visto na seção dedicada aos trabalhos relacionados, que há muito se pesquisa soluções de gestão de identidade e controle de acesso capazes de atender a demanda de associações *ad-hoc* entre parceiros das mais diversas áreas de atuação.

Entretanto, percebe-se que as soluções apresentadas pelos pesquisadores não contemplam, em sua totalidade, as necessidades de um controle de acesso capaz de suprir as características necessárias para operar em um ambiente aberto e distribuído como a Internet. Observa-se também que as propostas de controle de acesso para atuarem em organizações virtuais, estão centradas em regrar quem faz uso de um recurso hospedado na entidade provedora de serviço. Falhando em contornar as necessidades que surgem quando o dado (e.g um arquivos de imagem ou um documento texto) é exteriorizado da instituição provedora. No nosso contexto, os exames de imagens médicas deixam de estarem hospedados no gerador da imagem (e.g. hospitais ou clínicas) e passam a estarem alocados fisicamente em outras entidade. Portanto, é imperativo para o funcionamento do mecanismo de controle de acesso, que essa situação possa ser contornada.

Na Tabela 1, pode-se observar um comparativo das características presentes nos Trabalhos Relacionados, do DICOMFlow, que é a infraestrutura escolhida para validar nossa proposta e o DICOMFlowAccess (DFA), que é a nossa solução para controle de acesso em ambientes abertos e distribuídos. Nela pode-se observar como são contemplados cada critério de pesquisa estabelecido no início da seção em que são apresentados os Trabalhos Relacionados.

Tabela 1: Comparativo das funcionalidades das propostas discutidas.

| **Trabalhos Relacionados \ Critérios de pesquisa** | *PERIORELLIS, 2004* | *LIN et al., 2006* | *NASSER et al., 2005* | *MAVRIDIS et al., 2002* | *SILVA et al., 2018* | *DICOMFlow* | *DICOMFlowAccess* |
|---|---|---|---|---|---|---|---|
| Permitir associações dinâmicas entre entidades | - | + | + | - | + | √ | √ |
| Ser independente de base de dados centralizada | - | + | + | - | + | - | √ |
| Ser independente do estabelecimento de seções | - | - | - | + | - | √ | √ |
| Permitir Controle de Acesso aos dados mesmo que já compartilhados | √ | - | - | - | - | + | √ |
| Atender prováveis particularidades entre membros associados | √ | - | - | + | - | - | √ |
| Fazer uso de Certificados Digitais | - | - | - | √ | - | √ | √ |
| Possuir ligação com Cuidados em Saúde | - | - | - | √ | - | √ | √ |

Legenda: Totalmente Presente (√), Parcialmente Presente (+), Ausente (-).

Na tabela observa-se que o DICOMFlowAccess atua diretamente nas limitações encontradas em outras propostas para prover controle de acesso em ambientes similares aos criados pelo estabelecimento de organizações virtuais. No próximo capítulo será detalhado o funcionamento do DFA e como as tecnologias ou conceitos aqui apresentados são utilizados para juntos, construírem o mecanismo de controle de acesso para atuar na rede colaborativa para a prática da telerradiologia com as características que propomos.

# CAPÍTULO 3

# DICOMFLOWACCESS

Este capítulo propõe o DFA (DICOMFlowAccess), um mecanismo de controle de acesso que independe de conexões ativas para fins de autenticação e autorização, com granularidade fina de atributos para requisitos de autorização, expansível, não necessitando de base de dados de usuários centralizada para identificação e implementando o modelo de controle de acesso baseado em atributos (ABAC). Para atingir este objetivo, foi usada como referência a arquitetura do XACML (OASIS, 2017) em conjunto com o certificado de atributos da ICP-Brasil. O DICOMFlow (ARAUJO, 2017), introduzido no Capítulo 2, foi o modelo com compartilhamento de informações entre entidades de saúde escolhido para implementação do DFA. Os detalhes do DFA serão apresentado nas seções a seguir. Na Seção 3.1 será apresentada uma visão geral do funcionamento do DFA inserido na arquitetura proposta pelo DICOMFlow, também será detalhada a estrutura do certificado de atributos e como aplicá-lo ao modelo do DICOMFlow. Na Seção 3.2 é apresenta a arquitetura do DFA com seus módulos e as funções de cada um deles, posteriormente (Seção 3.3), são apresentados alguns cenários possíveis com a solução. Por fim, são feitas as considerações finais.

## 3.1 Visão geral

Esta seção tem a finalidade de apresentar as entidades envolvidas na infraestrutura proposta para validação do DFA e o fluxo das mensagens para a troca de imagens médicas entre parceiros com a finalidade de emissão de laudo médico. Este é o cenário mais elementar e será utilizado para demonstrar a nossa proposta. Entretanto, outros cenários serão discutidos, como a presença de um outro radiologista caso uma segunda opinião seja necessária para a emissão do laudo. Como proposto pelo DICOMFlow, o e-mail continua como meio de transporte das mensagens trocadas, por ser descentralizado e de fácil conectividade. Na Figura 16 existem três entidades que utilizam a Internet como infraestrutura no o processo de comunicação. Na figura também é possível ver outras entidades nomeadas com "B". Nossa intensão com isso é mostrar a ideia de pluralidade de entidades presentes na infraestrutura que propomos.

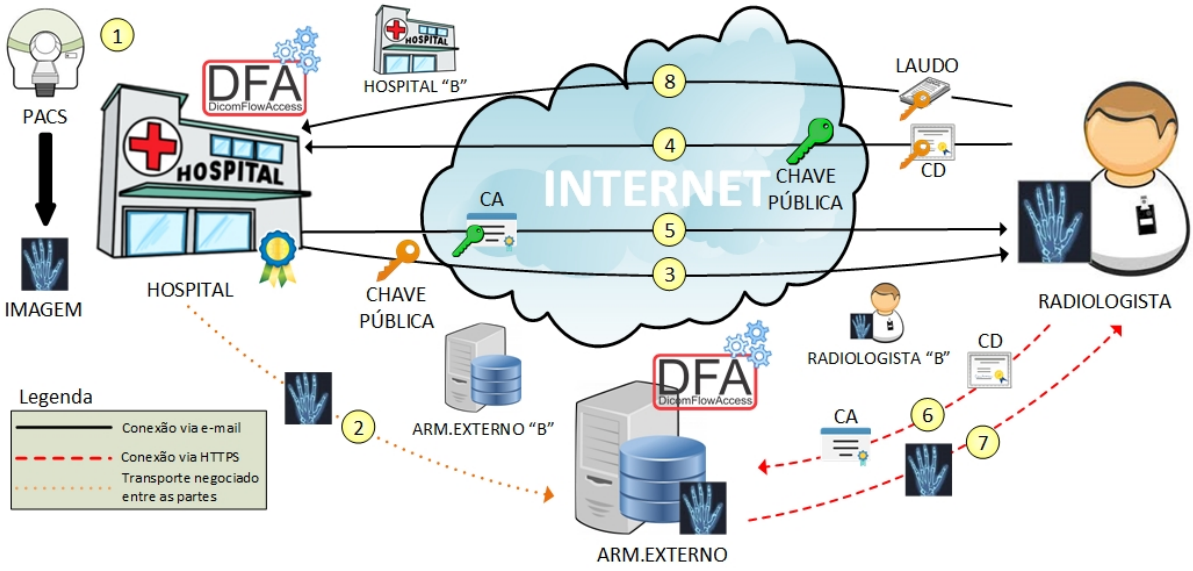



Figura 16: Visão geral da implementação do DFA.
Fonte: Próprio autor

HOSPITAL, que é o originador da imagem, o médico RADIOLOGISTA, que irá receber a solicitação de emissão de laudo de HOSPITAL, e o ARMAZENAMENTO EXTERNO, parceiro comercial de HOSPITAL que provê o serviço de armazenamento remoto das imagens geradas. A troca de mensagens é feita por módulos DICOMFlow instalados em cada uma das entidades do cenário, desde os e-mails para troca de certificados até a emissão do

laudo.

Como o e-mail e o HTTPS são protocolos que fazem o transporte das informações entre as entidades, eles devem sempre estar disponíveis para uso. A disponibilidade destes serviços não é o escopo desse trabalho. Detalhes de tecnologias (balanceamento de carga, IDS, IPS ou *firewall*) que proveem soluções para maior segurança desses e outros serviços podem ser encontradas em (NAKAMURA; GEUS, 2007) ou (STALLINGS, 2008). O papel de cada entidade ilustrada na Figura 16 é descrito a seguir.

1. HOSPITAL: entidade onde a imagem é gerada para posteriormente ser enviada para o armazenamento externo. Ele também desemprenha o papel de uma Entidade Emissora de Atributos (EEA). É o originador da imagem. Só ele poderá liberar o acesso a imagem através do certificado de atributos.

2. RADIOLOGISTA: destinatário da imagem, entidade (e.g um radiologista sem vínculo direto, uma clínica externa ou hospital parceiro) para onde ela deve ser transferida após a solicitação de laudo feita pelo originador da imagem, que neste cenário, é o HOSPITAL.

3. ARMAZENAMENTO EXTERNO: parceiro comercial de HOSPITAL que fornece o serviço de armazenamento para as imagens geradas. É a infraestrutura que será acessada pelo RADIOLOGISTA para obtenção da imagem.

A imagem também pode ser armazenada na infraestrutura de seu originador. Este cenário com um armazenamento externo é mais interessante para demonstrarmos a robustez e flexibilidade de nossa proposta. A seguir, detalhamos os passos de troca de mensagens até a obtenção do laudo pelo HOSPITAL.

1. **Passo 1:** A IMAGEM gerada pela modalidade (e.g equipamento de ressonância magnética, tomografia computadorizada) é armazenada temporariamente no PACS existente no HOSPITAL e, posteriormente, enviada para o armazenamento ARMAZENAMENTO EXTERNO permanente;

2. **Passo 2:** A IMAGEM é transferida de HOSPITAL para o seu parceiro comercial que é provedor de uma infraestrutura externa para armazenar dados, o ARMAZENA-

MENTO EXTERNO. Esta transferência pode utilizar o próprio protocolo DICOMFlow ou outra tecnologia como por exemplo, VPN. Os critérios de segurança ou protocolo utilizado para essa transferência são decididos em comum acordo entre o HOSPITAL e o ARMAZENAMENTO EXTERNO. É dever do ARMAZENAMENTO EXTERNO só permitir o acesso a IMAGEM após o processo de autenticação e autorização realizado pelo DFA, os detalhes desse processo são discutidos na Seção 3.2;

3. **Passo 3:** O HOSPITAL envia uma mensagem de solicitação de laudo para um RADIOLOGISTA. Nesta mensagem é enviado o certificado que contém a chave pública de HOSPITAL para que as próximas trocas de mensagens entre eles sejam criptografadas. Tal recurso é implementado pelo DICOMFlow com a finalidade de prover confidencialidade nas informações trafegadas através da criptografia;

4. **Passo 4:** O RADIOLOGISTA cifra a mensagem de resposta a solicitação com a chave pública do certificado enviado pelo HOSPITAL. Nesta resposta existem três informações, (1) confirmação/aceitação da solicitação para emissão do laudo, (2) chave pública do médico radiologista e (3) seu certificado digital, este último, para que o HOSPITAL possa gerar o certificado de atributos vinculado (CAV) a este certificado digital que será utilizado para acessar a IMAGEM. Os passos três e quatro são executados apenas no primeiro contato entre o HOSPITAL e o RADIOLOGISTA. Caso o HOSPITAL e o RADIOLOGISTA já tiverem realizado a troca de certificados, esses passos são suprimidos.

5. **Passo 5:** HOSPITAL, de posse da confirmação, chave pública e certificado digital do RADIOLOGISTA, gera o Certificado de Atributos e utilizando a chave pública do RADIOLOGISTA cifra a mensagem encapsulando o CA gerado e o envia para o RADIOLOGISTA. A estrutura da mensagem é similar a apresentada em (ARAUJO, 2017), entretanto existe a implementação do CA como credencial de acesso. Mais detalhes dessa modificação são discutidos na Subseção 3.1.3;

6. **Passo 6:** De posse da mensagem com o certificado de atributos encapsulado nela, o RADIOLOGISTA faz a requisição para baixar o exame utilizando a URL contida na mensagem. Neste momento, o protocolo de comunicação não é mais o e-mail, e sim

o HTTPS. Como o certificado de atributos utilizado é o CAV, o certificado digital do RADIOLOGISTA também é enviado para análise do DFA;

7. **Passo 7:** O DFA faz a validação e análise dos certificados apresentados e se as informações neles contidas, principalmente no certificado de atributos, explicitamente, permitirem o acesso a imagem requerida, o RADIOLOGISTA recebe a permissão para fazer o *download* da IMAGEM (ainda utilizando HTTPs como transporte). Maiores detalhes do funcionamento do DFA serão discutidos na Seção 3.2;

8. **Passo 8:** De posse da IMAGEM, o RADIOLOGISTA cria o laudo, assina-o digitalmente, criptografa com a chave pública do HOSPITAL a mensagem de retorno e faz o envio. Neste momento o e-mail volta a ser o protocolo de transporte.

Percebe-se que o fluxo de mensagens proposto pelo DICOMFlow em (ARAUJO, 2017) não sofreu alterações significantes, contudo, o funcionamento do controle de acesso, que foi uma das limitações apresentadas na proposta do DICOMFlow, sofreu alterações com a finalidade de propiciar maior flexibilidade, granularidade e controle na arquitetura inicialmente proposta. A principal característica de nossa proposta é que não se faz necessário o conhecimento prévio de informações do solicitante, isto torna desnecessária a existência de uma base de dados centralizada contendo por exemplo, informações de *login* e senha de usuários. Também não é necessária uma conexão ativa ou síncrona para obtenção do laudo pelo solicitante ou para que o radiologista obtenha o exame de imagem.

O HOSPITAL pode fazer a solicitação em um determinado momento e quando julgar conveniente o RADIOLOGISTA obtém a imagem e em um terceiro momento emite o laudo, não existe recebimento compulsório de grandes volumes de dados, apenas informações de controle existentes no protocolo é que são enviadas, como avisos e confirmações. Porém, acordos de níveis de serviços podem ser firmados entre as partes para determinar o funcionamento do fluxo de trabalho. Os certificados trocados inicialmente (passos 3, 4 e 5) entre HOSPITAL e o RADIOLOGISTA podem ser armazenados e futuras solicitações de laudo se tornarão mais rápidas, pois esses passos podem ser suprimidos, mas, por conveniência em uma determinada situação, o HOSPITAL pode optar pela execução de todas as etapas

descritas anteriormente.

As demais subseções são apresentadas na seguinte ordem. Na Subseção 3.1.1 detalhamos a Mensagem Original do DICOMFlow e o que será alterado com a implementação do DFA no mecanismo de controle de acesso do DICOMflow. Na Subseção 3.1.2 apresentamos o Certificado Digital de Atributos para a nossa solução e posteriormente (Subseção 3.1.3) discutimos como ficará a Nova Mensagem do DICOMFlow com a aplicação do DICOMFlowAccess (DFA).

### 3.1.1 Mensagem Original do DICOMFlow

Na Figura 17, pode-se analisar a estrutura da mensagem de e-mail originalmente proposta pelo DICOMFlow. Nota-se em destaque preto com a sinalização **CREDENCIAIS** os dados relacionados ao controle de acesso.

Para melhor compreensão de como os dados utilizados no controle de acesso do DICOMflow são estruturados e transmitidos na mensagem de email pode-se consultar (ARAUJO, 2017). Entretanto, de forma resumida, o controle de acesso funciona da seguinte forma:

1. O originador do exame de imagem (chamaremos de HOSPITAL) inicia via email a troca de credenciais com o médico radiologista (chamaremos de RADIOLOGISTA) para solicitar a emissão de um laudo;

2. No momento de troca de credenciais, o DICOMFlow do originador da solicitação (HOSPITAL) gera um número aleatório e único para ser a credencial, representado pela *tag* ***credentials*** na Figura 18. E através de um banco de dados local o associa a URL que contêm o exame a ser obtido, endereço de e-mail do destinatário (RADIOLOGISTA) e o identificador da mensagem (*tag* ***messageID***).

3. Quando o módulo DICOMFlow do destinatário (RADIOLOGISTA) faz a requisição para obter o exame, via HTTPS, o módulo DICOMFlow do originador (HOSPITAL) da solicitação faz a análise da mensagem e em seu banco de dados local compara se as informações conferem com a associação criada em seu banco de dados;

4. Caso a associação seja confirmada o envio da imagem é feito.

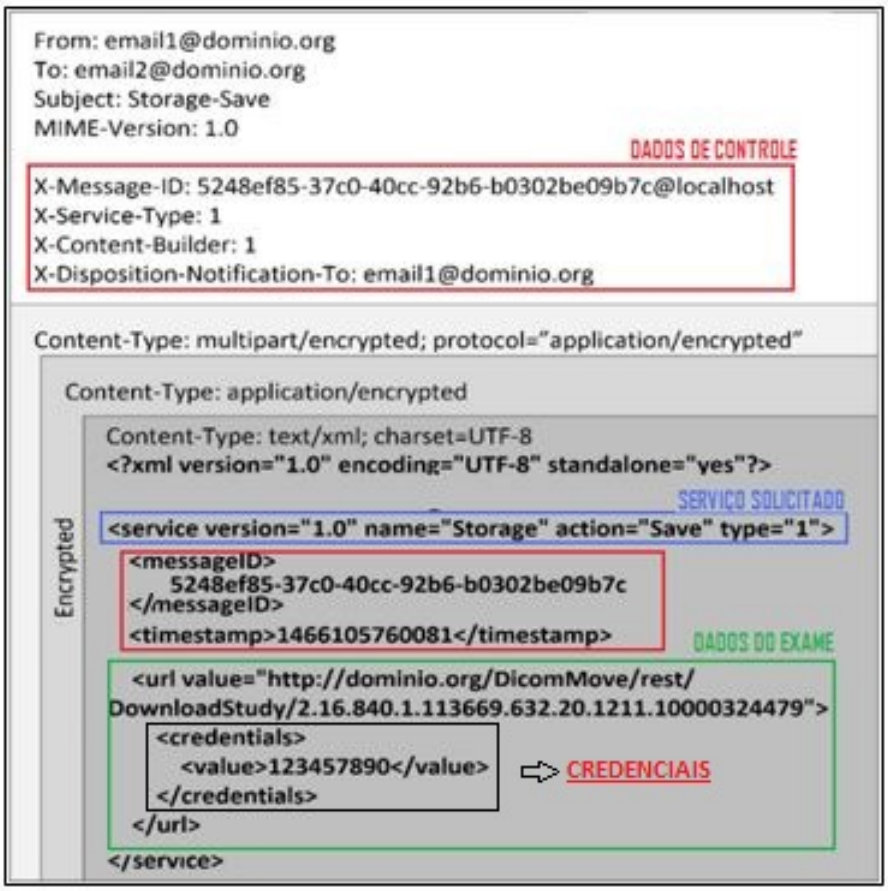



Figura 17: Estrutura de email proposta pelo DICOMFlow.
Fonte: Adaptada de (ARAUJO, 2017)

Com este cenário nota-se a grande dependência do originador da imagem para que o processo de emissão de laudo seja concluído com êxito. Este cenário funciona sem enfrentar maiores adversidades quando o exame de imagem está armazenado na própria entidade que solicitou o laudo.

Contudo, com a possibilidade de um armazenamento externo, o processo fica mais oneroso, pois, o proprietário da imagem (na Figura 16, HOSPITAL) terá que compartilhar a base de dados que mantem a associação entre URL da imagem, e-mail do radiologista e credencial gerada com o provedor de armazenamento externo e, sempre que alguma entidade externa necessitar acessar um exame armazenado externamente uma consulta deverá ser feita ao originador da imagem, tornando o processo síncrono, dependente da disponibilidade do originador da imagem e com uma base de dados centralizada, o que dificulta a escalabilidade

da solução.

Com a implantação do certificado de atributos a dependência e centralização pode ser removida dependendo da política de controle implementada. Ademais podem ser criadas funções de controle mais elaboradas, baseadas na checagem de data e hora de acesso ou tipo de exame requisitado. Outros detalhes da utilização do controle de acesso proposto pelo DFA são discutidos nas seções seguintes.

### 3.1.2 Criação do Certificado Digital de Atributos

A criação dos atributos para solução proposta, tem como principal finalidade prover maior flexibilidade ao controle de acesso original do DICOMFlow. Opções para controlar o dia de acesso, tipos de exames, intervalos de datas e outras opções que serão apresentadas ao longo dessa seção. Serão apresentados os atributos específicos para o controle de acesso e o papel de cada um deles e a implementação dos demais atributos presentes no certificado seguirá as recomendações da ICP-Brasil (ICP-BRASIL, 2016).

Os identificadores dos atributos (do inglês, Object Identifier (OID)) foram criados seguindo as orientações da Internet Assigned Numbers Authority (IANA), que é a entidade responsável por supervisionar a atribuição global dos números na Internet, como os números utilizados nas portas de comunicação, endereços IP ou números de domínio DNS. O prefixo desses identificadores foi cadastrado na IANA e pode ser consultado na URL http://oid-info.com/get/1.3.6.1.4.1.51022. Para fins de validação de nossa solução, os atributos necessários são apresentados na Tabela 2.

1. **version:** o valor deve ser "v2"conforme RFC 5755 (TURNER et al., 2010) e orientação da ICP-Brasil.

2. **holder:** Pessoa Jurídica ou Física que é titular do certificado de atributo. Neste atributo pode constar o CPF ou CNPJ do titular. Essa informação é retirada do Certificado Digital (CD) enviado para criação do Certificado de Atributos Vinculado. (CAV)

3. **idHolder:** Número de série do CD utilizado para vinculação durante a criação do CAV.

Tabela 2: Atributos do Certificado Digital de Atributos para uso no DFA.

| Nº | Atributo | OID | Descrição |
|---|---|---|---|
| 1 | version | 1.3.6.1.4.1.51022.1 | Versão |
| 2 | holder | 1.3.6.1.4.1.51022.2 | Titular do Certificado de Atributos |
| 3 | idHolder | 1.3.6.1.4.1.51022.3 | Número de Série do CD do titular |
| 4 | issuer | 1.3.6.1.4.1.51022.4 | Emissor do certificado de atributos |
| 5 | signature | 1.3.6.1.4.1.51022.5 | Algoritmo de Assinatura |
| 6 | serialNumber | 1.3.6.1.4.1.51022.6 | Número de série |
| 7 | validity | 1.3.6.1.4.1.51022.7 | Período de Validade do certificado |
| 8 | signatureValue | 1.3.6.1.4.1.51022.8 | Assinatura Digital |
| 9 | urlLCR | 1.3.6.1.4.1.51022.9 | Lista de Certificados Revogados da EEA |
| 10 | startDate | 1.3.6.1.4.1.51022.15 | Data inicial para acesso |
| 11 | endDate | 1.3.6.1.4.1.51022.16 | Data final para acesso |
| 12 | modalityType | 1.3.6.1.4.1.51022.17 | Tipo de estudo que poderá ser acessado |
| 13 | dayWeek | 1.3.6.1.4.1.51022.18 | Dia da semana de acesso |
| 14 | examId | 1.3.6.1.4.1.51022.19 | Identificador do exame a ser obtido |
| 15 | issuanceDate | 1.3.6.1.4.1.51022.20 | Data em que o certificado foi emitido |

4. **issuer:** Este campo contem nome único (*distinguished name-DN*) do emissor.

5. **signature:** Algoritmo utilizado para assinatura do CAV. Este algoritmo deve ser um dos algoritmos definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.

6. **serialNumber:** Número de série do certificado de atributos. O serialNumber deve ser um número inteiro e positivo com um limite máximo de até 20 octetos.

7. **validity:** Período de validade do certificado de atributos. Indica que ele não pode ser utilizado nem **antes** e nem **depois** das datas informadas nente atributo. Esta informação é referente a validade do certificado para fins de verificação de expiração. Não está vinculado aos atributos *startDate* e *endDate*, que servem para o controle de acesso validar o período de acesso as imagens. Formato: GeneralizedTime "AAAAMMDDHHMMSSZ".

8. **signatureValue:** Assinatura digital do emissor de certificado. Informação fundamental para conferir a autenticidade e validade jurídica do certificado de atributos emitido.

9. **urlLCR:** Endereço eletrônico que contem a base de dados para acesso a lista dos certificados revogados da EEA.

10. **startDate:** Data INICIAL para o acesso ao exame. Não será permitida tentativa de acesso antes desta data. Formato: GeneralizedTime "AAAAMMDDHHMMSSZ".

11. **endDate:** Data FINAL para o acesso ao exame. Não será permitida tentativa de acesso após esta data. Formato: GeneralizedTime "AAAAMMDDHHMMSSZ".

12. **modalityType:** Tipo do exame que poderá ser acessado. As *tags* seguiram a padronização proposta pelo protocolo DICOM. Exemplo: CT, CR, MR, US e outros.

13. **dayWeek:** Dia de semana em que a solicitação de acesso é permitida.

14. **examId:** Identificador Único do exame de imagem que poderá ser obtido. Todo exame de imagem encapsulado num objeto DICOM possui um identificador único na base de dados em que está armazenado. Apenas quando o identificador que constar neste atributo for igual ao do exame de imagem solicitado, a transferência será realizada.

15. **issuanceDate**: Data em que o certificado foi emitido. Parece uma redundância com o atributo *validity* mas ele se faz necessário em um cenário onde o uso do certificado é posterior a sua data de criação. Formato: GeneralizedTime "AAAAMMDDHHMMSS".

Nenhum dos atributos existentes no Certificado Digital de Atributos deve ser vazio ou duplicado. Uma situação possível é que seja necessário informar para os atributos de controle do DFA (*startDate, endDate, modalityType e dayWeek*) um valor genérico, como por exemplo, a necessidade do acesso acontecer todas as terças e quintas em um intervalo de datas, ou imagens de todas as modalidades podem ser obtidas por um determinado radiologista e outras inúmeras situações. Para isto, um carácter especial deve ser utilizado para generalizar o valor destes atributos, como por exemplo o asterisco ou cerquilha. Outra possibilidade é a necessidade de multi-valorar um atributo, *modalityType* por exemplo, isso é possível também fazendo a utilização de caracteres especiais dentro de uma mesma *string*.

### 3.1.3 Nova mensagem do DICOMFlow para aplicação do DFA

A proposta do DFA é alterar a forma como as credenciais são geradas e utilizadas durante o processo de controle de acesso a imagem proposto pelo DICOMFlow. As demais informações contidas na mensagem originalmente proposta não serão alteradas, exceto pela criação

de um novo serviço que será utilizado para solicitação de segunda opinião de um exame de imagem, situação que irá acrescentar algumas informações na estrutura da mensagem. Esse novo serviço será amplamente discutido na Seção 3.3. A Figura 18 contém um exemplo da estrutura da nova *tag*.


```
<credentials>
<value>
-------------------------- BEGIN CERTIFICATE --------------------------
PHZlcnNpb24+CnYyCjwvdmVyc2lvbj4KPGhvbGRlcj4KUmFkaW9sb2dpc3RhIEV4dGVybm8
KPC9ob2xkZXI+CjxpZEhvbGRlcj4KN2UgZDIgOTIgMTggMjEgMDAgNTEgZDYgNzMgOGYgMz
IgZTYgNjEgYWIgNDEgY2QKPC9pZEhvbGRlcj4KPGlzc3Vlcj4KSG9zcGl0YWwgU29saWN0Y
W50ZSBkbyBMYXVkbwo8L2lzc3Vlcj4KPHNpZ25hdHVyZT4KU2hhMXdpdGhSU0EKPC9zaWdu
YXR1cmU+CjxzZXJpYWxOdW1iZXI+CjUxIGU4IDUyIDExIDQ1ICBkYiA3OSA2OQo8L3Nlcml
hbE51bWJlcj4KPHZhbGlkaXR5PgoyMDE3MTEyNDIzNTk1OVoKPC92YWxpZGl0eT4KPHNpZ25
5hdHVyZVZhbHVlPgoyIDE2IDgwNCAxIDEwMSAzIDQgIDIgMQo8L3NpZ25hdHVyZVZhbHVlP
go8dXJsTENSPgpodHRwOi8vaG9zcGl0YWwuY29tLmJyL0xDQVIvbGlzdGEuY3JsCjwvdXJs
TENSPgo8c3RhcnREYXRlPgoyMDE3MTEyMDEyMzQzNVoKPC9zdGFydERhdGU+CjxlbmREYXR
lPgoyMDE3MTEyNDIzNTk1OVoKPC9lbmREYXRlPgo8bW9kYWxpdHlUeXBlPgpDVCNNUgo8L2
1vZGFsaXR5VHlwZT4KPGRheVdlZWs+ClRFUiNRVUEjUVVJCjwvZGF5V2Vlaz4KPGlzc3Vhb
mNlRGF0ZT4KMjAxNzEwMjAxMjM0MzVaCjwvaXNzdWFuY2VEYXRlPg==
--------------------------- END CERTIFICATE ---------------------------
</value>
</credentials>
```


Figura 18: Nova tag *credentials* na mensagem do DICOMFlow.
Fonte: Próprio autor

O certificado é codificado em Base64[1] e transportado dentro na *tag* **credentials** para posteriormente ser decodificado e fornecer uma estrutura XML com o conteúdo do certificado para análise do DFA.

Para atender a solicitação de acesso à imagem, o DICOMFlow instalado no ARMAZENAMENTO EXTERNO passará para o DFA o certificado de atributos e o certificado digital. Uma estrutura que representa o conteúdo do certificado de atributos no formato XML está na Figura 19. Com essas informações, o DFA fará a verificação sintática e analisará os atributos a fim de determinar se o acesso pode ser feito.

Na figura, é possível observar, agora em XML, os atributos existentes no Certificado

[1]É um método para codificação de dados para transferência na Internet. Constantemente utilizado na transmissão de dados que lidam apenas com texto, como por exemplo, no envio de arquivos anexados em e-mail. Mais detalhes podem ser obtidos na RFC 4648 (JOSEFSSON, 2006).


Figura 19: Estrutura XML do certificado de atributos decodificado.
Fonte: Próprio autor

Digital de Atributos apresentado pelo radiologista. Os atributos que referenciam datas (*validity, startDate, endDate e issuanceDate*) estão representados na notação Abstract Syntax Notation One[2] (ASN.1) como recomenda a ICP-Brasil. Observa-se também a utilização de um carácter curinga (a cerquilha) para atributos (*modalityType* e *dayWeek*) cujo conteúdo pode ser multi-valorado. Na seção a seguir é feito o detalhamento da análise dos atributos pelo DFA e qual o papel de cada módulo existente. Na próxima seção apresentaremos a arquitetura do DFA.

## 3.2 Arquitetura do DFA

O DFA está posicionado como um módulo de suporte ao controle de acesso do DICOM-Flow. Nesse novo esquema, a requisição de acesso que originalmente era encaminhada ao DICOMFlow para análise das credenciais e decisão de acesso, passa a ser desmembrada entre o DICOMFLow e o DFA. Em relação a autenticação, o processo adotado pelo DICOMFlow, que é a utilização do Amazon Web Services, continua funcional. Entretanto, o processo de autorização, que antes era feito através de uma base de dados centralizada, para a ser exe-

[2]É descrito por (LARMOUTH, 2000) como uma notação formal usada para descrever dados transmitidos por protocolos de telecomunicações, independentemente da implementação da linguagem e da representação física desses dados, seja qual for a aplicação, seja ela complexa ou muito simples.

cutado pelo DFA. Um aspecto interessante desta arquitetura, que foi concebida baseando-se na arquitetura de referência XACML, já introduzida no Capítulo 2, é que os módulos podem ser distribuídos em infraestruturas diferentes, pois não observou-se restrição no modelo de referência da arquitetura XACML para tal situação. Entretanto, não se deve alterar o fluxo em que os dados são repassados entre os módulos.

Com a finalidade de facilitar a implementação e validação da nossa proposta, decidimos combinar os módulos PAP, PRP e PIP em um único módulo que manteremos o nome PAP. Também implementamos algumas mudanças em suas funcionalidades originalmente especificadas em (OASIS, 2017) para tornar mais suave a acomodação de uma necessidade primária na infraestrutura como propomos. Que é fornecer um mecanismo de controle de uso dos recursos ofertados pelos parceiros das entidades de saúde (e.g. armazenamento e/ou processamento de exames de imagem). Basicamente, incorporamos as atividades que são relativas aos módulos PRP e PIP ao módulo PAP e, em nossa implementação, tudo é visto como um único módulo administrativo. Na Figura 20, apresentamos uma visão do fluxo interno do DFA e posteriormente é descrito o passo a passo até a resposta da decisão de acesso para o DICOMFlow. Nas subseções seguintes são detalhadas as atividades executadas por cada módulo.

1. **Passo 1:** o DICOMFlow recebe, via HTTPS, a solicitação de acesso a uma imagem e encaminha para o PEP os certificados (de atributos e digital) para serem validadas;

2. **Passo 2:** após o processo de validação, o PEP encaminha para o PDP os atributos afim de que sejam analisados.

3. **Passo 3:** após se certificar que os atributos permitem o acesso a imagem, o PDP consulta o PAP em busca de uma possível sinalização que remeta a negação do acesso.

4. **Passo 4:** o PAP responde essa solicitação do PDP analisando as informações contidas em sua base de dados.

5. **Passo 5:** de posse da resposta do PAP, o PDP encaminha que ação o PEP deve informação para o DICOMFlow.

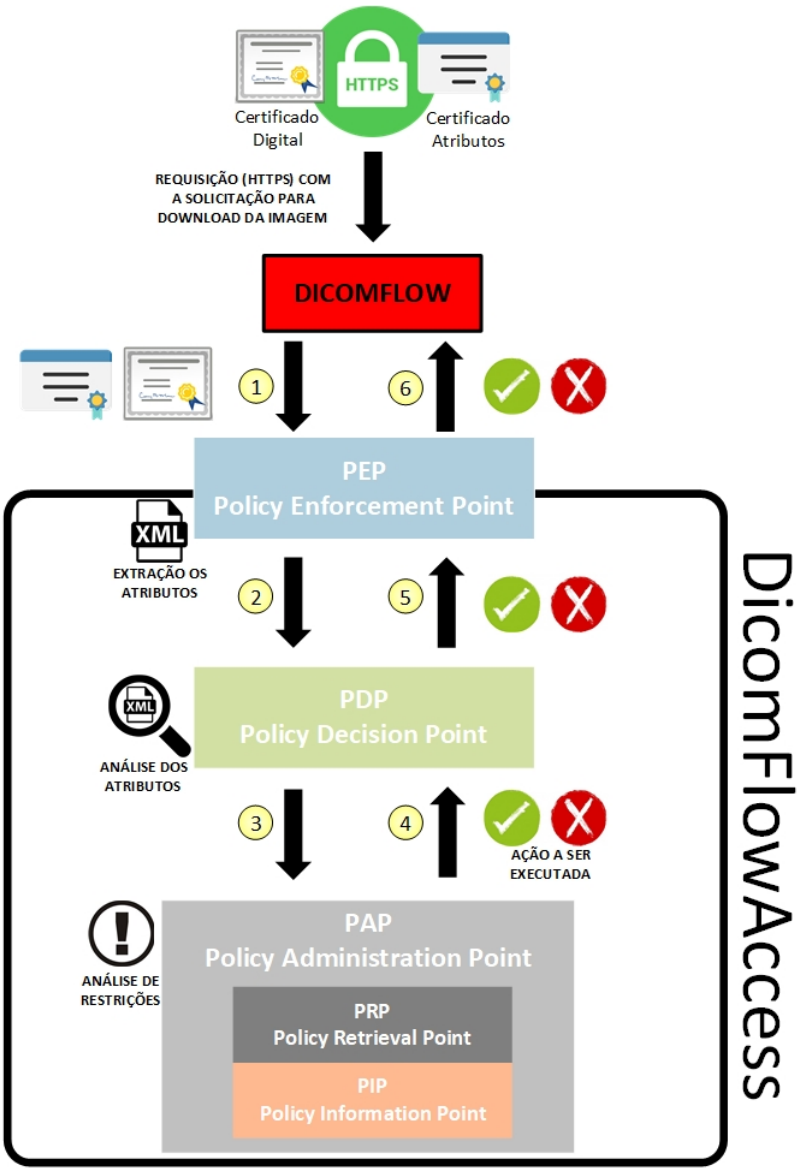



Figura 20: Arquitetura do DFA integrada ao DICOMflow.
Fonte: Próprio autor

6. **Passo 6:** o PEP informa ao DICOMFlow que ação executar. Se realiza ou não o envio da imagem.

Como dito anteriormente, os elementos PRP e PIP da arquitetura de referência do XACML foram incorporados pelo PAP. A base de dados e as informações dos atributos serão consideradas atividades administrativas pela nossa solução. Sendo assim, foram incorporadas pelo PAP. Nas demais subseções são apresentadas as funções de cada módulo existente na Arquitetura do DFA. Nas seções seguintes, são descritas as atividades executadas pelos módulos

do DFA. É importante ressaltar que tais ações são executadas após o processo de autenticação ter sido processado com sucesso pelo DICOMFlow. Como descrito na Seção 2.5 do Capítulo 2.

### 3.2.1 Ações executadas pelo Policy Enforcement Point (PEP)

O PEP é o módulo responsável pela emissão da resposta acerca da solicitação de acesso feita para o DICOMFlow instalado aonde a imagem está armazenada. Também é responsável pela validação de algumas políticas de controle de acesso pré-definidas na arquitetura. As tarefas incumbidas a este módulo são:

1. Conectar o DFA com o DICOMFlow. Apenas este módulo é acessível pelo DICOMFlow;
2. Receber e validar os certificados (atributos e digital) encaminhados pelo DICOMFlow;
3. Extrair as informações contidas no certificado de atributos e encaminhá-las para o PDP;
4. Informar ao DICOMFLow qual decisão foi tomada em relação ao acesso à imagem durante o processamento dos atributos.

O processo de validação do certificado de atributos passa pelas seguintes etapas: (1) verificar se o certificado está no período de validade, (2) validar a associação entre o certificado de atributos e o certificado digital do solicitante e (3) verificar se o certificado de atributos não está na lista de certificados revogados da EEA. Esta última é feita utilizando o protocolo Online Certificate Status Protocol (OCSP). Apenas após estas validações é que os atributos são passados para análise do PDP.

- **Verificação do período de validade:** esta informação obrigatoriamente deve estar presente no certificado. O campo *validity* possui duas informações que são analisadas: *notBeforeTime* e *notAfterTime*. Isto indica que o certificado não pode ser utilizado fora do intervalo dessas datas.
- **Validação da associação entre o CA e o CD:** todo certificado de atributo vinculado, que é o utilizado no DFA, possui o número de série do certificado digital utilizado

para fazer a associação entre CA e CD. Esta comparação é a forma de certificar que o certificado de atributos apresentado foi emitido para uso em conjunto somente com este certificado digital apresentado.

- **Verificação da lista de certificados revogados da EEA:** o PEP consulta a EEA a respeito do *status* do Certificado Digital de Atributos (utilizando o OCSP). Este mecanismo de validação é útil no caso de um certificado precisar ser suspenso por causa de um vínculo empregatício ou uma parceria ser encerrada. O certificado pode estar na validade, porém foi revogado pela EEA.

Caso alguma dessas validações tenha uma verificação negativa, o PEP imediatamente informa ao DICOMFlow que o acesso a imagem não pode ser realizado e o DICOMFlow não faz o envio do exame de imagem solicitado. É importante reforçar que o DFA é responsável pelo processo de autorização de acesso às imagens médicas. Sendo o DICOMFlow o responsável pelo processo de autenticação de usuários.

### 3.2.2 Ações executadas pelo Policy Decision Point (PDP)

O PDP tem a função de validar os atributos exclusivos do controle de acesso e verificar caso alguma restrição às entidades envolvidas na solicitação existe no PAP. Assim como o PEP, é responsável pela aplicação de algumas políticas de controlde de acesso pré-estabelecidas na arquitetura. O processo de validação consiste em verificar a sintaxe e lógica das informações presentes no certificado de atributos, porém, nenhuma ação relacionada à validação do certificado de atributos é feita neste módulo, pois seria redundância, já que essa é uma das atribuições PEP, e neste ponto da análise do controle de acesso, as validações relacionadas ao certificado de atributos já foram executadas. As atividades realizadas pelo PDP são discutidas a seguir.

- **Verificação da integridade dos atributos:** não só a sintaxe dos dados apresentados são analisados. Uma situação que exemplifica bem essa função é no caso de preenchimento equivocado de alguma informação, por exemplo, o valor da data do atributos *startDate* ser anterior ao valor preenchido no atributo *endDate*. Diante desta situação, o PDP informa ao PEP que existe inconsistência de informações e o PEP fará a negação do acesso.

- **Verificação da validade dos atributos:** neste momento da verificação, não foi constatada nenhuma inconsistência nos dados e a checagem é executada. Verificações como o tipo de exame permitido ou se a requisição está sendo realizada no intervalo de datas apresentado no certificado são feitas.

- **Consulta ao PAP:** eventualmente alguma restrição de acesso pode estar presente na entidade em que o exame de imagem é armazenado, esta informação é mantida pelo PAP e sempre será consultada pelo PDP antes da tomada de decisão, mais detalhes a respeito do PAP são discutidos na próxima seção.

### 3.2.3 Ações executadas pelo Policy Administration Point (PAP)

É o módulo responsável por manter as políticas dinâmicas de controle de acesso. Em nossa infraestrutura, o PAP atua como um módulo que servirá para prover a implantação das regras de negócio pela entidade contratada pelo originador da imagem (na Figura 16, ARMAZENAMENTO EXTERNO e HOSPITAL, respectivamente), visando atender a necessidades pontuais/contextuais. Essas questões seriam aplicadas através da expansão dos atributos dos Certificados de Atributos e consequentemente haverá a necessidade de uma política de controle de acesso para poder validar essas novas implementações.

Por exemplo, se um contratante está inadimplente ou o limite de *upload* em um determinado intervalo de datas foi excedido, e essas situações, contratualmente, são passíveis de interrupção do serviço, uma sinalização proibitiva de acesso às imagens armazenadas deste contratante pode ser criada e quando o PDP fizer a consulta sobre a condição do contratante, o PAP informará que existe uma restrição e então a decisão de não permitir a transferência da imagem é informada e repassada para o PEP para posteriormente ser informada ao DICOMFlow. Essa sinalização é prevista em nossa arquitetura, porém, não foi investigada profundamente e sua implementação nos experimentos (apresentados no Capítulo 4) visou apenas atestar a correta execução do fluxo de ações executadas pelo DFA. Todos os serviços sob a responsabilidade do PRP e PIP que são propostos na arquitetura de referência, já discutidos no Capítulo 2, também serão incorporados a estrutura do PAP.

### 3.2.4 PGCA - Política Geral de Controle de Acesso

Esta seção tem o objetivo de descrever a política básica que irá ser aplicada no processo de autenticação e autorização de solicitações. O DFA funciona com o mecanismo de *white list*, isto é, apenas o que está explícito no Certificado de Atributos apresentado durante a solicitação de resgate do exame de imagem é que será permitido. A aplicação desta política está distribuída entre os módulos PEP e PDP da infraestrutura do DFA e para tal, foi utilizada a codificação *hard code*[3] para sua implementação. O PAP é o módulo responsável por gerenciar as políticas dinâmicas, entretanto, para fins de validação de nossa solução, iremos utilizar a codificação *hard code* diretamente no PEP e PDP. Discutiremos mais a respeito da utilização do PAP ainda neste subseção.

Os termos abaixo, quando encontrados grafados em maiúsculos na descrição das políticas de controle de acesso, DEVEM ser interpretados conforme descrito abaixo.

1. DEVE (D): Esta palavra, ou os termos "EXIGIDO" ou "OBRIGATÓRIO", significa que a definição é um requisito absoluto da política.

2. NÃO DEVE (ND) Esta expressão, ou o termo "PROIBIDO" significa que a definição é uma proibição absoluta na política.

3. RECOMENDADO (R): Esta expressão significa que podem existir razões válidas, em situações específicas, para ignorar um ponto específico. Entretanto, as implicações completas precisam ser entendidas e ponderadas cuidadosamente antes de escolher uma atitude diferente.

4. NÃO RECOMENDADO (NR): Esta expressão significa que podem existir razões válidas, em situações específicas, em que o comportamento possa ser aceitável ou mesmo útil. Entretanto, as implicações devem ser entendidas e ponderadas cuidadosamente antes de realizar qualquer comportamento descrito com esse rótulo.

5. PODE (P): Esta palavra, ou o adjetivo "OPCIONAL", significa que é um item verdadeiramente opcional. Um implementador pode optar por incluir o item, enquanto outro

[3]Refere-se à prática de desenvolvimento de software de embutir dados diretamente no código fonte de um programa ou outro objeto executável, ao invés de obter os dados de fontes externas ou gerá-los dinamicamente em tempo de execução. Modificações são realizadas através do controle de versão.

pode omitir o mesmo. Uma aplicação que incluir uma determinada opção **DEVE** estar preparada para interoperar com outra aplicação que inclui aquela opção, embora talvez com funcionalidade reduzida.

### 3.2.5 Definição das política de controle de acesso

Esta subseção tem a finalidade de expor os pormenores da Política Geral de Controle de Acesso. É relevante reforçar três aspectos da implementação desta política. (1) Esta é uma política elementar para o funcionamento do DFA da forma que idealizamos, (2) foi implementa utilizando a metodologia *hard code* e (3) foi implementada nos mecanismos de PEP e PDP da infraestrutura. Implementações para atender as particularidades de situações que venham a surgir serão realizadas posteriormente, utilizando atributos dinâmicos manipulados via XACML. Abordaremos mais a respeito de atributos dinâmicos no final desta subseção. Abaixo apresentamos as políticas que implementamos do DFA e destacaremos que módulo do DFA a impõe.

- *Policy 1 (PEP):* Todo Certificado Digital de Atributos (CA) **DEVE** estar associado a um Certificado Digital de Identidade (CD). O atributo *idHolder* do CA **DEVE** corresponder ao atributo *serialNumber* do CD associado a ele.

- *Policy 2 (PEP):* Os certificados apresentados durante o resgate do exame de imagem **DEVEM** estar dentro de período de validade e, no caso do CD, ser válido na cadeia de certificados da ICP-Brasil.

- *Policy 3 (PEP):* É **OPCIONAL** fazer a implementação das três opções de validação dos certificados simultaneamente. Entretanto, é fortemente **RECOMENDADO** que todas estejam habilitadas para executar o processo de validação dos certificados apresentados.

- *Policy 4 (PEP):* O CA apresentado para solicitação de resgate do exame de imagem **NÃO DEVE** apresentar nenhum atributo sem valor. Caso o atributo seja multivalorado, um carácter especial deve representar essa condição. Por exemplo: Um CA permite obter várias modalidades de exame. O valor do atributo *modalityType* seria **DOC#CT#MR#ES#RF**. Nesta sintaxe, cada modalidade é separada pelo carácter #.

O caractere com a função de separação de atributos, que implica que todas as modalidades podem ser obtidas, é a palavra **ALL**.

- *Policy 5 (PDP):* É **PROIBIDO** o acesso aos exames de imagens em uma data que não esteja entre as datas apresentas nos atributos *startDate* e *endDate* do CA.
- *Policy 6 (PDP):* As modalidades inseridas no atributo *modalityType* do CA **DEVEM** pertencer ao conjunto de *tags* que representam as modalidades existentes na documentação do DICOM.
- *Policy 7 (PDP):* é **OPCIONAL** a utilização do atributo *dayWeek*, entretando, se utilizado, a requisição **DEVE** obedecer o(os) dia(as) especificados neste atributo com abreviação de TRÊS letras em português (e.g. SEG, TER, QUA). Um carácter que generalize **DEVE** ser utilizado para especificar todos os dias da semana.

Como citado anteriormente, a implementação da Política Geral de Controle de Acesso (PGCA) foi feita usando a metodologia *hard code*. Abaixo segue um código que exemplifica a implementação da *Policy 4*. Política que tem a finalidade de verificar se as modalidades que foram inseridas no CA apresentado durante a solicitação de resgate do exame de imagem correspondem as abreviações existentes da documentação DICOM.

```
1 public class ValidaModalidade {
2 public static void main(String[] args) {
3 String modalidadesCA = "DOC#CT#MR#ES#RF";
4 String[] modalidade = modalidadesCA.split("\\#+");
5 String regex = "(?i)ALL|AR|ASMT|AU|BDUS|BI|BMD|CR|CT|DG|DOC|DX|ECG|
   EPS|ES|FID|GM|HC|HD|IO|IOL|IVOCT|IVUS|KER|KO|LEN|LS|MG|MR|NM|OAM
   |OCT|OP|OPM|OPT|OPV|OSS|OT|PLAN|PR|PT|PX|REG|RESP|RF|RG|RTDOSE|
   RTIMAGE|RTPLAN|RTRECORD|RTSTRUCT|RWV|SEG|SM|SMR|SR|SRF|STAIN|TG|
   US|VA|XA|XC";
6 for (String str : modalidade) {
7 if (str.matches(regex)) {
8 System.out.println(str+ ": Modalidade valida"); }
9 else {
```

```
10 System.out.println(str+ ": Modalidade invalida");}
11           }
12      }
13 }
```

Na linha 3, a variável **modalidadesCA** corresponde as modalidades que foram autorizadas pelo solicitante do laudo, em nosso cenário, HOSPITAL 1. E foram extraídas do CA apresentado durante o resgate do exame de imagem. Na linha 4 é feita a separação dessas modalidades para verificação. Na linha 5, a variável **regex** armazena uma expressão regular[4] que armazena os modalidades existentes na documentação do padrão DICOM. No início do valor dessa variável podemos observar o texto *(?i)ALL*, a primeira parte do texto *(?i)* é usada para não fazer distinção entre caracteres maiúsculos e minúsculos, a segunda parte *(ALL)* foi utilizada por nós para informar que todas as modalidades de exame de imagem são autorizadas para resgate. O restante do código é o laço para validação das modalidades informadas no CA.

Entretanto, existe a possibilidade de mudanças nesses atributos. Por exemplo, as abreviações das modalidades podem ser alteradas, ocasionando a desatualização da expressão regular existente no código. Prevendo isso, o PAP é o módulo responsável pela implementação de políticas dinâmicas. Neste trabalho não fizemos este tipo de implementação, entretanto, criamos a possibilidade dessa expansão e fizemos uma simulação de seu funcionamento. Mais destalhes dessa simulação serão apresentados no Capítulo 4. Na próxima seção serão apresentados alguns cenários possíveis com o DFA desempenhando o papel de mecanismo de controle de acesso na rede proposta pelo DICOMFlow.

## 3.3 Cenários de uso

Nesta seção, serão discutidos dois cenários possíveis com a nossa solução que não é possível com o modelo de controle de acesso inicialmente proposto pelo DICOMFlow. O objetivo é mostrar que uma situação comum como a solicitação de uma segunda opinião, que é uma

[4]Uma expressão regular é uma notação para representar padrões em *strings*. Serve para validar entradas de dados ou fazer busca e extração de informações em textos.

ação que iriá demandar um fluxo de trabalho mais complexo utilizando a proposta inicial de controle de acesso, torna-se uma tarefa mais simples e segura com a implementação do DFA. O outro cenário é a transferência direta do exame de imagem entre radiologistas.

### 3.3.1 Emissão de segunda opinião de laudo

A emissão de laudo contendo uma segunda opinião é uma atividade bastante comum na telerradiologia. Contudo, o controle de acesso proposto pelo DICOMFlow apresenta dificuldades durante esta atividade, como a necessidade do compartilhamento da base de dados de controle de acesso. Inicialmente pensou-se que a forma mais simples seria o repasse direto da imagem entre os radiologistas, e tecnicamente é mais simples. Bastaria o radiologista destinatário da solicitação da segunda opinião instalar o DICOMFlow e ter uma conta de email, esta facilidade foi propositalmente criada pelo DICOMFlow. Todavia, desta forma, o proprietário do exame de imagem (e.g. um hospital ou clínica aonde o exame foi realizado) não teria o controle sob ela, fato este que não é o ideal.

Desta forma foi adicionado um novo serviço aos inicialmente propostos pelo DICOMFlow (ver Seção 4.2 de (ARAUJO, 2017)), o *SecondOpinion*, com duas ações, *put*, para indicar a solicitação da segunda opinião e o *result*, que é para confirmar o recebimento desta solicitação. Com isso o próprio médico radiologista emissor do primeiro laudo pode indicar ao hospital ou clínica a análise do exame de imagem por outro médico radiologista, cabendo a eles solicitar ou não. A vantagem obtida com essa nova forma de emissão de segunda opinião é o compartilhamento do *network* de vários médicos radiologistas de forma padronizada e escalável mantendo o controle do acesso a imagem com seu proprietário.

Durante a execução do passo 8, na Figura 16, o radiologista envia o laudo e, neste momento, ele indica na mensagem enviada ao hospital que seria recomendado obter uma segunda opinião. Nesta mensagem, tem o e-mail do médico radiologista indicado por ele. Caso este médico já faça parte da rede de contatos do hospital e possuir um certificado de atributos válido, o hospital encaminha uma solicitação de laudo sem a necessidade da troca de mensagens para criação do certificado. Caso o hospital não tenha registro do novo médico, o processo de emissão do certificado descrito na Figura 16 é feito desde o início. Vale

reforçar que o novo radiologista terá que possuir uma instância compatível com o protocolo do DICOMFlow instalada em seu computador. Desta forma, é possível criar uma rede social para telerradiologia compartilhando competências e ampliando seu alcance.

### 3.3.2 Transferência de imagens entre radiologistas

Ainda que a transferência direta não seja o cenário ideal, pois, conforme discutido na Subseção 3.3.1, o indicado é que o proprietário da imagem tenha esse controle sob sua distribuição, com o certificado de atributos e o estabelecimento de acordos de serviços, um hospital pode criar um certificado de atributos "genérico" que dará acesso as suas imagens hospedas em um armazenamento externo e o entregar a um radiologista de sua escolha para atuar, por exemplo, como consultor externo. A transferência da imagem não será feita diretamente de um radiologista para outro em uma conexão ponto-a-ponto. Para que isso fosse possível, cada radiologista teria que possuir um endereço IP público e estático para o serviço HTTPS ser configurado sobre ele e publicado na Internet, ou a adoção de mecanismos de redirecionamento de tráfego em conjunto com serviços de DNS Dinâmico, situações que tornariam o processo muito complexo.

A ideia é repassar ao médico radiologista que emitirá a segunda opinião a URL para obter o exame e o email do hospital que fez a solicitação inicial. De posse dessas informações o *download* da imagem pode ser feito e o laudo com a segunda opinião emitido. No momento desse repasse, o radiologista que recebeu a solicitação inicial pode informar ao hospital que está fazendo essa solicitação de segunda opinião. Esse recurso é utilizado na situação em que o médico radiologista emissor da segunda opinião já possui o certificado de atributos válido e emitido pelo originador da imagem, para só assim, obter a o exame de imagem. Caso o radiologista emissor da segunda opinião não tenha este certificado de atributos, o cenário exposto na Subseção 3.3.1 é o indicado.

A diferença entre as duas formas de emitir uma segunda opinião é que na primeira delas, o médico radiologista que recebeu a demanda inicial para emissão de laudo, indica ao hospital o contato (e-mail) do médico que poderá emitir a segunda opinião. E cabe ao hospital decidir se irá fazer a solicitação ou não. Na segunda forma, o hospital não toma essa decisão,

mas deve ser informado. Neste segundo cenário, o médico radiologista emissor do primeiro laudo quem faz o encaminhamento da solicitação para elaboração de um segunda opinião para outros radiologistas de sua rede de contatos. Na Figura 21, que utiliza como base a Figura 16, apenas adicionando a entidade RADIOLOGISTA 2, pode-se observar os passos de forma resumida para a emissão de segunda opinião com o encaminhamento direto entre radiologistas. Para facilitar o entendimento, estamos abstraindo as trocas de mensagens iniciais já discutidas anteriormente.

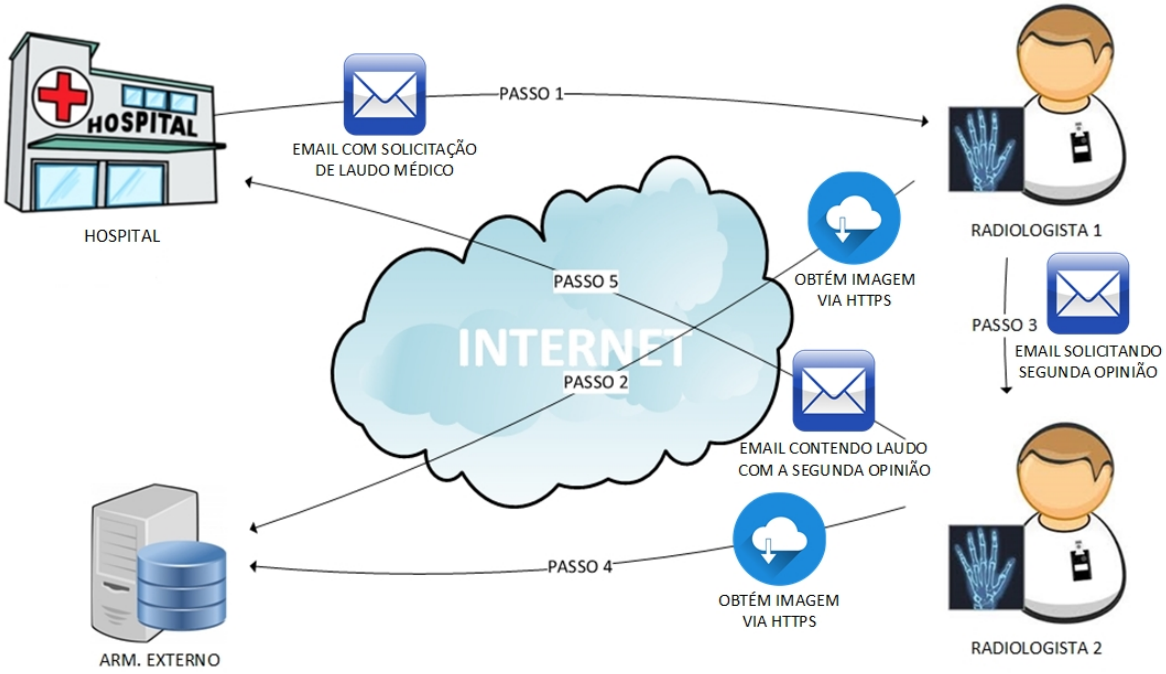



Figura 21: Fluxo de mensagens para a emissão de segunda opinião em laudo.
Fonte: Próprio autor

1. **Passo 1:** O HOSPITAL faz a solicitação de emissão de laudo para o RADIOLOGISTA 1. Nesta mensagem, como detalhado anteriormente, contém dentre outras informações, a URL para obter o exame e o email do solicitante do laudo, neste cenário, HOSPITAL;

2. **Passo 2:** O RADIOLOGISTA 1 obtém a imagem previamente enviada para o ARMAZENAMENTO EXTERNO pelo HOSPITAL;

3. **Passo 3:** O RADIOLOGISTA 1 encaminha a solicitação de segunda opinião para o RADIOLOGISTA 2. O RADIOLOGISTA 2 possui um Certificado de Atributos

emitido por HOSPITAL que dá acesso a qualquer imagem originada por ele, que foi transferida para o ARMAZENAMENTO EXTERNO. As regras desse Certificado de Atributos podem limitar qual modalidade de estudo ele poderá ter acesso, qual o intervalo de datas o acesso pode ser feito ou qual o horário do dia. Os atributos deste Certificado de Atributos é baseado no acordo previamente estabelecido entre HOSPITAL e RADIOLOGISTA 2.

4. **Passo 4:** De posse da URL para obter o exame, a imagem é obtida após passar pelo processo de validação do DFA;

5. **Passo 5:** O laudo com a segunda opinião é enviado para o HOSPITAL, que é o solicitante do laudo inicial.

Dois aspectos devem ser destacados neste momento. (1) Existe um acordo comercial previamente estabelecido entre HOSPITAL e RADIOLOGISTA 2. Caso não haja esse acordo e o RADIOLOGISTA 2 e HOSPITAL não sejam parceiros, a forma de emissão da segunda opinião é a descrita na Subseção 3.3.1, na qual o RADIOLOGISTA 1, juntamente com o seu laudo emitido, indica ao HOSPITAL outro radiologista para emissão de um laudo contendo a segunda opinião a respeito de exame de imagem e cabe ao HOSPITAL decidir se solicita ou não esse laudo com a segunda opinião. E (2) as entidades envolvidas devem possuir o módulo do DICOMFlow disponível para formar a rede colaborativa entre elas.

## 3.4 Considerações finais

Neste capítulo, foram apresentadas as abordagens para propor um mecanismo de controle de acesso que atendesse a demanda de uma infraestrutura que seja (1) descentralizada, isto é, sem um ponto central para sempre convergir o processo de autenticação e autorização, (2) aberta e compartilhada, na qual entidades podem associar-se para realizar atividades atendendo a requisitos mínimos para padronização e controle e (3) assíncrona, que não necessite de conexão ativa para o desenvolvimento das atividades desejadas.

O DICOMFlowAccess foi desenvolvido utilizando um conjunto de tecnologias existentes que foram apresentadas no Capítulo 2. Algumas já consolidadas, como certificados digitais

e protocolos para transmissão de dados na Internet e outras ainda em experimento ou não tão populares, como o DICOMFlow (ARAUJO, 2017) e o XACML[5] (OASIS, 2017). Seu principal propósito é ser um controle de acesso capaz de suprir as necessidades de entidades (no nosso cenário, são as que praticam telerradiologia) criarem livre associação, duradoura ou não, para realizarem atividades corriqueiras como o compartilhamento de exames de imagens médicas, emissão de laudos médicos e segunda opinião de um laudo. A respeito do *workflow* para emissão de segunda opinião de laudo, foi decido em projeto, que não haveria a total liberdade da delegação de acesso à imagem médica sem a prévia autorização do originador do exame de imagem (HOSPITAL), que é seu fiel depositário, visto que o proprietário da imagem, legalmente, é o paciente. Essa característica é um aspecto social da solução, uma vez que, tecnicamente, é possível fazer o repasse direto da imagem no modelo proposto, porém, esta funcionalidade não foi implementada.

O DICOMFlow, proposto em (ARAUJO, 2017), é um *gateway* cujo principal propósito é interligar, de forma padronizada, estruturas terradiológicas PACS/DICOM (ver Seção 2.5 do Capítulo 2) e foi utilizado como base para idealização do DICOMFlowAccess (DFA), que é um mecanismo de controle de acesso baseado em certificados digitais capaz de prover grande escalabilidade e flexibilidade para o compartilhamento seguro de informações. Na infraestrutura do DICOMFlow, o DFA atua como um módulo que receberá a demanda de solicitação de acesso a imagens médicas e internamente tomará a decisão de liberação utilizando uma arquitetura adaptada do XACML proposta por (OASIS, 2017).

Como resultado dessa soma de tecnologias, o DFA mostrou-se, teoricamente, ser uma ferramenta capaz de prover controle de acesso para compartilhamento de imagens médicas entre entidades numa rede colaborativa que utilizam a Internet como infraestrutura de interconexão. Cenário em que as atuais implementações/propostas de controle de acesso encontram muitos obstáculos para tornar essas associações funcionais, comprometendo principalmente a sua escalabilidade, que é um requisito fundamental no crescimento de uma infraestrutura aberta e compartilhada.

[5]Nessa primeira implementação, adaptamos a Arquitetura de Referência do XACML para criar o modelo arquitetural do DFA. Exite a possibilidade da aplicação do XACML para o funcionamento das políticas dinâmicas de controle de acesso. Contudo, mais estudos são necessários para tal aplicação.

# CAPÍTULO 4

# EXPERIMENTOS

Este capítulo tem como objetivo avaliar o funcionamento do DICOMFlowAccess (DFA) em ambiente simulado que reproduz cenários comuns, já descritos neste trabalho, para a prática da telerradiologia entre entidades de saúde e seus parceiros. O cenário utilizado será o apresentado na Figura 16 (ver Seção 3.1 do Capítulo 3) e levamos em consideração que os exames de imagens médicas já estão armazenadas no ARMAZENAMENTO EXTERNO, parceiro do HOSPITAL para prover o serviço de armazenamento remoto dos exames de imagens gerados por ele. Vale reforçar que o transporte desses exames entre as entidades supracitadas utiliza um protocolo previamente negociado entre elas. Pode-se utilizar uma rede privada virtual, soluções *peer-to-peer*, o próprio DICOMFlow ou outro protocolo já estabelecido na Internet. Outro aspecto relevante é que todas as entidades estão interligadas com um módulo DICOMFlow afim de estabelecer a rede colaborativa para troca de exames de imagens médicas e a emissão de laudos médicos. O restante deste capítulo está organizado da seguinte forma: A Seção 4.1 apresenta o ambiente utilizado e as tecnologias utilizadas para concebê-lo. A próxima seção (Seção 4.2) descreve cada um dos testes utilizados e apresenta seus resultados.

## 4.1 Ambiente utilizado na validação do DFA

Como comentado na introdução deste capítulo, utilizamos a tecnologia de virtualização de sistemas operacionais para montagem do cenário e cada entidade nele existente será representada por uma máquina virtual. Nesta seção descrevemos quais os *hardwares* e *softwares* utilizados. A Tabela 3 contem as configurações das máquinas utilizadas nos experimentos.

Tabela 3: Especificações do *hardware* e *software* utilizados nos experimentos.

| **Recurso** | **Hospedeiro** | **VM 1** | **VM 2** | **VM 3** |
|---|---|---|---|---|
| CPU | Intel i5 2.4Ghz | – | – | – |
| Memória | DDR3 8GB | 1GB | 1GB | 1GB |
| Disco | 640GB 7200 RPM | 15GB | 40GB | 15GB |
| OS | Windows 10 Pro x64 | Windows 7 Pro | Windows 2008 | Ubuntu 16.10 LTS |
| Endereço IP | – | 192.168.0.100 | 192.168.0.111 | 192.168.0.112 |
| JVM | – | JDK 9.0.1 | JDK 9.0.1 | JDK 9.0.1 |
| Virtualizador | VirtualBox 5.2.8 | – | – | – |
| BD | – | Postgres 8.3 | MySQL 5.1 | MySQL 5.1 |
| DCM4CHEE | – | versão 2.18.x | versão 2.17.x | versão 2.18.x |
| DCM4CHEEToolKit | – | versão2.0.23 | versão 2.0.29 | versão 2.0.23 |
| DICOMFlow | – | versão 1.2 | versão 1.2 | versão 1.2 |
| JBOSS | – | versão 4.2.3.GA | versão 4.2.3.GA | versão 4.2.3.GA |
| Tomcat | – | versão 7.0.29 | versão 7.0.29 | versão 7.0.29 |
| Entidade | – | HOSPITAL | ARM. EXTERNO | RADIOLOGISTA |

O HOSPITAL será representado pela VM1, as tarefas executadas ou direcionadas ao ARMAZENAMENTO EXTERNO serão realizadas pela VM2 e o RADIOLOGISTA será representado pela VM3. A rede virtual criada pelo *software* virtualizador é o meio de comunicação entre as máquinas virtuais. Todos as adaptadores estão configurados para permitirem a comunicação somente entre o ambiente virtual, sem qualquer conectividade com a Internet e nem com a máquina hospedeira. Todos os sistemas operacionais estão com as últimas atualizações de pacotes disponibilizadas pelos seus fabricantes até a da 05/10/2018. Nenhum aplicativo de antivírus foi utilizado, nenhuma regra de *firewall* foi implementada e não foi imposta nenhuma limitação no uso do processador pelas máquinas virtuais.

O serviço de correio eletrônico está configurado na VM2 (ARMAZENAMENTO EXTERNO). Decidiu-se não utilizar um serviço ofertado gratuitamente na Internet porque houve a necessidade da criação de várias contas de usuário durante a simulação de escalabilidade do DFA. Para ofertar este serviço, foi utilizado o *software* hMailServer v5.6.7 que é distribuído sob a licença AGPLv3 e nele configurado o domínio *@dfa.com*. O cenário implementado

pode ser visualizado na Figura 22.

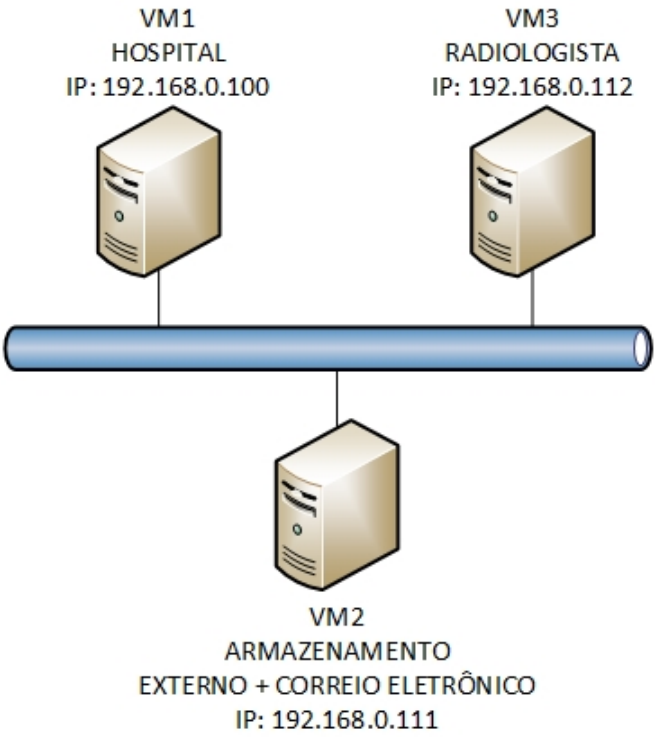



Figura 22: Cenário implementado para os testes.
Fonte: Próprio autor

Todas as máquias virtuais compartilham o mesmo barramento de comunicação. Nenhuma configuração de prioridade de processamento ou alocação de recursos da máquina hospedeira foi implementado. Os recursos, como quantidade de memória, volume do disco ou número de processadores foram distribuídos de forma estática. Para a criação e gerenciamento dos certificados digitais utilizados nos experimentos, foi utilizado o *keytool* presente no Java SE Development Kit (JDK) 1.8.0_171, versão utilizada para codificar a solução. Foram criadas duas *keystore*: (1) CD_CERT_DB para o armazenamento dos Certificados Digitais de Identidade (CD) e (2) CA_CERT_DB, para armazenar os Certificados Digitais de Atributos. Optou-se por segmentar as *keystore* para que ao final dos experimentos pudéssemos medir o volume de dados criado pelos certificados utilizados. Os comandos utilizados para a criação desses contêineres de armazenamento de chaves foram:

Para criação da *keysotre* dos Certificados Digitais de Identidade:

**# keytool -keystore CD_CERT_DB -genkey -alias CD_CERT_DB**

Para criação da *keysotre* dos Certificados Digitais de Atributos:
**# keytool -keystore CA_CERT_DB -genkey -alias CA_CERT_DB**

Ambas estão armazenadas na máquina virtual que representa o HOSPITAL. Os exames de imagens utilizados durante os experimentos estão armazenados no ARMAZENAMENTO EXTERNO. Na próxima seção, são detalhados os experimentos realizados durante o processo de validação do DFA.

## 4.2 Detalhamento dos experimentos

Os Certificados Digital de Atributos (CA) foram gerados de forma automática pelo proprietário do exame de imagem, em nosso cenário, HOSPITAL. A validade de todo CA solicitado será sempre 7 (sete) dias a partir da data de solicitação para criação. Por exemplo: se o HOSPITAL for criar um CA para o RADIOLOGISTA na data 05/05/2018, a validade do CA criado será dia 12/05/2018 e seu uso estará disponível a partir da data de emissão. Decidimos por isso para tornar mais ágil a emissão do certificado, porém, nada impede que a geração desses certificados seja manual, com o auxílio de um aplicativo para gestão de certificados digitais, ou até mesmo terceirizada. Discutiremos mais a respeito dessas possibilidades nas Considerações Finais deste capítulo.

Em ambiente de produção, nossa solução pressupõe que os Certificados Digital de Identidade (CD) já tenham sido emitidos por uma entidade vinculada a ICP-Brasil, se implementado no Brasil. Caso implementada em outros países, os certificados utilizados devem ser válidos na infraestrutura da entidade responsável pela gestão de certificados digitais daquela região. Entretanto, em nossos testes, utilizamos um CD auto-assinado para identificação das entidades e emissão dos CA. Isto é, um certificado gerado por nossa equipe, mas, sem validade jurídica alguma. Por não sermos uma Autoridade Certificadora vinculada a ICP-Brasil, este certificado, judicialmente falando, não tem valor algum. Nenhum documento assinado por ele teria valor legal em um eventual processo jurídico ou de validação. Contudo, ele possui todas as funcionalidades técnicas de um certificado emitido de acordo com as normas

legais, inclusive, assinar documentos. E esta função é a que utilizaremos juntamente com a de identificação do solicitante do exame de imagem. Já o Certificado Digital de Atributos (CA) não tem a finalidade de assinar documentos ou identificar uma entidade e sim qualificar seu portador. Não existe restrição para sua criação por uma entidade que não seja vinculada a ICP-Brasil. Qualquer entidade que pretenda utilizá-lo em suas aplicações poderá criar a estrutura de atributos desejada, assim como demonstramos da Seção 3.1.2 do Capítulo 3. Entretanto, como já dito anteriormente, para possuir validade legal o CA deve ser assinado digitalmente por um CD válido na cadeia de certificados da ICP-Brasil.

### 4.2.1 Ações simuladas

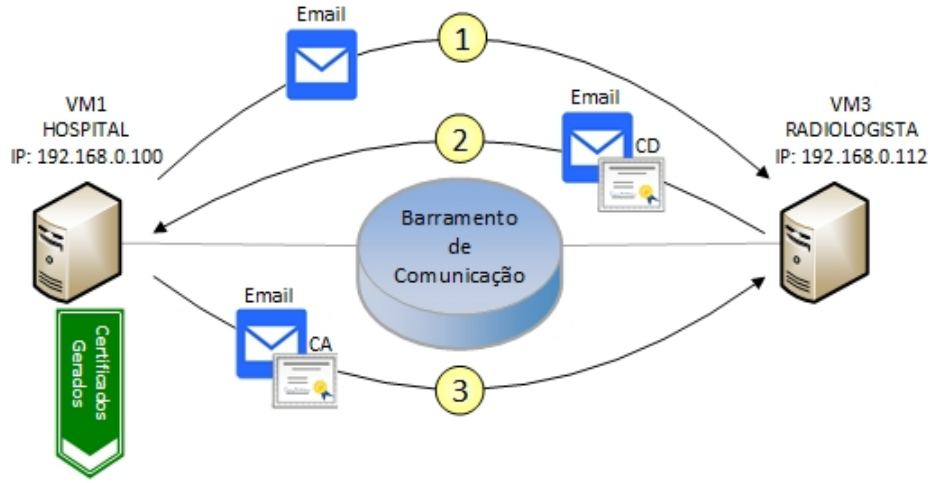
Nesta seção, são apresentadas as ações que são comuns em uma rede de colaboração que idealizamos para a prática da telerradiologia. Estas ações foram simuladas para validar as funcionalidades propostas pelo DFA e em cada ação poderá existir mais de um tipo de atividade. Por exemplo: a validação do CA expedido poderá ser feita consultando a lista de certificados revogados pela entidade emissora ou fazendo a simples verificação da validade do certificado. Caso o experimento tenha mais de uma atividade, esta será devidamente explicitada. Toda exibição do Certificado Digital de Atributos será feita utilizando a linguagem XML, similar a Figura 20 no Capítulo 3. Optamos por essa forma de exibição por entendermos que fica mais fácil a interpretação dos atributos e seus valores.

É importe frisar que a implementação que fizemos do DICOMFlowAccess (DFA) para ser o controle de acesso na infraestrutura criada pelo DICOMflow para compartilhamento de exames de imagens médicas segue os critérios de uma *white list* na verificação de acesso das solicitações para obtenção, isto é, apenas o que está explicitamente informado nos atributos do Certificado de Atributos será autorizado pelo DFA. Nas subseções seguintes serão feitos o detalhamento e a discussão dos experimentos realizados.

#### 4.2.1.1 EXPERIMENTO 1: Criação automática do Certificado Digital de Atributos por HOSPITAL

**Entidades envolvidas:** HOSPITAL e RADIOLOGISTA.

Esse experimento teve a finalidade de verificar a capacidade do DFA gerar um Certificado de Atributos vinculado ao Certificado Digital do médico radiologista que recebeu a solicitação de emissão de laudo. O teste não foi realizado apenas com um radiologista. Foram criados cinco emails (rad_a@dfa.com ... rad_e@dfa.com), cada um simbolizando um possível radiologista atuante na rede de colaboração criada. Desta forma, verificou-se a capacidade do DFA trabalhar com mais de uma requisição de criação de Certificado de Atributos simultaneamente. Todos os certificados foram criados e armazenados na *keystore* CA_CERT_DB conforme podemos visualizar na Figura 23.




```
C:\keystore>keytool -keystore CA_CERT_DB -list
Informe a senha da área de armazenamento de chaves:
Tipo de área de armazenamento de chaves: JKS
Fornecedor da área de armazenamento de chaves: SUN

Sua área de armazenamento de chaves contém 5 entradas

rad_a, 02/06/2018, trustedCertEntry,
Fingerprint (SHA1) do certificado: 41:64:2D:2A:60:EB:89:5C:FF:1A:39:8E:FA:77:1D:40:28:49:FE:0D
rad_b, 02/06/2018, trustedCertEntry,
Fingerprint (SHA1) do certificado: 9A:81:D2:63:00:0E:24:CC:48:C9:5D:B9:C0:0D:9F:89:FB:65:FF:56
rad_c, 02/06/2018, trustedCertEntry,
Fingerprint (SHA1) do certificado: BC:3D:A3:05:C9:EB:37:66:94:CA:13:0E:81:C9:A1:92:0C:90:E7:2D
rad_d, 02/06/2018, trustedCertEntry,
Fingerprint (SHA1) do certificado: 8E:7F:B5:45:FD:A3:1C:70:82:53:A7:0B:53:90:80:BA:55:9E:7B:91
rad_e, 02/06/2018, trustedCertEntry,
Fingerprint (SHA1) do certificado: E5:C9:2B:0F:13:3E:75:EB:2E:44:F7:F2:6B:6D:FD:0F:DF:E4:6E:57
```

Figura 23: Certificados criados no Experimento 1.
Fonte: Próprio autor

No *Passo1* o HOSPITAL faz a solicitação para que o RADIOLOGISTA emita um laudo de um exame de imagem. No *Passo2* o RADIOLOGISTA envia a confirmação de recebimento da solicitação e anexa o seu Certificado Digital de Identidade (CD). De posse deste certificado, no *Passo3*, o HOSPITAL gera o Certificado Digital de Atributos (CA) necessário para obtenção do exame de imagem e o encaminha para o RADIOLOGISTA. Na parte inferior da figura podemos ver os certificados existentes que estão armazenados na *keystore* CA_CERT_DB.

Duas características devem ser levadas em consideração neste momento. (1) Todas as entidades (HOSPITAL e RADIOLOGISTA) devem possuir um módulo do DICOMFlow funcionando e devidamente configurado e (2) o DICOMFlowAccess tem a finalidade de criar, exclusivamente, os Certificados Digitais de Atributos. Os Certificados Digitais de Identidade já estão criados e de posse dos médicos radiologistas. A VM3 que representa o ARMAZENAMENTO EXTERNO e também executa o serviço de Correio Eletrônico foi abstraída neste cenário por não ter grande relevância no fluxo das informações, apenas atuou como Servidor de Email. Com este experimento conseguimos atestar que o DFA é capaz de gerar e distribuir vários CA's simultaneamente de várias entidades diferentes.

#### 4.2.1.2 EXPERIMENTO 2: Resgate do exame de imagem indicado por HOSPITAL

**Entidades envolvidas:** RADIOLOGISTA e ARMAZENAMENTO EXTERNO.

Esse experimento teve a finalidade de atestar a capacidade do DFA de fazer o tratamento dos atributos existentes nos CAs utilizados. Vale lembrar que o DFA atua com o critério de lista branca para o controle de acesso, isto é, **apenas** o que está explícito no Certificado de Atributos será autorizado. Fizemos simulações com a finalidade de verificar a capacidade de permissão e restrição do DFA. Para facilitar o entendimento, serão expostos os certificados de atributos no formato XML. A Figura 24 mostra um CA que permite ao radiologista obter um exame de imagem entre o dia 08/06/2018 a partir das 13h:30m:00s (*startDate*) até o dia 12/06/2018 até às 20h:00m:00s (*endDate*). Também pode ser obtido qualquer tipo de exame (*modalityType*) de imagem e a requisição pode ser feita qualquer dia da semana (*dayWeek*). A URL que indica o endereço eletrônico para obtenção do exame permanece no corpo de

mensagem como pode ser revisto na Figura 18 apresentada da Seção 3.1.1 do Capítulo 3.

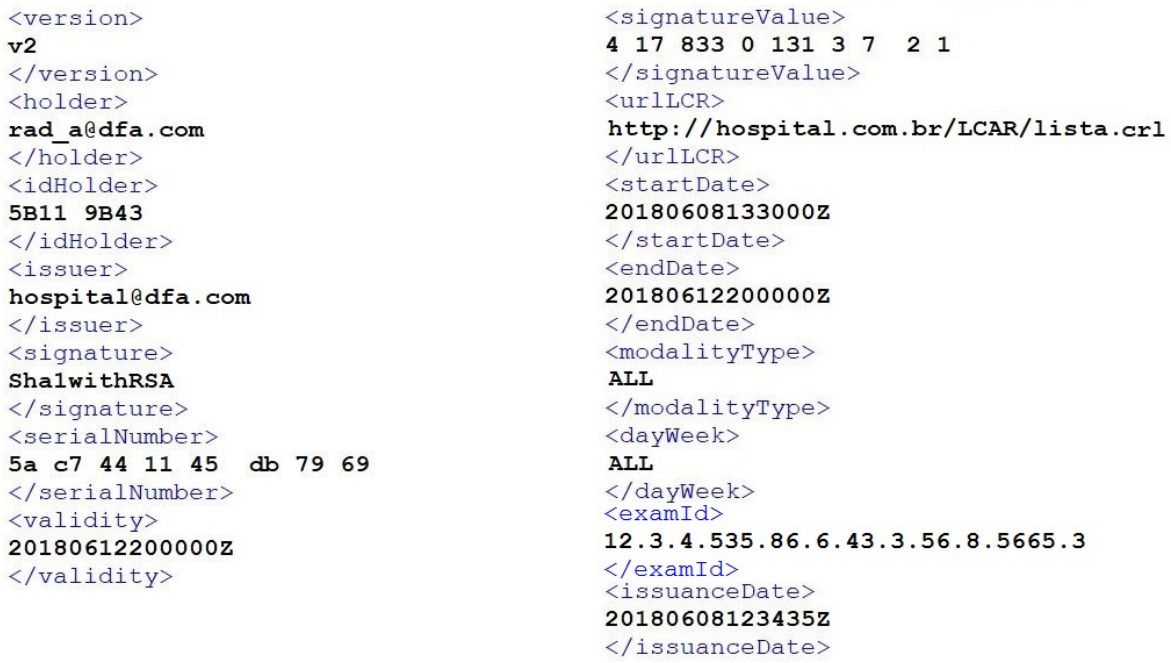



Figura 24: Atributos do CA utilizados no Experimento 2.
Fonte: Próprio autor

Todas as requisições de *download* de exame de imagens feitas com este certificado de atributos foram **autorizadas** pelo DFA. Para testarmos a flexibilidade de nossa solução, geramos um CA em que o atributo (*dayWeek*) foi alterado para "DOM" (abreviação de domingo), como pode ser visto na Figura 25. As requisições passaram a ser **bloqueadas** pelo DFA quando feitas em outros dias da semana. Simulamos também um teste para validar a política de que "nenhum exame deve ser obtido fora do intervalo de datas" existente nos atributos (*startDate*) e (*endDate*). Foi criado um CA em que a requisição para obter o exame foi feita pelo "rad_a" fora de intervalo datas informadas e, como esperado, a requisição também foi rejeitada pelo DFA.

Outro experimento realizado foi utilizado para atestar a funcionalidade do PAP. Módulo que é responsável pelas políticas dinâmicas de controle de acesso (discutidas nas Seções 3.2.4 e 3.2.5 da Capítulo 3). Inserimos, ainda que estaticamente, uma política de restrição para que Certificados de Atributos assinados pelo HOSPITAL, não pudessem obter um exame de imagem. Conforme esperado, mesmo que todos os atributos permitissem o envio do exame de imagem, a solicitação feita através de um CA assinado pelo HOSPITAL foi

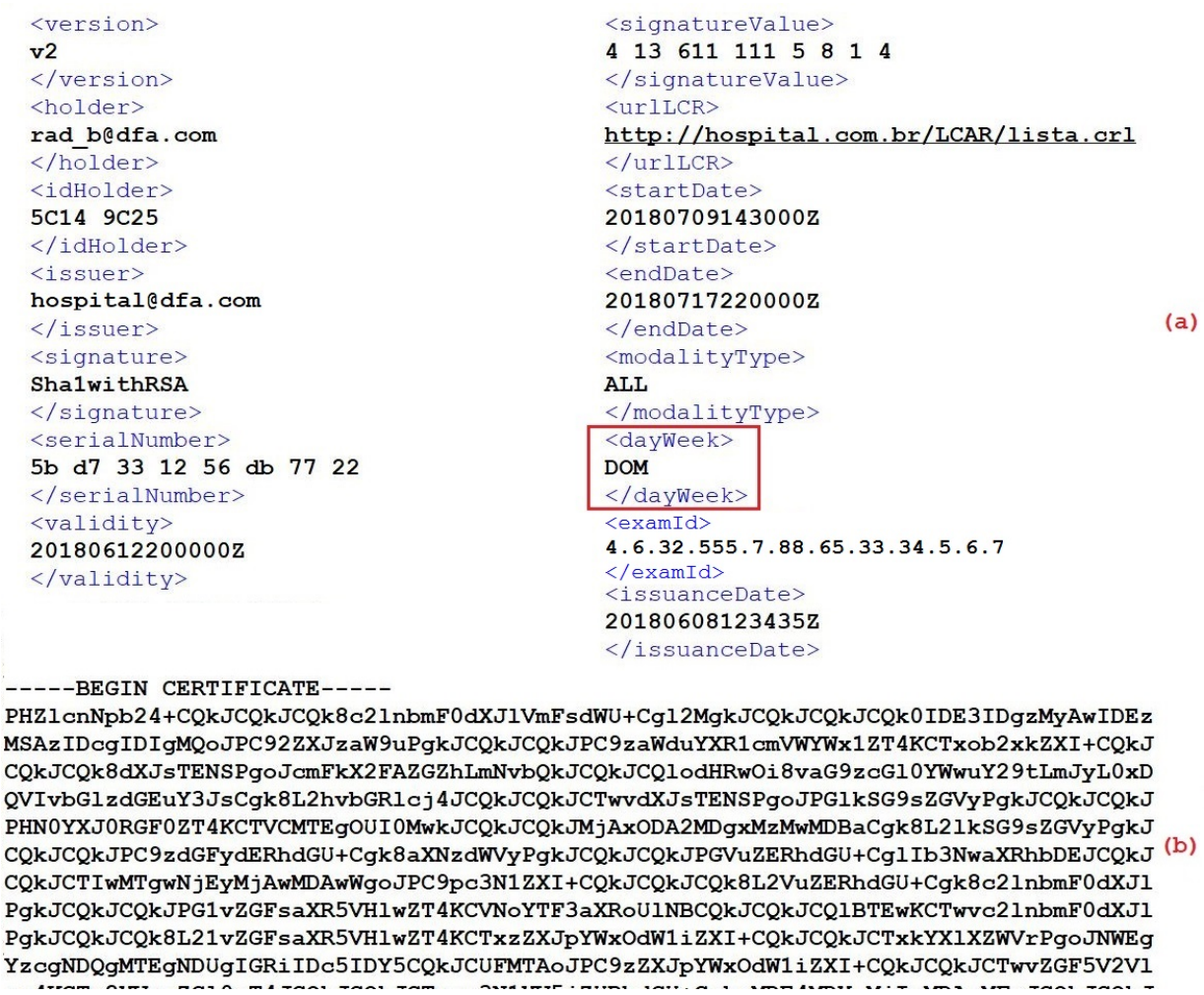



Figura 25: (a) Conteúdo do CA apresentado em XML. (b) Conteúdo do CA apresentado em Base64.

Fonte: Próprio autor

rejeitada pelo DFA e consequentemente, o exame de imagem não foi enviado. Para simularmos tal política, um arquivo texto foi criado localmente na máquina virtual que representa o ARMAZENAMENTO EXTERNO (VM2). Quando seu valor era *true*, o envio da imagem era negado. E quando era *false*, o envio era permitido. A implementação desta forma foi apenas para validar o funcionamento. Estudos mais específicos são necessários para avaliar a melhor maneira de implementar a manipulação de políticas dinâmicas no DFA.

Gerou-se também um certificado de atributos que permite apenas a obtenção de imagens de modalidades específicas. Como pode-se observar em destaque na Figura 26, o certificado gerado permite a obtenção de exames das modalidades Tomografia Computadorizada (do

inglês, Computed Tomography (CT)) e Ressonância Magnética (do inglês, Magnetic Resonance (MR)). E conforme esperado, solicitações visando a obtenção de exames de imagens gerados por outros modalidades foram **bloqueadas**.


Figura 26: CA gerado para validar o filtro de modalidades no controle de acesso.
Fonte: Próprio autor

Com estes experimentos, podemos observar a grande possibilidade de políticas de controle de acesso aplicáveis com nossa solução. Outro fator que expõe o potencial do DFA é que os atributos são expansíveis permitindo que outros critérios de acesso possam ser implementados para atender a necessidade de uma ou várias entidades.

#### 4.2.1.3 EXPERIMENTO 3: Verificação da Validade do Certificado de Atributos

**Entidades envolvidas:** ARMAZENAMENTO EXTERNO e HOSPITAL.

Este experimento buscou atestar a validação de um Certificado de Atributos pelo PEP (primeiro módulo da arquitetura do DFA). As três formas descritas na Subseção 3.2.1 do Capítulo 3 foram testadas. Apesar de ser perfeitamente possível aplicar simultaneamente as

três formas de validação, optamos por utilizar cada mecanismo de forma isolada em nossos testes com a finalidade de tornar mais fácil a simulação de várias situações em que o DFA deverá permitir ou bloquear o acesso ao exame de imagem.

A primeira, que é a verificação da data de validade do CA apresentado (atributo *validity*), podemos constatar que **nenhuma** requisição realizada fora do intervalo de datas deste atributo foi aceita pelo DFA. Este atributo específico tem como função informar que o certificado será considerado inválido se for usado antes (*notBefore*) da data especificada ou depois (*notAfter*.) O DFA mostrou-se funcional em realizar este tipo de validação, pois, só tiveram o acesso permitido as requisições que foram realizadas dentro deste intervalo de datas.

A segunda forma de validação testada foi checar a associação entre o CA emitido por HOSPITAL e o CD apresentado pelo RADIOLOGISTA. O atributo *idHolder* que consta no CA emitido/apresentado tem que conter o mesmo valor do atributo *serialNumber* do CD enviado pelo RADIOLOGISTA. Foram feitas tentativas de apresentar outro CD (com o *serialNumber* diferente do informado no atributo *idHolder* do CA) e todas as tentativas para obter o exame de imagem foram **bloqueadas** quando os dados não coincidiam e consequentemente o envio do exame de imagem não foi realizado.

A terceira e última forma de validação verificada, foi se do DFA tem a capacidade de consultar a Lista de Certificados Revogados (LCR) da Entidade Emissora de Atributos (EEA). É importante reforçar que é dever de toda EEA manter e disponibilizar uma lista para consulta externa pelos seus parceiros dos Certificados de Atributos que, por algum motivo, foram revogados por ela. Todo CA emitido pelo DFA possui um atributo *urlLCR* que contém a URL para acessar a base de dados com o *serialNumber* dos CAs que foram revogados. Inserimos alguns desses seriais e na medida que as consultas foram sendo realizadas, de acordo com a resposta emitida pela EEA, o DFA foi bloqueando o acesso ao exame de imagem. Para gerenciar e criar a requisição de consulta a LCR, foi utilizado o *plugin* publicado pela comunidade Bouncy Castle para consultas utilizando o Online Certificate Status Protocol (OCSP).

#### 4.2.1.4 EXPERIMENTO 4: Solicitação de segunda opinião

**Entidades envolvidas:** ARMAZENAMENTO EXTERNO, HOSPITAL, RADIOLOGISTA.

Das modificações no controle de acesso do DICOMFlow, a possibilidade de emissão de uma segunda opinião em um laudo médico foi a única que exigiu a adição de um novo tipo de serviço aos que foram propostos inicialmente em (ARAUJO, 2017). O *SecondOpinion*, implementado pelo DFA, junta-se aos demais tipos de serviços propostos para suprir uma limitação do DICOMFlow, que é a emissão de laudo contendo uma segunda opinião do laudo previamente emitido. Na Figura 18, que foi apresentada no Capítulo 3 Subseção 3.1.1, pode-se ver destacado na cor azul o serviço (*Storage*) solicitado na mensagem.

Com a implementação do DFA e agora com a possibilidade de emissão de segunda opinião, quando esta for solicitada, o serviço *SecondOpinion* é informado juntamente com o email do radiologista indicado. Na mensagem original foi criada uma nova *tag* contendo o email do emissor da segunda opinião. De forma resumida a mensagem que indicaria este tipo de serviço é **<service version="1.0" name="SecondOpinion" action="Put" type="1"/>** e no corpo da mensagem é informado o email do radiologista que irá emitir a segunda opinião na *tag* **<somail> rad_b@dfa.com </somail>**. Esta mensagem é enviada para o HOSPITAL. Estas são as modificações implementadas na mensagem do DICOMFlow. Que só serão utilizadas durante o processo de solicitação de uma segunda opinião de laudo médico.

O fluxo de trabalho simulado neste experimento foi executado da seguinte forma: (1) O HOSPITAL solicita a emissão de laudo para o radiologista (neste experimento usamos sempre o email rad_a@dfa.com como destino da primeira solicitação de emissão de laudo), que por sua vez (2) faz o envio de seu Certificado Digital de Identidade (CD) para o HOSPITAL gerar o Certificado Digital de Atributos (CA) que permitirá o acesso ao exame de imagem. (3) O exame de imagem é obtido pelo rad_a@dfa.com junto ao ARMAZENAMENTO EXTERNO, que emite o laudo primário e indica ao HOSPITAL outro radiologista de sua *network* (rad_b@dfa.com) para emissão de uma segunda opinião do laudo. É importante frisar que neste momento são enviadas **duas mensagens**. Uma contendo o laudo primário e outra a solicitação de segunda opinião. O HOSPITAL irá associar a solicitação de segunda

opinião a URL contendo o exame de imagem do paciente. Referenciando novamente a Figura 18 apresentada no Capítulo 3 Subseção 3.1.1, é a parte da mensagem destacada em verde. Essa URL é um identificador único deste exame no domínio do HOSPITAL. Quem garante a singularidade deste exame neste domínio é o próprio protocolo DICOM, que foi apresentado no Capítulo 1 Subseção 1.1.

Neste momento avaliamos dois cenários possíveis. O primeiro foi que o HOSPITAL iniciou todo o processo de solicitação de laudo para o "rad_b" desde o primeiro passo como se fosse uma primeira solicitação de laudo (Subseção 3.3.1 do Capítulo 3). E o segundo foi a utilização de um CA "coringa" (Subseção 3.3.2 do Capítulo 3) para que o radiologista (neste segundo cenário utilizamos o "rad_c") possa fazer o *download* do exame de imagem sem a necessidade da troca inicial dos certificados digitais. Neste segundo cenário, assim como todos os outros, as entidades envolvidas possuíam uma instância do DICOMFlow configurada e funcional. Em ambos os cenários o DFA mostrou-se capaz de manter o fluxo de trabalho totalmente funcional. Na próxima seção discutimos os resultados desses experimentos.

## 4.3 Considerações Finais

Com os experimentos realizados, foi possível identificar a necessidade de algumas mudanças nos critérios sóciotécnicos inicialmente concebidos, como por exemplo, a necessidade do desmembramento da solicitação de segunda opinião em duas mensagens. Uma contendo o laudo inicial e a outra com a solicitação propriamente dita. Inicialmente foi pensando em um tipo de serviço com contemplasse o envio do primeiro laudo e a solicitação de segunda opinião em uma só mensagem, com isso mudanças mais incisivas seriam necessárias na proposta original do DICOMFlow, situação que queríamos evitar deste o início da concepção de nossa solução. Contendo os dois serviços foi gerada uma mensagem mais complexa, com mais dados para serem transportados e verificados. Optamos por desmembrar, fato que tornou o processo mais simples de ser implementado e depurado. Exceto por esta situação, pudemos observar que a inserção do DFA no DICOMFlow foi feita de forma transparente e eficiente.

Os experimentos executados neste capítulo estavam alinhados com os objetivos descritos no Capítulo 1 deste trabalho. Após a realização destes experimentos, constatamos que todos os objetivos foram alcançados. O Objetivo 1 expõe a necessidade de manter-se o domínio sobre o acesso as imagens médicas pelo seu proprietário, mesmo já compartilhada. E como descrito na terceira validação do Experimento 3, conseguimos alcançar esse objetivo. O Objetivo 2, que remete a liberdade de acesso pelo requisitante do exame de imagem, independente da disponibilidade do proprietário da imagem foi atendido também com o Experimento2 como relatado na primeira e segunda forma de validação. O Objetivo 3, que trata da escalabilidade do modelo, foi atingido com o Experimento 1, quando foram feitas diversas requisições de acesso entre o HOSPITAL e cinco radiologistas distintos e todos os certificados de atributos foram gerados e o fluxo de trabalho pode seguir sem alterações.

O Objetivo 4, que remete a independência de uma base de dados centralizada com informações de usuários, foi contemplado no momento em que o RADIOLOGISTA faz o resgate do exame de imagem no ARMAZENAMENTO EXTERNO sem que este tenha um conhecimento prévio de sua existência, não necessitou de registro algum do RADIOLOGISTA. A checagem dos certificados foi suficiente para executar o processo de autenticação e autorização. Já o Objetivo 5, que remete a integração do DFA com o infraestrutura proposta pelo DICOMFlow, foi contemplado quando o processo desde sua origem na solicitação de emissão de laudo pelo HOSPITAL até a emissão de laudo emitido pelo RADIOLOGISTA após obter o exame de imagem de forma segura e padronizada no ARMAZENAMENTO EXTERNO foi completado com sucesso e sem anomalias identificadas.

O DFA também mostrou-se eficiente em sanar uma das limitações do DICOMFlow, a capacidade de suportar a emissão de uma segunda opinião de um laudo. Com o Experimento 4 podemos constatar que a utilização dos certificados digitais de identidade e atributos foi capaz de atender ao fluxo de trabalho criado com a atividade de solicitação e emissão de uma segunda opinião de um laudo médico. Atividade esta fortemente utilizada na prática da telerradiologia.

# CAPÍTULO 5

# CONCLUSÃO

Este trabalho apresentou o DICOMFlowAccess, um modelo de controle de acesso que se propõe em atuar como parte da infraestrutura de numa rede colaborativa aberta e distribuída que utiliza a Internet como meio de interconexão para compartilhamento de conteúdo, em particular, exames de imagens médicas para a prática da telerradiologia. No início deste trabalho (Capítulo 1), mostrou-se os benefícios e desafios para a criação de uma infraestrutura para prática da telerradiologia em escala global e que as principais tecnologias (PACS/DICOM) dos departamentos de radiologia estão modeladas para atuarem em um contexto de rede local, consequentemente, criando desafios para formação de uma rede telerradiológica colaborativa em escala global. Um desses desafios é a atuação do controle de acesso às informações compartilhadas. O conjunto de tecnologias e os estudos existentes nesta linha de pesquisa (Capítulo 2), proveram a sustentação sóciotécnica para a concepção do DICOMFlowAccess (Capítulo 3).

Os experimentos (Capítulo 4) realizados, mostraram que com a substituição do modelo de controle de acesso proposto originalmente no DICOMFlow (ARAUJO, 2017) pelo DICOMFlowAccess, foi possível aprimorar o dinamismo das associações da rede de colaboração proposta e novas funcionalidades foram incrementadas a infraestrutura. Como a emis-

são de segunda opinião de laudo médico e a terceirização do armazenamento dos exames de imagens. A utilização de certificados digitais (de identidade e de atributos), além de proporcionar maior flexibilidade nos atributos de controle e alinhamento com as atuais tecnologias de gestão de identidade na Internet, possibilitaram a independência de conexões ativas, a descentralização do processo de autenticação e autorização e favoreceram a possibilidade de crescimento das associações de forma mais ágil e segura. Os experimentos também atestaram que os objetivos traçados inicialmente neste trabalho foram alcançados pelo modelo de controle de acesso apresentado.

Ao confrontarmos as características existentes no DFA com as tecnologias atuais para prover controle de acesso à conteúdo compartilhado entre entidades, o DFA destaca-se pela independência de uma base de dados centralizada contendo informações de usuário e por não ser necessário o estabelecimento de sessão para fins de autenticação. Tais características são possíveis pela utilização dos certificados digitais, de identidade e atributos. Ao tornar dispensável o conhecimento prévio de usuários numa base de dados centralizada, o DFA independe de uma entidade administrativa central para prover o controle de acesso aos recursos compartilhados na rede colaborativa, possibilitando maior liberdade e dinamismo nas associações entre entidades. E por não possuir a necessidade do estabelecimento de sessão para fins de autenticação, o DFA proporciona assincronismo nas solicitações de acesso. Tornando mais simples o acesso aos recursos compartilhados, em nosso cenário, exames de imagens médicas. Criando uma conexão *ad-hoc* entre as entidades solicitante e armazenadora do recurso. E também, minimiza o impacto de uma eventual indisponibilidade do entidade originadora do exame de imagem, pois, as informações necessárias para a autenticação e autorização, são transportadas no Certificado de Atributos emitidos por esta entidade.

O conceito de organizações virtuais se assemelha a rede colaborativa proposta neste trabalho. Contudo, uma organização virtual remete à entidades que associam-se para a realização de uma atividade qualquer com a necessidade de uma análise de requisitos para entrada de um novo membro e após aprovação, este membro estará sujeito às políticas de acesso pré-estabelecidas que, comumente, estão sob a gestão de uma única entidade. Características que confrontem a necessidade abertura, distribuição e dinamismo da rede colaborativa

para prática da telerradiologia como propomos. O DFA é uma solução que prevê a formação de federações de entidades, em particular, para a prática da telerradiologia. Porém, está posicionado como uma camada de suporte para a formação destas. Sendo uma questão social e não técnica, tornar o processo de associação mais criterioso e com políticas de uso pré-estabelecidas, consequentemente, menos dinâmico.

## Limitações

Apesar dos experimentos comprovarem que o DFA é tecnicamente exequível, a solução apresenta algumas limitações que carecem de discussão. Uma das limitações não está diretamente vinculada a questões técnicas e sim legais. A prática da telerradiologia no Brasil é regulamentada pelo Conselho Federal de Medicina (CFM) e em sua RESOLUÇÃO CFM nº 2.107/2014 (CFM-2.107/14, 2014) define e normatiza a Telerradiologia no Brasil. O Art.3 determina que "*a transmissão dos exames por telerradiologia deverá ser acompanhada dos dados clínicos necessários do paciente, colhidos pelo médico solicitante, para a elaboração do relatório*". Isoladamente, nossa solução ainda não prevê a transmissão de dados clínicos. Sendo necessário estudos para viabilizarem a sua integração ao sistema que mantém os dados clínicos do paciente.

Outras limitações, agora relacionadas a questões técnicas, é que os experimentos foram executados em ambiente virtual que simulou a rede de colaboração para a telerradiologia num contexto global e foram utilizados certificados digitais de identidade auto-assinados. O ideal é atestar as funcionalidades do DICOMFlowAccess num ambiente de produção real e utilizando certificados válidos na cadeia da ICP-Brasil. Tecnicamente, não há mudanças entre o ambiente virtual e o real. Visto que os protocolos (HTTPS e e-mail) e tecnologias (Certificados Digitais) utilizados durante o experimento já são estabelecidos no contexto de virtualização de sistemas operacionais. Tornando possível simular suas funcionalidades neste ambientes. Entretanto, é relevante que os testes sejam submetidos ao *workflow* telerradiológico de um ambiente de produção para atestar a adaptação do DFA a este ambiente. A expansão dos atributos existentes no Certificado Digital de Atributos também é interessante que seja realizada, a fim de atestar a flexibilidade da solução.

## Trabalhos Futuros

Apesar dos objetivos traçados para a concepção do DICOMFlowAccess terem sido atingidos, algumas possibilidades de novas implementações foram identificadas e demandam maiores investigações para serem implementados.

Como já discutido, o processo de controle de acesso é dividido em duas partes, autenticação e autorização. Em nossa proposta, o processo de autenticação ainda é feito pelo mecanismo original proposto pelo DICOMFlow, ficando a cargo do DFA, o processo de autorização. Existindo assim a possibilidade de incorporar os atributos utilizados para prover a autenticação ao DICOMFlowAccess. A vantagem desta modificação é a concentração de todo controle de acesso em um único mecanismo, o DFA.

Além desta concatenação de processos do controle de acesso, existe a necessidade de implementação das políticas dinâmicas de controle de acesso. Visto que, a Política Geral de Controle de Acesso (PGCA) é implementada em *hard code*, tornando o processo de atualização destas políticas um tanto complexo. Implementar a política dinâmica irá tornar mais fácil a adaptação do DFA à situação pontuais que possam a surgir durante as associações formadas.

Por fim, o DICOMFlowAccess mostrou-se uma contribuição relevante para os estudos em informática em saúde que visam interconectar infraestruturas heterogêneas com a finalidade de realizar a prática da telerradiologia. Agregamos valor no controle de acesso inicialmente proposto pelo DICOMFlow, habilitando-o a ser uma infraestrutura sólida para tornar-se base de uma rede de colaboração global para a prática da telerradiologia, incrementando maior flexibilidade em suas políticas de segurança e alinhamento com as principais e atuais tecnologias de gestão de identidade e controle de acesso na Internet.

## Publicações

Até então, dois trabalhos foram publicados no âmbito desta pesquisa de mestrado. O primeiro, com foco específico nos benefícios de uma rede de colaboração global para a prática

da telerradiologia, foi apresentado no XVI Congresso Brasileiro de Informática em Saúde. E o segundo, com foco nos desafios da gestão de identidade e controle de acesso em um ambiente computacional distribuído, foi apresentado no XVIII Simpósio Brasileiro em Segurança da Informação de Sistemas Computacionais (SBSeg).

**Silva, D A B**; Motta, G H M B; Neto, J R L e Araújo, D A B. *DICOMFlowAccess: modelo de controle de acesso aberto, assíncrono e descentralizado para o compartilhamento de imagens médicas*. XVI Congresso Brasileiro de Informática em Saúde – CBIS 2018. Fortaleza - CE.

**Silva, D A B**; Motta, G H M B. *DICOMFlowAccess: um modelo de controle de acesso baseado em certificados digitais para prática da telerradiologia*. XVIII Simpósio Brasileiro em Segurança da Informação de Sistemas Computacionais (SBSeg). VIII Workshop de Gestão de Identidades Digitais (WGID). SBSEG 2018. Natal - RN.

# Referências Bibliográficas


ADAMS, C.; LLOYD, S. *Understanding PKI: concepts, standards, and deployment considerations*. [S.l.]: Addison-Wesley Professional, 2003.

ALSHEHRI, S.; RAJ, R. K. Secure access control for health information sharing systems. In: IEEE. *2013 IEEE International Conference on Healthcare Informatics (ICHI)*. [S.l.], 2013. p. 277–286.

ALZAHRANI, A.; JANICKE, H.; ABUBAKER, S. Decentralized xacml overlay network. In: IEEE. *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*. [S.l.], 2010. p. 1032–1037.

AMARAL, F. *Introdução à Ciencia de Dados: mineração de dados e big data*. [S.l.]: Alta Books Editora, 2016.

AMAZON. *Authenticating Requests Using the REST API*. 2017. Disponível em: <http://docs.aws.amazon.com/AmazonS3/latest/dev/S3_Authentication2.html>. Acesso em: 08/12/2018.

ARAUJO, D. A. B. de. Dicomflow: Gateway assíncrono e descentralizado para formação de uma infraestrutura de informação para distribuição de imagens médicas. 2017. Dissertação de Mestrado.

BENANTAR, M. *Access control systems: security, identity management and trust models*. [S.l.]: Springer Science & Business Media, 2006.

BENJAMIN, M.; ARADI, Y.; SHREIBER, R. From shared data to sharing workflow: Merging pacs and teleradiology. *European Journal of Radiology*, Elsevier, v. 73, n. 1, p. 3–9, 2010.

BOWKER, G. C.; BAKER, K.; MILLERAND, F.; RIBES, D. Toward information infrastructure studies: Ways of knowing in a networked environment. In: *International handbook of internet research*. [S.l.]: Springer, 2009. p. 97–117.

BUTLER, R.; WELCH, V.; ENGERT, D.; FOSTER, I.; TUECKE, S.; VOLMER, J.; KESSELMAN, C. A national-scale authentication infrastructure. *Computer*, IEEE, v. 33, n. 12, p. 60–66, 2000.

CFM-1.821/07. *Conselho Federal de Medicina. RESOLUÇÃO CFM Nº 1.821/2007*. 2007. Disponível em: <http://www.portalmedico.org.br/resolucoes/cfm/2007/1821-2007.pdf>. Acesso em: 11/12/2017.

CFM-1.983/12. *Conselho Federal de Medicina. RESOLUÇÃO CFM nº 1.983/2012*. 2012. Disponível em: <http://www.portalmedico.org.br/resolucoes/cfm/2012/1983-2012.pdf>. Acesso em: 18/12/2017.

CFM-2.107/14. *Conselho Federal de Medicina. RESOLUÇÃO CFM Nº 1.821/2007*. 2014. Disponível em: <http://www.portalmedico.org.br/resolucoes/CFM/2014/2107-2014.pdf>. Acesso em: 08/04/2018.

CHILD, J. *Organization: contemporary principles and practice*. [S.l.]: John Wiley & Sons, 2015.

DICOM. *Digital Imaging and Communications in Medicine*. 2017. Disponível em: <http://www.dicomstandard.org/about/>. Acesso em: 9/9/2017.

DRNASIN, I.; VUCICA, D.; TONKOVIC, S. Success of teleradiology as a confirmation of radiological excellence. In: IEEE. *Information Technology Interfaces, 2009. ITI'09. Proceedings of the ITI 2009 31st International Conference on*. [S.l.], 2009. p. 73–78.

DU, J.; EL-GAFY, M. Virtual organizational imitation for construction enterprises: Agent-based simulation framework for exploring human and organizational implications in construction management. *Journal of Computing in Civil Engineering*, American Society of Civil Engineers, v. 26, n. 3, p. 282–297, 2012.

EDWARDS, P. N.; JACKSON, S. J.; BOWKER, G. C.; KNOBEL, C. P. Understanding infrastructure: Dynamics, tensions, and design. 2007.

FERRAIOLO, D. F.; SANDHU, R.; GAVRILA, S.; KUHN, D. R.; CHANDRAMOULI, R. Proposed nist standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, ACM, v. 4, n. 3, p. 224–274, 2001.

FRANCO, E.; MUCHALUAT-SAADE, D.; CASTRO, N. C. Across: A generic framework for attribute-based access control with distributed policies for virtual organizations. *Future Generation Computer Systems*, Elsevier, v. 78, p. 1–17, 2018.

HANSETH, O.; LYYTINEN, K. Design theory for dynamic complexity in information infrastructures: the case of building internet. *Journal of Information Technology*, Springer, v. 25, n. 1, p. 1–19, 2010.

HU, V. C.; FERRAIOLO, D.; KUHN, R.; FRIEDMAN, A. R.; LANG, A. J.; COGDELL, M. M.; SCHNITZER, A.; SANDLIN, K.; MILLER, R.; SCARFONE, K. Guide to attribute based access control (abac) definition and considerations (draft). *NIST Special Publication*, v. 800, n. 162, 2013.

HUANG, H. *PACS and imaging informatics: basic principles and applications*. [S.l.]: John Wiley & Sons, 2011.

ICP-BRASIL. Doc-icp-16. visão geral sobre certificado de atributo para a icp-brasil. doc-icp-16. versão 1.0. 2012.

ICP-BRASIL. Doc-icp-16. perfil de uso geral e requisitos para geração e verificação de certificados de atributo na icp-brasil. versão 1.1. 2016.

JIN, X.; KRISHNAN, R.; SANDHU, R. S. A unified attribute-based access control model covering dac, mac and rbac. *DBSec*, Springer, v. 12, p. 41–55, 2012.

JOSEFSSON, S. *The Base16, Base32, and Base64 Data Encodings - RFC 4648*. Internet Engineering Task Force (IETF), 2006. Disponível em: <https://tools.ietf.org/html/rfc4648>. Acesso em: 12/08/2017.

LARMOUTH, J. *ASN. 1 complete*. [S.l.]: Morgan Kaufmann, 2000.

LEE, H. K.; LUEDEMANN, H. Lightweight decentralized authorization model for inter-domain collaborations. In: ACM. *Proceedings of the 2007 ACM workshop on Secure web services*. [S.l.], 2007. p. 83–89.

LIN, A.; VULLINGS, E.; DALZIEL, J. A trust-based access control model for virtual organizations. In: IEEE. *2006 Fifth International Conference on Grid and Cooperative Computing Workshops*. [S.l.], 2006. p. 557–564.

MAVRIDIS, I.; GEORGIADIS, C.; PANGALOS, G. Access-rule certificates for secure distributed healthcare applications over the internet. *Health Informatics Journal*, Sage Publications Sage CA: Thousand Oaks, CA, v. 8, n. 3, p. 127–137, 2002.

MAVRIDIS, I.; GEORGIADIS, C.; PANGALOS, G.; KHAIR, M. Access control based on attribute certificates for medical intranet applications. *Journal of medical Internet research*, JMIR Publications Inc., v. 3, n. 1, 2001.

MAVRIDIS, I.; PANGALOS, G.; KHAIR, M.; BOZIOS, L. Defining access control mechanisms for privacy protection in distributed medical databases. In: *Proceedings of IFIP Working Conference on User Identification and Privacy Protection*. [S.l.: s.n.], 1999.

MOTTA, G. H. M. B. Towards social radiology as an information infrastructure: Reconciling the local with the global. *JMIR medical informatics*, JMIR Publications Inc., Toronto, Canada, v. 2, n. 2, p. 27, 2014.

MUN, S. K.; TOHME, W. G.; PLATENBERG, R. C.; CHOI, I. Teleradiology and emerging business models. *Journal of telemedicine and telecare*, Sage Publications Ltd., v. 11, n. 6, p. 271, 2005.

NAKAMURA, E. T.; GEUS, P. L. de. *Segurança de Redes em Ambientes Cooperativos*. [S.l.]: Novatec, 2007.

NASSER, B.; LABORDE, R.; BENZEKRI, A.; BARRÈRE, F.; KAMEL, M. Access control model for inter-organizational grid virtual organizations. In: SPRINGER. *OTM Confederated International Conferences"On the Move to Meaningful Internet Systems"*. [S.l.], 2005. p. 537–551.

NGO, C.; MEMBREY, P.; DEMCHENKO, Y.; LAAT, C. de. Policy and context management in dynamically provisioned access control service for virtualized cloud infrastructures. In: IEEE. *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*. [S.l.], 2012. p. 343–349.

OASIS. *eXtensible Access Control Markup Language (XACML) Version 3.0 Plus. Errata 01*. 2017.

OSBORN, S. Mandatory access control and role-based access control revisited. In: ACM. *Proceedings of the second ACM workshop on Role-based access control*. [S.l.], 1997. p. 31–40.

PERIORELLIS, P.; PARASTATIDIS, S. Task-based access control for virtual organizations. In: SPRINGER. *International Workshop on Scientific Engineering of Distributed Java Applications*. [S.l.], 2004. p. 38–47.

RAY, I.; ONG, T. C.; RAY, I.; KAHN, M. G. Applying attribute based access control for privacy preserving health data disclosure. In: IEEE. *2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*. [S.l.], 2016. p. 1–4.

SAMARATI, P.; VIMERCATI, S. Access control: Policies, models, and mechanisms. In: SPRINGER. *International School on Foundations of Security Analysis and Design*. [S.l.], 2000. p. 137–196.

SANDHU, R. S. Lattice-based access control models. *Computer*, IEEE, v. 26, n. 11, p. 9–19, 1993.

SANDHU, R. S.; SAMARATI, P. Access control: principle and practice. *IEEE communications magazine*, IEEE, v. 32, n. 9, p. 40–48, 1994.

SHEN, H.; HONG, F. An attribute-based access control model for web services. In: IEEE. *Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT'06. Seventh International Conference on*. [S.l.], 2006. p. 74–79.

SILVA, E. F.; MUCHALUAT-SAADE, D. C.; FERNANDES, N. C. Across: A generic framework for attribute-based access control with distributed policies for virtual organizations. *Future Generation Computer Systems*, Elsevier, v. 78, p. 1–17, 2018.

STALLINGS, W. *Criptografia e Segurança de Redes*. [S.l.]: Pearson, 2008.

TIE, M.; KOCZWARA, B. Quality improvement through teleradiology: opportunities and challenges. *Australasian radiology*, Wiley Online Library, v. 48, n. 4, p. 476–479, 2004.

TURNER, S.; HOUSLEY, R.; FARRELL, S. *An Internet Attribute Certificate Profile for Authorization - RFC 5755*. Internet Engineering Task Force (IETF), 2010. Disponível em: <https://tools.ietf.org/html/rfc5755>. Acesso em: 07/08/2017.

VILLARRUBIA, G.; PAZ, J. F. D.; PELKI, D.; PRIETA, F. de la; OMATU, S. Virtual organization with fusion knowledge in odor classification. *Neurocomputing*, Elsevier, v. 231, p. 3–10, 2017.

YUAN, E.; TONG, J. Attributed based access control (abac) for web services. In: IEEE. *Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on*. [S.l.], 2005.