

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
MESTRADO EM INFORMÁTICA

DICOMFLOW: GATEWAY ASSÍNCRONO E DESCENTRALIZADO PARA
FORMAÇÃO DE UMA INFRAESTRUTURA DE INFORMAÇÃO
PARA DISTRIBUIÇÃO DE IMAGENS MÉDICAS

DANILO ALEXANDRE BARBOSA DE ARAÚJO

João Pessoa, PB
Agosto, 2017

**UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
MESTRADO EM INFORMÁTICA**

**DICOMFLOW: GATEWAY ASSÍNCRONO E DESCENTRALIZADO PARA
FORMAÇÃO DE UMA INFRAESTRUTURA DE INFORMAÇÃO
PARA DISTRIBUIÇÃO DE IMAGENS MÉDICAS**

DANILO ALEXANDRE BARBOSA DE ARAÚJO

**João Pessoa, PB
Agosto, 2017**

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
MESTRADO EM INFORMÁTICA

**DICOMFLOW: GATEWAY ASSÍNCRONO E DESCENTRALIZADO PARA
FORMAÇÃO DE UMA INFRAESTRUTURA DE INFORMAÇÃO
PARA DISTRIBUIÇÃO DE IMAGENS MÉDICAS**

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

João Pessoa, PB
Agosto, 2017

A663d Araújo, Danilo Alexandre Barbosa de.
DicomFlow: *Gateway* assíncrono e descentralizado para formação de uma
infraestrutura de informação para distribuição de imagens médicas/ Danilo
Alexandre Barbosa de Araújo. - João Pessoa, 2017.
184 f. : il.

Orientador: Prof. Dr. Gustavo H. M. B. Motta.
Dissertação (Mestrado) – UFPB/CI/PPGI

1. Informática. 2. Telerradiologia. 3. Imagens médicas - Distribuição.
I. Título.

UFPB/BC

CDU - 004(043)

FOLHA DE APROVAÇÃO



UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA



Ata da Sessão Pública de Defesa de Dissertação de Mestrado de Danilo Alexandre Barbosa de Araujo, candidato ao título de Mestre em Informática na Área de Sistemas de Computação, realizada em 31 de agosto de 2017.

1 Aos trinta e um dias do mês de agosto, do ano de dois mil e dezessete, às dezesseis horas,
2 no Centro de Informática da Universidade Federal da Paraíba, em Mangabeira, reuniram-se
3 os membros da Banca Examinadora constituída para julgar o Trabalho Final do Sr. Danilo
4 Alexandre Barbosa de Araujo, vinculado a esta Universidade sob a matrícula nº 2015104355,
5 candidato ao grau de Mestre em Informática, na área de "Sistemas de Computação", na linha
6 de pesquisa "Computação distribuída", do Programa de Pós-Graduação em Informática, da
7 Universidade Federal da Paraíba. A comissão examinadora foi composta pelos professores:
8 Gustavo Henrique Matos Bezerra Motta (PPGI-UFPB), Orientador e Presidente da Banca,
9 Gledson Elias da Silveira (PPGI-UFPB), Examinador Interno, Severino Aires de Araujo Neto
10 (UFPB), Examinador externo ao programa, e Paulo Mazzoncini de Azevedo Marques (USP),
11 Examinador Externo à Instituição. Dando início aos trabalhos, o Presidente da Banca,
12 cumprimentou os presentes, comunicou aos mesmos a finalidade da reunião e passou a
13 palavra ao candidato para que o mesmo fizesse a exposição oral do trabalho de dissertação
14 intitulado "DicomFlow: gateway assíncrono e descentralizado para formação de uma
15 infraestrutura de informação para distribuição de imagens médicas". Concluída a exposição,
16 o candidato foi arguido pela Banca Examinadora que emitiu o seguinte parecer: **"aprovado"**.
17 Do ocorrido, eu, Clauriton de Albuquerque Siebra, Coordenador do Programa de Pós-
18 Graduação em Informática, lavrei a presente ata que vai assinada por mim e pelos membros
19 da banca examinadora. João Pessoa, 31 de agosto de 2017.

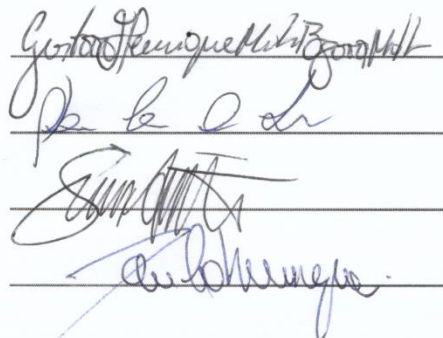

Prof. Dr. Clauriton de Albuquerque Siebra

Prof. Dr. Gustavo Henrique Matos Bezerra Motta
Orientador (PPGI-UFPB)

Prof. Dr. Gledson Elias da Silveira
Examinador interno (PPGI-UFPB)

Prof. Dr. Severino Aires de Araujo Neto
Examinador externo ao programa (UFPB)

Prof. Dr. Paulo Mazzoncini de Azevedo Marques
Examinador externo à Instituição (USP)



Em memória de Ana Maria Barbosa de Araújo Oliveira, Gilson Barbosa Ferreira
e Otaviano Henrique Silva Barbosa. Irmã, tio e primo amados.

AGRADECIMENTOS

A DEUS, por me guiar com sua luz divina permitindo a concretização de mais uma realização. Aos meus pais pelo exemplo. Aos meus irmãos pelos conselhos. A minha esposa Layse Ribeiro Araújo Barbosa pelo seu amor e paciência. Aos amigos da Superintendência de Tecnologia da Informação pelo apoio e suporte, em especial Juracy Regis de Lucena Neto, que trabalhou comigo durante todo o projeto. Aos amigos Paulo Mazzoncini e Saulo Cordeiro do Centro de Ciências das Imagens e Física Médica da Faculdade de Medicina de Ribeirão Preto (CCIFM-FMRP), Universidade de São Paulo (USP), pela ajuda com a validação da proposta. Aos professores que contribuíram com seus conhecimentos para meu aprendizado, em especial ao meu professor orientador Gustavo H. M. B. Motta, que sem ele este trabalho não seria possível.

SUMÁRIO

RESUMO	xii
ABSTRACT	xiii
1. Introdução	1
1.1. Objetivos	4
1.1.1. Objetivo geral	4
1.1.2. Objetivos específicos	4
1.2. Justificativa	4
1.3. Organização do trabalho	6
2. Referencial Teórico	8
2.1. Infraestrutura de Informação	8
2.1.1. Cultivando infraestruturas de informação	14
2.2. Infraestrutura de informação telerradiológica	18
2.2.1. Digitalização de imagens e arquitetura PACS/DICOM	18
2.2.2. Modelos de infraestrutura telerradiológica	22
2.2.3. Os perfis IHE	27
2.3. Considerações finais	31
3. Trabalhos relacionados	33
3.1. Critérios de identificação	33
3.2. Soluções em Nuvem (Cloud Computing)	35
3.3. Soluções com perfis de Integração IHE	40
3.4. Soluções Ponto-a-Ponto (P2P)	42
3.5. Soluções com e-mail	44
3.6. Considerações finais	46
4. DicomFlow	50
4.1. Metodologia	50
4.2. O protocolo de serviços	52
4.2.1. Segurança das informações	60
4.3. Cenários de uso	62
4.3.1. Transferência Simples	62
4.3.2. Distribuição compartilhada	63
4.3.3. Distribuição para diagnóstico	65
4.3.4. Distribuição para diagnóstico com repositório terceirizado	67
4.3.5. Rede social radiológica	68
4.4. A arquitetura do DicomFlow	69

4.4.1.	Módulo DicomMessage.....	73
4.4.2.	Módulo DicomMove	82
4.5.	Considerações finais	91
5.	Experimentos	93
5.1.	Testes de viabilidade técnica	93
5.1.1.	Ambiente de execução para viabilidade técnica.....	94
5.1.2.	Especificação dos experimentos de viabilidade técnica	95
5.1.3.	Resultados do experimento de viabilidade técnica.....	96
5.2.	Testes de implantação do gateway	98
5.2.1.	Ambiente de implantação do gateway.....	98
5.2.2.	Especificação dos experimentos de implantação do gateway	102
5.2.3.	Resultados da implantação do gateway	103
5.3.	Considerações finais	103
6.	Conclusão	105
6.1.	Resultados dos experimentos	105
6.2.	Objetivos alcançados	108
6.3.	Considerações finais	109
6.4.	Limitações.....	112
6.5.	Publicações.....	113
7.	Referências Bibliográficas	114
	APÊNDICE A – PROTOCOLO DE COMUNICAÇÃO DICOMFLOW	119

LISTA DE FIGURAS

Figura 1 - Modelo básico de arquitetura PACS.....	20
Figura 2 - Fluxo de trabalho radiológico	21
Figura 3 – Limitação na comunicação do protocolo DICOM.....	24
Figura 4 - Interoperabilidade entre PACS limita por firewalls.....	24
Figura 5 - Tensão entre demandas locais e globais para prática radiológica	26
Figura 6 - Atores e transações dos perfis XDS e XDS-I	29
Figura 7 - Atores e transações dos perfis XCA e XCA-I	30
Figura 8 - Protocolo atuando a margem da infraestrutura PACS/DICOM.....	53
Figura 9- Envio de mensagem contendo os dados do novo exame	55
Figura 10 - E-mail de Solicitação de armazenamento conforme especificado pelo Protocolo.....	56
Figura 11 - Transferência de Imagens para o receptor.....	60
Figura 12 - Cenário 1 e fluxo de Storage.....	63
Figura 13 - Cenário 2 e fluxo de Sharing.....	64
Figura 14 – Cenário 3 e o fluxo de Request	66
Figura 15 - Cenário 4 e fluxo de Storage e Request	67
Figura 16 - Cenário 5: Infraestrutura de Informação telerradiológica	69
Figura 17 – Arquitetura do DicomFlow e tecnologias empregadas.....	72
Figura 18 - Pacotes do módulo DicomMessage.....	74
Figura 19 - Interface e classes que representam a estrutura XML Storage	75
Figura 20 - Processo de criação, assinatura e criptografia da mensagem.....	77
Figura 21 - Exemplo de mensagem de serviço criada	78
Figura 22 - Conjunto de classes utilizadas para o envio e recebimento de mensagens de serviço.....	79
Figura 23- Diagrama de sequência de envio de mensagem de serviço.....	80
Figura 24 - Utilização da API em linha de comando.....	81
Figura 25- Informações de mensagens de serviço armazenadas no BD do DicomFlow	83
Figura 26 - Pacotes do módulo DicomMove	83
Figura 27 - Interfaces do pacote Entidade	84
Figura 28 - Classes ORM das mensagens de serviço	85
Figura 29 - Diagrama Entidade Relacionamento (ER) do DicomFlow.....	86
Figura 30 - Expressão regular de envio de mensagem	87
Figura 31 - Interfaces e classes do pacote Controle	88
Figura 32 - Classes do pacote Agendamento.....	89
Figura 33 - mecanismo de controle de acesso às imagens	91
Figura 34 - Tempo médio de transmissão (a) e requisição (b) por quant. de exames..	97
Figura 35 - Tempo médio de sincronização entre as Máquinas 1 e 2.	97
Figura 36 - Tempo médio de sincronização máquina 3.	98
Figura 37 - Interface da aplicação cliente.....	101

TABELAS

Tabela 1 - As propriedades das classes de projeto.....	9
Tabela 2 - Princípios da Teoria de Projeto para Infraestrutura de Informação	15
Tabela 3 - Regras de projeto relativas à adaptação	16
Tabela 4 - Regras de projeto relativas ao <i>bootstrap</i>	17
Tabela 5 - Comparação entre os trabalhos relacionados	49
Tabela 6 – Mensagens de Serviço do protocolo e suas principais ações.....	59
Tabela 7 - Especificações dos servidores de imagens.	94
Tabela 8 - Exames e arquivos XML empregados no experimento.	95
Tabela 9 - Configuração do ambiente do experimento A.....	99
Tabela 10 - Configuração do ambiente do experimento B	100
Tabela 11 - Comparação entre os trabalhos relacionados	111

RESUMO

ARAÚJO, Danilo Alexandre Barbosa. **DicomFlow: gateway assíncrono e descentralizado para formação de uma infraestrutura de informação para distribuição de imagens médicas**. 2017. 172 f. Dissertação (Mestrado em Informática) – Programa de Pós-Graduação em Informática, Universidade Federal da Paraíba, João Pessoa, 2017.

A digitalização de imagens médicas, o modelo PACS/DICOM e os avanços das tecnologias de informação e comunicação proporcionam as condições para formar uma infraestrutura para distribuição de imagens médicas em larga escala. Entretanto, mesmo considerando a grande base instalada PACS/DICOM, não se observa a formação de uma infraestrutura de informação para troca de imagens médicas entre entidades de saúde, pois a inércia da base instalada dificulta sua evolução. Uma infraestrutura de informação oferece um espaço de compartilhamento de informações e colaboração que permite a associação espontânea de pessoas, organizações e componentes tecnológicos situados em contextos geográficos distintos para desenvolvimento de alguma atividade. O objetivo desse trabalho foi elaborar o DicomFlow, um *gateway* assíncrono, assimétrico e descentralizado, construído sobre a base instalada PACS/DICOM e infraestrutura de e-mail da Internet visando promover a formação de uma infraestrutura de informação para a distribuição de imagens médicas, favorecendo a prática de trabalho radiológica. Para tanto, especificou-se um protocolo de comunicação com suporte a serviços de gerência de exames de imagens DICOM baseado em troca de mensagens assíncronas e transmissão de imagens médicas e construiu-se um modelo arquitetural para esse fim. Experimentos em ambiente simulado e ambiente real foram realizados para avaliar a infraestrutura quanto a sua viabilidade técnica e operacional. Concluiu-se que o DicomFlow possibilita a troca de imagens entre profissionais e organizações de saúde quaisquer, desde que pertençam à base instalada, fomentando a formação de uma infraestrutura de informação para distribuição de imagens médicas.

Palavras-Chave: Telerradiologia, PACS, DICOM, Infraestrutura de Informação, Imagens Médicas.

ABSTRACT

ARAÚJO, Danilo Alexandre Barbosa. **DicomFlow: asynchronous and decentralized gateway for the formation of an information infrastructure for distribution of medical images**. 2017. 172 f. Dissertação (Mestrado em Informática) – Programa de Pós-Graduação em Informática, Universidade Federal da Paraíba, João Pessoa, 2017.

Digitalization of medical images, the PACS/DICOM model and advances of information and communication technologies provide the conditions to form an infrastructure for a large scale distribution of medical images. However, even considering the large installed base of PACS/DICOM, the formation of a common information infrastructure for the exchange of medical images between health organizations is not observed, as the inertia of the installed base hinders its development. An information infrastructure offers a space for information sharing and collaboration that allows the spontaneous association of people, organizations and technological components located in different geographical contexts for the development of an activity. The aim of this study was to develop the DicomFlow, an asynchronous, asymmetric and decentralized *gateway*, built over the PACS/DICOM installed base and e-mail infrastructure of the Internet aiming to promote the formation of an information infrastructure for distribution medical imaging, favoring the radiological work practice. Therefore, it was specified a communication protocol that supports DICOM management services based on messages exchanges and transmission of medical images, built in a modular architecture. Experiments in simulated and real environment were conducted to preliminarily assess the infrastructure as its technical and operational feasibility. It was concluded that the DicomFlow enables the exchange of images between professionals and any health organizations, provided that they belong to the installed base, promoting the formation of an information infrastructure for distribution of medical images.

Keywords: Teleradiology, PACS, DICOM, Information Infraestructure, Medical Imaging.

1. Introdução

A digitalização de imagens médicas possibilitou aos departamentos de radiologia reduzir custos de aquisição de imagens, aumentar a qualidade de diagnósticos e estabelecer um fluxo de trabalho radiológico comum. O que estimulou organizações e profissionais de saúde, juntamente com a comunidade científica, a estabelecerem o padrão DICOM (*Digital Imaging and Communications in Medicine*) (DICOM, 2017) para tratamento, armazenamento e transmissão de imagens médicas (Pianykh, 2012), suportado pelos sistemas PACS (*Picture Archiving and Communication Systems*), formando uma base amplamente adotada nos departamentos de radiologia (Huang, 2010). Ainda, o avanço das tecnologias de informação e comunicação nas últimas décadas proporcionou as condições técnicas para formação de uma infraestrutura para distribuição de estudos de imagens médicas em larga escala.

Entretanto, não se observa a formação de uma infraestrutura de informação (II) telerradiológica comum para distribuição de imagens médicas entre profissionais e organizações de saúde de forma ampla, fácil, efetiva e segura (Motta, 2014). Pois, mesmo que a infraestrutura PACS/DICOM não possua grandes impedimentos para distribuir exames quando o acesso é feito no âmbito local dos departamentos de radiologia, existem sérios obstáculos quando se trata do acesso em uma escala global. Primeiro, o modelo PACS/DICOM foi concebido entre meados das décadas de 80 e 90, em um contexto de redes locais (Huang, 2010), fato que dificulta sua utilização através da Internet, por exemplo, devido à utilização de portas geralmente bloqueadas por *firewalls*, o excesso de informações de controle na comunicação de imagens (*overhead*) e a ausência de mecanismos de segurança para transmissão de informação do paciente (Pianykh, 2012). Segundo, o protocolo DICOM possibilita diversas formas de construção dos sistemas PACS (Huang, 2010), permitindo que os departamentos personalizem o modelo às suas necessidades, tornando as infraestruturas variadas e dificultando a elaboração de soluções que promovam interoperabilidade entre esses departamentos.

A limitação tecnológica e a heterogeneidade presente nas infraestruturas PACS/DICOM impõem uma inércia que tende a manter os exames de imagens no domínio local onde foram originados, dificultando seu compartilhamento (Hanseth

e Lyytinen, 2010; Star e Ruhleder, 1996). Por outro lado, a ausência de padrões viáveis na prática para interoperabilidade leva ao estabelecimento de acordos bilaterais entre as partes, caracterizados pela adoção de soluções *ad hoc* de integração (Ribeiro et al., 2011), em geral baseadas em redes privadas virtuais (VPN - *Virtual Private Networks*) e computação na nuvem (*Cloud Computer*) (Chatterjee et al., 2017).

Redes privadas virtuais são capazes de permitir a interpretação remota de imagens para locais predefinidos em um serviço de telerradiologia localmente gerenciado, contudo se limitam ao atendimento de demandas locais de compartilhamento à distância, por requererem configurações ponto-a-ponto, como por exemplo, sincronismo no estabelecimento de conexão (*tunneling*) (Silva et al. 2013). Ademais, são soluções proprietárias, não interoperáveis e não escaláveis.

Por outro lado, soluções baseadas em computação na nuvem (Silva et al. 2013; Monteiro et al., 2016; Yuan et al., 2015; Godinho et al., 2016), dependem de elementos centrais, por exemplo, para fins de armazenamento ou de comunicação (e.g. uso de *brokers*). Ainda, mesmo considerando as vantagens de permitir acesso a dados e serviços com um mínimo de infraestrutura pelos clientes, a computação em nuvem traz os riscos da dependência de um único provedor, aliada a requisitos especiais necessários, tais como manter a privacidade, a segurança, e acordos públicos, especialmente ao lidar com ambientes públicos de compartilhamento de imagem. Mesmo soluções em nuvem (Zhang et al., 2011; Ribeiro et al., 2014) baseadas nos padrões *Cross-Enterprise Document Sharing for Image* (XDS-I) (XDS-I, 2017) e *Cross-Community Access for Image* (XCA-I) (XCA-I, 2017), desenvolvidos e mantidos pela iniciativa IHE (*Integrating the Healthcare Enterprise*) (IHE, 2017) para compartilhamento de imagens entre múltiplas partes, também pressupõem autoridade ou elementos centrais, seja para coordenação, controle ou operação.

Então, essas soluções de integração apresentadas não se prestam para estabelecer uma infraestrutura de informação para troca de estudos de imagens entre múltiplas partes, uma vez que infraestruturas de informação possuem um controle distribuído e episódico e não têm autoridade ou elementos centrais. E mais, infraestruturas de informação envolvem a noção de uma infraestrutura aberta e compartilhada, considerada um bem comum, suportando um espaço social onde

pessoas, organizações e componentes técnicos podem espontaneamente formar associações para o desenvolvimento de alguma atividade (Bowker et al., 2010). Podemos citar a própria Internet como exemplo de infraestrutura de informação com essas características.

Ademais, é importante ressaltar que uma infraestrutura de informação não resulta da execução de um projeto especificado *a priori*. É formada por meio de um processo evolutivo, que contrariamente à abordagem tradicional de “projetar do zero”, segue um enfoque de “cultivar” uma infraestrutura preexistente, denominada base instalada, sobre a qual uma nova infraestrutura é formada (e.g., a *web* utilizou a infraestrutura TCP/IP como base instalada), a fim de fomentar seu crescimento dinâmico por meio de um processo de alavancagem (*bootstrap*) e crescimento adaptativo (Hanseth e Lyytinen, 2010). Isto é, uma infraestrutura de informação ocorre quando uma infraestrutura se auto reforça (alavancagem) a partir de uma base instalada e sustenta continuamente seu crescimento (adaptação) de modo a não ficar paralisada devido à inércia da própria base instalada (Hanseth e Lyytinen, 2010; Star e Ruhleder, 1996).

Assim, para favorecer o cultivo de uma infraestrutura de informação telerradiológica para distribuição de imagens médicas é necessária a utilização de métodos que possibilitem a elaboração de *gateways* capazes de dotar o modelo PACS/DICOM de flexibilidade que possibilite a interação de entidades arbitrárias de forma transparente, promovendo a auto-organização e adaptação da II (Star e Ruhleder, 1996). *Gateways* são soluções concebidas para contornar possíveis problemas de associação entre entidades heterogêneas. Como exemplo de *gateway*, tem-se o protocolo DNS, que funciona como um elo entre os seguintes elementos heterogêneos: endereços IP e nomes de domínio, que no seu surgimento, permitiu o estabelecimento da *web* sobre a então base instalada da Internet.

Com base no exposto, observa-se que a construção e adoção de um *gateway* de comunicação facilitará a troca de imagens médicas entre infraestruturas telerradiológicas distintas e possibilitará a formação de uma infraestrutura de informação global para a distribuição de imagens médicas e a prática radiológica.

1.1. Objetivos

1.1.1. Objetivo geral

O objetivo geral deste trabalho é contribuir para a melhora na distribuição de imagens médicas entre infraestruturas de saúde heterogêneas pertencentes a domínios de redes distintos, através da elaboração de uma solução (gateway) capaz de dotar a base instalada PACS/DICOM de flexibilidade e possibilitar a interação de entidades heterogêneas arbitrárias de forma transparente, promovendo a auto-organização e adaptação para formação de uma infraestrutura de informação global para distribuição de imagens médicas.

1.1.2. Objetivos específicos

- a) Definição e implementação de um protocolo de comunicação e suporte a serviços de gerência de exames de imagens DICOM.
- b) Elaboração de um Modelo Arquitetural de software, assíncrono e descentralizado, constituído de duas módulos, para comunicação da aquisição de novos exames e transferência de imagens médicas.
- c) Implementação do Modelo Arquitetural elaborado, em conformidade com as diretrizes especificadas no protocolo de comunicação.
- d) Testes de viabilidade das tecnologias empregadas na solução implementada.

1.2. Justificativa

Muitos países estão em um processo de implementação de infraestruturas de serviços eletrônicos de saúde (eHealth) em âmbito nacional, na expectativa de que tais serviços permitam formas mais eficientes e rentáveis de prestar assistência, tornando os cuidados e as informações de saúde mais acessíveis aos pacientes (Grisot e Vassilakopoulou, 2015). Dentre vários serviços a serem fornecidos, os profissionais de saúde destacam o serviço de diagnóstico por imagem médica como ferramenta de maior importância. Por essa razão organizações de saúde e de pesquisa aumentaram significativamente seus interesses na área de imagem médica, tentando desenvolver soluções para criação, armazenamento, troca e apresentação de imagens médicas (Ribeiro et al., 2010).

Após a consolidação dos sistemas PACS para colaboração entre membros de setores especializados dentro da mesma instituição, surgiu uma procura crescente por compartilhamento de estudos de imagens médicas entre profissionais de saúde situados em locais geograficamente distantes uns dos outros (Noumeir, 2011) (Figueiredo e Motta, 2012) (Chatterjee et al., 2017). Essa demanda desencadeou pesquisas que resultaram na formação de infraestruturas para compartilhamento de imagens entre profissionais geograficamente distribuídos, mas pertencentes a uma mesma entidade de saúde, ou seja, pertencentes a um mesmo domínio. Hoje, existem espalhadas pelo mundo diversas infraestruturas telerradiológicas adequadas às necessidades das entidades de saúde que as desenvolvem (MAPS, 2017).

O problema nessas infraestruturas ocorre quando os profissionais de saúde necessitam compartilhar ou acessar imagens médicas fora do domínio em eles atuam, por exemplo, quando um profissional de saúde precisa de uma segunda opinião sobre uma imagem por outro profissional situado fora do domínio da infraestrutura. Essa situação requer que entidades de saúde pertencentes a domínios distintos busquem associarem-se. Contudo, a diversidade e o arranjo das tecnologias empregadas nas infraestruturas envolvidas, como também a existência de diversas formas de organizar membros, atividades e processos para compartilhamento de informações e imagens médicas soluções, fazem com que as entidades de saúde adotem abordagens altamente centralizadas ou rigidamente hierárquicas para ampliar os serviços de saúde, que não são adequadas para as maneiras dinâmicas e imprevisíveis em que os serviços de saúde podem se expandir e tornar-se sustentável (Paina e Peters, 2012), principalmente o compartilhamento de imagens que favorece a prática radiológica (Motta, 2014). Assim, o surgimento de uma infraestrutura de informação para o compartilhamento de imagens médicas facilitaria a cooperação entre entidades e profissionais de saúde, inclusive de forma dinâmica e imprevisível, de modo a permitir a associação entre eles com o objetivo de promover a cooperação, celeridade e qualidade nos laudos a fim de melhorar o cuidado com os pacientes (Oliveira e Motta, 2014).

O problema apresentado é suficiente para incentivar tal pesquisa, e de fato é o ponto de partida. Não é satisfatório apenas empregar as tecnologias de forma a solucionar um problema imediato de associação entre duas infraestruturas, é

preciso analisar a forma como essas tecnologias serão empregadas em cada uma delas e fornecer soluções que possibilitem associações futuras, ainda não previstas, possibilitando que a infraestrutura resultante seja capaz de se adaptar a novos requisitos de compartilhamento de imagens entre domínios distintos, a fim de favorecer seu crescimento e evolução.

Portanto, através da compreensão das definições e dos conceitos empregados na construção de infraestrutura de informação, como também do entendimento da atual situação da telerradiologia, essa pesquisa contribui trazendo uma solução em forma de *gateway* que possibilita a associação facilitada entre infraestruturas pertencentes a entidades de domínios distintos e que promove a formação de uma infraestrutura de informação para a prática radiológica.

1.3. Organização do trabalho

O restante deste trabalho está organizado como segue:

Capítulo 2: Nesse capítulo são apresentadas as características das infraestruturas de informações e os aspectos relacionados à sua construção. Ainda, será apresentada a situação das infraestruturas telerradiológicas atuais através das definições do modelo PACS/DICOM e dos perfis de integração para compartilhamento de informações médicas, ressaltando as limitações que dificultam a interoperabilidade dessas infraestruturas para formação de uma infraestrutura de informação telerradiológica.

Capítulo 3: São abordados os aspectos técnicos e sociais presentes nos trabalhos relacionados que promovem interoperabilidade entre essas infraestruturas e que características esses trabalhos possuem que possibilitam a formação de uma infraestrutura de informação para a prática radiológica;

Capítulo 4: Descreve a metodologia empregada no trabalho. Ainda, descreve os aspectos técnicos e sociais do protocolo que servirá de *gateway* para prover interoperabilidade entre infraestruturas telerradiológicas. Elenca os cenários de uso para o *gateway*. Apresenta o Modelo arquitetural construído segundo as especificações do protocolo em observância aos cenários;

Capítulo 5: Descreve experimentos para avaliação da viabilidade técnica e operacional do *gateway* em ambiente simulado e real, assim como a apresentação dos resultados;

Capítulo 6: Esse capítulo apresenta as considerações finais do trabalho.

2. Referencial Teórico

O objetivo desse capítulo é definir o que são infraestruturas de informação e apresentar as principais diretrizes para sua formação. Ainda, apresentar as características presentes na infraestrutura telerradiológica atual (modelo PACS/DICOM) que são relevantes para a elaboração dos elementos que irão compor a solução que facilitará a formação de uma infraestrutura de informação telerradiológica global. Inicialmente, serão mostradas as características de uma infraestrutura de informação, seguidas dos princípios de construção de uma infraestrutura. Em seguida, serão mostradas a terminologia e os conceitos do padrão DICOM e serão descritos os principais elementos existentes na arquitetura PACS, a fim de identificar os facilitadores e os agravantes no processo de formação de uma infraestrutura de informação global para compartilhamento de imagens médicas. Por fim, será abordado o esforço despendido pela iniciativa *Integrating the Healthcare Enterprise* (IHE) em prover especificações padronizadas, organizadas em perfis de integração, para gerir o compartilhamento de registros eletrônicos em saúde (*Electronic Health Records* – EHR) entre organizações. O objetivo aqui é identificar as vantagens e as limitações nesses perfis que possam ajudar ou dificultar o processo de elaboração dos elementos necessários à solução.

2.1. Infraestrutura de Informação

O termo "infraestrutura" refere-se a conjuntos de equipamentos necessários às atividades humanas, como edifícios, estradas, pontes, estradas de ferro, canais, portos e redes de comunicações. Além disso, uma infraestrutura abrange também entidades mais abstratas, como protocolos (humanos e computadores) e padrões (Bowker et al., 2010). Quando associado ao termo "informação" envolvem recursos e serviços digitais projetados para suportar alguma atividade humana vinculada à Internet, por exemplo, serviços computacionais, centrais de ajuda, repositórios de dados (Bowker et al., 2010).

Dessa forma, uma infraestrutura de informação (II) constitui uma nova unidade de projeto quando comparada às tradicionais classes de soluções de Tecnologia de Informação (TI). Estas classes podem ser organizadas em sua ordem crescente de complexidade: recursos de TI, aplicações, plataformas e

infraestruturas de informação (Hanseth e Lyytinen, 2010). As principais diferenças entre essas classes residem em sua complexidade geral, como se relacionam com os seus ambientes de concepção e utilização, e como eles se comportam ao longo do tempo em relação a esses ambientes (Hanseth e Lyytinen, 2010). A Tabela 1 apresenta as principais propriedades das classes de projeto.

Tabela 1 - As propriedades das classes de projeto.

	Aplicações	Plataformas	Infraestruturas de Informação (II)
Compartilhamento	Localmente	Entre algumas comunidades de usuários	Universal
Abertura	Fechado a um grupo de usuários	Parcialmente, dependente do projeto	Universal, permite ilimitadas conexões entre comunidades de usuários
Heterogeneidade	Homogêneo	Parcial, dependendo das conexões entre os usuários das comunidades	Ilimitada pelo tempo ou comunidade de usuários
Evolução	Evolução delimitada, crescimento linear condicionado ao grupo de usuários	Evolução dependente da arquitetura e escolhas feitas pelas comunidades, crescimento linear	Evolução ilimitada, crescimento linear e não linear
Organização	Homogênea, composição direta de recursos de TI	Homogênea, composição direta de conjuntos de recursos de TI	Heterogêneo, composto recursivamente por classes de projeto
Controle	Centralizado	Centralizado	Distribuído e dinamicamente negociado

Fonte: Adaptado de Hanseth e Lyytinen, 2010.

Mais especificamente, recursos de TI são conjuntos de ações computacionais capazes de atender à necessidade de um usuário ou um grupo de usuários (e.g., editor de texto) enquanto aplicações são composições de recursos de TI mantidos em um contexto de projeto fechado para atender regras específicas de grupos de usuários (e.g. Microsoft Office). Ao passo que plataformas diferem de aplicações, pois seu contexto de projeto não é tão estável e possui uma base de usuários crescente, o que requer uma generalização constante de seus recursos de TI em consonância a organização dessa base de usuários (e.g., sistemas operacionais). Quanto às infraestruturas de informação, estruturalmente, são

recursivamente compostas por recursos de TI, aplicações, plataformas e outras infraestruturas. Um exemplo de infraestrutura de informação é a Internet, composta de vários recursos de TI, aplicações, plataformas e outras infraestruturas interconectadas, suportando atividades e práticas de trabalho de diversos grupos de usuários.

Logo, infraestruturas de informação podem ser definidas como estruturas que englobam aspectos técnicos e organizacionais, ambos compostos por elementos de natureza diversa, capaz de formar um sistema complexo para atendimento de uma determinada atividade ou prática de trabalho. Segundo Star e Ruhleder (1996), infraestruturas de informação emergem para as pessoas na prática, ligadas a atividades e estruturas, ou seja, surgem a partir das relações e organizações entre as soluções tecnológicas que compõem sistemas (elementos técnicos) e os usuários com suas políticas e culturas (elementos sociais) que determinam regras para uso dessas soluções. Hanseth e Lyytinen (2010) caracterizam uma infraestrutura de informação como uma infraestrutura heterogênea, aberta, compartilhada e evolutiva, construída sobre uma base instalada, formando um espaço onde pessoas, organizações e componentes tecnológicos podem espontaneamente formar associações para uma prática social comum.

Detalhando melhor as características de infraestrutura de informação, o que denominamos como base instalada são as classes de projeto preexistentes, inclusive outras infraestruturas, somadas às práticas sociais e de trabalho, sobre as quais, através de uma luta constante contra a inércia presente nessa base, se integram novos recursos de TI e novas práticas, fazendo com que a base instalada cresça e evolua (Bowker et al., 2010). Em outras palavras, a evolução de uma infraestrutura de informação está associada à base instalada na qual ela é construída. A tensão entre o fato de que as infraestruturas de informação não são facilmente alteradas e, ao mesmo tempo, estão em constante evolução, também chamada de tensão entre inovação e conservação, permite dizer que uma base instalada tanto favorece quanto limita a evolução da infraestrutura (Grisot e Vassilakopoulou, 2015). Desse modo, quando a infraestrutura evolui, herda os pontos fracos e fortes da base instalada, resultando numa nova infraestrutura que atende as práticas já existentes e ainda possibilita o surgimento de novas práticas.

A tensão com a inércia da base instalada exige projetos de plena compatibilidade com o que já existe em funcionamento (Da Silva e Motta, 2016). Portanto, construir uma infraestrutura de informação é dotar a base instalada de flexibilidade que possibilite a interação de entidades arbitrárias de forma transparente, promovendo a auto-organização e adaptação da infraestrutura de informação (Star e Ruhleder, 1996). Negligenciar esses aspectos inerentes à base instalada durante o processo de desenvolvimento de uma nova infraestrutura pode ser crítico para a sua formação (Star e Ruhleder, 1996). Como exemplo de base instalada, podemos citar a infraestrutura de redes de comunicação que compõem a Internet, construídas sobre as infraestruturas de telefonia e de rodovias, e que, durante seu processo de crescimento, mantiveram aquelas tecnologias e protocolos que possibilitam sua evolução.

Ainda sobre as características da infraestrutura de informação, sua heterogeneidade e abertura estão relacionadas à diversidade de elementos sociais e técnicos presentes nela, por exemplo, tecnologias, protocolos, comunidades de usuários e desenvolvedores, órgãos de governança e de padronização. Quanto a abertura, uma infraestrutura de informação pode incluir um número crescente desses elementos, participando tanto como usuários quanto desenvolvedores, pois não há fronteiras delimitadoras de que elementos podem ou não se integrar a ela (Hanseth e Lyytinen, 2010), desde que seja mantida a compatibilidade entre esses elementos para manter seu funcionamento (Star e Ruhleder, 1996). A agregação de elementos sociotécnicos possibilita a infraestrutura de informação expandir e formar novas conexões com outras infraestruturas, aumentando a complexidade nas relações envolvidas. Por exemplo, as comunidades de governança da Internet (IETF) e da web (W3C), embora interajam, são autônomas entre si.

A característica de compartilhamento está relacionada à infraestrutura de informação como um bem comum, não possuindo elementos centralizadores de controle, não pertencendo a uma única empresa ou organização, mas sendo usada por diversas comunidades e organizações por meios múltiplos e inesperados (Hanseth e Lyytinen, 2010). Quer dizer, infraestruturas de informação tipicamente abrangem uma coleção heterogênea de diferentes tecnologias, comunidades, organizações, componentes, pessoas, protocolos e aplicativos para suportar atividades variadas ao longo do tempo e em localidades geográficas distintas.

Devido a esta complexidade, a gestão da evolução gradual de uma infraestrutura de informação pode ser mais bem entendida como um ato de compartilhamento de responsabilidades sobre a infraestrutura por parte das comunidades, pessoas e organizações do que um ato de controle (Grisot e Vassilakopoulou, 2015).

Em relação à evolução, uma infraestrutura de informação evolui à medida que agrega novos elementos, assim estendendo suas práticas de trabalho e, conseqüentemente, resultando numa crescente heterogeneidade técnica e social, como também num aumento de complexidade nas relações envolvidas. A agregação de novos elementos é originada da reação dos seus usuários e seus desenvolvedores com aprendizado e imposição, devido à sucessão de tecnologias e interação desses usuários e desenvolvedores, que permitem a oferta de novas práticas de trabalho. Ou seja, durante seu crescimento, em um processo de design estendido, em que se observam os interesses da infraestrutura em um nível mais abrangente, artefatos inicialmente desenvolvidos com objetivo atender demandas locais são substituídos por outros de objetivo geral e que atendem múltiplos contextos. À medida que novos contextos são apresentados, num processo de design contínuo, esses artefatos evoluem ou dão espaço a novos artefatos mais genéricos, tornando a infraestrutura mais complexa (Monteiro et al., 2013).

Assim, durante o processo de crescimento e evolução, a infraestrutura de informação lida com as tensões entre as necessidades individuais de cada pessoa ou comunidade e a sua prática comum e, portanto, o objetivo é garantir que, através de padronização, as soluções tecnológicas possuam flexibilidade necessária para atender as necessidades individuais e particulares ao passo que estejam de acordo com as intenções e propósitos originais da própria infraestrutura quanto à interoperabilidade (Da Silva e Motta, 2016). Ademais, é importante destacar que, diferentemente de abordagens tradicionais de projeto, uma infraestrutura de informação nunca é modificada de cima para baixo (*top-down*) (Star e Ruhleder, 1996) e um controle distribuído e episódico é, em geral, a única forma de coordenar a sua evolução.

Sheard e Mostashari (2009) definem que infraestruturas de informação não surgem do novo e não seguem a abordagem tradicional de “projetar do zero”, como a dos princípios tradicionais de projeto de software, que empregam métodos altamente centralizados ou rigidamente hierarquizados. Neste sentido, uma

infraestrutura de informação não resulta da execução de um projeto especificado *a priori*, mas evolui à medida que emerge da contínua ação recíproca entre pessoas, organizações e componentes tecnológicos num processo concorrente de construção e reconstrução (Aanestad e Hanseth, 2000), também denominado de *continuous design* (Monteiro et al., 2013). Hanseth e Lyytinen (2010) reconhecem os obstáculos em lidar com projetos de infraestruturas de informação que buscam resolver as tensões oriundas dessas ações recíprocas, uma razão para isso são as dificuldades promovidas pelo comportamento diversificado e dinâmico da infraestrutura de informação, tornando a extração de requisitos, por exemplo, de pouca utilidade.

Erros na escolha de tecnologias, má tomada de decisão e desatenção às políticas existentes podem limitar a difusão e evolução da infraestrutura, consequentemente levando à reversos salientes (*Reverse Salients*) (Hughes, 1987). Esta é uma metáfora militar referindo-se a pontos onde uma frente de avanço é retida. Em termos de mudança tecnológica, a analogia refere-se a problemas de engenharia cuja solução é necessária para que a infraestrutura como um todo possa crescer (Edwards et al., 2007). Esses reversos não são necessariamente técnicos, de fato, a maioria deles são problemas legais, políticos, sociais e culturais. Uma vez que são amplamente compreendidos, tornam-se foco de esforços de investigação intensos. Tipicamente, vários grupos convergem em soluções ao mesmo tempo em torno dos reversos salientes (Edwards et al., 2007). Uma vez que os reversos salientes são contornados, a infraestrutura volta a crescer. Como exemplo, podemos citar o problema de comunicação entre equipamentos de radiologia de fabricantes distintos, cujo esforço para resolvê-lo resultou no padrão DICOM e possibilitou a formação da infraestrutura PACS/DICOM.

Portanto, o crescimento das infraestruturas de informação está associado a um esforço contínuo envolvendo seus componentes, como parte de um processo de inovação continuada, em que cultivar é mais relevante que construir. Isto é, substituir ou alterar elementos existentes sempre que necessário sem mudar radicalmente a arquitetura constituída, além de ampliar a infraestrutura de informação pela adição de novos componentes a partir de incrementos modulares, objetivando uma evolução (Grisot, Hanseth e Thorseng, 2014). Hanseth e Lyytinen (2010) descrevem a Internet como um exemplo de infraestrutura de informação

bem-sucedida, no qual eles analisaram o processo de sua evolução, destacando que seu controle é difundido entre comunidades diversas, é constituída de várias camadas fracamente acopladas, permitindo que as alterações não comprometam o trabalho das outras. Sua estrutura permite a livre inclusão ou exclusão de componentes que tanto podem ser equipamentos ou softwares, como uma nova comunidade de projetistas, um novo protocolo ou padrão e a natureza diversificada desses componentes faz com que a infraestrutura evolua e aumente sua heterogeneidade e complexidade.

2.1.1. Cultivando infraestruturas de informação

Como foi apresentado anteriormente, idealizar uma infraestrutura como uma infraestrutura de informação é dotá-la de uma flexibilidade que favoreça a associação espontânea entre usuários, organizações e componentes tecnológicos com atividades e estruturas situadas em contextos distintos (Bowker et al., 2010), a fim de formar um espaço social para a prática de uma determinada atividade, oferecendo compartilhamento de recursos e colaboração entre os elementos (Motta, 2014). Contudo, o desafio é como induzir um movimento para formação de uma infraestrutura de informação, visto que métodos tradicionais de desenvolvimento são incapazes de lidar com a complexidade da infraestrutura de informação, por exemplo, devido à ausência de autoridade central e ser projetada com especificações parciais (Paina e Peters, 2012). Em face desse desafio, Hanseth e Lyytinen (2010) apresentam a teoria de projeto para complexidade dinâmica em infraestruturas de informação (*Design Theory for Dynamic Complexity in Information Infrastructures – DTDC-II*). A DTDC-II é uma teoria normativa sistematizada a partir de descrições empíricas da evolução de infraestruturas de informação, em especial a Internet, que considera a complexidade dinâmica no projeto de uma infraestrutura de informação, visto como um sistema sociotécnico de TI com características de sistemas adaptativos complexos (*Complex Adaptive Systems - CAS*) (Oliveira e Motta, 2014).

O estudo de sistemas complexos surgiu como abordagens multidisciplinares para a compreensão do comportamento de agentes diversos e processos interligados a partir de uma perspectiva ampla do sistema. CAS, além de ser composta de muitos componentes que interagem, têm a capacidade de se auto

organizar, adaptar ou aprender com a experiência. As interações dos componentes do sistema são geralmente complexas e não-lineares, e não são facilmente controladas ou previsíveis em detalhe (Paina e Peters, 2012). Nesse tipo de sistema, não existe um controle central, seu conjunto é guiado pelo comportamento de seus agentes autônomos em reação a outros agentes e ao ambiente pelo qual estão incluídos (Hanseth e Lyytinen, 2010). Ainda, a base instalada é retratada como fonte que se retroalimenta (*feedback*) favorecendo surgimento de novas capacidades dentro da própria base, a partir de aprendizado e interações entre seus elementos, permitindo que a infraestrutura de informação evolua e revele novas capacidades (Hanseth e Lyytinen, 2010).

Hanseth e Lyytinen (2010) definem que a teoria de projetos para infraestrutura de informação visa orientar projetistas na criação e condução de projetos de infraestrutura de informação, tendo por base principal a teoria de CAS. Propõem 5 (cinco) princípios de projeto (Tabela 2) e um conjunto de 19 regras de distribuídas entre esses princípios para tratar dois problemas da construção de uma II: O problema da alavancagem (*bootstrap*) e o problema da adaptação.

Tabela 2 - Princípios da Teoria de Projeto para Infraestrutura de Informação

Princípios relativos ao <i>bootstrap</i>	Princípios relativos à adaptação
Projetar inicialmente para utilidade direta.	Criar recursos de TI o mais simples possível.
Projetar sobre uma base instalada existente.	Modularizar a infraestrutura de informação.
Expandir a base instalada por táticas persuasivas.	

Fonte: Adaptado de Hanseth e Lyytinen, 2010.

O problema do *bootstrap* refere-se a como provocar o interesse em uma base instalada, suscitando um atrator que sustente seu crescimento. Os CAS postulam que os agentes do sistema, conduzidos por esses atratores, empurram todo o sistema a uma ordem emergente, alcançando muitas vezes resultados não esperados inicialmente. Ainda, o sistema tende a se estabilizar após certo período de crescimento. A credibilidade e o valor de uma base instalada são diretamente proporcionais à quantidade de usuários que aderem a ela, tornando a base interessante para investimentos e adição de novos recursos, e assim novos usuários se integram e contribuem para essa expansão, devidos principalmente aos

feedbacks positivos, desse modo também cooperando para o fortalecimento da base (Hanseth e Lyytinen, 2010).

O problema da adaptabilidade e modularidade estão diretamente associadas. Quanto mais o sistema permite a agregação de elementos variáveis, mais adaptável ele será. Portanto, um sistema mutável e modular que apresente conexões fracas entre seus elementos será mais adaptável às demandas de sua base instalada, resultando em um sistema estável (Hanseth e Lyytinen, 2010). Como cita Hanseth e Lyytinen (2010), infraestruturas de informação apresentam-se modularmente, sendo constituídas de componentes fracamente acoplados com funções compartilhadas, decompostos em infraestruturas de aplicação e suporte, objetivando diminuir as dependências mais fortes entre eles.

Para cada um dos princípios de projeto existem regras de projeto a serem seguidas para atender cada um dos problemas citados anteriormente, totalizando um conjunto de 19 regras, como podem ser vistas na Tabela 3 e Tabela 4.

Tabela 3 - Regras de projeto relativas à adaptação

Princípio de Projeto	Regra de Projeto
Criar recursos de TI tão simples quanto possível	RP13. Criar recursos de TI tão simples quanto possível, em termos de sua complexidade técnica e social, reduzindo conexões e custos de governança;
	RP14. Promover sobreposições parciais de funcionalidades de TI, em vez de incorporar todas elas em um só componente;
Modularizar a Infraestrutura de Informação	RP15. Dividir a II recursivamente sempre como infraestruturas de transporte, suporte e aplicação;
	RP16. Utilizar <i>gateways</i> entre versões de padrões;
	RP17. Utilizar <i>gateways</i> entre camadas;
	RP18. Construir <i>gateways</i> entre infraestruturas;
	RP19. Desenvolver estratégias de transição em paralelo com <i>gateways</i> .

Fonte: Adaptado de Hanseth e Lyytinen, 2010

Tabela 4 - Regras de projeto relativas ao *bootstrap*

Princípio de Projeto	Regra de Projeto
Projetar inicialmente para utilidade direta	RP1. Destinar recursos de TI para pequenos grupos; RP2. Criar recursos de TI diretamente úteis sem a base instalada; RP3. Criar recursos de TI simples para usar e implementar; RP4. Projetar recursos de TI um para muitos em contraste a muitos para muitos;
Construir sobre a base instalada	RP5. Projetar os primeiros recursos de TI de forma que não requeira projetar e implementar novas infraestruturas de suporte; RP6. Distribuir sobre infraestruturas de transporte existentes; RP7. Construir <i>gateways</i> para infraestruturas de aplicação e serviço existentes; RP8. Usar <i>Bandwagons</i> associados com outras II;
Expandir a base instalada por táticas persuasivas para ganhar momentum	RP9 Usuários antes de funcionalidades – aumentar a base instalada sempre antes de adicionar funcionalidades; RP10. Melhorar qualquer recurso de TI dentro da II apenas quando necessário; RP11. Construir e alinhar incentivos tal que usuários tenham real motivação para usar recursos de TI da II de novas formas; RP12. Desenvolver comunidades de suporte e estratégias de governança flexíveis para feedback e aprendizado.

Fonte: Adaptado de Hanseth e Lyytinen, 2010

Ainda, existem elementos que facilitam a adaptação de duas ou mais infraestruturas para permitir a associação de suas estruturas modulares, compondo uma infraestrutura maior e favorecendo o crescimento de toda a infraestrutura de informação. Esses elementos são denominados *gateways*. Os *gateways* são elementos fundamentais para associar componentes inicialmente incompatíveis, pois fornecem uma estrutura capaz de integrar unidades heterogêneas (Edwards et al., 2007). Eles constituem um princípio fundamental do desenvolvimento de infraestruturas de informação e são definidos como tecnologias ou padrões capazes

de transpor sistemas para infraestruturas em rede de forma fácil e com pouca restrição (Edwards et al., 2007). Ou seja, são soluções concebidas para contornar possíveis problemas de associação entre entidades heterogêneas. Ainda, *gateways* não devem ser entendidos apenas como um hardware ou um software, mas sim uma combinação de solução técnica e escolha social, podendo não ser a melhor solução. Contudo deve ser genérica ou meta-genérica para ser amplamente adotada entre as comunidades (Edwards et al., 2007). Ademais, *gateways* são a principal resposta aos possíveis reversos salientes. Como exemplo de *gateway*, tem-se o *domain name system* (DNS), que funciona como um elo entre os seguintes elementos heterogêneos: endereços IP e nomes de domínio, que no seu surgimento, permitiu o estabelecimento da *web* sobre a então base instalada da Internet. Podemos citar ainda o padrão DICOM como solução que possibilitou a comunicação entre equipamentos de radiologia de fabricantes distintos (elementos heterogêneos).

2.2. Infraestrutura de informação telerradiológica

Para fornecer os elementos necessários à construção de uma infraestrutura de informação telerradiológica e alcançar a prática radiológica como um espaço global e expansível, aberto e flexível, é preciso compreender primeiramente como foi formada a infraestrutura telerradiológica atual sob a ótica da teoria de projeto para complexidade dinâmica, a fim de identificar características positivas alcançadas durante o processo de formação e consolidação da telerradiologia e destacar as limitações que ainda impedem sua evolução. O objetivo é conhecer os elementos que irão compor um *gateway* capaz de fornecer interoperabilidade entre infraestruturas telerradiológicas distintas. Portanto, a seguir serão abordados os aspectos inerentes à formação da infraestrutura telerradiológica atual, para que seja possível encontrar os elementos necessários ao *gateway*.

2.2.1. Digitalização de imagens e arquitetura PACS/DICOM

Quando a digitalização de imagens radiográficas foi implementada nos procedimentos de diagnóstico na radiologia e a leitura digital foi aceita pela comunidade médica, uma série de vantagens foi alcançada, por exemplo: melhoria da qualidade de diagnóstico a partir do procedimento radiológico, melhoria na

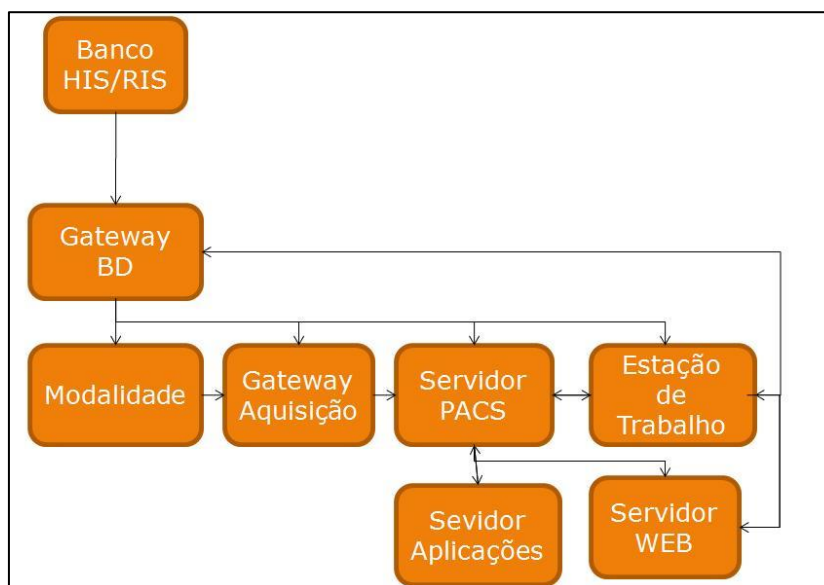
operação do *workflow* na assistência médica, resultando em maior velocidade de diagnóstico e redução de custos de operação (Zapf et al., 2011). A digitalização de imagens fez crescer o mercado e a produção de equipamentos radiológicos para aquisição de imagens médicas, estabelecendo infraestruturas radiológicas nos departamentos de radiologia. Contudo, cada fabricante estava focado em construir esses equipamentos a sua própria maneira, impossibilitando a comunicação e o funcionamento entre equipamentos de fabricantes distintos, forçando, muitas vezes, um departamento de radiologia a adotar apenas equipamentos de um mesmo fabricante, assim limitando a evolução tecnológica da infraestrutura radiológica à velocidade de inovação do fabricante (Pianykh, 2012). Dessa forma, a necessidade de aproveitar as melhores tecnologias existentes no mercado para arquivamento e distribuição de imagens médicas fez com que os grupos de radiologistas e de pesquisa, com apoio da indústria, se voltassem para um mesmo reverso saliente: a falta de padronização no armazenamento e na comunicação para distribuição de imagens médicas entre equipamentos de fabricantes distintos. A busca pela padronização do fluxo de distribuição e arquivamento de imagens médicas resultou no surgimento e evolução de sistemas de gerência para essas imagens, denominados sistemas PACS (*Picture Archiving and Communication Systems*), tendo por base o padrão DICOM (*Digital Imaging and Communications in Medicine*) (Huang, 2010).

Desde a sua conceituação entre meados dos anos 80 e 90, os sistemas PACS possibilitaram a integração de componentes relativos ao imageamento médico para a prática radiológica local, permitindo a formação de infraestruturas que compreendem tecnologias de hardware e software para aquisição, armazenamento e análise de imagens médicas localmente em departamentos de radiologia (Huang, 2010). Essa formação baseou-se no padrão de comunicação e arquivamento de imagens digitais em medicina (DICOM) (Pianykh, 2012), que atua como um *gateway* de comunicação entre os equipamentos de aquisição de imagens e que cobriu os aspectos da medicina contemporânea e, atualmente, desempenha um papel significativo na troca estruturada de imagens médicas e informações clínicas complementares entre equipamentos de fabricantes distintos (Azevedo-Marques e Salomão, 2009). O DICOM fornece definições e diretrizes de implementação para que os equipamentos possam interagir em um mesmo

departamento de radiologia e efetuar troca de imagens e outras informações relativas ao paciente e às modalidades radiológicas (e.g. Tomografia Computadorizada – CT, Ressonância Magnética - MR). O padrão especifica como esses dados devem ser estruturados em arquivos e o resultado da estruturação é dominado Objetos DICOM.

A Figura 1 apresenta a arquitetura do modelo PACS/DICOM, que tem como principais componentes os equipamentos de aquisição de imagem (Modalidades), um *gateway* de aquisição para acesso às imagens, um servidor de arquivamento que gerencia esses dados (Servidor PACS) e várias estações de trabalho (*Workstation* - WS) para manipulação de informações e visualização de imagens. Ainda, sistemas PACS podem ser conectados com Sistemas de Informação Hospitalar (*Hospital Information System* - HIS) e/ou Sistemas de Informação Radiológicos (*Radiology Information System* – RIS) por *gateways* de banco de dados e de comunicação.

Figura 1 - Modelo básico de arquitetura PACS.



Fonte: Adaptado de Huang, 2010.

Figura 2 - Fluxo de trabalho radiológico

Fonte: Próprio autor.

O DICOM tornou-se a espinha dorsal do imageamento moderno, a força motriz por trás de todo o fluxo de trabalho da prática radiológica (Figura 2). Ou seja, a padronização na forma de aquisição, comunicação e armazenamento de imagens médicas favoreceu o estabelecimento de um fluxo de trabalho para a prática radiológica, comumente adotado e definido em sete etapas (Zapf et al, 2011):

Requisição – Etapa em que o médico requisitante solicita um procedimento radiológico para um paciente, que em algum momento tem os seus dados e do procedimento cadastrados em um sistema HIS/RIS; **Agendamento** – São verificados e preparados os recursos existentes para execução do procedimento; **Exame** – Nesse ponto, a modalidade recupera do HIS/RIS as informações necessárias e o procedimento é realizado junto ao paciente; **Processamento** – As imagens geradas pela modalidade são manipuladas por um técnico e encaminhadas para armazenamento no servidor PACS; **Diagnóstico e Demonstração Clínica** – O radiologista utiliza a estação de trabalho para visualização e tratamento das imagens geradas a fim de produzir relatórios de diagnóstico; **Disseminação de Imagem** – Distribuição da imagem e informações complementares (e.g., laudo) para acesso pelo paciente, por outros radiologistas e pelo médico requisitante. Nesse contexto, o DICOM está presente na aquisição, no arquivamento, na transferência e na interpretação de imagens digitais, sendo um

padrão global e, conseqüentemente, tornando o modelo PACS/DICOM uma base instalada amplamente difundida e adotada pelos departamentos de radiologia.

2.2.2. Modelos de infraestrutura telerradiológica

Após a consolidação das infraestruturas PACS/DICOM e do fluxo de trabalho para colaboração entre membros de setores especializados em uma mesma instituição, somada a evolução dos algoritmos de compactação e das redes de comunicação, habilitando a transmissão veloz de grandes massas de dados (Binkhuysen e Ranschaert, 2011), originou-se uma procura crescente por compartilhamento de estudos de imagens médicas entre profissionais de saúde situados em locais geograficamente distantes uns dos outros (Figueiredo e Motta, 2012), cujo resultado foi o aumento da demanda pela telerradiologia. Definida comumente como a transmissão eletrônica de imagens médicas de uma localização geográfica para outra para fins de interpretação e consulta (Binkhuysen e Ranschaert, 2011), a telerradiologia tornou-se a principal solução de interpretação e diagnóstico à distância, principalmente em regiões que sofrem com falta de especialistas. A telerradiologia difere dos modelos de entrega de imagens médicas locais por ser mais rigorosa em relação à confidencialidade das informações que trafegam pela infraestrutura e os protocolos que irão facultar a comunicação entre pontos geograficamente distantes, pois ela trata da transmissão, visualização e diagnóstico de imagens, relacionadas com informações de pacientes, via conexão remota, entre uma organização local e outros centros especializados (HUANG, 2010).

Atualmente, é possível destacar três modelos de serviços telerradiológicos (Thrall, Huang e Pianykh apud Motta, 2014):

- ***Night-hawking/On-call/Off-hour reading***: neste modelo, radiologistas, terceirizados ou não, ficam de plantão ou estão noutra localidade e se beneficiam de fuso horário oposto ao de funcionamento de uma organização, a fim de fazer interpretação dos estudos de imagens. Este modelo é útil principalmente quando há insuficiência de especialistas;

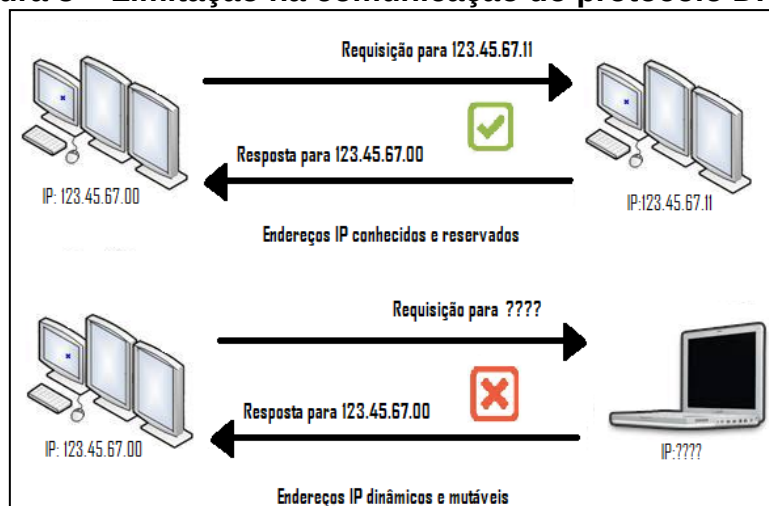
- **PACS regional:** este modelo é o mais frequente entre organizações. Nele um PACS local está conectado, via WAN, a outras organizações ou especialistas, de forma rígida e bem definida, permitindo assim conexões remotas para fins de interpretação e diagnóstico;
- **Outsourcing radiológico:** esse modelo é evidenciado, principalmente, em locais onde não há especialistas, assim, companhias são contratadas para prover serviços de interpretação de imagens, além de fornecer a infraestrutura necessária à telerradiologia.

Contudo, as infraestruturas que suportam esses modelos não possuem as características necessárias para formar uma infraestrutura de informação telerradiológica como um espaço social para práticas radiológicas locais e globais, ou seja, não constituem um espaço social de interações estáticas e dinâmicas onde pessoas, organizações e componentes técnicos estão associados a atividades e estruturas, formando um sistema sociotécnico (Motta, 2014). O desafio de formar essa infraestrutura de informação está associado à dificuldade de compartilhamento de imagens médicas com vários parceiros arbitrários, com o objetivo de colaboração entre especialistas ou organizações de saúde, com esses estudos podendo ser transmitidos para além do domínio onde eles foram originados (Oliveira e Motta, 2016).

O primeiro motivo que dificulta a formação de uma infraestrutura de informação aberta e compartilhada é a baixa flexibilidade presente nas infraestruturas telerradiológicas atuais. Geralmente construídas sobre a base instalada PACS/DICOM, essas infraestruturas herdaram as imperfeições dessa arquitetura e acabam se limitando a atender demandas locais de compartilhamento à distância. Isto é, o padrão DICOM, inicialmente projetado para ser suportado pelo hardware da época, principalmente redes locais, estabelece conexões ponto-a-ponto (P2P) em suas diretrizes de serviço (Pianykh, 2012). Dessa forma, cada hardware utiliza um IP e uma PORTA fixos para comunicação e fluxo de controle para encaminhamento de imagens médicas, funcionando bem em redes locais de alta velocidade. Porém, existe atualmente a possibilidade de hardwares localizados em redes distintas trabalharem com endereços IP dinâmicos e privados, em redes que usam *translation address network* (NAT) e *firewalls*. Então, a ausência de

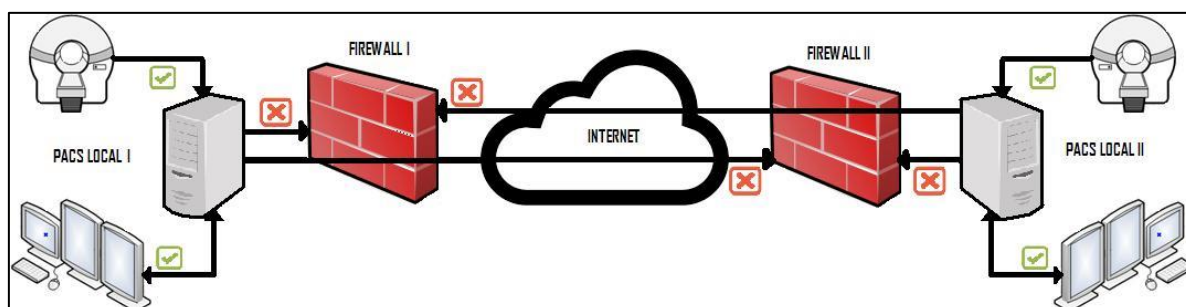
diretrizes de suporte ao redirecionamento de estudos de imagens para outros pontos da rede exerce uma barreira para interoperabilidade entre infraestruturas telerradiológicas, conforme ilustrado na Figura 3 e, de forma mais ampla, na Figura 4. Portanto, muitas soluções, geralmente baseadas em redes privadas virtuais (VPN - *Virtual Private Networks*) e computação na nuvem (*Cloud Computer*) (Monteiro et al., 2016; Silva e Oliveira, 2013; Godinho et al., 2016; Yuan et al., 2015) foram descritas para resolver esse e outros problemas inerentes ao DICOM, contudo pressupõem infraestruturas rígidas, nas quais participantes que pretendam fazer parte dessa infraestrutura estarão sujeitos a alterações significativas em seu ambiente local, criando uma inflexibilidade estrutural e reduzindo a capacidade de escala da infraestrutura.

Figura 3 – Limitação na comunicação do protocolo DICOM



Os dois hardwares acima possuem IP estático e conseguem comunicar-se, ao contrário dos hardwares abaixo, onde o IP dinâmico dificulta a comunicação. Fonte: Próprio autor.

Figura 4 - Interoperabilidade entre PACS limita por firewalls



Fonte: Próprio autor.

O segundo motivo está associado aos registros eletrônicos de saúde (*eletronic health records* - EHR), que oferecem aos profissionais de saúde informações que auxiliam no diagnóstico de seus pacientes. O EHR inclui dados dos pacientes, observações, resultados laboratoriais, prescrições e particularmente imagens médicas. A sua utilização melhora a qualidade de atendimento e cuidados de saúde, como também eficiência e eficácia do sistema de saúde, melhorando a produtividade, como por exemplo, reduzindo o número de testes duplicados. (Noumeir, 2011). O EHR é resultante da integração do sistema PACS com os sistemas hospitalares, sistema de informação de radiologia (*Radiology Information System* – RIS), sistema de informação hospitalar de alto nível (*Heathcare Information System* – HIS), dentre outros, por meio do padrão de dados médicos como o HL7 (*Health Level 7*) (<http://www.hl7.org>) (Zapf et al., 2011). Quando esses sistemas estão dispostos na rede de uma mesma organização ou de organizações parceiras, a troca de informações entre esses sistemas não apresenta grandes dificuldades, pois os registros eletrônicos são comuns, por exemplo, o identificador de um determinado paciente é único para todos os registros. As dificuldades surgem quando os registros de pacientes, incluindo imagens médicas, devem ser compartilhados entre diferentes redes e até mesmo com os próprios pacientes (Langer et al., 2015). Apesar da existência de conjunto de normas para a representação e a transferência de dados clínicos e imagens médicas entre sistemas de saúde, presentes nos padrões HL7 e DICOM, a abertura permitida pelos sistemas HIS/RIS/PACS no cadastro desses dados deixa os registros suscetíveis a duplicidade de identificadores dos pacientes e torna-os geralmente incompatíveis (Pianykh, 2012), complicando o processo de integração para troca de exames entre duas entidades arbitrárias.

Figura 5 - Tensão entre demandas locais e globais para prática radiológica



Fonte: Adaptado de Motta, 2014.

O terceiro motivo é a polarização que dificulta o surgimento de um espaço social como uma II para práticas radiológicas devido à tensão entre o local e o global (Motta, 2014), conforme ilustra a Figura 5. Ou seja, mesmo as infraestruturas telerradiológicas sendo rígidas, com o passar do tempo, há uma tendência natural de crescimento dessa infraestrutura constituída, pois surgem novas necessidades por parte de seus participantes. Dessa maneira, enquanto que alguns participantes preocupam-se com os objetivos e restrições relativos ao negócio de suas organizações ou restrições relativas à legislação vigente que rege o ambiente onde atuam, fazendo voltarem a sua atenção e investimentos para necessidades às práticas locais e modelarem a infraestrutura telerradiológica para satisfazer essas necessidades locais, outros participantes preocupam-se com o compartilhamento de estudos de imagem médica com base no interesse em atendimento ao paciente e buscam atender as mais diversificadas leis sobre compartilhamento de imagens, fazendo voltarem o foco para a busca de soluções de interoperabilidade globais que flexibilizem a formação espontânea e ágil de grupos de especialistas a fim de trocar opiniões sobre estudos. Então, a defesa dos interesses locais em detrimento aos interesses globais e vice-versa dificultam o surgimento de um espaço social como uma II para práticas radiológicas (Oliveira e Motta, 2016).

Portanto, as limitações existentes na base instalada PACS/DICOM em oposição às novas tecnologias de comunicação e transmissão, adicionadas as imperfeições do padrão para registro de pacientes dos sistemas HIS e RIS,

somadas aos conflitos de interesses locais e globais dos participantes envolvidos, faz com que telerradiologia atual não consiga formar uma infraestrutura de informação global e, assim, seja constituída por infraestruturas institucionais regionais para práticas radiológicas. Atualmente, em muitos países, a força motriz para desenvolver infraestruturas de informação telerradiológicas tem visado a uma melhor coordenação dos cuidados médicos (Aanestad et al., 2017) pela integração de infraestruturas regionais a fim de compor infraestruturas nacionais. Isso significa uma mudança de foco de processos internos às instituições para processos de cuidados gerais que ultrapassam às fronteiras institucionais (Aanestad et al., 2017). Assim, é primordial pensar na existência de uma infraestrutura que comporte as mais diversas configurações e propicie compatibilidade, de forma que proporcione a comunicação em larga-escala a qualquer lugar e em qualquer momento.

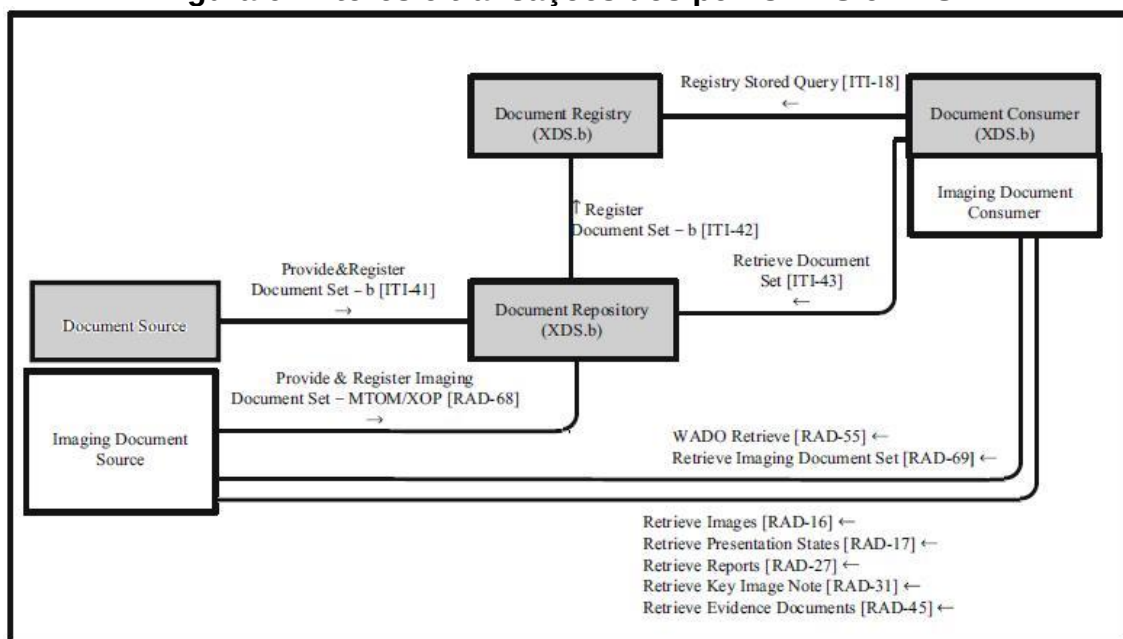
2.2.3. Os perfis IHE

Objetivando fornecer caminhos para elaboração de soluções que contornem as dificuldades e possibilitem o compartilhamento de informações clínicas entre organizações de saúde, a iniciativa *Integrating the Healthcare Enterprises* (IHE), fomentada pela *Radiological Society of North America* (RSNA) (RSNA, 2017), emergiu como o principal grupo de apoio a interoperabilidade transparente entre os muitos sistemas utilizados pelas organizações de saúde (Chatterjee et al., 2017) e elaborou perfis de integração para compartilhamento de EHR. Em outros termos, elaborou um conjunto de especificações, enriquecendo o uso dos padrões existentes (e.g., DICOM, HL7, ISO, IETF), para permitir a partilha de documentos médicos entre organizações de saúde (Noumeir, 2011). Os perfis identificam o conjunto de componentes funcionais da organização de saúde, denominados de atores, e especifica as interações entre esses atores em termos de um conjunto padronizado de transações. O foco dos perfis é garantir que, no tratamento de pacientes, as informações necessárias para decisões médicas estejam corretas e disponíveis para profissionais de saúde, constituindo uma oportunidade de readaptar o fluxo de HIS/RIS/PACS para troca de dados entre instituições (Godinho, 2016).

Foram elaborados quatro perfis para integração entre organizações de saúde. Dois deles, *Cross-Enterprise Document Sharing* (XDS) e *Cross-Enterprise*

Document Sharing for Imaging (XDS-I) (http://wiki.ihe.net/index.php/Cross-enterprise_Document_Sharing_for_Imaging), regulam a publicação, busca e recuperação de registros médicos e imagens médicas entre organizações que pertencem a um mesmo domínio de afinidade (*Affinity Domain*). Como os próprios perfis denominam, são organizações que compartilham do mesmo conjunto de políticas (geralmente através de acordos legais) e infraestrutura para troca de documentos (Langer et al., 2015; Chatterjee et al., 2017). Esses dois perfis oferecem diretrizes para implantar compartilhamento de documentos e de imagens médicas entre essas instituições com objetivo de formarem uma comunidade de compartilhamento de informações clínicas, proporcionando um mecanismo de descoberta centralizado para essas informações clínicas (Ribeiro et al., 2014). Os outros dois perfis, *Cross-Community Access* (XCA) (XCA, 2017) e sua extensão para imagens médicas, *Cross-Community Access for Imaging* (XCA-I) (XCA-I, 2017), suportam os meios para busca e recuperação de documentos e de imagens médicas entre comunidades de compartilhamento. Conforme especificado no próprio perfil, uma comunidade é identificável através de uma ID globalmente exclusiva chamada **homeCommunityId**, requerendo um controle através de uma autoridade central. Não há impedimentos para uma organização pertencente a uma comunidade ser membro de outra comunidade, uma facilidade, visto que é comum centros de imagens atenderem demandas de organizações que não pertencem a um mesmo domínio de afinidade. Tais comunidades podem ser domínios de afinidade XDS que definem a partilha de documentos usando o perfil XDS, ou quaisquer outras comunidades, não importando a sua estrutura de compartilhamento interno.

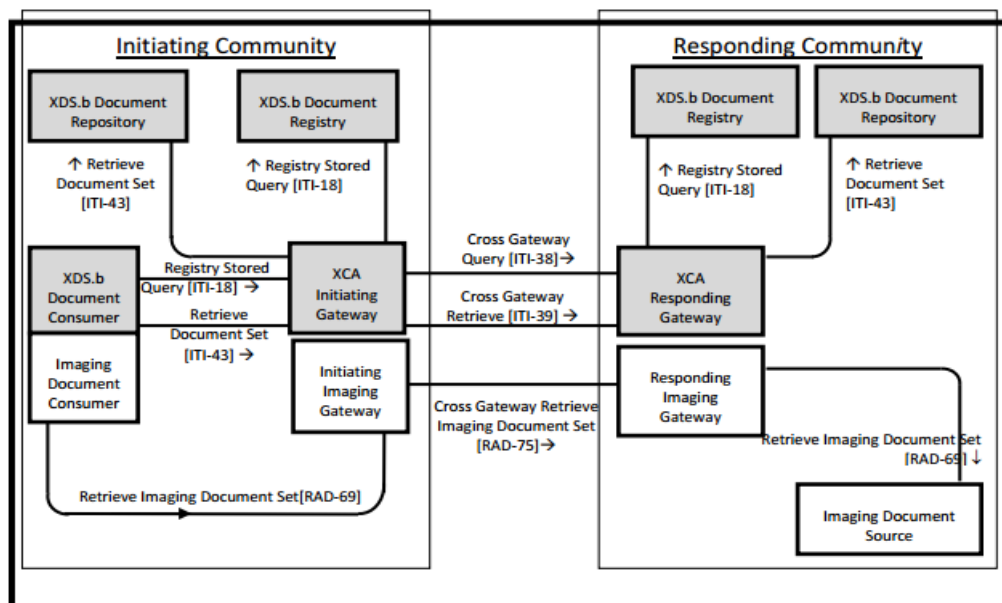
Figura 6 - Atores e transações dos perfis XDS e XDS-I



Fonte: adaptado de XDS-I, 2017.

A Figura 6 ilustra os atores para os perfis XDS e XDS-I. O ator **Document Repository** armazena documentos, podendo haver mais de um repositório no mesmo domínio de afinidade. O ator **Document Register** armazena os metadados necessários para localização desses documentos, só existe um registro no domínio de afinidade e ele é responsável por responder todas as consultas. Ainda, os atores **Document Source** e **Document Consumer**, respectivamente, fornecem e recuperam documentos através dos dois primeiros atores. Além dos atores anteriores, o XDS-I conta com **Imaging Document Source** e **Imaging Document Consumer**. Por fim, ambos os perfis XDS e XDS-I especificam transações para troca de documentos e imagens. É possível observar ainda na Figura 6 as principais transações para registro, busca e recuperação de documentos e imagens. Então, o processo de compartilhamento de dados começa com um **Source** enviando documentos ou imagens para um repositório através de uma transação ITI-41 ou RAD-68. O **Repository** indexa os documentos (ITI-42) no **Registry** que os torna disponíveis para o **Consumer** dentro do domínio de afinidade. Quando um consumidor deseja recuperar um documento ou imagem, ele primeiro executa uma consulta (ITI-18) no registro. Uma vez que tem uma lista de documentos correspondentes, ele executa as recuperações (ITI-43) no repositório. Entretanto, é feita uma operação de recuperação para cada documento (Langer et al., 2015).

Figura 7 - Atores e transações dos perfis XCA e XCA-I



Fonte: IT Infrastructure Technical Framework

A Figura 7 ilustra os atores e as transações definidas para os perfis XCA e XCA-I, que contribuem com dois novos atores, **XCA Initiating Gateway** e **Initiating Imaging Gateway**, ambos localizados a borda da comunidade. As transações especificadas devem ser efetuadas através de chamadas a Web Services e não são especificados requisitos de segurança a serem seguidos. Em vez disso, o perfil disponibiliza uma lista de checagem das principais políticas adotadas em transmissão de EHR. A única recomendação de segurança está relacionada à integridade das mensagens.

Segundo Chatterjee et al. (2017), a conformidade com as recomendações presentes no perfil IHE XDS-I para compartilhamento de imagens entre instituições é, dentre outros, um desafio técnico a ser considerado nas soluções telerradiológicas atuais. Hoje em dia, é possível ver o esforço de grupos de pesquisa espalhados pelo mundo buscando desenvolver suas soluções baseadas nas diretrizes definidas nos perfis IHE (Ribeiro, 2014; Zhang et al., 2016). A própria RSNA foi desafiada pelos centros de pesquisa biomédica dos Estados Unidos da América que compõem o *National Institutes of Health* (NIH) para desenvolver um método de transporte que poderia substituir a necessidade de meios físicos (para pacientes ou outros provedores), substituir VPN's entre os provedores e permitir o

intercâmbio de imagens numa base *ad hoc* entre redes de saúde arbitrárias sem longos atrasos legais (Langer et al., 2015). Dessa forma, o aumento de pesquisas sobre integração de sistemas para compartilhamento de imagens médicas e a conversão de soluções telerradiológicas baseados nos perfis IHE podem ser vistos como um ponto positivo segundo os aspectos definidos pela Teoria de Projetos em relação à construção de infraestruturas de informação.

Entretanto, mesmo que todos adotem os perfis de integração em suas soluções de compartilhamento de imagem, a telerradiologia ainda se encontra distante de conceber uma infraestrutura de informação para a prática radiológica global, devido a limitações presentes nos próprios perfis em relação aos princípios de construção de infraestrutura de informação. Como foi dito anteriormente, os perfis XDS estabelecem diretrizes apenas para transações entre entidades que com mesmo domínio de afinidade, assim instituições externas devem fazer uma reestruturação da sua organização, caso queiram ingressar na comunidade daquele domínio de afinidade. Essa exigência é diretamente contrária ao princípio de projetar sobre a base instalada existente presente na Teoria de Projetos, ou seja, modificar a base instalada aumenta a tensão existente entre os interesses locais da organização e interesses globais do domínio de afinidade. Ainda, os perfis XCA foram criados para comunicação entre comunidades quaisquer, contudo, conforme descrito nos perfis, as diretrizes são definidas apenas para transações entre comunidades que suportam o domínio de afinidade XDS. Então, quando uma comunidade não suporta a opção XDS, deduz-se que estejam sendo usadas localmente interações não especificadas pela IHE para comunicar dados de outra comunidade e a forma como essas interações devem ser conduzidas não está ainda descrita em qualquer perfil IHE. Essa escassez de diretrizes possibilita uma comunidade que não suporta XDS implementar uma solução de interconexão a sua maneira, requerendo posteriormente acordos bilaterais para interoperabilidade. Assim, tornando a infraestrutura limitada em relação à flexibilidade, limitando sua expansão.

2.3. Considerações finais

Tomando como base o que foi apresentado, é possível observar que a telerradiologia, ao longo do tempo, durante sua formação, passou por momentos

em que os envolvidos em seu desenvolvimento tiveram que lutar contra as limitações presentes na infraestrutura existente, principalmente no modelo PACS/DICOM, para que as novas necessidades fossem atendidas. A inércia em manter as estruturas desenvolvidas no formato em que foram concebidas inicialmente, vem dificultando a formação e o crescimento de uma infraestrutura telerradiológica global. Consequentemente, o que se observa é a formação de infraestruturas distintas e dissociadas, cada uma visando atender os interesses locais das partes que desejam compartilhar informações. Dessa forma, cada uma das soluções apresentadas anteriormente, desde as infraestruturas que utilizam puramente o modelo PACS/DICOM até aquelas baseadas em perfis IHE possuem lacunas e dependências que dificultam a conciliação das práticas de trabalho locais e globais a fim de formar um espaço social para telerradiologia como uma infraestrutura de informação.

Portanto, para fornecer uma solução em forma de um *gateway* que permitia essas infraestruturas interoperarem e formarem uma infraestrutura de informação telerradiológica, é necessário conhecer as tecnologias empregadas em cada uma delas, como também identificar os elementos sociais presentes e a influência deles, tudo com o objetivo agregar ao *gateway* os pontos fortes desses elementos e contornar os pontos fracos dessas infraestruturas. Segundo Motta (2014), essa é a forma que se pode fornecer uma solução que verdadeiramente diminui a tensão entre as práticas de trabalho locais e globais, contribuindo para o compartilhamento de imagens e informações de pacientes, como um espaço global e expansível, aberto e flexível, revelando assim a radiologia social como uma infraestrutura de informação.

3. Trabalhos relacionados

Visando contornar as limitações presentes nas infraestruturas telerradiológicas atuais, construídas sobre a base instalada PACS/DICOM, fornecendo uma solução baseada em um *gateway* que favoreça um controle distribuído visando impulsionar e acomodar um crescimento não-linear e heterogêneo dessas infraestruturas para a formação uma infraestrutura de informação telerradiológica, é necessário observar projetos de pesquisa descritos na literatura que promovem a interoperabilidade e o compartilhamento de exames médicos entre organizações de saúde. O que se busca é identificar fatores de sucesso presentes em suas soluções tecnológicas e as limitações que, respectivamente, impulsionam e impedem essas soluções serem adotadas em larga escala para formar uma infraestrutura de informação telerradiológica. Tais fatores positivos, denominados capacidades, orientam na padronização e modularização da solução proposta nesse trabalho e ajudam a manter a flexibilidade e usabilidade em larga escala da II, reorganizando os caminhos de dependência e reduzindo os seus efeitos (Knobel, 2007; Hanseth e Lyytinen, 2010).

Baseado nos argumentos apresentados, esse capítulo tem como objetivos: (subseção 3.1) Elencar as principais características a serem alcançadas pela solução proposta nesse trabalho; (subseções 3.2, 3.3, 3.4 e 3.5) Observar a presença dessas características em outros trabalhos de pesquisa e também as tecnologias empregadas por elas, visando encontrar os pontos positivos e negativos que elas possuem em termos de interoperabilidade para compartilhamento de imagens; (Seção 3.6) Concluir o capítulo com algumas considerações sobre esses pontos.

3.1. Critérios de identificação

Os projetos de pesquisa abordados nesse capítulo foram organizados de maneira a se ter representantes para cada tipo de abordagem: soluções em nuvem, soluções baseadas nos perfis IHE, soluções ponto-a-ponto, soluções baseadas em e-mail. O objetivo é reconhecer as tecnologias e padrões utilizados que possam ser avaliados comparativamente, revelando reais contribuições para a formação de uma infraestrutura de informação para telerradiologia com as seguintes

características: aberta, compartilhada, heterogênea, descentralizada, escalável, segura, assíncrona e assimétrica. Segue uma breve descrição de cada uma das características:

Aberta: Não há fronteiras delimitadoras para que usuários e organizações de saúde integrem a solução proposta. Ou seja, há uma capacidade para incluir um número crescente e não limitado de entidades, sejam elas componentes tecnológicos (e.g., software, dispositivos, padrões), comunidades (e.g., usuários, desenvolvedores), organizações (e.g., empresas), bem como órgãos de governança e padronização (e.g., IETF, W3C, IEEE, ISO) (Hanseth e Lyytinen, 2010).

Compartilhada: A proposta está disponível ao público, seja para fins de validação/comprovação do trabalho ou mesmo, e principalmente, para utilização por terceiros. Em outras palavras, a proposta é vista como um bem comum (Bowker et al., 2010), não pertencendo a uma única empresa ou organização, mas usufruída por múltiplas comunidades de formas variadas e não previstas originalmente (Hanseth e Lyytinen, 2010).

Heterogênea: A proposta é genérica o suficiente para comportar diversas situações de uso e suporte as características divergentes dos usuários e organizações que a utilizem. A heterogeneidade é alcançada através da abertura e do compartilhamento, permitindo a agregação livre de novos elementos sociotécnicos heterogêneos, consequentemente possibilitando a formação de novas conexões com outras infraestruturas.

Descentralizada: Não há a necessidade de elementos centrais para fins de comunicação e/ou transmissão de imagens médicas. De forma mais abrangente, a arquitetura não pressupõe autoridade ou elementos centrais, sendo seu controle e coordenação distribuídos e sua evolução dependente dos caminhos originados das conexões alcançadas através da abertura e compartilhamento.

Escalável: Através da descentralização, é capaz de impulsionar e acomodar o crescimento não-linear e suportar uma grande demanda do sistema sem causar impactos na operação. Ou seja, entende-se aqui a capacidade da solução crescer de forma arbitrária pela inclusão de novos usuários e organizações de saúde ao ambiente, formando um rede livre de escala que tenda a se expandir e aumentar a velocidade do crescimento (Hanseth e Lyytinen, 2010).

Segura: Utiliza padrões ou modelos baseados em padrões de segurança, para melhorar a estabilidade, confiabilidade e manutenibilidade. Ainda, permite que os usuários realizem a **autenticação** para acessar os exames de imagem disponíveis. E mais, possui mecanismos de **autorização** para acesso aos exames de imagem, permitindo que cada organização tenha autonomia para definir as suas próprias permissões de acesso. Por fim, oferece proteção quanto à **confidencialidade e integridade** dos dados de pacientes, em todo o âmbito de transmissão das imagens médicas.

Assíncrona: Essa característica remove a exigência de se manter uma conexão ativa durante a troca de informação, além disso, possui a característica de empurrar a informação para o destino, permitindo que usuários e organizações acessem em momento oportuno as informações disponíveis a qualquer momento, sem necessidade de uma sessão ativa em tempo real.

Assimétrica: Permite que a comunicação e a transmissão efetiva de exames de imagem ocorram em fluxos distintos. Ou seja, por uma via ocorre a transmissão de informações e metadados do estudo e por outra via ocorre a transferência efetiva das imagens. Então, uma vez que cada fluxo pode ser desenvolvido separadamente, diminui a complexidade de implementação. E assim, essa característica oferece ao receptor das informações a opção de decidir o momento da recuperação efetiva da imagem.

E mais, em quais dessas soluções, mesmo que de forma não intencional, podem ser observados os aspectos de construção de infraestruturas de informação: **utilização da base instalada PACS/DICOM, com recursos de TI simples, modulares e de utilidade direta**. No total, dez artigos foram analisados, dos quais três são publicações dos anos de 2007, 2010 e 2012, apesar de ser um período remoto, a relevância de paradigmas em relação à interconexão de redes ainda é notória. Ainda, um artigo de 2013, dois do ano de 2014, um do ano de 2015 e, finalmente, três trabalhos de 2016.

3.2. Soluções em Nuvem (*Cloud Computing*)

Alguns dos trabalhos relacionados apresentam propostas de interoperabilidade entre infraestruturas PACS/DICOM utilizando como base *Cloud Computing*, um paradigma que consiste em entregar computação como serviço ao

invés de produtos físicos. Três tipos de serviços oferecidos por essa tecnologia são identificados: *Software-as-a-Service* (SaaS), *Platform-as-a-Service* (PaaS) e *Infrastructure-as-a-Service* (IaaS) (Monteiro et al., 2016). O fato de que, com *Cloud Computing*, os recursos são providos de forma elástica, suportando escalabilidade horizontal, essa solução busca responder a um problema atual no campo médico: o aumento do volume de dados de saúde em todo o mundo (Viana-Ferreira, 2017). As principais vantagens de seu uso são a possibilidade de acesso aos dados com o mínimo de infraestrutura na empresa contratante do serviço, redução do custo de aquisição de hardware e software, inclusive os custos com pessoal para manutenção desses recursos (Silva e Oliveira, 2013). Atualmente, *Cloud Computing* é um ecossistema com uma gama de serviços complementares, que funcionam bem uns com os outros, providos por outra gama de empresas, configuráveis de acordo com a demanda do cliente. Contudo, não há garantias de que os provedores não aplicam mineração nos dados dos clientes e, portanto, algumas políticas proíbem o uso de repositórios terceirizados ou requerem garantias de preservação privacidade em relação a esses dados. As soluções apresentadas a seguir buscam se beneficiar das vantagens do *Cloud Computing* ao passo que elaboram mecanismos que garantem a integridade, autenticidade e confidencialidade dos dados.

Silva et al. (2013) apresentam um serviço de retransmissão das mensagens de comunicação do protocolo DICOM através da Internet, o *DICOM Relay Service* (DRS). A solução consiste em um agente de comunicação, com funcionalidades de retransmitir as mensagens de armazenamento, busca e recuperação de dispositivos DICOM em uma rede para outros dispositivos DICOM em outra rede. Funcionando como servidor na nuvem, utiliza o protocolo HTTP para estabelecer rotas de comunicação e retransmitir as mensagens. Segundo descrito no trabalho, dessa forma, seus serviços estão disponíveis em qualquer lugar a qualquer momento.

A arquitetura do DRS tem dois elementos chave, o Roteador (*DICOM Router*) que fica a borda da infraestrutura PACS/DICOM e a Ponte (*DICOM Bridge*), localizado no provedor na nuvem. A Ponte autentica, através de um processo sincronizado, os Roteadores, para então iniciar o processo de chaveamento das rotas. Toda comunicação é centralizada na Ponte e uma tabela de rotas é utilizada

no processo. As rotas são traçadas até os elementos presentes na infraestrutura PACS/DICOM (modalidades, servidor PACS, estações de trabalho) com base no mecanismo de endereçamento DICOM (*Application Entity Titles*). Isso requer nova configuração dos elementos presentes na infraestrutura, para redirecionarem suas mensagens para o roteador.

A troca de imagens médicas entre dois domínios é feita em duas etapas: primeiro a origem armazena os exames no provedor na nuvem e, em um segundo momento, o destino recupera essas imagens. As mensagens DICOM utilizadas na troca das imagens são estruturadas em XML e cifradas com chaves criptografadas. Um *middleware* foi desenvolvido para prover capacidade de troca de mensagens DICOM sem depender do tipo de provedor de nuvem, ou seja, a Ponte independe da arquitetura do provedor da nuvem.

O trabalho foi comparado com outras soluções baseadas em redes privadas virtuais (Virtual Private Network – VPN) e se mostrou satisfatório, contudo, segundo os próprios autores, a solução só vislumbrou um cenário de uso, a solução é específica para o cenário de neuroimagem, não podendo ser generalizada para outros cenários.

Analisando o trabalho sob a ótica de construção de infraestruturas de informação, observa-se que a utilização do protocolo HTTP para transmissão e XML como ferramenta de padronização das informações facilita a aceitação da proposta como solução de interoperabilidade, pois são tecnologias bastante difundidas e utilizadas e que proporcionam definições para segurança das informações trafegadas, possibilitando ultrapassar os limites de uma infraestrutura telerradiológica. Entretanto, o elemento central para armazenamento de informações limita a capacidade de ser escalável, o aumento do volume de informações trafegadas no elemento central diminui o desempenho do tempo de resposta, só isso é suficiente para não se adotar essa solução como base para formação de uma infraestrutura de informação telerradiológica.

Godinho et al. (2016), em sua solução, toma como base o DICOM Relay Service e, dessa forma, adquire suas características e limitações. Contudo, propõe resolver a latência presente na transmissão de imagens médicas entre instituições de saúde com a adição de um mecanismo de *cache* ao mecanismo de rotas do DRS. O mecanismo de *cache* fragmenta imagens em formato DICOM e mantém os

blocos (*chunks*) de imagem espalhados ao longo das rotas. Assim, a solução consegue contornar a limitação da escalabilidade e se torna capaz de atender uma infraestrutura PACS/DICOM mais abrangente, ou seja, torna-se capaz de formar uma infraestrutura PACS/DICOM regional. Entretanto, estabelecer essa proposta como solução de cultivo para prática radiológica global enfrenta algumas questões. A primeira questão, que está associada à adoção do DICOM Relay Service como base, é o sincronismo necessário entre as rotas, todos os pontos entre origem e destino devem estar ativos durante a transmissão, a retirada de um nó pode comprometer toda uma transmissão, tornando a infraestrutura mais rígida, dificultando a livre associação e dissociação, característica presente em infraestruturas de informação. Outro ponto está relacionado à complexidade da solução. O controle, a localização e a recuperação dos blocos de objetos DICOM requer a elaboração e utilização de algoritmos mais robustos, ou seja, a implementação dessa solução em uma infraestrutura requer conhecimento aprofundado sobre particionamento e distribuição de informação. Consequentemente, a adoção de recursos de TI mais simples pode diminuir a prioridade de utilização dessa solução.

Por outro lado, Monteiro et al. (2016) apresentam o termo *Teleradiology-as-a-Service* (TaaS) e propõem uma solução de serviços de telerradiologia em tempo real de forma assíncrona, mantida em nuvem, para a comunidade radiológica. A arquitetura da proposta é constituída de três elementos, um *gateway* presente na infraestrutura PACS/DICOM, uma plataforma colaborativa mantida na nuvem, e uma aplicação web para os clientes. A plataforma permite os usuários (e.g., médicos, radiologistas, pesquisadores de saúde) se autenticarem nela e se comunicarem com outros usuários através dela. Ainda, a plataforma armazena as imagens médicas dos usuários em formato DICOM. A comunicação entre todos os elementos é feita através de um protocolo com base em XMPP (*Extensible Messaging and Presence Protocol*), desenvolvido pelos próprios proponentes. Ademais, o *gateway* dá acesso ao servidor de arquivos na infraestrutura PACS/DICOM e apenas usuários presentes na lista de permitidos podem acessar o servidor. Um mecanismo de criptografia e controle de acesso ao servidor de arquivos garante segurança dos dados envolvidos das informações mantidas na nuvem, como também na transmissão de informação.

Yuan et al. (2015) também tem foco em fornecer serviços para usuários e a solução proposta possibilita utilizar os serviços especificados no protocolo DICOM (e.g., C-FIND, C-MOVE, C-GET) entre um grupo de hospitais em diferentes domínios (i.e., organizações de saúde com infraestrutura PACS/DICOM distintas) com garantia de custo efetivo e segurança de informação. A arquitetura elaborada assemelha-se à apresentada por Monteiro et al. (2016) e possui três elementos: um repositório para imagens, um indexador para busca dos exames situados na nuvem e um *webclient* na máquina do cliente, que possibilita acesso dos usuários para gerenciamento dos conteúdos armazenados.

Viana-Ferreira (2017) et al. Apresentam uma solução para interconexão entre infraestruturas PACS, objetivando formar uma única infraestrutura PACS regional. Para isso utilizam um repositório mantido a borda de uma das infraestruturas PACS. O foco principal dessa proposta é maximizar o desempenho do acesso aos estudos de imagens através de mecanismos de cache e predição. A arquitetura do repositório utiliza três componentes denominados pelos autores de sensores (*sensors*). O sensor de Mensagem (*Message sensor*) é responsável por atender as requisições, em formato DICOM, emitidas pelas infraestruturas PACS. O sensor de Estudo (*Study sensor*) é responsável por manter em cache informações de estudos médicos. Por fim, o sensor de rede (*Network sensor*) é responsável por monitorar as condições de rede e manter as predições para garantir desempenho.

As soluções apresentadas por Monteiro et al. (2016), Yuan et al. (2015) e Viana-Ferreira (2017) usam um *gateway*, mantido à borda da infraestrutura PACS/DICOM, que possibilita a comunicação e o acesso a informações de exames de imagem médicas. Esse *gateway* dota à infraestrutura de capacidade de abertura de acesso para o meio externo, ou seja, gera a possibilidade dessa infraestrutura associar-se a outras infraestruturas. Ainda, o gateway da solução de Monteiro et al. (2016) usa um protocolo de comunicação de mensagens que tem como base o protocolo XMPP. De forma semelhante, o gateway da solução de Viana-Ferreira (2017) faz uso do protocolo DICOM para a comunicação e utiliza de XML para estruturar o armazenamento das mensagens trocadas durante a comunicação. Em ambas soluções, essa abordagem possibilita que outras infraestruturas implementem sua comunicação baseada nesses protocolos, de modo a se adaptar

e associar a infraestrutura em Cloud. Contudo, essas três as soluções impõem um controle de liberação de acesso centralizado, o que dificulta a associação espontânea entre duas infraestruturas quaisquer e o crescimento arbitrário da infraestrutura como um todo.

3.3. Soluções com perfis de Integração IHE

Como observado na seção 2.2.3 do capítulo 2, os perfis de integração IHE oferecem diretrizes baseadas em padrões conhecidos pelas organizações de saúde (e.g., HL7, DICOM) para implantar para compartilhamento de registros de saúde, fornecendo um mecanismo de descoberta centralizado para esses registros (Ribeiro, 2014). Os trabalhos aqui abordados adotam os perfis de integração XDS e XDS-I para compartilhamento de registros eletrônicos de saúde (*Electronic Health Record* - EHR) e de imagens médicas, respectivamente. Contudo, cada um dos trabalhos utiliza um conjunto distinto de tecnologias e conceitos na implementação de suas soluções.

Assim como as propostas apresentadas na seção anterior, Ribeiro et al. (2014) seguem o paradigma de computação em nuvem para atender as orientações do Perfil XDS-I e apresenta o XDS *Proxy*, para compartilhamento de imagens DICOM entre infraestruturas PACS/DICOM. O XDS *Proxy* segue a mesma estrutura arquitetural dos trabalhos de Yuan et al. (2015) e Monteiro et al. (2016), porém sem o *webclient*, e implementa o ator **Repository** e o **Registry** em um provedor na nuvem, assegurando preservação de privacidade e confidencialidade dos dados através de um mecanismo de encriptação de busca elaborado pelos proponentes, com base em um esquema de encriptação probabilística, no qual duas encriptações do mesmo objeto são diferentes. O segundo elemento é um *proxy* localizado à borda da infraestrutura PACS/DICOM. Atuando como um *broker*, ele criptografa os dados enviados para o repositório na nuvem e executa o inverso também. A transmissão das informações utiliza protocolo de segurança SSL/TLS (*Transport Layer Security*) com certificados X.509 e isso é um ponto positivo que se pode destacar na implementação da solução. SSL/TLS é um protocolo relativamente fácil de ser implantado em um ambiente, pois, por usado em vários tipos de aplicações, diversas linguagens de programação possuem bibliotecas para seu uso (Polk et al., 2014).

O trabalho de Ribeiro et al. (2014), com foco na segurança dos dados clínicos, apresenta uma solução robusta baseada em criptografia, visando garantir uma elevada segurança das informações mantidas fora do domínio da infraestrutura PACS/DICOM. Entretanto, dados criptografados tendem a ficar maiores que os dados originais e concentrar o armazenamento desses dados em um ponto central pode comprometer a performance da infraestrutura à medida que essa infraestrutura agrega novas organizações de saúde, limitando seu crescimento.

Por outra via, Zhang et al. (2016) propõem uma solução orientada pelos preceitos contidos no perfil de XDS.b (a versão mais recente do perfil XDS), projetado e desenvolvido com Arquitetura Orientada a Serviço (*Service-Oriented Architecture* – SOA) e Arquitetura Orientada a Eventos (*Event-Driven Architecture* – EDA). Ainda, utilizando o conceito de Grades Computacionais (*Grids*), que tem como objetivo principal atender serviços como processamento e armazenamento de dados em larga escala, nesse caso, as organizações de saúde são agrupadas para atender serviços de acordo com as modalidades existentes, por exemplo, armazenamento de grandes volumes de imagens médicas. Ademais, o paradigma de *Grids* foi explorado para fornecer acesso aos repositórios de imagens distribuídas, formando uma rede federada.

A arquitetura possui dois elementos principais funcionando como atores **Registry**, um localmente em cada infraestrutura PACS/DICOM, denominado de *Edge Appliance* e outro central, denominado *Grid Manager*, posicionado em uma infraestrutura PACS/DICOM de maior porte. Ainda, a arquitetura utiliza transferência de dados em *stream* e tecnologias de apresentação progressiva para sobrepor a latência da rede, embora não tenham sido especificados detalhes de segurança utilizados na comunicação. E mais, a arquitetura da proposta visa atender não só entidades com infraestrutura PACS/DICOM, como também aquelas entidades com apenas modalidades de imagem digital, ou seja, aquelas que não possuem uma infraestrutura PACS/DICOM implementada. Por fim, a solução foi instalada em mais de 100 hospitais em três distritos de Xangai.

A solução apresentada por Zhang et al. (2016) possui características que fazem aproximar mais essa infraestrutura de uma infraestrutura de informação para telerradiologia, pois a solução em grid torna cada infraestrutura PACS/DICOM um

repositório de informações independente. Outro ponto positivo é que para usar o *gateway Edge Appliance*, as infraestruturas não necessariamente devem seguir o modelo PACS/DICOM, ou seja, o *gateway* foi construído para suportar a heterogeneidade das infraestruturas. Contudo, a solução possui algumas limitações. A escassez de detalhes sobre as garantias de segurança das informações é um ponto negativo que pode dificultar sua adoção e implantação. Ainda, o uso de um gerenciador central como registro para controle dos repositórios limita a associação entre entidades que fazem parte da federação e outras que não fazem parte, ou seja, limita a livre associação entre entidades arbitrárias. Por fim, todo acesso e comunicação entre as infraestruturas e os usuários ocorre através do *Grid Manager*, comprometendo a performance, que seria melhor aproveitada se houvesse um mecanismo que estabelecesse a conexão ponto-a-ponto entre o usuário e a entidade.

3.4. Soluções Ponto-a-Ponto (P2P)

Soluções Ponto-a-Ponto têm algumas vantagens que fazem dessa tecnologia uma ferramenta poderosa. Por exemplo, o conteúdo e os recursos podem ser compartilhados tanto do centro como da borda em uma rede P2P. Ao contrário da rede cliente/servidor, na qual o conteúdo e os recursos geralmente são compartilhados apenas do centro (Guo et al., 2011). Outra vantagem é que esse tipo de rede é facilmente dimensionado e mais confiável do que um único servidor. Um único servidor está sujeito a um único ponto de falha ou pode ser um gargalo em tempos de alta utilização da rede (Guo et al., 2011). Ainda, uma rede de pares pode compartilhar seu processador, consolidando recursos de computação para tarefas de computação distribuída, em vez de confiar em um único computador, como um supercomputador (Guo et al., 2011). Ademais, uma rede P2P dá autonomia significativa ao nó (*peer*) nas extremidades da rede. Dessa forma, os recursos compartilhados podem ser acessados diretamente. Em vez de compartilhar um arquivo armazenado em um servidor central, um nó pode compartilhar o arquivo diretamente (Guo et al., 2011).

É apoiado sobre esse paradigma que Urovi et al. (2014) apresentam uma solução que propõe a troca de registros eletrônicos de saúde seguindo as diretrizes do perfil XDS da IHE. A proposta, intitulada de *Semantic Health Coordination*

(SemHealthCoord), utiliza o conceito de comunidade em rede P2P para representar as organizações de saúde. A comunicação entre as comunidades é feita através de agentes autônomos, coordenados por um conjunto de regras para busca e acesso a registros de saúde. A tecnologia baseada em agentes é conhecida por adicionar algumas vantagens para a interoperabilidade das infraestruturas PACS/DICOM, como alta adaptabilidade na frente de mudanças, gerenciamento distribuído de fontes e acesso remoto aos dados de imagens (Urovi et al., 2014). A segurança na comunicação é mantida com chaves criptográficas e certificados digitais, controlados por uma autoridade certificadora central. Para verificação da autenticidade e integridade de informações de uma comunidade, um protocolo de interação foi desenvolvido pelos proponentes, após efetuar a autenticação junto à autoridade central, a comunidade ingressante pode comunicar-se na rede P2P.

A solução de Urovi et al. (2014) emprega a utilização de uma entidade certificadora central. A entidade certificadora registra a infraestrutura que pretende se associar a rede P2P e emite o certificado contendo o par de chaves pública e privada para a infraestrutura. Uma vez de posse do certificado e as chaves, a infraestrutura pode enviar mensagens para um espaço compartilhado, denominado *Policy Tuple Centre*. As mensagens nesse espaço contêm as informações sobre as imagens médicas a compartilhar e essas informações são criptografadas com a chave privada da infraestrutura detentora da imagem. Outra infraestrutura que quiser ter acesso a essa imagem, adquire a chave pública da infraestrutura detentora da imagem com a entidade certificadora, lê a mensagem criptografada e utiliza as informações para conectar diretamente com a infraestrutura detentora da imagem.

É possível observar que o trabalho apresentado por Urovi et al. (2014) facilita a associação de entidades a rede através da entidade certificadora. Ainda, o espaço compartilhado de mensagem dota a solução de assincronismo, uma vez que não existe a necessidade de duas entidades estarem ativas para troca de mensagens, que são mantidas no espaço compartilhado e as entidades acessam em momento oportuno. Outro ponto positivo é que as imagens são mantidas na origem e a comunicação é direta com a origem e, assim, há uma diminuição da latência da rede. Contudo, a entidade central e o espaço compartilhado de mensagens tornam-

se os pontos centrais da rede, uma falha nesses nós pode ocasionar a falha de comunicação da rede como um todo.

De forma semelhante a solução de Urovi et al. (2014), o SocialRAD, proposto por Figueiredo e Motta (2013), aborda a transmissão para além do domínio PACS, combinando dois conceitos P2P e *Cloud Computing*. Através de construção de uma infraestrutura distribuída, a arquitetura conta com três elementos principais. Um servidor (*Web Service Local*) presente na infraestrutura PACS/DICOM que executa o monitoramento e atendimento de requisições de busca por exames de imagem. O segundo elemento, um servidor na nuvem (*Web Service Cloud*) para armazenamento de metadados dos exames, que efetua controle de autenticação dos usuários do sistema e que se comunica com *Web Service Local* e o *webclient*. Por fim, o terceiro elemento, o *webclient*, presente na máquina do usuário, que possibilita consultar os metadados no *Web Service Cloud*, e gerencia a aquisição dos exames no *Web Service Local*. O *Web Service Cloud* agencia o processo comunicação entre o cliente e a infraestrutura PACS/DICOM, estabelecendo uma conexão ponto-a-ponto entre o *Web Service Local* e o *webclient*.

De forma análoga a solução de Urovi et al. (2014), a segurança da comunicação entre os elementos da solução de Figueiredo e Motta (2012) é feita utilizando certificados digitais. Um novo aspecto de segurança que essa solução aborda está associada a manutenção dos exames na máquina do cliente, para evitar que os exames sejam acessados de forma indevida, a solução utiliza unidade de disco virtual protegida por criptografia. É possível notar que pontos positivos alcançados com a solução de Urovi et al. (2014) estão presentes na solução de Figueiredo e Motta (2013), como também os pontos negativos em relação a troca de mensagens de comunicação sobre a existência de novos estudos. Manter essas mensagens em um repositório central é dotar a solução de um ponto de falha que pode interromper toda a comunicação.

3.5. Soluções com e-mail

Alguns trabalhos buscam beneficiar-se da natureza essencialmente assíncrona e descentralizada da infraestrutura de e-mail, que possui elevada conectividade, para trocar mensagens. Ainda, servidores de e-mail são confiáveis em termo de acesso, e-mails podem ser enviados através de *firewalls* sem a

necessidade de mudanças em suas políticas e possuem protocolos de criptografia para troca de dados. Por fim, existem contas de e-mail gratuitas confiáveis e que oferecem uma capacidade de armazenamento aceitável (por exemplo, Gmail), podendo ser dispensada a necessidade de preparação de um servidor próprio.

Ribeiro et al. (2010) propõem uma estrutura P2P sobre o *Internet Message Access Protocol* (IMAP), possibilitando a busca, troca e armazenamento de imagens médicas sobre um largo domínio composto de várias instituições de saúde. A arquitetura é composta pela plataforma Dicoogle (Costa et al., 2009), colocada sobre a borda de cada infraestrutura PACS/DICOM, que provê indexação e recuperação de arquivos DICOM entre instituições de saúde. Utiliza tecnologia JXTA, composta por uma série de protocolos de comunicação P2P e projetada para resolver problemas na área de computação distribuída (JXTA, 2017). Ainda, a arquitetura possui um servidor de e-mail central que funciona como um *relay peer*. Ademais, o mecanismo de comunicação funciona, semelhante ao apresentado em Figueiredo e Motta (2013), da seguinte forma: uma plataforma Dicoogle comunica-se com o *relay peer* e solicita conexão com outra plataforma Dicoogle, então o *relay peer* estabelece uma conexão ponto-a-ponto entre as plataformas. A solução de Ribeiro et al. (2010) diminui a limitação existente na comunicação apresentada nas soluções P2P anteriores através da utilização de um servidor de e-mail específico como repositório de mensagens, pois servidores de e-mail são mais tolerantes a falha, contudo ainda existe a necessidade da comunicação ser inicialmente estabelecida por um elemento central antes das conexões P2P serem formadas.

Sob outra perspectiva, o DICOM e-mail é um protocolo padronizado para troca de exames de imagens de médicas através de uma conexão segura entre dois parceiros que não precisam ser conhecidos *a priori* (*ad hoc teleradiology connection*) (Weisser et al., 2006). Especificado pelo *IT Working Group* (@GIT) da Sociedade Alemã de Radiologia (DRG), utiliza as especificações do protocolo de transmissão de mensagens (SMTP) e de anexo de objetos DICOM em e-mails (Supplement 54: DICOM MIME-Type) e garante a segurança das informações trafegadas aplicando criptografia PGP (*Pretty Good Privacy*) (www.pgpi.org) (Engelmann et al., 2005). O DICOM e-mail é um exemplo de infraestrutura construída sobre uma base instalada (Oliveira e Motta, 2016), não proprietária, que pode ser integrada a uma organização de saúde sem alterar significativamente o

workflow, arquitetura de *firewalls* e políticas locais de segurança (Weisser et al., 2006). Contudo, o recebimento compulsório de grandes volumes de dados de imagem como anexos de e-mail requer mecanismos de fragmentação e desfragmentação de imagens para empacotamento em diversas mensagens e mecanismos para garantir entrega e ordenação de mensagens, fato que torna a solução mais complexa.

Weisser et al. (2007) apresentam diferentes aplicações de telerradiologia com o DICOM e-mail, por exemplo, emissão de laudos e consultas de emergência ou a peritos. Através da sua simplicidade funcional, focada na transmissão assíncrona de imagens, foi possível integrá-lo com outras infraestruturas de serviços, de variadas formas, para compor aplicações de telerradiologia no *workflow* de mais de 240 instituições na Alemanha, tanto na região do Rhein-Neckar quanto no Vale do Ruhr. Como exemplo, no ano de 2013, o Hospital da Universidade de Mannheim recebeu mais de 6.000 exames de imagens e transmitiu cerca de 3.700 exames para 36 parceiros na rede, com um fluxo de envio/recepção de mais de 2.500.000 imagens (Oliveira e Motta, 2016).

3.6. Considerações finais

As soluções dos trabalhos apresentados nesse capítulo promovem interoperabilidade entre infraestruturas PACS/DICOM através de soluções que envolvem três principais conceitos: tradutores (*brokers*), repositórios centralizados e canais de comunicação bilaterais. Essas soluções apresentam algumas características que são necessárias para a formação de uma infraestrutura de informação global para prática radiológica. Dessa forma, algumas das tecnologias utilizadas para alcançar essas características serão empregadas em nossa proposta. Contudo, essas mesmas soluções também possuem outras características que não estão em conformidade com os princípios e regras de criação apresentados pela teoria de projetos e devem ser evitadas.

Primeiro, além de demandarem mudanças nos elementos tecnológicos das infraestruturas já existentes, requerem também mudanças nos processos de trabalho, limitam o uso apenas para aquelas envolvidas na fase inicial de projeto e exigem novas adaptações quando uma nova infraestrutura ou um novo fluxo de trabalho são acrescentados, tornando a infraestrutura geral mais homogênea. Tal

característica é mais visível quando as soluções dotam os elementos centrais de maior poder de controle, como é o caso das soluções baseadas em nuvem. Por outro lado, foi possível observar que as soluções mais descentralizadas possuem maior capacidade de assincronismo, pois as mensagens são trocadas entre as partes interessadas sem necessidade de conexões ativas, não requerendo autoridade central para intermediação.

Ainda, aquelas soluções baseadas repositórios centrais, em via oposta às vantagens de permitir acesso a dados e serviços em um único ponto, trazem riscos da dependência de um único provedor e requerem a elaboração de linguagens ou protocolos de comunicação próprios, elaborados para atender requisitos especiais necessários, tais como manter a privacidade, a segurança, e acordos públicos, especialmente ao lidar com ambientes públicos de compartilhamento de imagem, mesmo aquelas baseadas nos perfis de integração IHE. Entretanto, é possível perceber naquelas soluções que elaboram seus protocolos com base em tecnologias e outros protocolos bem difundidos uma certa facilidade de implementação, tornando-se um atrativo para os interessados que desejam se associar a infraestrutura.

Ademais, mesmo as soluções possuindo elementos capazes de diminuir as fronteiras que delimitam a integração de novos usuários e organizações, os trabalhos propõem soluções proprietárias, limitando a livre utilização e, conseqüentemente, limitando o compartilhamento e crescimento da infraestrutura.

Todavia, dentre as propostas, o DICOM e-mail é uma solução que prescinde de autoridade ou elementos centrais e que especifica um padrão aberto de comunicação para troca de mensagens, baseado na infraestrutura de e-mail disponível na Internet. Assim, o DICOM e-mail é um exemplo de infraestrutura para telerradiologia construída sobre uma base instalada, que pode favorecer o surgimento de uma infraestrutura de informação para telerradiologia, compartilhada, aberta, heterogênea e evolutiva (Oliveira e Motta, 2014). Embora bem-sucedido, o DICOM e-mail tem como desvantagem o recebimento compulsório de grandes volumes de dados de imagem como anexos de e-mail. Além disso, as especificações do mecanismo de controle para particionamento e reconstrução das imagens são complexas para implementar.

Ainda, mesmo sendo a solução mais antiga, o DICOM e-mail é a que mais se aproxima do conceito de *gateway* para formação de uma infraestrutura de informação. Dessa forma, o trabalho aqui proposto adotará os conceitos abordados pela solução apresentada no DICOM e-mail, buscando contornar suas limitações através da utilização das tecnologias empregadas nas demais soluções que, positivamente, favorecem a formação de uma infraestrutura de informação telerradiológica.

A seguir, apresentamos resumidamente a confrontação dos pontos positivos e negativos extraídos dos trabalhos abordados anteriormente. A Tabela 5 lista as propriedades necessárias em uma infraestrutura de informação, buscadas nos trabalhos abordados, com base nos critérios estabelecidos na seção 3.1. Os trabalhos estão agrupados por tipos de solução. Cada coluna indica se as propriedades são atendidas pela solução proposta, se não são atendidas ou se são atendidas parcialmente.

Tabela 5 - Comparação entre os trabalhos relacionados

Propriedades	Cloud Computer					IHE		P2P		E-mail	
	Silva et al. (2013)	Godinho et al. (2016)	Monteiro et al. (2016)	Yuan et al. (2015)	Viana-Ferreira et al. (2017)	Ribeiro et al. (2014)	Zhang et al. (2016)	Urovi et al. (2014)	Figueiredo e Motta (2012)	Ribeiro et al. (2010)	Weisser et al. (2007)
Aberta	-	-	-	-	-	-	+	+	+	+	√
Compartilhada	-	-	-	-	-	-	+	+	-	+	√
Heterogênea	-	-	-	-	-	-	-	+	+	+	√
Descentralizada	-	-	-	-	-	-	+	+	+	+	√
Escalável	-	+	+	+	+	-	√	√	√	√	√
Segura	√	√	√	+	-	√	-	√	√	-	√
Assíncrona	-	-	+	+	+	+	+	√	√	√	√
Assimétrica	-	-	-	-	-	-	-	+	+	+	-
Base Instalada	√	√	√	√	√	√	√	√	√	√	√
Recursos Simples de TI	√	+	-	-	-	+	-	-	-	√	+
Utilidade direta	√	√	√	√	√	√	√	√	√	√	√
Modular	+	+	√	√	√	√	√	√	√	√	-

Legenda: (√) atende completamente a propriedade. (+) atende parcialmente a propriedade. (-) não atende a propriedade. **Fonte:** Próprio autor.

4. DicomFlow

Este capítulo traz os detalhes da proposta que visa atender o objetivo de contribuir para a melhora na distribuição de imagens médicas entre infraestruturas de saúde heterogêneas pertencentes a domínios distintos. Intitulado DicomFlow, a solução proposta é um *gateway* assíncrono, assimétrico e descentralizado, que oferece flexibilidade à infraestrutura PACS/DICOM e possibilita a formação de uma infraestrutura de informação global para a distribuição de imagens médicas. Construído segundo os conceitos da teoria de projetos para a complexidade dinâmica (Hanseth e Lyytinen, 2010), o DicomFlow utiliza a ideia de comunicação empregada pelo DICOM e-mail, contornando as limitações da infraestrutura PACS/DICOM e do próprio DICOM e-mail através da utilização de tecnologias amplamente difundidas, não proprietárias, observadas nos demais trabalhos relacionados. Inicialmente, na subseção 4.1, é apresentada a metodologia adotada para a construção do *gateway*. Subsequentemente, na seção 4.2, apresenta-se como as características do *gateway* foram abordadas na elaboração de um protocolo que especifica as diretrizes para construção do próprio *gateway*. Em seguida, a seção 4.3 ilustra os cenários de uso baseados nos modelos telerradiológicos atuais e utilizados para especificar as diretrizes do protocolo e para codificação do *gateway*, vale observar que o uso do *gateway* não se limita apenas a esses cenários. Por fim, a arquitetura empregada na implementação do *gateway* é vista com mais profundidade na seção 4.4.

4.1. Metodologia

A execução do objetivo deste trabalho envolveu o emprego de duas metodologias de pesquisa: 1 – Leitura dos principais artigos referentes à área de infraestruturas de informação, mais especificamente artigos que identifiquem as características de II e seu processo de formação. Ainda, leitura de artigos mais recentes na área de telerradiologia, mais especificamente sobre distribuição de imagens médicas e interoperabilidade entre sistemas PACS/DICOM. 2 – Aplicação da metodologia de Construção (*Build*) (Amaral, 2011) observando os princípios e regras definidos na teoria de projetos para a complexidade dinâmica (Hanseth e Lyytinen, 2010), durante a implementação do *gateway* assíncrono, assimétrico e

descentralizado para formação de uma infraestrutura de informação telerradiológica.

A leitura dos artigos que identificam as principais características técnicas e sociais das infraestruturas de informação, além de aprofundar o conhecimento sobre essa nova classe de soluções de TI, auxiliou na definição dos macros requisitos necessários ao DicomFlow. Através dessa literatura, foi possível identificar, no requisito de comunicação assíncrona, a possibilidade de fornecer às infraestruturas radiológicas a capacidade de livre associação e dissociação. Ainda, identificou-se que a assimetria entre comunicação e transmissão efetiva das imagens médicas, facilita a implementação modular da solução. E mais, uma solução descentralizada torna a adoção do *gateway* dependente apenas da infraestrutura que a escolhe, sem interferir nas demais infraestruturas, facilitando a agregação de novas infraestruturas à infraestrutura de informação global, favorecendo, portanto, seu crescimento.

Continuando a leitura, os artigos que propõem soluções em interoperabilidade para distribuição de imagens médicas facilitaram na identificação de tecnologias que podem ser empregadas para atender aos macros requisitos definidos para o *gateway* e aspectos sociais que devem ser considerados em relação à segurança das informações comunicadas. Além do mais, foi possível identificar tecnologias abertas (*open source*) e difundidas (amplamente adotadas) que facilitam a implementação e configuração do *gateway* nas infraestruturas. Por fim, foi possível identificar as estratégias de como aplicar essas tecnologias na solução proposta, a fim de reduzir as alterações nas infraestruturas radiológicas já existentes. Por exemplo, identificou-se nas soluções as tecnologias que atuam como observadores e que se mantêm à borda da infraestrutura, possibilitando o *gateway* funcionar como uma nova camada na infraestrutura. Por fim, através da identificação dos modelos telerradiológicos atuais presentes na literatura, foram elaborados os cenários que guiaram a construção do DicomFlow durante o processo de sua construção.

O desenvolvimento do DicomFlow, orientado pelos conceitos da teoria de projetos para complexidade dinâmica, iniciou-se com a elaboração de um protocolo de comunicação para distribuição de imagens médicas entre infraestruturas radiológicas heterogêneas pertencentes a domínios de redes distintos. Os cenários

identificados orientaram na elaboração dos tipos de mensagens trocadas entre essas entidades e que serviços são demandados e atendidos por essas entidades. E mais, a diversidade de cenários possibilitou a elaboração de diretrizes mais genéricas, que possibilitam atender a infraestruturas radiológicas diversificadas.

Após a elaboração do protocolo, o desenvolvimento do DicomFlow foi realizado em etapas progressivas. Então, observando as diretrizes do protocolo, um protótipo inicial foi elaborado com apoio das tecnologias identificadas e elencadas dos trabalhos relacionados. Assim, testes de funcionalidade e simulações foram empregados para refinar as diretrizes do protocolo e do código implementado no *gateway* em um ciclo alternado e evolutivo. Ademais, a especificação do protocolo em dois conjuntos de diretrizes (diretrizes de comunicação e diretrizes de transferência) possibilitaram a implementação da arquitetura do *gateway* em dois módulos, com isso melhorando a flexibilidade e reduzindo a complexidade.

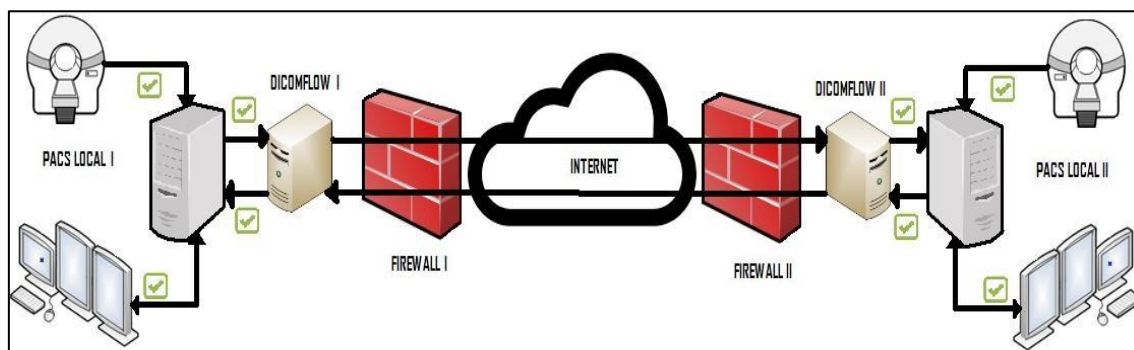
4.2. O protocolo de serviços

Tomando como foco as características necessárias a uma infraestrutura de informação e guiados pelas regras definidas na teoria de projetos para complexidade dinâmica, em especial a regra de construir *gateways* para infraestruturas de aplicação e serviço existentes (**RP7**) (Hanseth e Lyytinen, 2010), regra relativa ao princípio de construção sobre uma base instalada, foi elaborado um *gateway* em forma de protocolo de suporte a serviços gerência e transporte de exames de imagens médicas, que se apoia nos princípios e diretrizes do protocolo DICOM e nas características do modelo de arquitetura PACS.

O protocolo tem como objetivo padronizar a comunicação entre essas infraestruturas, contornando as limitações presentes no modelo PACS/DICOM (e.g. presença de *firewalls*) e provendo associação de forma facilitada. Ou seja, o protocolo foi construído para atuar a borda das infraestruturas e possui diretrizes genéricas suficiente, para minimizar mudanças nas infraestruturas, independentemente da heterogeneidade presente, facilitando sua adoção. Ainda, o protocolo possui diretrizes básicas, que permitem a composição dessas de forma variada, para atender as necessidades de comunicação de infraestruturas não previstas durante sua elaboração. Ademais, vale observar que o protocolo é aberto,

mesmo tento uma arquitetura implementada que serve de referência, veremos detalhes sobre essa arquitetura mais adiante. Ou seja, qualquer entidade que adote o modelo PACS/DICOM é livre para utilizar e implementar o protocolo DicomFlow.

Figura 8 - Protocolo atuando a margem da infraestrutura PACS/DICOM



Fonte: Próprio autor.

A Figura 8 ilustra a atuação do protocolo na infraestrutura PACS/DICOM. É possível observar o *gateway* DicomFlow mantido à borda, comunicando-se com a infraestrutura PACS retransmitindo as informações para outra infraestrutura PACS sem a interrupção do *firewall*, contornando uma das limitações expostas na seção 2.1.1, por exemplo, a utilização de portas geralmente bloqueadas pelos *firewalls*.

Então, para conseguir retransmitir informações e demandas de uma infraestrutura para outra, é necessário utilizar tecnologias amplamente adotadas, que tenham seus serviços permitidos pela maioria das regras de *firewall*. Como primeiro aspecto chave na elaboração desse protocolo, temos a utilização da base instalada de e-mail da Internet, definida pelo protocolo SMTP, que é amplamente difundido entre as infraestruturas. Assim, utilizamos os aspectos do protocolo SMTP como base na elaboração das diretrizes de comunicação do DicomFlow. Essa infraestrutura de e-mail possui como ponto forte a elevada conectividade, sendo capaz, na prática, de trocar mensagens entre uma ampla diversidade de profissionais e organizações de saúde. Assim, com um único recurso de TI, conseguimos atender um grupo numeroso e heterogêneo de usuários. Ademais, a maioria das infraestruturas permite o tráfego de mensagens de e-mail, não havendo a necessidade de modificação em seus *firewalls*, ocasionando um mínimo de mudanças na infraestrutura, possibilitando a integração do *workflow* radiológico para um contexto global. Além disso, o e-mail é assíncrono, não requer inicialmente o estabelecimento de conexão entre duas infraestruturas para que essas se

comuniquem. Tal aspecto fornece independência entre os elementos técnicos das infraestruturas, possibilitando a livre associação e dissociação entre essas, favorecendo a formação de uma infraestrutura de informação mais flexível. Ademais, a infraestrutura de e-mail permite transportar de forma segura (com confidencialidade, integridade e autenticidade) o conteúdo das mensagens, viabilizando implementar as políticas de segurança de dados clínicos de pacientes exigidas em infraestruturas de saúde.

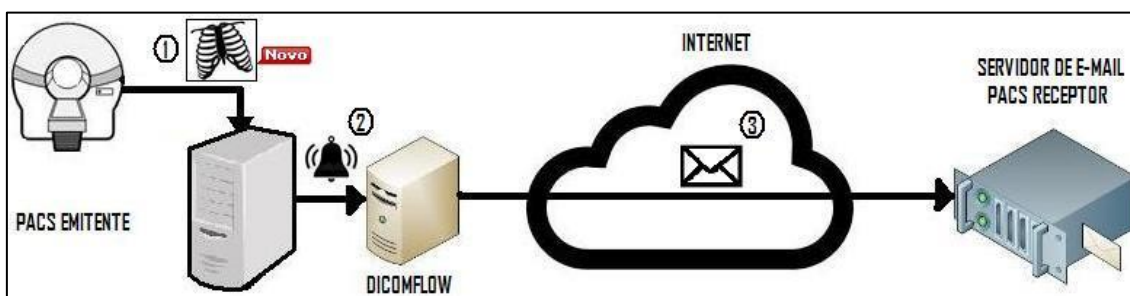
O segundo aspecto chave é aproveitar as diretrizes do DICOM e-mail (Weisser et al., 2007), um protocolo que é um exemplo de infraestrutura construída sobre uma base instalada PACS/DICOM. Dessa forma, o DicomFlow se orienta nessa recomendação de padrão, para definir suas diretrizes de formato de conteúdo de mensagens e proteção desse conteúdo. Porém, o ponto negativo do DICOM e-mail está na dificuldade em transportar exames médicos como anexos de e-mail devido ao tamanho das imagens (maiores que 30 MBytes). A proposta do DICOM e-mail é transmitir a imagem fragmentada em vários e-mails (Weisser et al., 2007). Assim, devido à complexidade do controle de transmissão das imagens através de e-mail, as especificações de transmissão de mensagens do DicomFlow diferem daquelas existentes no DICOM e-mail, pois dados brutos de imagens não são transmitidos em mensagens como anexos de e-mail, apenas metadados e outros tipos de informações clínicas (e.g., dados demográficos, laudos) são incluídos nas mensagens. Tal abordagem é vantajosa, pois diminui a complexidade de implementação do protocolo por prescindir da aplicação de mecanismos de fragmentação e desfragmentação de imagens, não havendo a necessidade de empacotamento dos exames médicos em diversas mensagens e nem mecanismos para garantir entrega e ordenação dessas mensagens. Então, uma única mensagem é capaz de transmitir as informações necessárias sobre um exame e, dessa forma é facilitada a elaboração de diretrizes para empacotamento e proteção da informação, focando em elaborar diretrizes que garantam maior desempenho e confiabilidade.

Uma vez que a transmissão dos exames médicos não é feita através do e-mail, é necessário utilizar uma tecnologia complementar para a transferência efetiva, contudo a teoria de projetos recomenda melhorar um recurso de TI dentro de uma infraestrutura apenas quando necessário (**R10**), ao passo não é

aconselhado implementar uma nova infraestrutura de suporte (**RP5**) (Hanseth e Lyytinen, 2010). Logo, optou-se por utilizar outro meio para a transferência de exames, utilizando uma infraestrutura já existente e direcionadas para esse fim, a infraestrutura HTTPS (*Hyper Text Transfer Protocol Secure* - protocolo de transferência de hipertexto seguro). Dessa maneira, o protocolo proposto utiliza em suas diretrizes mecanismos de controle de acesso baseados nessa infraestrutura.

Essa abordagem proporciona uma assimetria no funcionamento do protocolo. Pois, as diretrizes baseadas em DICOM e-mail e SMTP tratam da comunicação de informações de gerência e controle e as diretrizes baseadas em HTTPS tratam da transferência de exames. Ou seja, comunicação e transferência são tratados por vias distintas. Então, utiliza-se o e-mail para notificar o receptor da disponibilidade de um exame e solicitar que ele realize alguma ação (e.g., armazenar o exame, emitir um laudo), incluindo-se neste e-mail informações necessárias para o acesso ao exame (e.g., URL e credenciais de acesso).

Figura 9- Envio de mensagem contendo os dados do novo exame



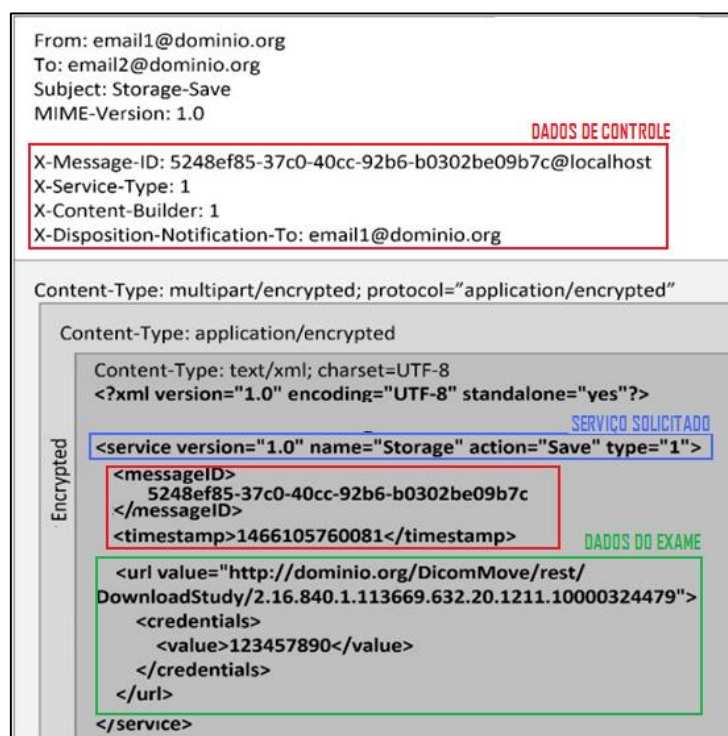
Fonte: Próprio autor

Como mostra a Figura 9, um exemplo de processo de envio de mensagem ocorre quando (1) o PACS emissor adquire novo exame de imagem e o armazena no servidor PACS, (2) o *gateway* DicomFlow monitora o servidor PACS e quando observa a existência de um novo exame, (3) envia uma mensagem com os dados do novo exame para o e-mail do PACS receptor.

As mensagens de e-mails transmitidas são estruturadas em linguagem de marcação XML e carregadas no corpo do e-mail, protegidas por criptografia. Essas estruturas XML carregam tanto dados necessários para identificação dos pacientes e estudos quanto dados de controle. Os dados de controle definem o serviço e a ação que o receptor da mensagem deve efetuar sobre as informações dos

pacientes e estudos, por exemplo, supondo que o receptor execute serviços de armazenamento de exames, o emissor envia uma mensagem com identificação do serviço (Armazenamento) e ação (Salvar). Informações dos serviços que não requerem proteção são trafegadas também no cabeçalho do e-mail para melhoria do desempenho. Por exemplo, o título do serviço e a ação requisitada estão presentes no cabeçalho para facilitar ao receptor a identificação rápida da intenção da mensagem. Então, as mensagens de e-mail transmitidas funcionam como requisições de ações e são denominadas **mensagens de serviço**. Existem mensagens de serviço que, além de requererem ações sobre informações da imagem, requerem ações sobre as imagens médicas (e.g. armazenamento da imagem, emissão de laudo) e carregam na estrutura da mensagem uma URL utilizada para transferência das imagens e, possivelmente, as credenciais para acesso às imagens médicas.

Figura 10 - E-mail de Solicitação de armazenamento conforme especificado pelo Protocolo



Fonte: Próprio autor.

A Figura 10 mostra um exemplo de mensagem de serviço de solicitação de armazenamento. É possível ver o serviço solicitado (destaque em azul), os dados

de controle (destaque vermelho), que também são encaminhados no cabeçalho da mensagem, não criptografados, para fins de pré-processamento, e os dados de acesso às imagens (destaque em verde), que são enviados criptografados e só podem ser vistos pelo receptor da mensagem.

É importante destacar que o protocolo não define políticas de encaminhamento das mensagens. Cada entidade que adota o protocolo tem a liberdade de implementar a política de encaminhamento que melhor atenda a sua realidade e fluxo de trabalho. Contudo, protocolo define um conjunto básico de tipos de mensagens de serviço. O uso de XML nas mensagens de serviço, elaboradas de forma simples, com descrição clara e fácil implementação, está em concordância com o princípio da criação de recursos de TI o mais simples possível (**RP3**) (Hanseth e Lyytinen, 2010). Isso foi alcançado devido à linguagem XML ser de fácil compreensão (legível por humanos), que possibilita incluir novos elementos a uma estrutura já existe e/ou compor novas estruturas de informação de forma recursiva. Dessa forma, através da composição desses tipos de mensagens de serviços, é possível atender a uma diversidade de políticas de encaminhamento e fluxos de trabalho presentes nos diversos tipos entidades de saúde e, ainda, é possível compor novos tipos de mensagens de serviços, caso seja necessário. Assim, o protocolo é capaz de dotar a infraestrutura de capacidade de adaptação e possibilita a associação de qualquer entidade arbitrária a essa infraestrutura, desde que adote o protocolo.

Assim, tomando como base o *workflow* radiológico e modelos telerradiológicos atuais (Motta, 2014), foram levantados os principais dados trafegados e definidos os seguintes tipos de mensagens de serviço:

Certificate: Mensagens de serviço desse tipo são utilizadas para troca de certificados digitais entre entidades de saúde que pretendem se comunicar entre si e executarem ações sobre as informações e imagens médicas. Os certificados digitais são utilizados para atender os aspectos de segurança definidos no protocolo e garantir o atendimento aos aspectos de segurança e confiabilidade impostos pelas políticas de tráfego de informações clínicas via Internet. Destaca-se que, antes de qualquer troca de mensagens dos demais serviços e transferência de imagens, ocorre troca de certificados digitais entre emitente e receptor.

Storage: Essas mensagens de serviço são responsáveis pela comunicação de requisições de transferência, arquivamento (permanente ou não) e manutenção de estudos de imagens em uma ou mais entidades externas àquela que os originou. Como também, mensagens desse tipo servem para comunicar as entidades originadoras dos estudos de imagem dos resultados obtidos do atendimento às requisições. Mesmo com as garantias de segurança das informações trafegadas, o protocolo não define política legais para esse tipo de transação, portanto supõe-se que as partes envolvidas já satisfaçam requisitos legais e possuam acordos de nível de serviço e confidencialidade, previamente definidos.

Sharing: Corresponde a mensagens responsáveis por sinalizar aos interessados a existência e localização de novos estudos de imagens em uma determinada entidade e que essas mensagens estão disponíveis para acesso e compartilhamento. Ou seja, esse tipo de mensagem de serviço é responsável por sinalizar aos interessados que um novo exame de imagem foi adquirido e pode ser acessado pelas entidades interessadas. Outras mensagens desse tipo comunicam respostas a essas sinalizações.

Request: Permite ao originador de um estudo requisitar a uma entidade externa (geralmente médicos radiologistas ou serviços de processamento) a realização de alguma operação tendo por base o estudo original, por exemplo, solicitações de criação de laudos ou processamento das imagens dos exames.

Find: Mensagens utilizadas por uma entidade de saúde, para localizar imagens médicas em outras entidades de saúde. O Find é responsável por solicitar que uma entidade efetue determinada consulta de um exame em uma entidade externa. Os dados do paciente e do exame usados para consulta são estruturados em XML e seguem a hierarquia especificada no padrão DICOM.

Discovery: Esse tipo é responsável por solicitar que uma entidade externa identifique quais os serviços do protocolo são suportados por ela, juntamente com as ações possíveis para cada serviço e status de disponibilidade de cada uma das ações. A entidade externa pode ainda informar que elementos da estrutura XML ela suporta para cada ação e serviço.

A Tabela 6 apresenta as ações de cada um dos tipos de mensagens de serviços, seguidas de uma breve descrição. Demais detalhes das ações e das

estruturas XML dos tipos de mensagens estão no protocolo presente no Apêndice A.

Tabela 6 – Mensagens de Serviço do protocolo e suas principais ações.

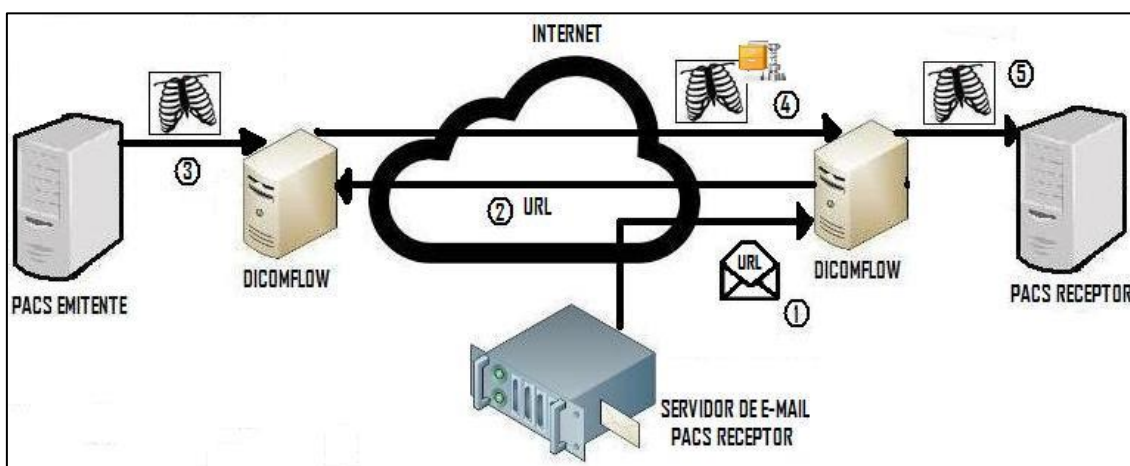
Serviço	Ação	Descrição
Certificate	Request	Solicitação de troca de certificado entre emitente e receptor. A Mensagem contém o certificado digital do emitente.
	Result	Resultado da solicitação de troca de certificado. A Mensagem contém o certificado digital do receptor.
	Confirm	Confirmação do recebimento da resposta de troca de certificado.
Storage	Save	Requisição de armazenamento de estudo.
	Result	Resultado da operação de armazenamento.
Sharing	Put	Sinalização de estudo disponível para compartilhamento.
	Result	Resultado informando registro de metadados de compartilhamento.
Request	Put	Requisição para realizar operação em um estudo (e.g. laudo).
	Result	Resultado da ação (e.g. laudo efetuado e retornado ao requisitante).
Find	Put	Solicitação de acesso às imagens do receptor conforme critérios de busca.
	Result	Resultado da solicitação de acesso às imagens do receptor.
Discovery	VerifyServices	Requisição das listas de serviços disponíveis.
	VerifyResult	Resultado contendo a lista de serviços.

Fonte: Próprio autor.

Continuando, conforme mencionado anteriormente, o protocolo utiliza uma via diferente para a transferência efetiva dos estudos de imagem médicas. A assimetria entre as duas vias dá a opção para o receptor resgatar o exame imediatamente ou num momento posterior, assim se mantém a conectividade entre as infraestruturas, mas com baixo acoplamento, característica necessária para o crescimento de infraestruturas de informação. Ainda, o protocolo define diretrizes para que as mensagens de serviços, que requerem ações sobre essas imagens, carreguem uma URL na estrutura do XML. Essa URL dá acesso ao exame de imagem. Dessa forma, o receptor desse tipo de mensagem resgata o exame

utilizando essa URL. De forma geral, o fluxo de transferência funciona da seguinte forma, como ilustra a Figura 11: (1) o protocolo do PACS receptor verifica seu e-mail e resgata a Mensagem de Serviço que solicita uma ação (e.g. armazenamento de exame), (2) então a URL é recuperada da mensagem, o protocolo do receptor inicia o resgate das imagens abrindo uma conexão utilizando a URL (3). O protocolo do emissor recebe a conexão, recupera e (4) transmite as imagens médicas compactadas para o protocolo do receptor que (5) armazena a imagem.

Figura 11 - Transferência de Imagens para o receptor



Fonte: Próprio autor.

4.2.1. Segurança das informações

A fim de atender as normas de segurança relacionadas à transmissão e ao acesso de informações de pacientes e de imagens médicas, aspectos de proteção contra violação do sigilo e manutenção da integridade dessas informações, tanto na origem quanto no destino, foram empregados princípios de criptografia de dados e credenciais de acesso nas diretrizes do protocolo proposto. Por uma via, os envios e leituras de mensagens de serviço utilizam o conceito chaves públicas e privadas para criptografar as informações contidas no XML de serviço e para assinar as mensagens enviadas. Dessa forma, as diretrizes do protocolo tomam como base o padrão *S/MIME (Secure/Multipurpose Internet Mail Extensions)*, definido segundo os RFCs 3369, 3370, 3850 e 3851, direcionado para proteção de mensagens de e-mails. Por outra via, o resgate de imagens utiliza requisitos de segurança parte a

parte definidos por diretrizes de transmissão de conteúdo, baseadas nas especificações contidas no protocolo HTTPS, que consiste na comunicação HTTP (RFC 7540) em uma conexão criptografada por TLS (*Transport Layer Service*), adicionados aos conceitos RESTful. Assim, as diretrizes do protocolo proposto especificam o uso de credenciais de acesso. Essas credenciais possuem um identificador único universal imutável (UUID - *Immutable Universally Unique Identifier*), definido segundo o RFC 4122. Elas são enviadas durante a abertura de conexão e carregam informações que, se válidas, possibilitam a liberação do resgate do exame indicado pela URL, por exemplo, a credencial pode conter informações como: uma validade (tempo para resgate), os tipos de exames que podem ser acessados, quem pode ter acesso (i.e. que certificados estão associados aquela credencial), etc.

Ainda, conforme especificado no protocolo, tanto os fluxos de troca de certificados digitais quanto os fluxos de mensagens de serviços, que disponibilizam uma URL de acesso às imagens, podem encaminhar as credenciais na estrutura de XML. Ou seja, é possível encaminhar as credencias de acesso juntamente com os certificados digitais durante a troca de mensagens para aquisição de certificados digitais (**Certificate**), nesse momento são encaminhadas credenciais com maior acessibilidade. Por outro lado, durante a transmissão de mensagens de solicitação de armazenamento (**Storage**), solicitação de laudos (**Request**) ou compartilhamento (**Sharing**), pode também haver a troca de credenciais de acesso, mas que permitem acesso limitado aos exames presentes nas URL carregadas por essas mensagens.

Por fim, as diretrizes do protocolo DicomFlow garantem a comunicação ponto-a-ponto entre as entidades envolvidas durante a comunicação e transmissão de informações e imagens médicas na Internet. Mais detalhes sobre a implementação dos mecanismos de segurança serão apresentados na seção 4.4, que descreve a arquitetura implementada para o protocolo DicomFlow.

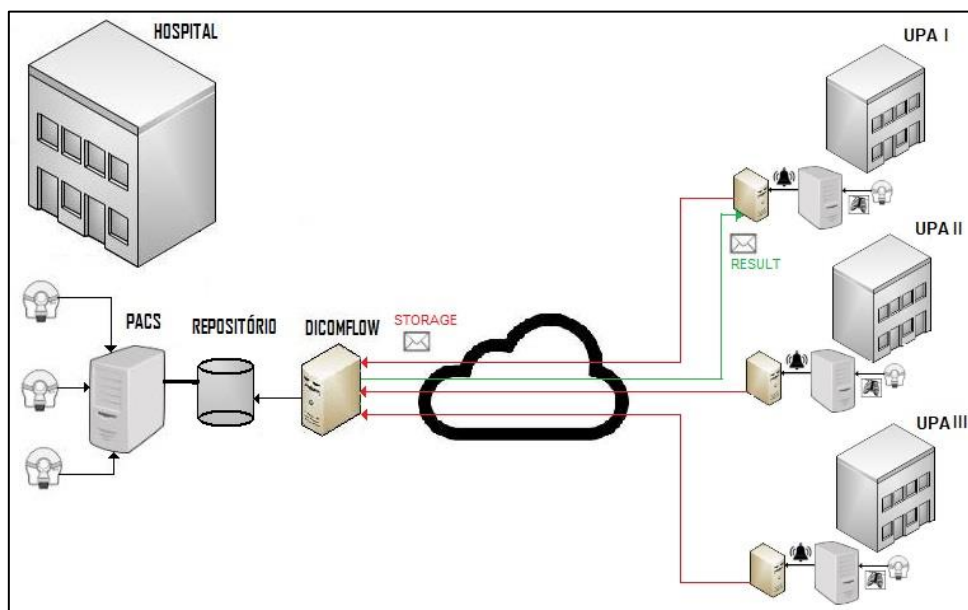
4.3. Cenários de uso

Para especificar o protocolo e alcançar o objetivo de prover interoperabilidade entre entidades de saúde pertencentes a domínios de rede distintos, buscou-se definir diretrizes que possibilitam a implementação de recursos de TI para tal fim de forma fácil, simples e de uso direto, sem que haja a necessidade de reconstruir ou redefinir esses recursos com o crescimento da infraestrutura. Incorporar esses princípios da teoria de projeto nas diretrizes só foi possível através da elaboração de cenários de uso. Esta seção descreve alguns cenários em que o protocolo pode ser aplicado e que se baseiam em problemas típicos para soluções de interoperabilidade na distribuição de imagens médicas. Ainda, tais cenários objetivam ilustrar a capacidade de adaptação do protocolo a diversas situações através da composição de seus tipos de mensagens de serviço. Ressalva-se que tais cenários não esgotam as situações de uso do protocolo, que não podem ser, em geral, completamente antecipadas.

4.3.1. Transferência Simples

Considere-se a situação em que um hospital central dispõe de uma infraestrutura PACS/DICOM completa, incluindo a capacidade de armazenamento permanente de exames de imagem. Por outro lado, organizações de saúde mais simples, como uma unidade de pronto atendimento (UPA), podem possuir equipamentos de imagem, mas não dispor da capacidade de armazenamento permanente. Nesse cenário, exames e laudos realizados em uma UPA são encaminhados para armazenamento permanente na infraestrutura PACS/DICOM de um hospital central. Assim, cada UPA envolvida possuem um *gateway* DicomFlow a borda da infraestrutura para monitorar a aquisição de novos exames e comunicar o gateway DicomFlow presente na extremidade da infraestrutura do hospital central.

Figura 12 - Cenário 1 e fluxo de Storage



Fonte: Próprio autor.

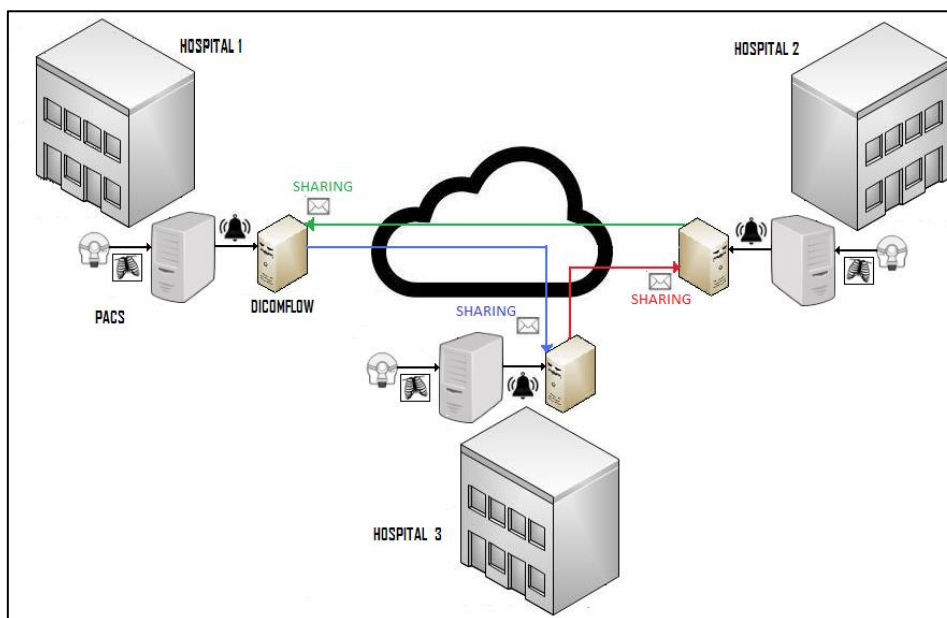
A Figura 12 ilustra o fluxo de funcionamento do cenário: Os exames são gerados por modalidades de imagens (e.g. Radiografia Computadorizada) presentes nas UPA e enviados para o servidor PACS das UPA. O DicomFlow presente nas UPA monitora o servidor de imagens e envia mensagens de solicitação de armazenamento (**Storage Save**) para DicomFlow do Hospital Central. O hospital Central efetua a transferência das imagens e armazena em seu servidor PACS. Por fim, o Hospital Central envia mensagens de serviço contendo os resultados (**Storage Result**) do armazenamento para as UPAS que solicitaram o armazenamento.

4.3.2. Distribuição compartilhada

Neste cenário, dois ou mais hospitais pertencem a uma mesma rede ou federação. Cada um deles mantém uma infraestrutura PACS/DICOM própria, armazenando os exames de imagem localmente. É preciso compartilhar entre si os exames de imagens realizados por seus pacientes em qualquer unidade da rede. Para isso, assim como foi explicado no cenário anterior, um *gateway* em cada hospital da rede monitora seus novos exames de imagem realizados. A cada novo exame, o *gateway* notifica os demais integrantes da rede enviando uma mensagem

de compartilhamento com os metadados contendo informações do exame, por exemplo, URL para baixá-lo e credenciais de acesso.

Figura 13 - Cenário 2 e fluxo de Sharing



Fonte: Próprio autor

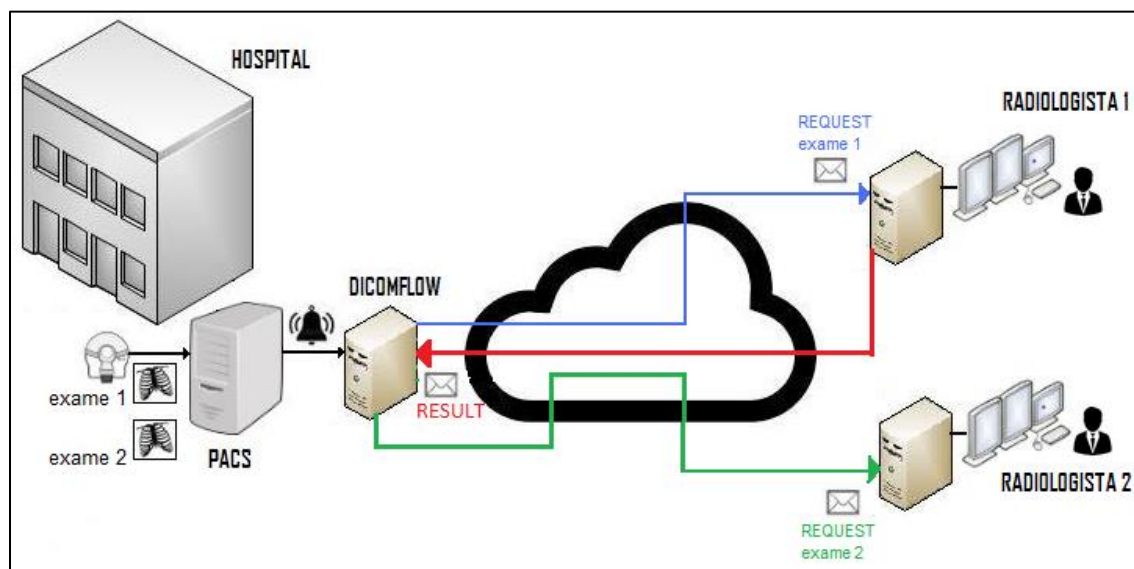
A Figura 13 ilustra o fluxo de funcionamento do cenário: Os exames são gerados por modalidades de imagens (e.g. Radiografia Computadorizada) e enviados para armazenamento no servidor PACS da entidade de origem, por exemplo, Hospital 1. O DicomFlow monitora esse PACS e, de acordo com a política de compartilhamento, envia mensagens de serviços de compartilhamento (**Sharing Put**) para o DicomFlow das entidades de saúde destino, nesse caso o Hospital 2. Da forma como foi ilustrado o cenário, as políticas de compartilhamento mostram que o Hospital 2 compartilha os exames adquiridos pelas suas modalidades com o Hospital 3 e o Hospital 3 compartilha suas aquisições com o Hospital 1. Por fim, As mensagens enviadas contêm informações do exame (e.g. dados do paciente) e a URL de acesso para as imagens. As entidades de destino recebem as mensagens e o protocolo pode acessar a URL.

4.3.3. Distribuição para diagnóstico

Geralmente, em regiões geográficas remotas, existe uma escassez de médicos radiologistas. No Brasil, um país de dimensões continentais, tal situação é ainda mais acentuada, uma vez que os médicos especialistas tendem a se concentrar nas grandes cidades das regiões mais ricas do Sul e Sudeste, enquanto que nas regiões mais pobres do Norte e Nordeste, a disponibilidade desses profissionais é menor (Figueiredo e Motta, 2013). Com isso, exames realizados em clínicas de imagem de tais localidades remotas ficam pendentes aguardando a disponibilidade de um médico para realizar os laudos. O DicomFlow pode auxiliar os radiologistas a realizar laudos de diagnóstico à distância, possibilitando um atendimento mais rápido aos pacientes e em uma redução de custos para os hospitais.

Neste cenário, os radiologistas são registrados nas clínicas e suas credenciais profissionais (e.g., inscrição no conselho de medicina) e de segurança (e.g., certificado digital, e-mail) são verificadas como parte de uma política de segurança. Um *gateway* instalado no computador do radiologista monitora, na caixa de entrada do seu e-mail, os novos exames direcionados a ele. O radiologista, mediante algum software aplicativo (fora do escopo do trabalho), construído sobre o *gateway* Dicomlow, pode baixá-los no momento desejado, interpretá-los e os respectivos laudos são enviados via e-mail para a clínica como anexos. Do lado da clínica ou hospital, um *gateway* monitora a caixa de e-mail em busca dos laudos enviados pelos vários radiologistas prestadores de serviço, para recepcioná-los para fins de armazenamento e posterior entrega ao paciente ou médico requisitante.

Figura 14 – Cenário 3 e o fluxo de Request



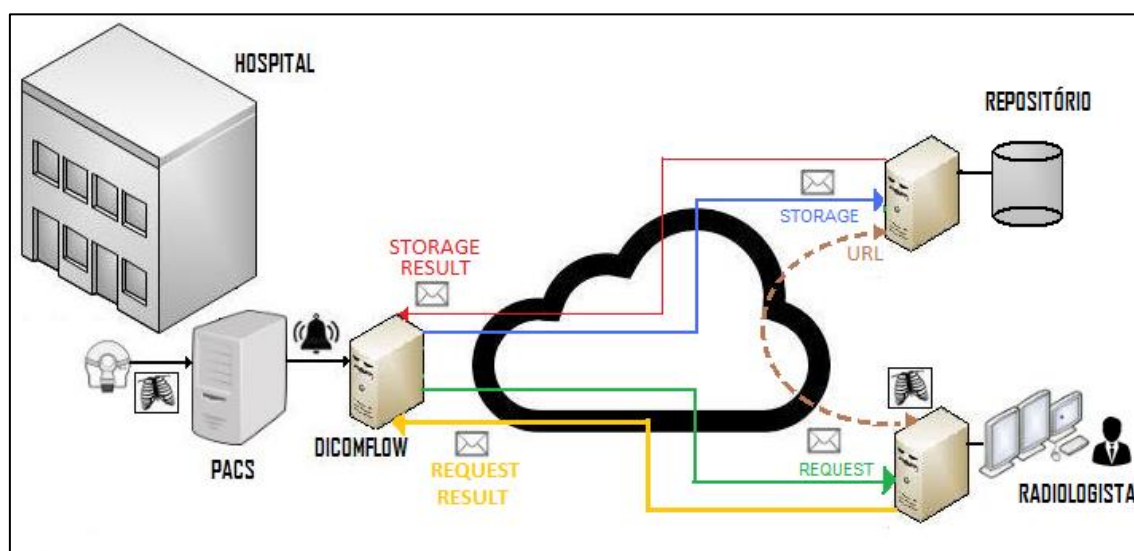
Fonte: Próprio autor.

A Figura 14 ilustra o fluxo de funcionamento do cenário: Os exames são gerados por modalidades de imagens (e.g. Radiografia Computadorizada) e enviados para armazenamento nos servidores PACS da entidade de saúde (Hospital). O Dicomflow monitora e envia mensagens de serviços para os radiologistas, solicitando que um laudo seja efetuado sobre as imagens disponibilizadas, as mensagens contêm informações do exame (e.g. dados do paciente) e a URL de acesso para as imagens (**Request Put**). Os radiologistas recebem as mensagens e o DicomFlow acessa a URL. As imagens são transferidas do servidor PACS para os radiologistas, por exemplo, através de um programa que implemente o protocolo DicomFlow. Os radiologistas produzem os laudos e enviam mensagens de serviço contendo os laudos dos exames para as entidades de origem (**Request Result**), como pode ser visto na figura, os Radiologistas 1e 2 receberam do Hospital solicitações de emissão de laudo, o Radiologista 1 resgatou as imagens e emitiu o laudo para o Hospital. O radiologista 2 em momento mais oportuno também pode resgatar as imagens e enviar o seu laudo para o Hospital.

4.3.4. Distribuição para diagnóstico com repositório terceirizado

Cenário semelhante ao anterior, porém, nesse caso, o armazenamento é realizado por serviço provido por uma empresa terceirizada (e.g. Armazenamento em Nuvem). O DicomFlow da clínica solicita à empresa o armazenamento dos novos exames, via mensagem de serviço. O DicomFlow da empresa recebe a mensagem de serviço com solicitações de armazenamento de seus clientes e, em um momento mais oportuno, armazena os exames. Nesse mesmo cenário, o DicomFlow da clínica notifica o DicomFlow dos radiologistas para emitir laudo, enviando na mensagem a URL e as credencias para acessar os exames na empresa terceirizada

Figura 15 - Cenário 4 e fluxo de Storage e Request



Fonte: Próprio autor.

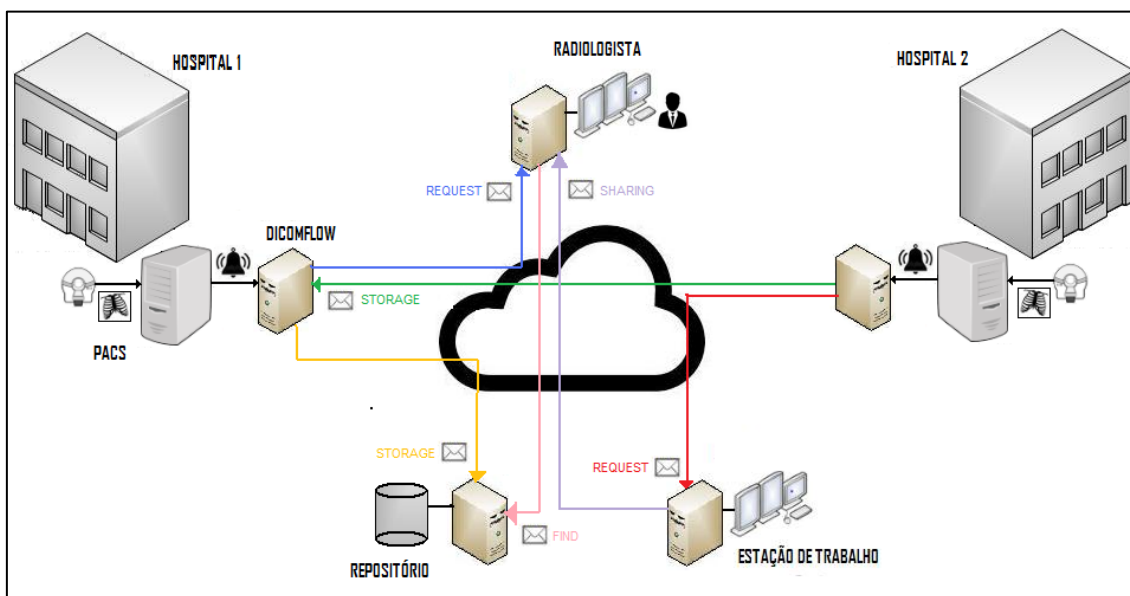
A Figura 15 ilustra o fluxo de funcionamento do cenário: Os exames são gerados por modalidades de imagens (e.g. Radiografia Computadorizada) e enviados para armazenamento no servidor PACS da entidade de saúde (Hospital). O DicomFlow monitora o PACS da entidade e envia mensagens de serviços solicitando que os novos exames sejam armazenados no repositório terceirizado, as mensagens contêm informações do exame (e.g. dados do paciente) e a URL de acesso para as imagens. O repositório terceirizado recebe as mensagens e o protocolo acessa a URL (**Storage Save**). As imagens são transferidas do servidor PACS de origem e armazenadas no repositório. O DicomFlow do repositório envia

mensagens de serviço contendo os resultados do armazenamento para a entidade de origem (**Storage Result**). Uma vez que os exames estejam armazenados no repositório, o DicomFlow do Hospital envia uma mensagem de serviço para o radiologista solicitando que um laudo seja efetuado sobre as imagens disponibilizadas no repositório terceirizado (**Request Put**), a mensagem contém informações do exame (e.g. dados do paciente), URL que direciona para o repositório e as credenciais de acesso e para as imagens. O radiologista ao receber a mensagem, através de um programa que implemente o protocolo DicomFlow, em momento mais oportuno, acessa o URL e resgata as imagens. Então, o radiologista envia uma mensagem de serviço contendo os laudos dos exames para o Hospital (**Request Result**).

4.3.5. Rede social radiológica

Uma Rede Social Radiológica consiste em um serviço que promove o relacionamento entre pacientes, profissionais de saúde (médicos radiologistas, técnicos, etc.) e as entidades originadoras de imagem, como clínicas e hospitais. O DicomFlow atuaria como infraestrutura integradora dos fluxos de exames de imagens e laudos entre tais entidades, estando, entretanto, abaixo da plataforma de suporte da rede social. Ou seja, este cenário é uma composição dos demais cenários apresentados anteriormente, onde os atores de um determinado cenário podem comunicar com atores de outro cenário, constituindo um espaço de fluxos diversos, formando uma infraestrutura de informação para a prática telerradiológica.

Figura 16 - Cenário 5: Infraestrutura de Informação telerradiológica



Fonte: Próprio autor.

A Figura 16 ilustra a junção dos diversos cenários descritos anteriormente, formando uma rede social para a prática radiológica. Na figura, temos hospitais pertencentes a domínios de redes distintos interagindo entre si, nesse caso, o hospital 2 solicitando armazenamento de seus exames de imagem no Hospital 1 (STORAGE) e também solicitando algum tipo de processamento sobre o exame à uma estação de trabalho remota (REQUEST). Por sua vez, a estação de trabalho pode compartilhar o exame com algum radiologista, por exemplo, para solicitar uma segunda opinião sobre o exame. Por outro lado, temos o Hospital 1 solicitando armazenamento de seus exames em um repositório externo, ao passo que solicita emissão de laudo ao radiologista que, por sua vez, acessa o repositório para resgatar os exames.

4.4. A arquitetura do DicomFlow

Pode ser observado nos cenários ilustrados na seção anterior um fluxo de troca de informações contínuo, sem que haja a necessidade de um elemento central de controle, onde cada entidade é independente e tem controle sobre seus processos, mas que compõem o mesmo espaço global de atuação, ou seja, as entidades, por livre escolha, atuam juntas para alcançar o objetivo de compartilhar exames de imagem entre si, sendo capazes de formar uma infraestrutura de

informação telerradiológica. Ainda, as diretrizes existentes no protocolo definem as mensagens de serviços com o mínimo de dependência entre elas, permitindo diversificar os fluxos de troca de mensagens. Dessa forma, atendem aos fluxos encontrados nos cenários, podendo, também, atender fluxos de outros tipos de cenários não previstos inicialmente.

Assim, a arquitetura proposta deve conter aspectos e tecnologias que permitam atender as características definidas nos cenários e nas diretrizes do protocolo DicomFlow. Então, para facilitar a construção dessa arquitetura, as diretrizes do foram organizadas em dois conjuntos distintos e que podem ser implementados de forma independente, pois um conjunto trata da comunicação e dos aspectos de segurança de envio e leitura de mensagens, enquanto que o outro conjunto trata da transmissão de imagens médicas e dos aspectos de segurança relacionados à transferência de informações de saúde. A única interseção se dá através das diretrizes que tratam da construção da URL e credenciais de acesso ao exame. Dessa maneira, é possível implementar soluções diferentes para cada um dos conjuntos de diretrizes de forma que essas tenham um mínimo de acoplamento possível.

Continuando, o protocolo foi especificado para atuar a borda de uma infraestrutura PACS/DICOM, junto ao servidor PACS, como observador do estado atual desse, ou seja, o protocolo observa se houve uma nova aquisição de exames ou mudanças nos exames existentes. O protocolo não especifica como os exames devem ser observados, por exemplo, se observados através dos registros existentes em uma tabela de banco de dados ou se observados através de um diretório de armazenamento de imagens. Assim, fica livre a escolha do método de observação a ser implementado para a solução. Além disso, o protocolo não especifica como devem ser as estruturas de e-mail utilizadas, só especifica como deve ser a construção das mensagens. Ainda, não faz uso de elementos centrais para comunicação, apenas define que as conexões para transferência dos exames são ponto-a-ponto e desfeitas ao término do resgate. Logo, o protocolo não impõe mudanças nas infraestruturas PACS das entidades que forem adotá-lo e possibilita o controle distribuído entre essas entidades.

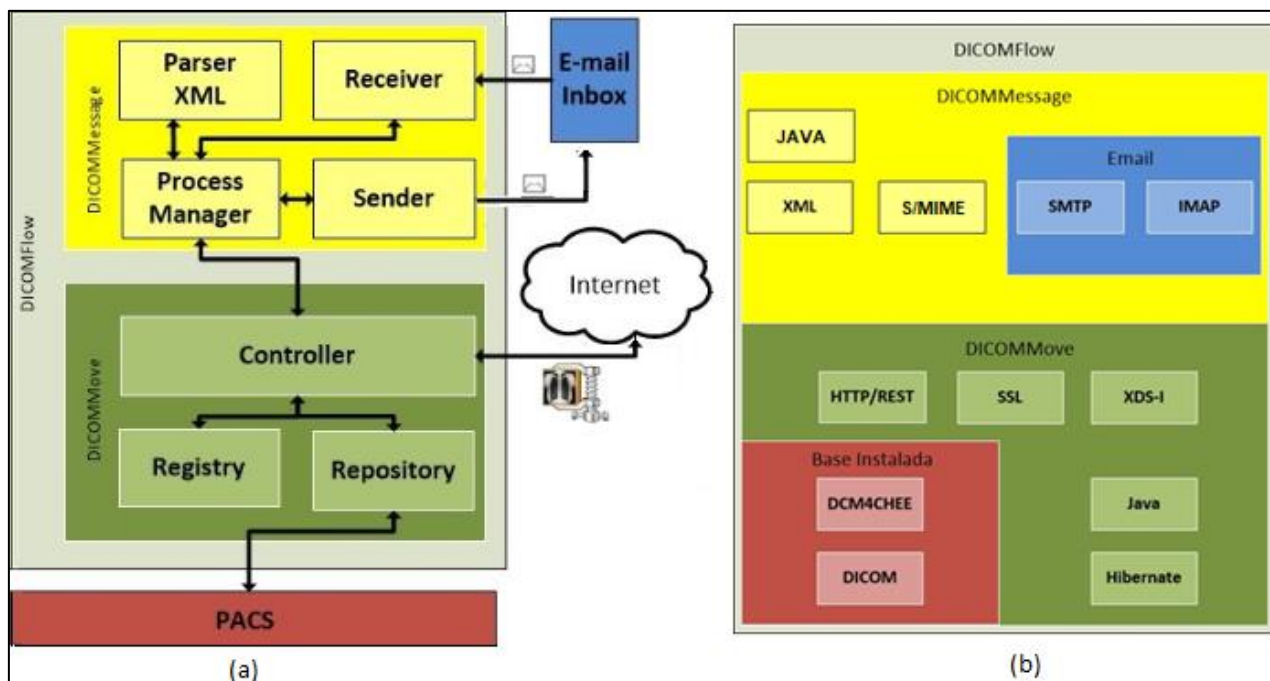
Dessa forma, todas essas características do protocolo foram abordadas a construção da solução, pois facilitaram o processo de geração do modelo

arquitetural. Ainda, analisando tecnicamente o funcionamento do protocolo, atentando para os fluxos presentes nos cenários de aplicabilidade, foi possível visualizar um processo comum de funcionamento de cada fluxo: observação de mudanças no estado atual do conjunto de exames de imagens contidos na infraestrutura PACS/DICOM, alerta aos interessados sobre essas mudanças através de mensagens de serviços e resgate dos exames que sofreram mudanças. E mais, durante a elaboração do modelo, aproveitou-se o ponto forte da infraestrutura PACS/DICOM, o amplo uso do DICOM como padrão de comunicação entre equipamentos presentes nos departamentos de radiologia, independentemente do fabricante. Ou seja, foram buscadas as tecnologias mais utilizadas na implementação do padrão DICOM, para empregá-las no modelo, a fim de facilitar o acesso e interpretação das informações de saúde contidas nos objetos DICOM, reforçando o uso do padrão e fortalecendo a infraestrutura PACS/DICOM.

Isto posto, foram definidos como principais macros requisitos do modelo: garantir a troca de mensagens entre instituições e profissionais de saúde de forma segura, segundo as políticas de tráfego de informações clínicas via internet; e possibilitar transferência de exames de imagem, também através da Internet, sem a interferência de *firewalls*. Assim, a primeira decisão de implementação foi definir o tipo de estrutura do modelo arquitetural do DicomFlow. Dessa forma, mantendo o foco em facilitar a implementação das diretrizes do protocolo e garantir o baixo acoplamento dos componentes da arquitetura, optou-se por um modelo composto de dois módulos, um módulo responsável pela comunicação de mensagens de serviço, denominado DicomMessage, outro módulo responsável pela transferência efetiva dos exames de imagem, denominado DicomMove. Tal decisão torna o modelo mais flexível, pois os módulos são independentes, permitindo que outras soluções possam ser empregadas sem prejudicar o funcionamento da arquitetura e desde de que essas outras soluções estejam em conformidade com o protocolo.

A arquitetura proposta para o DicomFlow é de referência e todo aquele que conhece seu protocolo é livre para fazer sua própria implementação, não se tendo controle de quem implementa. A seguir serão descritas as características e funcionalidades de cada um dos módulos do modelo e as tecnologias empregadas em cada um.

Figura 17 – Arquitetura do DicomFlow e tecnologias empregadas



Fonte: Próprio autor.

A Figura 17 (a) ilustra a arquitetura modular do DicomFlow, os principais componentes de cada módulo, a relação entre esses componentes e a relação com as infraestruturas PACS, e-mail e internet. No Módulo DicomMessage, temos o componente **Process Manager**, atuando como coordenador do fluxo de envio e recebimento de mensagens, ele define as informações a serem enviadas. O componente **Parser** converte informações em XML. Ainda, o **Process Manager** criptografa e assina o XML e solicita o envio. O **Sender** é responsável pelo envio, ele cria mensagens e insere o XML criptografada no conteúdo. Por outro lado, o componente **Receiver** monitora a caixa de e-mail para resgatar novas mensagens e junto com o **Process Manager** transforma XML em informações novamente. Continuando, no módulo DicomMove, o componente **Controller** atua como coordenador das atividades de toda o módulo, consulta a existência de novos exames médicos através do componente **Repository**, que monitora o servidor PACS. Ainda, o **Controller** solicita ao **Registry** a gerência informações de controle sobre o exame (e.g. a URL de acesso ao exame), para futuras consultas quando houver necessidade de resgate das imagens. O Controller é o responsável pela

gerência de transferência de imagens, ele libera o acesso e comprime as imagens antes de enviá-las.

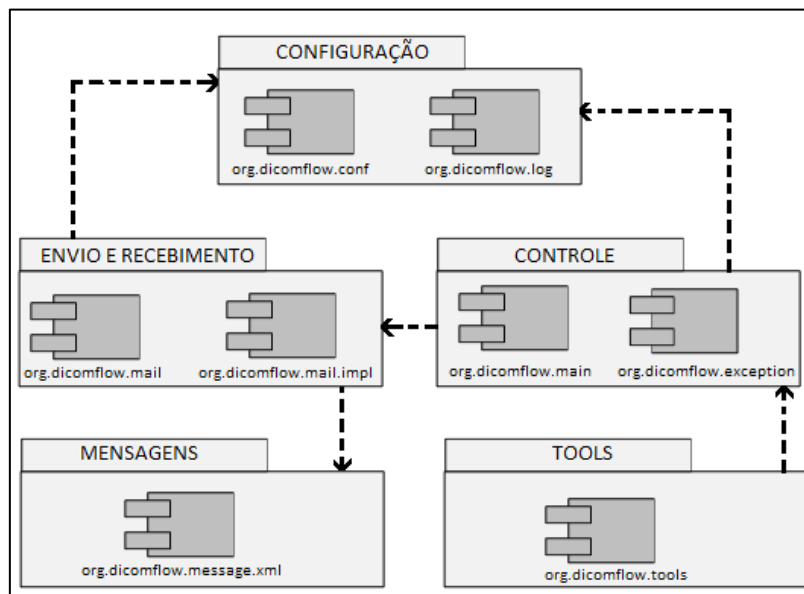
Por fim, a Figura 17 (b) apresenta as tecnologias empregadas para manter a relação entre os módulos e as infraestruturas existentes, como também para efetuar a comunicação de mensagens e transferências de imagens médicas. A seguir será descrito como essas tecnologias foram utilizadas.

4.4.1. Módulo DicomMessage

Conforme apresentado anteriormente, o módulo DicomMessage é responsável pela comunicação entre entidades de saúde através de mensagens, sendo assim, esse módulo implementa as diretrizes do protocolo que envolvem a criação, envio, leitura e proteção de mensagens de serviço. Suas funcionalidades englobam: criar as estruturas XML das mensagens de serviço, criptografar as estruturas XML com a utilização dos certificados digitais da origem e do destino, assinar com o certificado digital da origem as mensagens de serviço e enviá-las ao destino, receber as mensagens de serviços para a origem e verificar a assinatura com o certificado digital do destino, decodificar as estruturas XML com a utilização do certificado digital da origem.

Para a construção do código das funcionalidades mencionadas, optou-se pelo uso da linguagem de programação JAVA. Sendo orientada a objetos, facilita na organização dos componentes atômicos, utilizados no envio e recebimento de mensagens, como também para representar os elementos presentes nas estruturas XML. Ainda, a utilização de JAVA como linguagem e programação permitiu construir o módulo DicomMessage em forma de API (*Application Programming Interface*). API é um conjunto de códigos de suporte destinados a cumprir funções específicas que é dividido em diferentes partes funcionais chamadas pacotes (o que nós denominamos bibliotecas).

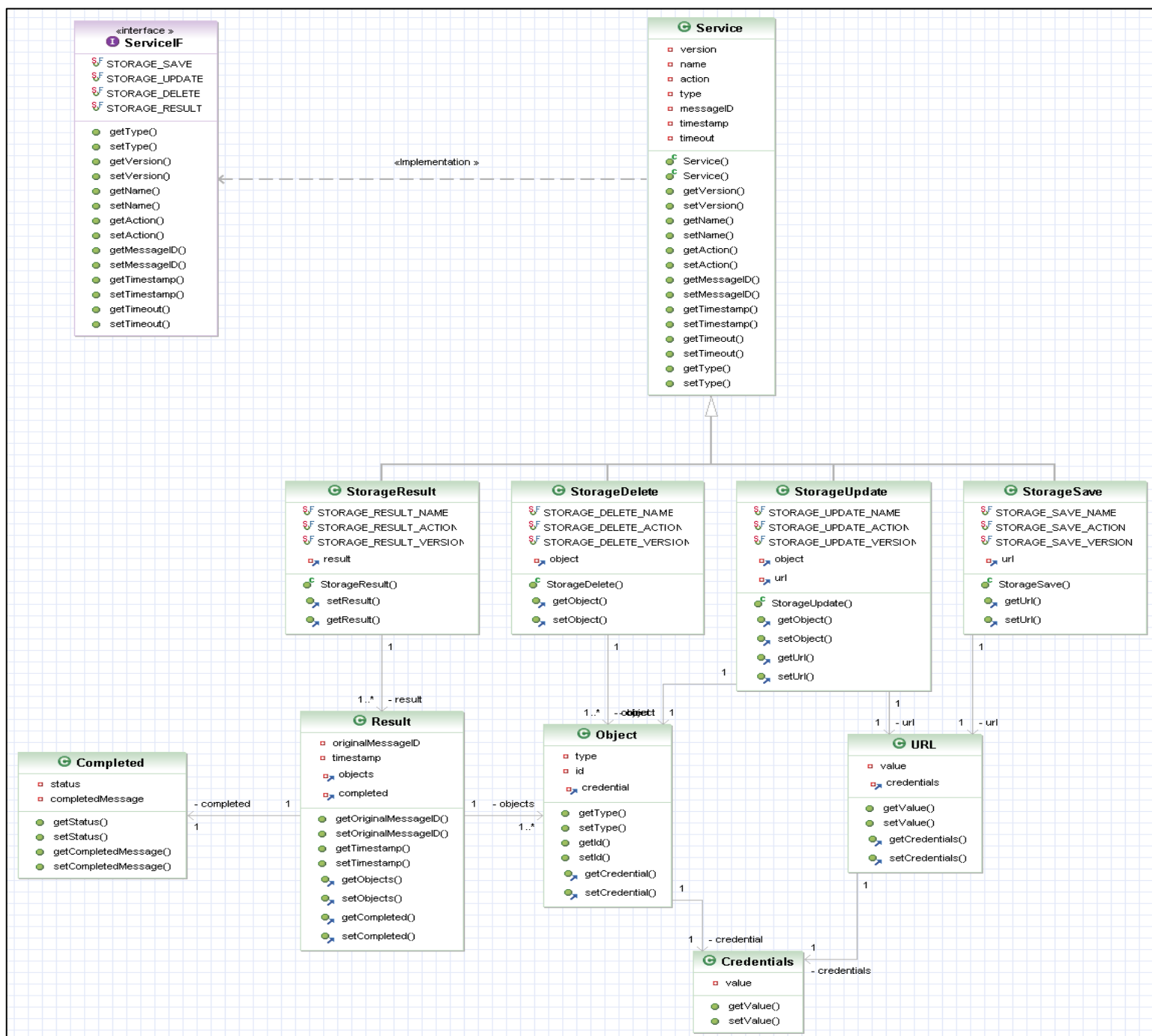
Figura 18 - Pacotes do módulo DicomMessage



Fonte: Próprio autor.

A Figura 18 apresenta a estrutura de pacotes da API para o módulo DicomMessage. Assim, foi possível organizar cada uma das funcionalidades elencadas em pacotes separados. Ainda, em completude ao código, para cada pacote foram definidas interfaces, minimizando o acoplamento entre esses conjuntos de classes. Dessa maneira, é possível compor novos componentes em acompanhamento às mudanças do protocolo (devido à criação de novos tipos de mensagens para atender à evolução das infraestruturas), sem que os pacotes sofram alterações e necessitem de reestruturação.

Figura 19 - Interface e classes que representam a estrutura XML Storage



Fonte: Próprio autor.

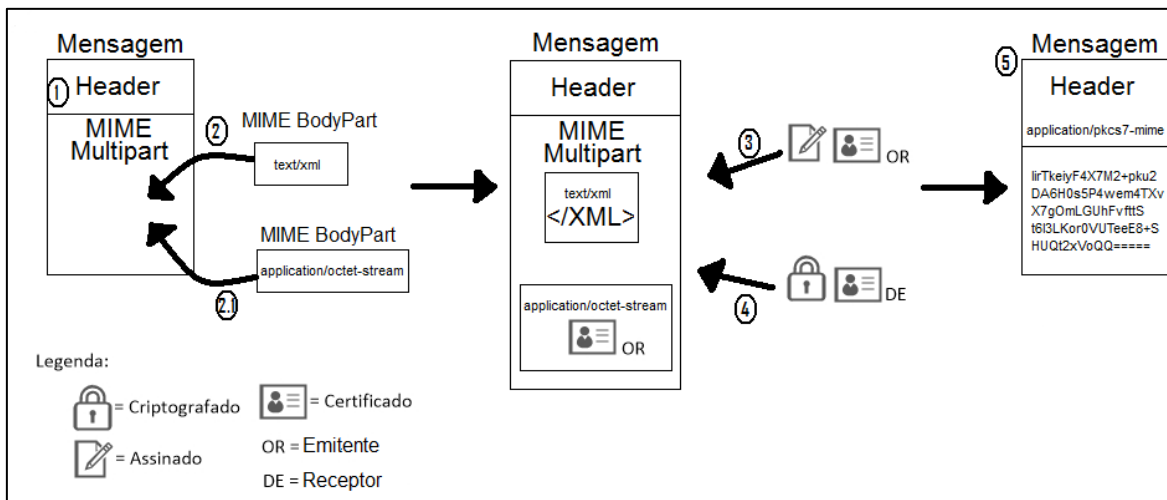
O pacote **Mensagens** possui um conjunto de classes JAVA responsáveis pela criação da estrutura XML enviadas nas mensagens de serviço. A Figura 19 apresenta um diagrama UML (*Unified Model Language*) contendo o conjunto de interfaces e classes utilizadas para representação em XML das estruturas do tipo de mensagens de serviço Storage e todas as ações requisitadas através dessas

mensagens de serviço (As demais estruturas seguem uma hierarquia de classes semelhante). Para isso foi utilizado a API JAXB (*Java Architecture for XML Binding*), criada e mantida pela Oracle, essa API possui funcionalidades de converter objetos JAVA em estruturas XML e vice-versa. Ainda, com auxílio do JAXB é possível ler arquivos de definição de XML (do inglês, XSD – *XML Schema Definition*) e transformá-los em classes JAVA organizadas hierarquicamente também criada em JAVA. Como o protocolo possui em suas diretrizes as estruturas XML definidas em formato XSD, facilita a implementação dessas classes.

Ainda, O pacote **Configuração** é utilizado para manter as propriedades do e-mail utilizado para envio e recebimento de mensagens (e.g. host do servidor de e-mail, porta, protocolo, etc), como também manter as propriedades para registro das atividades desempenhadas pela API (logs). Assim, para manutenção das propriedades utilizou-se as classes utilitárias do próprio JAVA e para manutenção dos registros de atividades utilizou-se a API Log4J, mantida pela Apache.

Continuando, o pacote **Envio e Recebimento**, além de possuir classes responsáveis pelo envio e recebimento das mensagens de serviços, é responsável pela assinatura e criptografia dessas mensagens. As classes presentes são compostas por classes pertencentes a duas API. A primeira delas, a API JavaMail, também mantida pela Oracle, permite estabelecer conexão com servidores de e-mail para troca de mensagens. O JavaMail possui funcionalidades que permitem o estabelecimento de conexões através do protocolo SMTP (*Service Mail Transfer Protocol*) e também IMAP (*Internet Message Access Protocol*), dessa maneira, utilizando as propriedades configuradas, é possível ler e enviar mensagens de e-mail. Por outro lado, a API BouncyCastle, mantida pelo grupo australiano Legion of the Bouncy Castle, implementa as diretrizes especificadas no padrão PGP, como também especificadas no padrão S/MIME de criptografia com chaves públicas. Conforme especificado em sua documentação de uso, o BouncyCastle utiliza o conjunto de classes JAVA para criptografia, dessa forma utiliza certificados gerados no padrão X.509, certificados de chaves assimétricas (pública e privada) e assim, estando em harmonia as especificações do protocolo proposto nesse trabalho.

Figura 20 - Processo de criação, assinatura e criptografia da mensagem



Fonte: Próprio autor.

A Figura 20 ilustra o mecanismo de criação, assinatura e criptografia de mensagens de serviço executado pelo pacote de **Envio e Recebimento**. Segue a descrição de funcionamento do mecanismo: **(1)** O emissor cria a mensagem de múltiplos conteúdos (MIME Multipart). **(2)** inclui um conteúdo (MIME BodyPart) com a estrutura XML do serviço e define seu tipo (Content-Type) como XML (`text/XML`; `charset=UTF-8`). **(2.1 - condicional)** inclui outro conteúdo (MIME BodyPart) contendo o certificado digital do emissor e define seu tipo (Content-Type) como anexo (`application/octet-stream`). **(3)** O emissor assina a mensagem com seu certificado digital, **(4)** criptografa a mensagem com o certificado digital do receptor e **(5)** define no cabeçalho da mensagem o tipo da mensagem como criptografada (`application/pkcs7-mime`; `name="smime.p7m"`; `smimetype= enveloped-data`).

Figura 21 - Exemplo de mensagem de serviço criada

```

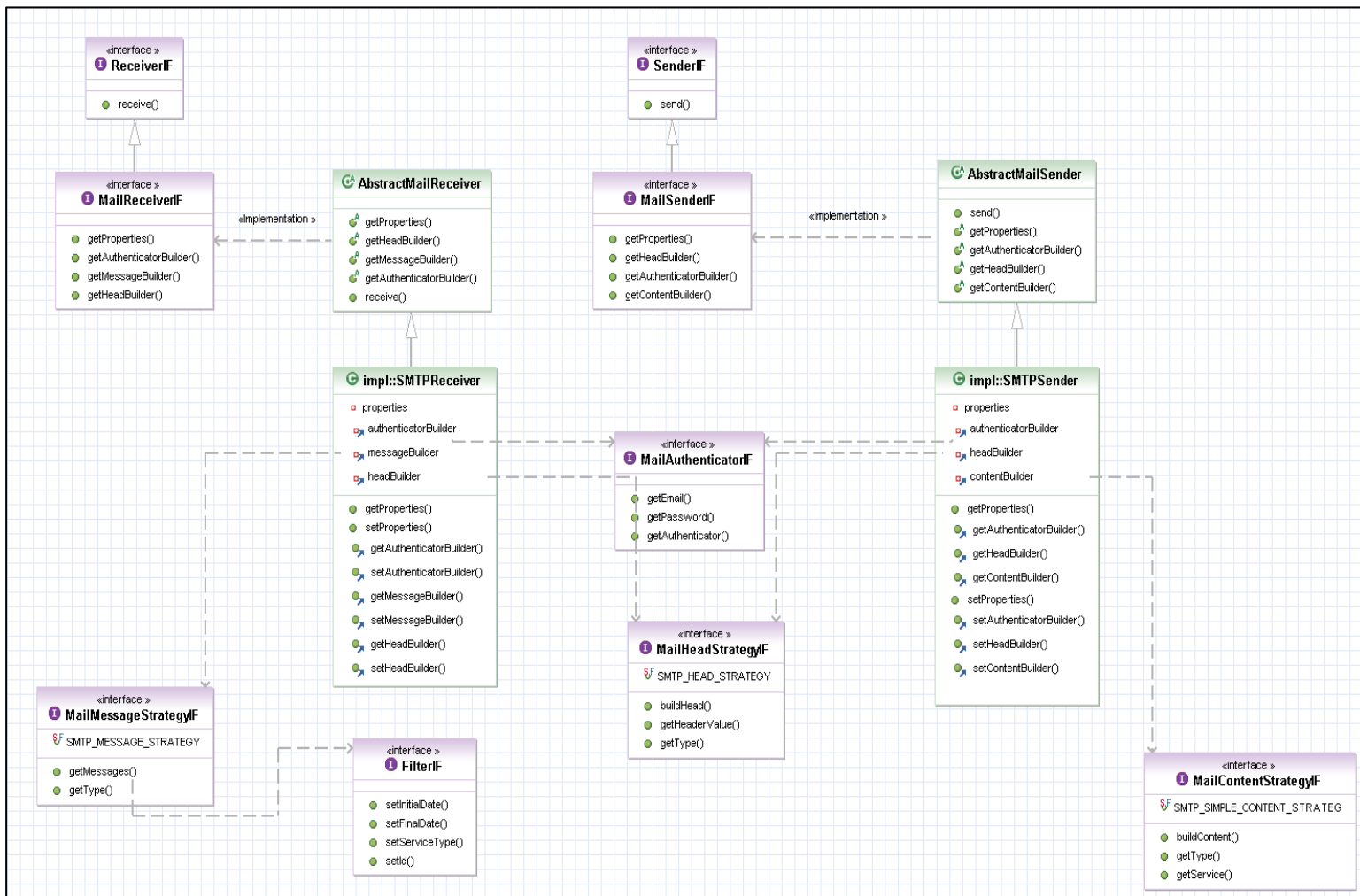
From: <dicomflow@email.com>
Date: 2017-01-01 23:59 GMT-03:00
Subject: Storage-Delete
To: protocolo@mail.com
X-Message-ID: 5248ef85-37c0-40cc-92b6-b0302be09b7c@localhost
X-Service-Type: 1
X-Content-Builder: 1
X-Disposition-Notification-To: dicomflow@email.com
--001a114792bc1a997f0550e94c1d
Content-Type: application/pkcs7-mime;name="smime.p7m";smime-type=enveloped
Content-Disposition: attachment; filename="smime.p7m"
Content-Transfer-Encoding: base64
X-Attachment-Id: 4addde3b5d38573f_0
MIAGCSqGSIb3DQEHAA6CAMIACAQAxggGDMIIBfwIBADBnMF8xCzAJBgNVBAYTAzJyMQswCQYDVQQL
EwJwYjELMAkGA1UEBxMCanAxCzAJBgNVBAoTAmNpMQ0wCwYDVQQLEwR1ZnBiMR0wGAYDVQQDEExFh
cGlbnRlZ3JhY2FvLm9yZWIEG1YHqzANBgkqhkiG9w0BAQEFAASCAQBN5hEjzfnWYkPT887KQOWi
bsWp3+TYAvzLnKffaNFSE1rrW56CKVeLwJCYKMYctGpBjXxYb+94oYghNxrMAC6vfbPq0J0VFkCo
5zPcDWtaa+ukmF7W3+r1pEh3JNPOKS1skJoS4ujBcWnWNvD4KY/iWd1+F906mEnN+Gndq+adu2jJ
XVZHRqK0reCDP+3x/e10Xmgu3WhRNCDDvkbmvB1SjOnGEQJoALfQDTmtmUTNbSBLxmW2uP68N0CG
JBAB7U8URF0XDWR1h2IVYw/52ApeF6iJsksz5YrsEcUXJMHeo1215peBsoOdJoXgCWeUgqH34k
cK8ftqWB+xQDqtiFMIAGCSqGSIb3DQEHATAZBgkqhkiG9w0DAjANAgE6BAirBLf0tafMn6CABIID
6D18A7uZ1zz06fo8ePEtaKDFsX8318EqRj3n4ogtYp9Y7tFHaADORGXIez1GJ/17tC0bcR2YoN94
PgU13Qzsh55EZL1VekJ1Fse0Bgo8WW1nZzSan2v1/g7RZiDiE26os1LX9/IwRGhZVrBPhUmqZ8Tj
TirVMnLR3C7T1j/bE3uxcl/Veq6nXSy++cd1/yJMK6qh6HW5Khwpfz1uud9B2kauOtwpVgBDvtOu
4i/f2buCBqp0gLeqYpogExVXuJDGsV6cuvMdFIeBpAAAAAAAAAAAAAAAA=
--001a114792bc1a997f0550e94c1d--

```

Fonte: Próprio autor.

A Figura 21 ilustra um exemplo de mensagem criada com o mecanismo de criptografia e assinatura com certificados digitais. Na imagem, é possível visualizar os dados de controle e o cabeçalho da mensagem com a identificação o tipo de conteúdo. Todas as demais informações estão protegidas por criptografia.

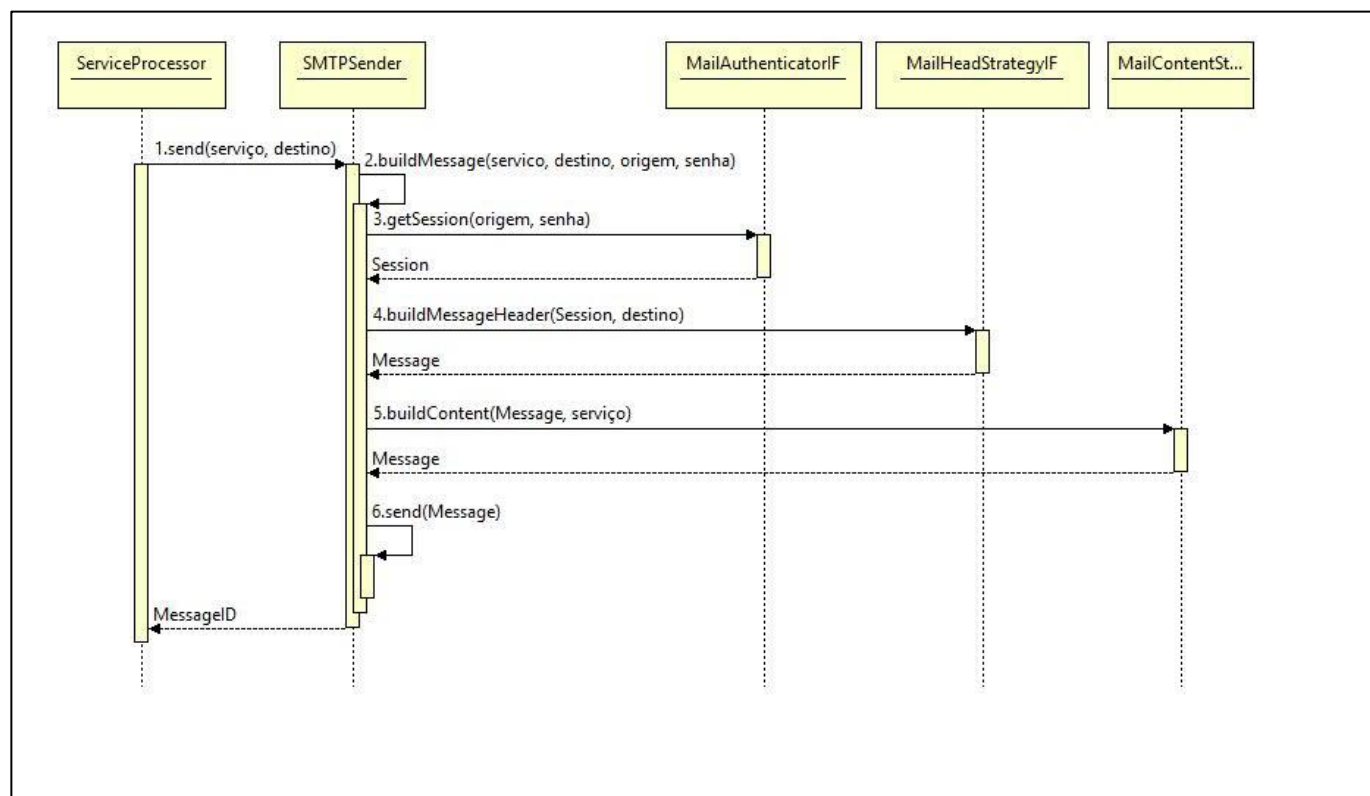
Figura 22 - Conjunto de classes utilizadas para o envio e recebimento de mensagens de serviço



Fonte: Próprio autor.

O conjunto de classes responsáveis pelo funcionamento do mecanismo de transporte das mensagens de serviço está no diagrama UML da Figura 22. Existem ilustrados na figura dois conjuntos de interfaces. O conjunto de interfaces a esquerda da figura é responsável pela leitura de mensagens recebidas, as classes que implementam essas interfaces podem filtrar as mensagens. Os filtros ajudam a definir o fluxo de acesso e comunicação de mensagens. Os demais conjuntos de interfaces definem como devem ser construídas as mensagens e como essas devem ser enviadas.

Figura 23- Diagrama de sequência de envio de mensagem de serviço



Fonte: Próprio autor

O diagrama de sequência presente na Figura 23, ilustra as etapas descritas no mecanismo de criação, assinatura e criptografia de mensagens implementadas nas classes e interfaces. Ela mostra especificamente o funcionamento de envio de uma mensagem de serviço: A classe **ServiceProcessor**, pertencente ao pacote **Controle**, **(1)** solicita o envio de um serviço para o e-mail de destino. Então, a classe **SMTPSender**, utilizando as implementações das interfaces do pacote **Envio e Recebimento**, **(2)** inicia a construção da mensagem, **(3)** abre uma sessão com o e-mail de origem da mensagem, **(4)** cria o cabeçalho da mensagem com as informações do remetente e destinatário, **(5)** converte o serviço em XML e adicionando no corpo da mensagem, **(6)** envia a mensagem. Após o envio, finaliza o processo retornando o identificador da mensagem enviada.

Ademais, o pacote **Controle** verifica e valida as configurações de conexão de e-mail mantidas pela API, ao passo que solicita e gerência o fluxo de funcionamento de envio e recebimento de mensagens, ou seja, registra e contorna os possíveis erros que venham a acontecer durante o funcionamento da API, seja por má configuração das propriedades, impossibilidade de conexão com o servidor de e-mail, má formação da estrutura XML recebida em uma mensagem de serviço.

Figura 24 - Utilização da API em linha de comando

```
usage: SendService -P <file> -R <mail> -S <file> [-E] [-k <file>] [-p
<password>] [-a <keyalias>] [-w <password>] [-c <keyalias>] [-V]
[-T <class>] [-A <file>]
The SendService tool implements a dicomflow-service sender.
An e-mail containing the dicomflow-service in XML format is sent from a
sender to a recipient.
The message can also be sent signed and encrypted as standard SMIME.
-
OPTIONS:
-P,--properties <file>          Use the properties file to connect the
                                server.
-R,--receiver <mail>           Use the given mail to indicate the
                                service receiver.
-S,--service <file>            Use the given file to configure a
                                service. the content must be a service
                                in xml format.
-E                               Send encrypted service.
-k,--keystore <file>           Use the given keystore file to locate
                                the certificates. use the located
                                certificates to sign and encrypt the
                                service. the given file must be a JKS
                                keystore.
-p,--keystore-pwd <password>    The given keystore file password.
-a,--private-cert <keyalias>    Use the given keyalias to get the
                                private certificate. The keyalias must
                                be a certificate with private key.
-w,--private-cert-pwd <password> The private certificate password.
-c,--public-cert <keyalias>     Use the given keyalias to get the
                                public certificate. The keyalias must
                                be a certificate with public key.
-V                               Be extra verbose.
-T,--service-class <class>      Use the given class to configure its
                                content with the given file.
-A,--attach <file>             Attach the given file.
-
Example 1: SendService -P smtp.properties -R receiver@mail.com -S
storage-save.xml
=> Sends a e-mail containing a storage-save service to receiver@mail.com.
-
Example 2: SendService -P smtp.properties -R receiver@mail.com -S
storage-save.xml -A certificate.crt
=> Sends a e-mail containing storage-service.xml and a certificate as
attach.
-
Example 3: SendService -P smtp.properties -R receiver@mail.com -S
storage-save.xml -E -k keystore.jks -p keystorePwd -a signerAlias -w
signerAliasPwd -c cipherAlias
=> Sends a e-mail containing storage-service.xml signed by signerAlias
certificate and cipher by cipherAlias certificate.
```

Fonte: Próprio autor.

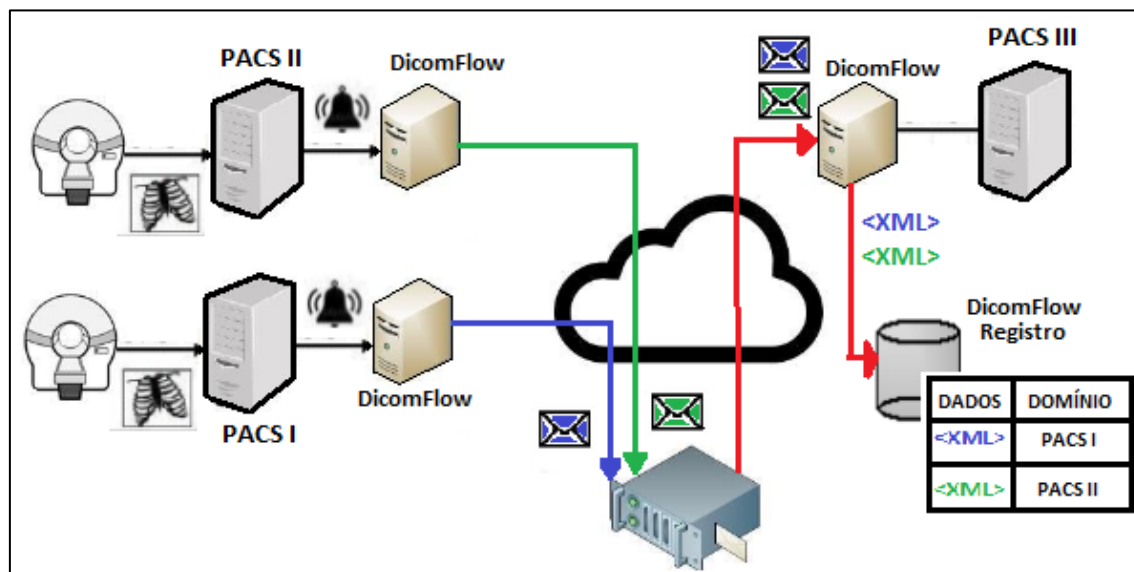
Por fim, o pacote **Tools** é composto por um conjunto de classes que possibilita executar a API, utilizando as configurações padrão especificada na própria API. Através desse pacote, também é possível executar a API de forma independente, ou seja, existem classes que podem ser usadas em scripts de linha de comando, isso possibilita que API possa ser usada em outra arquitetura, com outras linguagens de programação, provendo flexibilidade para usa da mesma. Um exemplo de seu uso em linha de comando é mostrado na Figura 24.

4.4.2. Módulo DicomMove

Como apresentado nas seções anteriores, o protocolo define uma linguagem de comunicação padrão para troca de informações de imagens médicas que serão compartilhadas, como também define os mecanismos de segurança para transmissão dessas imagens. Ainda, os fluxos definidos no protocolo são utilizados apenas para identificar a ordem entre mensagens que requisitam ações e mensagens que respondem essas ações. Dessa forma, o protocolo não especifica o tempo para que uma resposta seja dada a uma requisição e nem especifica como essas mensagens devem ser organizadas e mantidas na origem ou no destino. Assim, é livre a implementação de políticas de controle de armazenamento e tempo de resposta para as mensagens de serviços.

Dessa maneira, o DicomMove além de ser o módulo responsável por implementar as diretrizes de controle da transmissão dos exames de imagem, também é responsável pela gerência das informações que as mensagens de serviço carregam sobre as imagens a serem compartilhadas. Então, para implementar o controle de armazenamento de informações das imagens compartilhadas, complementando o protocolo proposto, o DicomMove utiliza a especificação dos perfis XDS e XDS-I como referência, adotando as definições dos atores desse padrão e dos fluxos de comunicação entre esses atores em sua implementação. Entretanto, a elaboração do DicomMove busca beneficiar-se apenas do conceito de indexação e localização de informações da arquitetura XDS e XDS-I, sem empregar a ideia do registro central entre organizações distintas, para busca e localização de documentos. As informações dos exames compartilhados (os metadados, a URL para acesso e as credenciais de autorização) são organizadas em banco de dados no destino da mensagem, dessa forma cada entidade envolvida tem controle sobre suas informações. Ou seja, as diretrizes de controle e armazenamento de informações compartilhadas definidas pelos perfis XDS e XDS-I são usadas localmente.

Figura 25- Informações de mensagens de serviço armazenadas no BD do DicomFlow

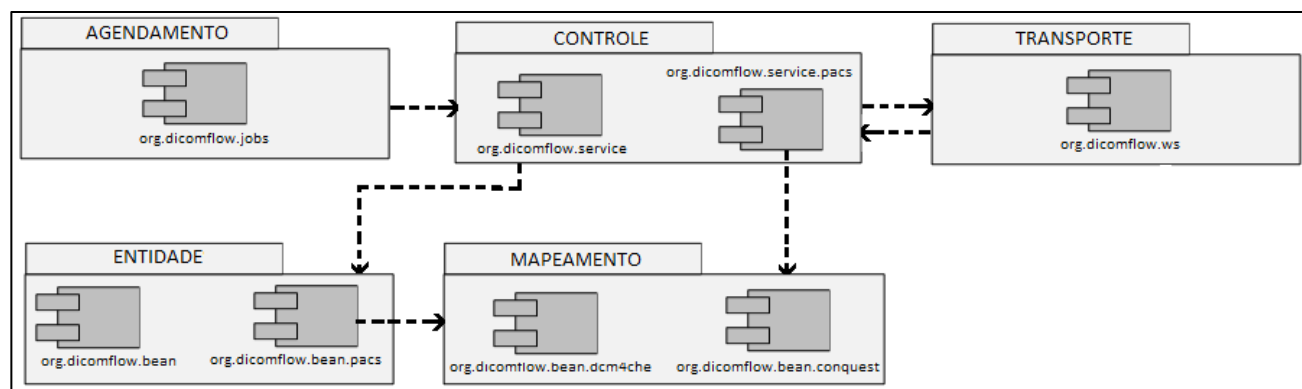


Fonte: Próprio autor.

Conforme ilustra a Figura 25, as mensagens enviadas pelos *gateways* do PACS I e II são recebidas pelo *gateway* do PACS III, que recupera as estruturas XML contidas nessas mensagens e armazena no Banco de dados do próprio *gateway*. Esse banco de dados funciona como o ator **Registry** especificado nos perfis XDS e XDS-I.

O DicomMove utiliza a linguagem de programação JAVA em sua codificação, mais especificamente a arquitetura J2EE para desenvolvimento de sistemas WEB, que fornece suporte à tecnologia HTTPS e REST. A estrutura desse módulo também está organizada em pacotes (Figura 26).

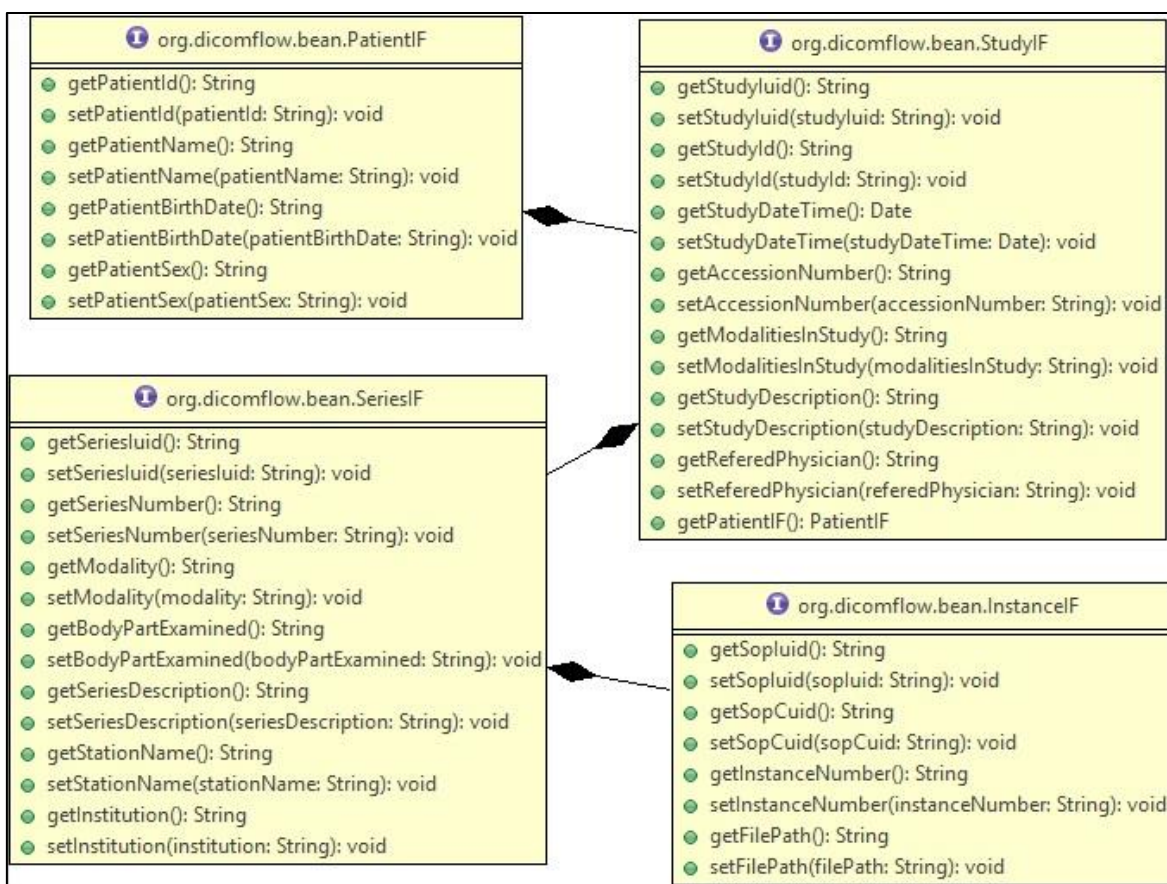
Figura 26 - Pacotes do módulo DicomMove



Fonte: Próprio autor.

Conforme descrito na seção 4.4, a escolha da forma como observar a infraestrutura PACS/DICOM não é definida no protocolo proposto, dessa forma, o módulo DicomMove propõe um monitoramento via banco de dados e implementa um pacote responsável por observar as mudanças do estado atual do banco de dados da infraestrutura PACS/DICOM, o pacote **Entidade**. Esse é implementado utilizando o framework Hibernate para realizar o mapeamento do banco de dados do Servidor PACS em objetos relacionais (ORM – *Object-relational mapping*) escritos na linguagem JAVA. Assim, é possível utilizar consultas baseadas em linguagem SQL e verificar se houve inserção de novos registros de exames no banco de dados do servidor PACS.

Figura 27 - Interfaces do pacote Entidade



Fonte: Próprio autor.

Ainda, como explicado na seção 2.2, as infraestruturas PACS possuem arquiteturas variadas, sendo assim, um conjunto de interfaces foi acrescentado ao pacote Entidade para atender as variações de banco de dados dos servidores dessas infraestruturas (Figura 27). As interfaces seguem a hierarquia estrutural dos

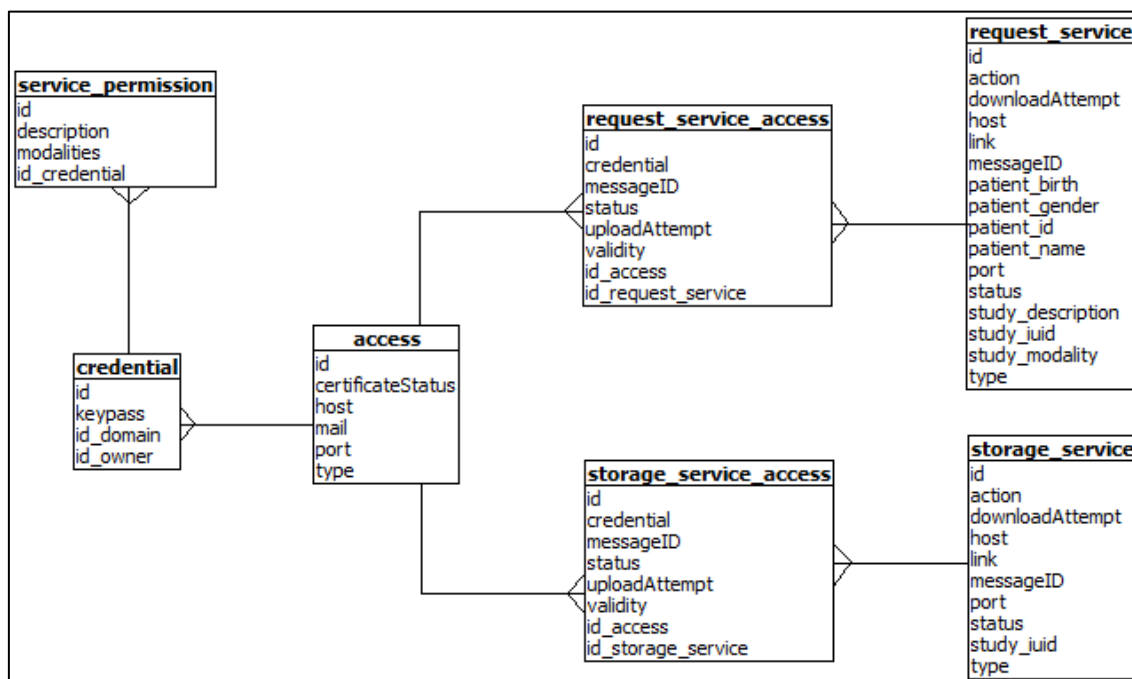
objetos DICOM (Paciente > Estudo > Serie > Instância) (Pianykh, 2012) e mapeiam seus principais atributos. Ainda, foi criado o pacote **Mapeamento**, contendo classes ORM que implementam essas interfaces e representam as tabelas dos bancos do DCM4CHEE e do CONQUEST, servidores PACS amplamente difundidos e utilizados. Por fim, o pacote Entidade também possui classes ORM que implementam o banco de dados do DicomFlow para armazenar os registros de informações das mensagens de serviço. A Figura 28, logo abaixo, ilustra as classes que mapeiam as tabelas para armazenamento de informações de mensagens de serviço **Request** e **Storage**. As demais mensagens de serviço têm classes com a mesma estrutura, variando algumas poucas propriedades.

Figura 28 - Classes ORM das mensagens de serviço



Fonte: Próprio autor.

Figura 29 - Diagrama Entidade Relacionamento (ER) do DicomFlow



Fonte: Próprio autor.

O diagrama de Entidade relacionamento presente na Figura 29 ilustra as tabelas e os relacionamentos que as classes apresentadas anteriormente mapeiam. Ainda, existem as tabelas **access**, **credential** e **service_permission**, para armazenar informações de controle de permissão para acesso as imagens durante o resgate de imagens médicas. Mais adiante será mostrado o mecanismo para resgate e como essas informações são utilizadas.

Por sua vez, o pacote **Controle** contém classes para gerenciar as consultas SQL no banco de dados do PACS, a fim de monitorar o estado atual desse. Dessa forma, juntamente com as classes que implementam as interfaces para a estrutura hierárquica dos objetos DICOM, o pacote **Mapeamento** contém dois conjuntos de classes de consulta SQL implementadas para cada um dos dois tipos de bancos dos servidores DCM4CHE e CONQUEST. Neste caso, o conjunto de classes de responsáveis pelas consultas SQL constituem o que denominamos de **serviço de gerência de BD PACS**. Existe outro serviço de gerência de banco no pacote Controle, o **serviço de gerência de BD DicomFlow**, funciona de forma análoga ao serviço de gerência citado anteriormente e é responsável pelo controle das informações de mensagens de serviço enviadas e recebidas, mantidas no banco de dados do DicomFlow. Ainda, há o **serviço de gerência de certificados digitais** que controla o armazenamento e manutenção dos certificados digitais trocados

através das mensagens de serviço **Certificate**. Esse serviço é responsável por resgatar o certificado digital associado ao destinatário e fornecê-lo durante a criação de mensagens de serviço a serem enviadas, como também é responsável por verificar a veracidade do certificado digital do solicitante, durante o resgate de imagens médicas. Continuando, o **serviço de gerência de URL** também se encontra no pacote Controle, ele define o formato das URL de resgate dos exames que é enviada nas mensagens de serviço, ou seja, quando solicitado esse serviço cria a URL utilizando os identificadores das imagens, o domínio onde o DicomMove está hospedado e o caminho padrão do webservice de resgate de imagens médicas, que falaremos mais adiante. Já o **serviço de gerência de mensagens** é o pacote que utiliza o módulo DicomMessage para criar as mensagens de serviço de acordo com as políticas de envio definidas em um arquivo de configuração. O arquivo de configuração de envio de mensagens, através de uma linguagem baseada em expressões regulares, armazena os destinatários das mensagens e define que tipos de mensagens de serviço aquele destinatário pode receber. Dessa forma, quando o estado atual do banco muda e um novo exame de imagem é inserido, as políticas de envio são verificadas e as mensagens são enviadas.

Figura 30 - Expressão regular de envio de mensagem



```
IN#radiologista1@domain1.com#domain1.com#Storage CT,MR
OUT#radiologista2@domain.com#domain.com#Request *
```

Fonte: Próprio autor.

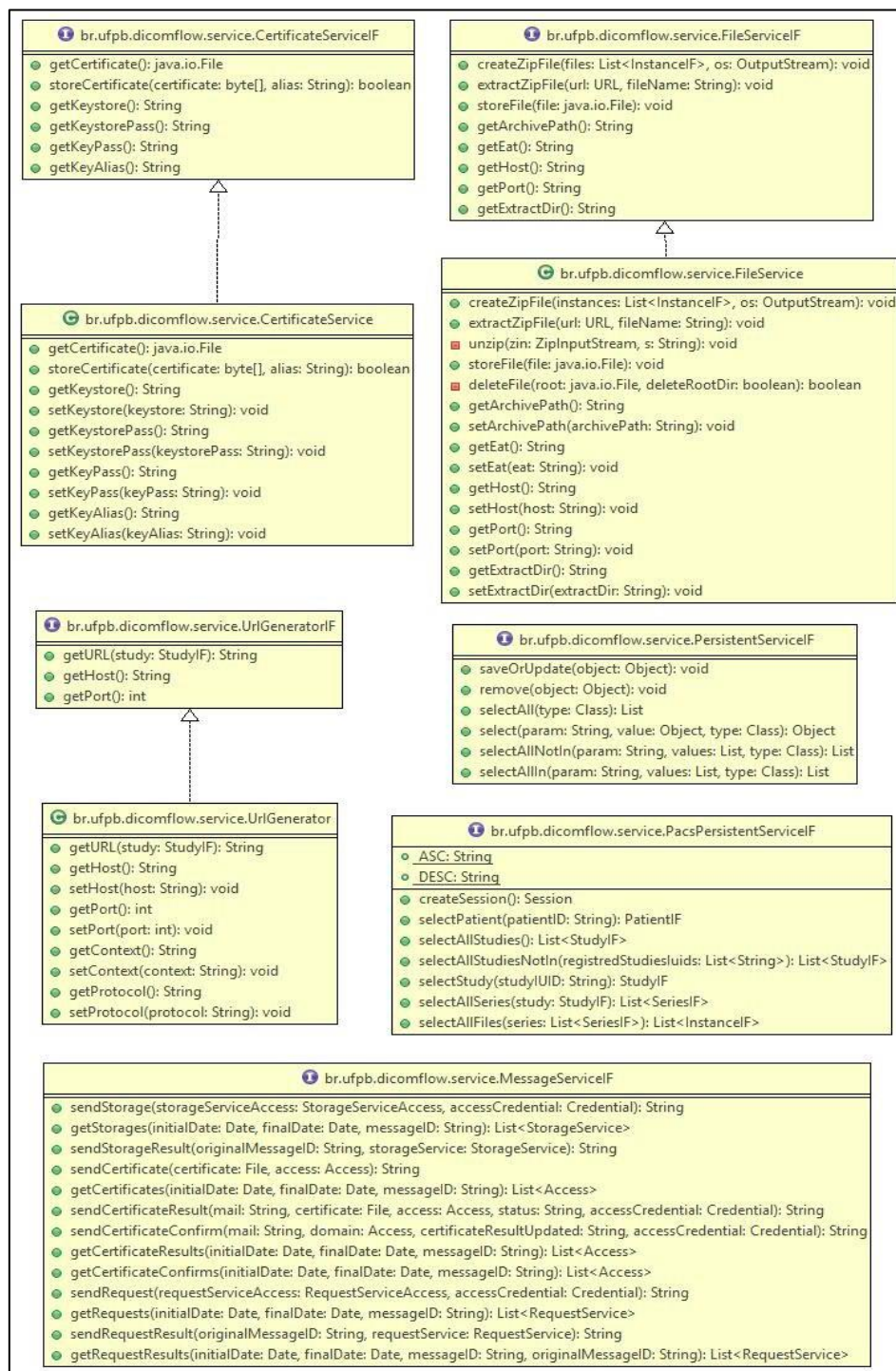
A Figura 30 apresenta um exemplo de arquivo de configuração de envio de mensagens, a primeira linha indica que serão lidas mensagens de serviço **Storage**, contendo informações de imagens de tomografia computadorizada (**CT**) ou ressonância magnética (**MR**) do e-mail radiologista@domain1.com, pertencente ao domínio domain1.com. A segunda linha indica que serão enviadas mensagens de serviço Request, contendo informações de qualquer tipo de imagens para o e-mail radiologista2@domain.com, pertencente ao domínio domain.com.

Por fim, existe o **serviço de gerência de arquivos**, utilizado pelo webservice, para compactar os exames de imagens durante o resgate de imagens médicas, e usado pelo solicitante, para descompactar e enviar as imagens para o servidor PACS. As imagens envolvidas na transferência são compactadas

utilizando o algoritmo de compressão sem perdas DEFLATE, com base no algoritmo L77, simples de implementar e largamente utilizado.

A Figura 31 apresenta as interfaces de todos os serviços e as principais classes que implementam esses serviços.

Figura 31 - Interfaces e classes do pacote Controle



Fonte: Próprio autor.

Continuando a apresentação da estrutura de pacotes do DicomMove, temos o pacote **Agendamento**. Composto por um conjunto de classes que desenvolvidas sobre o conceito de Threads JAVA, ou seja, são classes que executam um conjunto de instruções de forma independente em simultâneo à execução de outras classes. Através desse conceito, foi possível separar e construir uma classe para cada etapa dos dois principais fluxos do módulo DicomMove, dessa forma, conseguimos fragmentar os fluxos de monitoramento da infraestrutura PACS/DICOM para envio de mensagens e os fluxos de resgate de imagens médicas. Ainda, utilizando o Framework Spring, foi possível definir gatilhos de execução (*Triggers*) para cada classe, ou seja, através de arquivo de configuração é possível definir os momentos em que cada etapa dos fluxos deve ser executada. As classes desse pacote fazem uso das classes de serviços do pacote Controle.

Figura 32 - Classes do pacote Agendamento

The diagram illustrates the structure of the `org.dicomflow.job` package and its configuration in Spring XML.

Class: `org.dicomflow.job.PrepareRequests`

- Attributes: `DAILY_STRATEGY: String`, `INTERVAL_STRATEGY: String`, `CURRENT_STUDY_STRATEGY: String`
- Fields: `initialDate: String`, `finalDate: String`, `modalities: String`, `strategy: String`
- Methods: `execute(): void`, `insertRegistries(accesses: List<Access>): void`, `getStudies(): List<StudyIF>`, `verifyAccess(access: Access, study: StudyIF, serviceType: String): boolean`

Spring XML Configuration for `PrepareRequests`:

```
<bean id="prepareRequestsJob" class="org.dicomflow.job.PrepareRequests"/>
<bean id="prepareRequestsCronTrigger" class="org.springframework.scheduling.quartz.CronTriggerBean">
  <property name="jobDetail" ref="prepareRequestsJob"/>
  <property name="cronExpression" value="0 * * * * ?"/>
</bean>
```

Annotations: "Classe da etapa do fluxo de monitoramento do BD PACS" (pointing to the class name), "Agendamento da execução da etapa" (pointing to the cron expression).

Class: `org.dicomflow.job.SendRequests`

- Method: `execute(): void`

Spring XML Configuration for `SendRequests`:

```
<bean id="sendRequestsJob" class="org.dicomflow.job.SendRequests"/>
<bean id="sendRequestsCronTrigger" class="org.springframework.scheduling.quartz.CronTriggerBean">
  <property name="jobDetail" ref="sendRequestsJob"/>
  <property name="cronExpression" value="0 * * * * ?"/>
</bean>
```

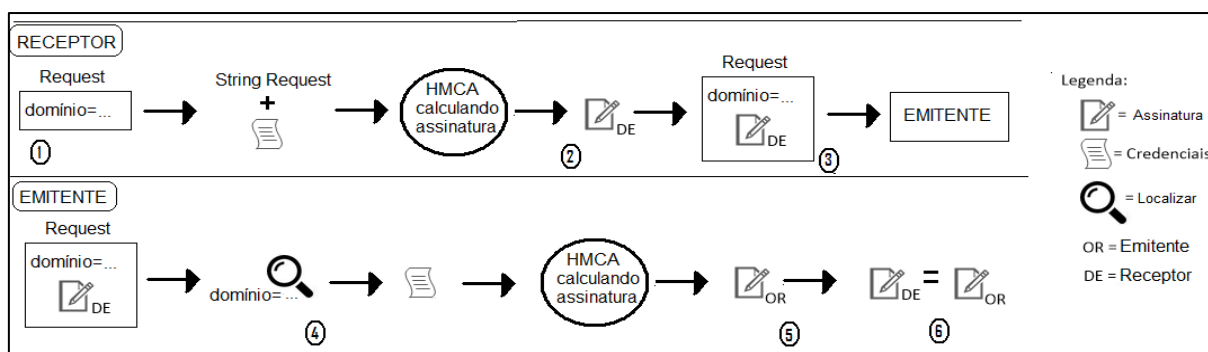
Fonte: Próprio autor.

A Figura 32 ilustra um exemplo de classes e suas configurações. As classes aqui listadas representam duas das etapas do fluxo de monitoramento do estado atual do Banco de dados do servidor PACS. A classe **PrepareRequests** prepara

informações para envio, ela utiliza o serviço de **gerenciamento de BD PACS** para resgatar os exames recém inseridos e utiliza o serviço de **gerenciamento do BD DicomFlow** para armazenar as informações que irão compor a mensagem de serviço **Request**. Por sua vez, a classe `SendRequest`, envia as mensagens, utilizando os serviços de **gerenciamento de certificados**, **de gerenciamento de URL** e **de gerenciamento de mensagens** para esse fim.

Concluindo, o pacote de **Transporte** é responsável pelo controle da transferência das imagens médicas, as classes contidas nesse pacote utilizam a API Jersey para implementar o *Web Services* totalmente baseado no conceito REST (*Web Service RESTful*), que permite o receptor das mensagens de serviço recupere as imagens através de requisição via URL. O pacote faz uso do serviço de **gerência de arquivo** para permitir que o emissor das mensagens de serviço possa compactar e enviar as imagens. Mas primeiro, o pacote verifica quem é o receptor da mensagem de serviço que originou requisição, utilizando o certificado digital para isso, a comunicação é feita de forma segura através do protocolo TLS (*Transport Layer Security*). O serviço de **gerência de certificados** é usado nessa etapa para leitura e verificação dos certificados digitais. Em seguida, é verificado através das credenciais se o acesso é permitido para o receptor da mensagem de serviço. Então, se todas as etapas anteriores forem verificadas sem problemas, a transferência das imagens é liberada pelo emissor. A implementação do mecanismo de controle acesso aos exames de imagem baseia-se na documentação da *Amazon Web Services* (AWS) para solicitações de autenticação com REST (AMAZON, 2017).

Figura 33 - mecanismo de controle de acesso às imagens



Fonte: Próprio autor.

O mecanismo ilustrado na Figura 33 funciona da seguinte forma: A transferência inicia após o receptor resgatar a URL e a credencial da mensagem de serviço. Então, (1) o receptor prepara uma Request HTTPS, é colocado o domínio do receptor no cabeçalho dessa requisição. (2) a Assinatura de verificação é calculada com HMAC-SHA1 (RFC 2104) usando a representação textual (String) do cabeçalho concatenada com a credencial. (3) a assinatura é adicionada ao cabeçalho da requisição que é enviada para o emissor da mensagem de serviço. (4) O emissor recebe a requisição e utiliza o domínio presente no cabeçalho para localizar a credencial correspondente. Após localizar a credencial, (5) O emissor calcula com HMAC-SHA1 a assinatura de verificação. (6) O emissor compara a assinatura calculada com a assinatura recebida na requisição. A requisição é liberada se as assinaturas forem idênticas.

4.5. Considerações finais

Esse capítulo discutiu as abordagens realizadas para elaboração do DicomFlow, uma solução em forma *gateway* que contorna as limitações presentes nas infraestruturas atuais, frequentemente observadas na literatura, e cultiva a formação de uma infraestrutura de informação telerradiológica global. Foram percorridos sobre os principais componentes concebidos/desenvolvidos, bem como a arquitetura simplificada, em alto nível.

O desenvolvimento do Dicomflow, seguindo os conceitos da teoria de projeto, contemplou uma série de características necessárias em uma infraestrutura de informação aberta, compartilhada e descentralizada, abordando desde definição de uma linguagem comum para comunicação, passando pela seleção de tecnologias não proprietárias e amplamente difundidas, até mecanismos para comunicação assíncrona, assimétrica e ponto-a-ponto entre os diversos elementos do ambiente distribuído. Também foram consideradas características concernentes a problemas legais e de privacidade desde os fundamentos da pesquisa, tendo sido desenvolvidos métodos para o sigilo dos dados com o uso das boas práticas das tecnologias de criptografia e *Web Services*. O DicomFlow atua como *gateway* de comunicação entre a infraestrutura PACS/DICOM e a Internet, mantendo-se a borda da primeira não interferindo no fluxo de trabalho da organização. Uma vasta variedade de tecnologias e serviços foi utilizada, tendo em vista cobrir cada objetivo proposto. Entre as tecnologias utilizadas, e não discutidas no decorrer deste capítulo, pode-se citar: *Container* Java Apache Tomcat, *toolkit* de comunicação DICOM do DCM4CHE e os Banco de dados MySQL e Postgres. Vale ressaltar que o protocolo do DicomFlow é aberto, sendo livre seu uso, e a implementação do DicomFlow é de referência.

5. Experimentos

Esse capítulo tem por objetivo apresentar a validação do DicomFlow tanto em ambiente simulado quanto em ambiente real. Para isso, foi verificada a composição dos elementos construídos em conjunto com as tecnologias empregadas, assim, nesse primeiro momento, em ambiente simulado, foi analisado o funcionamento dos fluxos de comunicação e transferência de imagens médicas do DicomFlow, ao passo que foi verificada a capacidade de o *gateway* recuperar-se de possíveis desvios nesses fluxos e manter-se funcionando corretamente. Em seguida, o *gateway* foi introduzido e monitorado em um cenário real, para validação de seu uso em um fluxo de trabalho de uma infraestrutura de telerradiologia.

O restante desse capítulo está organizado da seguinte forma: A seção 5.1 descreve três experimentos efetuados em ambiente simulado, o cenário elaborado para esses testes e os resultados obtidos. A seção 5.2 descreve dois experimentos em ambiente real no qual o *gateway* foi introduzido, o ambiente e o fluxo de trabalho que ele deve atender e os resultados obtidos. Por fim, a seção 5.3 traz algumas considerações finais sobre os experimentos.

5.1. Testes de viabilidade técnica

Os experimentos descritos a seguir visaram avaliar de forma preliminar a infraestrutura proposta quanto a sua viabilidade técnica e operacional dos fluxos de comunicação e de transferência de imagens. Além de verificar a capacidade de funcionamento do *gateway*, foram avaliadas a capacidade de composição e comunicação entre as tecnologias empregadas, principalmente as tecnologias de e-mail e HTTP. O objetivo principal foi localizar os principais pontos críticos de interconexão entre essas tecnologias e fornecer elementos que permitam diminuir a complexidade de comunicação, dotar de maior flexibilidade sua composição e manter o funcionamento contínuo da solução proposta. Para isso, foram realizados três experimentos: A) Avaliação de performance na distribuição de imagens; B) Sincronização de PACS entre entidades; C) Associação de uma nova entidade à rede. Antes de descrever os como foram realizados os experimentos (seção 5.1.2), será apresentado o ambiente de execução elaborada para a realização (seção 5.1.1). A seção 5.1.3 expõe os resultados obtidos sobre o experimento.

5.1.1. Ambiente de execução para viabilidade técnica

Baseado no fluxo de distribuição e nas principais entidades presentes nos cenários de uso elaborados no capítulo 4.3, foi idealizado um ambiente composto por três computadores interconectados às margens de uma rede metropolitana (MAN) com capacidade de 5Mbps/s, distando 5Km entre si e protegidos por *firewalls*. As máquinas representam servidores de armazenamento de imagens médicas, como os encontrados nos sistemas PACS de hospitais e clínicas. Em cada uma das máquinas, foi instalado o sistema de gerenciamento de imagens DCM4CHEE e seu toolkit, o Banco de Dados PostgreSQL e MySQL, Java Virtual Machine (JMV), os servidores de aplicações JBOSS e TOMCAT como plataformas web para o DCM4CHE e o *gateway* DicomFlow, respectivamente. A configuração das máquinas pode ser vista na Tabela 7. As mensagens do protocolo de serviços dos DicomFlow foram trocadas através do servidor de e-mail Gmail. Não houve alterações nas configurações de *firewall*, visto que o DicomFlow utiliza as portas padrão tipicamente liberadas para os protocolos HTTP e de e-mail.

Tabela 7 - Especificações dos servidores de imagens.

Recurso	Máquina 1	Máquina 2	Máquina 3
CPU	Intel I3 2.13 Ghz x2	Intel Core2 Duo 2.11Ghz x2	AMD Athlon 2.11Ghz x2
Memória	DDR2 667Mhz 4GB	DDR2 667Mhz 4GB	DDR2 667Mhz 4GB
OS	Windows 10	Windows Vista	Ubuntu 16.05
JVM	versão 1.7.x+JDK	versão 1.7.x+JDK	versão 1.7.x+JDK
BD	Postgres 8.3	MySQL 5.1	MySQL 5.1
DCM4CHEE	versão 2.18.x	versão 2.17.x	versão 2.18.x
DCM4CHEToolkit	versão 2.0.23	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

Fonte: Próprio autor.

As etapas configuradas nos fluxos executados pelo DicomFlow nos servidores incluem: Monitoração do banco de dados do DCM4CHEE para envio dos serviços aos interessados quando da chegada de novos exames pelo PACS; Acesso ao diretório de armazenamento de imagens, para envio dos objetos DICOM quando requisitados; Armazenamento de objetos DICOM no DCM4CHEE quando baixados os exames. Os objetos DICOM envolvidos nos experimentos contêm imagens de Tomografias Computadorizadas (CT) e o exame utilizado contém 360 imagens de CT, proveniente do repositório Osirix (OSIRIX, 2017). Vale ressaltar que os exames foram atualizados apenas para fins de pesquisa, conforme as políticas de uso impostas pela empresa detentora da imagem (OSIRIX, 2017). O exame foi replicado 80 vezes para ser utilizado nestes experimentos. O total de exames e o total de arquivos XML dos serviços enviados por mensagem em cada experimento podem ser vistos na Tabela 8.

Tabela 8 - Exames e arquivos XML empregados no experimento.

Arquivo	Tamanho unitário	Quantidade utilizada	Tamanho Total
Exame de CT	32,4MB	80	2,53GB
XML de Serviços	1KB	160	160KB

Fonte: Próprio autor.

5.1.2. Especificação dos experimentos de viabilidade técnica

O experimento A (avaliação de desempenho de distribuição de imagens) objetivou testar o desempenho e a capacidade de carga do DicomFlow através da transferência concorrente de exames da **máquina 2** para a **máquina 1**. O experimento ocorreu da seguinte forma: foram introduzidos 10 exames no DCM4CHEE da **máquina 2** através do toolkit, em seguida foi inserido o endereço de e-mail da **máquina 1** no DicomFlow da **máquina 2** e, por fim, foram iniciadas as aplicações de ambas as máquinas nos respectivos servidores web. Na **máquina 1**, foi medido o tempo total de transferência dos 10 exames. Na **máquina 2**, foi medido o tempo de atendimento às requisições de transferência. Foram executadas dez repetições do experimento e o teste foi reproduzido com 20, 30 e 60 exames.

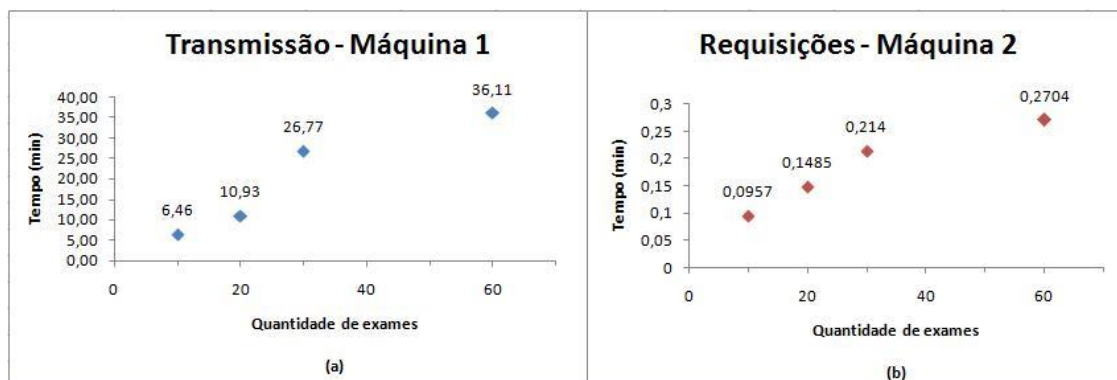
O experimento B (sincronização de PACS entre entidades) teve o objetivo de aferir a capacidade de sincronização de exames entre a **máquina 1** e a **máquina 2**. Foram introduzidos 10 exames no DCM4CHEE de ambas as máquinas através do toolkit, logo após foi inserido o endereço de e-mail da **máquina 2** no DicomFlow da **máquina 1** e vice-versa. Depois, as aplicações de ambas as máquinas foram iniciadas em seus respectivos servidores web. Em cada máquina foi medido o tempo de transferência desses exames, de acesso ao BD do DCM4CHEE, de escrita dos objetos no DCM4CHEE e de envio e leitura de mensagens de requisição de arquivamento (**Storage-Save**). Este processo foi repetido 3 vezes. Por fim, o teste foi reproduzido para a sincronização de 20 e 40 exames.

Por fim, o experimento C (associação de uma nova entidade à rede) teve o propósito de testar o crescimento da arquitetura com a inclusão da **máquina 3** à rede. Esse teste foi efetuado logo após o término do experimento B e ocorreu da seguinte forma: o endereço de e-mail da **máquina 3** foi inserido no DicomFlow da **máquina 1** e da **máquina 2**, então, foi iniciada a aplicação da máquina 3 em seu servidor web. Foi mensurado na **máquina 3** o tempo total de transferência dos exames contidos nas demais. Todo o processo foi repetido 3 vezes com 10, 20 e 40 exames inclusos nas máquinas 1 e 2.

5.1.3. Resultados do experimento de viabilidade técnica

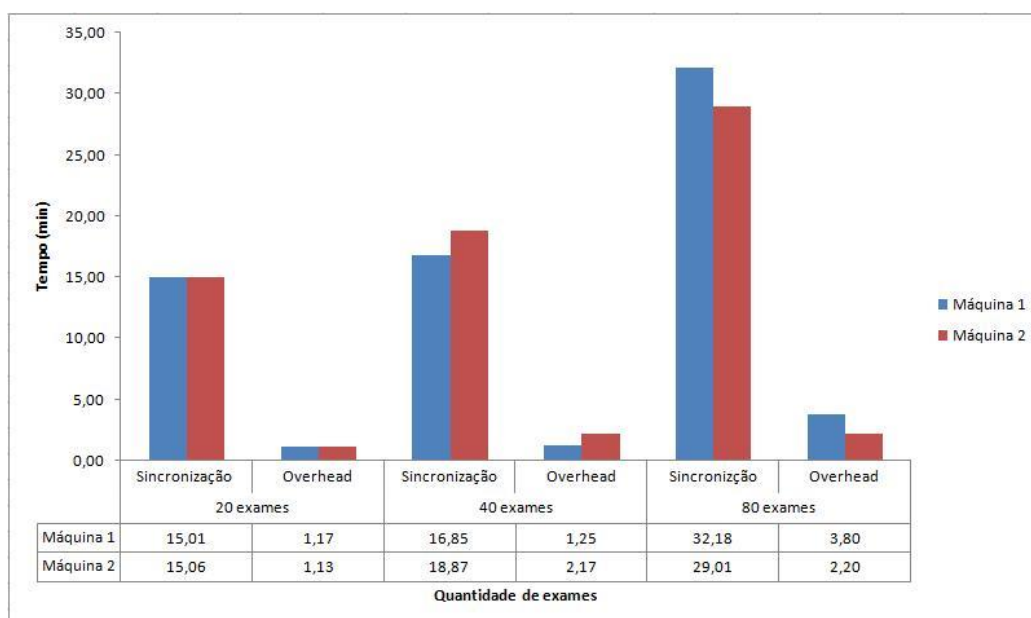
Os resultados apresentados a seguir são de métricas colhidas dos experimentos efetuados para a verificação da viabilidade técnica do DicomFlow. O gráfico (a) (Figura 34) mostra o tempo médio das transferências de exames efetuados pela máquina 1. O gráfico (b) (Figura 34) apresenta o tempo médio de atendimento da máquina 2 às requisições de transferências.

Figura 34 - Tempo médio de transmissão (a) e requisição (b) por quant. de exames



Fonte: Próprio autor.

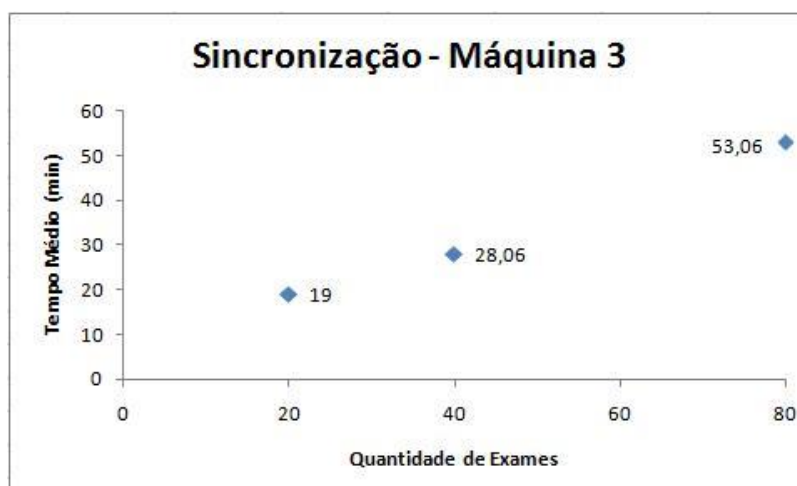
Figura 35 - Tempo médio de sincronização entre as Máquinas 1 e 2.



Fonte: Próprio autor.

O histograma na Figura 35 apresenta o tempo médio de sincronização e o overhead originado pelo processamento de controle nas transferências efetuadas pelas máquinas 1 e 2. O gráfico na Figura 36 ilustra o tempo médio total utilizado pela máquina 3 para sincronizar os estudos contidos nas máquinas 1 e 2. O eixo horizontal mostra o somatório dos exames contidos em cada uma das demais máquinas.

Figura 36 - Tempo médio de sincronização máquina 3.



Fonte: Próprio autor.

5.2. Testes de implantação do *gateway*

A implantação do gateway visou avaliar o comportamento do DicomFlow quanto ao desempenho e efetividade dos fluxos de comunicação e de transferência de imagens em um ambiente telerradiológico real. O objetivo principal foi verificar a flexibilidade de adaptação da solução proposta em ambientes distintos, ao passo que mantém a capacidade de funcionamento semelhante para ambos os ambientes. Para isso, foram realizados dois experimentos: A) Avaliação da distribuição de imagens para armazenamento em um repositório externo; B) Avaliação da distribuição de imagens para emissão de laudos. A seção 5.2.1 descreve o ambiente de execução e a seção 5.2.2 especifica cada um dos experimentos. Os resultados do experimento são apresentados na seção 5.2.3.

5.2.1. Ambiente de implantação do *gateway*

Para o experimento A, o ambiente real de execução foi constituído de um servidor de armazenamento de imagens médicas mantido na infraestrutura telerradiológica do Centro de Ciências das Imagens e Física Médica da Faculdade de Medicina de Ribeirão Preto (CCIFM-FMRP), Universidade de São Paulo (USP). Esse servidor, denominado **Servidor 1**, possui o sistema de gerenciamento de

imagens CONQUEST, o Banco de Dados MySql, Java Virtual Machine (JMV), o servidor de aplicações TOMCAT como plataforma web para o *gateway* DicomFlow. Outro servidor de armazenamento foi mantido na Infraestrutura de TI da Superintendência de Tecnologia da Informação da Universidade Federal da Paraíba (STI-UFPB), esse servidor, denominado **Servidor 2**, possui o sistema de gerenciamento de imagens DCM4CHEE e seu toolkit, o Banco de Dados MySql, Java Virtual Machine (JMV), os servidores de aplicações JBOSS e TOMCAT como plataformas web para o DCM4CHE e o *gateway* DicomFlow, respectivamente. Por fim, as mensagens de solicitação de armazenamento e suas respostas foram trocadas através do servidor de e-mail Gmail. Não houve alteração nas configurações de *firewall* de ambos os ambientes. A configuração das máquinas pode ser vista na Tabela 9.

Tabela 9 - Configuração do ambiente do experimento A

Recurso	Servidor 1	Servidor 2
CPU	Intel Xeon E5-2620 v2 2.10GHz	AMD PRO A8-8600B R6, 10 Compute cores 4C+6G 1.60GHz
Memória	DDR2 667Mhz 32GB	DDR2 667Mhz 16GB
OS	Debian 7.6	Windows 10 Pro
JVM	Versão 1.7.x+JDK	Versão 1.7.x+JDK
BD	MySQL 5.1	MySQL 5.1
CONQUEST	Versão 1.4.19	-
DCM4CHEE	-	Versão 2.17.x
DCM4CHEToolkit	-	Versão 2.0.29
DICOMFLOW	Versão 1.2	Versão 1.2
JBOSS	-	Versão 4.2.3.GA
Tomcat	Versão 7.0.29	Versão 7.0.29

Fonte: Próprio autor

As etapas configuradas nos fluxos executados pelo DicomFlow no **Servidor 1** incluem: Monitoramento do banco de dados do CONQUEST para envio das

mensagens de serviços aos interessados quando da chegada de novos exames; Acesso ao diretório de armazenamento de imagens, para envio dos objetos DICOM quando requisitados. Por outro lado, os fluxos configurados no **Servidor 2** incluem: Leitura de mensagens de serviço que requisitam armazenamento e armazenamento de objetos DICOM no DCM4CHEE, quando baixados os exames. Os objetos DICOM envolvidos nos experimentos contêm imagens de ultrassonografia (US).

Para o experimento B, o ambiente real de execução foi constituído de um servidor de armazenamento de imagens médicas mantido na infraestrutura telerradiológica da Clínica Radiológica de Patos. Esse servidor, denominado **Servidor 3**, possui o sistema de gerenciamento de imagens DCM4CHE, o Banco de Dados MySql, Java Virtual Machine (JMV), o servidor de aplicações TOMCAT como plataforma web para o *gateway* DicomFlow. Foi utilizado 1 computador para atender as mensagens de requisição de laudo, denominado **Computador 1**. As mensagens do protocolo de serviços dos DicomFlow foram trocadas através do servidor do Gmail. A configuração das máquinas pode ser vista na Tabela 10.

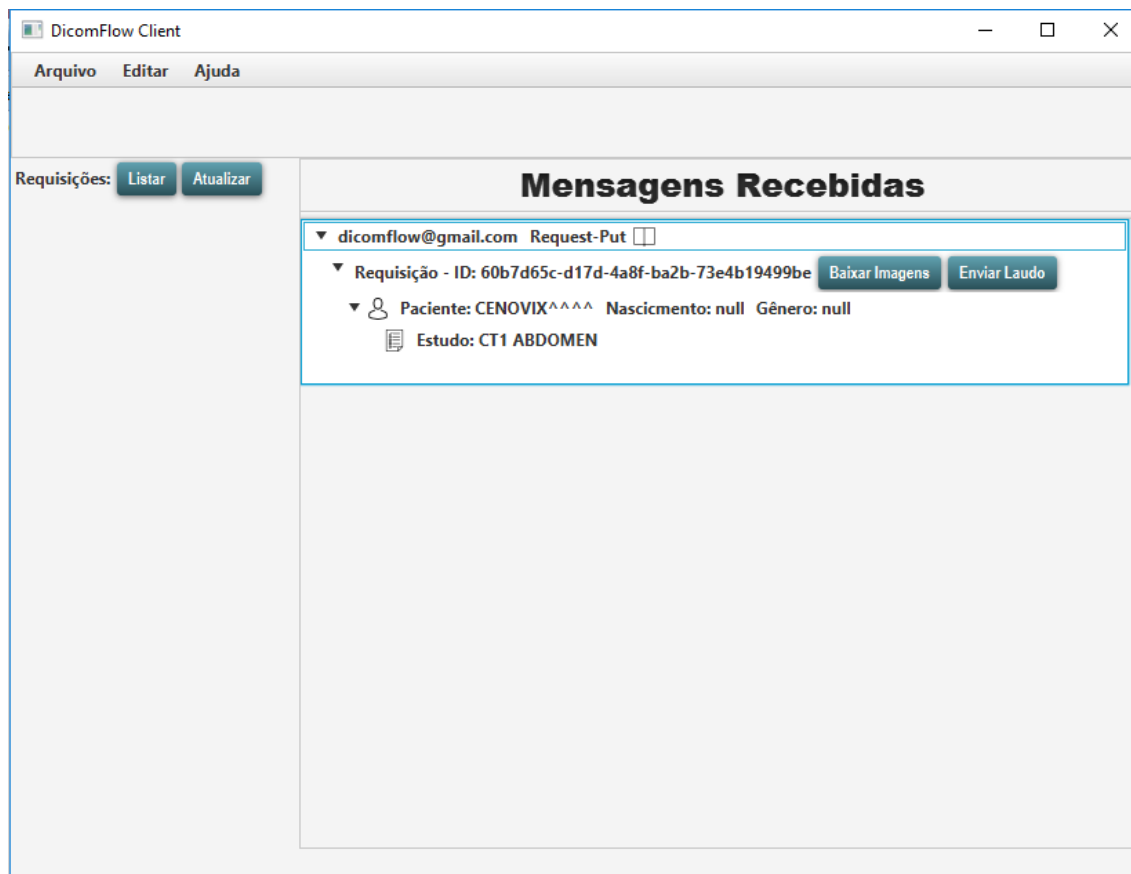
Tabela 10 - Configuração do ambiente do experimento B

Recurso	Servidor 3	Computador 1
CPU	Intel Xeon E5-2620 v2 2.40GHz	Intel Core i5 7ª geração 2.7GHz
Memória	DDR2 667Mhz 4GB	DDR2 667Mhz 8GB
OS	Ubuntu v2.6.38	Windows 10 Home
JVM	Versão 1.6.x+JDK	Versão 1.7.x+JDK
BD	MySQL 5.1	MySQL 5.1
DCM4CHEE	Versão 2.16.x	Versão 2.17.x
DCM4CHEToolkit	Versão 2.0.29	Versão 2.0.29
DICOMFLOW	Versão 1.2	Versão 1.2
JBOSS	Versão 4.2.3.GA	Versão 4.2.3.GA
Tomcat	Versão 7.0.29	Versão 7.0.29

Fonte: Próprio autor

Para complementar o ambiente do experimento, foi desenvolvida uma aplicação cliente, mantida no **Computador 1**. A aplicação apresenta as informações das mensagens de requisição de emissão de laudo e possibilita o resgate das imagens médicas e o envio dos respectivos laudos médicos. A Figura 37 apresenta a *interface* da aplicação.

Figura 37 - Interface da aplicação cliente



Fonte: Próprio autor

A aplicação cliente não requer nenhuma instalação de software adicional, ela possui em sua implementação banco de dados embarcado e todas as bibliotecas necessárias para criptografia e envio de mensagens, armazenamento de certificados digitais, abertura de conexão e download das imagens. Toda implementação seguiu as diretrizes do protocolo do DicomFlow. Ainda, toda a configuração necessária é feita através de sua interface. Para seu uso é necessário ter a versão 1.8 do JAVA. Por fim, a aplicação não requer alterações das

configurações de firewall do computador. Os demais recursos mínimos são: 1.6GHz de CPU, 4GB de Memória RAM, independentemente do sistema operacional.

As etapas configuradas nos fluxos executados pelo DicomFlow no **Servidor 3** incluem: Monitoramento do banco de dados do DCM4CHEE para envio das mensagens de serviços aos interessados quando da chegada de novos exames; Acesso ao diretório de armazenamento de imagens, para envio dos objetos DICOM quando requisitados. Por outro lado, os fluxos configurados na aplicação cliente incluem: Leitura de mensagens de serviço que requisitam emissão de laudo, resgate das imagens e envio de laudos.

5.2.2. Especificação dos experimentos de implantação do *gateway*

O experimento A (avaliação da distribuição de imagens para armazenamento em um repositório externo) objetivou testar o desempenho e a capacidade de carga do DicomFlow e de recuperação de possíveis exceções causadas pelo ambiente, através da transferência concorrente para armazenamento de exames adquiridos em tempo real do Servidor 1 para o Servidor 2. O experimento ocorreu da seguinte forma: foi adicionado o endereço de e-mail do Servidor 2 no Servidor 1, que adquire exames e armazena no CONQUEST, o gateway DicomFlow do Servidor 1 monitora o Banco de dados do CONQUEST e, ao verificar a inserção do novo exame de medicina nuclear, envia uma mensagem de solicitação de armazenamento para o Servidor 2, que possui um gateway DicomFlow monitorando as mensagens de solicitação e armazenando os exames no DCM4CHEE. Os gateways foram mantidos ativos durante 8 horas consecutivas.

O experimento B (avaliação da distribuição de imagens para emissão de laudos) objetivou testar o desempenho e a capacidade do DicomFlow em atender diversos fluxos concorrentes de direcionamento de mensagens e transferência de imagens das imagens de exames adquiridos em tempo real pelo servidor 3. O experimento ocorreu da seguinte forma: foram adicionados no DicomFlow do servidor 3 os endereços de e-mail dos usuários envolvidos. O *gateway* envia mensagens de solicitação de laudo para os e-mails dos médicos envolvidos. Os computadores dos usuários possuem aplicações clientes configuradas com seus e-mails, essas aplicações monitoram as mensagens de solicitação de laudo.

5.2.3. Resultados da implantação do gateway

Durante os experimentos de implantação da solução proposta nos dois ambientes de produção, não foram colhidas métricas nos testes, que ocorram em tempo real. O primeiro motivo foi para não sobrecarregar os sistemas em produção nos ambientes envolvidos nos testes. O Segundo motivo é que os testes objetivaram verificar o correto funcionamento e a capacidade de recuperação do gateway em situações de exceção e comportamentos inesperados que geralmente são observados em ambientes de produção reais. Ainda assim, alguns dados puderam ser observados. No experimento A, os gateways se mantiveram ativos **durante as 8 horas** consecutivas e foram trocadas **426 mensagens de serviços** entre solicitações e respostas às solicitações. E mais, foram transferidos um total de **213 exames de imagem**, totalizando um tráfego de aproximadamente **2,5 Giga Bytes**. Por outro lado, o experimento B envolveu o DicomFlow do **Servidor 3** e a aplicação cliente do **Computador 1**. Esse experimento teve **duração de 12 horas**, foram enviados ao cliente **157 mensagens de requisição de laudos** e transferidos **157 exames de radiografia computadorizada (CR)**, totalizando aproximadamente **3,1 Giga Bytes** de tráfego.

5.3. Considerações finais

Os experimentos empregados possibilitaram descobrir as mudanças necessárias nos aspectos técnicos e sociais empregados, para melhorar as diretrizes do protocolo e a implementação do código do DicomFlow. Através dos experimentos de viabilidade técnica foi possível aprimorar o uso das tecnologias adotadas e até mesmo a substituição de algumas, a fim de diminuir a complexidade da solução, por exemplo, substituição de criptografia baseada em PGP (*Pretty Good Privacy*) por S/MIME, tendo em vista que o segundo possui diretrizes de criptografia direcionado para mensagens de e-mail. Ainda, através dos arquivos de logs, puderam ser observadas exceções nos testes de viabilidade técnica, por exemplo, exceções relativas à quantidade de conexões ativas durante a leitura de e-mails. Essas exceções possibilitaram melhorar os algoritmos nos processos que efetuam leituras, tanto leitura de e-mails quanto leitura de informações no banco de dados dos servidores PACS. A melhoria consistiu na elaboração de elementos

facilitadores de interconexão entre as tecnologias empregadas e as infraestruturas pré-existentes (base instalada), o que tornou a solução mais flexível.

Por outro lado, os experimentos em ambiente real possibilitaram identificar características sócias, relativas aos fluxos de trabalho existentes, que não foram previstas anteriormente e que devem ser contempladas para que o gateway seja implantado de forma completa, por exemplo, as políticas de direcionamento de mensagens devem levar em conta o período em que o médico radiologista trabalha, para encaminhar e receber mensagens no momento correto. Ainda, ambos os tipos de experimento ajudaram a identificar que elementos do *gateway* são mais acessados e consomem mais recursos, a fim de aplicar melhorias nos algoritmos para, respectivamente, dotar esses elementos de melhor desempenho de execução. Por fim, as falhas durante a execução em tempo real permitiram identificar onde o processamento de dados é mais críticos, por exemplo, durante o experimento efetuado entre os servidores PACS de Ribeirão Preto e STI (experimento A de implantação), o processo de resgate de informações de exames médicos contidos no banco de dados do servidor PACS de Ribeirão Preto tornou-se bastante lento, devido à grande massa de dados contidas nele, essa falha no desempenho permitiu definir estratégias de acesso à banco de dados, essas estratégias podem ser configuradas pelo usuário de forma que se adapte da melhor forma a realidade da infraestrutura existente.

Ademais, apesar das melhorias alcançadas tornarem a solução mais robusta, buscou-se minimizar a complexidade durante a implementação, através do fornecimento de elementos técnicos capazes de se comporem de forma variada, configuráveis através de arquivos de configuração que utilizam uma linguagem de fácil interpretação, como por exemplo, linguagem XML e expressões regulares. Dessa forma, foi alcançada uma maior capacidade de adaptação da solução.

6. Conclusão

Este capítulo conclui a apresentação da proposta do DicomFlow, que percorreu, no capítulo 1, sobre os desafios relacionados à formação de uma infraestrutura de informação global para telerradiologia, a importância e as limitações que impedem essa formação. Então, foi elencado um conjunto de metas, com suas respectivas justificativas, tendo em vista contornar as principais barreiras. Enquanto que o capítulo 2 explicou as diretrizes existentes na teoria de projetos para a formação de uma infraestrutura aberta, compartilhada e descentralizada. Abordou as características e limitações presentes nas infraestruturas telerradiológicas em relação aos modelos de trabalho telerradiológicos atuais. Uma vez que o capítulo 3 exibiu os resultados de uma análise crítica realizada em trabalhos relacionados, que propõe suas próprias soluções de infraestrutura telerradiológica. Identificou-se as vantagens e desvantagens, bem como os componentes e tecnologias influenciadores nos resultados obtidos por esses, por fim, as abordagens foram confrontadas seguindo um conjunto de critérios elencados. O capítulo 4 apresentou a proposta elaborada, os pontos que foram desenvolvidos e concluiu explanando uma breve discussão sobre a abordagem de desenvolvimento. Por fim, o capítulo 5 mostrou os experimentos realizados para validar tecnicamente do DicomFlow e comprovar sua aplicabilidade em uma infraestrutura telerradiológica.

Dessa forma, esse capítulo tem o objetivo de discutir sobre os principais aspectos da solução proposta, começando pelos resultados alcançados com os experimentos e objetivos alcançados, passando pelas contribuições, seguindo para ressaltar quanto às limitações de maior importância e concluindo com uma comparação com as outras soluções apresentadas nesse trabalho. Ademais, os trabalhos acadêmicos desenvolvidos e publicados no âmbito desta pesquisa são citados no final do capítulo.

6.1. Resultados dos experimentos

Conforme observado nos experimentos, a composição das tecnologias empregadas na solução mostrou que a arquitetura do DicomFlow é tecnicamente

viável, pois não foram observados erros operacionais críticos por incompatibilidade entre as tecnologias. Ou seja, a composição das tecnologias permitiu que todas as requisições de serviços encaminhadas durante a comunicação e troca de mensagens de e-mail fossem atendidas, nenhuma transferência de imagem foi interrompida após sua inicialização e, ao termino, todas as imagens requisitadas foram entregues, não houve comprometimento dos exames de imagem durante o processo de transmissão, se mantiveram íntegros na origem e no destino.

E mais, as exceções e falhas nos testes possibilitaram melhorar os elementos presentes na arquitetura e aprimorar o protocolo de comunicação proposto. Quando essas falhas ocorreram durante os testes, não interromperam o fluxo geral de execução do *gateway*, ou seja, nos momentos em que as falhas ocorreram, apenas os processos relacionados a essas é que foram suspensos, entretanto o DicomFlow foi capaz de identificar o processo que falhou e repeti-lo, assim retomando seu fluxo normal. Por outro lado, houveram momentos em que a solução proposta foi completamente interrompida pelo usuário, para fins de ajustes das estratégias de acesso, comunicação e transferência das informações médicas. Contudo, no momento em que o *gateway* era interrompido o estado atual dos processos era mantido e, ao reiniciar seus processos, o fluxo de execução dava continuidade do momento em que foi suspenso. Assim, além de comprovar a capacidade que o DicomFlow tem em manter seu funcionamento em situações de fluxos de exceção, também foi possível observar a capacidade de adaptação dinâmica que a ferramenta possui. Essas capacidades possibilitam a ferramenta ajustar-se às diferentes infraestruturas radiológicas existentes, ao passo que é capaz de acompanhar as mudanças que essas sofram durante o processo de evolução.

Relativo às métricas obtidas nos testes, o crescimento linear dos tempos de atendimento a requisições e de transferência efetiva mensurado nos experimentos de viabilidade técnica em relação ao aumento do número de exames transferidos demonstrou a capacidade de carga o DicomFlow suporta. Essa capacidade de carga adicionada a possibilidade de configuração de estratégias de acesso, comunicação e transporte melhoram a qualidade de processamento do *gateway*, pois permitem que possam ser adotadas estratégias diferentes para os diferentes

tipos de processos, garantindo uma melhor performance de funcionamento do *gateway*.

Ainda, os experimentos de viabilidade técnica possibilitaram validar a robustez do fluxo dos serviços empregados, pois o percentual de overhead foi baixo, uma média de 9,001% em relação aos tempos de sincronização e transferência efetiva de exames médicos, sendo que 1% desse foi gerado pelo controle do DicomFlow (acesso ao Banco de Dados e I/O), o restante corresponde aos serviços externos (armazenamento no servidor DCM4CHEE e acesso ao servidor de e-mail). Esses experimentos também comprovaram a capacidade que a infraestrutura resultante da implantação dos *gateways* tem em agregar uma nova infraestrutura PACS, permitindo o crescimento da infraestrutura resultante, sem comprometer o funcionamento ou requerer mudanças críticas nessa. Outro ponto positivo que facilita o crescimento da infraestrutura existente é a adoção de tecnologias escaláveis na implementação do DicomFlow, ou seja, foram utilizadas tecnologias de comunicação e transferência interoperáveis com infraestruturas de e-mail e HTTP já existentes, essas infraestruturas são descentralizadas e possibilitam a agregação de novos elementos de forma facilitada.

Relativo a implantação do DicomFlow em ambiente real, os experimentos ajudaram a observar a capacidade que a solução proposta tem em manter o controle de coordenação distribuídos. Primeiro, devido a arquitetura modular que permite independência dos processos de acesso a informação, comunicação e transferência, ou seja, foi possível nos experimentos permitir que cada entidade envolvida nos testes configurasse as estratégias de execução de cada processo funcionar de forma isolada e assíncrona, dessa forma cada um dos processos foi executado no melhor momento, em acordo com as estratégias escolhidas. Segundo, devido a arquitetura não pressupor de elementos centrais, cada entidade teve a capacidade de manter sua infraestrutura sobre seu controle, por exemplo, apesar de serem empregados um serviço de e-mail externo as instituições envolvidas, cada uma tem a possibilidade de manter uma infraestrutura de e-mail dentro do seu domínio, como foi feito com os servidores HTTP. Dessa forma, cada instituição envolvida tem autonomia sobre sua infraestrutura DicomFlow e, como os processos do fluxo de comunicação e transporte são independentes entre si, o funcionamento do *gateway* em uma entidade não foi comprometido por falha na

execução do *gateway* em outra entidade. Por exemplo, no experimento A entre a instituição de Ribeirão Preto e o STI, houve a necessidade de parar a execução do *gateway* de Ribeirão Preto, para reconfigurar a estratégia de acesso às informações de exames do Banco de Dados do servidor PACS, contudo o funcionamento do *gateway* e da infraestrutura mantida no STI não foi comprometida, uma vez reestabelecido o funcionamento do *gateway* de Ribeirão Preto, o fluxo de comunicação e transferência foi reestabelecido do ponto onde havia parado.

Resumindo, através dos experimentos foi possível comprovar a capacidade do *gateway* em manter seu funcionamento em situações de fluxos de exceção. Ainda, foi possível comprovar a capacidade de processamento e escala do *gateway* em relação a quantidade crescente de exames empregados. E mais, através dos experimentos em ambiente real de produção, foi possível avaliar a capacidade assíncrona do *gateway* em atender requisições, pois nenhuma mensagem de requisição foi perdida, corrompida ou deixou de ser processada e nenhum dado (exame ou laudo) transferido foi comprometido.

6.2. Objetivos alcançados

O objetivo geral deste trabalho foi contribuir para a melhora na distribuição de imagens médicas entre infraestruturas de saúde heterogêneas pertencentes a domínios de redes distintos, através da elaboração de uma solução em forma de *gateway* que fosse capaz de dotar a as infraestruturas PACS/DICOM de flexibilidade, possibilitando a interação entre essas infraestruturas de forma arbitrária e transparente. Dessa forma, a utilização das diretrizes dos protocolos de e-mail e de suas tecnologias tanto na elaboração do protocolo proposto quanto na implementação de referência possibilitou o DicomFlow beneficiar-se da alta conectividade oferecida pela infraestrutura e-mail amplamente difundida. Ainda, favorecer-se dos pontos-fortes do PACS-DICOM e contornar as suas limitações. Esse fato reforçou a estrutura e permitiu que esta vencesse a inércia imposta, transpassasse os limites de uma única organização e compartilhasse seus exames clínicos.

Assim, para contornar a limitação do tamanho do anexo enviado e evitar a complexidade de implementação de mecanismos de compactação e fragmentação das imagens médicas durante o transporte via e-mail, foi utilizada a infraestrutura

HTTP. Utilizar HTTP apenas na transferência de imagens, diminui a complexidade de implementação das diretrizes de controle de comunicação, uma vez que a comunicação via e-mail tem o aspecto ponto-a-ponto. Ou seja, empregar a tecnologia de e-mail possibilita implementar de forma mais simples uma comunicação direta entre médicos especialistas sem a necessidade de um mediador central para controlar o fluxo e troca de mensagens durante a troca de informação, por exemplo, a comunicação entre médicos para solicitação de segunda opinião sobre um exame. Esse tipo de comunicação utilizando HTTP requer um mediador que dê garantias de entrega de mensagens, requisito já presente na infraestrutura de e-mail. Ainda, seria necessário manter sincronismo entre os envolvidos na comunicação e o mediador, fato que diminuiria a independência entre as infraestruturas envolvidas. Em outras palavras, para que uma entidade envie informações para outra, seria necessário que ambas estivessem ativas no momento do envio. Isso é diferente com o e-mail, é possível enviar informações independentemente da disponibilidade do destino. Por outro lado, o destino tem a capacidade de decidir o melhor momento para acessar as informações recebidas.

Portanto, a composição entre as infraestruturas de e-mail e HTTP fortificam as infraestruturas PACS/DICOM, dotando de poder de comunicação e transferência de informações médicas para fora dos seus limites, ao passo que a infraestrutura resultante da composição dessas torna as entidades envolvidas independentes entre si. Assim, as composições dessas tecnologias reforçam os pontos fortes e minimizam os pontos fracos da infraestrutura resultante e possibilitam maior flexibilidade para acomodar o crescimento e a adaptação perante as mudanças nas entidades envolvidas.

6.3. Considerações finais

Comparado a outras soluções, como aquelas baseadas em computação na nuvem (Silva et al. 2013; Monteiro et al., 2016; Yuan et al., 2015; Godinho et al., 2016; Viana-Ferreira et al., 2017) ou em padrões perfis de integração IHE (Zhang et al., 2016; Ribeiro et al., 2014), o principal fator que distingue o DicomFlow é a sua arquitetura não pressupor autoridade ou elementos centrais, sendo seu controle e coordenação distribuídos. A presença desses elementos dificulta a livre

associação de entidades arbitrárias, requerendo em geral a satisfação de políticas para federalização. Do ponto de vista operacional, limita o crescimento em larga escala da infraestrutura, por exemplo, para lidar com uma grande quantidade de integrantes com elevada heterogeneidade técnica e social. Ainda, o DicomFlow também possui vantagens em relação ao DICOM e-mail (Weisser et al., 2007), pois transmitir objetos DICOM através do e-mail torna necessário o uso de técnicas de fragmentação e verificação de integridade, fato que sobrecarrega o protocolo. O modelo aqui proposto contorna essa sobrecarga devido a sua assimetria, onde comunicação de informações e transferência de imagens ocorrem por vias distintas, o que dota a solução também assíncrona, oferecendo ao receptor das mensagens a opção de decidir o momento da recuperação efetiva do estudo de imagem, dessa forma, cada gateway funciona de forma independente.

Do ponto de vista técnico, a arquitetura foi implementada utilizando tecnologias de código aberto, inclusive a própria implementação tem seu código aberto, acessível para quem tiver interesse de usá-la e possui documentação para desenvolvimento, instalação e configuração de uso. Ainda, o uso de interfaces e componentes simples na codificação possibilita tanto a combinação desses quanto a criação de novos componentes para atender demandas da infraestrutura que possam surgir no futuro. Por fim, todo o código é mantido em versão de controle, dessa forma a comunidade que adote o *gateway* como solução de comunicação para distribuição de imagens possam cooperar para o aprimoramento e evolução da solução.

Então, o DicomFlow possibilita a troca de imagens entre profissionais e organizações de saúde quaisquer, desde que pertençam à base instalada PACS/DICOM e de e-mail na Internet. É importante destacar que o *gateway* DicomFlow atua abaixo da camada de trabalho e não interfere diretamente em como o trabalho deve ser realizado ou em como as imagens trocadas serão utilizadas entre as partes. Tal característica torna o DicomFlow versátil, com grande capacidade de adaptação em contextos com diferentes práticas de trabalho. Assim, a elevada conectividade da base instalada aliada a capacidade de adaptação tem o potencial para fomentar o surgimento de uma infraestrutura de informação para distribuição de imagens médicas.

A Tabela 11, a seguir, revela às capacidades cumpridas pelo Dicomflow, confrontando-o com as propostas analisadas no capítulo 3.

Tabela 11 - Comparação entre os trabalhos relacionados

	Cloud Computer					IHE		P2P		E-mail		Nossa Proposta
	Silva et al. (2013)	Godinho et al. (2016)	Monteiro et al. (2016)	Yuan et al. (2015)	Viana-Ferreira et al. (2017)	Ribeiro et al. (2014)	Zhang et al. (2016)	Urovi et al. (2014)	Figueiredo e Motta (2012)	Ribeiro et al. (2010)	Weisser et al. (2007)	
Aberta	-	-	-	-	-	-	+	+	+	+	√	√
Compartilhada	-	-	-	-	-	-	+	+	-	+	√	√
Heterogênea	-	-	-	-	-	-	-	+	+	+	√	√
Descentralizada	-	-	-	-	-	-	+	+	+	+	√	√
Escalável	-	+	+	+	+	-	√	√	√	√	√	√
Segura	√	√	√	+	-	√	-	√	√	-	√	√
Assíncrona	-	-	+	+	+	+	+	√	√	√	√	√
Assimétrica	-	-	-	-	-	-	-	+	+	+	-	√
Base Instalada	√	√	√	√	√	√	√	√	√	√	√	√
Recursos Simples de TI	√	+	-	-	-	+	-	-	-	√	+	√
Utilidade direta	√	√	√	√	√	√	√	√	√	√	√	√
Modular	+	+	√	√	√	√	√	√	√	√	-	√

Legenda: (√) – disponível. (+) – parcialmente disponível. (-) – não disponível.

Portanto, a solução proposta é um exemplo de infraestrutura construída sobre uma base instalada que favorece o surgimento de uma Infraestrutura de Informação Telerradiológica como um sistema sociotécnico de TI compartilhado, aberto, heterogêneo e evolutivo. Aberto, pois permite que novas instituições façam parte da infraestrutura, mesmo não havendo acordo de nível de infraestrutura entre elas, bastando para isso possuir uma forma de ser endereçada (e-mail). Compartilhada porque não tem um único proprietário, todos são livres para usar e desenvolver seu próprio *gateway* com bases em protocolos públicos, incluindo o protocolo do DicomFlow, além da infraestrutura de e-mail. Heterogênea porque qualquer instituição, independentemente de sua estrutura interna, pode fazer parte da infraestrutura, a flexibilidade presente. Por fim, evolutiva, uma vez que o protocolo desenvolvido na arquitetura é constituído constituídos de serviços atômicos, possibilitando uma maior composição entre esses, permitindo o desenvolvimento de novos cenários de aplicação e novos modelos de negócio.

6.4. Limitações

Entre as limitações com impactos relevantes, distinguem-se as abaixo enumeradas e ponderadas:

Não foram implementadas características síncronas, para atender demandas de serviços em tempo real, por exemplo emissão de laudos de urgência. O protocolo até define elementos para esse fim nas estruturas XML, porém é necessário um estudo sobre a relevância, de fato, dessas características, bem como dos seus possíveis impactos negativos.

O mecanismo de geração de credenciais de acesso precisa ser aprimorado e testado em outros tipos de cenários. O uso de um UUID garante que um certificado identifica um único conjunto de permissões para um único usuário, ou seja, não pode ser utilizado por outro usuário que queira ter acesso as imagens. Contudo, um cenário muito comum é de um médico radiologista solicitar uma segunda opinião de outro médico radiologista, quando isso ocorre, surge a necessidade de gerar uma nova credencial na origem da imagem e emití-la para o outro médico radiologista, dessa forma, aumenta o fluxo de comunicação. Faz-se necessário um mecanismo que permita a passagens de permissões para terceiros.

Não foi especificado no protocolo diretrizes de manutenção para manter as URL ativas, nem foi implementado mecanismo para esse fim. Quando um domínio contido na URL sofre alteração ou é movido para outro domínio, a URL torna-se inválida. Esse tipo de cenário é comum entre entidades de saúde, por exemplo, um departamento de radiologia pertencente a uma rede de hospitais pode ser adquirido por outra rede de hospitais.

Tais limitações são os principais pontos a serem considerados nos trabalhos futuros. Como próxima meta, pretende-se desenvolver aplicativos para desktop e dispositivos móveis, utilizando como base instalada o DicomFlow, para torná-lo mais atrativo.

6.5. Publicações

Até então, dois trabalhos foram publicados no âmbito desta pesquisa de mestrado, tendo sido um deles com foco especificamente em um modelo de arquitetura distribuída, capaz de formar uma infraestrutura de informação aberta compartilhada e descentralizada para telerradiologia. Este teve importância fundamental nas bases da solução aqui desenvolvida. O outro trabalho tem foco no desenvolvimento de um *gateway* baseado no modelo arquitetural proposto pelo primeiro trabalho. Foram abordadas as tecnologias empregadas no modelo e verificada a viável técnica da composição dessas tecnologias.

Araújo, D. A. B., Neto, J. R., Damasceno, H. H., Silva, D. A., & Motta, G. H. DicomFlow: Um modelo de arquitetura para formação de uma infraestrutura de informação telerradiológica. Proceedings of the XII Brazilian Symposium on Information Systems, ISBN 978-85-7669-317-8, p. 458-465, 2016.

Neto, J. R., Damasceno, H. H., Silva, D. A., **Araújo, D. A. B.**, & Motta, G. H. DicomFlow: Uma infraestrutura assíncrona, assimétrica, descentralizada para distribuição de imagens médicas. XV Congresso Brasileiro de Informática em Saúde, 2016. (Artigo vencedor em primeiro lugar do prêmio CBIS'2016).

7. Referências Bibliográficas

- AANESTAD, M., GRISOT, M., HANSETH, O., & VASSILAKOPOULOU, P. Information Infrastructures within European Health Care. Working with the Installed Base. Springer, 2017.
- AANESTAD, Margun; HANSETH, Ole. Implementing open network technologies in complex work practices: a case from telemedicine. In: Organizational and social perspectives on information technology. Springer US, 2000. p. 355-369.
- AMARAL, José Nelson. About computing science research methodology. 2011.
- AMAZON. Authenticating Requests Using the REST API. Disponível em: <http://docs.aws.amazon.com/AmazonS3/latest/dev/S3_Authentication2.html>. Acesso em: 20 out. 2017.
- AZEVEDO-MARQUES, Paulo Mazzoncini; SALOMÃO, Samuel Covas. PACS: sistemas de arquivamento e distribuição de imagens. Revista Brasileira de Física Médica, v. 3, n. 1, 2009.
- BINKHUYSEN, FH Barneveld; RANSCHAERT, E. R. Teleradiology: evolution and concepts. European journal of radiology, v. 78, n. 2, p. 205-209, 2011.
- BOWKER, Geoffrey C. et al. Toward information infrastructure studies: Ways of knowing in a networked environment. In: International handbook of internet research. Springer Netherlands, 2010. p. 97-117.
- CHATTERJEE, A. R., Stalcup, S., Sharma, A., Sato, T. S., Gupta, P., Lee, Y. Z., & Kansagra, A. P. Image Sharing in Radiology—A Primer. The Association of University Radiologists - Elsevier, 2017.
- COSTA, Carlos et al. Indexing and retrieving DICOM data in disperse and unstructured archives. International journal of computer assisted radiology and surgery, v. 4, n. 1, p. 71-77, 2009.
- DICOM. DICOM *Homepage*. *About DICOM*. Disponível em:< <http://dicom.nema.org/Dicom/about-DICOM.html>>. Acesso em: 19 jul. 2017.
- DOTSON, A. T. Interoperability In radiography data: the impossible dream. Radiol Open J, v. 1, n. 1, p. 13-16, 2016.
- ENGELMANN, U. et al. DICOM E-mail: Germany's minimum standard for teleradiology. In: International Congress Series. Elsevier, 2005. p. 926-931.

- FIGUEIREDO, J. F.; MOTTA, G. H. SocialRAD: an infrastructure for a secure, cooperative, asynchronous teleradiology system. *Studies in health technology and informatics*, v. 192, p. 778-782, 2012.
- GODINHO, Tiago Marques et al. A Routing Mechanism for Cloud Outsourcing of Medical Imaging Repositories. *IEEE journal of biomedical and health informatics*, v. 20, n. 1, p. 367-375, 2016.
- GRISOT, Miria; HANSETH, Ole; THORSENG, Anne Asmyr. Innovation of, in, on infrastructures: Articulating the role of architecture in information infrastructure evolution. *Journal of the Association for Information Systems*, v. 15, n. 4, p. 197, 2014.
- GRISOT, Miria; VASSILAKOPOULOU, Polixeny. Creating a national e-health infrastructure: The Challenge of the installed base. In: **ECIS**. 2015.
- GUO, Yang et al. Using P2P technology to achieve e-Health interoperability. In: **ICSSSM11**. IEEE, 2011. p. 1-5.
- HANSETH, Ole; LYYTINEN, Kalle. Design theory for dynamic complexity in information infrastructures: the case of building internet. *Journal of Information Technology*, v. 25, n. 1, p. 1-19, 2010.
- HUANG, H. K. PACS and imaging informatics: basic principles and applications. 2nd ed. New Jersey: Wiley-Blackwell; 2010. 1048 p.
- HUGHES, Thomas P., 1987. The evolution of large technological systems. In: *The Social Construction of Technological Systems*. Cambridge, MA: MIT Press. p. 51-82. ISBN 0262022621.
- IHE. *Integrating the Healthcare Enterprise Homepage*, 2016. Disponível em: <<http://www.ihe.net>>. Acessado em: 19 Jul. 2017.
- JXTA. JXTA Technology, 2017. Disponível em: <<http://www.oracle.com/technetwork/java/index-jsp-136561.html>>. Acessado em: 29 de Jul. 2017.
- KNOBEL, Cory. Understanding Infrastructure: Dynamics, Tensions, and Design. Relatório Técnico, US National Science Foundation, 2007. Disponível em: <<https://deepblue.lib.umich.edu/bitstream/handle/2027.42/49353/UnderstandingInfrastructure2007.pdf>>. Acessado em: 20 out. 2017
- LANGER, Steve G. et al. The RSNA image sharing network. *Journal of digital imaging*, v. 28, n. 1, p. 53-61, 2015.

- MAPS. *Google Maps. Where in the World is XDS and XCA*. Disponível em: <<https://www.google.com/maps/ms?gl=us&ie=UTF8&oe=UTF8&msa=0&msid=110535847732151766411.00047b0b46314e91435c9>>. Acessado em: 19 Jul. 2017.
- MONTEIRO, EJ Melício; COSTA, C.; OLIVEIRA, J. L. *A Cloud Architecture for Teleradiology-as-a-Service. Methods of information in medicine*, v. 55, n. 3, p. 203-214, 2016.
- MONTEIRO, Eric; POLLOCK, Neil; HANSETH, Ole; WILLIAMS, Robin. From artefacts to infrastructures. *Computer supported cooperative work (CSCW)*, v. 22, n. 4-6, p. 575-607, 2013.
- MOTTA, Gustavo Henrique Matos Bezerra. Towards social radiology as an information infrastructure: Reconciling the local with the global. *JMIR medical informatics*, v. 2, n. 2, 2014.
- NOUMEIR, Rita. Sharing medical records: The XDS architecture and communication infrastructure. *IT Professional Magazine*, v. 13, n. 4, p. 46, 2011.
- OLIVEIRA, Márcio Adamec Lopes, MOTTA, Gustavo Henrique Matos Bezerra. Teoria de Projeto para Infraestruturas de Informação em Teleradiologia: um Estudo de Caso do DICOM e-mail na Alemanha. Congresso Brasileiro em Informática em Saúde – CBIS, 2014.
- OLIVEIRA, Márcio Adamec Lopes; MOTTA, Gustavo Henrique Matos Bezerra. Formação de uma infraestrutura de informação para telerradiologia: um estudo de múltiplos casos baseado na teoria de projeto para complexidade dinâmica. *J Health Inform.* 2016.
- OSIRIX. Osirix - DICOM Image Library. Disponível em: <<http://www.osirix-viewer.com/resources/dicom-image-library/>>. Acessado em: 20 out. 2017.
- PAINA, Ligia; PETERS, David H. Understanding pathways for scaling up health services through the lens of complex adaptive systems. *Health Policy and Planning*, v. 27, n. 5, p. 365-373, 2012.
- PIANYKH, Oleg S. *Digital Imaging and Communications in Medicine (DICOM)*. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012. 423 p.
- POLK, Tim; MCKAY, Kerry; CHOKHANI, Santosh. Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations. *NIST special publication*, v. 800, n. 52, p. 32, 2014.

- RIBEIRO, Luís S. et al. Email-P2P Gateway to Distributed Medical Imaging Repositories. In: HEALTHINF. 2010. p. 310-315.
- RIBEIRO, Luís S. et al. XDS-I outsourcing proxy: ensuring confidentiality while preserving interoperability. IEEE journal of biomedical and health informatics, v. 18, n. 4, p. 1404-1412, 2014.
- RIBEIRO, Luís S.; COSTA, Carlos; OLIVEIRA, José Luís. Current Trends in Archiving and Transmission of Medical Images. INTECH Open Access Publisher, 2011.
- RSNA. *Radiological Society of North America Homepage*, 2016. Disponível em: <<http://www.rsna.org/>>. Acessado em: 22 Jul. 2017.
- SHEARD, Sarah A.; MOSTASHARI, Ali. Principles of complex systems for systems engineering. Systems Engineering, v. 12, n. 4, p. 295-311, 2009.
- SILVA, Alandey Severo Leite. Framework para Análise das Tensões da Base Instalada no estabelecimento de uma Infraestrutura de Informação. Dissertação (Mestrado em Informática). Universidade Federal da Paraíba, 2017.
- SILVA, Luís A. Bastião; COSTA, Carlos; OLIVEIRA, José Luis. DICOM relay over the cloud. International journal of computer assisted radiology and surgery, v. 8, n. 3, p. 323-333, 2013.
- STAR, Susan Leigh; RUHLER, Karen. Steps toward an ecology of infrastructure: Design and access for large information spaces. Information systems research, v. 7, n. 1, p. 111-134, 1996.
- UROVI, Visara et al. Secure P2P cross-community health record exchange in IHE compatible systems. International Journal on Artificial Intelligence Tools, v. 23, n. 01, p. 1440006, 2014.
- VIANA-FERREIRA, Carlos et al. An Intelligent Cloud Storage Gateway for Medical Imaging. Journal of Medical Systems, v. 41, n. 9, p. 141, 2017.
- WEISSER, G. et al. Standardization of teleradiology using Dicom e-mail: recommendations of the German Radiology Society. European radiology, v. 16, n. 3, p. 753-758, 2006.
- WEISSER, G. et al. Teleradiology applications with DICOM-e-mail. European radiology, v. 17, n. 5, p. 1331-1340, 2007.

- XCA. *Cross-Community Access*. Disponível em: <http://wiki.ihe.net/index.php/Cross-Community_Access>. Acessado em: 19 Jul. 2017.
- XCA-I. *Cross-Community Access for Imaging*. Disponível em: <http://wiki.ihe.net/index.php/Cross-Community_Access_for_Imaging>. Acessado em: 19 Jul. 2017.
- XDS. *Cross-enterprise Document Sharing*. Disponível em: <http://wiki.ihe.net/index.php/Cross-Enterprise_Document_Sharing>. Acessado em: 19 Jul. 2017.
- XDS-I. *Cross-enterprise Document Sharing for Imaging*. Disponível em: <http://wiki.ihe.net/index.php/Cross-enterprise_Document_Sharing_for_Imaging>. Acessado em: 19 Jul. 2017.
- YUAN, Youwei et al. Sharing of Larger Medical DICOM Imaging Data-Sets in Cloud Computing. *Journal of Medical Imaging and Health Informatics*, v. 5, n. 7, p. 1390-1394, 2015.
- ZAPF, Christian; BERMAN, Andreas; SUNDERBRINK, Dirk. PACS and RIS. In: *Springer handbook of medical technology*. Springer Berlin Heidelberg, 2011. p. 1199-1208.
- ZHANG, Jianguo et al. Design of image sharing and exchanging for cross-enterprise and cross-domain collaborative healthcare in Shanghai. In: *SPIE Medical Imaging. International Society for Optics and Photonics*, 2011. p. 79670R-79670R-9.
- ZHANG, Kai et al. Clinical experiences of collaborative imaging diagnosis in Shanghai district healthcare services. In: *SPIE Medical Imaging. International Society for Optics and Photonics*, 2016. p. 97890X-97890X-12.

APÊNDICE A – PROTOCOLO DE COMUNICAÇÃO DICOMFLOW

1. O PROTOCOLO

O presente protocolo, denominado DICOMFLOW, teve como motivação o avanço da telerradiologia, que impulsionou a busca por novas técnicas de compartilhamento de imagens entre Sistemas de Comunicação e Arquivamento de Imagens Médicas (PACS, *Picture Archiving and Communication System*), seu principal objetivo é padronizar a comunicação e prover interoperabilidade de forma facilitada entre infraestruturas de saúde heterogêneas pertencentes a domínios de redes distintos que desejam compartilhar imagens médicas.

O protocolo DICOMFLOW foi elaborado pela equipe de pesquisa do Laboratório de Arquitetura de Sistemas e Software – LARSS, do Programa de Pós-Graduação em Informática – PPGI, da Universidade Federal da Paraíba – UFPB e seu conteúdo é público.

2. CENÁRIOS DE APLICABILIDADE

Os cenários enumerados a seguir representam configurações reais e foram elaborados a partir de soluções apresentadas em estudos e pesquisas. Esses cenários orientaram a elaboração dos tipos de mensagens de serviços existentes no protocolo de comunicação para troca de informações médicas. Ainda, orientaram a elaboração do fluxo de comunicação e troca das mensagens entre os atores presentes em cada cenário. Ainda, os tipos de serviços e os fluxos de comunicação elaborados possuem descrição clara e de fácil implementação, permitindo ainda a derivação de novos tipos de serviços e novos fluxos de comunicação a partir da composição dos já existentes, possibilitando adaptação do protocolo para compor novos cenários.

2.1. CENÁRIO 01 - TRANSFERÊNCIA SIMPLES

Atores:

- Entidade de saúde com servidor PACS (e.g. Hospital ou Clínica);
- Entidades consumidoras de imagens médicas (e.g. estações de trabalho remotas).

Descrição:

- Uma Entidade de saúde que adquire imagens médicas dos pacientes e provê essas imagens para as Entidades consumidoras localizadas remotamente consultarem.

Fluxos:

- Os exames são gerados por modalidades de imagens (e.g. Radiografia Computadorizada) e enviados para armazenamento no servidor PACS. O protocolo monitora o PACS e envia mensagens de serviços para os consumidores informando que essas imagens estão disponíveis para compartilhamento, as mensagens contêm informações do exame (e.g. dados do paciente) e os links de acesso para as imagens. Os consumidores recebem as mensagens e o protocolo acessa os links. As imagens são transferidas do servidor PACS para os consumidores de imagem.

O fluxo descrito identifica uma solicitação de compartilhamento de imagens,

portanto as mensagens trocadas nesse fluxo pertencem ao tipo de serviço definido como **SHARING**.

- Os consumidores enviam mensagens contendo informações de consulta contendo filtros (e.g. dados do paciente, tipo do exame) para a entidade de saúde. A entidade de saúde recebe as mensagens e o protocolo acessa as informações. O protocolo efetua uma busca no servidor PACS pelas imagens utilizando os filtros. O protocolo envia mensagens de serviços com o resultado da consulta para os consumidores informando as imagens encontradas com os filtros informados, as mensagens contêm os filtros e os links de acesso para as imagens. Os consumidores recebem as mensagens e acessam os links. As imagens são transferidas do servidor PACS para os consumidores de imagem.

O fluxo descrito identifica uma solicitação de busca de imagens, portanto as mensagens trocadas nesse fluxo pertencem ao tipo de serviço definido como **FIND**.

2.2. CENÁRIO 02 – DISTRIBUIÇÃO COMPARTILHADA

Atores:

- Duas ou mais entidades de saúde com servidores PACS (e.g. Hospitais e Clínicas).

Descrição:

- Duas ou mais entidades de saúde independentes e geograficamente distribuídas adquirem imagens médicas, compartilham entre si e disponibilizam as imagens para que possam ser acessadas em qualquer uma das entidades envolvidas.

Fluxos:

- Os exames são gerados por modalidades de imagens (e.g. Radiografia Computadorizada) e enviados para armazenamento no servidor PACS da entidade de origem. O protocolo monitora o PACS e envia mensagens de serviços solicitando que os novos exames sejam armazenados nas entidades de saúde destino, as mensagens contêm informações do exame (e.g. dados do paciente) e os links de acesso para as imagens. As entidades de destino recebem as mensagens e o protocolo acessa os links. As imagens são transferidas do servidor PACS de origem e armazenadas nos servidores PACS de destino. Os protocolos das entidades de destino enviam mensagens de serviço contendo os resultados do armazenamento para a entidade de origem.

O fluxo descrito identifica uma solicitação de armazenamento de imagens, portanto as mensagens trocadas nesse fluxo pertencem ao tipo de serviço definido como **STORAGE**.

2.3. CENÁRIO 03 – DISTRIBUIÇÃO PARA DIAGNÓSTICO

Atores:

- Duas ou mais entidades de saúde com servidores PACS (e.g. Hospitais e clínicas);
- Dois ou mais consumidores de imagens médicas (e.g. Radiologistas).

Descrição:

- Duas ou mais entidades de saúde independentes e geograficamente distribuídas adquirem imagens médicas e enviam essas imagens aos consumidores de imagens médicas, que são independentes entre si, e estes podem realizar o diagnóstico e enviar o laudo de volta às clínicas.

Fluxos:

- Os exames são gerados por modalidades de imagens (e.g. Radiografia Computadorizada) e enviados para armazenamento nos servidores PACS das entidades de saúde. Os protocolos monitoram e enviam mensagens de serviços para os consumidores solicitando que um laudo seja efetuado sobre as imagens disponibilizadas, as mensagens contêm informações do exame (e.g. dados do paciente) e os links de acesso para as imagens. Os consumidores recebem as mensagens e o protocolo acessa os links. As imagens são transferidas do servidor PACS para os consumidores de imagem. Os consumidores de imagens produzem os laudos e enviam mensagens de serviço contendo os laudos dos exames para as entidades de origem.

O fluxo descrito identifica uma solicitação de laudo sobre as imagens, portanto as mensagens trocadas nesse fluxo pertencem ao tipo de serviço definido como **REQUEST**.

2.4. CENÁRIO 04 - DISTRIBUIÇÃO PARA DIAGNÓSTICO COM REPOSITÓRIO TERCEIRIZADO

Atores:

- Duas ou mais entidades de saúde com servidores PACS (e.g. Hospitais e clínicas);
- Dois ou mais consumidores de imagens médicas (e.g. Radiologistas).
- Um repositório de imagens terceirizado (e.g. servidor da Amazon)

Descrição:

- Duas ou mais entidades de saúde independentes e geograficamente distribuídas adquirem imagens médicas e enviam essas imagens para o repositório terceirizado. Os consumidores de imagens médicas, que são independentes entre si, podem acessar esse repositório, resgatar as imagens, realizar o diagnóstico e enviar o laudo de volta às clínicas.

Fluxos:

- Os exames são gerados por modalidades de imagens (e.g. Radiografia Computadorizada) e enviados para armazenamento no servidor PACS da entidade de origem. O protocolo monitora o PACS e envia mensagens de serviços solicitando que os novos exames sejam armazenados no repositório terceirizado, as mensagens contêm informações do exame (e.g. dados do paciente) e os links de acesso para as imagens. O repositório terceirizado recebe as mensagens e o protocolo acessa os links. As imagens são transferidas do servidor PACS de origem e armazenadas nos repositórios. O protocolo do repositório envia mensagens de serviço contendo os resultados do armazenamento para a entidade de origem.

O fluxo descrito identifica uma solicitação de armazenamento de imagens, portanto as mensagens trocadas nesse fluxo pertencem ao tipo de serviço definido como **STORAGE**.

- Os exames são gerados por modalidades de imagens (e.g. Radiografia Computadorizada) e enviados para armazenamento nos servidores PACS das entidades de saúde. Os protocolos monitoram e enviam mensagens de serviços para os consumidores solicitando que um laudo seja efetuado sobre as imagens disponibilizadas no repositório terceirizado, as mensagens contêm informações do exame (e.g. dados do paciente) e os links de acesso para as imagens no repositório terceirizado. Os consumidores recebem as mensagens e o protocolo acessa os links. As imagens são transferidas do repositório para os consumidores de imagem. Os consumidores de imagens produzem os laudos e enviam mensagens de serviço contendo os laudos dos exames para as entidades de origem.

O fluxo descrito identifica uma solicitação de laudo sobre as imagens, portanto as mensagens trocadas nesse fluxo pertencem ao tipo de serviço definido como **REQUEST**.

2.5. CENÁRIO 05 – REDE SOCIAL RADIOLÓGICA

Descrição:

- Este cenário é uma composição dos demais cenários apresentados anteriormente, onde os atores de um determinado cenário podem comunicar com atores de outro cenário, constituindo um espaço de fluxos diversos, formando uma infraestrutura de informação para a prática telerradiológica.

3. DETALHAMENTO DOS FLUXOS DOS SERVIÇOS

Cada mensagem de solicitação identifica um tipo de serviço e a ação a ser executada, por exemplo, supondo que o receptor execute serviços de armazenamento de exames, o emitente que precise armazenar um novo exame, envia uma mensagem com identificação do serviço de Armazenamento e ação de Salvamento. Caso o emitente necessite excluir um exame, envia uma mensagem com identificação do Serviço de Armazenamento e a ação de Exclusão.

Toda mensagem de solicitação de um serviço requer uma mensagem de resposta, indicando que a solicitação foi completada. Por exemplo, no serviço de armazenamento, para cada mensagem de solicitação de salvamento de um novo exame, existe uma mensagem de resultado que informa o estado atual da solicitação e encerra o ciclo do serviço de armazenamento.

O detalhamento dos ciclos de cada um dos fluxos de serviço definiu as ações que cada serviço possui. Ainda, o detalhamento identificou que informações dos exames são necessárias em cada mensagem de solicitação e que atributos de controle são importantes para mapear corretamente mensagens de resultado a suas respectivas mensagens de solicitação. A Tabela 1 lista os Serviços e suas ações definidos pelo protocolo DICOMFLOW.

Tabela 1 - Serviços e ações

Serviço	Ação	Descrição
CERTIFICATE Serviço utilizado para troca de certificados entre entidades de saúde que pretendem comunicar-se para executar ações sobre imagens médicas.	REQUEST	Solicitação de troca de certificado entre emitente e receptor. Mensagem contendo certificado digital do emitente, requisitando o certificado do receptor.
	RESULT	Resultado da solicitação de troca de certificado. Mensagem de resposta à solicitação contendo o certificado digital do receptor e contendo credencial de acesso do emitente.
	CONFIRM	Confirmação do recebimento da resposta de troca de certificado. Mensagem de resposta ao resultado contendo a credencial de acesso do receptor.
STORAGE Serviço utilizado por uma entidade de saúde para solicitação de armazenamento e manutenção de imagens médicas em outra(s) entidade(s) de saúde.	SAVE	Solicitação de armazenamento de imagens do emitente no receptor. Mensagem contendo os dados da imagem presente no emitente e uma URL para seu acesso.
	UPDATE	Solicitação de atualização de imagens do emitente no receptor. Mensagem contendo os dados da imagem atualizada no emitente e uma URL para seu acesso.

	DELETE	Solicitação de remoção de imagens do emitente no receptor.
		Mensagem contendo os dados da imagem removida no emitente.
	RESULT	Resultado de solicitação de armazenamento, atualização ou remoção de imagens do emitente no receptor.
SHARING		Mensagem contendo o status da ação solicitada.
	PUT	Solicitação de compartilhamento de imagens do emitente com o receptor.
		Mensagem contendo os dados da imagem atualizada no emitente e uma URL para seu acesso.
	RESULT	Resultado de solicitação de compartilhamento de imagens do emitente com o receptor.
		Mensagem contendo a confirmação de recebimento status da ação solicitada.
REQUEST	PUT	Solicitação de emissão de laudo ou processamento da imagem do emitente no receptor.
		Mensagem contendo dados da imagem presente no emitente, URL de acesso e identificação do tipo de atividade (laudo ou processamento)

Serviço utilizado por uma entidade de saúde para informar a existência de imagens médicas e compartilhar essas imagens com outra(s) entidade(s) de saúde.

Serviço utilizado por uma entidade de saúde para solicitar emissões de laudo ou processamento de imagem por outra(s) entidade(s) de saúde.

	RESULT	Resultado de solicitação de emissão de laudo ou processamento da imagem.
		Mensagem contendo o status da ação solicitada e, laudo ou URL da imagem processada pelo receptor
FIND	PUT	Solicitação de acesso às imagens do receptor conforme critérios de busca.
Serviço utilizado por uma entidade de saúde para localizar imagens médicas em outra(s) entidade(s) de saúde.		Mensagem contendo alguns ou todos os dados do paciente e dados da imagem.
	RESULT	Resultado da solicitação de acesso às imagens do receptor.
		Mensagem contendo a URL de acesso às imagens encontradas no receptor conforme os critérios de busca.
DISCOVERY	VERIFYALLSERVICES	Solicitação de identificação de todos os serviços e ações atendidos pelo receptor.
Serviço utilizado por uma entidade de saúde para identificar e confirmar que serviços outra(s) entidade de saúde atende.		Mensagem contendo o grau de detalhamento dos serviços.
	VERIFYSERVICES	Solicitação de confirmação dos serviços e ações listados pelo emitente e atendidos pelo receptor.
		Mensagem contendo a lista de serviços a serem confirmados pelo receptor e o grau de detalhamento dos serviços.
	VERIFYRESULT	Resultado da solicitação de identificação ou

confirmação dos serviços.

Mensagem contendo os serviços atendidos pelo receptor, detalhados conforme o grau especificado pelo emiteente.

3.1. FLUXO DO SERVIÇO CERTIFICATE

Antes de qualquer troca de mensagens de demais serviços e transferência de imagens, ocorre troca de certificados digitais entre emiteente e receptor, através do serviço CERTIFICATE. Os certificados são utilizados pelos mecanismos de segurança durante as emissões de Mensagens de Serviços e transferência de imagens. A troca inicia quando o DICOMFLOW emiteente envia seu certificado e, possivelmente, a credencial de acesso do DICOMFLOW receptor através de e-mail, o DICOMFLOW receptor responde com outro e-mail contendo o certificado do receptor e, possivelmente, a credencial de acesso do emiteente. Somente após a troca dos certificados, outras mensagens de serviços podem ser transmitidas e links podem ser acessados para transferência de imagens. A Figura 1 ilustra o fluxo de troca de certificados entre emiteente e receptor.

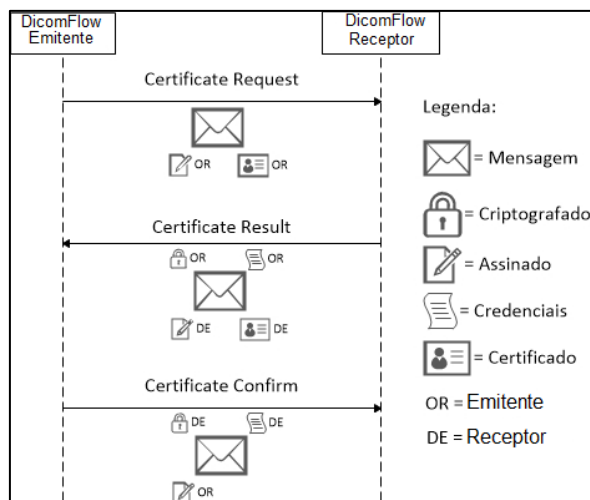


Figura 1 - Fluxo de Troca de Certificados

3.2. FLUXO DO SERVIÇO STORAGE

O serviço STORAGE é responsável por proporcionar o armazenamento permanente dos exames de imagem em uma entidade externa àquela que realizou os exames. Ao iniciar um relacionamento deste tipo, ambas as partes da transação passam a ter acordos legais, de nível de serviço, confidencialidade, etc.

O início da transação é feito pela entidade originadora da nova imagem, que solicita armazenamento dessa imagem na entidade receptora, ou seja, o emiteente envia uma mensagem de STORAGE SAVE para o receptor, a mensagem é assinada pelo

emissor e criptografada com o certificado digital do receptor. O emissor envia na mensagem os dados da imagem, a URL de acesso e as credenciais de acesso (se necessário) que serão utilizados para obter o exame localizado no lado do emissor. O receptor, após download e armazenamento da imagem, envia uma mensagem contendo o resultado da operação (STORAGE RESULT), a mensagem de resultado é assinada pelo receptor e criptografada com o certificado digital do emissor.

O fluxo pode ter continuidade com a manutenção da imagem, se a entidade emissor solicitar atualizar (STORAGE UPDATE) ou remover (STORAGE DELETE) a imagem já armazenada pelo receptor, as mensagens trocadas nessa continuação do fluxo também são criptografadas e assinadas. A Figura 2 ilustra o fluxo de armazenamento e manutenção de imagens entre emissor e receptor.

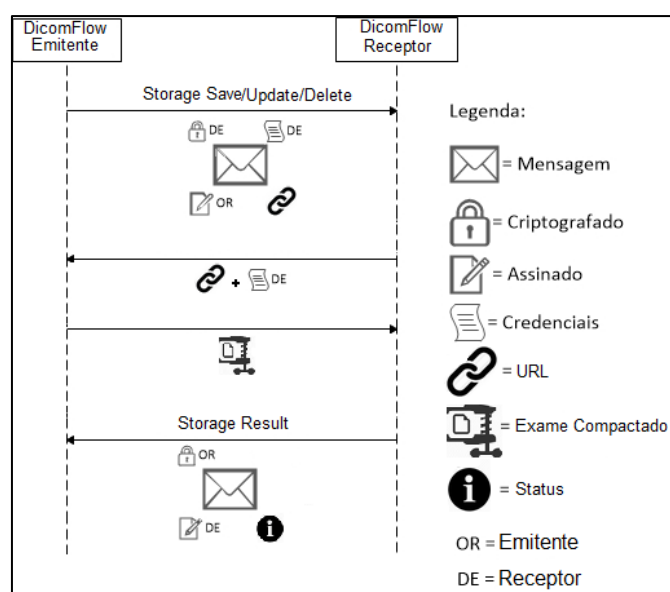


Figura 2 - Fluxo de Armazenamento e Manutenção

3.3. FLUXO DO SERVIÇO SHARING

O serviço SHARING é responsável por sinalizar aos interessados que um novo exame de imagem foi adquirido e pode ser acessado pelas entidades interessadas.

O início da transação é feito pela entidade adquire uma imagem e informa as demais sobre a aquisição, ou seja, o emissor envia uma mensagem de SHARING PUT para o receptor, a mensagem é assinada pelo emissor e criptografada com o certificado digital do receptor. O emissor envia na mensagem os dados da imagem, a URL de acesso e as credenciais de acesso (se necessário) que serão utilizados para obter o exame localizado no lado do emissor. O receptor envia uma mensagem contendo a confirmação do recebimento da mensagem (SHARING RESULT), a mensagem de resultado é assinada pelo receptor e criptografada com o certificado digital do emissor.

A Figura 3 ilustra o fluxo de compartilhamento de imagem entre emissor e receptor.

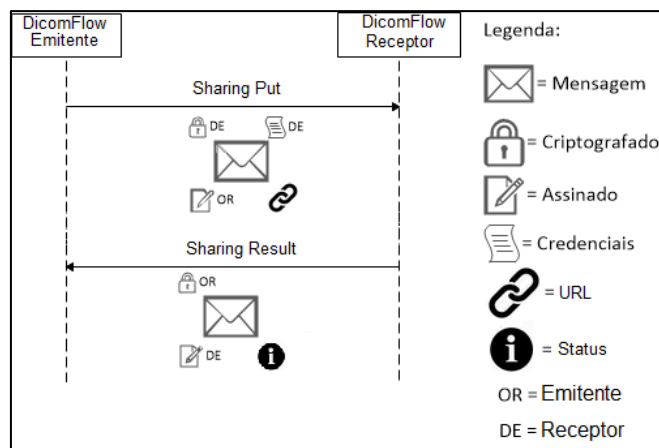


Figura 3 - Fluxo de Compartilhamento

3.4. FLUXO DO SERVIÇO REQUEST

O serviço REQUEST é responsável por solicitar que uma entidade externa (geralmente médicos radiologistas ou serviços de processamento) realize alguma operação sobre o exame de imagem original. Pode haver solicitações de criação de laudos ou processamento das imagens dos exames.

O início da transação é feito pela entidade originadora da nova imagem, que solicita emissão de laudo ou processamento dessa imagem na entidade receptora, ou seja, o emitente envia uma mensagem de REQUEST PUT para o receptor, a mensagem é assinada pelo emitente e criptografada com o certificado digital do receptor. O emitente envia na mensagem os dados da imagem, a URL de acesso e as credenciais de acesso (se necessário) que serão utilizados para obter o exame localizado no lado do emitente. O receptor, após download e, emissão de laudo ou processamento da imagem, envia uma mensagem contendo o resultado da operação (REQUEST RESULT), a mensagem carrega um arquivo contendo o laudo ou uma URL de acesso para a imagem processada, essa mensagem é assinada pelo receptor e criptografada com o certificado digital do emitente.

A Figura 4 ilustra o fluxo de requisição de laudo ou processamento de imagem entre emitente e receptor.

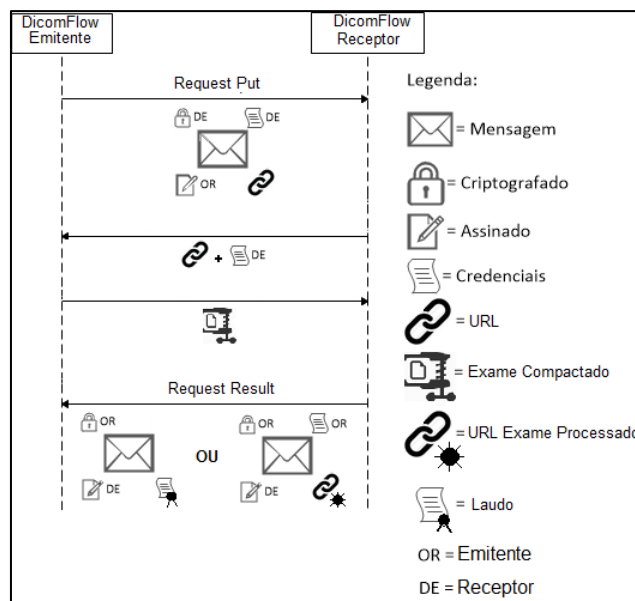


Figura 4 - Fluxo Requisição de Laudo ou Processamento

3.5. FLUXO DO SERVIÇO FIND

O serviço FIND é responsável por solicitar que uma entidade efetue determinada consulta de um exame em uma entidade externa. Os dados do paciente e do exame são usados para consulta que seguem a hierarquia especificada no padrão DICOM.

O início da transação é feito pela entidade que solicita localizar uma imagem na entidade originadora da imagem, ou seja, o emissor envia uma mensagem de FIND PUT para o receptor, a mensagem é assinada pelo emissor e criptografada com o certificado digital do receptor. O emissor envia na mensagem os dados da busca, a estrutura dos dados segue a hierarquia de dados de imagem definida pelo DICOM (Instância – Paciente – Serie – Imagem). O receptor, após efetuar a busca com os dados informados, envia uma mensagem contendo o resultado da operação (FIND RESULT), a mensagem carrega uma URL de acesso para as imagens localizadas ou carrega um status quando não localiza imagens com os dados fornecidos, essa mensagem é assinada pelo receptor e criptografada com o certificado digital do emissor.

A Figura 5 ilustra o fluxo de busca de imagem entre emissor e receptor.

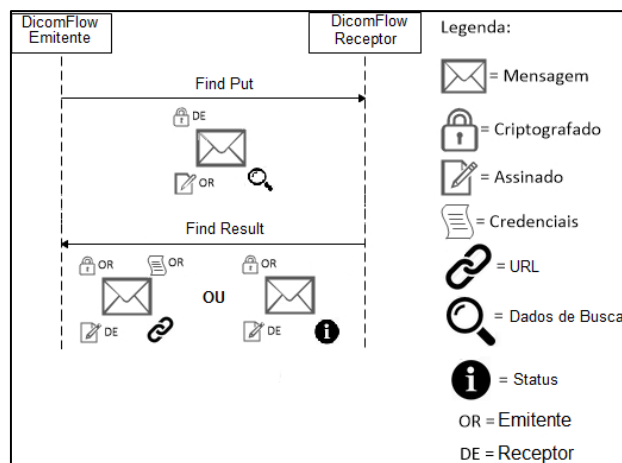


Figura 5 - Fluxo de Busca

3.6. FLUXO DO SERVIÇO DISCOVERY

O serviço DISCOVERY é responsável por solicitar que uma entidade externa identifique quais os serviços do protocolo são suportados por ela, juntamente com as ações possíveis para cada serviço e status de disponibilidade de cada uma das ações. A entidade externa pode ainda informar que campos ela suporta para cada ação e serviço.

O início da transação é feito pela entidade que solicita saber os serviços do protocolo prestados pela entidade externa, ou seja, o emissor envia uma mensagem de DISCOVERY para o receptor, essa mensagem é assinada pelo emissor e criptografada com o certificado digital do receptor. O emissor especifica na mensagem se quer saber todos os serviços (DISCOVERY VERIFYALLSERVICES) ou especifica os serviços que deseja identificar (DISCOVERY VERIFYFYSERVICES), em ambos os casos é enviada a informação do nível de detalhes dos serviços. O receptor, após detalhar os serviços de acordo com o nível de detalhes especificado, envia uma mensagem contendo o resultado da operação (DISCOVERY VERIFYRESULT), essa mensagem é assinada pelo receptor e criptografada com o certificado digital do emissor.

A Figura 6 ilustra o fluxo de identificação de serviços entre emissor e receptor.

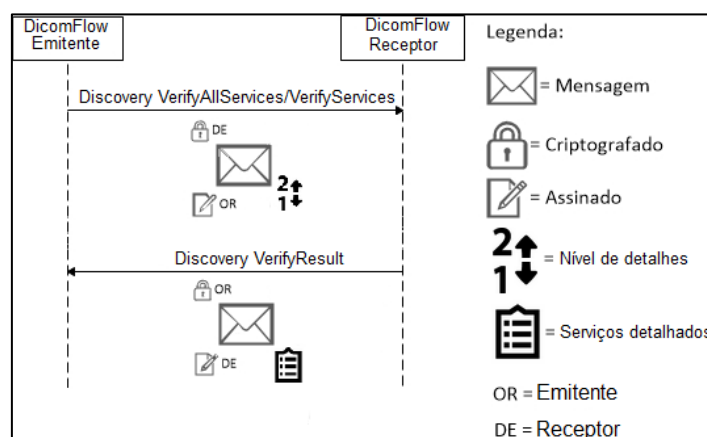


Figura 6 - Fluxo de Identificação de Serviços

4. ESTRUTURA DAS MENSAGENS DE SERVIÇOS

4.1. DEFINIÇÃO DAS INFORMAÇÕES DAS MENSAGENS DE SERVIÇOS

A seguir são definidas em tabelas as informações que cada uma das mensagens de serviço deve conter. Ainda, como as mensagens são estruturadas em XML, são definidas a obrigatoriedade (M – Majoritário/O – Opcional), a multiplicidade e a descrição de cada campo. O Escopo de cada campo é definido segundo o formato:

1 – O caractere ‘>’ indica o Nível de Escopo do campo, por exemplo, a ausência do caractere indica primeiro nível; > indica segundo nível; >> indica terceiro nível e assim por diante.

2 – O caractere ‘-’ indica os atributos de cada um dos campos. Cada campo tem seus atributos descritos abaixo de sua definição e em sequência.

Além das mensagens em XML, podem ser enviados anexos, por exemplo, as mensagens do serviço CERTIFICATE que carregam a estruturada em XML e os certificados digitais em anexo.

4.1.1. CERTIFICATE REQUEST

A Tabela 2 define os campos da estrutura XML de CERTIFICATE REQUEST.

Tabela 2 - Campos da mensagem CERTIFICATE REQUEST

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: CERTIFICATE
-action	M	1	Ação do serviço. Valor: REQUEST
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>Mail	M	1	E-mail do emitente
-value	M	1	O valor do e-mail. Formato: email do RFC 2822
>Domain	M	1	IP ou Domínio do emitente
-value	M	1	O valor do domínio. Formato: DNS - RFCs 882 e 883, e

			foi atualizado nas RFCs 1034 e 1035
>Port	M	1	Porta do domínio do emitente
-value	M	1	O valor da porta.
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Timeout	M	1	Tempo de validade da mensagem. Formato: milisegundos

Anexos enviados junto à estrutura XML: Certificado Digital do emitente da Mensagem CERTIFICATE REQUEST.

4.1.2. CERTIFICATE RESULT

A Tabela 3 define os campos da estrutura XML de CERTIFICATE RESULT.

Tabela 3 - Campos da mensagem CERTIFICATE RESULT

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: CERTIFICATE
-action	M	1	Ação do serviço. Valor: REQUEST
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>Mail	M	1	E-mail do emitente
-value	M	1	O valor do e-mail. Formato: email do RFC 2822

>Domain	M	1	IP ou Domínio do emitente
-value	M	1	O valor do domínio. Formato: DNS - RFCs 882 e 883, e foi atualizado nas RFCs 1034 e 1035
>Port	M	1	Porta do domínio do emitente
-value	M	1	O valor da porta.
>Credentials	O	1	Credenciais de acesso para exames.
>Status	M	1	Status do recebimento e processamento da mensagem CERTIFICATE REQUEST. Valores: SUCCESS, ERROR
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Timeout	M	1	Tempo de validade da mensagem. Formato: milisegundos

Anexos enviados junto à estrutura XML: Certificado Digital do emitente da Mensagem CERTIFICATE RESULT.

4.1.3. CERTIFICATE CONFIRM

A Tabela 4 define os campos da estrutura XML de CERTIFICATE CONFIRM.

Tabela 4 - Campos da mensagem CERTIFICATE CONFIRM

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: CERTIFICATE

-action	M	1	Ação do serviço. Valor: REQUEST
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>Mail	M	1	E-mail do emitente
-value	M	1	O valor do e-mail. Formato: email do RFC 2822
>Domain	M	1	IP ou Domínio do emitente
-value	M	1	O valor do domínio. Formato: DNS - RFCs 882 e 883, e foi atualizado nas RFCs 1034 e 1035
>Port	M	1	Porta do domínio do emitente
-value	M	1	O valor da porta.
>Credentials	O	1	Credenciais de acesso para exames.
>Status	M	1	Status do recebimento e processamento da mensagem CERTIFICATE RESULT. Valores: SUCCESS, ERROR
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Timeout	M	1	Tempo de validade da mensagem. Formato: milisegundos

4.1.4. STORAGE SAVE

A Tabela 5 define os campos da mensagem de STORAGE SAVE.

Tabela 5 - Campos da mensagem STORAGE SAVE

Nome	Tipo	Multiplicidade	Descrição
------	------	----------------	-----------

Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: STORAGE
-action	M	1	Ação do serviço. Valor: SAVE
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>URL	M	1	URL para acesso ao exame (conjunto de objetos DICOM).
-value	M	1	O valor da URL
>>Credentials	O	1	Credenciais de acesso ao exame (conjunto de objetos DICOM).
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Timeout	M	1	Tempo de validade da mensagem. Formato: milisegundos

4.1.5. STORAGE UPDATE

A Tabela 6 define os campos da mensagem de STORAGE UPDATE.

Tabela 6 - Campos da mensagem STORAGE UPDATE

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço

-name	M	1	Nome do serviço. Valor: STORAGE
-action	M	1	Ação do serviço. Valor: UPDATE
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>URL	M	1	URL para acesso ao exame (conjunto de objetos DICOM).
-value	M	1	O valor da URL
>>Credentials	O	1	Credenciais de acesso ao exame (conjunto de objetos DICOM).
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Timeout	M	1	Tempo de validade da mensagem. Formato: milisegundos
>Object	M	1	O objeto DICOM a ser atualizado
-type	M	1	Tipo de objeto a ser atualizado. Valores: Study, Serie, Instance
-id	M	1	Identificador único do objeto a ser atualizado. Valores: id do objeto DICOM

4.1.6. STORAGE DELETE

A Tabela 7 define os campos da mensagem de STORAGE DELETE.

Tabela 7 - Campos da mensagem STORAGE DELETE

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço

-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: STORAGE
-action	M	1	Ação do serviço. Valor: DELETE
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>URL	M	1	URL para acesso ao exame (conjunto de objetos DICOM).
-value	M	1	O valor da URL
>>Credentials	O	1	Credenciais de acesso ao exame (conjunto de objetos DICOM).
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Timeout	M	1	Tempo de validade da mensagem. Formato: milisegundos
>Objects	M	1	Lista de objetos DICOM
>>Object	M	1-n	O objeto DICOM a ser removido
-type	M	1	O tipo de objeto. Valores: Study, Serie, Instance
-id	M	1	Identificador único do objeto a ser apagado. Valores: id do objeto DICOM

4.1.7. STORAGE RESULT

A Tabela 8 define os campos da mensagem de STORAGE DELETE.

Tabela 8 - Campos da mensagem STORAGE RESULT

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: STORAGE
-action	M	1	Ação do serviço. Valor: RESULT
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>Results	M	1	Resultados em lotes podem ser enviados
>>Result	M	1-n	Um resultado
>>>OriginalMessageID	M	1	Identificador único da mensagem originadora da transação
>>>Timestamp	M	1	Momento do processamento de cada mensagem original. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>>>Objects	O	1	Conjunto de objetos DICOM recém armazenados
>>>>Object	O	1-n	Objeto DICOM recém armazenado
-type	O	1	O tipo de objeto. Valores: Study, Serie, Instance

-id	O	1	Identificador único do objeto a ser apagado. Valores: id do objeto DICOM
>>>Completed	M	1	Status da operação.
-status	M		Valor do status da operação. Valores: SUCCESS, ERROR
>>>>CompletedMessage	O	1	Mensagem descritiva do estado final da operação

4.1.1.8. SHARING PUT

A Tabela 9 define os campos da mensagem de SHARING PUT.

Tabela 9 - Campos da mensagem de SHARING PUT.

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: SHARING
-action	M	1	Ação do serviço. Valor: PUT
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>URLs	M	1	Conjunto de URL para acesso aos exames (conjunto de objetos DICOM)

>>URL	M	1-n	URL para acesso ao exame (conjunto de objetos DICOM)
-value	M	1	O valor da URL
>>>Patient	O	1	Metadados do paciente relacionado ao exame.
-id	O	1	Identificador do paciente. Valores: id do paciente DICOM
-name	O	1	Nome do paciente
-gender	O	1	O gênero do paciente
-birthdate	O	1	Data de nascimento do paciente
>>>>Study	O	1	Metadados do exame a ser obtido através da URL
-id	O	1	Identificador único do exame. Valores: id do exame DICOM
-type	O	1	tipo do exame. Valores: CT, MR, etc.
-description	O	1	Descrição do estudo
-datetime	O	1	Data de aquisição do exame. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
-size	O	1	Tamanho total do exame. Formato: bytes
>>>>>Serie	O	1-n	Metadados da série relacionada ao exame
-id	O	1	Identificado único da série. Valores: id da serie DICOM

-bodypart	O	1	Parte corporal envolvida no exame.
-description	O	1	Descrição da série
-instances	O	1	Número de instâncias
>>>Credentials	O	1	Credenciais de acesso ao exame (conjunto de objetos DICOM).
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Timeout	O	1	Tempo de validade da mensagem. Formato: milisegundos

4.1.9. SHARING RESULT

A Tabela 10 define os campos da mensagem de SHARING RESULT.

Tabela 10 - Campos da mensagem de SHARING RESULT.

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: SHARING
-action	M	1	Ação do serviço. Valor: RESULT
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822

>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Results	M	1	Resultados em lotes podem ser enviados
>>Result	M	1 - n	Um resultado
>>>OriginalMessageID	M	1	Identificador único da mensagem originadora da transação
>>>Timestamp	M	1	Momento do processamento de cada mensagem original. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>>>Completed	M	1	Status da operação.
-status	M	11 1	Valor do status da operação. Valores: SUCCESS, ERROR
>>>>CompletedMessage	O	1	Mensagem descritiva do estado final da operação

4.1.10. REQUEST PUT

A Tabela 11 define os campos da mensagem de REQUEST PUT.

Tabela 11 - Campos da mensagem de REQUEST PUT.

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço

-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: REQUEST
-action	M	1	Ação do serviço. Valor: PUT
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Timeout	O	1	Tempo de validade da mensagem. Formato: milisegundos
>RequestType	M	1	Qual o tipo de solicitação. Valores: LAUDO, PROCESSAMENTO
>URL	M	1	URL para acesso ao exame (conjunto de objetos DICOM).
-value	M	1	O valor da URL
>>Patient	O	1	Metadados do paciente relacionado ao exame.
-id	O	1	Identificador do paciente. Valores: id do paciente DICOM
-name	O	1	Nome do paciente
-gender	O	1	O gênero do paciente
-birthdate	O	1	Data de nascimento do paciente
>>>Study	O	1	Metadados do exame a ser obtido através da URL

-id	O	1	Identificador único do exame. Valores: id do exame DICOM
-type	O	1	tipo do exame. Valores: CT, MR, etc.
-description	O	1	Descrição do estudo
-datetime	O	1	Data de aquisição do exame. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
-size	O	1	Tamanho total do exame. Formato: bytes
>>>>Serie	O	1-n	Metadados da série relacionada ao exame
-id	O	1	Identificado único da série. Valores: id da serie DICOM
-bodypart	O	1	Parte corporal envolvida no exame.
-description	O	1	Descrição da série
-instances	O	1	Número de instâncias
>>Credentials	O	1	Credenciais de acesso ao exame (conjunto de objetos DICOM).

4.1.11. REQUEST RESULT

A Tabela 12 define os campos da mensagem de REQUEST RESULT.

Tabela 12 - Campos da mensagem de REQUEST RESULT.

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço

-name	M	1	Nome do serviço. Valor: REQUEST
-action	M	1	Ação do serviço. Valor: RESULT
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Results	M	1	Resultados em lotes podem ser enviados
>>Result	M	1-n	Um resultado
>>>OriginalMessageID	M	1	Identificador único da mensagem originadora da transação
>>>Data	O	1	O Laudo ou outro tipo de arquivo.
-filename	O	1	O nome e extensão do arquivo
>>>>Bytes	O	1	O conjunto de bytes do arquivo
>>>URLs	O	1	Conjunto de URL para acesso aos exames processados (conjunto de objetos DICOM)
>>>>URL	O	1-n	URL para acesso ao exame processado (conjunto de objetos DICOM)

>>>Completed	M	1	Status da operação.
-status	M	11 1	Valor do status da operação. Valores: SUCCESS, ERROR
>>>Timestamp	M	1	Momento do processamento de cada mensagem original. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"

4.1.12. FIND PUT

A Tabela 13 define os campos da mensagem de FIND PUT.

Tabela 13 - Campos da mensagem de FIND PUT.

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: FIND
-action	M	1	Ação do serviço. Valor: PUT
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Timezone	M	1	<i>time zone set</i> do domínio para manter sincronismo

>Searchs	M	1	A lista de buscas a serem efetuadas
>Search	M	1-n	A busca a ser efetuada
>>Patient	O	1-n	Metadados do paciente para busca
-id	O	1	Identificador do paciente. Valores: id do paciente DICOM
-name	O	1	Nome do paciente
-gender	O	1	O gênero do paciente
-birthdate	O	1	Data de nascimento do paciente
>>>Study	O	1-n	Metadados do exame para busca
-id	O	1	Identificador único do exame. Valores: id do exame DICOM
-type	O	1	tipo do exame. Valores: CT, MR, etc.
-description	O	1	Descrição do estudo
-datetime	O	1	Data de aquisição do exame. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
-size	O	1	Tamanho total do exame. Formato: bytes
>>>>Serie	O	1-n	Metadados da série para a busca
-id	O	1	Identificado único da série. Valores: id da serie DICOM
-bodypart	O	1	Parte corporal envolvida no exame.
-description	O	1	Descrição da série

-instances	O	1	Número de instâncias
>Priority	O	1	Identifica o nível de prioridade da mensagem. Valores: inteiro de 1 a 5
>Timeout	O	1	Tempo de validade da mensagem. Formato: milisegundos

4.1.13. FIND RESULT

A Tabela 14 define os campos da mensagem de FIND RESULT.

Tabela 14 - Campos da mensagem de FIND RESULT.

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: FIND
-action	M	1	Ação do serviço. Valor: PUT
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Results	M	1	Resultados em lotes podem ser enviados
>>Result	M	1-n	Um resultado

>>>OriginalMessageID	M	1	Identificador único da mensagem originadora da transação
>>>Completed	M	1	Status da operação.
-status	M	11 1	Valor do status da operação. Valores: SUCCESS, ERROR
>>>>CompletedMessage	O	1	Mensagem descritiva do estado final da operação
>>>Timestamp	M	1	Momento do processamento de cada mensagem original. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>>>URLs	M	1	Conjunto de URL para acesso aos exames processados (conjunto de objetos DICOM)
>>>>URL	M	1-n	URL para acesso ao exame processado (conjunto de objetos DICOM)
>>>>>Credentials	O	1	Credenciais de acesso ao exame (conjunto de objetos DICOM).
>>>>>Patient	O	1-n	Metadados do paciente relacionado ao exame.
-id	O	1	Identificador do paciente. Valores: id do paciente DICOM
-name	O	1	Nome do paciente

-gender	O	1	O gênero do paciente
-birthdate	O	1	Data de nascimento do paciente
>>>>>>Study	O	1-n	Metadados do exame a ser obtido através da URL
-id	O	1	Identificador único do exame. Valores: id do exame DICOM
-type	O	1	tipo do exame. Valores: CT, MR, etc.
-description	O	1	Descrição do estudo
-datetime	O	1	Data de aquisição do exame. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
-size	O	1	Tamanho total do exame. Formato: bytes
>>>>>>>Serie	O	1-n	Metadados da série relacionada ao exame
-id	O	1	Identificado único da série. Valores: id da serie DICOM
-bodypart	O	1	Parte corporal envolvida no exame.
-description	O	1	Descrição da série
-instances	O	1	Número de instâncias

4.1.14. DISCOVERY VERIFYALLSERVICES

A Tabela 15 define os campos da mensagem de DISCOVERY VERIFYALLSERVICES.

Tabela 15 - Campos da mensagem de DISCOVERY VERIFYALLSERVICES

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: DISCOVERY
-action	M	1	Ação do serviço. Valor: VERIFYALLSERVICES
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Timezone	M	1	<i>time zone set</i> do domínio para manter sincronismo
>Detail	M	1	define o grau de detalhamento dos serviços. Valores: inteiro de 1 a 3. Sendo 1 o menos detalhado e 3 o mais detalhado
>Priority	O	1	Identifica o nível de prioridade da mensagem. Valores: inteiro de 1 a 5. Sendo 1 o mais alto e 5 o mais baixo
>Timeout	O	1	Tempo de validade da mensagem. Formato: milisegundos

4.1.15. DISCOVERY VERIFYSERVICES

A Tabela 16 define os campos da mensagem de DISCOVERY VERIFYSERVICES.

Tabela 16 - Campos da mensagem de DISCOVERY VERIFYSERVICES

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: DISCOVERY
-action	M	1	Ação do serviço. Valor: VERIFYSERVICES
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Timezone	M	1	<i>time zone set</i> do domínio para manter sincronismo
>Services	M	1	A lista de serviços a serem verificados
>>ServiceDescriptor	M	1-n	O serviço a ser verificado
-name	M	1	O nome do Serviço
>>>ActionDescriptor	O	1-n	A ação associada ao serviço
-name	O	1	O nome da Ação
>>>>FieldDescriptor	O	1-n	O campo presente na ação
-name	O	1	O nome do Campo

>Priority	O	1	Identifica o nível de prioridade da mensagem. Valores: inteiro de 1 a 5. Sendo 1 o mais alto e 5 o mais baixo
>Timeout	O	1	Tempo de validade da mensagem. Formato: milisegundos

4.1.16. DISCOVERY VERIFYRESULT

A Tabela 17 define os campos da mensagem de DISCOVERY VERIFY RESULT.

Tabela 17 - Campos da mensagem de DISCOVERY VERIFYRESULT

Nome	Tipo	Multiplicidade	Descrição
Service	M	1	Identificação do serviço
-version	M	1	Versão do serviço
-name	M	1	Nome do serviço. Valor: DISCOVERY
-action	M	1	Ação do serviço. Valor: VERIFYRESULT
>MessageID	M	1	Identificador único da mensagem. Formato: message-id do RFC 2822
>Timestamp	M	1	Momento do envio da mensagem. Formato: ISO 8601 timestamp "YYYY-MM-DDThh:mm:ssZ"
>Timezone	M	1	<i>time zone set</i> do domínio para manter sincronismo
>Result	M	1	Resultado da requisição

>>OriginalMessageID	M	1	Identificador único da mensagem originadora da transação
>>Services	M	1	Lista de serviços verificados
>>>ServiceDescriptor	M	1 - n	O serviço verificado
-status	M	1	estado do serviço: ONLINE, OFFLINE, UNKNOWN
>>>>ActionDescriptor	O	1 - n	A ação verificada
-status	O	1	estado do serviço: ONLINE, OFFLINE, UNKNOWN
>>>>>FieldDescriptor	O	1 - n	O campo verificado
-status	O	1	estado do serviço: ONLINE, OFFLINE, UNKNOWN
>>Completed	M	1	Status da operação.
-status	M		Valor do status da operação. Valores: SUCCESS, ERROR
>>>CompletedMessage	O	1	Mensagem descritiva do estado final da operação

4.2. ESQUEMA XML DAS MENSAGENS DE SERVIÇO

A definição do esquema XML (XSD – XML Schema Definition) abaixo descreve como deve ser a composição dos elementos XML que contém as informações necessárias para cada tipo de mensagem de serviço.

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

```

<xs:element name="object" nillable="true" type="xs:anyType"/>
<xs:element name="result" type="result"/>
<xs:element name="service" nillable="true" type="xs:anyType"/>
<xs:complexType name="service">
  <xs:sequence>
    <xs:element name="messageID" type="xs:string" minOccurs="0"/>
    <xs:element name="timestamp" type="xs:string" minOccurs="0"/>
    <xs:element name="timeout" type="xs:string" minOccurs="0"/>
  </xs:sequence>
  <xs:attribute name="version" type="xs:string"/>
  <xs:attribute name="name" type="xs:string"/>
  <xs:attribute name="action" type="xs:string"/>
  <xs:attribute name="type" type="xs:int" use="required"/>
</xs:complexType>

<xs:complexType name="certificateRequest">
  <xs:complexContent>
    <xs:extension base="service">
      <xs:sequence>
        <xs:element name="domain" type="xs:string" minOccurs="0"/>
        <xs:element name="mail" type="xs:string" minOccurs="0"/>
        <xs:element name="port" type="xs:int" minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="certificateResult">
  <xs:complexContent>
    <xs:extension base="service">
      <xs:sequence>

```

```

    <xs:element name="credential" type="xs:string" minOccurs="0"/>
    <xs:element name="domain" type="xs:string" minOccurs="0"/>
    <xs:element name="mail" type="xs:string" minOccurs="0"/>
    <xs:element name="port" type="xs:int" minOccurs="0"/>
    <xs:element name="status" type="xs:string" minOccurs="0"/>
  </xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>

```

```

<xs:complexType name="certificateConfirm">
  <xs:complexContent>
    <xs:extension base="service">
      <xs:sequence>
        <xs:element name="credential" type="xs:string" minOccurs="0"/>
        <xs:element name="domain" type="xs:string" minOccurs="0"/>
        <xs:element name="mail" type="xs:string" minOccurs="0"/>
        <xs:element name="port" type="xs:int" minOccurs="0"/>
        <xs:element name="status" type="xs:string" minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

```

<xs:complexType name="storageSave">
  <xs:complexContent>
    <xs:extension base="service">
      <xs:sequence>
        <xs:element name="url" type="url" minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

```

</xs:complexContent>
</xs:complexType>

<xs:complexType name="storageUpdate">
  <xs:complexContent>
    <xs:extension base="service">
      <xs:sequence>
        <xs:element ref="object" minOccurs="0"/>
        <xs:element name="url" type="url" minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="storageDelete">
  <xs:complexContent>
    <xs:extension base="service">
      <xs:sequence>
        <xs:element name="objects" minOccurs="0">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="object" type="object" nillable="true"
minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="storageResult">

```

```

<xs:complexContent>
  <xs:extension base="service">
    <xs:sequence>
      <xs:element name="results" minOccurs="0">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="result" type="result" nillable="true"
minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:extension>
</xs:complexContent>
</xs:complexType>

<xs:complexType name="sharingPut">
  <xs:complexContent>
    <xs:extension base="service">
      <xs:sequence>
        <xs:element name="urls" minOccurs="0">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="url" type="url" nillable="true" minOccurs="0"
maxOccurs="unbounded"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

```

<xs:complexType name="sharingResult">
  <xs:complexContent>
    <xs:extension base="service">
      <xs:sequence>
        <xs:element name="results" minOccurs="0">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="result" type="result" nillable="true"
minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

```

<xs:complexType name="requestPut">
  <xs:complexContent>
    <xs:extension base="service">
      <xs:sequence>
        <xs:element name="requestType" type="xs:string" minOccurs="0"/>
        <xs:element name="url" type="url" minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

```

<xs:complexType name="requestResult">
  <xs:complexContent>

```

```

<xs:extension base="service">
  <xs:sequence>
    <xs:element name="results" minOccurs="0">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="result" type="result" nillable="true"
minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>

<xs:complexType name="findPut">
  <xs:complexContent>
    <xs:extension base="service">
      <xs:sequence>
        <xs:element name="priority" type="xs:int"/>
        <xs:element name="search" type="search" nillable="true" minOccurs="0"
maxOccurs="unbounded"/>
        <xs:element name="timezone" type="xs:string" minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="search">
  <xs:sequence>

```

```

    <xs:element name="patient" type="patient" nillable="true" minOccurs="0"
maxOccurs="unbounded"/>

```

```

</xs:sequence>

```

```

</xs:complexType>

```

```

<xs:complexType name="findResult">

```

```

  <xs:complexContent>

```

```

    <xs:extension base="service">

```

```

      <xs:sequence>

```

```

        <xs:element name="results" minOccurs="0">

```

```

          <xs:complexType>

```

```

            <xs:sequence>

```

```

              <xs:element name="result" type="result" nillable="true"
minOccurs="0" maxOccurs="unbounded"/>

```

```

            </xs:sequence>

```

```

          </xs:complexType>

```

```

        </xs:element>

```

```

      </xs:sequence>

```

```

    </xs:extension>

```

```

  </xs:complexContent>

```

```

</xs:complexType>

```

```

<xs:complexType name="discoveryVerifyAllServices">

```

```

  <xs:complexContent>

```

```

    <xs:extension base="service">

```

```

      <xs:sequence>

```

```

        <xs:element name="detail" type="xs:int"/>

```

```

        <xs:element name="priority" type="xs:int"/>

```

```

        <xs:element name="timezone" type="xs:string" minOccurs="0"/>

```

```

      </xs:sequence>

```

```

    </xs:extension>

```

```

  </xs:complexContent>

```

```
</xs:complexType>
```

```
<xs:complexType name="discoveryVerifyServices">
```

```
<xs:complexContent>
```

```
<xs:extension base="service">
```

```
<xs:sequence>
```

```
<xs:element name="priority" type="xs:int"/>
```

```
<xs:element name="services" minOccurs="0">
```

```
<xs:complexType>
```

```
<xs:sequence>
```

```
<xs:element name="serviceDescriptor" type="serviceDescriptor"
nillable="true" minOccurs="0" maxOccurs="unbounded"/>
```

```
</xs:sequence>
```

```
</xs:complexType>
```

```
</xs:element>
```

```
<xs:element name="timezone" type="xs:string" minOccurs="0"/>
```

```
</xs:sequence>
```

```
</xs:extension>
```

```
</xs:complexContent>
```

```
</xs:complexType>
```

```
<xs:complexType name="discoveryVerifyResult">
```

```
<xs:complexContent>
```

```
<xs:extension base="service">
```

```
<xs:sequence>
```

```
<xs:element name="priority" type="xs:int"/>
```

```
<xs:element name="result" type="result" nillable="true" minOccurs="0"
maxOccurs="unbounded"/>
```

```
<xs:element name="timezone" type="xs:string" minOccurs="0"/>
```

```
</xs:sequence>
```

```
</xs:extension>
```

```
</xs:complexContent>
```

```
</xs:complexType>
```

```
<xs:complexType name="completed">
```

```
  <xs:sequence>
```

```
    <xs:element name="completedMessage" type="xs:string" minOccurs="0"/>
```

```
  </xs:sequence>
```

```
  <xs:attribute name="status" type="xs:string"/>
```

```
</xs:complexType>
```

```
<xs:complexType name="serviceDescriptor">
```

```
  <xs:sequence>
```

```
    <xs:element name="actionDescriptor" type="actionDescriptor"
nillable="true" minOccurs="0" maxOccurs="unbounded"/>
```

```
  </xs:sequence>
```

```
  <xs:attribute name="name" type="xs:string"/>
```

```
  <xs:attribute name="status" type="xs:string"/>
```

```
</xs:complexType>
```

```
<xs:complexType name="actionDescriptor">
```

```
  <xs:sequence>
```

```
    <xs:element name="fieldDescriptor" type="fieldDescriptor" nillable="true"
minOccurs="0" maxOccurs="unbounded"/>
```

```
  </xs:sequence>
```

```
  <xs:attribute name="name" type="xs:string"/>
```

```
  <xs:attribute name="status" type="xs:string"/>
```

```
</xs:complexType>
```

```
<xs:complexType name="fieldDescriptor">
```

```
  <xs:sequence/>
```

```
  <xs:attribute name="name" type="xs:string"/>
```

```
  <xs:attribute name="status" type="xs:string"/>
```

```
</xs:complexType>
```

```

<xs:complexType name="result">
  <xs:sequence>
    <xs:element name="completed" type="completed" minOccurs="0"/>
    <xs:element name="data" type="data" minOccurs="0"/>
    <xs:element name="objects" minOccurs="0">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="object" type="object" nillable="true" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
    <xs:element name="originalMessageID" type="xs:string" minOccurs="0"/>
    <xs:element name="services" minOccurs="0">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="serviceDescriptor" type="serviceDescriptor"
nillable="true" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
    <xs:element name="timestamp" type="xs:string" minOccurs="0"/>
    <xs:element name="urls" minOccurs="0">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="url" type="url" nillable="true" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>

```

```
</xs:complexType>
```

```
<xs:complexType name="data">
```

```
  <xs:sequence>
```

```
    <xs:element name="bytes" type="xs:base64Binary" minOccurs="0"/>
```

```
  </xs:sequence>
```

```
  <xs:attribute name="filename" type="xs:string"/>
```

```
</xs:complexType>
```

```
<xs:complexType name="object">
```

```
  <xs:sequence>
```

```
    <xs:element name="credential" type="credentials" minOccurs="0"/>
```

```
  </xs:sequence>
```

```
  <xs:attribute name="id" type="xs:string"/>
```

```
  <xs:attribute name="type" type="xs:string"/>
```

```
</xs:complexType>
```

```
<xs:complexType name="url">
```

```
  <xs:sequence>
```

```
    <xs:element name="credentials" type="credentials" minOccurs="0"/>
```

```
    <xs:element name="patient" type="patient" nillable="true" minOccurs="0"
maxOccurs="unbounded"/>
```

```
  </xs:sequence>
```

```
  <xs:attribute name="value" type="xs:string"/>
```

```
</xs:complexType>
```

```
<xs:complexType name="credentials">
```

```
  <xs:sequence>
```

```
    <xs:element name="value" type="xs:string" minOccurs="0"/>
```

```
  </xs:sequence>
```

```
</xs:complexType>
```

```

<xs:complexType name="patient">
  <xs:sequence>
    <xs:element name="study" type="study" nillable="true" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="id" type="xs:string"/>
  <xs:attribute name="name" type="xs:string"/>
  <xs:attribute name="gender" type="xs:string"/>
  <xs:attribute name="birthdate" type="xs:string"/>
</xs:complexType>

<xs:complexType name="study">
  <xs:sequence>
    <xs:element name="serie" type="serie" nillable="true" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="id" type="xs:string"/>
  <xs:attribute name="type" type="xs:string"/>
  <xs:attribute name="description" type="xs:string"/>
  <xs:attribute name="datetime" type="xs:string"/>
  <xs:attribute name="size" type="xs:long" use="required"/>
</xs:complexType>

<xs:complexType name="serie">
  <xs:sequence/>
  <xs:attribute name="id" type="xs:string"/>
  <xs:attribute name="bodypart" type="xs:string"/>
  <xs:attribute name="description" type="xs:string"/>
  <xs:attribute name="instances" type="xs:int" use="required"/>
</xs:complexType>
</xs:schema>

```

4.3. CABEÇALHO DAS MENSAGENS DE SERVIÇO

Conforme descrito nas considerações gerais, as estruturas XML que carregam os dados e informações de controle são criptografadas nas mensagens de serviço, portanto foram definidas X-TAGS que são utilizadas no cabeçalho das mensagens e que carregam as informações de controle que não precisam de proteção, o objetivo das X-TAGS é melhorar o desempenho na identificação e pré-processamento da mensagem de serviço.

A Tabela 18 apresenta as X-TAGS elaboradas para o cabeçalho das mensagens. Estão definidos o nome da X-TAG, o tipo (M – Mandatório, O – Opcional) e a finalidade

Tabela 18 - X-TAGS definidas para o cabeçalho das mensagens

Nome	Tipo	Finalidade
X-Service-Type	M	Definir o nome do serviço e da ação a qual a mensagem se refere.
X-Message-ID	M	Definir uma identificação única da mensagem Formato: <message-id>@<domain> message-id = message-id do RFC 2822 domain = IP ou domínio do emitente segundo DNS - RFCs 882 e 883, e foi atualizado nas RFCs 1034 e 1035.
X-Head-Builder	O	Identificar a estratégia de construção do cabeçalho da mensagem. Omitir a X-TAG, indica utilização a estratégia de maior identificador.
X-Content-Builder	O	Identificar a estratégia de segurança das informações da mensagem (criptografia e assinatura). Omitir a X-TAG, indica utilização a estratégia de maior identificador.
X-Disposition-Notification-To	O	Identificar o e-mail ao qual deve ser reportado erro de processamento da mensagem

4.3.1 ESTRATÉGIAS DE CONSTRUÇÃO DO CABEÇALHO

Aqui estão definidas todas as estratégias de construção de cabeçalho. São definidos os tipos e formatos de valores que cada X-TAG deve conter.

Tabela 19 - Estratégia 1 de construção de cabeçalho

IDENTIFICADOR DA ESTRATÉGIA = 1

X-Service-Type	Tipo: Número inteiro Mapeamento: STORAGE_SAVE = 1
----------------	---

STORAGE_UPDATE = 2
 STORAGE_DELETE = 3
 STORAGE_RESULT = 4
 CERTIFICATE_REQUEST = 5
 CERTIFICATE_RESULT = 6
 CERTIFICATE_CONFIRM = 7
 SHARING_PUT = 8
 SHARING_RESULT = 9
 REQUEST_PUT = 10
 REQUEST_RESULT = 11
 DISCOVERY_VERIFY_ALL_SERVICES=12
 DISCOVERY_VERIFY_SERVICES = 13
 DISCOVERY_VERIFY_RESULT = 14
 IF.FIND_PUT = 15
 FIND_RESULT = 16

X-Message-ID

Tipo: Texto

Formato: <message-id>@<domain>

Onde:

- <message-id> = message-id do RFC 2822
- <domain> = IP ou domínio do emitente segundo DNS - RFCs 882 e 883, e foi atualizado nas RFCs 1034 e 1035

X-Disposition-Notification-To

Tipo: Texto

Valor: o mesmoda TAG From da mensagem

5. ESPECIFICAÇÕES DE SEGURANÇA DAS INFORMAÇÕES

Conforme descrito nas considerações gerais do protocolo, as mensagens carregam informações em formato XML e também podem carregar arquivos anexos, tudo é protegido por criptografia e assinatura através da utilização de certificados digitais. Nesse capítulo serão especificadas as estratégias de criptografia definidas pelo protocolo.

5.1. ESTRATÉGIAS DE SEGURANÇA DAS INFORMAÇÕES

Aqui são especificadas as estratégias de assinatura e criptografia da mensagem. Cada estratégia define os padrões aplicados nos tipos de

credenciais utilizados pelo protocolo, como também os padrões utilizados na assinatura e criptografia das mensagens.

Tabela 20 - Estratégia 1 de assinatura e criptografia da mensagem

IDENTIFICADOR DA ESTRATÉGIA: 1

Certificados Digitais	Padrão X.509 V3
Mensagem	Formato: SMTP/MIME (RFC's 822, 2822)
Criptografia e Assinatura	Padrão S/MIME (RFC's 3369, 3370, 3850 e 3851)

Mecanismo: (1) O emissor cria a mensagem MIMEMultipart. (2) Inclui um MIMEBodyPart contendo a estrutura XML do serviço e define seu Content-Type como "text/XML;charset=UTF-8". (2.1 - condicional) Inclui um MIMEBodyPart contendo o certificado digital do emissor e define seu Content-Type como "application/octet-stream". (3) O emissor assina a mensagem com seu certificado digital, (4) criptografa a mensagem com o certificado digital do receptor e (5) define no cabeçalho da mensagem o Content-Type do MIMEMultipart como "application/pkcs7-mime; name="smime.p7m"; smimetype=enveloped-data". (5) Envia a mensagem para o receptor. Após receber a mensagem, (6) o receptor descodifica a mensagem, (7) checa a validade da assinatura comparando com o certificado digital que possui do emissor e (8) extrai a estrutura XML do serviço.

A Figura 7 ilustra o mecanismo da estratégia 1.

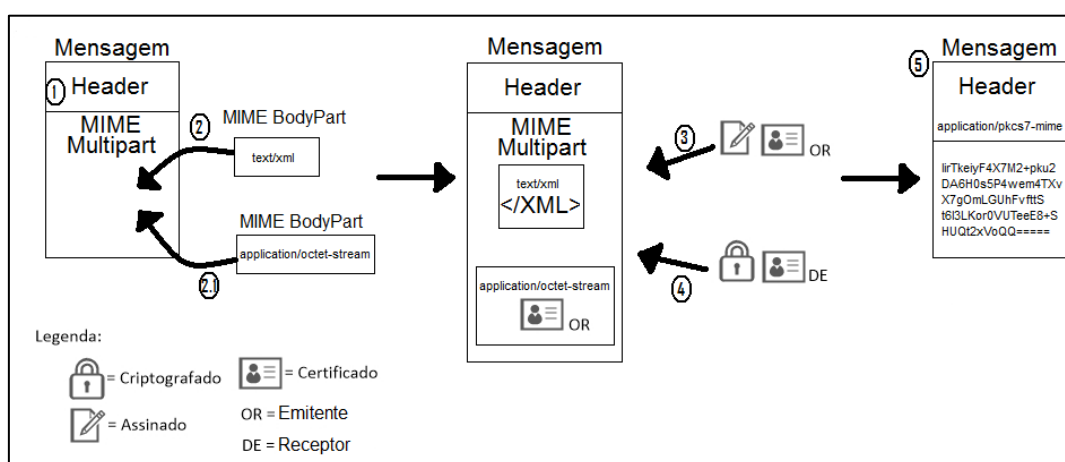


Figura 7 - Mecanismo da estratégia 1 de assinatura e criptografia

6. MECANISMO PARA TRANSFERÊNCIA SEGURA DAS IMAGENS.

Conforme especificado nos fluxos das mensagens de serviço, tanto o fluxo de troca de certificados quanto os fluxos de serviços que disponibilizam uma URL de acesso às imagens, podem ser encaminhadas as credenciais na estrutura de XML. As credencias são utilizadas na liberação do acesso as imagens localizadas pela URL.

6.1. ESTRATÉGIAS DE LIBERAÇÃO DE ACESSO

Aqui são especificadas as estratégias liberação de acesso para transferência das imagens. Cada estratégia define formato das credenciais e o mecanismo de transferência adotado.

IDENTIFICADOR DA ESTRATÉGIA: 1

Credencial	Formato: Immutable Universally Unique Identifier (UUID) (RFC 4122)
Domínio	Formato: IP ou domínio do emitente segundo DNS - RFCs 882 e 883, e foi atualizado nas RFCs 1034 e 1035
Transferência	Protocolo HTTPS (RFC's 822, 2616, 2660) (WebService REST Requests)
Assinatura de verificação	Calculada com HMAC-SHA1 (RFC 2104)

Mecanismo: A transferência inicia após o receptor resgatar a URL e a credencial da mensagem de serviço. Então, (1) o receptor prepara uma Request HTTPS, é colocado o domínio do receptor no cabeçalho dessa requisição. (2) a Assinatura de verificação é calculada usando a representação textual (String) do cabeçalho concatenada com a credencial. (3) a assinatura é adicionada ao cabeçalho da requisição que é enviada para o emitente da mensagem de serviço. (4) O emitente recebe a requisição e utiliza o domínio presente no cabeçalho para localizar a credencial correspondente. Após localizar a credencial, (5) O emitente calcula a assinatura de verificação. (6) O emitente compara a assinatura calculada com a assinatura recebida na requisição. A requisição é liberada se as assinaturas forem idênticas.

A Figura 8 ilustra o mecanismo da estratégia 1.

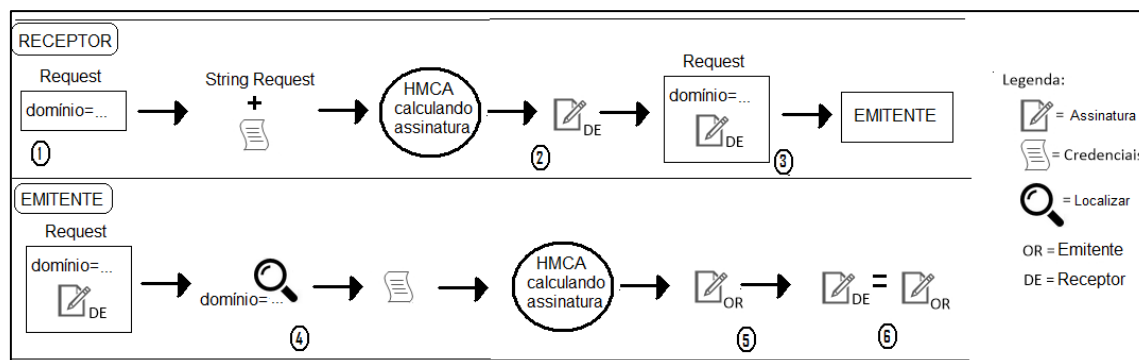


Figura 8 - Mecanismo da estratégia 1 de liberação e transferência