Instituto Superior de Engenharia do Porto

Implementação ESB numa unidade hospitalar

Uso normalizado de mensagens HL7

Ruben Fernando Santos Silva Ribeiro

Dissertação para a obtenção do grau de Mestre em

Engenharia Informática

Área de Especialização em

Arquiteturas, Sistemas e Redes

Orientador: Professor Doutor Ângelo Martins

Júri:

Presidente:

Professora Doutora Maria de Fátima Coutinho Rodrigues, Professora Coordenadora do Departamento de Engenharia Informática do Instituto Superior de Engenharia do Porto

Vogais:

Porto, Outubro de 2012

AGRADECIMENTOS

O meu agradecimento sentido é para a minha esposa Paula e meus filhos Bernardo e Francisco, que permitiram e sempre acreditam nas minhas capacidades assim como apoiaram as minhas decisões.

À restante família, agradeço a compreensão demonstrada, pela força que transmitiram que impulsionou o meu trabalho assim como de deram confiança para o futuro.

À unidade hospitalar pelo facto de ter acedido a realização deste estudo.

Ao Professor Doutor Ângelo Martins, orientador da dissertação, agradeço as horas de contacto presencial, assim como interlocutor com a unidade hospitalar e apoio nas demais valiosas contribuições para este trabalho.

RESUMO ALARGADO

Atualmente, os sistemas de informação hospitalares têm de possibilitar uma utilização diferenciada pelos diferentes intervenientes, num cenário de constante adaptação e evolução. Para tal, é essencial a interoperabilidade entre os sistemas de informação do hospital e os diversos fornecedores de serviços, assim como dispositivos hospitalares. Apesar da necessidade de suportar uma heterogeneidade entre sistemas ser fundamental, o acesso/troca de informação deve ser feito de uma forma protocolada, segura e transparente.

A infraestrutura de informação médica moderna consiste em muitos sistemas heterogéneos, com diversos mecanismos para controlar os dados subjacentes. Informações relativas a um único paciente podem estar dispersas por vários sistemas (ex: transferência de pacientes, readmissão, múltiplos tratamentos, etc.). Torna-se evidente a necessidade aceder a dados do paciente de forma consolidada a partir de diferentes locais. Desta forma, é fundamental utilizar uma arquitetura que promova a interoperabilidade entre sistemas.

Para conseguir esta interoperabilidade, podem-se implementar camadas de "middleware" que façam a adaptação das trocas de informação entre os sistemas. Todavia, não resolvemos o problema subjacente, ou seja, a necessidade de utilização de um standard para garantir uma interacção fiável entre cliente/fornecedor. Para tal, é proposto uma solução que passa por um ESB dedicado para a área da saúde, denominada por HSB (Healthcare Service Bus).

Entre as normas mais usuais nesta área devem-se salientar o HL7 e DICOM, esta última mais especificamente para dispositivos de imagem hospitalar, sendo a primeira utilizada para gestão e trocas de informação médica entre sistemas.

O caso de estudo que serviu de base a esta dissertação é o de um hospital de média dimensão cujo sistema de informação começou por ser uma solução monolítica, de um só fornecedor. Com o passar dos anos, o fornecedor único desagregou-se em vários, independentes e concorrentes, dando lugar a um cenário extremamente preocupante em termos de manutenção e evolução futura do sistema de informação existente. Como resultado do trabalho efetuado, foi proposta uma arquitetura que permite a evolução do sistema atual de forma progressiva para um HSB puro.

Keywords: ESB, HL7, Sistemas de Informação, HSB

ABSTRACT

Currently, healthcare information systems must customizable to meet each actor's needs, in a scenario of continuous adaptation and evolution. To achieve this it is essential interoperability between the multiple hospital information systems and between these and the external service providers'. Despite the need to support heterogeneous systems, access/exchange of information should be in a standard, secure and transparent way.

The infrastructure of modern health information consists of many heterogeneous systems, with different mechanisms to control the underlying data. Information on a single patient may be scattered across multiple systems (e.g. patient transfer, readmission, multiple treatments, etc.). It becomes evident the need to access patient data in a consolidated manner from different locations. Thus, it is essential to use an architecture that promotes interoperability between systems.

To achieve this interoperability, layers of "middleware" can be implemented that adapt information exchange between systems. However, this does not solve the underlying problem, namely the need to standardize information to ensure reliable interaction between customer / supplier. To this end, we propose a solution based on an ESB specially tailored for the healthcare business, the so-called HSB (Healthcare Service Bus).

Among the information exchange standards in this area, HL7 and DICOM are the most common, the latter specifically for hospital imaging devices, the first being used for information exchange between medical information systems.

The case study in this dissertation addresses the problems of a medium-sized hospital information system, which began as a monolithic solution from one supplier. Over the years, the sole supplier split into multiple competing suppliers, giving rise to a very worrying scenario in terms of maintenance and further development of the existing information system. As a result of this work, we propose an architecture that enables the gradual evolution of the current system to a pure HSB.

Keywords: ESB, HL7, Information Systems, HSB

ÍNDICE

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

ACRÓNIMOS

ASCII	-	american standard code for information interchange
CEI	-	common event infrastructure
EAI	-	enterprise application integration
EHR	-	electronic health record
EIS	-	executive information system
EJB	-	enterprise javabeans
EPR	-	electronic patient record
ERP	-	enterprise resource planning
ESB	-	enterprise service bus
FTP	-	file transfer protocol
HIPAA	-	health insurance portability and accountability act united states
HIS	-	hospital information system
HL7	-	health level 7
HSB	-	healthcare service bus
HTTP	-	hypertext transfer protocol
ISO	-	international organization for standardization
J2EE	-	java 2 enterprise edition
JMS	-	java message service
JMS	-	java message service
LDAP	-	lightweight directory access protocol
LIS	-	laboratory information system
MQ	-	message queue
OASIS	-	advancing open standards for the information society
OSI	-	open systems interconnection
REST	-	representational state transfer
RIS	-	radiology information
SCA	-	service component architecture
SCM	-	supply chain management
SDO	-	service data object
SI	-	sistema de informação

SLA	-	service level agreement
SMO	-	service message object
SOA	-	service-oriented architecture
SOAP	-	simple object access protocol
SOI	-	service-oriented infrastructure
SSL	-	secure sockets layer
TIC	-	tecnologias de informação e comunicação
VPN	-	virtual private network
WSDL	-	web services description language
XMLERP	-	extensible markup language enterprise resource planning
XQUERYSL	-	xml query service level agreement
XSLTEIS	-	extensible stylesheet language transformations executive information

CAPÍTULO 1

Introdução

Este documento descreve o trabalho de dissertação de mestrado na área de informática tendo como especialização o ramo de Arquitetura, Sistemas e Redes, tendo como caso de estudo um hospital de média dimensão da zona do Porto, no âmbito de uma parceria entre este e o ISEP[1]. Atualmente, a unidade hospitalar tem como um dos seus objetivos melhorar a interoperabilidade entre os diversos serviços assim como parceiros/fornecedores, especialmente quando se perspectiva a autonomização ou subcontratação de alguns serviços. Perante esta nova estrutura organizacional, torna-se necessário evoluir duma topologia cliente/servidor fechada, onde os diversos módulos do SI[2] estão integrados verticalmente não trocam facilmente informação entre si, para uma solução que favoreça a interoperabilidade dos sistemas internos e dos fornecedores.

A realidade do hospital em estudo não é muito diferente da de muitos hospitais nacionais e estrangeiros, pelo que o primeiro passo foi analisar o estado da arte das arquiteturas de sistemas de informação hospitalar. Após análise da realidade do hospital (sistemas de informação, unidades funcionais, etc.), foi proposto um cenário de troca de mensagens gerido por um Entreprise Service Bus (ESB) para o ambiente hospitalar. Neste tipo de ambiente, o ESB é usualmente apelidado de Heathcare Service Bus (HSB).

Um ESB é um modelo de arquitetura de software usado para projetar e implementar a interação e comunicação entre aplicações de software que interagem mutuamente numa arquitetura orientada a serviços (SOA). Como modelo de arquitetura de software para computação distribuída, o ESB é uma variante especial do modelo cliente/servidor orientado para a troca assíncrona de mensagens entre quaisquer elementos do sistema. O seu

[1] ISEP – Instituto Superior Engenharia do Porto

[2] SI – Sistema de Informação

principal uso é na interligação de aplicações heterogéneas e complexas, especialmente em cenários de contínua evolução/reconfiguração.

A implementação de um ESB é uma tarefa complexa, pois requer conhecimento profundo das trocas de informação do SI existente, sendo relativamente fácil menosprezar o esforço e o tempo de implementação. Existe para a área da saúde um "key player" no mercado com uma solução sólida para ESB, que é a IBM.

1.1 Objetivos

Foi proposto por uma entidade externa ao ISEP[3], um hospital da zona do Porto, no âmbito de uma proposta de dissertação de mestrado, que um aluno analisasse o atual modelo de informação que tem implementado e proporcionar uma solução para a interligação desse modelo com entidades externas e equipamentos ativo, assim como scanners, equipamento de laboratório etc.

Era necessário que para o novo modelo de sistema de informação fossem introduzidas normas da indústria hospitalar que garantam a interoperabilidade entre parceiros, fornecedores, equipamentos e possíveis extensões da unidade hospitalar em causa.

O trabalho de campo proposto foi o levantamento do sistema de informação que o hospital detém e avaliar a possibilidade de migrar para uma arquitetura orientada a serviços, eventualmente um ESB. Mais tarde, com o desenvolver do estudo, foi verificado que há soluções específicas de ESB para área da saúde, ou seja os HSB.

1.2 Contribuição e Motivação

No contexto em que o tema se insere, o facto de ter conseguido desenvolver a dissertação com factos reais e não teóricos são uma mais valia e motivação para conseguir atingir os objetivos de uma forma célere e o mais apurada possível.

[3] ISEP – Instituto Superior de Engenharia do Porto

O trabalho de campo foi bastante motivador pois o contacto com o ambiente e com as pessoas facilitam o desenrolar do estudo.

Nesta dissertação o estudo abordado é fundamental para o cenário inicial proposto a estudar pois possibilita a unidade hospital uma visão das necessidades reais de um ESB.
Este estudo também pode servir de referência para outras unidades hospitalares cujo cenário se possa verificar como semelhante.

1.3 Suporte institucional

Esta dissertação foi desenvolvida ao abrigo de uma colaboração entre o ISEP e o hospital, acordo este que possibilita a alunos de mestrado a realização dos trabalhos conducentes à dissertação em instituições que necessitem de apoio para áreas específicas de atuação.

1.4 Estrutura desta Dissertação

Esta dissertação está organizada da seguinte forma:

Capítulo 1 apresenta os principais objetivos que fundamentam este trabalho. Também faz transparecer uma descrição do contexto, motivação, contribuição e informação institucional.

Capítulo 2 fornece uma breve discrição de HL7 e foca em mostrar o estado de arte para o mesmo e sua evolução. A evolução e o estado de arte corrente de um ESB também são apresentados para melhor compreensão do leitor sobre o trabalho apresentado nesta dissertação.

Capítulo 3 este capítulo introduz os aspetos base que caracterizam um HSB, aqui são abordadas as questões de segurança, física e logica. As questões de segurança dos web services também são abordadas assim como a criptografia. Para facilitar a compreensão do conceito HSB é justificada a aplicabilidade do mesmo.

Capitulo 4 neste capítulo é apresentado o contexto atual da unidade hospitalar e a análise dos sistemas de informação, apresentando-se uma proposta de solução.

Capítulo 5 este capítulo é a conclusão desta dissertação onde é feita a análise a recolha de informação e proposta a possível solução para o problema descrito, solução esta que foi alcançada após estudo das possíveis soluções mais viáveis para a resolução do problema tendo como base o cenário proposto.

CAPÍTULO 2

Health Level 7 e o ESB

O Health Level 7 tem uma grande importância na área das tecnologias de informação no campo da saúde. Este conjunto de protocolos dá algumas garantias que a informação é trocada corretamente e facilita a interoperabilidade entre sistemas. Para poder apresentar este conceito, este capítulo demonstra um breve estado de arte sobre HL7, focando nos aspetos mais importantes e nos trabalhos mais relevantes que encontrei na literatura. É também dada especial importância ao ESB assim como abordar qual o posicionamento atual do ESB no mercado. O objetivo é dar ao leitor o conhecimento necessário acerca do que está a ser feito nestes campos de atuação.

2.1 Introdução ao Health Level 7

HL7 cria normas para ajudar os sistemas de informação dentro e entre organizações de saúde a comunicar uns com os outros. Em poucas palavras, quando implementado, utilizando-se uma implementação padrão que permite interoperabilidade dos sistemas de informações na área da saúde. O HL7 cria normas para a troca, gestão e integração eletrónica de informações de saúde.

HL7 comunica por mensagem entre os modelos, as mensagens podem ser expressas por campos ou por objetos. A comunicação HL7 fornece duas linhas para troca de dados, uma é o motor HL7 a outra é HL7 “ready”. O primeiro é objeto para o antigo sistema continuar a funcionar, este importa a interface do mecanismo para fazer o antigo sistema ter a capacidade de comunicar com outro sistema desenvolvido pelo critério HL7. O último é objeto para desenvolver novos programas, este usa o critério HL7 para integrar na plataforma diferentes aplicações que fornecem a entrada “standard” e saída. Também

utilizando o HL7 pode ser feita uma especificação da aplicação clínica e do registo de informações médicas, fornecendo o interface “standard” para o sistema de informação hospitalar e apoiar o critério de desenvolvimento de código. [Lanhua Zhang, Jan. 2011]

Health Level 7 (HL7) é um padrão internacional criado há mais de 20 anos. O tema central HL7 é a integração de dados clínicos e administrativos. Cria normas para a troca, gestão e integração eletrónicos de informações de saúde. Também desenvolve especificações, por exemplo, um padrão de mensagens que permite que diferentes aplicações da saúde possam trocar conjuntos de dados clínicos e administrativos. É credenciado pelo ANSI (America National Standards Institute) e com sede em Ann Arbor, Michigan.

O HL7 é também uma organização sem fins lucrativos cujos membros contribuem numa base de voluntariado. A organização (como tantas outras) tem como objetivo tornar-se o melhor padrão e o mais amplamente utilizado na indústria de cuidados de saúde que lidam com informática na saúde. Hoje, existem organizações filiais HL7 em mais de 40 países. Hospitais e demais estabelecimentos médicos costumam usar diferentes tipos de sistemas para comunicar uns com os outros. Tudo desde registos de pacientes com informações de faturação é monitorizado e gravado em sistemas de informação. Para que estes diferentes tipos de sistemas possam comunicar uns com os outros, eles usam um padrão como o HL7. [HL7.org]

“Level Seven" refere-se ao mais alto nível da Organização Internacional de Normalização (ISO[4]) das comunicações sendo segundo o modelo OSI[5], a camada de aplicação. O nível de aplicação define os dados a serem trocados, o momento da troca, bem como a comunicação de certos erros para a aplicação. O sétimo nível suporta funções tais como controlo de segurança, identificação do participante, verificações de disponibilidade, as negociações mecanismo de troca e o mais importante a estruturação de troca de informação.

O padrão HL7 é direcionado a desenvolvedores de software e fabricantes de equipamentos médicos com o objetivo declarado de normalizar as trocas e o registo da informação utilizada em unidades e organizações na área da medicina. Há outros padrões dedicados para o sector médico, mas em domínios muito específicos: farmácia, dispositivos

[4] ISO – International Organization for Standardization

[5] OSI – Open Systems Interconnection

médicos, imagiologia e seguros. O HL7 é, nesta matéria, dedicado ao processamento e gestão de dados administrativos e clínicos. O HL7 foca os seguintes campos / domínios [Cordos,Orza,Vlaicu,Meza,Avram,Petrovan, 2010]:

- Gestão do Paciente - admitir, descarga, transferência paciente (ADT);
- As consultas, os recursos (quartos, camas, aparelhos, etc.)
- Agendamento de pacientes
- Agendamento de procedimentos médicos, resultados
- Ensaios clínicos;
- Administração Financeira
- Documentos médicos
- Registos médicos
- Tratamentos médicos

A norma HL7 fornece uma sintaxe neutra para a representação de informação relacionada com a saúde, incluindo a criação de novos formatos de dados e customização de formatos existentes. A utilização desta norma permite que as aplicações utilizadas na área da saúde comunicarem entre si independentemente da plataforma de tecnologia de informação, arquitetura e linguagem de programação. [Corepoint Health, 2010]

O “standard” HL7 tem até aos dias de hoje três versões, nomeadamente:

- **HL7 - v1**
  - Introduzido em 1987, esta versão define o formato de representação das mensagens. Esta implementação era muito limitada em termos de funcionalidades dai ter rapidamente evoluído para a versão seguinte.

- **HL7 - v2**
  - Um ano após a primeira versão ou seja em 1988 chega a segunda versão, que depois de passar por algumas atualizações, foi credenciada só em 1994 pelo ANSI, tornando-se na prática o “standard“ para utilização na área da saúde. Esta versão é atualmente a que é mais utilizada no domínio da saúde. O uso de versões diferentes na norma HL7 não é um aspeto limitador ou redutor para a mesma uma vez que existe compatibilidade entre diferentes versões. As mensagens desta versão da norma HL7 representam dados de

diferentes fontes, tais como resultados e observações clínicas, a troca de dados do paciente, aplicações de serviços clínicos (laboratório, farmácia, triagem, etc.)

- O “standard” HL7 v2 tem ainda algumas ainda limitações. A entidade HL7 procurou abordar junto da comunidade e constatou lacunas entre elas as seguintes foram as mais relevantes que puderam ser constatadas:
  - Ausência de um modelo de dados
  - Falta de regras para o uso e para as aplicações
  - Redução do grau de flexibilidade e de escolha
  - Interoperabilidade pobre com as novas tecnologias (XML, WEB).

- **HL7 - v3**
  - As limitações apresentadas pela versão 2 da norma HL7 levaram a um subconjunto da comunidade HL7 propor a criação de uma nova versão, a versão 3, foram então definidos um conjunto de objectivos:
    - Internacionalização - A capacidade de qualquer organização usando o padrão HL7 v3 para atender às necessidades de variantes locais;
    - Modelo de dados consistente - A necessidade HL7v3 para definir um modelo de dados, usado por aplicações HL7, para garantir a consistência dos dados;
    - Necessidade Standard - A necessidade HL7v3 levar a informação aprendida com todas as versões HL7, criando um padrão que contém todos os dados que é necessário e um tanto vago e flexível;
    - Nova regra - Quando a comunidade começou a definir a versão 3, foi decidido que esta versão é incompatível com a versão 2 por várias razões. Primeiro, se a versão 3 fosse compatível com a versão 2, esta nova versão seria condicionada por problemas herdados da versão 2. Qualquer tentativa de reabilitar dados explícitos ou modelos aplicacionais da versão 2 seria muito difícil. Finalmente, a norma exige espaço para respirar e poder mudar radicalmente, melhorando assim a qualidade de interfaces clínicas.

2.1.1 Importância do HL7

A importância do uso do HL7 é realçada em muitos artigos de pesquisa, revistas, jornais de ciência, etc. Sendo assim, os factos mais relevantes que o justificam são:

- HL7 é um ANSI standard acreditado, o que facilita a interoperabilidade de sistemas.
- HL7 e apoiado pelo HIPAA[6] como sendo um dos mais importantes standards em cuidados de saúde.
- O standard HL7 é amplamente utilizado em muitos países, na tabela1 podemos ver os países onde existem escritórios da organização HL7.
- Um estudo de vários EHR standards mostra a relevância do standard HL7 no Mercado. [Thomas Aden, 2005]. A tabela 3 mostra a consolidação entre domínio da informática na saúde e o respectivo standard adotado.
- Evolução do protocolo HL7 pode ser observada na tabela 2.

Tabela 1 - Países que contêm escritórios HL7. [Imran Khan, 2007]

COUNTRY	WEBSITE
Argentina	http://www.hl7argentina.org.ar
U.K.	http://www.hl7.org.uk
Japan	http://www.hl7.jp
Ireland	http://www.hl7.ie
Germany	http://www.hl7.de
Finland	http://www.hl7.fi
China	http://www.hl7.cn/
Canada	http://hl7canada.cihi.ca/
Australia	http://www.hl7.org.au

[6] HIPAA – Health Insurance Portability and Accountability Act of United States

Tabela 2 - Evolução histórica HL7, [Imran Khan, 2007]

DATE	EVENT
Mar, 1987	Conception of HL7 standard
Oct, 1987	HL7 Version 1
1988	HL7 Version 2
1990	HL7 Version 2.1
1994	HL7 Version 2.2
1997	HL7 Version 2.3
1999	HL7 Version 2.3.1
2005	HL7 Version 3

Tabela 3 - Consolidação entre domínio da informática na saúde e o respectivo standard adotado. [Imran Khan, 2007]

DOMAIN	ADOPTED STANDARD
Laboratory Results Names	Logical Observation Identifiers Names and Codes (LOINC)
Messaging Standards: General	Health Level Seven (HL7)
Messaging Standards: Retail Pharmacy	National Council for Prescription Drug Programs (NCPDP) SCRIPT Transactions
Messaging Standards: Connectivity	IEEE 1073
Messaging Standards: Image information to workstations	Digital Imaging and Communications In Medicine (DICOM)
Medications	Federal Drug Standards
Interventions/Procedures: Lab Test Order Names	LOINC
Interventions/Procedures: Non-Laboratory	Systematized Nomenclature of Medicine, Clinical Terms (SNOMED CT)
Demographics	HL7
Immunizations	HL7
Lab Results Contents	SNOMED CT
Units	HL7
Anatomy	SNOMED CT for Anatomy
Diagnosis/Problem Lists	SNOMED CT
Nursing	SNOMED CT
Financial/Payment	Health Insurance Portability and Accountability Act of United States (HIPAA) Approved Code Sets and Transactions
Clinical Encounters	HL7
Text-Based Reports	HL7

2.1.2 Arquitetura do HL7

O Modelo de Referência de Informação (RIM [7]) é um modelo de informação para os dados na área da saúde desenvolvidos pelo Health Level 7 International (HL7). Baseado numa linguagem de modelação (UML [8]), o Modelo de Referência de Informação consiste num conjunto genérico de classes do qual as classes mais específicas na saúde são derivados. Por exemplo, subclasses da classe "agir" incluir a observação e procedimento.

A versão primeira versão do Modelo de Referência de Informação foi lançada em Junho de 1996, a versão 1.0 saiu em janeiro de 2001. RIM agora é utilizado em conjunto com sistemas de codificação.

A figura 1 mostra o diagrama de classes do Modelo de Referência de Informação.

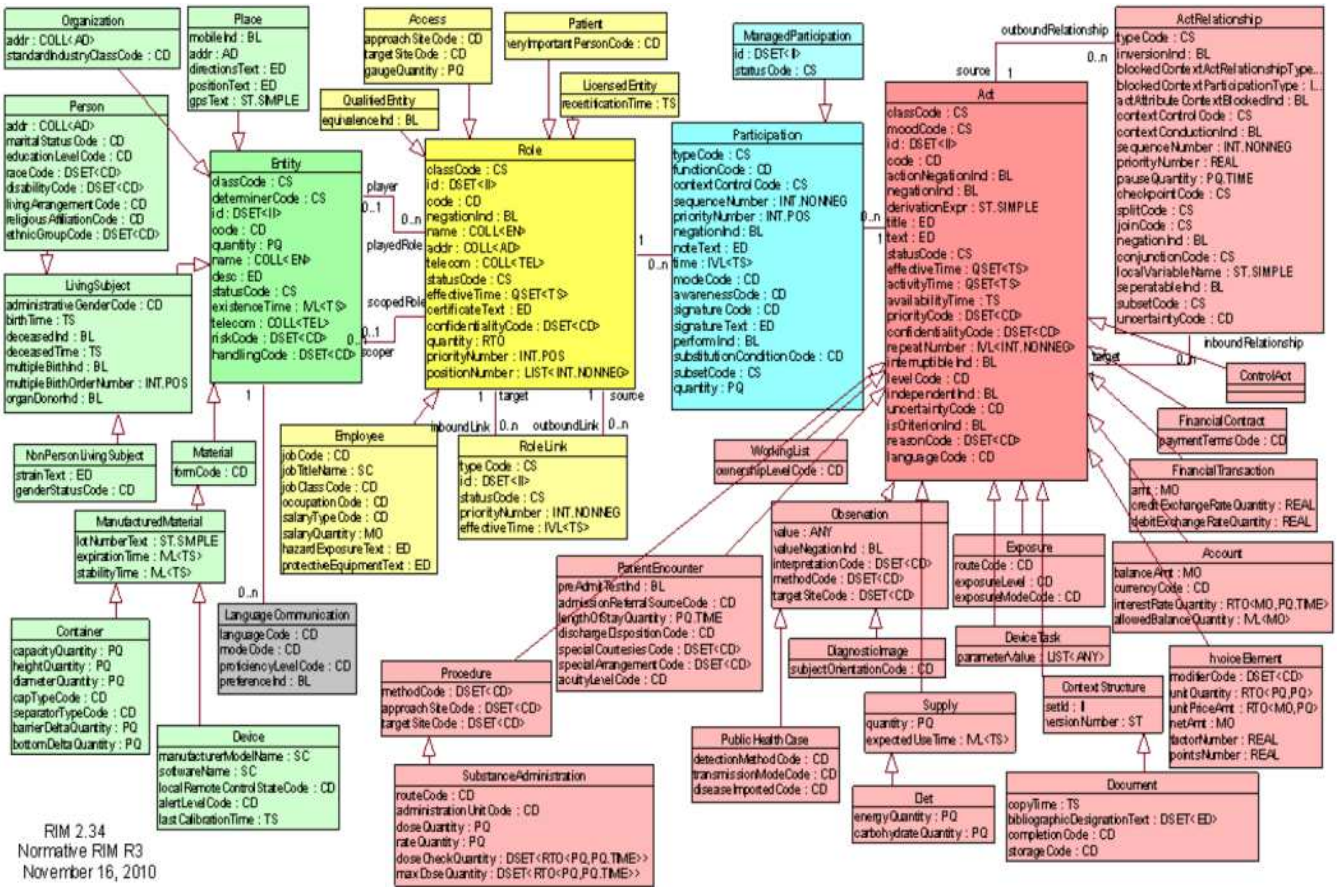

Figura 1 - Reference Information Model (RIM), [RIM 2.34, 2010]

[7] RIM – Reference Information Model

[8] UML- Unified Modelling Language

2.1.3 Tipo de mensagens e segmentos HL7

As mensagens HL7 geralmente são criadas e enviadas por um sistema de informação em resposta à ocorrência de determinado acontecimento. O evento pode ser algo como uma admissão do paciente, um resultado final de patologia, ou pode ser uma consulta a partir de um outro sistema, cada mensagem contém informações sobre esse evento.

Uma mensagem HL7 é composta por segmentos, cada um tendo um nome de três caracteres e um formato pré-definido de áreas específicas. Os campos são separados pelo caracter | (pipe), e pode ser dividida em subcomponentes com o caracter ^.

Os segmentos permitem agrupar informações relacionadas. Por exemplo, o segmento de PID contém informações do paciente, tais como números de identificação, nome, endereço e data de nascimento.

Diferentes eventos HL7 desencadeiam diferentes tipos de mensagens. Cada tipo de mensagem tem um conjunto definido de segmentos que são unidas para fornecer todas as informações necessárias sobre o evento. Alguns segmentos são obrigatórios, e deve ser incluído na mensagem, e os outros segmentos são opcionais. [Kestral Computing, 2012]

Abaixo podemos ver tipos de mensagens.

ADT (Admissão, Alta Medica e Transferência)

- EVN - event type segment
- PID - patient identification segment
- PV1 - patient visit segment
- PV2 - patient visit - additional information segment
- NK1 - next of kin / associated parties segment
- AL1 - patient allergy information segment
- NPU - bed status update segment
- MRG - merge patient information segment
- PD1 - patient additional demographic segment
- DB1 - Disability segment

Order Entry

- ORC - common order segment
- BLG - billing segment

Observations reporting

- OBR - observation request segment
- OBX - observation/result segment

Patient referral

- RF1 - referral information segment
- AUT - authorization information segment
- PRD - provider data segment
- CTD - contact data segment

Financial management

- FT1 - financial transaction segment
- DG1 - diagnosis segment
- DRG - diagnosis related group segment
- PR1 - procedures segment
- GT1 - guarantor segment
- IN1 - insurance segment
- IN2 - insurance additional information segment
- IN3 - insurance additional information, certification segment
- ACC - accident segment
- UB1 - UB82 data segment
- UB2 - UB92 data segment

Master files

- MFI - master file identification segment
- MFE - master file entry segment
- MFA - master file acknowledgment segment

Patient care

- GOL - goal detail segment
- PRB - problem detail segment
- ROL - role segment
- PTH - pathway segment
- VAR - variance segment

Scheduling

- ARQ - appointment request segment
- SCH - schedule activity information segment
- RGS - resource group segment
- AIS - appointment information - service segment
- AIG - appointment information - general resource segment
- AIL - appointment information - location resource segment
- AIP - appointment information - personnel resource segment
- APR - appointment preferences segment

Medical records/information management

- The segments are
- TXA - transcription document header segment
- OBX - observation segment usage

2.1.4 Uso de HL7

Tendo em consideração a enorme variedade de aplicações envolvidas nos processos médicos e a necessidade para troca de informação/dados entre esses processos, é claro que muitos destes interfaces de comunicações beneficiarão imenso com um padrão de comunicação.

O padrão HL7 vem exatamente resolver este problema e facilitar a penosa passagem de mensagens e troca de dados entre diversas aplicações, proporcionando uma estrutura muito precisa que deve ser cumprida par ser possível a troca de mensagens.

O sintagma “Level Seven” que faz parte do nome do padrão indica que este padrão pertence à sétima camada do modelo (OSI [9]), também chamado de camada de aplicação. Sendo assim, as aplicações médicas podem usar vários protocolos de comunicação, e no nível de aplicação que irá comunicar utilizando o padrão HL7.

O protocolo de comunicação mais utilizado para HL7 é o TCP/IP. [Alin Cordos, Bogdan Orza, Aurel Vlaicu,Serban Meza, Carmen Avram, Bogdan Petrovan, Octobrer 2010]

[9] OSI - Open Systems Interconnection

O Modelo OSI na implementação de TCP/IP para a comunicação é ilustrado abaixo:

OSI Model	
7	Application Layer **HL7**
6	Presentation Layer
5	Session Layer
4	Transport Layer
3	Network Layer
2	Data Link Layer
1	Physical Layer

TCP/IP Model	
7	Application Layer **HL7**
6	Doesn't exist
5	Doesn't exist
4	Doesn't exist
3	Doesn't exist
2	Host-to-Network
1	

HL7 Application (client or server), Telnet, DNS, FTP, SMPT, POP3, HTTP, etc.	Application
TCP UDP	Transport
IP	Network
LAN, WAN, Radio with packets	Physical and Data Link

Figura 2 - Comparação entre os modelos OSI e TCP/IP

Na figura seguinte podemos visualizar um caso de uso com recurso a troca de mensagens HL7. Aqui podemos ver a troca de mensagens HL7 neste caso versão 3 entre colaboradores da admissão, clinica, cobrança e laboratório.

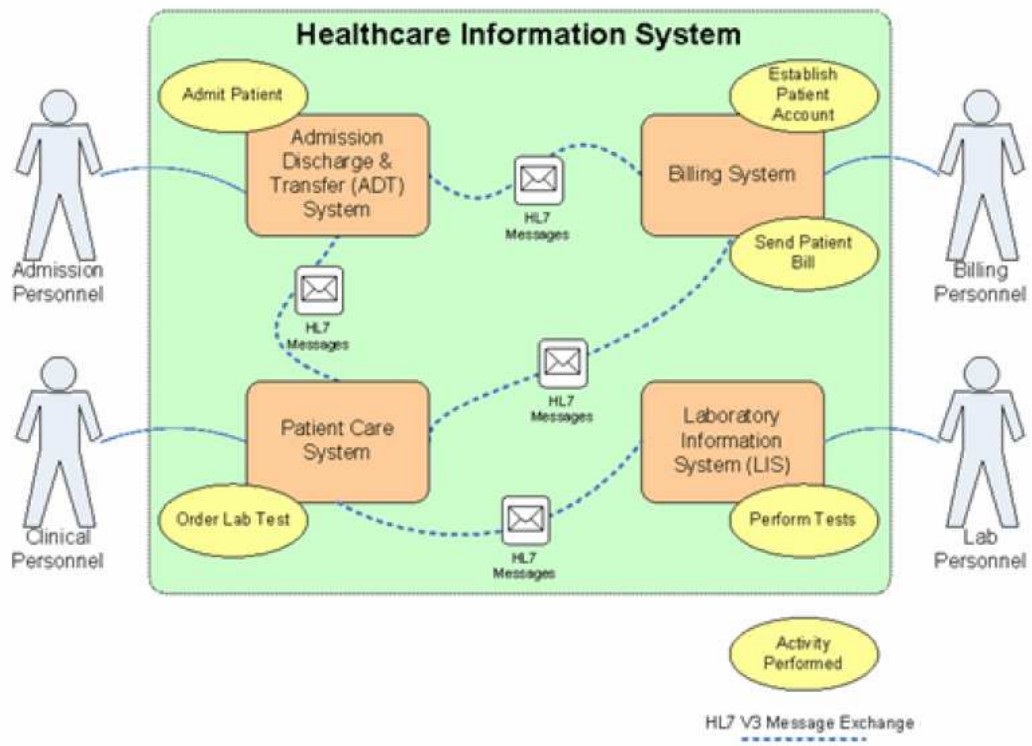

Figura 3 - Utilização HL7 (troca de mensagens)

Um cenário usado atualmente por “Medical-Objects” é normalmente utilizado para explicar o uso de um sistema de informação e como este interage com a base de dados.

A figura 4 representa um diagrama de sequência que descreve passo a passo o processo de aceder a uma base dados utilizando mensagens HL7 num determinado ponto. Neste diagrama de sequência é utilizado para explicar a interação e para mostrar que medidas foram tomadas no processo de acesso a uma base de dados.

Quando as mensagens HL7 são armazenadas numa base de dados as colunas e tabelas são definidas pelos segmentos HL7 de uma mensagem. Nem todos os segmentos são utilizados como mensagens HL7 pois estes contêm grandes quantidades de campos que nem sempre contêm dados que são necessários, de modo que os dados são armazenados como BLOBS e são recuperados por meio de métodos de indexação e de extração quando assim é necessário. [Lynden Crawford, 2010]

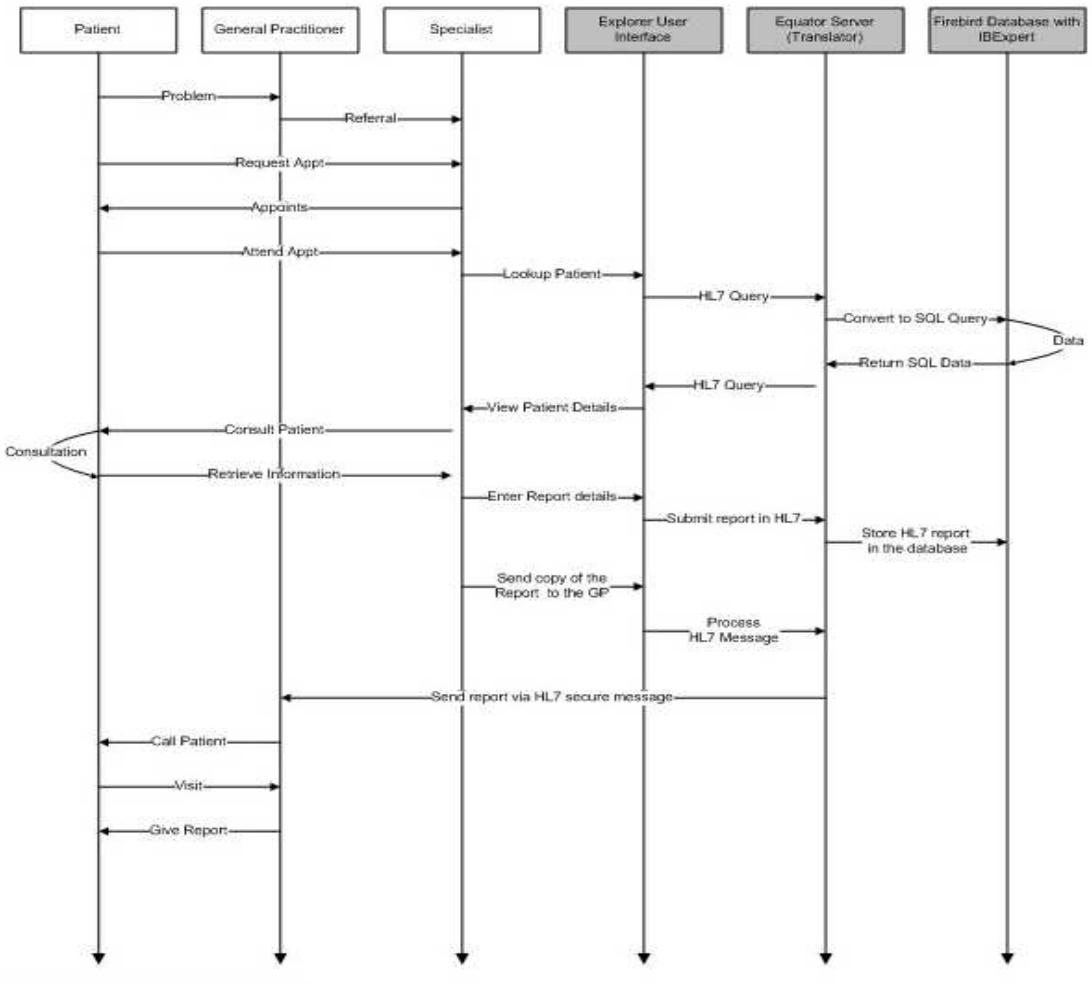

Figura 4 – Diagrama Sequencia troca menagens HL7 [Lynden Crawford, 2007]

Na Figura a baixo podemos ver mais uma troca de mensagens HL7

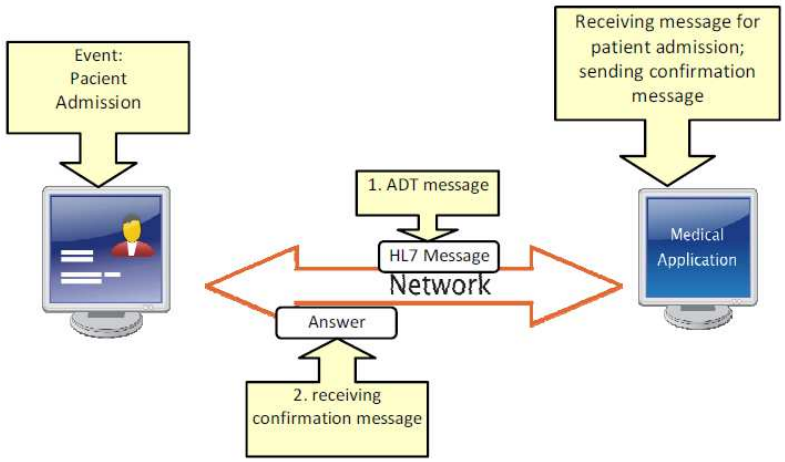

Figura 5 – Exemplo Utilização Mensagens HL7 [Cordos,Orza,Vlaicu,Meza,Avram, Bogdam, Petrovan, 2010]

2.2 Introdução ao Enterprise Service Bus

Arquiteturas Orientadas a Serviços (SOA[10]) oferecem uma abordagem flexível, extensível e compatível para reutilização e extensão de aplicações existentes assim como construção de novas. A característica mais importante de um sistema SOA é a flexibilidade para tratar elementos de processos de negócios e elementos subjacentes à infraestrutura como a segurança e serviços padronizados que podem ser reutilizados sem as preocupações de mudanças aos requisitos de negócio iniciais. Serviços baseados em SOA têm interfaces bem definidas que são estruturadas por um conjunto de mensagens que o serviço recebe e envia, mais uma implementação da interface.

Um Enterprise Service Bus (ESB) é um "standard" de arquitetura que suporta virtualização e gestão das interações de serviço entre a comunicação dos participantes. Este atua como um intermediário para serviços de conectividade entre os prestadores de serviço e solicitantes para SOA. A conectividade é flexível e estruturada que facilita a integração de sistemas seguros, reduzindo o número, tamanho e complexidade de interfaces de aplicações [Grund, Rexroad, 2007].

As Redes empresariais atuais normalmente implementam centenas de aplicações de diferentes fornecedores. Existe pouca ou nenhuma padronização de protocolos de comunicação entre os sistemas individuais da empresa, e as trocas de dados entre aplicações de diferentes fornecedores é surpreendentemente difícil de conseguir. A falta de um padrão para a plataforma de aplicações empresariais distribuídas aumenta o custo e a complexidade do desenvolvimento assim como a implantação de soluções de negócios. Padrões emergentes e outros para as comunicações entre as diversas aplicações nas empresas, a conectividade, a portabilidade, a transformação e a segurança tentaram simplificar a integração da empresa assim como resolver o problema do "middleware".

O Enterprise Service Bus (ESB) é uma nova geração de middleware da empresa destinadas a atenuar estes e outros problemas que possam surgir. Um Enterprise Service Bus fornece uma oportunidade para aplicar à indústria um padrão verdadeiramente aberto, heterogéneo, num melhor ambiente baseado em standards.[Fiorano ESB, 2011]

[10] SOA – Arquitetura Orientada para o Serviço.

Um ESB é a base SOA para toda a empresa, permitindo as empresas integrar aplicações e processos baseados em standards, serviços orientados ao evento altamente distribuídos, com uma infraestrutura gerida centralmente.

A arquitetura distribuída do ESB potencia a escalabilidade e a robustez do sistema de informação. Os serviços de um ESB (incluindo as aplicações / lógica de negócio, bem como transformações fundamentais, roteamento, conectividade e distribuição de serviços) podem ser implementados e geridos a partir de qualquer localização física na rede da empresa. Construído inteiramente em padrões da indústria, incluindo XML e Web services, os ESBs permitem desenvolver soluções de integração abrangentes e acessíveis através da promoção da reutilização de componentes e da flexibilidade de configuração, inclusive em tempo real. Um ESB é uma plataforma da empresa que implementa interfaces padronizadas para comunicação, conectividade, transformação, portabilidade e segurança. [Fiorano ESB, 2011]

Atualmente no mercado existe varias empresas que comercializam ESB's, destas salientam-se três empresas, tanto pela sua dimensão neste tipo de mercado como pelas soluções que foram implementadas. A IBM com o "websphere", a Microsoft com o "biztalk" e a Fiorano com o seu ESB baseado em JMS.

Na perspectiva da Microsoft, um Enterprise Service Bus (ESB) é um padrão de arquitetura e uma ferramenta fundamental na implementação da infraestrutura para uma arquitetura orientada a serviços (SOA). Um ESB é apenas um dos muitos componentes necessários para construir uma infraestrutura abrangente orientada a serviços (SOI[11]). A crescente adoção de SOA e a proliferação de serviços Web têm revelado uma necessidade cada vez maior em fornecer uma camada de ligação entre os seus serviços e seus consumidores. Um ESB fornece suporte para a interação entre os serviços heterogéneos e interfaces que podem ser incompatíveis, ou que podem mudar ao longo do tempo de acordo com as necessidades do negócio.

Um ESB é vocacionado em resolver problemas de integração de uma forma que maximiza a reutilização de serviços ao mesmo tempo que mantém a flexibilidade dos mesmos. [Microsoft BizTalk, 2011]

O termo ESB é amplamente utilizado no contexto de implementação de uma infraestrutura para permitir uma arquitetura SOA. No entanto, no mundo real a experiência

[11] SOI – Service Oriented Infrastructure

com a implantação de SOA demonstrou que um ESB é apenas um dos muitos blocos de construção que compõem um SOI. O termo ESB transformou-se em diferentes direções, e sua definição depende da interpretação individual do ESB e nos requisitos de fornecedores de plataformas de integração SOA. A Microsoft com base na sua experiência conseguiu efetuar muitas implementações SOI de sucesso do mundo real. Podemos pensar que um ESB é como uma coleção de padrões de arquitetura baseada na integração de aplicações corporativas tradicionais (EAI[12]), middleware orientado a mensagem, serviços Web, .NET e interoperabilidade Java, integração de sistemas "host" e interoperabilidade com registos de serviços e repositórios. [Microsoft BizTalk, 2011]

Porquê recorrer ao uso de um ESB?

Um ESB é uma construção de arquitetura de software que fundamentalmente disponibiliza um motor de mensagens, o (BUS) para serviços de arquiteturas complexas via "event-driven" e "standards-based".

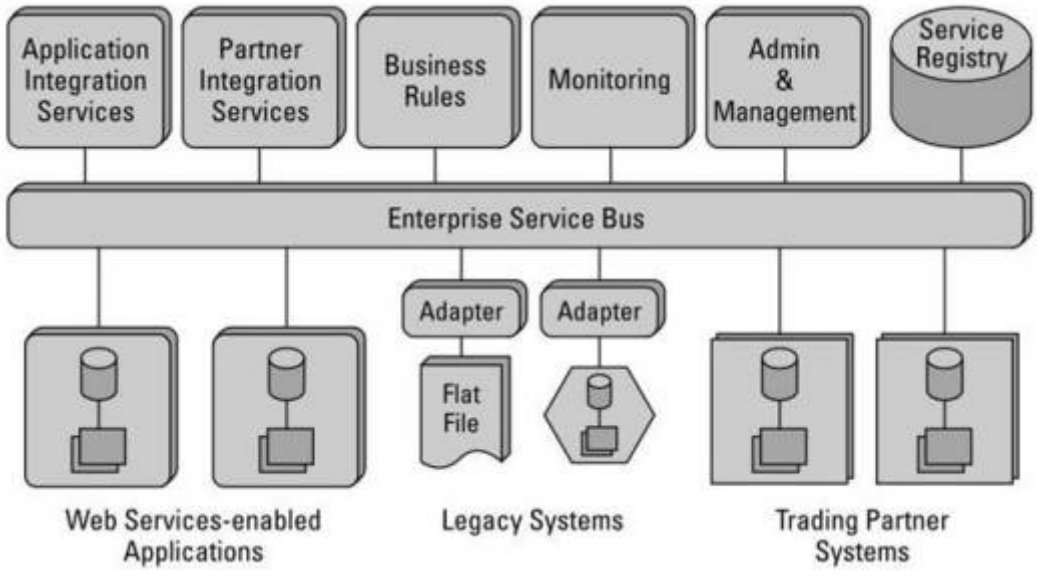

Figura 6 – Arquitetura ESB [IntroPro, 2012]

O ESB geralmente disponibiliza uma camada de abstração em cima de uma implementação de um sistema de mensagens da empresa, que permite aos

[12] EAI – Enterprise Application Integration

desenvolvedores de integração explorar o valor das mensagens sem escrever código. Ao contrário de uma abordagem clássica de integração entre aplicações que corresponde a uma abordagem de arquitetura monolítica, um enterprise service bus é construído sobre a base de funções divididas nas suas partes constituintes, com a implantação distribuída quando necessário.

Neste tipo de arquitetura, o ESB representa a parte do software que fica entre as aplicações de negócios e permite a comunicação entre eles. Idealmente, o ESB deve ser capaz de substituir todo contacto direto com as aplicações no “bus”, de modo que toda a comunicação seja realizada através do ESB.

Para atingir este objetivo, o ESB deve encapsular a funcionalidade oferecida pelas aplicações que o compõem de forma significativa. Isto ocorre tipicamente através da utilização de um modelo de mensagens empresariais. O modelo de mensagem define um conjunto padrão de mensagens que o ESB irá enviar e receber. Quando o ESB recebe uma mensagem, encaminha a mensagem para a aplicação correta. Muitas vezes, porque a aplicação evolvida não utiliza o mesmo modelo de mensagem, o ESB terá que transformar a mensagem num formato que a aplicação a possa interpretar.

Um software "adaptador" cumpre a tarefa de efetuar essas transformações (de forma análoga a um adaptador físico).

É expectável que um ESB tenha as seguintes características:

- Agnosticismo geral de sistemas operativos e linguagens de programação, por exemplo, deve permitir a interoperabilidade entre Java e .Net.
- Uso de XML como linguagem de comunicação padrão
- Suporte de standards para web-services
- Suporte para vários padrões de troca de mensagens (MEPs[13]) (por exemplo: pedido síncrono / resposta, pedido assíncrono / resposta, “send and forget”, publish / subscribe)
- Adaptadores para apoiar a integração com sistemas legados, possivelmente com base em padrões como o J2EE Connector Architecture (JCA[14])

[13] MEP – Message Exchange Protocol

[14] JCA – Java Connector Architecture

- Um modelo padronizado de segurança para autorizar, autenticar e auditar o uso do ESB
- Facilitação dos formatos de dados e transformação de valores, incluindo serviços de transformação, muitas vezes através de Extensible Stylesheet Language Transformation (XSLT) ou XQuery, entre os formatos de origem e de destino das aplicações.
- Validação contra esquemas de mensagens enviadas e recebidas
- Capacidade de aplicar regras de negócio de maneira uniforme
- Enriquecimento da mensagem proveniente de outras fontes
- Divisão e combinação de várias mensagens e tratamento de exceções
- Encaminhamento de mensagens condicional ou a transformação com base em uma política de não centralizada (sem "core" central de regras)
- "queuing" de mensagens e pausa quando as aplicações se tornam indisponíveis temporariamente

Os principais benefícios do ESB são:

- Manutenção mais rápida e económica dos sistemas existentes
- Maior flexibilidade, fácil modificação de acordo com as mudanças de requisitos
- Baseados em padrões ("standards")
- Escalabilidade a partir do ponto de soluções com ESB para toda a empresa (implantação de bus distribuídos)
- Tipos de serviço pré-definidos prontas para o utilização
- Mais configuração em vez de integração de codificação
- Nenhum motor central de regras ou "broker" central é necessário
- Atualização incremental com zero em tempo de indisponibilidade do serviço

Transparência de localização:

O ESB está isolado das alterações de localização, o serviço cliente não necessita de ter a manutenção do Universal Resource Locator (URL[15]) do serviço web. É sim necessário o URL do ESB, que acuará como o serviço web para o cliente. O ESB irá reencaminhar o pedido para o URL apropriado e devolverá a resposta ao cliente.

[15] URL – Universal Resource Locator

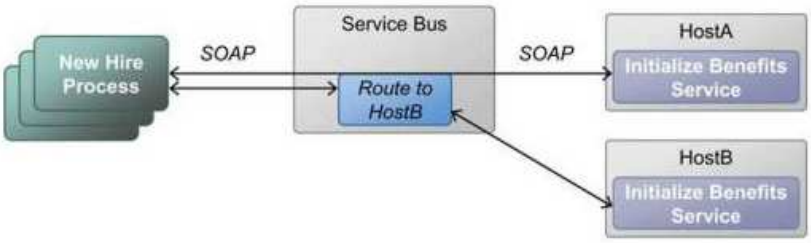

Figura 7 – Transparência Localização (URL) ESB [IntroPro, 2012]

Compatibilidade com versões anteriores:

O ESB está isolado das alterações/mudanças de interface:

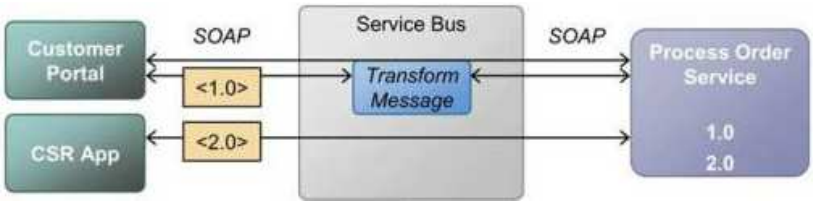

Figura 8 – Compatibilidade de mensagens ESB [IntroPro, 2012]

Os dados do pedido podem ser facilmente e eficientemente transformados antes de ser enviados para o respectivo serviço, a mesma circunstância é aplicada ao cliente ou seja os dados podem ser transformados antes do envio para o respectivo cliente do serviço web.

Ativação de serviços:

O ESB permite que múltiplos protocolos/mensagens participar em SOA:

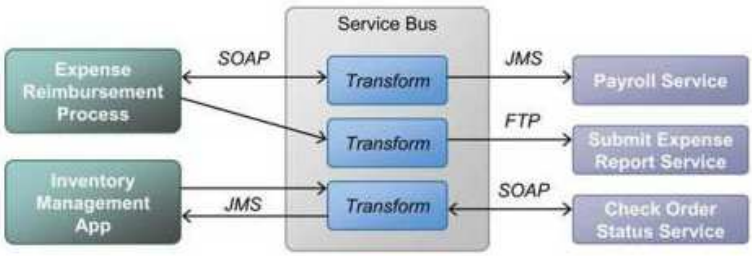

Figura 9 – Compatibilidade mensagens ESB [IntroPro, 2012]

Encaminhamento dinâmico:

O ESB utiliza regras de negócio para determinar o destino do serviço.

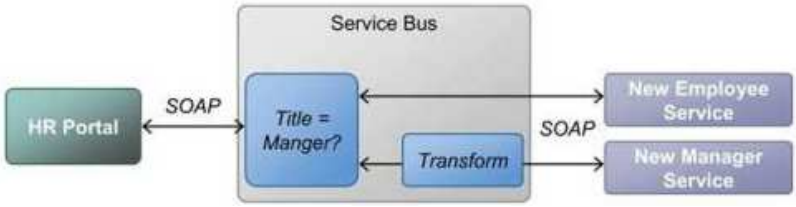

Figura 10 – Encaminhamento dinâmico mensagens ESB [IntroPro, 2012]

Enriquecimento de mensagens:

Uma mensagens pode ser enriquecida com a utilização da resposta de outro serviço:

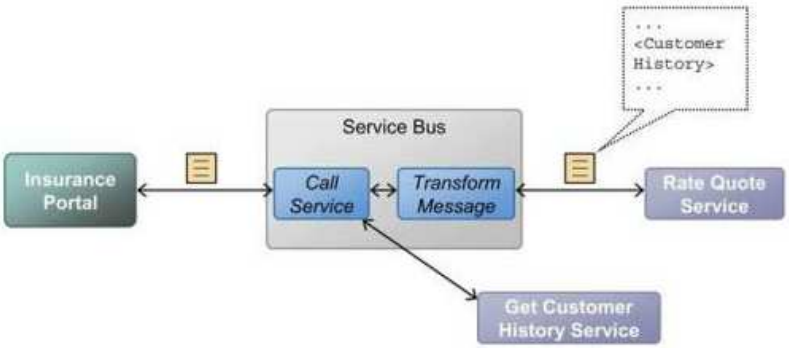

Figura 11 – Enriquecimento de mensagens ESB [IntroPro, 2012]

Orquestração de Serviços:

Uma tarefa comum é também uma composição de novos serviços a partir dos já existentes:

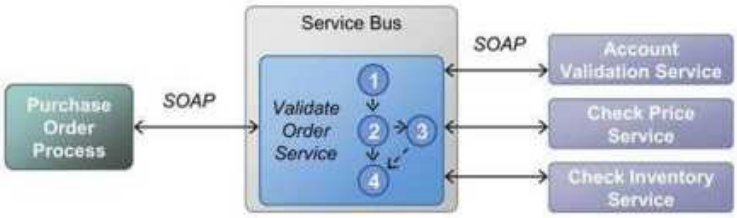

Figura 12 – Orquestração de Serviços ESB [IntroPro, 2012]

2.2.1 ESB (Fioriano) :

O ESB da Fiorano é um Enterprise Service Bus que permite às empresas integrar aplicações e processos transversalmente a todos os departamentos da empresa usando um serviço padrão tipo (SOA). Com uma arquitetura altamente distribuída, mas mesmo assim gerido centralmente, este ESB pretende superar os problemas de fornecedores de software de integração monolítica e serviços de aplicação.

Este permite as empresas recorrerem a lógica de negócios existente e residente em qualquer lugar dentro da empresa para montar rapidamente soluções eficientes para os negócios.

A arquitetura Fiorano ESB é baseada em “event-driven“ ou seja é “guiada” por eventos, permite melhor capacidade de resposta para mudanças nas condições de negocio, levando a uma flexibilidade incomparável e aumento de produtividade.

O Fiorano ESB foi implantado em grande escala, seguras, ambientes de missão crítica. Com uma aplicação de serviços distribuída, Fiorano ESB permite a reutilização eficaz, permitindo que projetos possam ser escalados de forma incremental e estendidos por toda a empresa.

O Fiorano ESB foi projetado tendo como base a fiabilidade e flexibilidade, permitindo assim um design de aplicação lógica a ser mapeada diretamente para a implementação física, tornando o processo de desenvolvimento mais intuitivo e mais fácil do que o de utilização de “suites” de integração convencionais.

A arquitetura de serviços de ESB distribuídos da Fiorano permite a reutilização eficaz, fornecendo a capacidade de extrair valor de negócio do negócio existente e aplicações legadas, permitindo a fácil coordenação de processos através de redes heterogéneas.

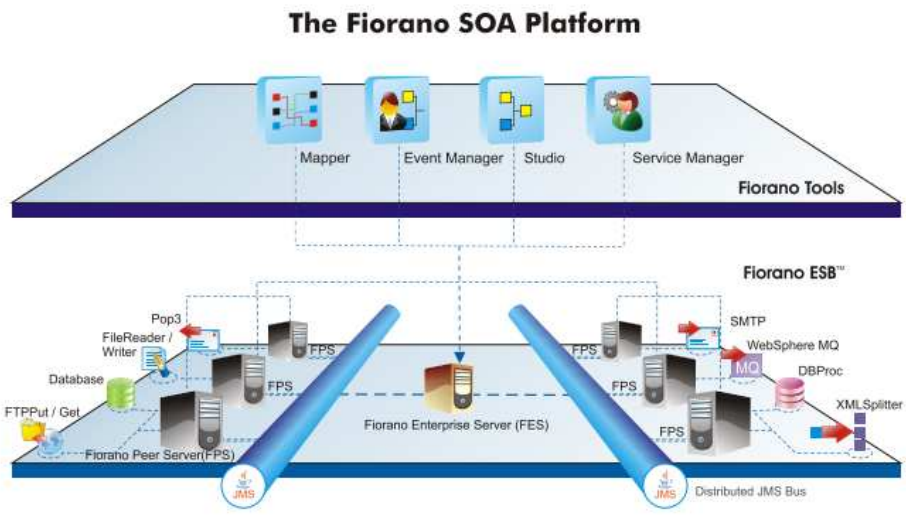

Figura 13 – Plataforma SOA Fioriano [Fiorano, 2011]

Comunicação:

Infraestrutura de comunicação: (ex.: JMS[16]).

Os serviços necessitam de comunicar com fiabilidade entre si através da rede. Fiabilidade, escalabilidade, comunicações robustas e independentes da localização, reduzem o tempo de desenvolvimento de aplicações para sistemas distribuídos assim com aumentam a sua fiabilidade.

Conectividade:

A conectividade baseada em standards, incluindo serviços Web, Java 2 Enterprise Edition (J2EE[17]) e adaptadores .NET. (Suns J2EE e Microsoft .NET que são os dois tipos de frameworks de arquitetura de computação distribuída dominante. J2EE oferece portabilidade de um único idioma [Java] sobre vários sistemas operacionais e plataformas de hardware. .NET suporta uma grande variedade de linguagens de programação, mas é principalmente ligada à Microsoft (sistema operativo Windows e hardware Intel). Para extrair dados de um serviço é preciso primeiro ser capaz de facilmente poder ligar-se a esse serviço. Na ausência de qualquer padrão standard tal torna-se difícil.

[16] JMS – Java Message Service

[17] J2EE – Java 2 Enterprise Edition

Transformação:

A transformação é baseada em standards de motores de transformação (por exemplo, XSLT[18] e XQuery[19]). Dados produzidos por um determinado serviço que normalmente não é facilmente compreendida por outro serviço, para tornar os dados digestíveis por outro serviço, ele primeiro precisa de ser devidamente transformado.

Portabilidade:

As implementações modernas de um ESB tipicamente suportam o desenvolvimento em múltiplas linguagens de programação. Isso, juntamente com a portabilidade inerente à infraestrutura ESB, faz com que o Enterprise Service Bus seja verdadeiramente o "backbone" da empresa que suporta multilingua (programação) assim como multiplataforma. A maioria das empresas tem uma variedade de sistemas informáticos, que vão desde tablets, PCs[20] de trabalho (Windows), servidores UNIX, servidores Windows e sistemas de mainframe[21]. Portabilidade e facilidade de comunicação entre diferentes ambientes operacionais permanecem preocupações para soluções corporativas.

Segurança:

A segurança é baseada em standards tais como LDAP[22] e SSL[23].

Toda a conectividade e comunicações entre os serviços da empresa precisam de ser seguros de acordo com as necessidades da mesma. Para tal é necessário fazer uso de firewall[24], a segurança é muito importante.

[18] XSLT – Extensible Stylesheet Language Transformations

[19] XQuery – XML Query

[20] PC – Computador Pessoal

[21] mainframe – Computadores com grande capacidade de processamento

[22] LDAP - Lightweight Directory Access Protocol

[23] SSL - Secure Sockets Layer

[24] Firewall – Equipamento ativo de rede que permite negar ou permitir acesos.

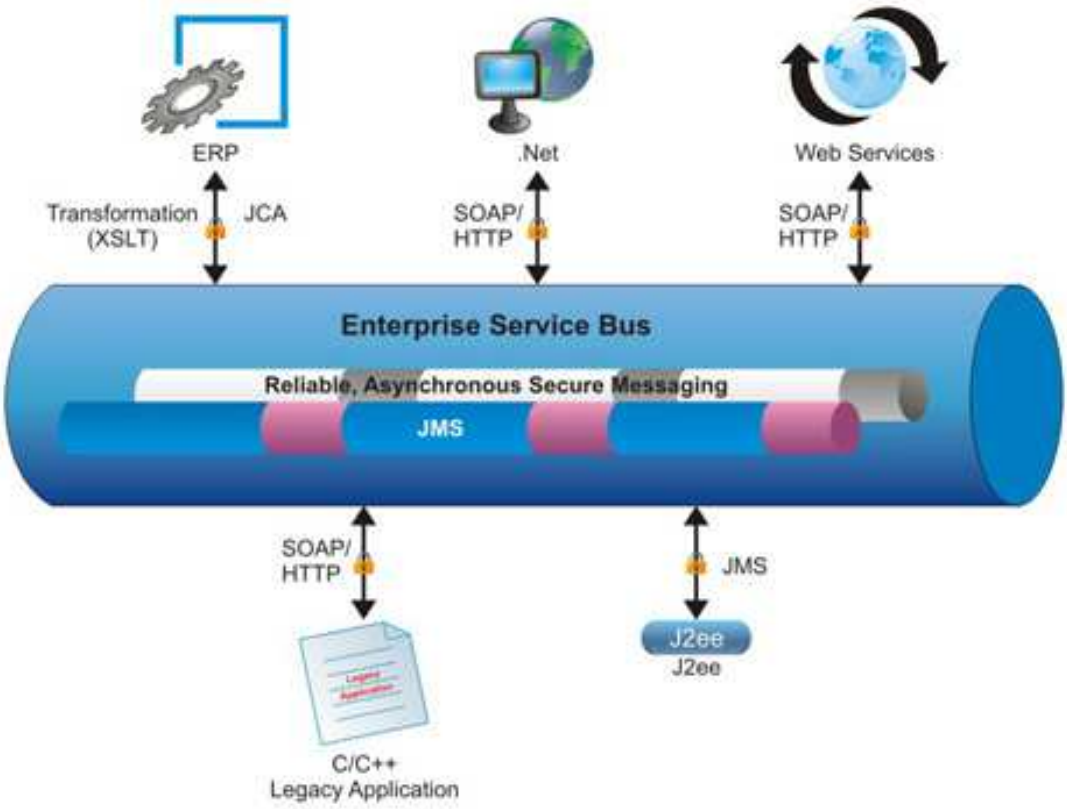

Figura 14 – Modelo de um ESB [Fiorano, 2011]

2.2.2 BizTalk ESB (Microsoft BizTalk)

O BizTalk ESB Toolkit consiste numa série de componentes de interoperabilidade que permitem apoiar e implementar um ambiente de mensagens flexível que torna mais fácil para construir aplicações baseadas em mensagens. Os serviços e componentes encaixam-se nas seguintes categorias:

- Serviços web. Tem com finalidade expor serviços internos, tais como processamento de itinerário, gestão de exceções, resolução de terminais e mapas das operações do BizTalk, assim como transformação de mensagens.
- Serviços de itinerário. Estes incluem serviços de orquestração baseada em mensagens para a realização de itinerário para roteamento baseado em Microsoft BizTalk. Podem ser criados serviços personalizados para roteamento baseado em Itinerários.
- Itinerário "on-ramps". Estes recebem mensagens externas e anexam o itinerário adequado para cada mensagem e executam o processamento de itinerário.
- Rampas de acesso. Estas receberem mensagens externas de uma gama de formatos e meios de transporte, tais como HTTP[25], JMS, WMQ, FTP[26], Flat File[27], e XML.
- "Off-ramps". Estes implementam portas de envio para a entrega de mensagens usando formatos e transportes, tais como SOAP, WCF, JMS, WMQ, FTP, HTTP, Flat File, XML, ou quaisquer outros formatos personalizados.
- Gestão de exceções. Isto inclui exceções para serviços Web, a API de gestão e componentes que enriquecem e permitem processar e transmitir os detalhes da exceção portal de gestão do ESB.
- Gestão do portal ESB. Isto proporciona o provisionamento de registos, mediação de exceções, notificações de alerta e análises.

[25] HTTP – Hypertext Transfer Protocol

[26] FTP – File transfer protocol

[27] Flat File – Ficheiro sem protocolo associado

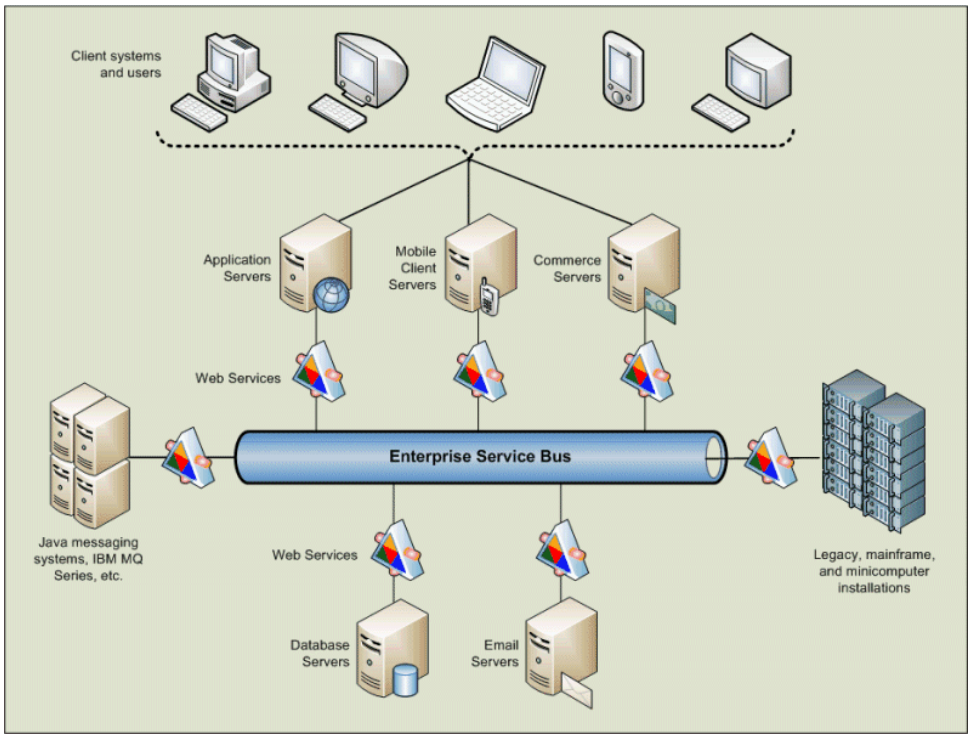

Figura 15 - Modelo de alto nível ESB [Microsoft BizTalk, 2011]

O BizTalk ESB Toolkit aceita mensagens de entrada e opera sobre elas, por vezes (mas não sempre) através da realização de processos como a transformação, a entrega ou qualquer outro processo personalizado definido.

Para especificar as operações necessárias, os componentes do núcleo de processamento requerem uma mensagem que contem instruções associadas ou meta dados que definem os processos a aplicar e as tarefas a executar ao conteúdo da mensagem.

Esta abordagem fornece acoplamento fraco entre os serviços, o que significa que o ESB não exige conhecimento prévio do processamento específico para cada mensagem. Este só tem que saber o leque de processos possíveis e como o aplicar a cada processo

A ampla gama de opções para especificar os processos disponíveis e o mapeamento entre os processos e as instruções dentro de mensagens fornecem um mecanismo flexível para a configuração e ajuste de comportamento sem exigir alterações no código e consequentemente reafectação de componentes. [Microsoft, 2011]

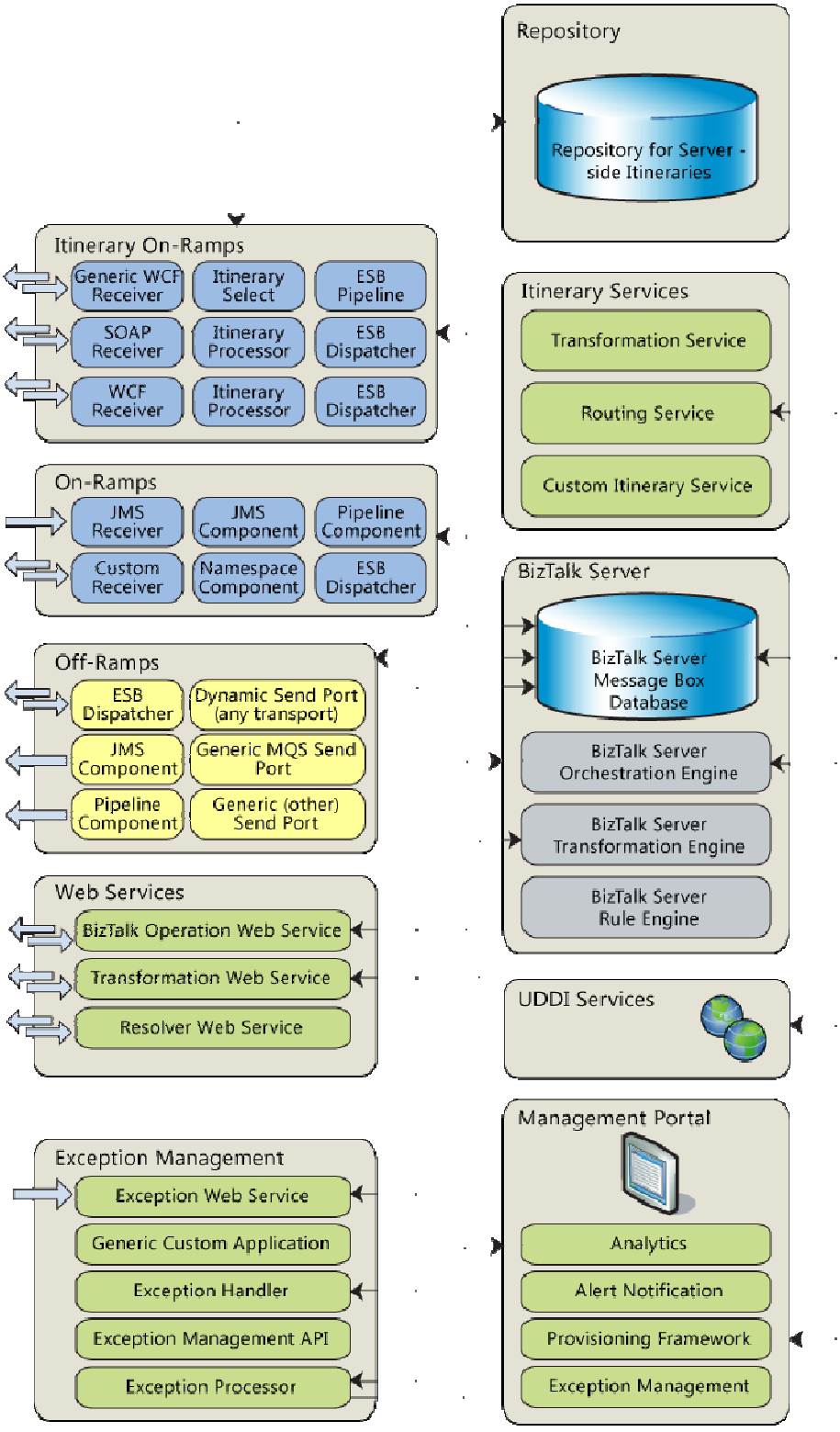

Figura 16 – Arquitetura e componentes do toolkit BizTalk. [Microsoft, 2011].

2.2.3 IBM WebSphere ESB

O WebSphere Enterprise Service Bus fornece uma infraestrutura do tipo ESB para permitir a interligação de aplicações que têm como base padrões de interfaces (tipicamente um interface de serviço web descrito em WSDL[28]). Este disponibiliza mecanismos para processar pedidos e respostas aos consumidores e prestadores de serviços web que se ligam ao ESB.

WebSphere Enterprise Service Bus é a camada de mediação que funciona por cima da camada de transporte dentro do WebSphere Application Server. Assim sendo o WebSphere Enterprise Service Bus fornece funções de mediação pré-definidas e ferramentas fáceis de usar para permitir a rápida construção e implementação de um ESB como um valor agregado em cima do WebSphere Application Server.

O WebSphere Enterprise Service Bus é equivalente ao WebSphere Application Server Network Deployment que utiliza as suas qualidades de serviço, com o seu "clustering", "failover", escalabilidade, segurança e um fornecedor de mensagens "built-in". Com essas qualidades, o WebSphere Enterprise Service Bus inclui uma série de características-chave relacionadas com o WebSphere Application Server, incluindo UDDI, registo de serviço, o gateway de serviços Web, o Tivoli Access Manager, DB2 Universal Database, e componentes "Edge".

WebSphere Enterprise Service Bus acrescenta o seguinte valor para o servidor de aplicações:

- Fornece funções de mediação que podem ser utilizadas para criar uma lógica de integração para conectividade.
- O modelo de programação SCA[29] suporta o rápido desenvolvimento de componentes de fluxo de mediação.
- WebSphere Integration Developer é uma ferramenta "easy-to-use" ferramenta que suporta WebSphere Enterprise Service Bus.
- Aproveitando o WebSphere Application Server, WebSphere Enterprise Service Bus oferece interoperabilidade para sistema de mensagens JMS e WebSphere MQ[30] na

[28] WSDL – Web Service Definition Language

[29] SCA - Service Component Architecture

troca de mensagens, bem como um pacote abrangente para conectividade de clientes.

- Dispõem de suporte para J2EE Connector Architecture baseados em adaptadores WebSphere.

De acordo com a IBM, para implementar corretamente SOA é necessário ter um modelo único de invocação e um modelo único de dados. O Service Component Architecture (SCA) é o modelo de invocação, cada componente de integração é descrito através de uma interface. Estes serviços podem então ser assemblados num editor de assemblagem de componentes, permitindo assim uma solução encapsulada e muito flexível.

O WebSphere Enterprise Service Bus introduz um tipo novo de componente para o modelo SCA sendo este o componente de mediação de fluxo. A partir da perspectiva SCA, um componente de mediação de fluxo não é diferente de qualquer componente de outros serviços.

O Business Objects é a descrição universal de dados. Eles são utilizados como objetos de informação e são passados entre serviços, são baseados no Service Data Object (SDO[31]) padrão. No WebSphere Enterprise Service Bus um tipo especial de SDO é introduzido, o Service Message Object (SMO[32]).

Também parte da infraestrutura é o Common Event Infrastructure (CEI[33]) este é a base para aplicações de monitorização. A IBM usa esta infraestrutura ao longo da sua carteira de produtos, assim como o mais conhecido o Tivoli, bem como WebSphere Business Monitor.

A definição de eventos (Common Business Event) é padronizado através da OASIS[34], para que outras empresas, bem como os clientes possam utilizar a mesma infra-estrutura para monitorizar o seu ambiente. [Keen, Mais, Carvalho, Hamann, Imani, Lotter, Norton, Ringler, Telerman, 2006]

---

[30] MQ – Message Queuing

[31] SDO – Service Data Object

[32] SMO – Service Message Object

[33] CEI – Common Event Infrastructure

[34] OASIS – Advancing open standards for the information society

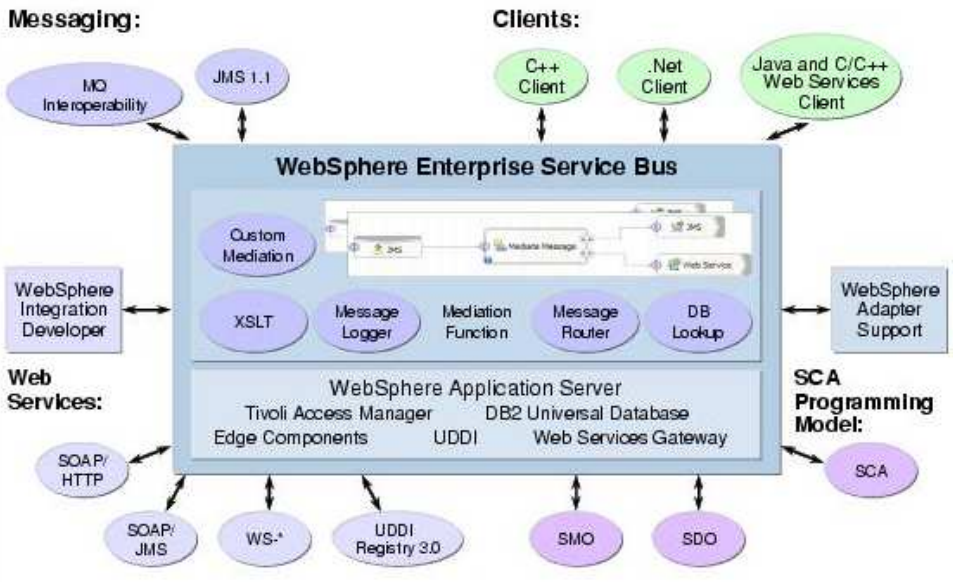

Figura 17 – Arquitetura e componentes do WebSphere. [IBM, 2011].

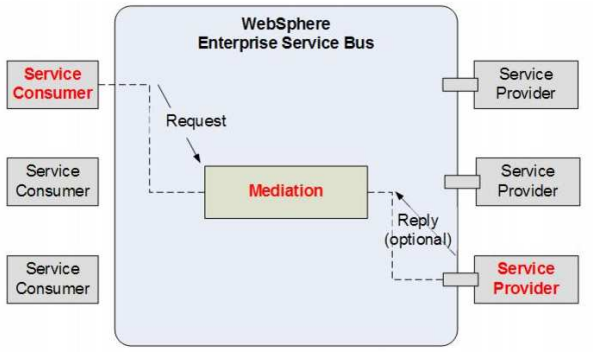

Figura 18 – Detalhes de um pedido [IBM, 2011]

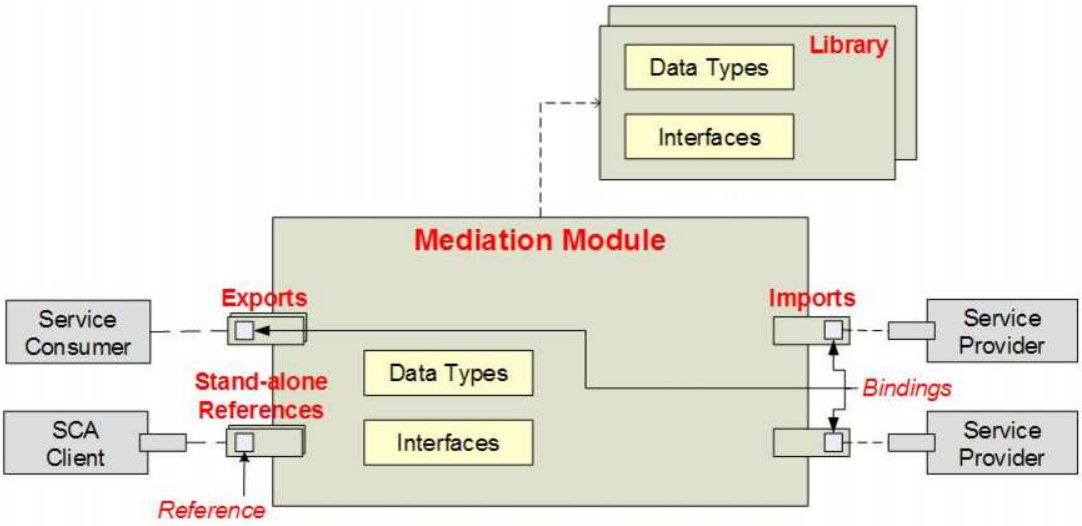

Figura 19 – Módulos de Mediação [IBM, 2011]

CAPÍTULO 3

Healthcare Service Bus

Num ambiente ideal, os diversos serviços que os pacientes necessitam deveriam interligarem-se e interoperar de uma forma que melhorasse a eficácia e qualidade dos serviços de cuidados de saúde. O serviço de informação de um hospital tem de suportar uma variedade de serviços críticos relacionados com saúde, bastando pensar nas necessidades de um paciente na urgência que requer cuidados que lhe podem salvar a vida. A título de exemplo, também se pode considerar que qualquer hospital tem um software de EMR[35] que tem de ser usado e integrado nas práticas clínicas, garantindo que diferentes sistemas que suportam essas práticas possam comunicar entre si. Ou seja, é necessário garantir que existe interoperabilidade, é precisamente aqui que o HSB é utilizado, sendo uma plataforma integradora específica de serviços na área da saúde tendo por base um ESB.

O HSB é baseado na tecnologia de um ESB, mas especializado para o domínio da saúde., estes serviços potenciam comunicações mais ricas, complexas e de alto valor que estão ou não dispersas entre si de um forma geográfica, e vai garantir a sua interoperabilidade.

O HSB vai fornecer um pacote rico numa plataforma de conjunto base de serviços para garantir um rápido desenvolvimento. Ira certamente garantir que aplicações possam consumir mais facilmente serviços de outros fornecedores de software. Um bom exemplo é o facto de ao utilizar-se um HSB, os processos clínicos e de faturação possam ser integrados utilizando fluxos sofisticados. [Gillson, 2010]

[35] EMR – Electronic medical record

Neste capítulo vão-se detalhar alguns aspectos críticos do HSB, que o distinguem das implementações mais usuais de um ESB, dando particular relevo à segurança.

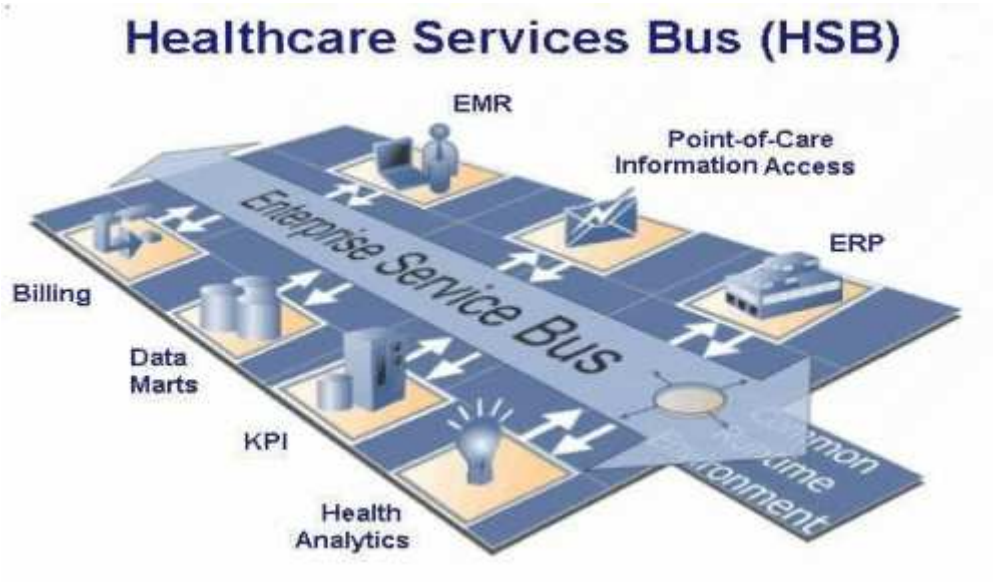

Figura 20 – Representação de um HSB [Gilson, 2011]

3.1 Segurança

A informação médica é utilizada para descrever cenários e acontecimentos passados com relevância futura, a importância desta informação é tal que desde muito cedo foi necessário criar mecanismos para gestão e tratamento e difusão desta. Os arquivos em papel, nomeadamente o processo clínico, é um elemento chave na prática médica, tendo até especial tratamento em muitos diplomas legais e no Código Deontológico da Ordem dos Médicos (capítulo XIV, artigos 100º a 103º).

As tecnologias de informação vieram disseminar a forma como a informação é distribuída e tratada assim como facilitar o acesso a mesma. A necessidade de um acesso rápido e constante à informação levanta questões: qual a fiabilidade da informação, esta é fidedigna? Ou seja a necessidade de tratar a vulnerabilidade. Aqui é criado um espaço para a necessidade de fazer passar informação com a garantia que não foi adulterada na fonte, percurso e no destinatário.

Quando existe a necessidade de partilhar informação por um determinado grupo de indivíduos, a partilha é feita normalmente utilizando um acesso constituído por login e password que validam uma conta de utilizador em determinado sistema. Este processo é

apelidado de autenticação e apresenta algumas falhas de segurança, que podem ser exploradas recorrendo a técnicas de Phishing, Sniffing e visualização direta da informação teclada.[Paul Ducklin, 2006]

O phishing, consiste num processo de obtenção de dados recorrendo a utilização de entidades credíveis para o utilizador. O sniffing é um processo de descodificação de pacotes de rede recorrendo a aplicações capazes de monitorizar o trafego, visualizando assim dados não encriptados, normalmente este procedimento é utilizado em redes não seguras. A visualização direta da informação acontece quando algum ou algum dispositivo de vídeo capta o momento no qual estamos a inserir os dados num determinado interface de input neste caso o teclado.

É por isto necessário a implementação de mecanismos de segurança que garantam a integridade, autenticidade, confidencialidade da informação minimizando assim as vulnerabilidades existentes.

3.1.1 Criptografia

A criptografia tem como origem a criptologia e é um ramo da matemática. Este termo resulta da junção de duas palavras gregas, “kyptós” e “gráphein”, isto significa escondido e escrita. Desta forma esta ciência tem como objetivo tornar informação que é legível e que faz nexo em outra informação aleatória, recorrendo a técnicas e conceitos que permitam ao emissor ou seja, quem cifra, ter acesso à informação. [Wikipedia, 2011]

3.1.1.1 Cifras

As cifras utilizam chaves para gerarem “ciphertext” únicos, a transformação de dados cifrados em texto corrente é possível com a mesma chave (cifra simétrica) ou com a sua chave correspondente (cifra assimétrica). [Fernando, Rodrigo, 2011]

As chaves podem ser simétricas ou assimétricas, variando em função da necessidade da encriptação dos dados.

Para além das chaves também são utilizados algoritmos matemáticos para cifrar e decifrar dados.

As cifras são utilizadas para manter a informação secreta, transformando informação legível (plaintext) em informação ilegível (ciphertext) e vice-versa.

Para criptografar uma pequena quantidade de dados é utilizada a criptografia simétrica. Uma chave simétrica é usada no em ambos os processos de encriptação e desencriptação sobre criptografia. Para decifrar um pedaço de texto cifrado é necessário utilizar a mesma chave que foi usada para criptografar esse mesmo texto.

O objetivo de cada algoritmo de encriptação é tornar difícil desencriptar a mensagem cifrada que foi gerada sem usar a chave de encriptação. Se um algoritmo de criptografia utilizado for realmente bom, não há nenhuma técnica significativamente melhor do que tentar metodicamente cada chave possível. Para tal algoritmo, quanto maior a chave, maior a dificuldade para decifrar um pedaço de texto cifrado sem possuir a chave de encriptação.

É difícil determinar a qualidade do algoritmo de encriptação. Pois algoritmos promissores, por vezes, acabam por ser muito fáceis de quebrar, dado o ataque adequado par tal ação. Ao selecionar um algoritmo de criptografia, é boa ideia escolher um que esteja em uso há vários anos e com sucesso a resistir a ataques. [MSDN, 2012]

3.1.1.2 Algoritmos de Criptografia e Protocolos

Muitas vezes, algoritmos criptográficos e protocolos são necessários para manter um sistema seguro, especialmente quando se comunicam dados através de redes não confiáveis tal como a Internet. Sempre que possível, usar a tecnologia de criptografia para autenticar informações e manter a informação privada (não se deve assumir que a criptografia simples automaticamente autentica também). Normalmente é necessário usar um conjunto de ferramentas disponíveis para proteger os dados.

Algoritmos criptográficos e protocolos são difíceis de combinar, por isso não se deve cair na tentação de criar algoritmos próprios. Em vez disso, devem ser utilizados protocolos e algoritmos que são amplamente utilizados, fortemente analisados, e aceites como seguros.

Vários algoritmos são patenteados, mesmo que os proprietários permitam a utilização em “free use” no momento. Sem um contrato assinado estes podem sempre mudar de ideia, pondo-o em risco os utilizadores mais tarde. Em geral, deve ser evitado o uso de algoritmos patenteados a não ser que exista um contracto, evitando assim problemas

futuros [Wealer, 2003]. Um outro possível problema é que muitos países regulam ou restringem a criptografia de alguma forma.

Ao utilizar um protocolo de segurança, deve ser utilizado conforme o padrão. Como tal existem o IPSec, SSL, TLS, SSH, S/MIME, OpenPGP/GnuPG/PGP, e Kerberos. Cada um tem vantagens e desvantagens, muitos deles pouco se sobrepõem em funções, mas tendem a ser utilizados em diferentes áreas.

Na utilização de chaves simétricas, está implícito o uso pelos utilizadores deste tipo de cifra de uma chave secreta que é partilhada, sendo esta utilizada para cifrar e decifrar o conteúdo trocado.

Por si, só o facto de existir uma chave que é partilhada por todos os intervenientes, é problemático pois levanta questões de segurança, criando assim uma possível falha em qualquer dos pontos de ligação. Se um atacante tiver acesso à chave consegue cifrar e decifrar a informação trocada.

Apesar das desvantagens, este sistema é ainda hoje muito utilizado para tratar da encriptação de dados, pois apresenta como vantagens um bom desempenho e rapidez. Os que mais se destacaram na cifra simétrica foram o DES[36] e AES[37].

O algoritmo DES foi desenvolvido pela IBM nos anos 70, este algoritmo cifra informação em blocos de 64bits, utilizando para isso uma chave de 56bits. A utilização deste algoritmo nos dias de hoje é desaconselhada pois é considerado inseguro.

O algoritmo AES foi a alternativa a utilizar como o novo padrão de encriptação de dados, é também conhecido como “rijndael”, utiliza uma cifra simétrica utilizando blocos de cifra com tamanho variável entre 128, 192 ou 256bits. É considerado um algoritmo seguro e é utilizado nos EUA como sendo o algoritmo padrão para codificação de dados. [RSA, 2011]

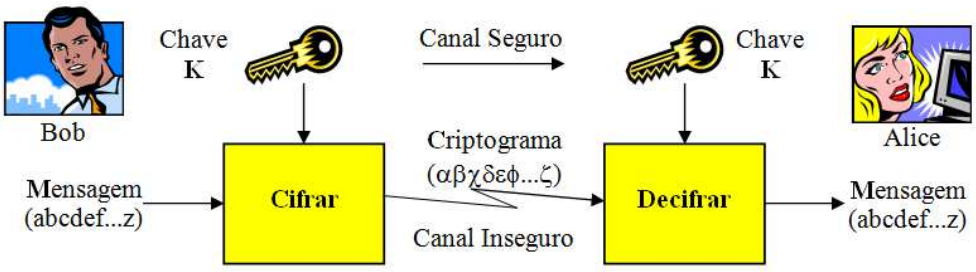

Figura 21 – Criptografia Simétrica [Fernando, Rodrigo, 2011]

[36] DES – Data Encryption Standard

[37] AES – Advanced Encryption Standard

O sistema de cifras assimétricas, este sistema é caracterizado por uma chave privada e uma chave pública, a chave pública é de acesso a todos os intervenientes e a chave privada diz respeito normalmente ao emissor e cada emissor tem a sua própria chave privada e única. Este sistema é diferenciado em relação ao sistema simétrico, pois com este sistema podemos garantir a confidencialidade e autenticidade ao combinar a chave pública de um recetor com a privada do emissor para troca de mensagens. Também, por analogia com o sistema simétrico, este último procedimento é mais lento pois para o processo de encriptação e desencriptação é necessário sempre utilizar as duas chaves.

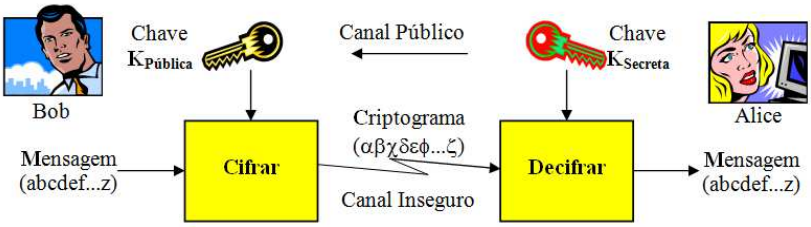

Figura 22 – Criptografia Assimétrica. [Fernando, Rodrigo, 2011]

O sistema de cifras hibridas, consiste na combinação de uma cifra assimétrica e simétrica, a combinação destes dois tipos de cifras permite implementar um sistema hibrido. O sistema de cifra assimétrica é utilizado para cifrar a informação enquanto o sistema assimétrico tira partido de uma chave privada, existe nos dias de hoje um protocolo que implementa este sistema, o TLS[38].

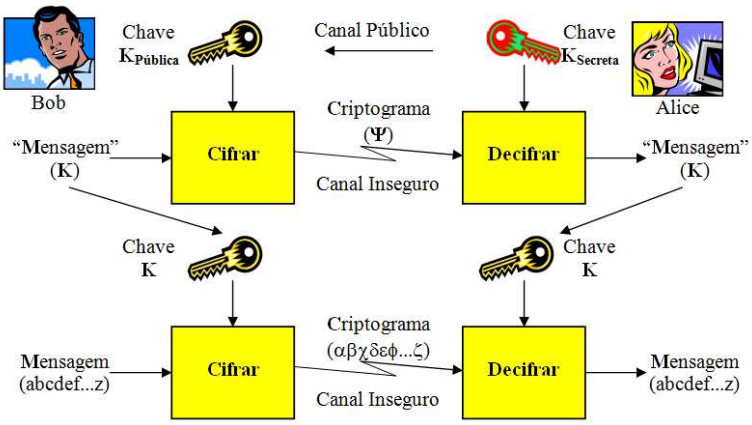

Figura 23 – Criptografia Hibrida [Fernando, Rodrigo, 2011]

[38] TLS – Transport Layer Security

As funções de hash permitem ao utilizador construir a partir da mensagem a transmitir de tamanho variável, um output de tamanho fixo, conhecido como hash ou digest. A partir do output gerado não é possível determinar o input inicial. Estas funções são designadas de one-way function.

As mensagens digest são muito uteis para assegurar que os dados não são alterados quando em trânsito de um ponto para o outro. Uma implementação prática das funções de hash é o protocolo de segurança TLS, v1.2 que utiliza para implementação de canais seguros os algoritmos de hash: MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512. [RFC, 2008]

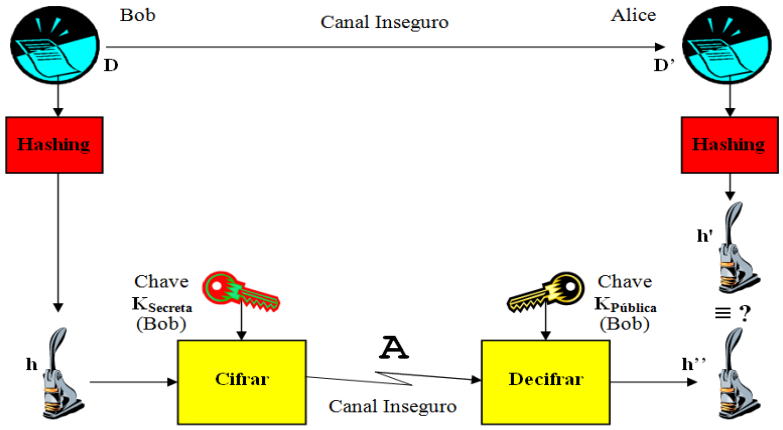

Figura 24 – Função de hashing com cifra assimétrica [Fernando, Rodrigo, 2011]

3.1.2 Chaves Criptográficas

Este tipo de chaves, são o segredo das mensagens cifradas, pois apresentam um conjunto de variáveis que são utilizados como parâmetros nos algoritmos criptográficos controlando a transformação em texto cifrado e texto não cifrado. [Anderson, 2008]

3.2 Segurança HSB.

É fundamental a segurança no ESB ou mais especificamente no HSB. Devem ser atribuídos níveis de acesso por utilizador, grupo e unidades funcionais, sendo que estes acessos devem permitir isolar indivíduos na sua área de atuação, não permitindo acesso a recursos que estes não devam ter acesso. O controlo de utilizador deve ser tido em conta ao ser validado o mesmo nas respectivas horas de trabalho assim como onde esta a ser validado (ex.: acesso na urgência ser utilizado na manutenção).

Aos acessos de utilizadores e equipamentos devem ser criadas políticas de acesso restritivas em ordem de validar os mesmos na sua área de atuação, permitindo assim restringir o nível de acesso ao HSB, assim como identificar equipamentos que não estão no seu departamento.

Estes acessos devem respeitar as regras de negócio e explicitamente garantir que a informação disponível está de acordo com o acesso do utilizador, ou seja, pode ter acesso ao todo ou a partes da informação disponível, havendo assim acessos diferenciados.

Os acessos devem ser condicionados por forma a ser possível criar “ilhas” isoladas de informação.

Os canais de acesso ao HSB devem ser todos controlados de forma a garantir que não existe algum acesso sem restrições de firewall ou tunneling VPN de dados.

É também igualmente importante garantir que a informação está guardada de forma persistente em BD relacionais com dados devidamente encriptados de forma a garantir uma consistência de informação.

Existem muitas transformações de informação no bus, como tal a segurança da informação é fulcral. Não se pode esquecer que o HSB entra em todas as transformação de dados dos sistemas de informação de uma forma transversal, logo o HSB tem acesso transversal as mensagens como tal ter em atenção a questão da segurança.

3.2.1 Segurança Web Services.

Os WEB services foram projetados para reduzir os custos de integração e de facilitar novas formas de fazer negócios. Muitas organizações ainda estão relutantes em abrir os seus negócios à internet, embora padrões como SOAP e WSDL estejam em vigor há quase uma década.

Um dos principais fatores para que tal não aconteça deve-se à compreensão inadequada dos riscos de segurança envolvidos e da falsa crença de que as empresas vão ter de fazer reinvestimentos caros nas suas infraestruturas de segurança.

Na tentativa de tornar os Web services um terreno seguro, OASIS tem um número normalizado de extensões para mensagens SOAP que abordam questões de segurança relacionadas a diferentes Web services. Estas extensões são WS-Security, WS-Trust, WS-Federation, WS-SecureConversation e WS-Policy (este último foi apresentado para a normalização do W3C).

Para além das extensões SOAP, as especificações de segurança de outros pode ser utilizado em combinação com Web services- XACML, SAML, ou as assinaturas digitais Serviços são alguns exemplos.

Estas especificações definem técnicas de segurança e mecanismos que devem ser aplicados a mensagens individuais SOAP (codificações, trocas de mensagens, etc), mas estas especificações não definem “guidelies” para possíveis implementações.

Para tal deve ser proposto a utilização de uma arquitetura de sistemas de segurança para os Web services: o Serviço Orientada Segurança Arquitetura, SOSA. Esta arquitetura é baseada na arquitetura Enterprise Services Bus (ESB).

A ideia por trás disso é a construção modular de segurança serviços que atendam as funções de segurança bem definidos (ou seja, autenticação, autorização, etc.), técnicas de roteamento de mensagens pode ser utilizado para combinar esses serviços de segurança e para desenvolver soluções de segurança mais complexas.

Requisitos de segurança para Web services:

- Autenticação: O requerente pode ser solicitado a fornecer credenciais antes de aceder a um determinado Web service. A autenticação é uma questão-chave, pois sem conhecer a identidade do requerente, outras funções de segurança não podem ser realizadas. A autenticação é validada por várias especificações, o mais importante é o WS-Security e SAML.

- Autorização: Autorização ao acesso a Web services devem ser restringidos com base em políticas de autorização, ou seja, devem ser declaradas condições claras

sob o qual uma entidade é permitida aceder aos Web services corretos. A autorização é abordada em XACML.

- Confidencialidade: O fluxo de informações entre os serviços deve ser protegido. Devemos ter em conta o facto que as mensagens SOAP muitas vezes passam por vários servidores antes de chegar a seu destino. A confidencialidade é abordada em XML-Encryption e WS-Security.

- Integridade: A informação recebida por um Web service deve ser a mesma que foi enviada pelo requerente. As mensagens não devem ser alteradas ao longo do caminho. Integridade é abordada em XML-Signature e WS-Security.

- Não repúdio: O prestador de serviços deve ser capaz de provar que o requerente usou um determinado Web servisse e o requerente deve ser capaz de provar que a informação que ele tem, tem como origem a partir de um fornecedor de determinado serviço. Não-repúdio é abordada em XML-Digital Signature.

- Privacidade: Ambos requerente do serviço e o prestador de serviços deve ser capaz de definir políticas de privacidade. Ambos devem concordar com estas políticas antes da efetiva entrega do serviço. A privacidade é abordada em WS-Policy e WS-SecurityPolicy.

- Auditoria: O acesso do utilizador e o seu comportamento deve ser marcado, de modo a assegurar que as obrigações estabelecidas sejam respeitadas. A auditoria é aplicada por auditores, que pode ser tanto ativa e passiva.

- Confiança: O requerente e prestadores de serviço devem ser capazes de determinar se confiam em um no outro. A confiança é abordada em WS-Trust.

3.2.2 Segurança física do broker HSB.

A segurança física tem requisitos que dependem do rigor da proteção necessária. É claro que a necessidade não deve exceder o recurso financeiro para proteger o bem.

As bases de dados, assim como toda a informação relativa ao broker para troca de mensagens deve estar confinando num espaço denominado por centro de dados (“datacenter”).

O objetivo da segurança física do centro de dados é basicamente o mesmo em todo mundo, impedir quaisquer restrições regulamentares locais, ou seja manter as pessoas que não queremos no neste local, e se eles conseguirem entrar, identificá-los assim que possível (Idealmente mantê-los contidos numa seção do edifício). O velho ditado de especialistas em segurança de rede diz "a segurança é como uma cebola" (que nos faz chorar!) porque precisa-mos de ter construído em camadas a partir da área que estamos a tentar proteger.

Existem recursos em abundância para nos guiar através do processo de conceção de um centro de dados altamente seguro que vai focar na construção de um "padrão gold" capaz de armazenar a mais sensível informação. Para a maioria das empresas esta abordagem será um exagero e acabar por custar milhares de euros a implementar.

Ao olhar para a segurança física para um centro de dados novos ou existentes, primeiro precisamos de realizar uma avaliação de risco básica dos dados e equipamentos das instalações para realizar uma escala “impact-versus-likelihood”, i.e. the impact of a breach of the data center versus the likelihood of that breach actually happening (ou seja, o impacto de uma brecha do centro de dados versus a probabilidade de brecha que realmente possa acontecer).

Esta avaliação deve servir como base de até onde devemos ir com as questões da segurança física. É impossível combater todas as potenciais falhas com as quais nos podemos debater, e é aqui que a identificação de uma falha, seguida de contenção, deve ser tomada em conta. Da mesma forma, precisamos de perguntar a nos mesmos se a área a proteger necessita, por exemplo, impedir explosivos.[Barker, 2012]

Existem alguns princípios básicos que qualquer edifício datacenter deve seguir:

- Aparência discreta: Especialmente numa área povoada, não deve atrair publicidade. Evitar qualquer sinalização que com referências "data center" e tentar manter o exterior do edifício como inclassificável e igual as outras instalações na zona.

- Evitar janelas: Não deve haver janelas com acesso direto do exterior e quaisquer vidros necessários devem ser utilizados vidro laminado ou duplo.

- Limitar os pontos de entrada: O acesso ao edifício precisa ser controlado. Ter um único ponto de entrada para os visitantes e técnicos, juntamente com um cais de carga para entregas, permite canalizar todos os visitantes através de um local onde podem ser identificados. É claro que toda a atividade deve ser monitorizada por CCTV.

- Tele-vigilância: as câmaras de CCTV cumprem um dos principais princípios de segurança, que é a identificação. No mínimo devemos ter câmaras completas “pan”, “tilt” e “zoom” no perímetro do prédio.

- Portas corta-fogo: portas corta-fogo são um requisito para a saúde e segurança, mas devemos verificar que abrem para fora e ter alarmes ativos em todas.

- Equipa de segurança permanente: Muitas instalações têm pessoal contratado de empresas de segurança. Isto é o ideal, pois este é o negócio destas empresas.

3.2.3 Recursos Necessários de um HSB

De uma forma sintética, podem-se indicar alguns requisitos chave um HSB, que deve:

- Manter um registo de todos os prestadores de serviços que estão ligados a si para que possa encaminhar um determinado pedido para o respectivo fornecedor de serviços.
- Fornecer um mecanismo standard que permita a interconectividade entre os prestadores de serviços permitindo a estes conversar entre si através do “service bus”.
- Permitir que outros HSBs se possam ligar a este.
- Dependendo do grau de exigência de SLA[39], utilizar redundância em caso de falha.

[39] SLA – Service level agreement

3.3 Cenário de aplicabilidade de um HSB.

Quando o paciente chega a um hospital (centro médico), o médico que o atende utiliza uma aplicação que usa o "service bus" para aceder ao histórico do paciente. O médico também cria as observações iniciais sobre a condição do paciente numa aplicação de prescrição médica que está ligada ao "service bus". As observações que o médico teceu sobre o paciente são então validadas por um serviço que está ligado as diversas companhias de seguros que o centro hospitalar tem protocolo, desta forma as observações do médico percorrem o "service bus" até o serviço corresponde ao portal das companhias de seguros.

Sendo assim, fica logo disponível o tipo de seguro que o paciente tem ou não.

O médico prescreve então uma transfusão de sangue para o paciente na mesma aplicação de prescrição. A prescrição é então enviada automaticamente através do "service bus" para o banco de sangue local. Caso não seja possível acesso as quantidades de sangue necessárias, o sistema encarrega-se também de enviar para uma aplicação de doadores de grupo, que por sua vez envia Mensagens "SMS[40]" para os doadores cujo tipo de sangue é igual ao do paciente.

A exigência de sangue, assim como a necessidade de sua reposição na aplicação de doadores, também viaja ao longo do "service bus". O médico também prescreve uma receita para medicamentos de emergência e um teste de radiologia, que são alimentados na aplicação de receita. A aplicação de prescrição envia essas prescrições sobre o "service bus" para o farmacêutico que está nas instalações da farmácia e também é enviada a prescrição através do "service bus" para o departamento de radiologia com as respectivas indicações.

Os medicamentos prescritos foram validados previamente também através do "service bus", pois a aplicação de prescrição também comunica com o módulo farmácia que permite confirmar stocks de medicamentos.

Caso o medicamento não exista em stock sugere um outro com as mesmas características terapêuticas que existe em stock. Sempre que um determinado fármaco atinge o seu valor de margem de segurança o mesmo é reposto pela aplicação de gestão de stocks, tal ocorre através do "service bus" ao bus também estão ligados diversos fornecedores entre eles os fornecedores de fármacos, sendo assim a aplicação de gestão encarrega-se de colocar a encomenda ao fornecedor sem que exista outro tipo de intervenção.

[40] SMS – small message service

Tudo isto funciona em cima do “service bus”.

Neste caso de uso, podemos verificar que o HSB permite que diversas aplicações se interliguem e interoperem, permitindo assim a agregação de serviços. Existem assim dois tipos de aplicações principais, as consumidoras e as prestadoras de serviços, que se ligam ao HSB. A aplicação de prescrição que enviou a necessidade de transfusão de sangue para o HSB agiu como um consumidor do serviço (uma aplicação que consome ou solicita o serviço).

A aplicação de doadores de sangue que enviou mensagens SMS a potenciais doadores atuou como prestador de serviço (uma aplicação que fornece o serviço solicitado).

A interligação e a interoperabilidade são requisitos diferentes que juntos proporcionam a agregação de serviços. Interligação, significa que os prestadores de serviço e consumidores de serviços têm uma forma comum de ligarem-se um ao outro, de modo a que possam trocar informações e mensagens.

O HSB usa normalmente o popular formato XML para troca de mensagens, sendo este verdadeiramente interoperável. [IBM, Apache ServiceMix 2010]

CAPÍTULO 4

Recolha de dados na unidade hospitalar

Neste capítulo são demonstrados os resultados que foram obtidos através da recolha de dados colecionados na unidade hospitalar e a forma como foram recolhidos. Também aborda o contexto atual da unidade hospitalar no que diz respeito aos sistemas de informação que fazem parte do seu sistema de informação. Os requisitos de confidencialidade impedem que sejam apresentados dados detalhados sobre a arquitetura do sistema de informação da unidade hospitalar.

Como foi já descrito nos capítulos anteriores a escolha como ferramenta agregadora será um ESB como está implícito nesses mesmos capítulos. A tecnologia foi descrita com algum pormenor, sendo que para esta área específica é sempre recomendável que seja utilizada uma tecnologia madura e estável.

Entre todos os ESB's analisados o da IBM é aquele que já amadureceu o suficiente nesta área e que tem uma serie de ferramentas que evoluíram com a própria necessidade do mercado. É claro que também é necessário garantir uma continuidade de suporte por parte das marcas desenvolvedoras para futuros cenários possíveis.

4.1 Sistema de informação da unidade hospital

A unidade hospitalar, para iniciar a sua atividade recorreu ao mercado para adquirir aplicações informáticas que permitissem o correto funcionamento da mesma. Contratou uma empresa de software que lhe vendeu todos os módulos aplicacionais numa solução integrada chave na mão. Nessa altura não existia a necessidade de interligação com equipamentos e provedores de serviço externo ou outros. A empresa de software cresceu e criou várias subsidiárias que ficaram cada uma com uma parte do negócio, ou seja a unidade hospitalar deixou de ter um fornecedor de serviços e passou a ter vários que dependem uns dos outros para funcionar.

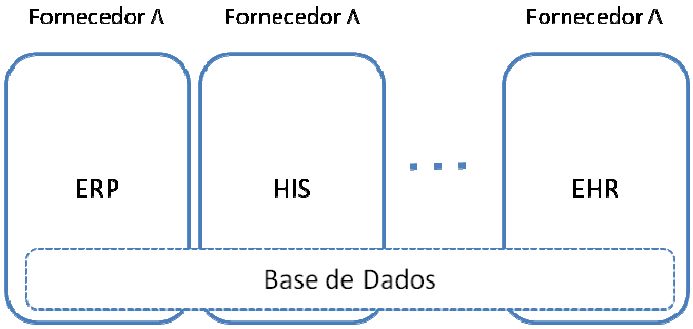

Figura 25 – Solução adquirida pela unidade hospitalar

A solução adquirida tem uma estrutura monolítica, pois a única forma dos diversos módulos trocarem informação é diretamente sobre a base de dados, que é transversal a todo o sistema. Isto levanta graves problemas de evolução dos diferentes módulos, que agora têm distintos fornecedores.

É claro que o problema só pode ser agravado pois sempre que é necessário a aquisição de um novo modulo aplicacional ou a evolução do existente obriga ao desenvolvimento de “remendos” na base de dados existente e/ou ao desenvolvimento de módulos de sincronização da informação entre as diferentes bases de dados.

A unidade hospitalar vesse assim com o problema de não dispor de interfaces normalizados e assim perder a capacidade de poder optar por outras soluções de software que possam ser interligadas com o que esta dispõe.

Neste momento o problema é como manter uma solução “legacy” com vários fornecedores de software pois inicialmente era só um.

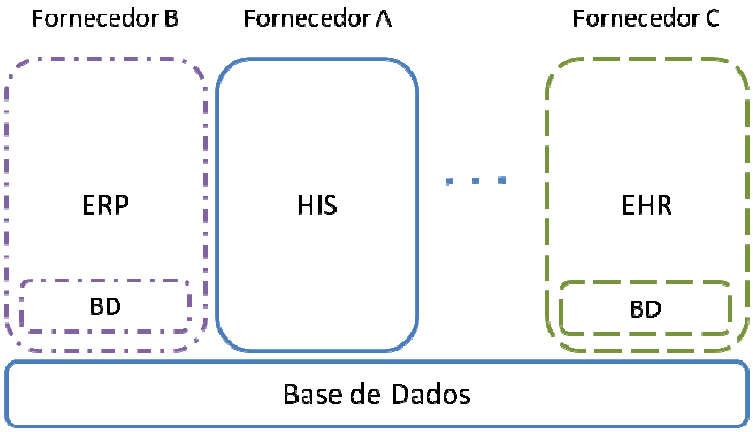

Figura 26 – Solução atual da unidade hospitalar

4.2 Descrição do problema a analisar para a unidade hospital

O problema a tratar na unidade hospital é a criação de um ESB ou outra forma de disponibilização de um conjunto de interfaces capazes de suprimir o problema que surge com a necessidade de implementação de software e hardware.

Para tal devem ser utilizados protocolos de comunicação “standard” cujas suas necessidades deveriam ser alvo de análise de forma a validar qual a melhor maneira de interligação entre as mesmas.

Tal acontece numa altura em que a entidade necessita de uma interoperabilidade entre sistemas, mas como é solicitado a entidade pretende que tal aconteça de uma forma transparente e heterogénea entre sistemas de informação para que não seja posto em causa a continuidade do serviço de sistema de informação.

Foi solicitado que fosse feita uma análise preliminar aos diversos sistemas de informação que perfazem da instituição para que tal tivesse impacto no desenrolar da mesma, sendo assim o “background” para o ponto de partida da auditoria.

O objetivo não é reformular os sistemas de informação que estão a funcionar corretamente mas sim prestar a consultadoria necessária para que possa ser criada a interoperabilidade desejada sem impacto de maior nos sistemas atuais.

A solução a adotar deverá ter em conta as formas de implementação uma vez tratar-se de um ambiente hospitalar onde os sistemas de informação são fulcrais/fundamentais para o funcionamento da unidade hospital. Desta forma, é imperativo que a solução a adotar possa ser construída tendo por base um sistema de implementação paralelo ao que esta a funcionar.

É também um fator fundamentar que a solução a implementar tenha a possibilidade de crescimento com a plataforma da unidade hospitalar de forma transparente e ilimitada com recurso a normas “standard” da indústria, não ficando de certa forma dependentes de terceiros para poder avançar com novas implementações quer a nível de software quer a nível de hardware.

Para a unidade hospital a sua principal preocupação era a de analisar o atual modelo de troca de informação que tem implementado e, partindo deste pressuposto, proporcionar uma solução para a interligação desse modelo existente com um modelo mais abrangente no que toca a interoperabilidade com entidades externas e equipamentos ativos, assim como scanners médicos (imagiologia), equipamento de laboratório (patologia, analises) e os demais necessários.

Esta análise servirá de ponto de partida para uma possível fundamentação no que diz respeito a uma alteração no rumo de evolução dos sistemas de informação da entidade hospitalar.

A entidade pretende que a/as possíveis formas de resolução para o problema exposto culminem a lacuna existente no cenário atual e que acima de tudo seja fundamentada com normas de comunicações assim como normas modulares de implementação nos cenários possíveis.

Para tal foi utilizada uma metodologia de abordagem direta com base nos conhecimentos dos responsáveis pelas áreas de sistemas de informação assim como responsáveis administrativos da organização.

Não foi feita de forma exaustiva uma análise a troca de mensagens pois toda a plataforma da unidade hospitalar não dispõe de interfaces que permitam tal análise.

É necessário que para o novo modelo de funcionamento hospitalar fossem introduzidas normas da indústria hospitalar que garantam a interoperabilidade entre parceiros, fornecedores, equipamentos e possíveis extensões da unidade hospitalar em causa.

4.3 Dados para a recolha de informação na unidade hospitalar

Os dados a recolher na unidade hospitalar retratam o estado atual do SI da unidade hospitalar e é objetivo para esta recolha abordar os seguintes itens:

- Identificar os centros de responsabilidade (ex. ambulatório, internamento, imagiologia, etc.)

- Identificar as unidades funcionais que implementam os centos de responsabilidade e diferenciar as internas das em outsourcing (ex. analises clínicas, patologia, imagiologia, etc.)

- Identificar os sistemas (equipamentos) existentes.
    - Identificar as trocas de informação
        - Formatos (SOA, etc.)
        - Eventuais normas nacionais, internacionais ou sectoriais aplicáveis
        - Regras de negócios existentes
        - Volume de mensagens
        - Frequência de alterações nos formatos
        - Requisitos de segurança, restrições de acesso e confidencialidade
    - Identificar as características técnicas (cada um)
        - Tipo de Plataforma tecnológica, idade, tempo reminiscente de serviço
        - Fornecedor (interno/externo), manutenção e facilidade de alteração/configuração
        - Identificar os mecanismos de autenticação e segurança

4.4 Método utilizado para recolha de dados.

Foi utilizada uma metodologia de observação direta com base nos conhecimentos dos responsáveis pelas áreas de sistemas de informação assim como responsáveis administrativos da organização. Uma ferramenta fundamental foi o recurso ao Plano Diretor do hospital.

Não foi feita de forma exaustiva uma análise da troca de mensagens entre os diferentes sistemas, pois a plataforma da unidade hospitalar não dispõe de interfaces públicos (serviços expostos) que permitam tal análise.

4.5 Contexto atual da unidade hospitalar

A unidade hospitalar serve um grande número de pacientes que necessitam de intervenção cirúrgica, o meio envolvente é uma zona densamente povoada sendo que os pacientes são oriundos de um raio de cerca de 50 km, dispondo o hospital condições excelentes de acolhimento e internamento caso seja estritamente necessário.

A unidade hospitalar foi crescendo como maior parte das empresas que utilizam os sistemas de informação de uma forma comedida, ou seja sempre que foi sendo necessário cresciam nesse mesmo sentido (adquiriam o respectivo software). Os sistemas de informação foram sendo adquiridos consoante as necessidades.

Como tal para cada vantagem existe uma desvantagem, logo estas aquisições eram mais simples de adjudicar pelo seu valor e tempo de implementação pois trata-se de adquirir módulos e acopla-los aos já existentes isto neste caso foi sempre privilegiado o mesmo fornecedor de serviços (software) para os sistemas de informação fornecedor este tem vindo a ser utilizado desde o início e que forneceu os respectivos sistemas.

É claro que a decisão de adquirir o próximo módulo para os sistemas de informação fica muito limitado uma vez que a unidade hospitalar torna-se cada vez mais dependente do provedor de software pelas seguintes razões:

- Protocolos de comunicação não standard
- Retro compatibilidade e compatibilidade com módulos existentes

- Protocolos de comunicação proprietários
- Plataforma fechada sem exposição exterior
- Plataforma uniforme do ponto de vista do provedor de serviços
- Facilidade de interação entre módulos do sistema de informação

4.6 Levantamento de dados relacionados com a unidade hospitalar

Esta unidade hospitalar dispõe de uma serie de áreas funcionais (ex. ambulatório, internamento, imagiologia, etc.), que implementa em cada área vários módulos funcionais.

Para exemplo ilustrativo vou utilizar o Hospital Information System (HIS), não em grande detalhe para não expor o SI da unidade hospitalar.

Cada área funcional pode ter como relação de interligação uma relação de n x m sendo n a área funcional e m a módulo funcional implementado, ou seja no caso estudado existe sempre uma área funcional que implementa vários módulos funcionais.

O HIS cobre uma ampla serie de unidades funcionais como:

- Admissão de doentes
- Bloco operatório
- Faturação
- Enfermagem
- Consulta externa
- Gestão de Agenda
- Ehr portal do doente
- Bloco operatório
- Gestão lista espera
- Internamento
- Gestão visitas
- Arquivo clinico
- Programa cirúrgico
- Gestão atendimento

O HIS é utilizado nas seguintes áreas funcionais:

- Anestesia
- Cardiologia
- Cirurgia geral
- Queimados
- Oftalmologia
- Bloco operatório
- Consulta externa
- Imagiologia

Por questões de confidencialidade, não é conveniente explicar detalhadamente e demonstrar da mesma forma as suas ligações por forma a proteger a entidade estudada.

A unidade hospitalar tem como base do seu SI[41]/TIC[42] as seguintes plataformas modulares.

- SCM (Supply Chain Management)
- ERP (Enterprise Resource Planning)
- HIS (Hospital Information System)
- EIS (Executive Information System)
- EPR (Eletronic Patient Record)
- LIS/RIS (Laboratory Information System / Radiology Information System)
- EHR (Eletronic Health Record)

As plataformas modulares podem ser observadas na figura 28.

Quanto ao objetivo de identificar os centros de responsabilidade e as respectivas unidades funcionais que implementam esses mesmos centros, tal não foi possível efetuar este cruzamento de informação pois para os responsáveis as próprias unidades funcionais são centros de responsabilidade.

[41] SI – Sistema Informação

[42] TIC – Tecnologias de Informação e Comunicação

No decorrer do levantamento foram identificadas 3 áreas principais, sendo que duas delas pertencem aos “Cuidados” e uma outra pertence à “Gestão”. Podemos ver na figura 27 as principais áreas da unidade hospitalar.

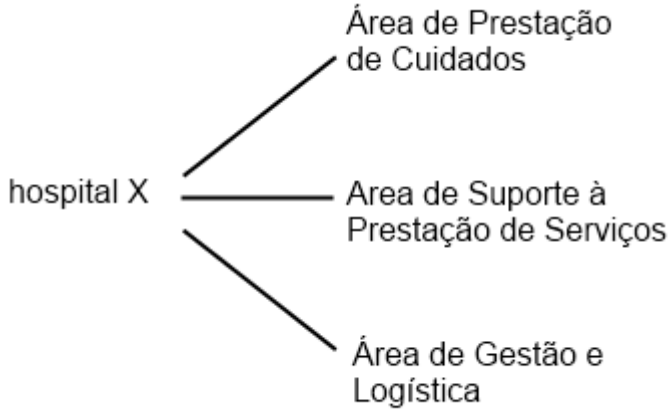

Figura 27 - Áreas da unidade hospitalar

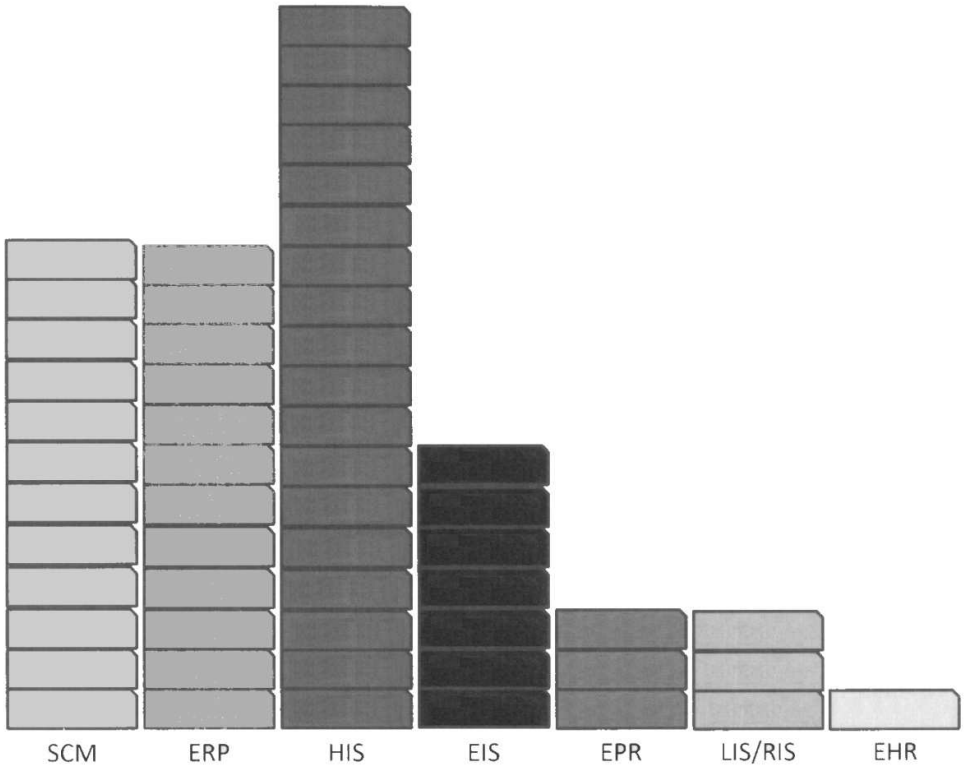

Figura 28 – Modelo SI/TIC da unidade hospitalar.

4.7 Solução encontrada para a unidade hospitalar

A solução que melhor se preconiza para este cenário será conseguir separar progressivamente os sistemas de DB para um sistema hibrido, paralelamente ao que está a ser utilizado pela unidade hospitalar, garantindo assim a continuidade do serviço.

Esta deve utilizar adaptadores e ter interfaces standards, para intercomunicação ente módulos aplicacionais assim como disponibilizar interfaces para fornecedores externos/internos.

Deve ser utilizar um meio-termo sem que seja feita uma mudança radical nos SI ou seja devemos ter a consciência para o facto que a unidade hospitalar x não pode parar. Para tal deve estar a ser implementada paralelamente um HSB “hibrido” que suporte as necessidades imediatas assim como a disponibilização de um interface HL7 para ligar novos equipamentos da imagiologia.

O desenvolvimento paralelo à solução existente é uma necessidade, garantindo a continuidade do serviço, apostando-se no desacoplamento progressivo das diferentes aplicações dos sistemas de informação da sua interligação direta.

O investimento inicial também é menor e mais fácil de gerir no tempo, tendo em conta que não se está a falar de criar uma solução de raiz mas sim moldar a existente. Com este novo sistema híbrido é possível conseguir desacoplar o sistema existente para este novo. O objetivo é permitir implementar regras de negócio que permitam à unidade hospitalar a independência necessária de um fornecedor original que se transformou em vários podendo assim garantir a continuidade e crescimento da sua plataforma.

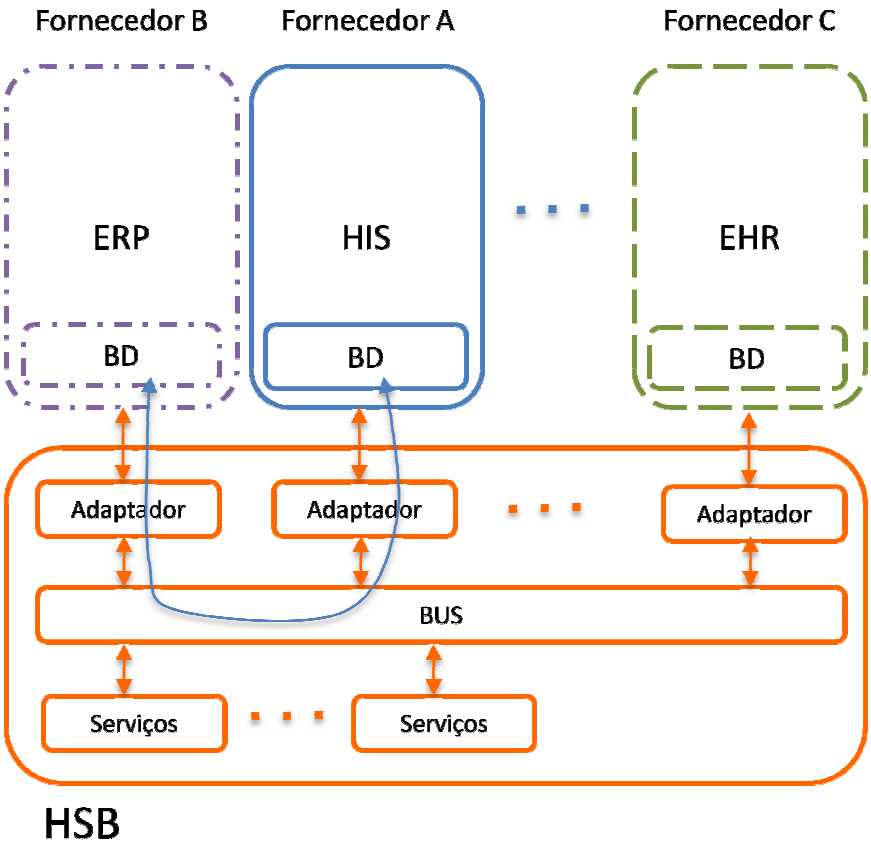

Figura 29 – Solução hibrida proposta para unidade hospitalar.

Neste novo cenário podemos verificar que o HSB híbrido continua a interagir com os demais SGBD que existem e criando um novo sistema de DB que opera sobre o bus, mas também é necessário referir que o HL7 não vai dar resposta a todos os problemas de normalização de informação. Como tal, é necessário que a organização aposte na normalização da informação interna, de forma a garantir o futuro da plataforma que for desenhada.

O ESB disponibiliza uma camada de abstração em cima de uma implementação de um sistema de mensagens da empresa, permite aos parceiros desenvolvedores de integração explorar o sistema, este representa a parte do software que fica entre as aplicações de negócios e permite a comunicação entre eles. Idealmente, o ESB deve ser capaz de substituir todo contacto direto com as aplicações no “bus”, de modo que toda a comunicação seja realizada através do ESB. Um software "adaptador" cumpre a tarefa de efetuar essas transformações (de forma análoga a um adaptador físico).

A interoperabilidade e flexibilidade de interligações entre sistemas e demais parceiros de desenvolvimentos, justificam o ESB ou neste caso um ESB mais especificamente o HSB per si.

Consideremos o exemplo de um novo equipamento na imagiologia com interface HL7 v2.3. Ao existir uma camada aplicacional que permita a inserção de imagens feita de uma forma genérica pelo provedor de software e disponibilizado segundo normas e standards de comunicação, é muito simples para a equipa de desenvolvimento da unidade hospitalar x criar um interface aplicacional para que o equipamento possa comunicar diretamente com os sistemas existentes.

CAPÍTULO 5

Conclusões e trabalho futuro

Esta tese envolveu a análise de uma unidade hospital de média dimensão, diagnosticar o estado atual do sistema de informação e propor uma solução para a arquitetura do sistema de informação da unidade hospitalar que seja fácil de evoluir, escalável e interoperável com fornecedores externos.

Parar que tal fosse possível, foi necessário analisar o estado da arte das tecnologias de interligação de sistemas de informação a propor à unidade hospitalar, assim como as vertentes da segurança na área da saúde, o que é muito relevante dadas as questões legais, de fiabilidade e confidencialidade.

Foi também necessário analisar standards de representação de informação médica e troca de mensagens, nomeadamente o HL7.

Fez-se uma análise do sistema de informação da unidade hospital, que por questões de confidencialidade não pode ser aqui completamente detalhado. Foi possível constatar que a unidade hospitalar tinha uma solução monolítica e neste momento depara-se com o problema de interligar sistemas de múltiplos fornecedores que foram evoluindo a partir de uma solução inicial monolítica. Os custos para manter este sistema estão a tornar-se incorporáveis, pelo que existe a necessidade de efetuar uma transformação a sua atual arquitetura para uma solução de baixo custo de integração com fornecedores.

Neste momento qualquer alteração tem enormes custos, pois não temos soluções externas diretas, logo coloca o hospital na mão do fornecedor inicial que foi desmembrado em vários.

Após análise do sistema de informação da unidade hospitalar x e dos requisitos de evolução futura apresentados pela direção, chegou-se à conclusão que a implementação de um HSB na unidade hospitalar trás variadíssimas vantagens para interoperabilidade imediata, assim como futura.

O cenário de interligação de todos os sistemas atuais ao HSB traria custos de implementação muito elevados, pois seria necessário proceder a uma revolução total no sistema de informação hospitalar. A solução proposta é utilizar uma solução hibrida e criar adaptadores no HSB adaptando-se o sistema atual de forma a funcionar como complemento à solução existente.

Esta solução necessita sempre da colaboração dos fornecedores de software atuais para que estes possam disponibilizar uma camada de “middleware” composta por um conjunto serviços web que permita a comunicação com o sistema de base de dados existente.

Conclui-se então que a melhor solução para a unidade hospitalar passaria pela implementação de um sistema híbrido constituído por uma serie de serviços do tipo SOA que possibilitassem a interação entre os sistemas e equipamentos a interligar.

Como trabalho futuro coloquei-me a disposição da unidade hospitalar para poder apoiar e fundamentar o trabalho junto desta pois, como esta dissertação tem uma componente confidencial de informação, será necessário fornecer ao hospital informações mais detalhadas sobre as necessidades de implementação de “middleware” prioritárias (aplicações mais utilizadas e/ou críticas, etc.).

BIBLIOGRAFIA

Bilal Siddiqui. Integrating healthcare services, Part 1: Using an Enterprise Service Bus for healthcare. In Using an Enterprise Service Bus for healthcare, IBM Corporation 2010.

Fabrizio Pecoraro and Daniela Luzi. The use of HL7 in the domain of Medical Devices. National Research Council - Institute of Research on Population and Social Policies (IRPPS), Rome, Italy, May 2011

Alin CORDOS, Bogdan ORZA, Aurel VLAICU, Serban MEZA, Carmen AVRAM, Bogdan PETROVAN. Technical University of Cluj Napoc, Pixeldata Cluj Napoca. Hospital Information System using HL7 and DICOM standards, ISSN: 1790-0832, Issue 10, Volume 7, October 2010, pp. 1295-1304

Amanda RYAN and Peter EKLUND.A Framework for Semantic Interoperability in Healthcare: A Service Oriented Architecture based on Health Informatics Standards. Centre for Health Services Development, University of Wollongong, Australia, 2008.

Lanhua Zhang. Studies of the HMIS Based on HL7 Criterions. Department of Information and Engineering, Taishan Medical University, Jan. 2011

T. J. Eggebraaten, J. W. Tenner, & J. C. Dubbels. (2007). A health-care data model based on the HL7 Reference Information Model. IBM SYSTEMS JOURNAL, 46, 1, 5-17.

Imran Khan. Health Level Seven Compliance and Clinical Decision Support System for an Intensive Care Unit. INDIAN INSTITUTE OF INFORMATION TECHNOLOGY ALLAHABAD, June 2007

Marco Eichelberg, Thomas Aden, and Jo¨ Rg Riesmeier, “A Survey and Analysis of Electronic Healthcare Record Standards”, ACM Computing Surveys, Vol. 37, No. 4, December 2005, pp. 277–315.

Martin Keen, Bill More, Antonio Carvalho, Michael Hamann, Prasad Imani, Ron Lotter, Philip Norton, Christian Ringler, Gabriel Telerman. Getting Started with WebSphere Enterprise Service Bus. ISBN-073849710X. IBM Redbooks. June 2006

Michael Taylor. Securing the Enterprise Service Bus: Protecting business critical web-services. SANS Institute, April 2009

Integrating the Healthcare Enterprise (IHE) achievements, expansion in new clinical domains and deployment, Nikolaus Wirsz, Siemens AG-Medical Solutions, 2005

Heath Level Seven (HL7), June 2011, URL www.hl7.org

A Guide to Physical Security for Data Centers, The Data Center Journal, july 2012, URL: http://www.datacenterjournal.com/facilities/a-guide-to-physical-security-for-data-centers/

Fiorano Enterprise Service Bus Architecture, Enterprise Service Bus, Fiorano ESB, August 2011 URL www.fiorano.com

Microsoft BizTalk, 2011. URL http://www.microsoft.com/biztalk/en/us/esb-guidance.aspx

BizTalk ESB Toolkit Forum, Jully 2011, URL http://social.msdn.microsoft.com/Forums/en-US/biztalkesb/threads

Advancing open standards for the information society. August 2011.
URL http://www.oasis-open.org/

Interoperability Between Healthcare Applications, John Gillson, ICW Labs, June 2010. URL http://www.slideshare.net/blues_fc/interoperability-between-healthcare-applications

Corepoint. The HL7 Evolution: Comparing HL7 Version 2 to Version 3, Including a History of Version 2. 2007, August 2011,
URL http://www.corepointhealth.com/sites/default/files/whitepapers/hl7-v2-v3-evolution.pdf ,

“HL7 v3 RIM: Is It Really that Intimidating?” RIM data model. May 2011. URL: http://www.hl7standards.com/blog/2011/05/31/hl7-v3-rim-is-it-really-that-intimidating/

"Why ESB?" June 2012, IntroPro, URL: http://www.intro-pro.com

"Data Encryption and Decryption", MSDN, May 2012, URL: http://msdn.microsoft.com/en-us/library/windows/desktop/aa381939(v=vs.85).aspx

"HL7 - A brief overview", HL7 Connect, October 2012.
URL: http://www.hl7connect.com/education

"Um Estudo sobre Criptografia e Assinatura Digital", June 2012, Fernando Antonio Mota Trinta; Rodrigo Cavalcanti de Macêdo
URL: www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm

"White paper on the impact of the Public Key technology and Digital Signatures on CAD.", June 2012, URL: http://www.datakey.com/SignaSURE-EDM_white_paper.htm.

"CAN STRONG AUTHENTICATION SORT OUT PHISHING AND FRAUD?", June 2012, Paul Ducklin, "paper" URL: http://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/phishingandfraud.pdf?dl=true

"Código Deontológico", Ordem dos Médicos, October, 2012,
URLhttps://www.ordemdosmedicos.pt/send_file.php?tid=ZmljaGVpcm9z&did=c06d06da9666a219db15cf575aff2824

Dave Shaver. HL7 and HIPAA. Carepoint Health. December 2010. URL
http://www.corepointhealth.com/whitepapers/hl7-and-hippa-what-you-need-know