

**UNIVERSIDADE FEDERAL DE SÃO CARLOS**

**CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA**

**PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO**

**H-PMI: UMA ARQUITETURA DE  
GERENCIAMENTO DE PRIVILÉGIOS PARA  
SISTEMAS DE INFORMAÇÃO DA ÁREA DE SAÚDE**

**IGOR VITÓRIO CUSTÓDIO**

**ORIENTADOR: PROF. DR. HÉLIO CRESTANA GUARDIA**

São Carlos - SP  
Janeiro/2010

**UNIVERSIDADE FEDERAL DE SÃO CARLOS**

CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

**H-PMI: UMA ARQUITETURA DE GERENCIAMENTOS  
DE PRIVILÉGIOS PARA SISTEMAS DE  
INFORMAÇÃO DA ÁREA DE SAÚDE**

**IGOR VITÓRIO CUSTÓDIO**

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de São Carlos, como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação, área de concentração: Sistemas Distribuídos e Redes.  
Orientador: Dr. Hélio Crestana Guardia.

São Carlos - SP  
Janeiro/2010

**Ficha catalográfica elaborada pelo DePT da  
Biblioteca Comunitária da UFSCar**

C987ha

Custódio, Igor Vitório.

H-PMI : uma Arquitetura de Gerenciamentos de Privilégios para Sistemas de Informação da Área de Saúde / Igor Vitório Custódio. -- São Carlos : UFSCar, 2010.  
134 f.

Dissertação (Mestrado) -- Universidade Federal de São Carlos, 2010.

1. Redes de computação - medidas de segurança. 2. Controle de acesso. 3. Serviços da web. 4. Redes de computação - segurança. 5. Prontuário. I. Título.

CDD: 005.8 (20<sup>a</sup>)

# Universidade Federal de São Carlos

Centro de Ciências Exatas e de Tecnologia

Programa de Pós-Graduação em Ciência da Computação

## “H-PMI: Uma Arquitetura de Gerenciamento de Privilégios para Sistemas de Informação da Área de Saúde”

IGOR VITÓRIO CUSTÓDIO

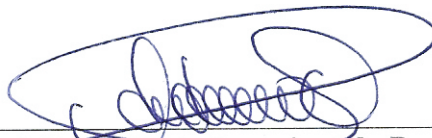
Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de São Carlos, como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação

Membros da Banca:



---

Prof. Dr. Hélio Crestana Guardia  
(Orientador - DC/UFSCar)



---

Prof. Dr. Antonio Francisco do Prado  
(DC/UFSCar)



---

Prof. Dr. Ivan Torres Pisa  
(DIS/UNIFESP)

São Carlos  
Fevereiro/2010

Dedico este trabalho a todos que direta ou indiretamente torcem por mim.

# AGRADECIMENTO

Gostaria de agradecer primeiramente a Deus Pai, Nossa Senhora Aparecida e a todos os Santos, pela força e ajuda nos momentos difíceis desta e de outras caminhadas, além das graças alcançadas.

Albertina e Osvaldo, mãe e pai, que investiram em minha educação e sempre me incentivaram para que eu progredisse, sou eternamente grato a tudo.

Meus irmãos Luzia e Venicius, pelos sobrinhos que tanto me alegram e pela convivência harmoniosa em família, além das horas de diversão.

A minha namorada, amada, parceira, amiga, confidente, incentivadora, designer de interface, de imagens, Maria Alice Torres por toda a ajuda desde a graduação até os dias atuais.

À família dela, Dona Cleonice, Seu José Torres, Regina, pela ajuda, respeito, acolhida e consideração obtida desde sempre.

A todos do Departamento de Computação que participaram da minha formação e que passaram pela minha vida, em especial o professor Doutor Helio Crestana Guardia, amigo e orientador de longa data.

Aos professores doutores: Sérgio Donizetti Zorzo, Wanderley Lopes de Souza, Hermes Senger, pelas considerações e compartilhamento de conhecimento durante este trabalho.

Aos brasileiros, que pagando seus impostos permitem que pessoas possam estudar em cursos públicos de qualidade.



Um pai sábio deixa que os filhos cometam erros.  
É bom que, de quando em quando, queimem os dedos

Gandhi



# RESUMO

A informatização dos ambientes da área de saúde, como a substituição dos prontuários em papéis por versões eletrônicas, permitiu diversas melhorias no atendimento aos pacientes, além da disponibilização de informações de forma mais acessível.

Porém, com esta tecnologia surgiram preocupações maiores por parte dos pacientes em relação ao controle de acesso aos seus dados confidenciais, uma vez que com a acessibilidade facilitada, a possibilidade de pessoas não autorizadas acessarem tais dados também é ampliada.

É neste cenário que está incluído o Health - Privilege Management Infraestructure, ou H-PMI, tratado neste trabalho, que visa a apresentar uma Arquitetura para o Gerenciamento de Privilégios para Sistemas de Informação da área de saúde. H-PMI almeja ser aderente às normas e leis brasileiras, sendo fiel às regras de certificação de sistemas da área de saúde definidas pelo Conselho Federal e Medicina em conjunto com a sociedade Brasileira de Informática em Saúde.

O objetivo deste trabalho é especificar o H-PMI, de forma que ele seja capaz de fornecer garantias de seguranças necessárias segundo a legislação vigente, permitindo um acesso legítimo a dados confidenciais, além de conceder o acesso a dados restritos em situações excepcionais em que isto é autorizado.

Como resultado do desenvolvimento do trabalho proposto, implantou-se o Web H-PMI integrado com o Google Health demonstrando a capacidade de implantação de parte substancial da arquitetura proposta em ambientes existentes.

**Palavras-chave:** Infraestructura de gerenciamento de privilégios, Web services, Segurança, Registro Eletrônico em Saúde, Google Health.

# ABSTRACT

The use of Information Systems in health environments, like the substitution of paper versions of medical records by electronics ones, has improved patient assistance and allowed such information to be available in a more accessible way.

Along with this technology, however, there are significant issues raised by the patients about the access control over their confidential data, which becomes more available and could be accessed by unauthorized people.

It is in this scenario that Health - Privilege Management Infrastructure, or H-PMI, is presented in this work. It aims to provide a software architecture for privilege management in health environments. H-PMI aims to be adherent to the Brazilian laws and rules related to the access to electronic medical records, like the ones defined in Manual de Certificação de Sistemas da Área de Saúde by Conselho Federal de Medicina and Sociedade Brasileira de Informática em Saúde.

The main objective of this work is to specify the envisioned H-PMI, so it can provide restricted access to electronic medical records in accordance with the appropriate law and recommendations security guarantees, allowing trusted access to sensitive data while allowing circumstantial access to these data in exceptional situations.

In order to evaluate the applicability of the proposed H-PMI architecture we have developed the Web H-PMI, which is integrated with the Google Health platform. The obtained results show that the developed architecture can be applied in existing health environments.

**Keywords:** PMI, Web services, Security, Electronic Medical Records, Google Health.

# LISTA DE FIGURAS

Figura 2-1 - Exemplo certificado digital ICP-Brasil .....	22
Figura 2-2 - Certificado Digital Ligado a Certificados de Atributos .....	26
Figura 2-3 - Passaporte e Vistos, analogia com Certificado Digital e Certificado de Atributos .....	27
Figura 2-4 - Exemplo de ligação entre Certificado Digital e Certificado de Atributo ..	30
Figura 2-5 - Fragmento de política de acesso em XACML.....	32
Figura 3-1 - Fragmento de um CCR armazenado no Google Health .....	39
Figura 4-1 - Exemplo de Delegação (Zhang, Ahn <i>et al.</i> , 2002) .....	45
Figura 6-1 - Registro de tela do ambiente de produção Google Health .....	52
Figura 6-2 - Modelo de autorização OAuth (OAuth for Web Applications, 2009) .....	53
Figura 6-3 - Modelo de autorização AuthSub (AuthSub for Web Applications, 2009)	54
Figura 6-4 - Registro de tela do ambiente H9.....	56
Figura 7-1 - Modelo Geral de Controle .....	59
Figura 7-2 - Modelo de Delegação .....	60
Figura 8-1 - Hierarquia de papéis (Motta e Furuie, 2002) .....	62
Figura 8-2 - Arquitetura MACA (Motta e Furuie, 2002).....	64
Figura 8-3 - Arquitetura RDM2000 (Zhang, Ahn <i>et al.</i> , 2003).....	65
Figura 8-4 - Gerenciamento de regras RDM2000 (Zhang, Ahn <i>et al.</i> , 2003).....	66
Figura 8-5 - Exemplo de representação de Permissões de Confidencialidade em XML usados no TCM (Longstaff, Lockyer <i>et al.</i> , 2003) .....	68
Figura 8-6 - Arquitetura OASIS (Bacon, Moody <i>et al.</i> , 2002) .....	70
Figura 8-7 - Arquitetura MEDIS (Sucurovic, 2007) .....	71
Figura 9-1 - H-PMI: Arquitetura Geral .....	75
Figura 9-2 - Estrutura de um Registro Eletrônico em Saúde dividido em objetos distintos .....	79
Figura 9-3 - H-PMI: Modelo de Controle .....	81
Figura 9-4 - H-PMI: Modelo de Delegação Direta .....	85
Figura 9-5 - H-PMI: Exemplo de hierarquia de papéis .....	86
Figura 9-6 - H-PMI: Modelo de Delegação Indireta .....	87

Figura 10-1- Arquitetura Web H-PMI.....	97
Figura 10-2 - Página principal do Web H-PMI.....	101
Figura 10-3 - Página de administração do Web H-PMI.....	102
Figura 10-4 - Página de vinculação de perfil H9 com Web H-PMI .....	103
Figura 10-5 - Página de autenticação H9 para vinculação do perfil com Web H-PMI .....	104
Figura 10-6 - Página de consentimento de vinculação do H9 com Web H-PMI.....	104
Figura 10-7 - Página do Web H-PMI informando do sucesso do processo de vinculação .....	105
Figura 10-8- Página do menu de delegação do Web H-PMI.....	106
Figura 10-9 - Página do menu de delegação do Web H-PMI ao se clicar sobre usuário que possui delegação.....	107
Figura 10-10 - Página do menu de delegação do Web H-PMI ao se clicar sobre opção Delegar .....	108
Figura 10-11 - Página do menu de delegação do Web H-PMI sucesso na delegação .....	109
Figura 10-12 - Página do menu de Políticas do Web H-PMI.....	110
Figura 10-13 - Página do menu de Políticas do Web H-PMI ao se clicar "Detalhes" .....	111
Figura 10-14 - Página do menu de Políticas do Web H-PMI ao se clicar "Visualizar" .....	111
Figura 10-15 - Página do menu de Prontuário do Web H-PMI.....	112
Figura 10-16 - Página do menu de Prontuário do Web H-PMI o se clicar "Detalhes" .....	113
Figura 10-17 - Página do menu de Prontuário do Web H-PMI o se clicar "CCR"....	113
Figura 10-18 - Página do menu de Logs do Web H-PMI.....	114
Figura 10-19: Integração entre as tecnologias utilizadas .....	116

# LISTA DE TABELAS

Tabela 2-1 - Campos do Certificado de Atributos.....	28
Tabela 9-1 - Tabela de Permissões de Acesso ao Objeto Restrito B.....	80
Tabela 9-2- Perfis vinculados ao Agente A .....	82
Tabela 9-3 - Comparativo entre trabalhos relacionados e o H-PMI.....	91
Tabela 10-1 - comparação entre nomenclatura de módulos H-PMI e Web H-PMI....	95

# LISTA DE ABREVIATURAS E SIGLAS

**AA** - *Autoridade de Autorização*

**AC** - *Autoridade Certificadora*

**BDA** - *Base de Dados de Autorização*

**CABA** - *Controle de Acesso Baseado em Atributos*

**CABI** - *Controle de Acesso Baseado em Identidade*

**CABP** - *Controle de Acesso Baseado em Papéis*

**CA<sub>t</sub>** - *Certificado de Atributo*

**CCR** - *Continuity of Care Record*

**CD** - *Certificado Digital*

**CFM** - *Conselho Federal de Medicina*

**CN** - *Nome Comum*

**DD** - *Delegação Direta*

**DI** - *Delegação Indireta*

**HIPAA** - *Health Insurance Portability and Accountability Act of 1996*

**H-PMI** - *Health-Privilege Management Infrastructure*

**ICP** - *Infraestrutura de Chaves Públicas*

**DIRPF** - *Declaração de Imposto de Renda de Pessoa Física*

**LDAP** - *Lightweight Directory Access Protocol*

**MACA** - *Middleware para Autorização e Controle de Acesso*

**MEDIS** - *MEDical Information System*

**NGS** - *Nível de Garantia de Segurança*

**NIST** - *National Institute of Standards and Technology*

**OA** - *Origem de Autorização*

**OASIS** - *Open Architecture for Securely Interworking Services*

**PAdP** - *Ponto de Administração de Políticas*

**PAP** - *Policy Administration Point*

**PAR** - *Ponto de Aplicação de Regras*

**PBI** - *Ponto de Busca de Informação*

**PC** - *Permissões de Confidencialidade*

**PD** - *Ponto de Decisão*

**PDAM** - *Proposed Draft Amendment*  
**PDP** - *Policy Decision Point*  
**PEP** - *Policy Enforcement Point*  
**PIP** - *Policy Information Point*  
**PMI** - *Privilege Management Infrastructure*  
**PP** - *Prontuário do Paciente*  
**RA** - *Repositório de Atributos*  
**RD** - *Repositório de Delegações*  
**RES** - *Registros Eletrônicos em Saúde*  
**SD** - *Sistema de Delegação*  
**SGBD** - *Sistema de Gerenciamento de Banco de Dados*  
**SGH** - *Sistema de Gestão Hospitalar*  
**SGP** - *Sistema de Gestão e Privilégios*  
**SIG** - *Sistemas de Informações Gerenciais*  
**S-RES** - *Sistema de Registro Eletrônico em Saúde*  
**VA** - *Validador/Autorizador*  
**XACML** - *eXtensible Access Control Markup Language*  
**XML** - *eXtensible Markup Language*

# SUMÁRIO

<b>CAPÍTULO 1 - INTRODUÇÃO.....</b>	<b>14</b>
1.1 Considerações Iniciais.....	14
<b>CAPÍTULO 2 - AUTENTICAÇÃO E AUTORIZAÇÃO .....</b>	<b>17</b>
2.1 Autenticação/Autorização.....	17
2.2 Autenticação.....	18
2.2.1 Certificação Digital X.509 .....	19
2.2.2 Certificação Digital no Brasil.....	21
2.3 Autorização .....	23
2.3.1 Certificados de Atributos .....	24
2.3.2 Políticas de acesso .....	30
2.4 Considerações Finais.....	32
<b>CAPÍTULO 3 - REGISTRO ELETRÔNICO EM SAÚDE.....</b>	<b>33</b>
3.1 Registro Eletrônico em Saúde.....	33
3.2 Modelo de Referência .....	36
3.3 Continuity of Care Record .....	38
3.4 Considerações Finais.....	40
<b>CAPÍTULO 4 - CERTIFICAÇÃO PARA SISTEMAS DE REGISTRO ELETRÔNICO EM SAÚDE .....</b>	<b>41</b>
4.1 Manual de Certificação para Sistemas de Registro Eletrônico em Saúde .....	41
4.2 A delegação de poderes.....	43
4.3 Considerações Finais.....	45
<b>CAPÍTULO 5 - WEB SERVICES .....</b>	<b>47</b>
5.1 Introdução .....	47
5.2 Segurança em Web services.....	48
5.3 Considerações Finais.....	49
<b>CAPÍTULO 6 - GOOGLE HEALTH.....</b>	<b>50</b>
6.1 O Google Health.....	50



6.2 Google Health API.....	53
6.3 Considerações Finais.....	56
<b>CAPÍTULO 7 - INFRAESTRUTURA DE GERENCIAMENTO DE PRIVILÉGIOS ....</b>	<b>57</b>
7.1 Infraestrutura de Gerenciamento de Privilégios .....	57
7.2 Considerações Finais.....	60
<b>CAPÍTULO 8 - TRABALHOS RELACIONADOS .....</b>	<b>61</b>
8.1 Introdução .....	61
8.2 MACA: Middleware para Autorização e Controle de Acesso.....	62
8.3 RDM2000 .....	64
8.4 Tees Confidentiality Model (TCM).....	66
8.5 Open Architecture for Securely Interworking Services (OASIS) .....	68
8.6 MEDical Information System (MEDIS) .....	70
8.7 Considerações Finais.....	72
<b>CAPÍTULO 9 - H-PMI.....</b>	<b>73</b>
9.1 Introdução .....	73
9.2 H-PMI .....	74
9.3 Modelo de Gerenciamento de Privilégios ( <i>Privilege Management Model</i> ) .....	74
9.4 Modelo de Controle .....	76
9.5 Modelo de Delegação .....	82
9.5.1 Delegação Direta (DD) .....	83
9.5.2 Delegação Indireta (DI) .....	86
9.6 H-PMI e trabalhos relacionados .....	89
9.7 Considerações Finais.....	93
<b>CAPÍTULO 10 - WEB H-PMI .....</b>	<b>94</b>
10.1 Introdução .....	94
10.2 H-PMI e o Web H-PMI.....	95
10.3 Módulos Web H-PMI .....	96
10.3.1 Policy Enforcement Point (PEP).....	98
10.3.2 Policy Decision Point (PDP) .....	98
10.3.3 Policy Information Point (PIP).....	99
10.3.4 Policy Administration Point (PAP) .....	99

10.3.5 Interface Web .....	100
10.3.5.1 Página principal .....	100
10.3.5.2 Página de administração .....	101
10.3.5.3 Página de vinculação de perfil.....	102
10.3.5.4 Página de delegação.....	105
10.3.5.5 Página de políticas .....	109
10.3.5.6 Página de políticas .....	112
10.3.5.7 Página de logs.....	113
10.3.5.8 Web H-PMI Web service .....	114
10.3.6 Informações gerais de ambiente .....	115
10.4 Considerações Finais .....	117
<b>CAPÍTULO 11 - CONSIDERAÇÕES FINAIS.....</b>	<b>118</b>
11.1 Considerações Finais.....	118
11.2 Trabalhos futuros .....	119
<b>REFERÊNCIAS BIBLIOGRÁFICAS.....</b>	<b>120</b>
<b>APÊNDICE A.....</b>	<b>125</b>

# Capítulo 1

## INTRODUÇÃO

---

*Neste capítulo serão abordadas considerações gerais sobre este trabalho.*

### 1.1 Considerações Iniciais

Em ambientes da área de saúde trabalha-se com informações pessoais que devem ser tratadas com sigilo garantido por mecanismos como regimentos das profissões, códigos de ética, ou legislações próprias.

A garantia de que o acesso às informações armazenadas nos Registros Eletrônicos em Saúde (Waegemann, 1996) obedece às recomendações estabelecidas pelos órgãos reguladores e pelas especificações e padrões internacionais contudo, não é facilmente obtida.

De maneira geral, o paciente é o dono das informações acerca de seu prontuário médico, que pode ser acessado pelo profissional de saúde que o está tratando (Motta, 2003). Por outro lado, outros profissionais em exercício legítimo da profissão podem necessitar, em casos excepcionais, do acesso a esses dados considerados sigilosos, como em um atendimento de urgência.

Em ambientes da área de saúde também é comum que profissionais deleguem a outrém o acesso a determinadas informações para que seja dada continuidade a um atendimento ou simplesmente para que seja fornecida uma segunda opinião sobre um caso (Zhang, Ahn *et al.*, 2002).

Em condições normais, contudo, apenas o paciente tem acesso às informações de seu prontuário e pode autorizar profissionais de saúde a acessá-las.

Arquiteturas de gerenciamento de privilégios, previstas para estes casos são geralmente compostas por diversos sistemas e têm como finalidade prover mecanismos de segurança para garantir acesso legítimo a conteúdos sigilosos e que não devem ser acessados sem que os devidos controles sejam fornecidos. Além disso, devem possibilitar a delegação de permissões quando necessário e a garantia de sigilo se esta for a decisão.

Embora essas questões apresentadas sejam comumente vivenciadas nas áreas de saúde, não há sistemas de gerenciamento desses privilégios em amplo uso na rede de saúde pública, solucionando de maneira absoluta as questões de manutenção do sigilo e de possibilidade de acesso controlado aos dados em momentos excepcionais.

Diversos estudos e propostas de arquiteturas de gerenciamento de privilégios estão em uso e em desenvolvimento, mas normalmente têm funcionalidade restrita ou atendem a requisitos específicos da legislação de diferentes países.

Assim, arquiteturas que abordem os problemas gerais da área e as especificidades locais, a fim de permitir que todos os requisitos sejam respondidos adequadamente segundo as leis e normas vigentes em cada país, ainda são uma necessidade.

Com vista a isto, este trabalho apresenta o *Health - Privilege Management Infrastructure*, ou H-PMI, que é uma Infraestrutura de Gerenciamento de Privilégios para sistemas de informações da área de saúde.

Dentre outros pontos relacionados ao acesso a essas informações, H-PMI visa resolver questões relacionadas com:

- Segurança: ser um sistema capaz de prover as funcionalidades de segurança inerentes à área de saúde;
- Regulamentações: ser aderente às normas oficiais existentes;
- Flexibilidade: ser utilizado convenientemente nos diversos segmentos da área de saúde;
- Delegação: prover um mecanismo real e flexível para garantir o acesso legítimo a dados restritos em situações de emergência;
- Sigilo: garantir que dados sigilosos sejam tratados adequadamente.

Uma vez definida uma arquitetura de segurança que atenda os aspectos relacionados, este trabalho também trata da implementação de um conjunto deles. Para tanto, o desenvolvimento de uma interface Web para acesso e gerenciamento e a integração com os dados armazenados no sistema **Google Health** foram realizados.

O restante deste documento aborda os pontos principais que fundamentam o H-PMI e está organizado como segue.

Primeiro apresentam-se os conceitos de Autenticação e Autorização necessários para todos os sistemas de segurança, abordando os aspectos principais de cada área, diferenciando-as e justificando os pontos que serão utilizados pelo H-PMI. Após isto, apresenta-se o Registro Eletrônico de Saúde (Resolução Conselho Federal de Medicina n. 1.638/2002a. Define prontuário médico e dá outras providências, 2002), que corresponde à estrutura básica de todos os sistemas da área de saúde que deseja-se proteger pelo H-PMI. É neste ponto que são apresentados também os conceitos de Delegação de Poder, procedimento utilizado na área de saúde e que requer um tratamento especial. Também neste trabalho é apresentado o Manual de Certificação para Sistemas de Registro Eletrônico de Saúde, cujas regras nortearam a proposta do H-PMI, além de fornecer informações sobre as normas e padrões nacionais e internacionais vigentes sobre o assunto.

A seguir, apresenta-se uma arquitetura geral de um *Privilege Management Infrastructure*, base do H-PMI. Analisam-se também alguns projetos de Infraestruturas de Gerenciamento de Privilégios, a fim de servir de comparativo com a arquitetura proposta.

Com estes tópicos analisados é, então, apresentado o *Health - Privilege Management Infrastructure*, uma arquitetura de gerenciamentos de privilégios desenvolvida para sistemas de informação da área de saúde com suporte a delegação de autorização. A arquitetura proposta é descrita com detalhes, começando pela estrutura geral, passando pela estrutura de controle e por fim, chegando à sua estrutura de delegação.

Uma vez apresentado o H-PMI, é realizada uma comparação da arquitetura proposta com os outros sistemas analisados anteriormente.

Por fim, apresenta-se o Web H-PMI, a implementação prova de conceito da arquitetura proposta seguindo-se das considerações finais.

# Capítulo 2

## AUTENTICAÇÃO E AUTORIZAÇÃO

---

*Este capítulo apresenta os conceitos de autenticação e autorização.*

### 2.1 Autenticação/Autorização

Autenticação, em linhas gerais, é a capacidade de se atribuir corretamente uma identidade a um determinado agente<sup>1</sup> (Sandhu e Samarati, 1994), (Burrows, Abadi *et al.*, 1990), ou seja, é um mecanismo que comprova que os agentes envolvidos em uma transação são quem realmente afirmam ser, não permitindo que nenhum intruso consiga se passar por um agente real e legítimo na transação citada.

Como exemplo de mecanismos de autenticação, podemos citar: uso conjunto de nome de usuário e senha, uso de mecanismos biométricos, como digitais ou imagens da íris, cartões inteligentes, uso de certificados digitais, como será mostrado mais adiante, dentre outros.

Já autorização, por sua vez, é a capacidade de um sistema de permitir ou não a um agente devidamente autenticado utilizar esse sistema, tratando o acesso a objetos restritos, a execução de determinadas tarefas, a delegação de acesso, etc. (Sandhu e Samarati, 1994). Ou seja, é o sistema que verifica se um agente tem ou

---

<sup>1</sup> Agente: Define-se como agente um usuário, um sistema ou um computador que executa determinada operação

não permissão para realizar o que ele deseja no momento da requisição, o que é caracterizado como um privilégio.

Exemplos de autorizações são muitos, como os utilizados em Sistemas Operacionais na gestão de privilégios de acesso a recursos, como acesso a arquivos, permissão de uso de hardware, como impressoras, etc.

Na vida diária, estes conceitos também estão presentes, como no uso de documentos de identificação, como a Carteira Nacional de Habilitação, solicitada por um agente de trânsito para autenticar o condutor do veículo através da análise da foto e certificar-se da permissão de direção ao verificar as categorias em conjunto com outras informações presentes no documento.

Neste exemplo, verificamos a ação dos dois mecanismos, a autenticação, através da análise da foto, bem como a autorização, através da análise das restrições de direção e de categorias presentes neste documento. Quando se utilizam mecanismos de autenticação e autorização juntos, pode-se definir que há um mecanismo de Controle de Acesso. Neste caso, define-se como aquele que implementa mecanismos de Autenticação e de Autorização a fim de assegurar o acesso correto e legítimo às requisições, além de possuir mecanismos de auditoria para certificar que os mecanismos estão funcionando adequadamente e não foram adulterados (Sandhu e Samarati, 1994).

Neste trabalho serão consideradas sempre em conjunto a autenticação e a autorização, bem como a auditoria, pois cada um tem seu papel fundamental na arquitetura proposta.

## 2.2 Autenticação

Existem diversos mecanismos de autenticação, cada um com suas especificidades, com seus pontos fortes e fracos.

Por exemplo, o uso de um mecanismo de nome de usuário e senha por si só é uma forma de autenticação largamente utilizada, porém, a sua utilização em sistemas distribuídos pode causar falha de autenticação (Blaze, Feigenbaum *et al.*, 1999),(Neuman e Ts'o, 1994). Um caso em que isto pode ser detectado é quando ocorre compartilhamento de informações secretas (dados de acesso), como o uso

por um agente intruso, que as obteve através de um analisador de pacotes de rede. Com isto, verifica-se a possibilidade de um agente não cadastrado se passar por um agente válido ao fazer uso dos dados compartilhados, de um agente devidamente cadastrado para usar o sistema, obtidos através da análise de pacotes na rede.

Para evitar este tipo de falha existem aperfeiçoamentos de mecanismos de autenticação baseados em usuários e senhas, como a utilização de senhas de uso único, ou *One-Time passwords*, que possuem mecanismos de sincronização e de geração de senhas únicas, permitindo que uma senha utilizada para uma autenticação não seja válida para uma próxima utilização.

Kerberos é outro mecanismo de autenticação utilizado em sistemas distribuídos (Neuman e Ts'o, 1994). Segundo Neuman e Ts'o, 1994, Kerberos pode ser definido como um serviço de autenticação distribuído que permite um processo cliente, ativado em nome de um usuário, provar sua identidade a uma aplicação verificadora que está em modo servidor, sem ter que enviar dados através da rede que possam permitir a um atacante ou o próprio verificador personificar o usuário.

Assim, Kerberos fornece um serviço de autenticação em sistemas distribuídos capaz de autenticar um cliente, sem possuir a vulnerabilidade das senhas, por exemplo.

Porém, como todos os mecanismos de autenticação, Kerberos também possui algumas limitações, como ser vulnerável a ataques em que são feitas tentativas exaustivas de descobrir as senhas através do pedido de autenticação de determinado usuário usando combinações aleatórias de caracteres, dentre outros, conforme mostrado em (Neuman e Ts'o, 1994).

Para evitar este tipo de vulnerabilidade bem como ampliar a segurança, pode-se utilizar outros mecanismo de autenticação, como certificados digitais, baseados em pares de chaves público/privadas (Souza, Cunha *et al.*, 2004).

### **2.2.1 Certificação Digital X.509**

Um Certificado Digital (CD) é um dos elementos finais de uma estrutura complexa chamada Infraestrutura de Chaves Públicas (ICP), que pode ser definida como um conjunto de leis, de normas, de práticas e de procedimentos que, utilizando aparatos em hardware e software, implementam a certificação digital utilizando criptografia de chaves públicas (Souza, Cunha *et al.*, 2004).



Um Certificado Digital é basicamente um conjunto de informações previamente determinadas e agregadas à cópia da chave pública de um agente a ser certificado. Estas informações reunidas são então organizadas a fim de serem assinadas digitalmente por uma entidade confiável, no caso uma Autoridade Certificadora (AC).

Assim, o conjunto de dados e a chave pública do agente assinados digitalmente é o que se define como um Certificado Digital.

Uma autoridade certificadora, ao assinar digitalmente o certificado de um agente, atesta que as informações contidas nesse certificado são legítimas e podem ser usadas para verificar as seguintes ações do usuário que possui a chave privada associada ao certificado:

- Autenticidade: que algo foi realmente feito pelo agente que o diz ter feito;
- Não repúdio: que algo foi efetivamente realizado pelo agente;
- Confidencialidade: que o acesso a algum conteúdo seja impedido a agentes não autorizados;
- Integridade: que um conteúdo assinado não foi modificado, acidental ou intencionalmente;
- Temporalidade: que determinada ação foi feita num instante de tempo específico.

Os processos que definem os funcionamentos das AC's são especificados por regras, que podem permitir a delegação da permissão de emissão de certificados entre AC's, criando uma estrutura hierárquica de Certificação Digital. Assim, as AC's filhas, numa hierarquia, devem garantir o cumprimento das regras, bem como respeitar as leis e normas vigentes ao executar a sua atividade.

Um exemplo do uso de certificados digitais na vida cotidiana é visto no acesso a servidores de instituições financeiras de páginas da Internet, para garantir que um site bancário é realmente do banco que se deseja acessar.

Outro exemplo ocorre no acesso a serviços oficiais, como o envio autenticado de Declaração de Imposto de Renda de Pessoa Física (DIRPF).

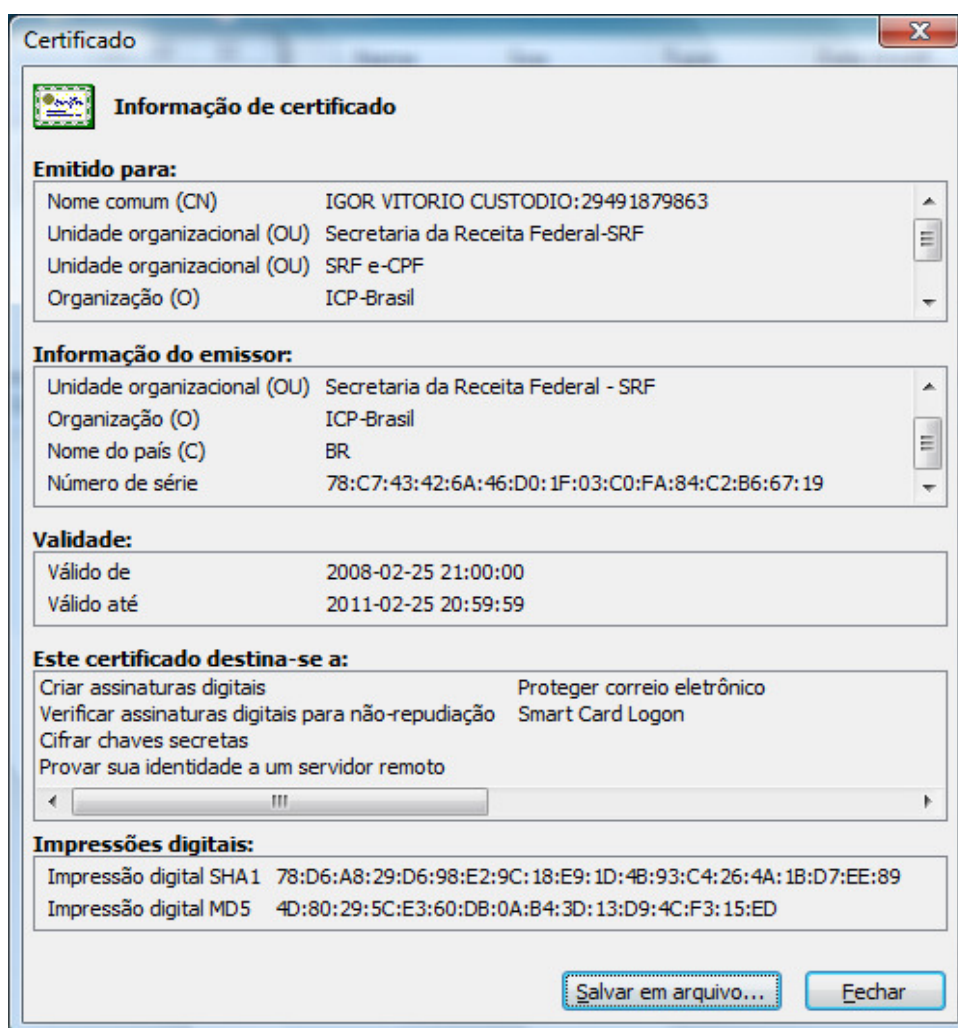
### 2.2.2 Certificação Digital no Brasil

O Brasil possui uma Infraestrutura de Chaves Públicas chamada ICP-Brasil, instituída oficialmente pela Medida Provisória 2.200-2 publicada em 24 de agosto de 2001. Com esta medida tornaram-se oficiais os esforços para validar juridicamente a utilização de certificados digitais provenientes desta estrutura. Também com ela criou-se e instituiu-se um Comitê Gestor da ICP-Brasil, responsável por gerenciar e aprovar os documentos que regem a estrutura, bem como a Autoridade Certificadora Raiz da ICP-Brasil, responsável por controlar a emissão de certificados para Autoridades Certificadoras subordinadas, como a do SERPRO ou CAIXA, etc.

Com isto, todas as AC's vinculadas à ICP-Brasil devem se submeter aos documentos que regem a ICP-Brasil.

Um destes documentos é a Declaração das Práticas de Certificação da AC-Raiz, que define os detalhes da operação da certificação deste nível, como as informações contidas nos certificados digitais assinados/emitidos pela AC.

Na Figura 2-1 verifica-se um exemplo de um Certificado Digital ICP-Brasil pessoal, como os utilizados para o envio de Declarações de IRPF.



**Figura 2-1 - Exemplo certificado digital ICP-Brasil**

Neste exemplo é possível identificar alguns pontos-chaves do Certificado Digital, versão 3 (Recommendations series X.509: Information Technology – Open Systems Interconnection - The Directory: Authentication Framework, 2001) como:

- Nome comum (CN): Nome da pessoa que detém o direito de utilização do certificado;
- Validade do Certificado;
- Identificador do algoritmo da assinatura: apesar do certificado digital ter sido emitido no ano de 2008, ele não seguiu as recomendações do ETSI TS 102 176-1 que dizem para evitar o uso de SHA1 nos próximos anos (Etsi, 2007), atitude que poderia garantir uma segurança adicional;
- Identificador do emissor, no caso a Secretaria da Receita Federal – SRF;

- Usos previstos do Certificado, como o uso para assinaturas digitais, uso em ferramentas de autenticações, etc.

## 2.3 Autorização

Autorizações são definidas como a capacidade de definir se um agente devidamente autenticado tem direitos de realizar determinada tarefa, como acessar determinado objeto<sup>2</sup>, bem como quais modos de acesso a este objeto ele tem (Sandhu e Samarati, 1994).

Ou seja, um agente pode ter o direito de executar uma tarefa, que seja de acessar determinada pasta do sistema somente no modo de leitura, porém outro pode ter permissões diferentes como, no caso citado, direitos de leitura e escrita.

Neste trabalho, os termos: direito de acesso, permissão ou privilégio são utilizados para referenciar as autorizações sem fazer distinção.

Utiliza-se também um modelo de autorização chamado Controle de Acesso Baseado em Papéis (CABP), definido pelo *National Institute of Standards and Technology* (NIST) (Ferraiolo, Sandhu *et al.*, 2001).

Este tipo de controle de acesso possui características que atendem aos requisitos de controle de acesso aos Registros Eletrônicos em Saúde (RES), sendo uma recomendação do *Health Insurance Portability and Accountability Act of 1996* (HIPAA) para controle de acesso aos dados dos pacientes (Security and electronic signature standards, 1998),(Motta e Furuie, 2002).

Segundo Motta e Furuie (2002) o CABP permite controlar o acesso de agentes às informações contidas no RES com base nos papéis que eles exercem no ambiente. Estes papéis denotam as funções, com as autoridades e responsabilidades inerentes ao agente para qual o papel foi designado (Ferraiolo, Sandhu *et al.*, 2001).

Com isto, é feita uma associação entre autorizações e papéis de acordo com as atribuições adequadas e não diretamente aos agentes. Papéis são ligados aos agentes segundo as funções que eles exercem.

---

<sup>2</sup> Objeto: Define-se como objeto um recurso a ser acessado

Por exemplo, em um hospital foi levantado que existem, dentre outros papéis, os de Médico e de Diretor Clínico, cada um com permissões de acesso ao RES de acordo com sua necessidade.

Assim, um médico que acumule a função de Diretor Clínico irá possuir neste sistema os papéis de Médico e de Diretor Clínico.

Além disto, o CABP favorece a administração da política de acesso, pois permite que esta seja colocada na perspectiva de um modelo organizacional (Oh e Park, 2001), ou seja, permite-se que o modelo organizacional vigente seja refletido nas políticas adotadas, como por exemplo, uma pessoa do departamento de vendas será considerada na política como do papel de vendas.

Assim, usuários podem ser mais facilmente remanejados de um papel para outro, bem como novas autorizações e papéis podem ser criados e concebidos de acordo com as necessidades da organização.

Ao permitir que privilégios não sejam concebidos diretamente a usuários, mas a papéis, a rotatividade de pessoal tem um baixo impacto na administração da política de autorização, que pode então ser realizada de forma unificada por papéis específicos.

No caso do médico que acumulava papéis, caso deixe de ter a atribuição de Diretor Clínico, basta remover a atribuição do papel a este usuário que ele passará automaticamente a não ter mais as permissões que ele possuía quando desempenhava aquela função.

Assim, este modelo de controle de acesso tem todas as características necessárias para a aplicação em questão, fornecendo a flexibilidade necessária para as aplicações deste trabalho, bem como a sua aplicação em outros domínios correlatos, como a proteção de áreas restritas em ambientes corporativos, áreas de Sistemas de Informações Gerenciais (SIG), etc.

### **2.3.1 Certificados de Atributos**

Certificados de atributos são definidos por Farrel e Housley (2002) e, assim como os Certificados Digitais X.509, são arquivos contendo informações estruturadas e que possuem seu conteúdo assinado por um agente capacitado, no caso, a Autoridade de Autorização (AA).

Certificados de Atributos são utilizados para garantir que os dados em seu interior carreguem informações autenticadas que possam ser consideradas válidas desde que a estrutura do certificado esteja válida.

Assim, analogamente à Autoridade Certificadora, que analisa a requisição de um Certificado Digital antes de assiná-lo, a Autoridade de Atributo também tem esta finalidade. Ela analisa, constrói e assina digitalmente o Certificado de Atributo para que ele tenha validade e seu uso seja efetivo.

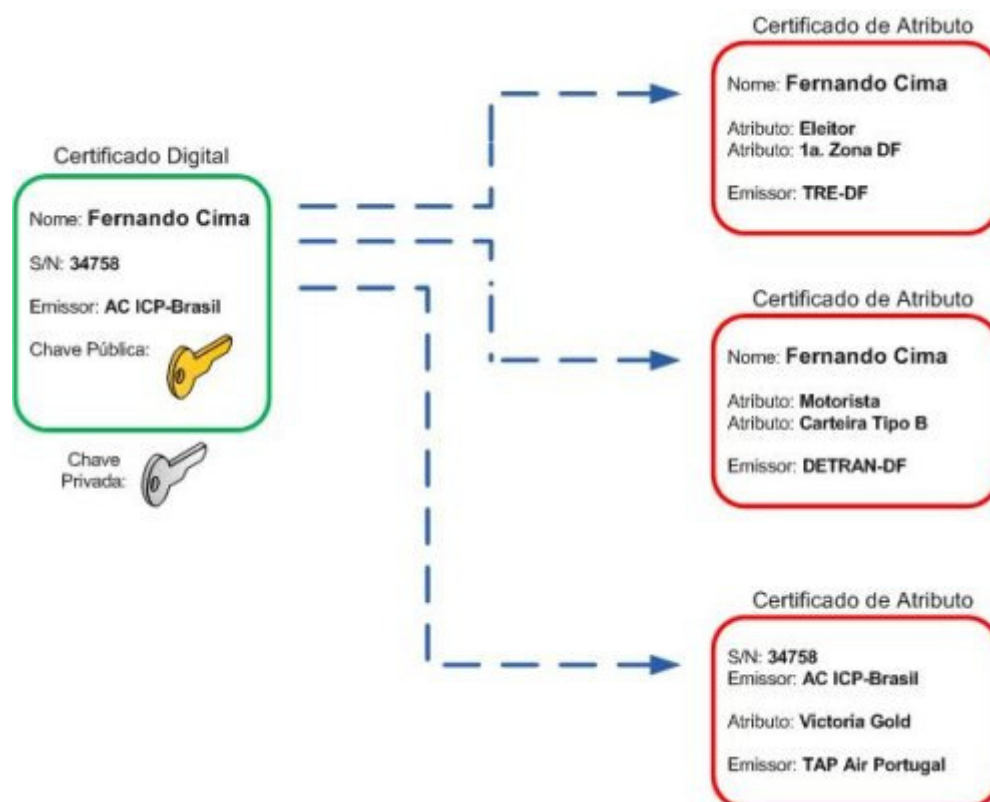
A principal diferença entre um Certificado de Atributo (CA<sub>t</sub>) e um Certificado Digital é que o Certificado de Atributo não estabelece a garantia de autenticidade do proprietário, já que não há uma associação direta entre o certificado e uma chave pública, como no CD.

Isto porque o Certificado de Atributo serve para determinar os atributos vinculados a determinado Certificado Digital, ligado indiretamente a ele (Souza, Cunha *et al.*, 2004).

Como exemplo desta característica, pode-se citar a Figura 2-2<sup>3</sup>, que ilustra um Certificado Digital e apresenta três certificados de atributos vinculados a ele.

---

<sup>3</sup> Imagem obtida em: <http://blogs.technet.com/fcima/archive/2007/07/22/certificados-de-atributos.aspx> Acesso: 30 de março de 2009. Página de concentração de informações de segurança da informação mantida pela equipe de segurança da Microsoft Brasil.



**Figura 2-2 - Certificado Digital Ligado a Certificados de Atributos**

Em Farrel e Housley (2002) existe um exemplo que define a diferença entre os CD e os CAT. Este exemplo baseia-se na comparação entre um passaporte e um visto de entrada em um país. O passaporte é a representação do Certificado Digital, pois ele identifica a pessoa que possui o documento, possuindo um período de validade muito grande. Já o Certificado de Atributo é a representação de um visto de entrada em um país, vinculado a um passaporte e que possui seu período de validade diferente do passaporte (geralmente menor) (Farrell e Housley, 2002).

Um exemplo desta analogia pode ser visto na Figura 2-3.

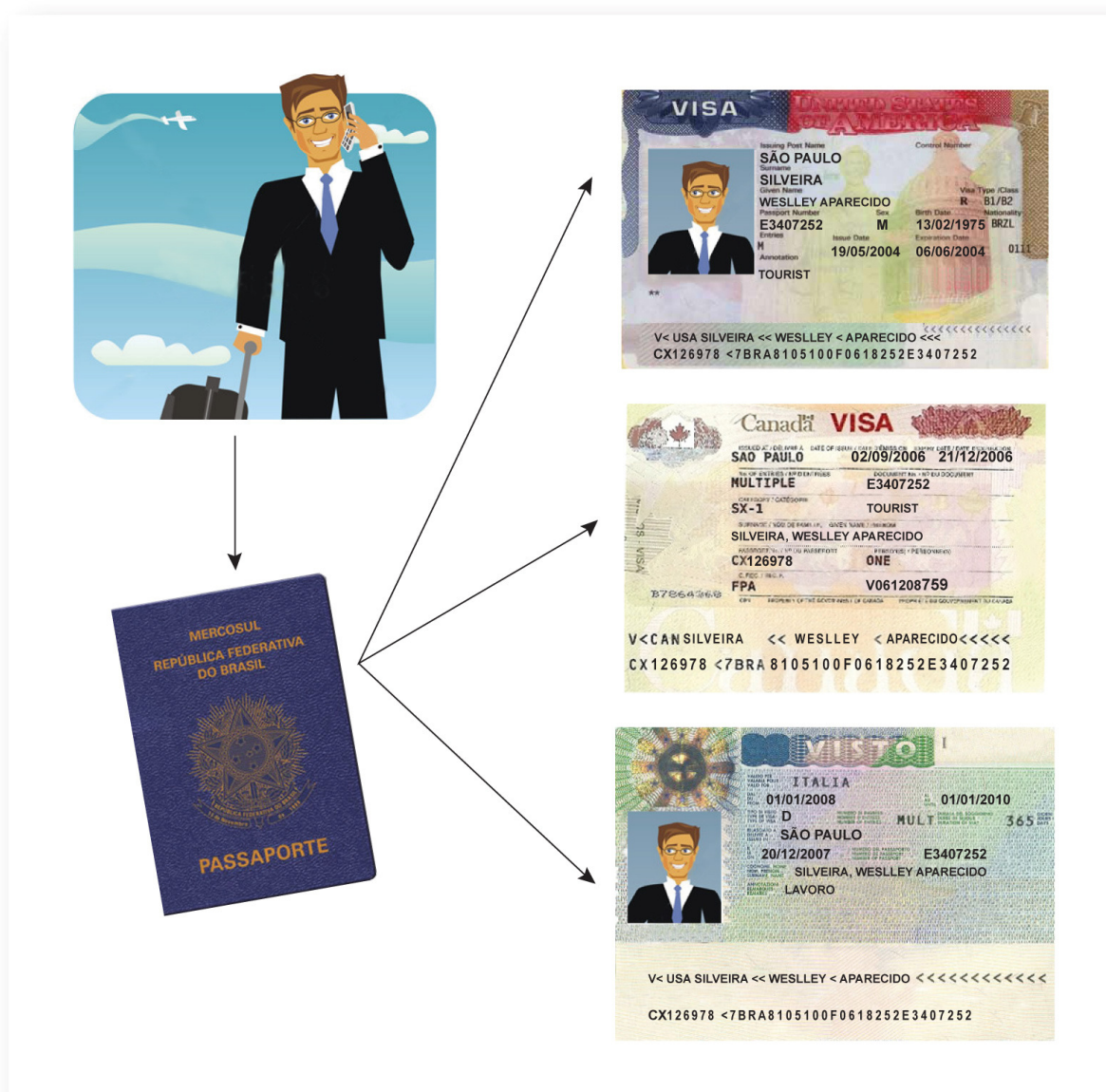


Figura 2-3 - Passaporte e Vistos, analogia com Certificado Digital e Certificado de Atributos

Em **Recommendations series X.509: Information Technology – Open Systems Interconnection - The Directory: Authentication Framework (2001)** está prevista na versão 3 do certificado digital X.509 a presença de campos de extensões do Certificado Digital para uso de atributos assinados dentro do próprio CD. Porém este tipo de utilização é desencorajado devido à constatação de que um Certificado Digital tem, geralmente, validade superior às permissões vinculadas a ele (Farrell e Housley, 2002).

Por exemplo, caso seja emitido um CD com validade de 3 anos para um agente, presente na extensão um atributo que atribui a ele a permissão do papel de



auxiliar administrativo, e depois de um mês ele é transferido de área e passa a ser encaixado no papel de auxiliar técnico, seu certificado digital deveria ser revogado e outro emitido.

Outro ponto importante ao utilizar CAAt ao invés de CD para guardar papéis, é que é desvinculada a necessidade das AC's saberem e estarem capacitadas a atribuir todos os tipos de papéis válidos na hora de assinar o certificado digital. Isto poderia ser inviável. Basta verificar a estrutura da ICP-Brasil, com suas AC de ramos distintos, como a do SERPRO e da Presidência da República, necessitar saber de todos os atributos necessários. Assim, utilizando o outro tipo de certificado para atribuição de papéis, deixamos as AC responsáveis pelo trabalho de identificar univocamente o usuário receptor do certificado, ficando a cargo das AA específicas a atribuição dos papéis (Oppliger, Pernul *et al.*, 2000).

No caso da utilização de Certificado de Atributo isto não ocorreria, pois somente seria necessária a revogação do CAAt de auxiliar administrativo e seria gerado outro com o novo papel.

Assim, utilizando-se os CAAt como mecanismos de atribuição de papéis, consegue-se flexibilizar a atribuição de papéis, já que:

- É possível adicionar e remover papéis sem interferir no CD vinculado ao agente;
- Atribuir prazos de validades diferentes e desvinculados do prazo de validade do CD;
- Não sobrecarregar as AC's com a atribuição de papéis.

Na Tabela 2-1, verificam-se os campos propostos na RCF 3128 (Farrell e Housley, 2002) para os campos do CAAt.

**Tabela 2-1 - Campos do Certificado de Atributos**

<b>Campo</b>	<b>Nome</b>	<b>Descrição</b>
version	Versão	Identifica a versão da especificação do Certificado utilizado
holder	Sujeito	Agente proprietário do

		certificado em questão. Deve estar vinculado ao CD
issuer	Emissor	Nome distinto da AA que emitiu o certificado
signature	Assinatura	Detalhes do algoritmo utilizado na assinatura do certificado
serialNumber	Número Serial	Identificador único do CA
attrCertValidityPeriod	Validade	Indica o período de validade do certificado
attributes	Atributos	Contêm os atributos a serem assinados
issuerUniqueID	Identificador do emissor	Identificador único do emissor
extensions	Extensões	Utilizado para estender o certificado com novas funcionalidades

Na Figura 2-4, adaptada de Souza, Cunha *et al.* (2004), verifica-se o vínculo possível entre um CD e um CA.

Assim, para a utilização efetiva de CD e CA é necessário que seja feito um vínculo único entre eles. Este vínculo será realizado entre o Número Serial do Certificado Digital em conjunto com o Nome do Emissor.

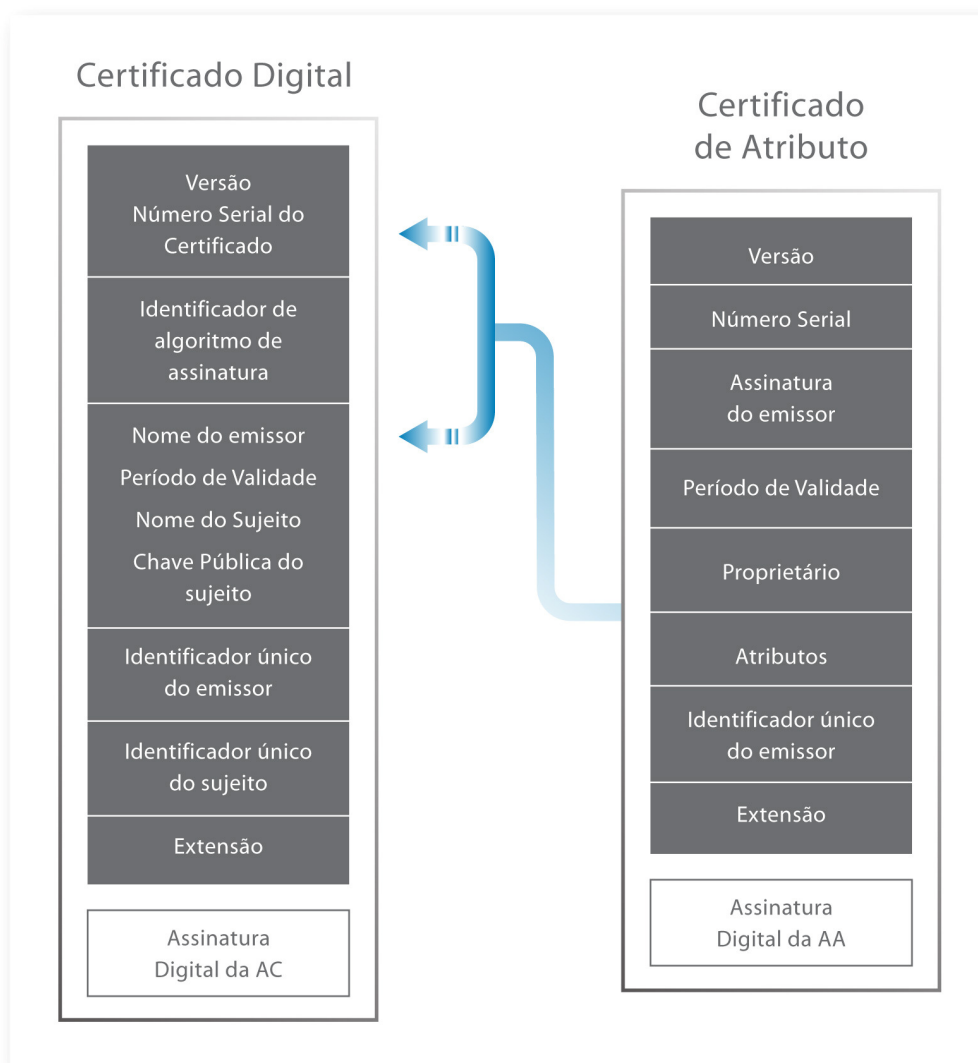


Figura 2-4 - Exemplo de ligação entre Certificado Digital e Certificado de Atributo

### 2.3.2 Políticas de acesso

Um dos aspectos chaves da autorização é a representação das regras e permissões de acesso aos objetos protegidos. Elas representam as condições para permitir, negar ou informar que não há condições baseadas nas políticas existentes de se determinar que uma autorização deve ser concebida.

*eXtensible Access Control Markup Language* (XACML), padronizado pela *Organization for the Advancement of Structured Information Standards* (OASIS) é uma linguagem de uso geral para políticas de controle de acesso usada para descrever tanto decisões de acesso para requisições e respostas, quanto as políticas em si (Anderson, 2005).

XACML foi desenvolvida para suportar abordagens centralizadas e descentralizadas de gerenciamento de políticas (Anderson, 2006), além de poder ser interpretada por máquinas.

A segunda versão desta linguagem, descrita em Anderson (2005), fornece dentre outras melhorias a capacidade de expressão do Controle de Acesso Baseado em Papéis hierárquico que, até então, até então não era possível na versão anterior do padrão. Também trata do uso de atributos arbitrários, da expressão de autorizações negativas, de algoritmos para resolução de conflitos etc. (Kolovski, Hendler *et al.*, 2007).

Na Figura 2-5 é possível visualizar um fragmento de uma política de acesso em XACML, que expressa a permissão de acesso de um determinado papel (*Physician*) a um objeto protegido, cuja identificação possui o valor “ha0zoLeLhQQBr6iYhOuwXAOuelrkq.6sE”.

Devido à grande capacidade de expressão, políticas expressas em XACML podem gerar uma falsa sensação do completo entendimento dos efeitos e consequências das políticas expressas. Ou seja, não se tem a certeza de que aquela política não possuirá uma falha, ou de que em conjunto com outra, permitirá um acesso a determinado recurso que deveria ser negado, não cumprindo com seu papel.

Para solucionar este problema, Kolovski, Hendler *et al.* (2007) descrevem uma maneira de se formalizar as políticas expressas em XACML utilizando Lógica Proposicional e lógicas de Primeira-Ordem, o que possibilita gerar-se provas lógicas de que as políticas realmente cumprem o papel para qual foram determinadas. Com isto, é possível verificar a validade de uma regra antes de armazená-la, alertando ao usuário existência de inconsistências.

No Apêndice A.1 pode-se verificar a política completa exibida na Figura 2-5.

```

<Description>
  A modified policy from the Draft XACML2.0 Conformance Test IIA002 Downloaded from:
  http://www.oasis-open.org/committees/download.php/14846/xacml2.0-ct-v.0.4.zip
</Description>
<Target/>
<Rule RuleId="urn:oasis:names:tc:xacml:2.0:conformance-test:IIA002:rule" Effect="Permit">
<Description>
  A subject with a role attribute of "Physician" can read specific Bart Simpson's CCR record.
</Description>
<Target>
<Subjects>
<Subject>
  <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
      Physician
    </AttributeValue>
    <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:example:attribute:role"
  DataType="http://www.w3.org/2001/XMLSchema#string"/>
  </SubjectMatch>
</Subject>
</Subjects>
<Resources>
<Resource>
  <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
      ha0zoLeLhQQBr6iYh0uwXA0ue1rkq.6sE
    </AttributeValue>
    <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
  DataType="http://www.w3.org/2001/XMLSchema#string"/>
  </ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
  <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
    <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType=
  "http://www.w3.org/2001/XMLSchema#string"/>

```

Figura 2-5 - Fragmento de política de acesso em XACML

## 2.4 Considerações Finais

Neste capítulo foram apresentados de forma concisa os conceitos de Autorização e Autenticação, focando-se na aplicação destes Conceitos ao apresentar os Certificados Digitais, os Certificados de Atributos e a definição de políticas de acesso em XACML.

# Capítulo 3

## REGISTRO ELETRÔNICO EM SAÚDE

---

*Neste capítulo serão apresentados conceitos fundamentais sobre os Registros Eletrônicos em Saúde, bem como aspectos legais que cercam o assunto.*

### 3.1 Registro Eletrônico em Saúde

Publicada em 10 de julho de 2002, a resolução do Conselho Federal de Medicina (CFM) de número 1638 define Prontuário do Paciente (PP) como sendo o documento único constituído de uma série de informações, sinais e imagens registradas, gerados durante o atendimento ao paciente.

Este documento deve ter seu caráter legal, sigiloso e científico, mantido, possibilitando o intercâmbio de informações entre os membros de uma equipe multiprofissional durante a evolução do tratamento do paciente (Resolução Conselho Federal de Medicina n. 1.638/2002a. Define prontuário médico e dá outras providências, 2002).

Assim, um **Registro Eletrônico em Saúde (RES)** ou **Prontuário Eletrônico em Saúde**<sup>4</sup> (PEP) nada mais é que um prontuário de paciente armazenado em meio digital.

---

<sup>4</sup> Prontuário Eletrônico do Paciente (PEP) e Registro Eletrônico em Saúde (RES) são utilizados como sinônimos em todo o trabalho

Uma discussão sobre a classificação e nomenclaturas pode ser vista no trabalho de Peter Waegemann (1996).

O CFM determina regras próprias para a gestão de informações de paciente em meios eletrônicos, aprovados pela Resolução 1639 do mesmo ano (Resolução Conselho Federal de Medicina n. 1.639/2002b. Dispõe sobre as normas técnicas para uso de sistemas informatizados para guarda e manuseio do prontuário médico e dá outras providências, 2002).

Nesta resolução ficam determinados alguns aspectos considerados mandatórios para a gestão de tais informações, como:

- Preocupação com a integridade e com a segurança do sistema;
- Determinação da existência de cópias de segurança periódicas dos dados;
- Preocupação com a privacidade e a confidencialidade dos dados;
- Preocupação em haver mecanismos seguros de autenticação;
- Preocupação em haver mecanismos para auditoria;
- Preocupação em possibilitar a certificação de Sistemas de Registro Eletrônico de Saúde (S-RES).

Assim, seguindo-se as determinações do CFM pode-se estabelecer um Sistema de Registros Eletrônicos em Saúde (S-RES) que atenda as principais características positivas do RES (Marin, Massad *et al.*, 2003), incluindo:

- Acesso remoto e compartilhado: com o manuseio eletrônico do prontuário dos pacientes é possível utilizar ferramentas computacionais para disponibilizar os dados quando e onde forem necessários. Isso ocorre diferentemente dos prontuários físicos, que necessitam estar armazenados em locais devidamente localizados e têm seu acesso restrito a quem tiver acesso físico a eles;
- Durabilidade: em teoria um prontuário eletrônico tem sua validade de tempo determinada pelos meios eletrônicos que o armazenam. Diferentemente de um prontuário em papel, que tem sua validade baseada na vida útil do papel em que as informações estão armazenadas, bem como nos cuidados durante o seu armazenamento;

- Organização: sendo organizadas digitalmente as informações do prontuário, facilita-se a localização das informações disponibilizadas, bem como se possibilita a geração de relatórios, com dados atualizados em tempo-real;
- Aquisição automática de dados: com o aumento do número de equipamentos médicos sendo utilizados, o registro automático de informações nos RES dos pacientes é uma realidade;
- Eliminação de ambiguidade: como as informações necessitam de um dispositivo de entrada preciso para fornecer dados ao sistema, evitam-se problemas de interpretação devido à escrita dos usuários.

Porém, o RES também apresenta desvantagens, como as apresentadas por Wechsler, Anção *et al.* (2003) :

- Necessidade de investimentos em Software e Hardware;
- Necessidade de investimentos em Treinamento;
- Elevado custo de investimento em segurança dos dados;
- Problemas na relação entre médico e paciente durante o uso do sistema.

Conclui-se que, apesar das desvantagens do RES, as vantagens se sobressaem e o investimento neste tipo de tecnologia tem certamente seu retorno garantido.

Para se ter uma ideia deste encaminhamento, o próprio CFM, através da resolução 1821 de 2007, permite a substituição por completo dos documentos em papéis por prontuários eletrônicos assinados com Certificados Digitais padrão ICP-Brasil (Resolução Conselho Federal de Medicina n. 1.821/2007. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde, 2007).



## 3.2 Modelo de Referência

Não há na área de saúde um consenso sobre as informações que devem estar contidas em um prontuário do paciente.

O CFM, através da resolução 1638/2002 (Resolução Conselho Federal de Medicina n. 1.638/2002a. Define prontuário médico e dá outras providências, 2002) em seu artigo quinto, define alguns campos considerados obrigatórios nos prontuários, independentemente da forma:

1. Identificação do paciente – nome completo, data de nascimento (dia, mês e ano com quatro dígitos), sexo, nome da mãe, naturalidade (indicando o município e o estado de nascimento), endereço completo (nome da via pública, número, complemento, bairro/distrito, município, estado e CEP);
2. Anamnese, exame físico, exames complementares solicitados e seus respectivos resultados, hipóteses diagnósticas, diagnóstico definitivo e tratamento efetuado;
3. Evolução diária do paciente, com data e hora, discriminação de todos os procedimentos aos quais o mesmo foi submetido e identificação dos profissionais que os realizaram, assinados eletronicamente quando elaborados e/ou armazenados em meio eletrônico;
4. Nos prontuários em suporte de papel é obrigatória a legibilidade da letra do profissional que atendeu o paciente, bem como a identificação dos profissionais prestadores do atendimento. São também obrigatórios a assinatura e o respectivo número do Conselho regional de Medicina (CRM);
5. Nos casos emergenciais nos quais seja impossível a coleta da história clínica do paciente, deverá constar relato médico completo de todos os procedimentos realizados e que tenham possibilitado o diagnóstico e/ou a remoção para outra unidade.

Durante uma das oficinas da Rede Interagencial de Informações para a Saúde no Brasil (RIPSA), foi elaborado um relatório que recomendou a criação de uma comissão permanente de padronização da informação em saúde, sob a

coordenação do ministério da Saúde (Conjunto Essencial de Informações do Prontuário para Integração da Informação em Saúde, 1999).

Assim, foi criado o Comitê Temático Interdisciplinar “Padronização de Registros Clínicos” (PRC), que se reuniu em março de 1998.

As recomendações deste comitê, juntamente com outras atividades de padronização conduzidas no âmbito da RIPSA, culminaram com a portaria GM 3947/98, que determina, no inciso II do artigo 6º, o prazo de 31 de dezembro de 1999 para o estabelecimento de padrões universais para registros clínicos nos serviços de saúde.

Um dos documentos produzidos pelo grupo foi o Conjunto Essencial de Informações do Prontuário para Integração da Informação em Saúde (Conjunto Essencial de Informações do Prontuário para Integração da Informação em Saúde, 1999), onde estão previstas as informações consideradas essenciais, definidas por uma equipe de renome na área.

O documento agrupa estas informações em áreas, para facilitar a apresentação, sendo elas:

- Dados Administrativos Demográficos: contendo as informações como, Nome do paciente, data de nascimento, sexo, escolaridade, etc;
- Dados Administrativos do Prestador da Assistência e da Fonte Pagadora: contendo os dados da entidade que está prestando assistência ao paciente. Nele devem estar presentes dados como o Nome Completo e CNPJ da Instituição Prestadora da Assistência;
- Dados Clínicos Relevantes;
- Alergias e/ou Reações Adversas: contendo informações como, tabela de diagnóstico utilizada e a respectiva codificação do diagnóstico da alergia;
- Doenças Crônicas Pré-Existentes: contendo informações como, tabela de diagnóstico utilizada e a respectiva codificação do diagnóstico;
- Dados do Evento ou Atendimento Realizado: contendo informações como, tipo do evento, nome do profissional responsável pelo atendimento, data, hora, etc;

- Óbito: caso o evento seja óbito, deve-se informar, dentre outros campos, a data e hora do ocorrido, bem como a causa imediata do óbito;
- Diagnósticos: dentre outras informações, deve-se informar o código do diagnóstico;
- Procedimentos Realizados ou Associados ao Evento: para o registro de eventos mais relevantes, como procedimentos cirúrgicos, exames de alto custo, quimioterapia, hemodiálise e imunizações;
- Exames Realizados: com informações do instante de realização do exame, bem como o resultado.

Mesmo com estas recomendações, os prontuários dos pacientes podem variar de local para local, adicionando informações mais relevantes a seu tipo de atendimento, bem como adicionando informações mais detalhadas para contabilidade, etc.

### 3.3 Continuity of Care Record

Um modelo de armazenamento e estruturação de dados da área de saúde é o *Continuity of Care Record (Atsm)*.

Este modelo, utiliza o *eXtensible Markup Language (XML)* e é definido pelo padrão *ASTM E2369 - 05e1 Standard Specification for Continuity of Care Record (CCR)* definido pelo *American Society for Testing and Materials (ATSM) (Atsm)*.

O CCR contempla as informações mais relevantes administrativamente, demograficamente e fatos clínicos sobre o tratamento do paciente.

A Figura 3-1 expressa fragmento de um CCR utilizado pelo Google Health (Google Health Data API CCR Reference, 2009) para armazenamento de informações de saúde.

O serviço Google Health utiliza um subconjunto de campos definido da especificação CCR, chamado *Google Health UI* (Google Health Data API CCR Reference, 2009). Isto não significa que a sua plataforma descarte outros campos

presentes na especificação oficial e que não fazem parte do seu subconjunto. Ao contrário, esta plataforma aceita, armazena e envia quando solicitado o CCR tal qual fora submetido.

Porém, os campos adicionais que não pertencem ao subconjunto *Google Health UI* são ignorados durante o processamento na plataforma do Google Health e não podem ser visualizados pela página da Internet disponibilizada pela empresa para acesso às informações armazenadas.

Esta característica permite que seja utilizado o sistema do Google Health para armazenagem de informações importantes para outros sistemas de Registros Eletrônicos de Saúde, como assinaturas digitais do conteúdo, sem afetar o funcionamento da plataforma em si.

```
<ContinuityOfCareRecord xmlns='urn:astm-org:CCR' >
  <CCRDocumentObjectID>ha0zoLeLhQQBr6iYh0urXA0ue1rkq.6sE</CCRDocumentObjectID>
  <Language> (...) </Language>
  <Version>V1.0</Version>
  (...)
  <From> (...) </From>
  <Body>
    <Results>
      <Result>
        <CCRDataObjectID>0ue1rkq.6sE-1</CCRDataObjectID>
        <Source>
          <Actor>
            <ActorID>bartsimpson@gmail.com</ActorID><ActorRole><Text>Patient</Text></ActorRole>
          </Actor>
        </Source>
        <Test>
          <CCRDataObjectID>0ue1rkq.6sE-0</CCRDataObjectID>
          <DateTime>
            <Type><Text>Collection start date</Text></Type><ExactDateTime>2009-10-20</ExactDateTime>
          </DateTime>
          <Description><Text>Blood Pressure</Text>
          <Code><Value>36.1870</Value>
            <CodingSystem>Google</CodingSystem>
          </Code>
        </Description>
        <Source> (...) </Source>
        <TestResult><Value>12/7</Value>
        <ResultSequencePosition>0</ResultSequencePosition>
      </TestResult>
    </Results>
  </Body>
  (...)
</ContinuityOfCareRecord>
```

Figura 3-1 - Fragmento de um CCR armazenado no Google Health

A representação completa do CCR representado pela Figura 3-1 pode ser visualizada no Apêndice A.2.

### **3.4 Considerações Finais**

Neste capítulo foram apresentados os aspectos principais dos Registros Eletrônicos em Saúde, bem como os esforços em se determinar um modelo padrão para as informações nele contidas. Por fim, apresentou-se o modelo CCR utilizado pelo Google Health para armazenamento de informações médicas.

# Capítulo 4

## CERTIFICAÇÃO PARA SISTEMAS DE REGISTRO ELETRÔNICO EM SAÚDE

---

---

*Neste capítulo são apresentados os conceitos e definições presentes no Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, além do conceito de Delegação de poder.*

### **4.1 Manual de Certificação para Sistemas de Registro Eletrônico em Saúde**

O Conselho Federal de Medicina publicou em sua resolução 1639 (Resolução Conselho Federal de Medicina n. 1.639/2002b. Dispõe sobre as normas técnicas para uso de sistemas informatizados para guarda e manuseio do prontuário médico e dá outras providências, 2002), informações que citam um convênio com a Sociedade Brasileira de Informática em Saúde (SBIS) para emitir certificados para sistemas que armazenam informações de paciente de acordo com as normas regentes.

Fruto deste convênio foi criado o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, que visa definir quais são os critérios levados em conta pela equipe de auditores para certificar um sistema de Registro Eletrônico de Saúde (RES) (Leão, Costa *et al.*, 2008).

Este manual de certificação está baseado em diversos padrões mundiais sobre o assunto (Leão, Costa *et al.*, 2008), como:

- ISO 27.799: Norma internacional de segurança da informação em Saúde;
- ISO/TR 20.514:2005: Norma internacional que estabelece as definições de RES e de Sistemas de RES. Descreve as principais categorias de sistemas, define cenários de utilização, e a necessidade de interoperabilidade semântica entre os diferentes S-RES;
- ISO/TS 18.308:2004: define os requisitos para um S-RES. A norma apresenta os requisitos categorizados em estrutura, processo, comunicação, privacidade e segurança, médico-legal, ético, consumidor/cultural e também os requisitos relacionados à evolução de sistemas de RES;
- ISO/DIS 27.799: *Health informatics - "Information security management in health using ISO/IEC 17.799"*. Destaca a importância do emprego dos controles de segurança descritos na ISO/IEC 27.002 com foco na área de saúde;
- ISO/IEC JTC1/SC27: definiram a norma ISO/IEC 27.002:2005 *"Information technology - Security techniques - Code of practice for information security management"*, anteriormente ISO/IEC 17.799. É a norma mais difundida mundialmente no assunto segurança e apresenta os principais controles de segurança a serem empregados por qualquer instituição com o objetivo de proteger suas informações. Tem sua versão brasileira, a norma NBR ISO/IEC 27.002:2005 "Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação";
- ISO/IEC 15.408:2005: *"Information technology -- Security techniques - Evaluation criteria for IT security"*, que estabelece critérios e requisitos para certificação de segurança de sistemas;
- *ANSI HL7 Functional Model* (EHR-S FM): HL7 é o mais utilizado padrão para intercâmbio de dados na área da saúde no cenário internacional.

Basicamente, o processo de certificação faz diferença entre dois grandes grupos, os que usam os Certificados Digitais ICP-Brasil e os que não usam. Os que

utilizam mecanismos de segurança para acesso e certificação das informações com Certificados Digitais, são certificados com Nível de Garantia de Segurança (NGS) 2, os demais, com NGS 1.

Aqueles que procuram certificação com NGS 2 possuem respaldo legal para a eliminação dos prontuários em papéis, como garantido pela resolução 1639, desde que sejam utilizados no processo os referidos certificados digitais ICP-Brasil.

Além desta distinção, estão presentes no documento os requisitos utilizados durante o processo de homologação, utilizados como referências para proceder as homologações.

Estes requisitos são apresentados e classificados segundo os seguintes critérios:

- Mandatórios: indicados pela letra M. Os requisitos que possuem esta classificação devem estar presentes no RES, sob a pena de este não receber a certificação;
- Recomendados: indicados pela letra R. Os requisitos enquadrados nesta classificação podem ou não estar presentes no atual sistema. Por outro lado, são considerados recomendados porque serão considerados Mandatórios em versões futuras do documento de certificação;
- Opcionais: indicados pela letra O. São os requisitos considerados opcionais e acessórios ao processo de certificação. Sua presença/ausência não interfere no processo de homologação.

## 4.2 A delegação de poderes

Um dos pontos a ser citado sobre o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (Leão, Costa *et al.*, 2008) é o requisito de número NSG1.04.07 chamado “Delegação de poder”.

Como exemplo de delegação, pode-se citar um médico que delega o poder de entrada de informação ao RES de um paciente para uma enfermeira.

Em (Leão, Costa *et al.*, 2008), define-se como **atribuidor** aquele responsável por autorizar a delegação de poder e **delegado** aquele que recebe a delegação de poder. Assim:



- O atribuidor deve ser previamente autorizado para conceder tais classes de autorização;
- A delegação de poder deve ser registrada no sistema;
- A delegação de poder deve informar:
  - O atribuidor;
  - O delegado;
  - O motivo;
  - O instante da concessão;
  - O período de vigência.

Em suma, este requisito visa permitir que um agente do sistema possa delegar a outro agente partes ou todas as suas permissões de acesso a determinado objeto (Zhang, Ahn *et al.*, 2002).

Um exemplo deste tipo de interação pode ser visto na Figura 4-1, retirada de Zhang, Ahn *et al.*(2002). Nela pode-se verificar que as permissões de acesso do paciente Jennifer estão vinculadas a dois médicos, o Dr. Chen e a Dra. Jain. Neste caso, o Dr. Chen, em algum momento necessitou da opinião de um especialista, o Dr. White, sobre a paciente Jennifer. Para tanto, o Dr. Chen pode delegar a permissão de acesso aos dados da Jennifer com o Dr. Whyte e assim ele pode participar do caso, sem, no entanto, ter todas as permissões de ambos os médicos que cuidam da paciente.

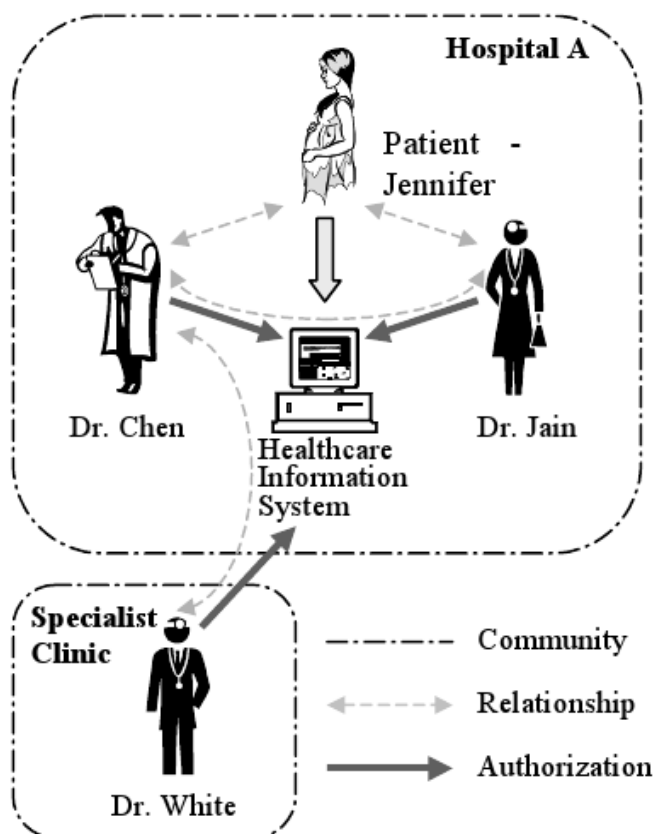


Figura 4-1 - Exemplo de Delegação (Zhang, Ahn *et al.*, 2002)

Outro exemplo de delegação possível é a delegação de um Médico a um sistema automatizado de captação de dados para a inserção das leituras no prontuário do paciente monitorado no momento.

A atenção a este requisito é um dos pontos principais deste trabalho, que consiste em fornecer uma estrutura capaz de permitir a delegação de poder de maneira mais eficaz e segura.

### 4.3 Considerações Finais

Neste capítulo foi apresentado o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, documento base que contém os requisitos de segurança e funcionalidade para certificar que determinado software seja compatível com o nível de segurança a que se propõem.

Dentre estes requisitos existe o da Delegação de Poder, destacada neste texto.

# Capítulo 5

## WEB SERVICES

---

*Neste capítulo serão apresentados alguns conceitos fundamentais da tecnologia de Web services, bem como de aspectos de segurança relacionado.*

### 5.1 Introdução

Web services foram criados para fornecer um arcabouço sistemático e extensível para a interação entre aplicações, criadas sobre os protocolos Web existentes e nos padrões XML abertos (Bosworth, 2001) (Curbera, Duftler *et al.*, 2002).

Esta tecnologia oferece uma interface independente de plataforma e de mecanismos de comunicações, possuindo uma vasta infraestrutura de suporte em termos de servidores e ambientes de desenvolvimento.

Web services são utilizados de maneira crescente em Registros Eletrônicos de Saúde (RES)(Mykkänen, Riekkinen *et al.*, 2007).

Utilizando-se a tecnologia de Web services do Google Health, por exemplo, é possível resolver grande parte dos desafios da área de gerenciamento de registros eletrônicos de saúde, já que a empresa possui grande conhecimento em armazenagem e redundância de dados e a tecnologia de acesso oferecida é suportada por uma multiplicidade de plataformas.

Como resumiu Curbera, Duftler *et al.*, (2002), a tecnologia Web services está baseada em três pilares: protocolos de comunicação, descritores de serviços e descoberta de serviços.

Algumas características desses pilares são:

- *Simple Object Access Protocol* (SOAP) permite a comunicação entre os Web services;
- *Web Services Description Language* (WSDL) permite uma descrição formal dos serviços num formato tal que computadores possam entendê-la; e
- O diretório chamado *Universal Description, Discovery and Integration* (UDDI), que registra as descrições dos Web services.

A utilização desta tecnologia aliada a outros conceitos deu origem à Arquitetura Orientada a Serviços (AOS) ou *Service-oriented Architecture* (SOA) (Papazoglou, 2003).

## 5.2 Segurança em Web services

Segurança em Web services é um assunto amplamente discutido na literatura, sendo que questões como autenticação, confidencialidade, autenticidade no uso desta tecnologia são desafiadoras e fontes de pesquisas contínuas (Power, Politou *et al.*, 2006).

Uma das especificações que tratam das questões de confidencialidade, de integridade e de autenticação em Web Services é a *WS-Security* (Nadalin, Kaler *et al.*, 2004), que permite a descrição de mecanismos de segurança na troca de mensagens entre Web services.

Com relação à segurança dos acessos aos dados armazenados, e o acesso via Web Services, Google Health requer que as requisições efetuadas no ambiente de produção sejam assinadas digitalmente com uma chave privada correspondente a uma chave pública previamente cadastrada em seu sistema (AuthSub for Web Applications, 2009).

A autenticação de clientes pode ser feita através de nomes de usuários e senhas, tokens, certificados X.509, tokens Kerberos entre outros (Power, Politou *et al.*, 2006) nos servidores que fornecem os serviços.

### **5.3 Considerações Finais**

Neste capítulo foram abordados conceitos gerais de Web services, apresentando-se brevemente aspectos de segurança.

# Capítulo 6

## GOOGLE HEALTH

---

*Neste capítulo serão apresentadas as estruturas de funcionamento da plataforma do Google para Registros Eletrônicos em Saúde.*

### 6.1 O Google Health

O Google Health (About Google Health, 2009) é um serviço oferecido gratuitamente aos usuários pela Google que visa ser um ponto de centralização de informações médicas.

O acesso aos dados é feito de duas formas: uma página na Internet, que permite a gestão completa dos dados pelos usuários e um conjunto de bibliotecas de software que permitem a desenvolvedores criarem aplicações para realizar operações sobre estes dados.

Os serviços oferecidos pelo Google Health permitem (About Google Health, 2009):

- Que os registros médicos sejam mantidos atualizados de maneira simples pelos usuários, mesmo após mudanças de empregos, endereços, instituições de tratamentos, etc;
- O compartilhamento seguro destes dados com amigos, parentes ou profissionais de saúde;

- O acesso de qualquer lugar a qualquer hora das informações lá presentes.

Também há a garantia, de acordo com uma política de privacidade<sup>5</sup>, que os dados serão armazenados de maneira segura e que não serão disponibilizados para terceiros. Somente o usuário da informação possui o direito de definir quem terá acesso aos dados.

A interface WWW do sistema (Figura 6-1) possibilita o uso direto pelos usuários e fornece mecanismos para inserir, editar e remover dados do prontuário, como resultado de exames, prescrições médicas etc. Permite também a definição de compartilhamentos dos dados com outros usuários, bem como a visualização de registros simples de auditoria que resumem as atividades realizadas e quem as realizou. Por exemplo, é possível ver quem realizou acesso ao Prontuário, qual a data e hora do acesso, e qual a atividade executada, como leitura, edição e remoção. Porém, não é possível verificar o que especificamente foi feito, como qual registro foi editado, removido ou inserido.

---












<sup>5</sup> Política de Privacidade disponível em: <http://www.google.com/intl/pt-BR/health/privacy.html>



igorh9teste@gmail.com | [New Features](#) | [Take our survey!](#) | [Settings](#) | [Help](#) | [Sign out](#)

**Google health**

[Read about health topics »](#)

igorh9teste	Profile summary 	
<ul style="list-style-type: none"> <li><a href="#">Notices</a></li> <li><a href="#">Drug interactions</a></li> <li>☰ <a href="#">Profile details</a> <ul style="list-style-type: none"> <li><a href="#">Age, sex, height...</a></li> <li><a href="#">Conditions</a></li> <li><a href="#">Medications</a></li> <li><a href="#">Allergies</a></li> <li><a href="#">Procedures</a></li> <li><a href="#">Test results</a></li> <li><a href="#">Immunizations</a></li> <li><a href="#">Insurance</a></li> <li><a href="#">Files and images</a></li> </ul> </li> <li> <a href="#">Add to this profile</a></li> <li> <a href="#">Import medical records</a></li> <li> <a href="#">Explore health services</a></li> <li> <a href="#">Share this profile</a></li> <li> <a href="#">See who has access</a></li> <li> </li> <li><a href="#">Medical contacts</a></li> <li> <a href="#">Find a doctor</a></li> <li> </li> <li>Caring for someone? <a href="#">Add a profile for them</a></li> </ul>	<ul style="list-style-type: none"> <li> <a href="#">Add to this Google Health profile</a> Learn about your health issues and find helpful resources</li> <li> <a href="#">Import medical records</a> Copy and get automatic updates of your records</li> <li> <a href="#">Explore online health services</a> Find online tools for managing your health</li> <li> <a href="#">Find a doctor</a> Search by name, location, and specialty</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">Age, sex, height...</a> 28 years old Male 65.0 kilograms 175 centimeters 21.2 body mass index (BMI)</li> <li><a href="#">Test results</a> Blood Typing, ABO - O-</li> </ul>

©2010 Google - [About Google Health Beta](#) - [For partners](#) - [Google Health privacy policy](#) - [Terms of service](#) - [Google home](#)

**Figura 6-1 - Registro de tela do ambiente de produção Google Health**

Outra limitação do serviço fornecido são as permissões de acesso. O sistema só permite que os compartilhamentos sejam feitos através de autorizações de leitura, ou de leitura e escrita. Estas autorizações não podem ser definidas para cada objeto, mas apenas para o prontuário inteiro. Em suma, ao permitir a visualização de dados, permite-se que todo e qualquer dado seja visualizado pela entidade autorizada.

Assim, caso um paciente em um procedimento tenha realizado algum exame considerado “confidencial”, por padrão o sistema tem permissão para acessar o prontuário completo, verificando não só a realização do exame, mas também o resultado dele. Não há mecanismos para que o paciente possa permitir ou negar o acesso ao exame realizado, bem como ao resultado.

## 6.2 Google Health API

O acesso aos dados armazenados na plataforma do Google Health é feito através chamadas de funções de bibliotecas fornecidas pela própria empresa.

Porém, para acessar estes dados é necessária a obtenção de **tokens** de acesso. Para a obtenção destes tokens é necessário utilizar um de três métodos de autenticação: *OAuth*, *AuthSub* ou usuário e senha.

O modelo de autorização *OAuth* (OAuth for Web Applications, 2009) está exposto na Figura 6-2:

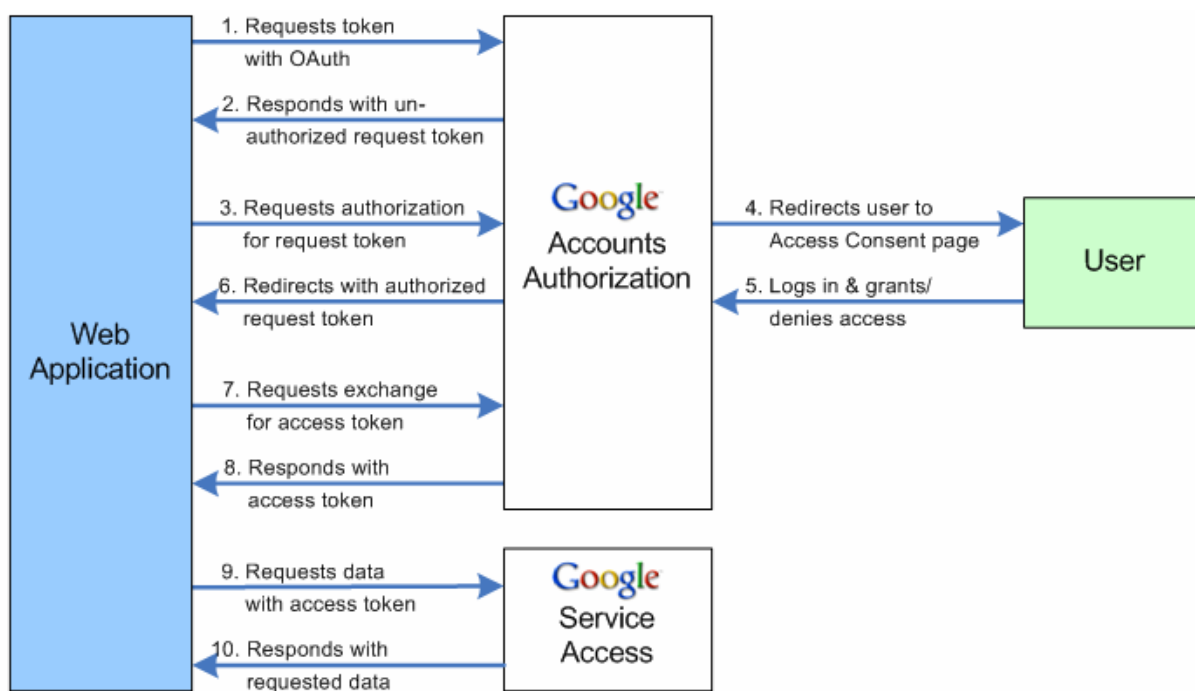


Figura 6-2 - Modelo de autorização OAuth (OAuth for Web Applications, 2009)

O funcionamento deste método está baseado na requisição de um **token** de autorização. De posse dele é possível solicitar ao serviço que o **token** fornecido seja autorizado. Caso o usuário permita a operação, ou seja, permita que o Google forneça acesso aos serviços com a conta do usuário, isso será respondido com um token de autorização.

Com este **token**, é possível realizar uma solicitação de outro tipo, que tem permissão de acesso aos dados, que então permite o acesso aos serviços.

Há uma necessidade destes passos, pois este processo permite que sejam desenvolvidas aplicações com sistema de autenticação federativos, bem como integração com outras formas de autenticação, como *OpenID* (OAuth for Web Applications, 2009), Recordon e Reed, 2006), não abordadas nesta proposta.

Já o modelo de autorização *AuthSub* (AuthSub for Web Applications, 2009), visualizado na Figura 6-3, possui seu funcionamento simplificado. Basicamente, ao solicitar o **token** de acesso o cliente já é redirecionado à página de autorização, semelhante ao *OAuth*. Assim que o cliente autorizar/negar o acesso, um **token** é fornecido e então a aplicação pode realizar solicitações aos serviços.

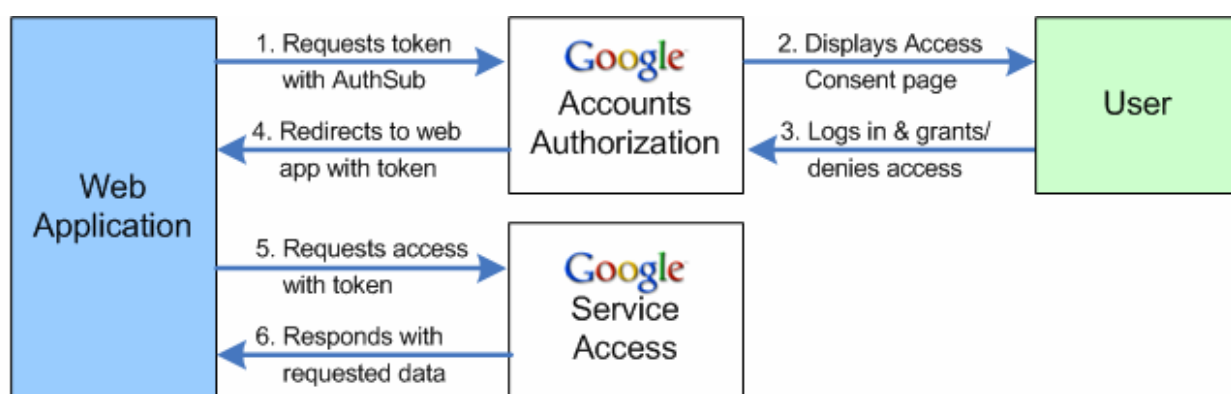


Figura 6-3 - Modelo de autorização AuthSub (AuthSub for Web Applications, 2009)

Os mecanismos de autenticação e autorização *OAuth* e *AuthSub* detalhados permitem que sistemas de terceiros não precisem lidar com os dados da conta do usuário, como nome de usuário e senha, deixando a cargo do Google esta gestão, sendo indicados para aplicativos com interface Web.

**Tokens** obtidos ficam ativos até que sejam revogados ou tenham seu período de expiração atingido.

Além de fornecer as bibliotecas para acesso aos serviços fornecidos pela empresa, Google também disponibiliza um ambiente de testes completo para desenvolvimento e integração de sistemas com a plataforma do Google Health.

Este ambiente, chamado de **H9 Sandbox**, é uma cópia real e completa do sistema oficial Google Health (produção). Neste ambiente, porém, os dados nele armazenados não são compartilhados com o sistema de produção, possuindo funcionamento independente.

**H9** permite a simulação de todas as funcionalidades de Google Health, além de possibilitar que algumas questões de segurança consideradas obrigatórias no ambiente de produção sejam utilizadas opcionalmente neste ambiente, como a assinatura digital de todas as requisições e a utilização de **tokens** seguros. Somente através deste ambiente é possível a utilização de endereços de desenvolvimento (localhost) nas requisições (The H9 Developer's Sandbox, 2009).

Qualquer usuário pode obter uma conta no Google Health de produção através do endereço <http://www.google.com/health> e no ambiente de desenvolvimento H9 através do endereço: <http://www.google.com/h9>.

Na Figura 6-4 é possível visualizar a interface Web de gestão de informações do H9. Observa-se que a única diferença entre esta interface e a de produção (Figura 6-1) é uma inscrição em vermelho, alertando que este é um ambiente de desenvolvimento.

igorh9teste@gmail.com | [Take our survey!](#) | [Settings](#) | [Help](#) | [Sign out](#)

**H9 development sandbox**  
-- for developer testing only.

[Read about health topics >](#)

---

**igorh9teste** **Profile summary** [Print](#)

[Notices](#)

[Drug interactions](#)

[Profile details](#)

[Age, sex, height...](#)

[Conditions](#)

[Medications](#)

[Allergies](#)

[Procedures](#)

[Test results](#)

[Immunizations](#)

[Insurance](#)

[Files and images](#)

[Add to this profile](#)

[Import medical records](#)

[Explore health services](#)


[Share this profile](#)


[See who has access](#)


[Medical contacts](#)


[Find a doctor](#)


Caring for someone?  
[Add a profile for them](#)

 **Add to this Google Health profile**  
Learn about your health issues and find helpful resources

 **Import medical records**  
Copy and get automatic updates of your records

 **Explore online health services**  
Find online tools for managing your health

 **Find a doctor**  
Search by name, location, and specialty

 **localhost**

[Age, sex, height...](#)  
14 years old  
Male  
55.1 kilograms  
172 centimeters  
18.6 body mass index (BMI)

[Allergies](#)  
Abacavir - Severe

[Procedures](#)  
Blood Transfusion

[Test results](#)  
Blood Pressure - 12/7  
Blood Typing, ABO - O-  
Blood Typing, Rh (D) - +  
Thyroid Stimulating Hormone (TSH) - 5.14 def

©2010 Google - [About Google Health Beta](#) - [For partners](#) - [Google Health privacy policy](#) - [Terms of service](#) - [Google home](#)

**Figura 6-4 - Registro de tela do ambiente H9**

## 6.3 Considerações Finais

Neste capítulo foi apresentado o Google Health, serviço de centralização de informações médicas mantido pela Google. Apresentaram-se também os métodos de autenticação para acesso aos dados lá armazenados, bem como o ambiente de desenvolvimento disponibilizado.

# Capítulo 7

## INFRAESTRUTURA DE GERENCIAMENTO DE PRIVILÉGIOS

---

*Neste capítulo são apresentados conceitos básicos de uma Infraestrutura de Gerenciamento de Privilégios.*

### 7.1 Infraestrutura de Gerenciamento de Privilégios

Uma Infraestrutura de Gerenciamento de Privilégios (IGP) ou em inglês *Privilege Management Infrastructure* (PMI) é um sistema capaz de fornecer o gerenciamento de privilégios para sistemas que necessitem prover controles de acessos a dados importantes, bem como fornecer mecanismos de delegação de acesso a estes objetos protegidos.

A discussão e definição deste tipo de estrutura com a utilização de certificados de atributos foi feita pela introdução de uma emenda sugerida em 1998 ao padrão ISO/IEC 9594-8. Este tipo de sugestão de melhoria do documento é chamado em inglês *Proposed Draft Amendment* (PDAM) (Linn e Nyström, 1999).

Segundo este PDAM, um modelo de PMI baseado em Certificados de Atributos pode ser dividido em três partes:

- Um modelo geral de gerenciamento de privilégios;
- Um modelo de controle;

- Um modelo de Delegação.

O **modelo de gerenciamento** de privilégios é aquele que define o modelo geral de controle de acesso aos objetos protegidos, ou seja, ele expressa uma visão ampla dos mecanismos e processos necessários para que o controle de acesso aos objetos seja efetuado.

Este modelo define três macroentidades:

- O objeto requisitado;
- Quem solicita o objeto, ou o agente solicitante;
- O verificador.

Cada objeto possui seus métodos característicos, como métodos de leitura e gravação que são acessíveis pelos agentes.

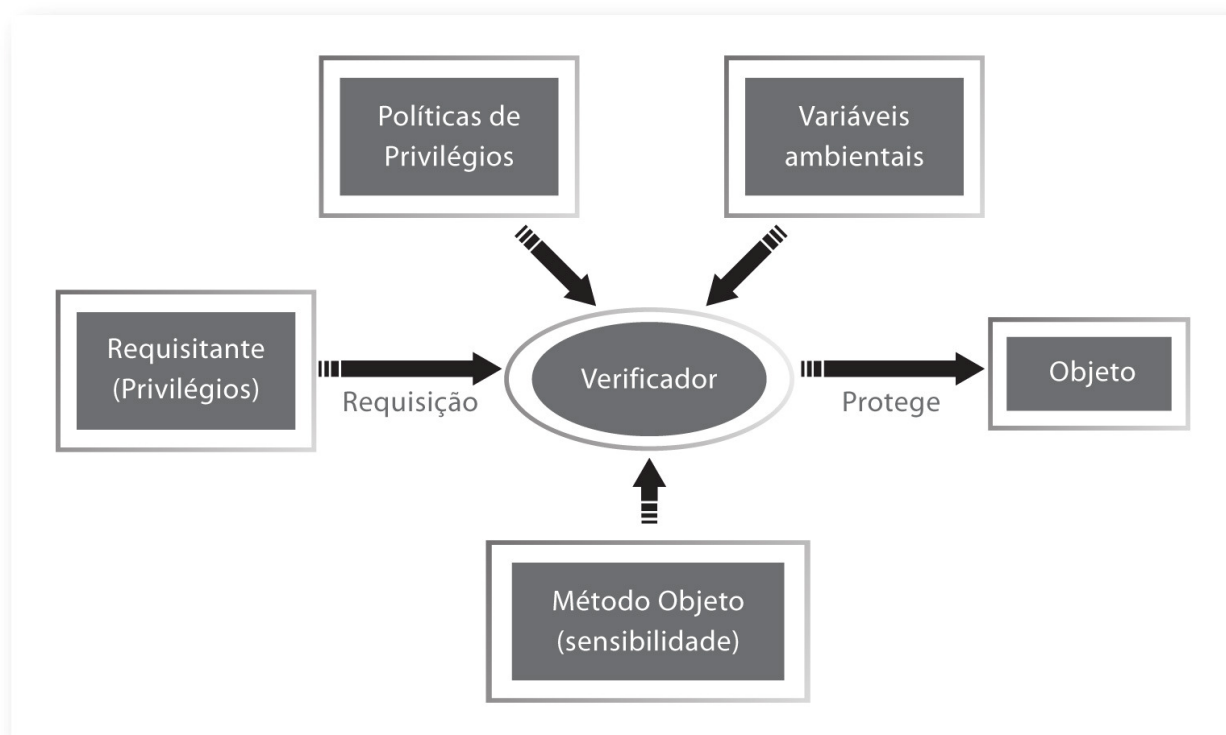
Assim, a validação do acesso ou a permissão de uso do objeto protegido requisitado dependerá da análise de uma série de fatores definidas pelo modelo, como:

- Método requisitado e operação;
- Privilégios do agente que requisita a operação;
- Políticas de privilégios em operação;
- Variáveis que podem influenciar a decisão, como data e hora da requisição, etc.

Já o **modelo de controle** é aquele que define como o controle será exercido através dos métodos sensíveis dos objetos. Este modelo define cinco componentes:

- O solicitante;
- O verificador;
- O método do objeto;
- A política de privilégios;
- As variáveis do ambiente.

A relação entre estes componentes pode ser vista na Figura 7-1, adaptada de Linn e Nyström (1999).



**Figura 7-1 - Modelo Geral de Controle**

Na Figura 7-1, observa-se que para o verificador decidir se o agente requisitante tem ou não permissão de acessar o objeto protegido ele deve observar diversos pontos, como as políticas de privilégios, as variáveis de ambientes, por exemplo, o dia ou hora de acesso e as permissões de acesso.

O **Modelo de Delegação** ilustra como a delegação de privilégios deve ser efetuada.

Este modelo define três componentes:

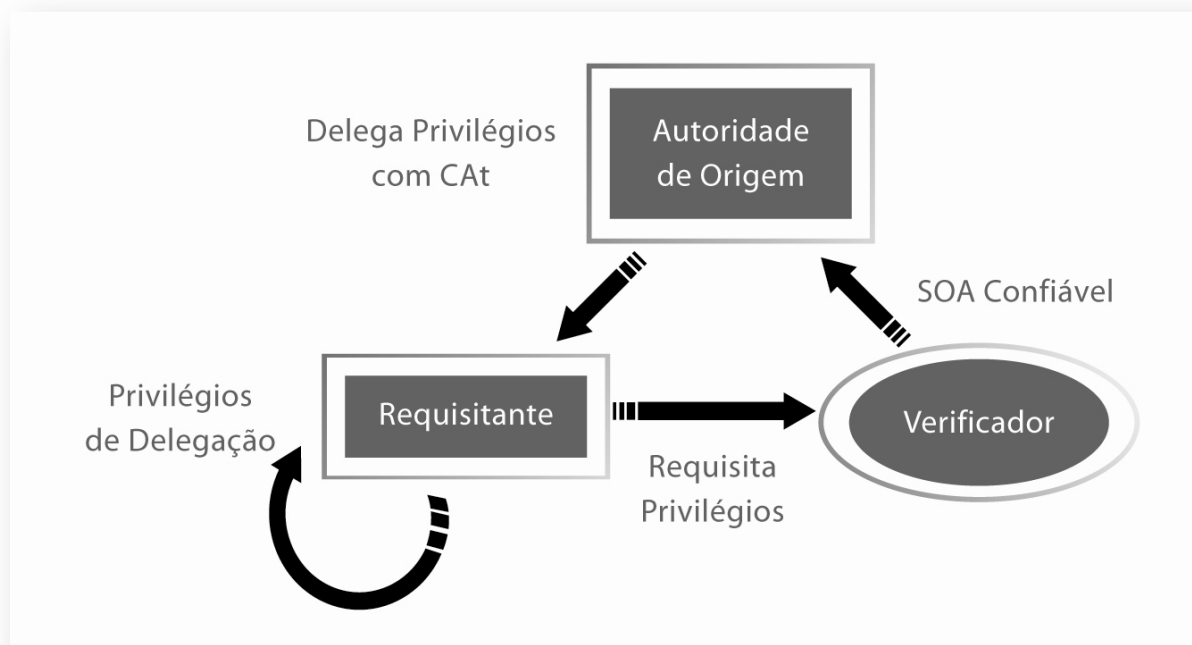
- O verificador;
- A Origem de Autorização (OA) ou *Source of Authority* (SOA), em inglês;
- O solicitante.

A base de funcionamento deste modelo reside no fato de que a Origem de Autorização possua todos os privilégios possíveis para todos os objetos sob sua jurisdição e ela fique responsável por delegar as permissões de acessos através da emissão de Certificados de Atributos aos solicitantes.



Cabe ao verificador checar se todos os solicitantes na cadeia de delegação possuem privilégios suficientes para delegar ou acessar o objeto.

A relação entre estes componentes pode ser visualizada na Figura 7-2, adaptada de Linn e Nyström (1999).



**Figura 7-2 - Modelo de Delegação**

Assim, o modelo de delegação começa com a solicitação de delegação de acesso a um objeto feito por um agente solicitante ao verificador.

Caso este agente tenha permissão para efetuar tal delegação, solicita-se à OA um Certificado de Atributo que indica que esta delegação é válida, ou seja, emite-se um certificado ao solicitante que dá as permissões solicitadas.

Este certificado, ao ser emitido, é enviado para o solicitante, que poderá fazer uso dele para acessar o objeto, utilizando-se do modelo de controle.

## 7.2 Considerações Finais

Neste capítulo foram apresentados os conceitos básicos de uma Infraestrutura de Gerenciamento de Privilégios, seu funcionamento e estrutura de delegação.

# Capítulo 8

## TRABALHOS RELACIONADOS

---

*Neste capítulo são apresentados trabalhos relacionados que contemplam o desenvolvimento e a manutenção de uma Infraestrutura de Gerenciamento de Privilégios para ambientes da área de saúde.*

### 8.1 Introdução

A seguir estão relacionados alguns modelos de Infraestruturas de Gerenciamento de Privilégios selecionados com base em uma catalogação prévia que procurou identificar aqueles que tivessem utilização em ambiente da área de saúde, implementassem processos de delegação ou se destacassem em algum aspecto relacionado aos itens analisados.

Os modelos identificados foram analisados segundo alguns aspectos:

- Tipo de Organização dos Agentes: verificar como é feito o agrupamento dos usuários, dos computadores ou sistemas que executam as operações a fim de gerenciar os privilégios de tal execução;
- Mecanismo de autenticação: verificar os modelos de autenticação utilizados;
- Mecanismos de autorização: verificar os modelos e mecanismos de autorizações utilizados;
- Hierarquia de papéis: verificar se existem e como funcionam os mecanismos de hierarquia de papéis;

- Aplicação na área médica: verificar a utilização destes mecanismos em sistemas da área médica;
- Outros aspectos: verificar outros detalhes relevantes das estruturas.

## 8.2 MACA: Middleware para Autorização e Controle de Acesso

Segundo Motta e Furuie (2002), MACA (*Middleware para Autorização e Controle de Acesso*) é uma ferramenta que implementa um modelo de autorização contextual para o Controle de Acesso Baseado em Papéis (CABP). Para tanto, MACA organiza os agentes em papéis e também suporta a hierarquia de papéis, em que um papel pode possuir papéis derivados.

Assim, ao alocar um agente a determinado papel filho, ele herda automaticamente os privilégios do papel pai.

Um exemplo desta hierarquia pode ser visto na Figura 8-1.

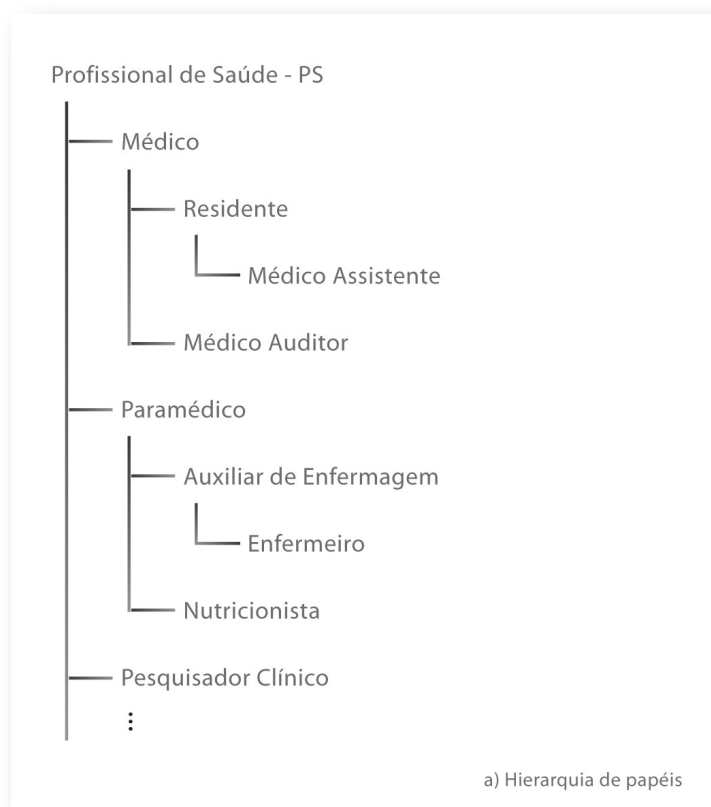


Figura 8-1 - Hierarquia de papéis (Motta e Furuie, 2002)

Nesta figura, pode-se verificar que o papel pai de todos é o Profissional de Saúde, e dele derivam-se alguns papéis filhos, como o papel de médico, o de Paramédico, etc. Assim, ao alocar um agente ao papel de médico, este agente receberá automaticamente as permissões dos Profissionais de saúde e assim sucessivamente.

A autenticação é feita via *Lightweight Directory Access Protocol* (LDAP), e utilizam-se mecanismos de troca de informações seguras para as transferências entre os módulos do sistema.

O mecanismo de autorização é contextual, ou seja, a permissão de acesso pode basear-se em informações contextuais do momento de acesso. Por exemplo, um paramédico só pode acessar determinada parte do sistema quando está no período de seu turno. Assim, o contexto no caso, é o horário de acesso (Motta e Furuie, 2002).

Cita-se que este sistema foi implementado e utilizado no Instituto do Coração (InCor)/SP possuindo em sua base de dados cerca de 1400 usuários registrados e cerca de 56 papéis(Motta e Furuie, 2002).

MACA utiliza a tecnologia de LDAP para armazenamento de informações de permissões, além de dados de usuários, etc. Também faz uso dos serviços *Corba Healthcare*, Serviços de Segurança Corba (SSC), serviços de decisão para acesso a recursos *RAD- Facility*, etc.(Motta e Furuie, 2002)

Na Figura 8-2, pode-se verificar uma visão geral da arquitetura MACA.

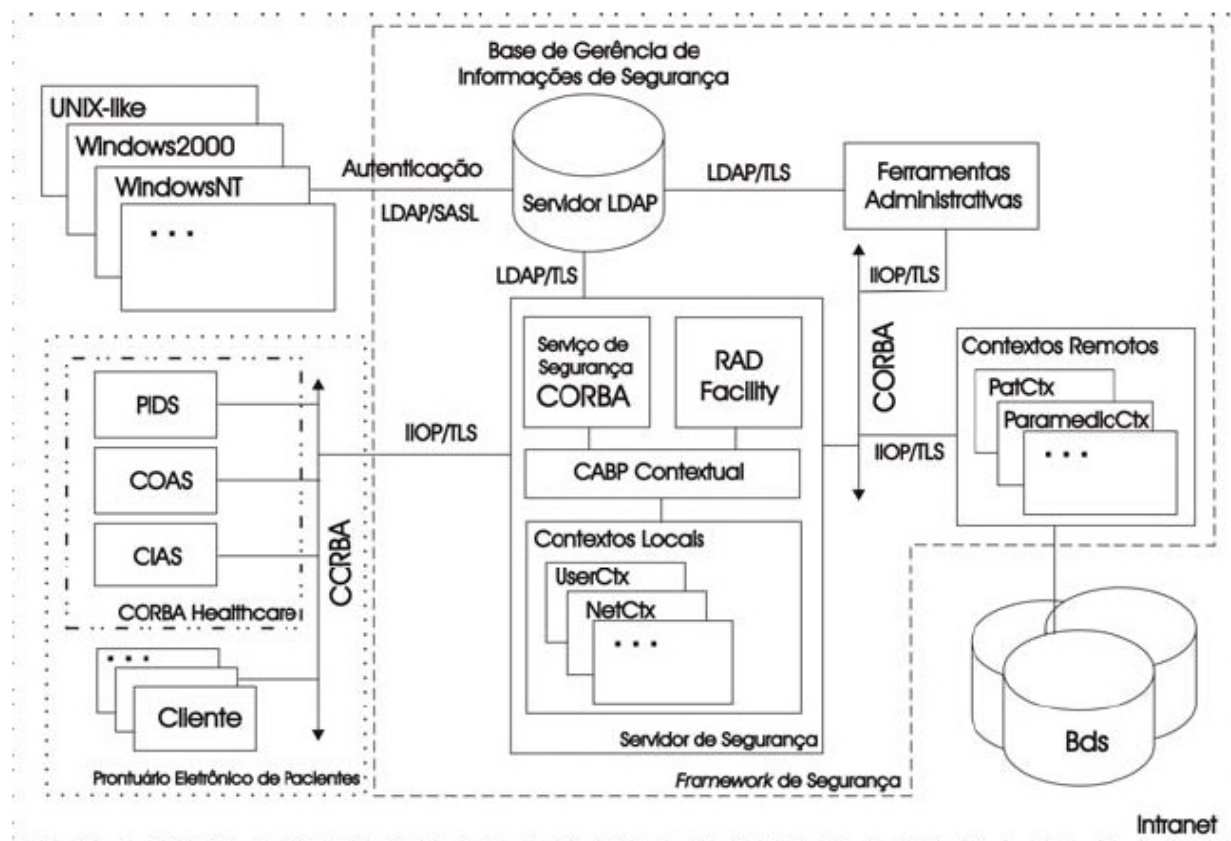


Figura 8-2 - Arquitetura MACA (Motta e Furuie, 2002)

Contudo, até onde se pode inferir, MACA não trata a delegação de papéis efetivamente, sendo indicado como um trabalho futuro (Motta, 2003).

A Base de Gerência de Informações de Segurança (BIGS) é a responsável pela gerência das permissões e por conter as regras de negócios necessárias para a implantação das permissões de acesso.

### 8.3 RDM2000

O RDM2000 (Zhang, Ahn *et al.*, 2003) é uma extensão do modelo RBAC96 (Sandhu e Samarati, 1994), cujo objetivo principal é permitir a delegação de permissão entre usuários, bem como a hierarquia de papéis além da delegação de vários níveis. Ou seja, o RDM2000 permite que um conjunto de privilégios delegados a um determinado agente seja delegado por este mesmo agente a um terceiro. Isto

se repete até que seja alcançado um nível de delegação que a arquitetura determina (Zhang, Ahn *et al.*, 2002).

A arquitetura proposta por RDM2000 está mostrada na Figura 8-3.

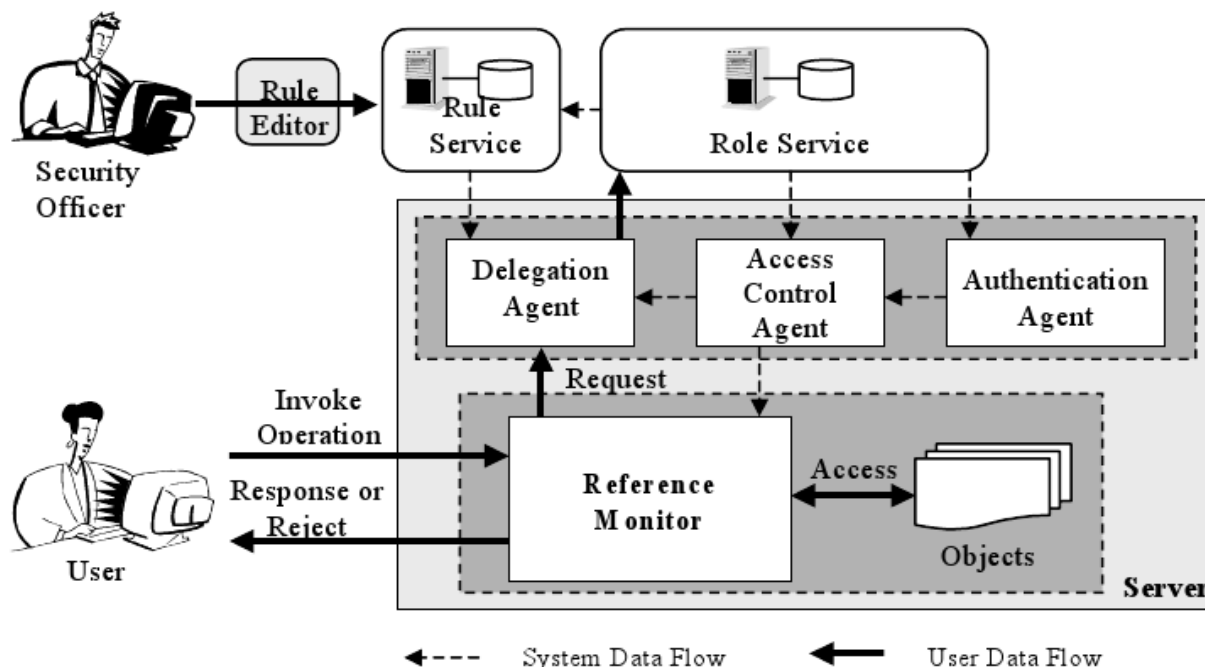


Figura 8-3 - Arquitetura RDM2000 (Zhang, Ahn *et al.*, 2003)

A autenticação é feita com a utilização de certificados digitais X.509 e os papéis são vinculados aos usuários identificados pelos CD através da utilização da chave pública como ligação.

Este modelo também implementa a capacidade de variar as permissões de acesso baseando-se em contexto.

O gerenciamento de permissões é feito com o gerenciamento de regras, definidas para papéis específicos e feitas por um usuário que as gerencia e cria, como pode ser visualizado na Figura 8-4.

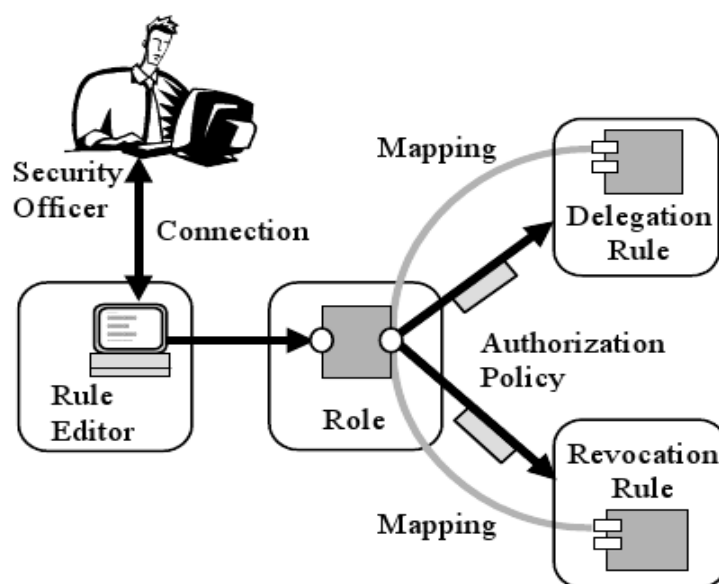


Figura 8-4 - Gerenciamento de regras RDM2000 (Zhang, Ahn *et al.*, 2003)

Zhang, Ahn *et al.* 2003 propõem a pesquisa futura de mecanismos de assinatura digital a fim de vincular usuários autenticados a seus atributos, utilizando arquivos assinados digitalmente no formato *eXtensible Markup Language* (XML).

## 8.4 Tees Confidentiality Model (TCM)

O modelo TCM, desenvolvido por Longstaff, Lockyer *et al.* (2003), visa a ser um modelo mais poderoso que o Controle de Acesso Baseados em Papéis (CABP) para o gerenciamento de privilégios pois, além de utilizar este modelo, usa em conjunto o Controle de Acesso Baseado em Identidade (CABI).

Assim, no CABI todo agente registrado no sistema possui uma identidade e pode acessar determinados objetos, mesmo não fazendo parte de nenhum papel.

Uma das particularidades do modelo proposto, segundo o autor, é a capacidade de garantir o acesso aos objetos protegidos em circunstâncias excepcionais, como em uma emergência médica.

Quando este for o caso, mensagens eletrônicas são disparadas para órgãos competentes avisando tal situação, possibilitando o seu acompanhamento em tempo real e desestimulando assim o uso inadequado desta capacidade.

Outra particularidade é a redefinição do conceito de permissões que, no modelo, é tratado como “Permissões de Confidencialidade”. Existem cinco tipos de Permissões de Confidencialidade (PC) para permitir o acesso de identidades e papéis e para não permitir este acesso aos objetos protegidos (Longstaff, Lockyer *et al.*, 2003), são eles:

- *Identity Role Confidentiality (IRC)*
- *Identity Specific Confidentiality (ISC)*
- *Identity General Confidentiality (IGC)*
- *Role Specific Confidentiality (RSC)*
- *Role General Confidentiality (RGC)*

O TCM utiliza o conceito de Coleção, ao invés do modelo hierárquico comum do CABP, para que seja possível estruturar não só papéis, mas também identidades, recursos e tipos de recursos, criando assim uma hierarquia mais completa.

O modelo proposto por TCM foi desenvolvido para o desenvolvimento de um Prontuário Eletrônico do Paciente Nacional do reino Unido, com permissões de leitura somente. Para tanto, faz referência à implementação deste modelo proposto com a utilização de dados fictícios, além da utilização em outros dois sistemas comerciais da área médica, o *Torex GP* e o *OLM Carefirst Social Services* (Longstaff, Lockyer *et al.*, 2003). Não há, porém, referências sobre mecanismos de autenticação utilizados.

As regras de Permissões de Confidencialidade são representadas através de arquivos no formato XML, como o exemplificado na Figura 8-5.



```
<RSCs>
  <RSC>
    <role> Gynaecological Consultant </role>
    <permissionVal>a</permissionVal>
    <inherit>down</inherit>
  </RSC>
  <RSC>
    <role>Health Care</role>
    <permissionVal>d</permissionVal>
    <inherit>down</inherit>
  </RSC>
</RSCs>
```

Figura 8-5 - Exemplo de representação de Permissões de Confidencialidade em XML usados no TCM (Longstaff, Lockyer *et al.*, 2003)

Nesta figura, observam-se a descrição de PC de *Role Specific Confidentiality*, mais especificamente as regras de PC específicos dos papéis, no caso de Consultor em Ginecologia e de cuidados gerais.

## 8.5 Open Architecture for Securely Interworking Services (OASIS)

O modelo *Open Architecture for Securely Interworking Services* (OASIS), definido por Bacon, Moody *et al.* (2002,2001), Bacon, Loyd *et al.* (2002), foi desenvolvido pensando-se em atender aos requisitos de permissões de acessos baseados em contextos de sistemas grandes e complexos, como os Prontuários Eletrônicos dos Pacientes (PEP).

Para possibilitar o gerenciamento de identidade, OASIS utiliza o conceito de “designação”. Esta designação só pode ser feita por usuários com permissões especiais de administração que, então, fornecem “certificados de designação” a outros usuários que poderão requerer a participação em um ou mais papéis.

Assim, após a autenticação no sistema, um agente pede a ativação de suas designações, representadas através de certificados X.509 para acessar objetos específicos. Como exemplo, um agente previamente designado como médico, ao autenticar-se no sistema, pode solicitar a ativação de sua designação de médico para acessar o prontuário de determinado paciente (objeto restrito), desde que

algumas restrições sejam obedecidas, como: estar no turno de médico, ser responsável pelo paciente em questão e ter a designação de médico (Motta, 2003).

Este modelo faz o uso de uma extensão do Controle de Acesso Baseado em Papéis (CABP), com a inclusão de parametrizações de papéis necessários para garantir uma granularidade mais fina de permissões.

A arquitetura dos serviços pode ser visualizada na Figura 8-6(a). Já na Figura 8-6(b), verifica-se o modelo de autenticação proposto. Nela, observa-se que um agente ao autenticar-se no sistema solicita a ativação de determinado papel, que deverá ser utilizado para fornecer as permissões de acesso aos objetos protegidos.

Nesta arquitetura, apesar de ser possível a integração com uma ICP para autenticar um usuário baseando-se no protocolo de desafio-reposta ISO/9798, utiliza-se como mecanismo de autenticação os valores de "usuário e senha". Porém, sabendo-se da vulnerabilidade de tal utilização, cita-se como pesquisa futura a utilização de mecanismos de autenticação através de biometria (Bacon, Moody *et al.*, 2002).

Embora documentos citem a implementação de um sistema para a utilização com RES de uma região do Reino Unido, não se encontraram referências sobre a funcionalidade de hierarquia de papéis ou sobre seu funcionamento.

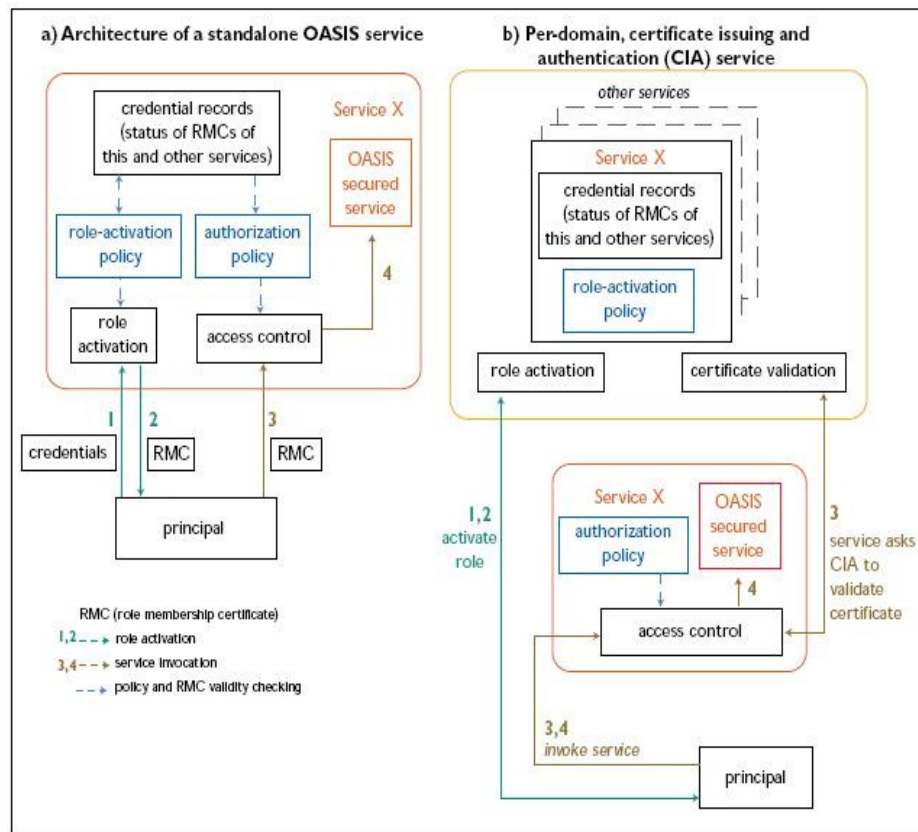


Figura 8-6 - Arquitetura OASIS (Bacon, Moody *et al.*, 2002)

## 8.6 MEDical Information System (MEDIS)

O modelo *MEDical Information System* (MEDIS), definido por Sucurovic (2007), foi um protótipo para um sistema nacional da Sérvia e Montenegro que fosse seguro para armazenamento e gerenciamento de informações médicas.

Sucurovic (2007) menciona que os sistemas da área de saúde na Sérvia e Montenegro originalmente não foram implementados com recursos para serem expandidos, de forma que o projeto visou em seu início à integração destes sistemas por si só.

Aproveitando o crescimento do uso da Internet no país nos últimos anos, capacitando a implementação de um paradigma compartilhado de informações e observando esta especificidade dos sistemas presentes no país, MEDIS foi ampliado.

MEDIS está baseado em um modelo de informações federativo, sendo que parte das informações está armazenada nas máquinas centrais e outras informações são armazenadas nos servidores das clínicas. A comunicação entre os servidores é feita utilizando Web Services (Bosworth, 2001).

Esta arquitetura segue o padrão "Comitê Européen de Normalisation (CEN)" chamado ENV 13606.

Uma visão geral da arquitetura MEDIS pode ser visualizada na Figura 20.

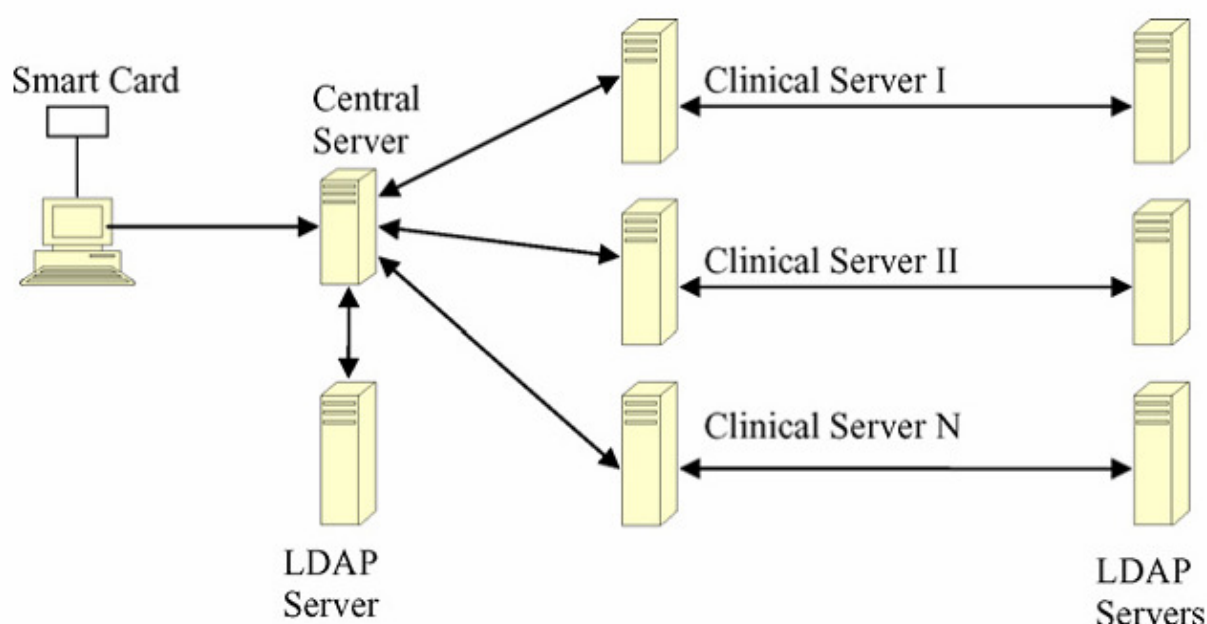


Figura 8-7 - Arquitetura MEDIS (Sucurovic, 2007)

A arquitetura MEDIS utiliza Certificados Digitais X.509 como mecanismo de autenticação, bem como Certificados de Atributos para representar os atributos dos usuários. Os atributos são organizados em esquemas XML.

As políticas de autorizações são armazenadas nos servidores LDAP locais e centrais da arquitetura proposta e têm sua estrutura baseada nas perguntas: "Who, Where, When, Why, How" para liberação dos acessos.

Verifica-se também a implementação do Controle de Acesso Baseado em Papéis (CABP), com suporte a hierarquia.

## **8.7 Considerações Finais**

Este capítulo apresentou uma análise dos principais trabalhos relacionados ao foco desta pesquisa, de seus aspectos principais e de suas aplicações em ambientes da área de saúde. Conceitos importantes como a hierarquia de papéis, permissões de confidencialidade e Certificados de Atribuições também foram apresentados.

# Capítulo 9

## H-PMI

---

*Neste capítulo é apresentada a proposta de Arquitetura H-PMI.*

### 9.1 Introdução

O objetivo deste trabalho é propor, implementar e validar uma arquitetura de gerenciamento de privilégios para sistemas de informações da área de saúde. Essa arquitetura deve ser capaz de:

- Fornecer controle de acesso com a flexibilidade necessária para o ambiente;
- Fornecer segurança inerente à aplicação;
- Fornecer mecanismos de autorização compatíveis com as necessidades;
- Fornecer ferramentas de gerenciamento adequadas à aplicação.

Em suma, objetiva-se propor uma arquitetura capaz de ser homologada segundo o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, com o máximo nível de garantia de segurança. Para tanto, a arquitetura a ser especificada deve utilizar os conceitos de autenticação e autorização apresentados até então, para proteger objetos, como os Registros Eletrônicos em Saúde, baseando-se nos modelos de referências e nas regulamentações existentes.

## 9.2 H-PMI

O *Health-Privilege Management Infrastructure*, apresentado neste trabalho, visa a ser uma arquitetura de gerenciamento de privilégios da área de saúde, segura, confiável e flexível, que utiliza o Controle de Acesso Baseado em Papéis (CABP).

Pode-se citar como pontos fortes da arquitetura desejada a capacidade de delegação de poderes entre os participantes, além da capacidade de acesso a dados restritos em momentos de emergência através de uma abordagem inovadora de delegação.

A arquitetura deve também prover a capacidade de fornecer mecanismos de interpretação de hierarquia de papéis, com herança de permissões entre eles.

## 9.3 Modelo de Gerenciamento de Privilégios (*Privilege Management Model*)

O H-PMI é composto de três estruturas principais:

- O Sistema de Gestão e Privilégios (SGP): responsável pela análise das requisições e pelo processamento dos privilégios de acesso, respondendo positivamente ou negativamente a uma requisição feita a ele. Também é responsável pelo gerenciamento de um Repositório de Atributos (RA);
- O Validador/Autorizador (VA): responsável pela validação de entradas e de requisições, também o principal agente na comunicação com o SGP e com o Sistema de Gestão Hospitalar em si;
- O Sistema de Delegação (SD): responsável por prover a funcionalidade de delegação de autorização.

Uma visão geral da arquitetura é apresentada na Figura 9-1. Nesta figura pode-se observar a interação entre os agentes e as principais estruturas da

arquitetura, bem como a utilização de certificados digitais X.509 pelos agentes para autenticar-se no sistema através de dispositivos variados.

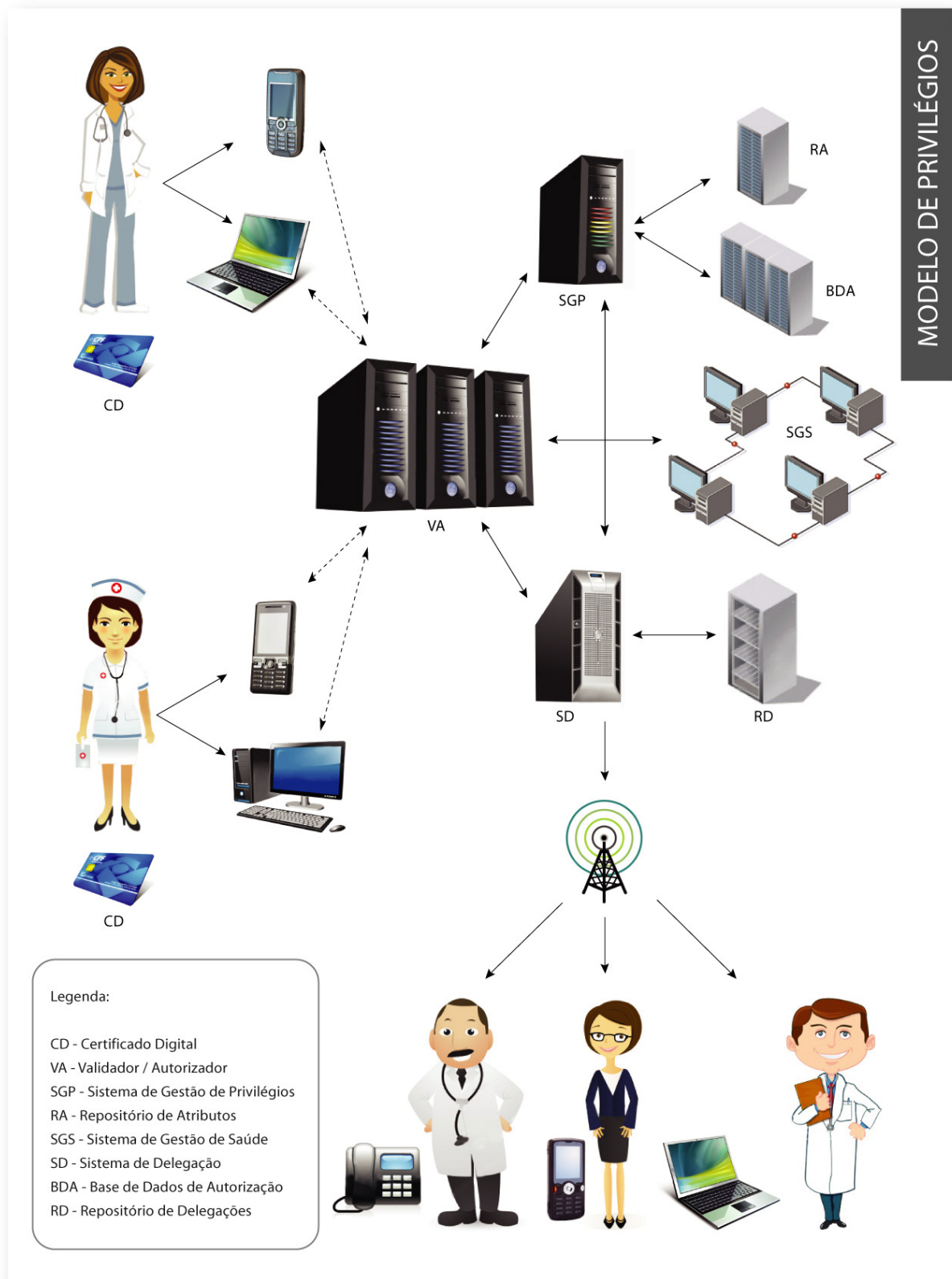


Figura 9-1 - H-PMI: Arquitetura Geral



A autenticação/validação do certificado do agente é feita pelo **validador** (VA), que é responsável por verificar informações como:

- Período de validade de um certificado: verificar se o certificado digital está sendo utilizado no período de validade estabelecido no momento da sua emissão;
- Estado de Revogação do certificado: verificar se o certificado digital foi revogado e não está mais válido, apesar de estar dentro do período de validade;
- Objetivo do uso: verificar se o certificado está sendo utilizado para o objetivo que foi emitido.

Além da utilização para autenticação, certificados digitais X.509 também são previstos para o fornecimento de chaves públicas no estabelecimento de um canal seguro de comunicação entre os dispositivos de acesso e os serviços oferecidos pelo sistema via HTTPS.

Outro ponto a ser citado é a integração entre o módulo SGP e o SD, intermediado pelo validador (VA). Isto porque, em momentos de emergência, apesar do Sistema Gerenciador de Privilégios negar acesso ao objeto protegido, o VA pode fornecer uma forma de acesso legítimo ao objeto através de um dos mecanismos de delegação, apresentados na seção Modelo de Delegação desta proposta.

Além destas estruturas principais, verifica-se a existência do Sistema de Gestão de Informações, que é basicamente uma relação dos sistemas acessados/utilizados pelos agentes.

Toda a arquitetura, apesar de estar inter-relacionada, pode estar disposta em um sistema distribuído interligado, possibilitando uma escalabilidade do sistema.

## 9.4 Modelo de Controle

O modelo de controle do H-PMI está baseado na implementação de um Controle de Acesso Baseado em Papéis, sendo que os papéis são representados dentro do sistema com o uso de Certificados de Atributos.

A ligação entre os Certificados Digitais e os Certificados de Atributos é feita com utilização da chave composta de **Nome comum** do sujeito (CN) e o **número de série** do certificado presentes no CD.

Considera-se que cada atributo terá a correspondência de um certificado de atributo, ou seja, para cada papel associado a cada agente devidamente cadastrado no sistema existirá apenas um papel em cada Certificado de Atributo emitido pelo SGP.

Isto visa a uma maior facilidade de gestão de Certificados de Atributos, uma vez que, ao revogar determinado papel<sup>6</sup>, não será necessário reemitir um novo Certificado de Atributos com os papéis que ainda continuariam válidos, caso fosse emitido em um mesmo CAAt mais de um papel.

Por exemplo, suponha que um agente cadastrado no sistema possui primeiramente um perfil de médico. Neste caso, o SGP emitiu para ele um CAAt com o atributo perfil com valor “Médico”(a). Após um tempo, este agente, além do perfil de médico, deverá desempenhar um papel de Auditor. Neste caso, o SGP emitirá um novo CAAt com o atributo perfil com o valor “Auditor”(b). Assim, os CAAt a e b são independentes entre eles, podendo durante um gerenciamento futuro a revogação independente de **a**, de **b** ou de ambos, sem a necessidade de reemissão de novos CAAt. Ou seja, é possível revogar todas as autorizações, ou parte delas a qualquer momento.

Caso fosse utilizado em um mesmo CAAt mais de um atributo perfil (CAAt composto), no exemplo citado, seria preciso que, ao determinar que o agente possuísse também o papel de auditor, as seguintes tarefas fossem realizadas:

1. Leitura de todos os Atributos do CAAt em uso atualmente pelo agente;
2. Revogação deste CAAt;
3. Emissão de um novo CAAt com os atributos do item 1, e mais o novo atributo.

Além desta capacidade de permitir a emissão e revogação de CAAt independentes um dos outros, a escolha de separar os perfis em CAAt independentes

---

<sup>6</sup> Atributos e papéis são referências as mesmas informações e são usadas indistintamente no decorrer do texto

visa também prover uma maior flexibilidade na capacidade de se gerenciar a validade dos Atributos.

Isto é possível já que cada CA<sub>t</sub>, vinculado a somente um perfil, terá sua validade individual, evitando a necessidade de sobrecarregar o SGP no cálculo de validades intermediárias ou na reemissão de CA<sub>t</sub> compostos, ou na gestão de outros atributos que indicassem a validade específica de cada atributo dentro dele.

Utilizando novamente o exemplo citado com a aplicação da modelagem escolhida, a validade do atributo *a* é independente da *b*. Caso fosse utilizada a outra abordagem, com o uso de um mesmo CA<sub>t</sub> para todos os perfis, seriam necessários vários passos para a determinação da validade do CA<sub>t</sub> composto, como o processamento das validades individuais, etc.

Prevê-se que cada objeto protegido possua suas permissões de acesso determinadas na Base de Dados de Autorização (BDA).

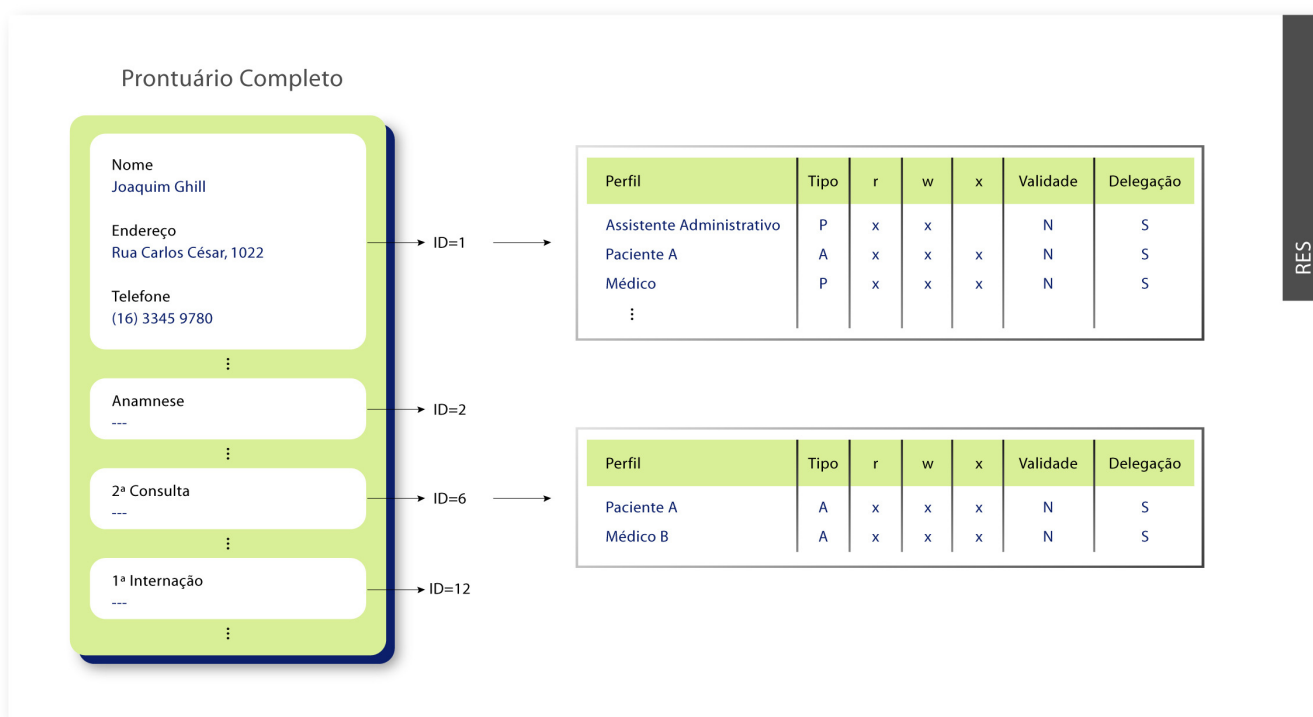
As informações presentes nesta base de dados devem ser estruturadas da seguinte maneira:

- Presença de um identificador único do objeto protegido;
- Regras gerais de acesso a tal objeto, sendo possível definir permissões de:
  - Leitura (R) (Permitir a visualização de dados);
  - Escrita (W) (Permitir a edição/inserção de novos dados);
  - Execução (X) (Permitir operar sobre os dados, como pesquisar etc.).
- Agentes/Perfis donos do objeto: definindo a identificação de quem pode editar, adicionar ou remover permissões a tal objeto, bem como delegar tais permissões ou partes delas a outrem;
- Regras específicas de acesso, sendo possível definir, além das permissões citadas, a ligação de permissões específicas a Agentes/Perfis determinados;
- Determinar se esta regra tem validade específica ou dependerá da validade dos atributos:
  - N: significa que a validade desta regra depende da validade do atributo;

- S: significa que esta regra tem uma validade específica, que não deve ser usada antes, nem depois dos intervalos de tempo.
- Determinar se tal objeto possui permissão para delegação. Este mecanismo é necessário para que objetos protegidos tenham um mecanismo de privacidade total, não permitindo qualquer acesso sem os explicitamente autorizados.

As regras que não forem definidas são automaticamente consideradas como não autorizadas.

Um exemplo desta definição pode ser visto na Figura 9-2. Ela ilustra um Registro Eletrônico em Saúde, dividido em áreas, cada uma delas com identificação e privilégios de acessos distintos.



**Figura 9-2 - Estrutura de um Registro Eletrônico em Saúde dividido em objetos distintos**

Uma visão mais geral do modelo de controle de acesso aos objetos pode ser vista na Figura 9-3. Nela é possível verificar um exemplo de um agente **a**, devidamente autenticado através do uso de seu Certificado Digital, pedindo acesso através do Sistema de Gestão Hospitalar (SGH), na data de 14 de junho de 2009, para leitura de determinada informação dentro do objeto protegido **b**. Este objeto

protegido **b** possui as permissões de acesso determinadas na Base de dados de Autorização.

Nesta base, verificam-se para o objeto B as permissões segundo a Tabela 9-1.

**Tabela 9-1 - Tabela de Permissões de Acesso ao Objeto Restrito B**

Perfil	Tipo	R	W	X	Validade	Delegação
Agente B	Agente	S	S	S	N	Direta/Indireta
Médico	Perfil	S	S	S	N	Direta/Indireta
Médico X	Agente	S	N	N	N	Direta/Indireta

O agente **a**, ao executar tal pedido ao SGH, estará indiretamente solicitando tal permissão ao VA, que será responsável por direcionar as requisições e as respostas ao SGH. Um exemplo desta atividade do VA pode ser visto como a atividade executada anteriormente por ele durante a autenticação do agente e a validação do seu certificado digital (CD).

O VA fará uma requisição ao SGP em nome do Agente **a**, solicitando acesso ao Objeto **b**.

O SGP verificará quais os perfis ativos do agente em questão estão ativos através de uma busca em seu Repositório de Atributos.

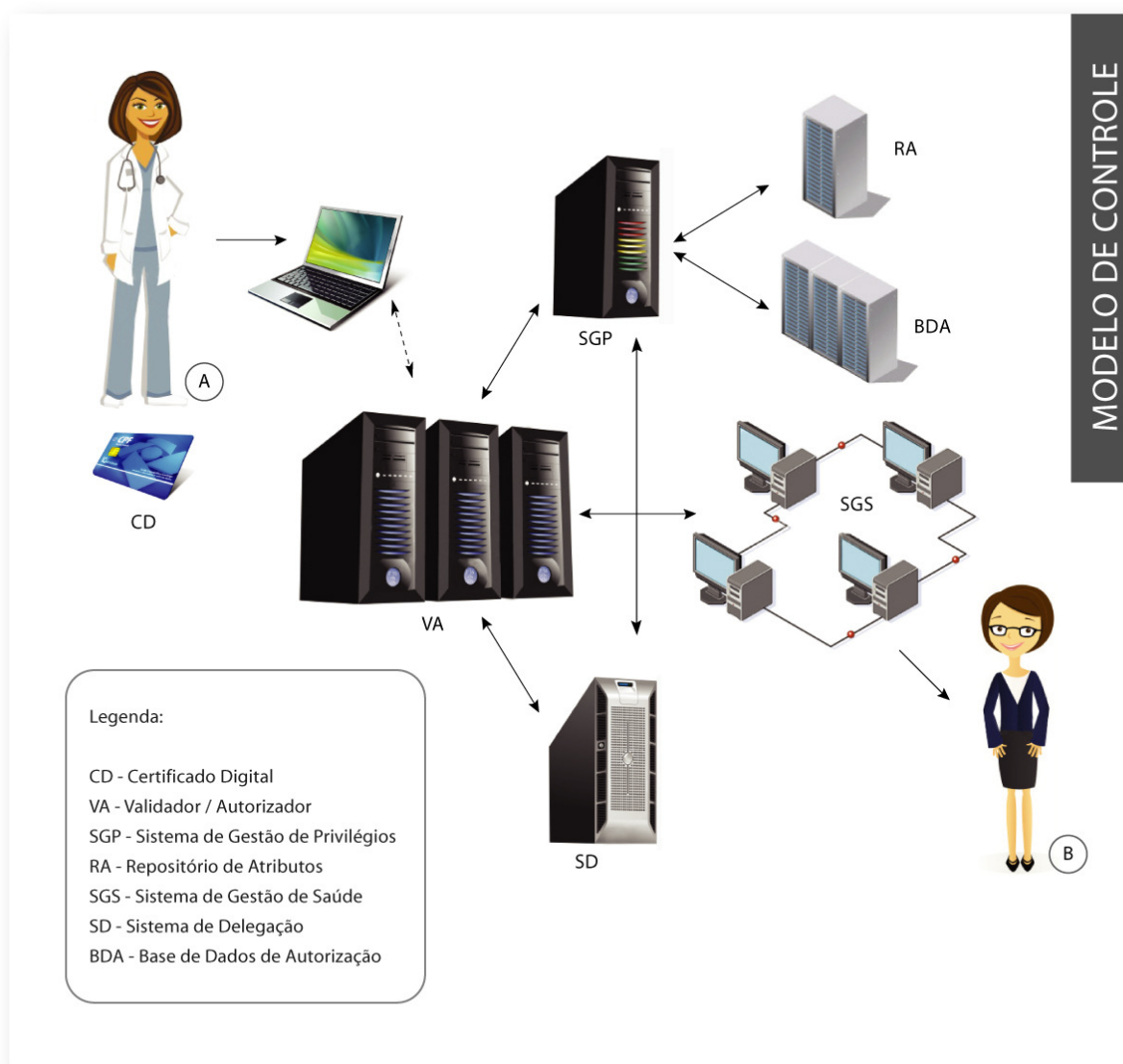


Figura 9-3 - H-PMI: Modelo de Controle

Em posse de todos os perfis, o Sistema de Gestão de Privilegios verificará em sua Base de Dados de Autorizações se algum dos perfis do Agente **a** (Tabela 9-2), a Identidade dele, ou algum dos perfis da hierarquia estão vinculados a permissões determinadas no Banco de Dados de Autorizações para regulamentar o acesso ao objeto **b**.

**Tabela 9-2- Perfis vinculados ao Agente A**

Perfil	Validade	
	De	Até
Médico	01/01/2009	01/01/2010
Auxiliar Administrativo	23/03/2009	23/09/2009
Auditor	12/04/2009	15/04/2009

Verifica-se que existe uma entrada na Tabela 9-1 que identifica permissões explícitas ao perfil de Médico, que se enquadra em um dos perfis do Agente A, conforme Tabela 9-2.

Assim, neste caso, o SGP deverá retornar uma mensagem positiva ao VA, dizendo que o agente em questão pode acessar o objeto protegido A com todas as permissões.

Com posse destes dados, o VA vai redirecionar a requisição ao SGH que procederá ao processamento e a exibição do resultado.

Esta operação se repetirá para todos os acessos de todos os agentes aos objetos protegidos do SGH.

Quando comparado com a estrutura básica de um PMI (Figura 7-1), verifica-se que a estrutura do H-PMI é um pouco mais complexa:

- A Política de Privilégios é representada no H-PMI através do conjunto de Atributos com a Base de Dados de Autorizações;
- O verificador fica a cargo da estrutura Validador/autorizador;
- Os objetos protegidos são comuns a ambos;
- A única variável de ambiente utilizada são os instantes, com data e hora, para verificação de períodos de validades, etc;
- A sensibilidade dos métodos do objeto não é utilizada, pois o objeto será protegido como um todo.

## 9.5 Modelo de Delegação

O modelo de delegação do H-PMI está dividido em dois tipos:

1. Delegação Direta;
2. Delegação Indireta.

Define-se Delegação Direta (DD) como o processo feito diretamente por um Agente para outro Agente, concedendo ao receptor toda ou parte de suas permissões de acesso ou atributos.

Já Delegação Indireta (DI) é o mecanismo de delegação utilizado por um Agente para acessar determinado objeto em situações de emergência que, a priori, ele não teria permissão de acesso.

### 9.5.1 Delegação Direta (DD)

O processo de Delegação Direta visa a atender as necessidades dos usuários em compartilhar parte ou todas suas permissões de acesso ou perfis, conforme apresentado em “Delegação de Poder”.

Um esquema mostrando este modelo de delegação pode ser visto na Figura 9-4. Nela, observa-se o processo de Delegação Direta entre os agentes **a** e **b**., sendo que o agente **a** delegará uma parte de suas permissões ao agente **b**, de acordo com uma necessidade específica.

O passo 1 corresponde ao processo de interação inicial entre o agente delegador e o sistema, no qual o agente irá se autenticar e indicar seu desejo de executar a operação de delegação. Esta requisição será interpretada pelo Validador/Autorizador (2) que, então, cuidará de solicitar ao SGP (3) que forneça uma lista de papéis (4) e privilégios (5) que o agente **a** possa delegar. Esta lista retornada ao VA (6) será então passada ao Sistema de Delegação (7), que preparará a exibição e o processo de delegação.

A requisição neste ponto sofrerá algumas operações a cargo do SD, como:

- Listar os papéis e privilégios possíveis de delegação;
- Prover sugestões de datas limites para a delegação, que serão utilizados para a geração dos papéis/permissões provisórios;
- Após a seleção, providenciar a solicitação da assinatura digital de uma declaração que formaliza a delegação dos papéis/permissões associadas, que será encaminhado ao agente. Este irá efetuar a



assinatura da requisição e enviar ao VA, que a validará e reencaminhará ao SD;

- Com a assinatura efetuada sobre a requisição, o SD armazenará em seu Repositório de Delegação e então informará, e solicitará ao SGP (8) a emissão dos papéis (9) ou a inserção em sua BDA (10) das autorizações delegadas ao receptor.

Após estes passos, o SGP informará o VA da conclusão da operação (11), bem como os agentes delegador e receptor (13) da conclusão da operação.

O VA então propagará o aviso ao SD (12). O SD por sua vez providenciará o armazenamento da solicitação assinada em seu Repositório de Delegações.

Na prática, dependendo da plataforma de software usada, esse modelo pode sofrer alterações a fim de adaptação. Por exemplo, podem ser utilizados Web Services para representar os servidores.

Utilizando o *Globus Toolkit*, por exemplo, é possível tratar-se o modelo de delegação previsto através de Credenciais Proxys e de Credenciais Proxys Restritas (Ferreira, Thakore *et al.*, 2004).

Um diagrama de sequência que ilustra este processo de Delegação Direta pode ser visualizado no Apêndice A.3.

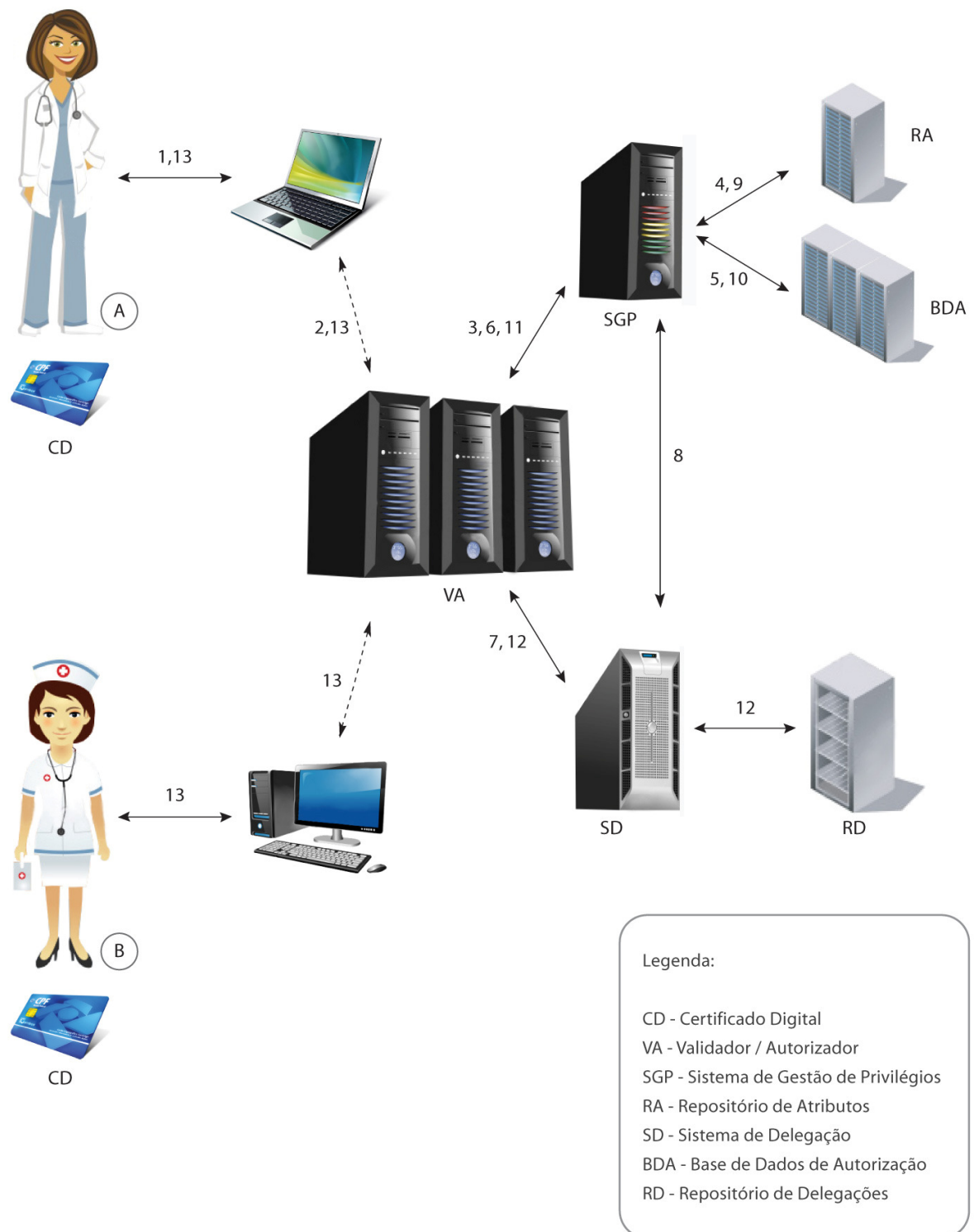


Figura 9-4 - H-PMI: Modelo de Delegação Direta

### 9.5.2 Delegação Indireta (DI)

O mecanismo de Delegação Indireta visa a fornecer uma flexibilidade maior à arquitetura proposta do H-PMI, possibilitando o disparo da delegação através de um pedido de um agente que a priori não tinha acesso a um objeto.

Esta situação pode ocorrer em casos emergenciais, por exemplo, quando um paciente tem sua entrada registrada em uma sala de emergência e os médicos responsáveis, ou seja, que possuem permissões de acesso a seu prontuário, além do próprio paciente, não se encontram fisicamente no local para atendê-lo ou não estão em condições de delegar a permissão de acesso aos outros médicos plantonistas por **Delegação Direta**.

A Figura 9-6 fornece visão detalhada dos passos da **Delegação Indireta**. Ela deve ser vista como uma continuação da Figura 9-3, já que este processo só poderá ser disparado caso seja retornado pelo Modelo de Controle uma negação de acesso e a operação em questão tenha permissões de Delegações, no caso especificamente, da Indireta.

Outro ponto da DI é que ela só poderá ser processada caso o agente solicitante tenha um perfil igual ou superior<sup>7</sup> hierarquicamente aos perfis com permissão de acesso padrão do objeto.

Utilizando como exemplo a Hierarquia apresentada na Figura 9-5, o agente **a** somente poderia solicitar a Delegação Indireta do objeto, cujas permissões de acesso estão representadas na Tabela 9-1, aos médicos e seus papéis derivados, como Plantonistas e Cirurgiões Gerais.

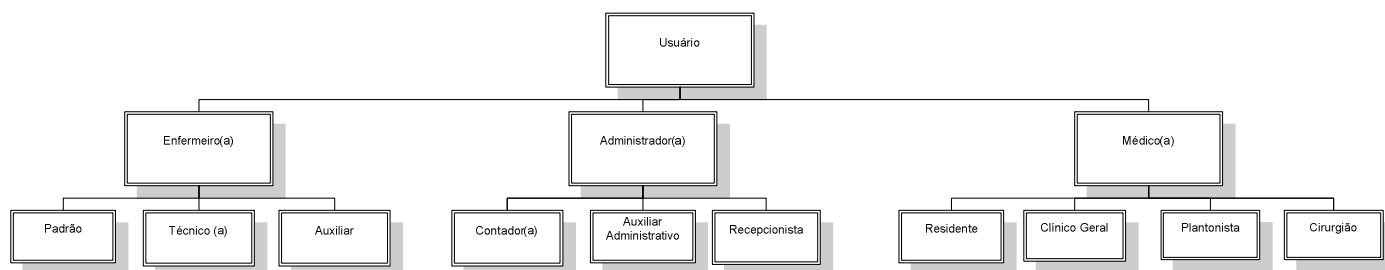


Figura 9-5 - H-PMI: Exemplo de hierarquia de papéis

<sup>7</sup> Hierarquia superior: ramo mais baixo da árvore, mais específico

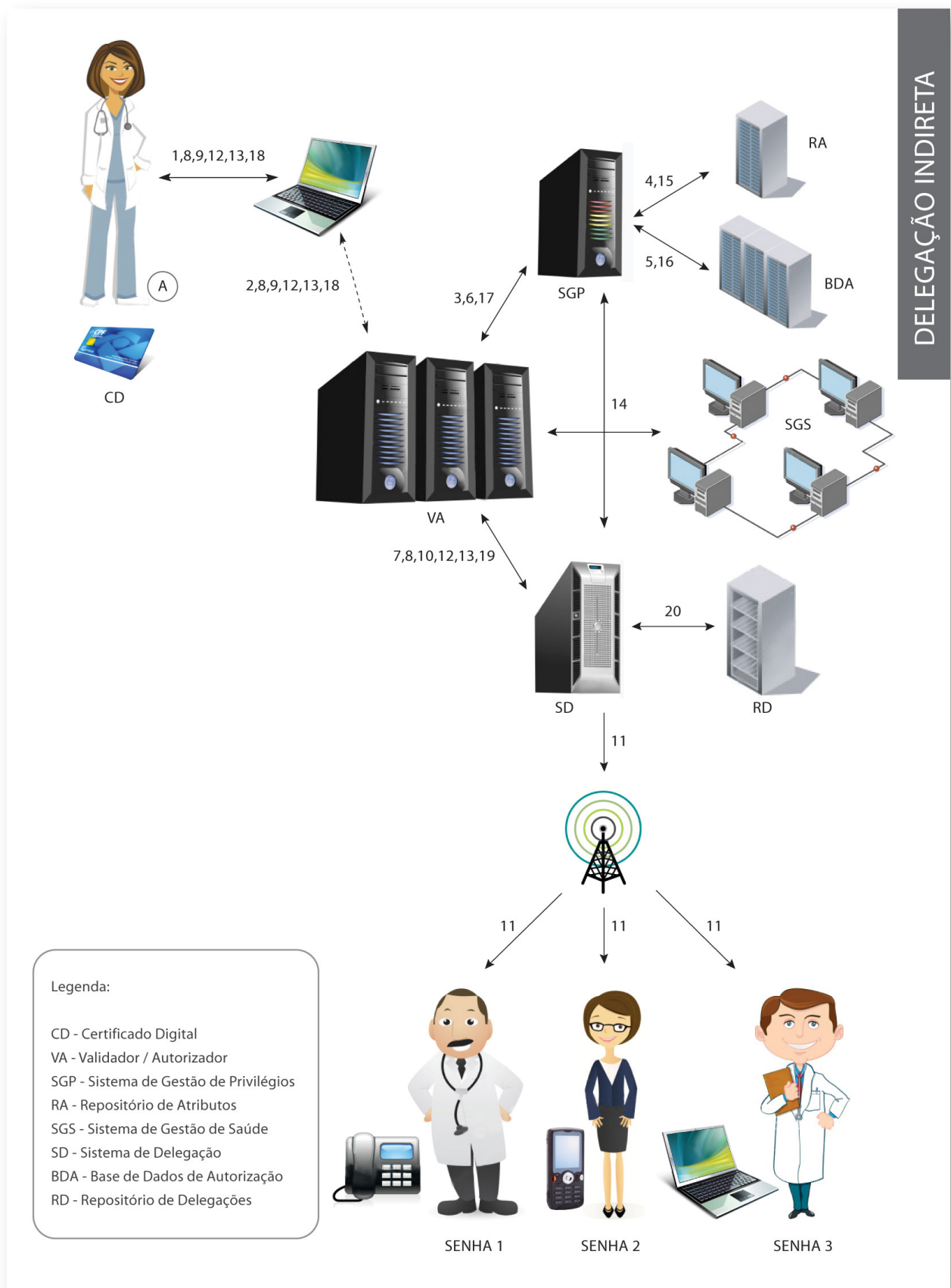


Figura 9-6 - H-PMI: Modelo de Delegação Indireta

Retornando à Figura 9-6, o passo (1) indica que o agente **a** em questão, apesar de não ter a permissão de acessar o objeto protegido, é elegível de participar da Delegação Indireta, por possuir o atributo de Médico, fazendo parte assim de um perfil que possui permissão de acesso ao objeto e cuja permissão de delegação indireta está explicitamente autorizada.

Neste caso, será fornecida automaticamente para ele a possibilidade de participar da DI de acesso ao objeto em questão. Ao prosseguir, aceitando participar da DI, ele passará a requisição ao VA (2). A aceitação pode ser implementada pelo simples clique em um botão programado para esta finalidade.

O VA, em posse de tal informação, solicitará ao SGP as informações de perfis (4) e privilégios (5) que possuem acesso máximo<sup>8</sup> a tal objeto. Esta lista pronta será enviada ao VA (6) que então, irá analisá-la e encaminhara ao SD (7).

O SD então processará as seguintes operações:

- Criação de uma requisição de Delegação Indireta com os perfis/privilégios retornados, dizendo que pelo menos um deles será utilizado para acesso ao Objeto restrito;
- Envio desta requisição para assinatura digital do requerente (8), que passará pelo VA para validação da assinatura da requisição (9);
- Quando o VA validar a assinatura, reencaminhará a solicitação assinada ao SD (10) que então continuará o processo de delegação, gerando N senhas provisórias de delegação que são então enviadas aos agentes (11) possuidores das permissões retornadas em (6);
- Concomitantemente, são mostrados ao Agente solicitante os telefones de contato dos agentes que receberam as senhas (12);
- Cabe ao agente solicitante entrar em contato com os agentes mostrados e solicitar a senha de autorização;

---

<sup>8</sup> Define-se acesso máximo como a maior capacidade de operação sobre o objeto, sendo que quanto mais operações são permitidas, maior é sua classificação. Por exemplo: permissão de leitura, escrita e execução em conjunto é considerada maior que leitura e gravação somente.

- Quando o agente solicitante conseguir a senha de autorização, ele a informa na interface que é então encaminhada pelo VA ao SD que a processa (13);
- O SD, de posse desta senha, definirá qual o perfil/permissão que deverá ser delegado. A partir deste ponto, o Sistema de Delegação gerará uma requisição autoassinada de Delegação Indireta para o perfil/permissão determinada e informará o SGP para que providencie o papel (14) ou a entrada (15) no BDA para permitir o acesso delegado.

Com estas operações realizadas, o SGP avisará o VA (16) através de mensagens padronizadas. O VA por sua vez avisará o agente solicitante que a permissão foi concebida com alguma mensagem, bem como enviará mensagem ao SD (17) para que ele possa arquivar as solicitações assinadas em seu repositório (18).

O modelo de delegação apresentado difere da estrutura básica de PMI apresentada na Figura 7-1, como:

- Não há a presença de um *Source of Authority*, que possui os privilégios que devem ser delegados, mas sim um conjunto de atividades que geram tais privilégios;
- No H-PMI verifica-se mais de um tipo de delegação, a DD e a DI, no caso do PMI clássico, verifica-se somente uma.

Um diagrama de sequência que ilustra este processo de Delegação Direta pode ser visualizado no Apêndice A.4.

Está disponível no Apêndice A.5 um diagrama de relacionamento do Banco de Dados que demonstra em uma visão geral a inter-relação entre as partes e objetos integrantes do H-PMI.

## 9.6 H-PMI e trabalhos relacionados

Verifica-se após a apresentação do H-PMI que ele possui consideráveis diferenças em relação aos trabalhos relacionados descritos neste documento.

Um resumo das principais características dos trabalhos analisados pode ser visualizado na Tabela 9-3.

O H-PMI, conforme apresentado, implementará o Controle de Acesso Baseado em Papéis (CABP), sem ter necessariamente foco no controle de acesso contextual, diferentemente dos modelos MACA e RDM2000, que priorizam tais informações para determinação de direitos de acesso. Isto porque a única variável contextual importante para o modelo proposto é o momento do acesso, ou seja, a informação do instante de requisição, quando serão levadas em conta as permissões e suas respectivas validades.

Outro ponto, é que o H-PMI prevê o uso de Certificados Digitais X.509, como mecanismo de autenticação, o mesmo mecanismo utilizado pelo RDM2000.

A proposta inclui a utilização do CD padrão ICP-Brasil, visando à adequação do sistema às normas de certificações expostas.

Tabela 9-3 - Comparativo entre trabalhos relacionados e o H-PMI

Projeto	Mecanismo de Autenticação	Mecanismo de Autorização	Hierarquia de Papéis	Aplicação em Ambientes médicos	Suporta Delegação	Outros detalhes
MACA	LDAP	Uso de BIGS	Sim	Sim	Não	Utiliza serviços Corba Healthcare, Serviços de Segurança Corba e RAD-Facility. Implementa o CABP Contextual.
RDM2000	Certificados X.509	Uso de regras em BD	Sim	Não definido	Sim	Possui suporte a regras de acessos contextuais. Permite delegação em vários níveis.
TCM	Não definido	Uso de Permissões de Confidencialidade	Sim	Sim	Sim	Implementa o CABI. Foco no direito de acesso em momentos de emergência. Estende o conceito de hierarquia para Coleções
OASIS	Usuário e senha	Uso de regras em BD	Não definido	Sim	Sim	Utiliza conceito de designação, além de Certificados X.509 para identificar as designações
MEDIS	Certificados X.509	Políticas em LDAP	Sim	Sim	Não	Federação com Web services
H-PMI	Certificados X.509	Uso de regras em BD	Sim	Sim	Sim	



Uma característica quase comum a todos os trabalhos relacionados e que também está presente no H-PMI é o suporte a Hierarquia de Papéis que, exceto para o RDM2000, é oferecido por todos os trabalhos analisados relacionados.

As implementações nestes casos variam desde hierarquias simples, utilizadas para herança de privilégios, como é o caso do MACA e do próprio H-PMI, bem como hierarquias mais complexas, como a do TCM, que implementa o conceito de coleções, ampliando-se hierarquia de papéis para permissões, etc.

Outra característica comum em quase todos os projetos é o uso de regras de autorizações presente em Banco de dados, que serão utilizadas para determinar o acesso aos objetos. A única exceção para esta regra é o MEDIS, que utiliza regras armazenadas em servidores LDAP.

Apesar de quase todos os modelos suportarem a delegação de permissões, H-PMI propõe e estende o modelo proposto pelo TCM, para ser utilizado em momentos de emergência.

H-PMI define este modelo como Delegação Indireta e aprimora o sistema do TCM, já que não só avisa os responsáveis pelos objetos que determinada delegação indireta está em percurso, mas força a participação destes agentes no sistema independente de sua localização, permitindo uma maior confiabilidade no uso da ferramenta e podendo até desencorajar má utilização por agentes mal intencionados.

Porém, este modelo de delegação indireta proposta ainda precisa ser avaliado quanto à viabilidade, aos procedimentos, às leis e normas, etc.

O H-PMI prevê o uso de Certificados de Atributos para a atribuição dos papéis aos agentes, como faz o MEDIS. Uma forma possível, porém não selecionada de atribuir papéis é a proposta adotada pelo OASIS, que utiliza extensões do certificado X.509 para referir-se estas designações.

## 9.7 Considerações Finais

Neste capítulo, apresentou-se a proposta de um modelo de controle de acesso com delegações, desenvolvido neste trabalho, o H-PMI, definido em módulos para possibilitar a implantação independente e distribuída, caso necessário.

Apresentou-se do Modelo de Gerenciamento de Privilégios, que fornece uma visão geral da arquitetura e da interação entre os módulos da proposta.

Posteriormente, definiu-se o Modelo de Controle, que partiu do princípio de que os objetos a serem protegidos, no caso as informações presentes nos Registros Eletrônicos de Saúde, são identificados univocamente por identificadores, utilizados como chave para a definição de políticas de acesso a tais objetos, com permissões de leitura, escrita e execução. Todas as operações dos sistemas geram registros de auditoria.

As políticas, que devem ser definidas através de interfaces de administração, estão vinculadas a papéis, representados por Certificados de Atributos (CA) e ligados a Certificados Digitais (CD) dos usuários do sistema.

Os Certificados Digitais são previstos também para uso com o mecanismo de Autenticação para acesso aos sistemas que compõem, identificando e autenticando univocamente os agentes que fazem acesso à arquitetura e de Assinatura Digital, no uso para verificação de assinaturas de requisições e solicitações.

O agrupamento de usuários em papéis visa facilitar a administração de políticas como um todo.

Detalharam-se também os processos de delegação, direta e Indireta, projetadas de maneira segura para permitir que o requisito de delegação do Manual de Certificação para Sistemas de Registros Eletrônicos em Saúde fosse contemplado, além de permitir a delegação indireta, ou seja, o acesso legítimo a dados confidenciais em momentos de emergência, registrando estes processos com Assinaturas Digitais.

Por fim, foi apresentada uma comparação entre a proposta desenvolvida e os trabalhos relacionados a esta proposta.

# Capítulo 10

## WEB H-PMI

---

*Neste capítulo é apresentada uma implementação prova de conceito da arquitetura de gerenciamento de privilégios proposta.*

### 10.1 Introdução

A fim de avaliar e validar a arquitetura proposta foi desenvolvido um sistema “*proof of concept*” do modelo especificado, chamado **Web H-PMI**.

Denomina-se “*proof of concept*” a coleta de evidências de que determinado modelo é factível<sup>9</sup>.

Utilizando uma interface Web, esse sistema permite que usuários comuns visualizem e compartilhem acesso a seus dados presentes na plataforma do Google Health com outros usuários, fornecendo:

- Controle de acesso com flexibilidade superior à oferecida pelo Google Health;
- Mecanismos de delegação amplos e flexíveis;
- Mecanismo detalhado de registros de auditoria;
- Interface de acesso através de **Web services** possibilitando integrações com terceiros.

Nos próximos tópicos serão detalhados a implantação do Web H-PMI e seus módulos.

---

<sup>9</sup> Pela definição obtida em: [http://www.investorwords.com/3899/proof\\_of\\_concept.html](http://www.investorwords.com/3899/proof_of_concept.html)

## 10.2 H-PMI e o Web H-PMI

O mecanismo H-PMI implementado no Web H-PMI, aqui apresentado, é simplificado, mas provê a grande maioria das funcionalidades previstas na arquitetura, como a delegação direta, os registros detalhados de auditoria e uma granularidade mais fina do controle de acesso dos objetos compartilhados.

Ele também está baseado na utilização de permissões de acesso no formato XACML em conjunto com informações armazenadas em um Sistema de Gerenciamento de Banco de Dados Relacional, vinculadas com as informações armazenadas no Google Health.

Com base nisto e seguindo os trabalhos de Ardagna, Damiani *et al.* (2004) e na especificação de Anderson (2005), foi criada uma nomenclatura especial para os módulos do Web H-PMI quando comparado com a arquitetura proposta.

Apesar da nova nomenclatura, há uma equivalência entre os módulos, conforme pode ser visualizado na Tabela 10-1:

**Tabela 10-1 - comparação entre nomenclatura de módulos H-PMI e Web H-PMI**

<b>Nomenclatura H-PMI</b>	<b>Nomenclatura Web H-PMI</b>
Validador/Autorizador	<i>Policy Enforcement Point (PEP)</i>
Sistema de Gestão de Privilégios	<i>Policy Decision Point (PDP)</i>
Repositório de Atributos	<i>Policy Information Point (PIP)</i>
Sistema de Gestão de Saúde	Google Health
Sistema de Delegação	<i>Policy Administration Point (PAP)</i>
Base de dados de autorização	<i>Policy Information Point (PIP)</i>
Repositório de Delegações	<i>Policy Information Point (PIP)</i>

Outra diferença do H-PMI em comparação com o Web H-PMI é a implementação do Controle de Acesso Baseado em Atributos (CABA), ou em inglês, *Attributed Based Access Control (ABAC)*, proposto por Yuan e Tong (2005) que é uma extensão do CABP tradicional. ABAC possui dentre outras vantagens a possibilidade de se expressar uma permissão de acesso a um usuário que não

pertence a um grupo, mas que passa a ter acesso a determinado recurso, bastando que ele possua os atributos descritos na política utilizada.

Com esta abordagem é possível uma maior flexibilidade nas definições de políticas de acesso, permitindo que os pacientes possam expressar suas permissões de acesso sem ter que necessariamente conhecer a estrutura hierárquica que compõem o CABP implantando para acessar os seus dados.

### 10.3 Módulos Web H-PMI

Seguindo a arquitetura proposta, o web H-PMI está estruturado de acordo com os seguintes módulos:

- *Policy Enforcement Point* (PEP), ou Ponto de Aplicação de Regras (PAR);
- *Policy Decision Point* (PDP), ou Ponto de Decisão (PD);
- *Policy Information Point* (PIP), ou Ponto de Busca de Informação (PBI);
- *Policy Administration Point* (PAP), ou Ponto de Administração de Políticas (PAdP).

Uma visão geral dos módulos do Web H-PMI é apresentada na Figura 10-1. Nela é possível verificar a inter-relação entre um **Web service** cliente que utiliza a infraestrutura provida pelo Web H-PMI para acessar determinado registro armazenado no Google Health e que, conseqüentemente, está vinculado ao acesso ao Web H-PMI.

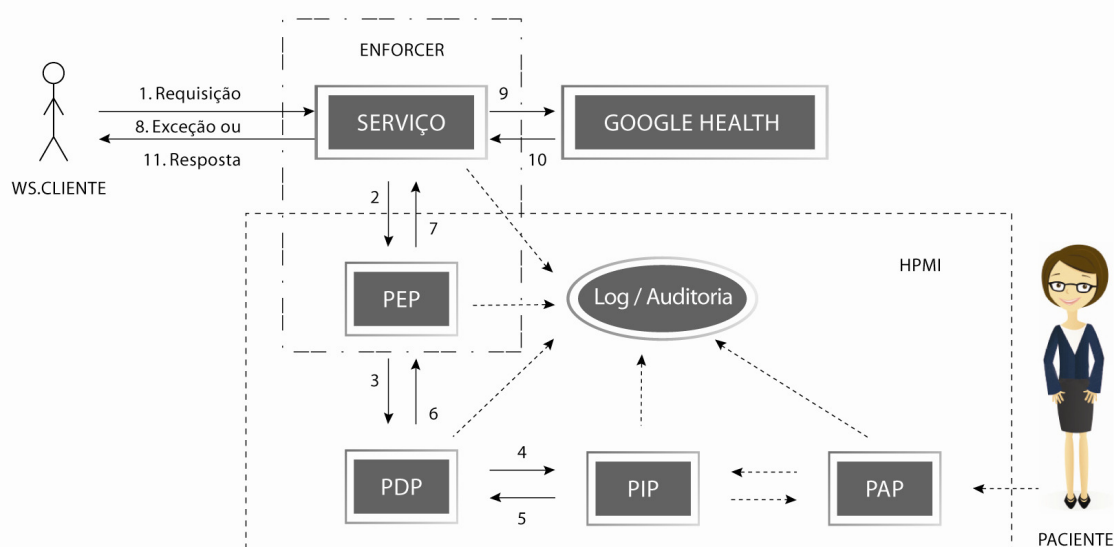


Figura 10-1- Arquitetura Web H-PMI

O funcionamento segue analogamente o modelo de controle do H-PMI mostrado na Figura 9-3. Um **Web service** cliente, ao solicitar ao serviço do Web H-PMI acesso à determinada informação armazenada no Google Health (1) terá a requisição interceptada e processada pelo *Policy Enforcement Point* (PEP) (2).

O PEP encaminhará uma solicitação ao *Policy Decision Point* (PDP) (3) solicitando o que deve ser feito com a requisição, se deve ser autorizada ou negada. O PDP, para tomar a decisão, requisitará informações armazenadas no *Policy Information Point* (PIP) (4), como regras de acesso, atributos do requisitante, além de políticas gerenciadas pelo paciente através do *Policy Administration Point* (PAP).

Em posse destas informações (5), o PDP retornará ao PEP a decisão (6) que então encaminhará para o Serviço (7). O serviço poderá retornar erro ao cliente (8) ou efetuar a requisição ao Google Health e retornar a solicitação (9 a 11).

Todas as operações geram informações de auditoria e podem ser visualizadas pelo paciente através do Web H-PMI.

### 10.3.1 Policy Enforcement Point (PEP)

O *Policy Enforcement Point* (PEP) ou Ponto de Aplicação de Regras (PAR) é o módulo responsável por gerenciar para que nenhuma requisição acesse os serviços sem ser interceptada e tenha recebido autorização do PDP para prosseguir.

Sua função é auxiliada pelo o mecanismo de autorização do Google Health. Isto porque, nenhuma informação armazenada na infraestrutura da empresa pode ser acessada sem um **token** de autorização. Este token fica em posse do Web H-PMI, só sendo retornado ao serviço que irá efetuar a requisição ao Google Health caso a autorização decidida pelo PDP seja de autorizar que tal operação ocorra.

Ele também é responsável por armazenar as primeiras informações de auditoria.

### 10.3.2 Policy Decision Point (PDP)

O *Policy Decision Point* (PDP) ou Ponto de Decisão (PD) é o módulo principal do Web H-PMI, que é responsável por juntar todas as informações da requisição, as políticas de acesso e definir se a solicitação pode prosseguir ou, não, ou se não há informações o suficiente para uma decisão.

Para tanto, ele é capaz de contatar o *Policy Information Point* (PIP) solicitando as políticas referentes àquela solicitação, que deverão vir acompanhadas dos atributos adicionais da requisição, como dados contextuais (data, hora, origem, etc.) bem como solicitar as políticas ativas no formato XACML para processá-las.

Assim, de posse de todas as informações disponíveis, PDP processa a requisição, informando ao PEP qual deve ser a atividade a ser executada, seja de negar/autorizar o acesso ao recurso, seja negar o acesso informando que as informações que foram coletadas não foram suficientes para que a decisão fosse tomada.

Fica a cargo do PDP o registro de traços de auditoria, capazes de identificar quais foram às informações utilizadas e quais as políticas processadas a fim de gerar o veredito de acesso enviado ao PEP.

### 10.3.3 Policy Information Point (PIP)

O *Policy Information Point* (PIP) ou Ponto de Busca de Informação (PBI) é o sistema responsável por atender as requisições do PAP e do PDP. Isto porque ele é responsável por armazenar, catalogar e manter consistentes as políticas de acesso no formato XACML, bem como as demais informações e atributos necessários para que as decisões de acesso sejam efetuadas de maneira mais rápida, segura e confiável possível.

Ele também é responsável por manter registros de auditoria sobre toda e qualquer requisição feita para ele, permitindo o rastreamento completo das operações executadas.

### 10.3.4 Policy Administration Point (PAP)

O *Policy Administration Point* (PAP) ou Ponto de Administração de Políticas (PApP) é uma das interfaces de comunicação entre o sistema e os pacientes.

Esta interface permite que o paciente interaja administrando as políticas de acesso, adicionando, editando ou removendo regras especiais para controle de acesso refinado aos dados lá armazenados.

Para que isto seja possível, ao vincular o perfil ao sistema, é feita uma consulta aos dados armazenado no Google Health, quando todas as informações presentes no CCR do usuário são mapeadas e identificadas univocamente. Após isto, são fornecidos mecanismos para que o paciente visualize estes dados e possa definir minuciosamente quais dados podem ser acessados e por quem. No final deste procedimento, políticas de acesso no formato XACML são atualizadas no PIP.

Antes da atualização, é possível que sejam efetuados procedimentos de checagem lógicas a fim de permitir ao paciente uma visualização mais apurada da regra atualizada, possibilitando que inconsistências sejam detectadas e corrigidas, evitando a criação de regras falhas que permitam operações que deveriam ser negadas.

Cabe também ao PAP o registro de traços de auditoria a fim de garantir que todas as políticas de acesso lá operacionalizadas reflitam as operações realizadas pelos pacientes.



### 10.3.5 Interface Web

O Web H-PMI possui uma interface Web que permite a sua utilização pelos usuários do sistema.

Além disto, ela permite a obtenção dos dados necessários para que os outros módulos possam interagir com os dados armazenados no Google Health.

Por ser um sistema prova de conceito foi utilizada a integração com os dados presentes no ambiente H9 do Google Health, sendo a autorização efetuada através do mecanismo *AuthSub*.

A seguir serão apresentadas as principais funcionalidades do sistema desenvolvido e os registros de telas que exemplificam a utilização.

A identificação unívoca de cada objeto é obtida através de mecanismos próprios do SGBD ou através da característica do objeto, como o caso de parte do atributo *CCRDocumentObjectID* presente nos CCRs do Google Health.

#### 10.3.5.1 Página principal

A página principal do Web H-PMI (Figura 10-2) tem como objetivo propiciar ao usuário uma porta de entrada ao sistema, seja através da possibilidade de **login** (usuário já cadastrado), seja possibilitando que novos usuários se cadastrem para uso.

The screenshot shows the main page of the Web H-PMI system. At the top, there is a green navigation bar with a login form. The form includes two input fields labeled 'Usuário' and 'Senha', followed by an 'Entrar' button. To the right of the form, there is a link that says 'Ainda não possui cadastro Cadastrar'. Below the navigation bar, the page greets the user with 'Seja bem - vindo ao H-PMI na Web'. The central part of the page contains a diagram illustrating the system architecture. The diagram shows a central server labeled 'SGP' (Sistema de Gestão de Privilegios) connected to various components: 'VA' (Validador / Autorizador), 'BA' (Base de Dados de Autorização), 'BDA' (Base de Dados de Autorização), 'SGS' (Sistema de Gestão de Saúde), and 'SD' (Sistema de Delegação). There are also icons for a doctor (A) and a user (B). A legend box on the left side of the diagram defines the abbreviations: CD - Certificado Digital, VA - Validador / Autorizador, SGP - Sistema de Gestão de Privilegios, BA - Base de Dados de Autorização, SGS - Sistema de Gestão de Saúde, SD - Sistema de Delegação, and BDA - Base de Dados de Autorização. To the right of the diagram, a vertical label reads 'CONTROL MODEL (CM)'. Below the diagram, a list of capabilities is provided: 'Com o H-PMI você pode:' followed by four bullet points: 'Compartilhar seu prontuário com outros usuários', 'Compartilhar uma parte do prontuário', 'Controlar o que, quem e quando poderá acessar', and 'Ter registros completos de acesso a seus dados'. Below this list, it says 'E muito mais...'. At the bottom right, the 'Google health beta' logo is displayed with the text 'Powered by'.

Figura 10-2 - Página principal do Web H-PMI

### 10.3.5.2 Página de administração

A página de administração do Web H-PMI (Figura 6-2) somente é visualizada quando um usuário foi autenticado adequadamente, fornecendo seu nome de usuário e a senha previamente cadastrados na plataforma.

Através dela é possível visualizar os menus que representam as principais atividades presentes no sistema:

- Prontuário: visualização dos dados presentes no perfil H9 do usuário;
- Vinculação de perfil: vinculação do perfil H9 com a plataforma Web H-PMI;
- Políticas: gestão de políticas de acesso a objetos delegados;
- Delegação: delegar acesso aos objetos pessoal presentes no H9;
- Logs: visualizar os registros de auditoria.



Figura 10-3 - Página de administração do Web H-PMI

### 10.3.5.3 Página de vinculação de perfil

A página de vinculação de perfil é uma das principais interfaces do sistema. Sem que o usuário a tenha acessado e vinculado o seu perfil no H9 com o Web H-PMI não é possível que o sistema tenha acesso aos seus dados e possa oferecer os demais serviços.

Nesta tela está encapsulado o processo de autenticação e armazenamento de **token AuthSub**. Através dela, o usuário é solicitado a vincular seus dados armazenados no H9 com o Web H-PMI. Assim que esta vinculação é efetuada, é salvo ou atualizado o token de acesso aos dados para utilizações futuras.

O usuário pode revogar este token a qualquer momento através da página do H9.

Através das Figuras 10-4 a 10-7 é possível visualizar o processo de vinculação de perfil na plataforma.

Na Figura 10-4 é possível verificar a tela do Web H-PMI de “Vinculação de Perfil”, que fornece algumas informações iniciais e pede para o usuário clicar em “Vincular” caso deseje que seu perfil seja vinculado.



Figura 10-4 - Página de vinculação de perfil H9 com Web H-PMI

Após clicar, o usuário é enviado à página de autenticação do próprio Google (Figura 10-5). Neste ponto é necessário fornecer usuário e senha da conta do Google.

Ao autenticar corretamente, o usuário é levado à outra tela da empresa, agora do sistema H9. Este passo, mostrado na Figura 10-6 é a página oficial de vinculação de perfil. Caso o usuário deseje que seu perfil seja realmente vinculado, ele deve clicar em “*Yes, link my accounts*”.

O usuário, ao clicar neste **link**, automaticamente está aceitando os termos e condições do compartilhamento e disparará o redirecionamento de volta à página do Web H-PMI com um **token** como parâmetro. Utilizando as bibliotecas fornecidas pela Google é possível solicitar um **token** de longa duração, que poderá então ser armazenado e utilizado a posteriori.





Esta é a função que exibida na Figura 10-7.

## Google accounts

### Sign in to personalize your Google experience.

Google has more to offer when you sign in to your Google Account. You can customize pages, view recommendations, and get more relevant search results.

Sign in on the right or [create one for free](#) using just an email address and password you choose.

-  [Gmail](#)  
Get a fresh start with email that has less spam
-  [Web History](#)  
Access and manage your web activity from any computer
-  [iGoogle](#)  
Add news, games and more to the Google homepage
-  [Google Checkout](#)  
A faster, safer and more convenient way to shop online

Sign in to Weaver with your  
**Google Account**

Email: **igorh9teste@gmail.com**

Password:

[Can't access your account?](#)  
[Sign in as a different user](#)

**Don't have a Google Account?**  
[Create an account now](#)

©2010 Google - [Google Home](#) - [Terms of Service](#) - [Privacy Policy](#) - [Help](#)

**Figura 10-5 - Página de autenticação H9 para vinculação do perfil com Web H-PMI**

igorh9teste@gmail.com | [Help](#) | [Sign out](#)

**H9 development sandbox**  
**-- for developer testing**  
**only.**

### Confirm linking of accounts

You are preparing to give **localhost** ongoing access to read your **entire** profile and send information to it. If you decide to link accounts, your profile will continue to be shared with localhost unless you decide to unlink the accounts.

To unlink, just sign into Google Health and delete localhost from the list under "Settings > Profile name > Linked accounts".

**Select the profile you want localhost to link with:**

igorh9teste

Google Health won't allow localhost to read or send information unless you click "Yes, link my accounts" below. Google won't share your password or any other Google Accounts information with localhost.

©2009 Google [About Google Health](#) - [For partners](#) - [Google Health privacy policy](#) - [Terms of service](#) - [Google home](#)

**Figura 10-6 - Página de consentimento de vinculação do H9 com Web H-PMI**



**Figura 10-7 - Página do Web H-PMI informando do sucesso do processo de vinculação**

#### **10.3.5.4 Página de delegação**

A página de delegação foi desenvolvida a fim de permitir aos usuários do Web H-PMI a possibilidade de compartilhar um ou mais objetos de seu perfil no Google Health para serem acessados através da página de visualização de Prontuário do próprio Web H-PMI, ou através do **Web service** disponibilizado, processo previsto no H-PMI como Delegação Direta.

Ela possibilita também uma visão geral das delegações efetuadas e uma gestão agrupada de tais operações.

Como a estrutura de Controle de Acesso Baseado em Papéis (CABP) não está visível ao usuário, é implementado o Controle de Acesso Baseado em Atributos (CABA) (Yuan e Tong, 2005), que permite a vinculação de determinada política de acesso a algum usuário que tenha um atributo pré-determinado.

Para que isto seja possível, cada usuário possui um identificador único, que será usado como chave para o processo de delegação e identificação.

A página está organizada a fim de guiar o usuário no processo de delegação, sendo a primeira página exibida ao visitar o menu “Delegação” a que mostra um

menu com a listagem dos usuários cadastrados na plataforma do Web H-PMI (Figura 10-8).



The screenshot displays the 'Delegação' (Delegation) menu in the Web H-PMI system. The page header includes the user name 'Igor Vitorio Custodio' and a 'Sair' (Logout) button. The navigation menu contains 'Prontuário', 'Vinculação de Perfil', 'Políticas', 'Delegação', and 'Logs'. The main content area is titled 'Usuários' and lists several users with corresponding 'Delegar', 'Visualizar', and 'Revogar' (Revoke) buttons.

Usuários	Delegar	Visualizar	Revogar
Bart Simpsons	Delegar	Visualizar	Revogar
Teste da Silva	Delegar	Visualizar	Revogar
Placa da silva	Delegar	Visualizar	Revogar
Maria alice torres	Delegar	Visualizar	Revogar
xis pe te o	Delegar	Visualizar	Revogar
y da silva sauro	Delegar	Visualizar	Revogar

Powered by **Google health** beta

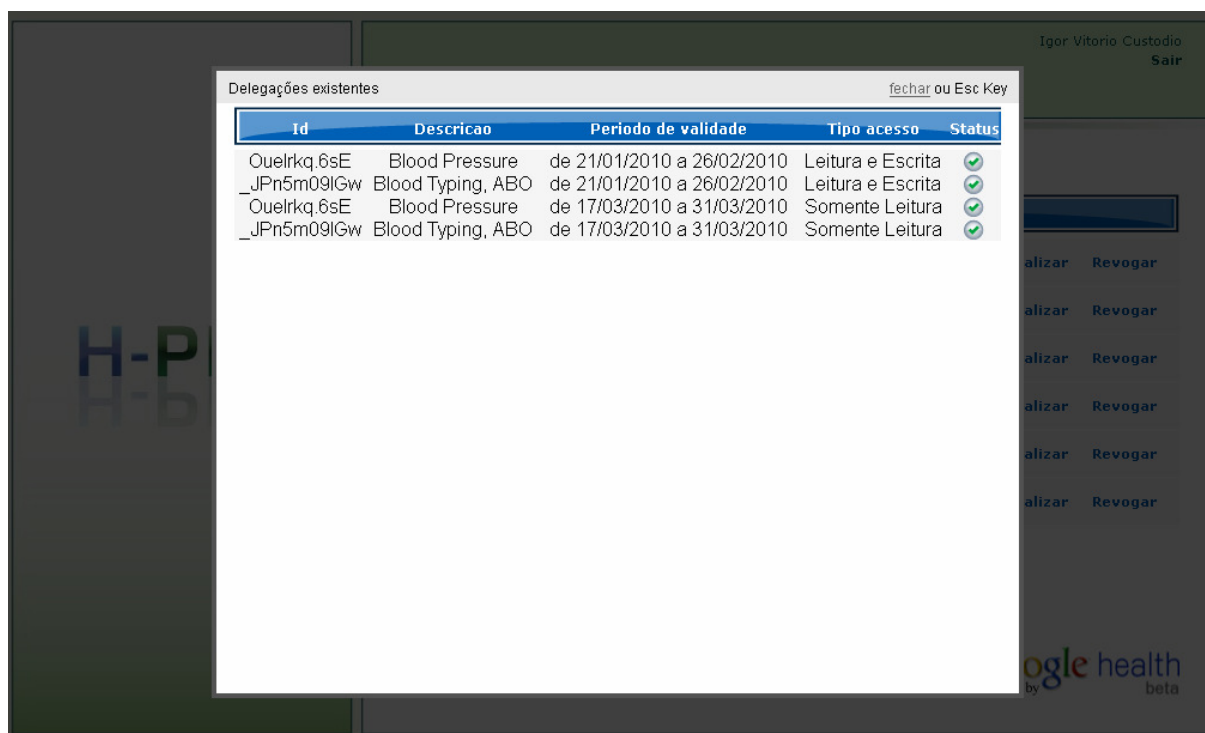
**Figura 10-8- Página do menu de delegação do Web H-PMI**

Através dela é possível iniciar um processo de delegação com um usuário, clicando em “Delegar”, visualizar as delegações existentes para aquele usuário, bem como os detalhes dela (Figura 10-9), ou revogar todas as delegações para determinado usuário.

Caso o usuário selecione a opção de delegar, será realizado um pedido de confirmação do procedimento; se estiver ciente do processo, o usuário é redirecionado à tela (Figura 10-10) em que são preenchidos os critérios de delegação:

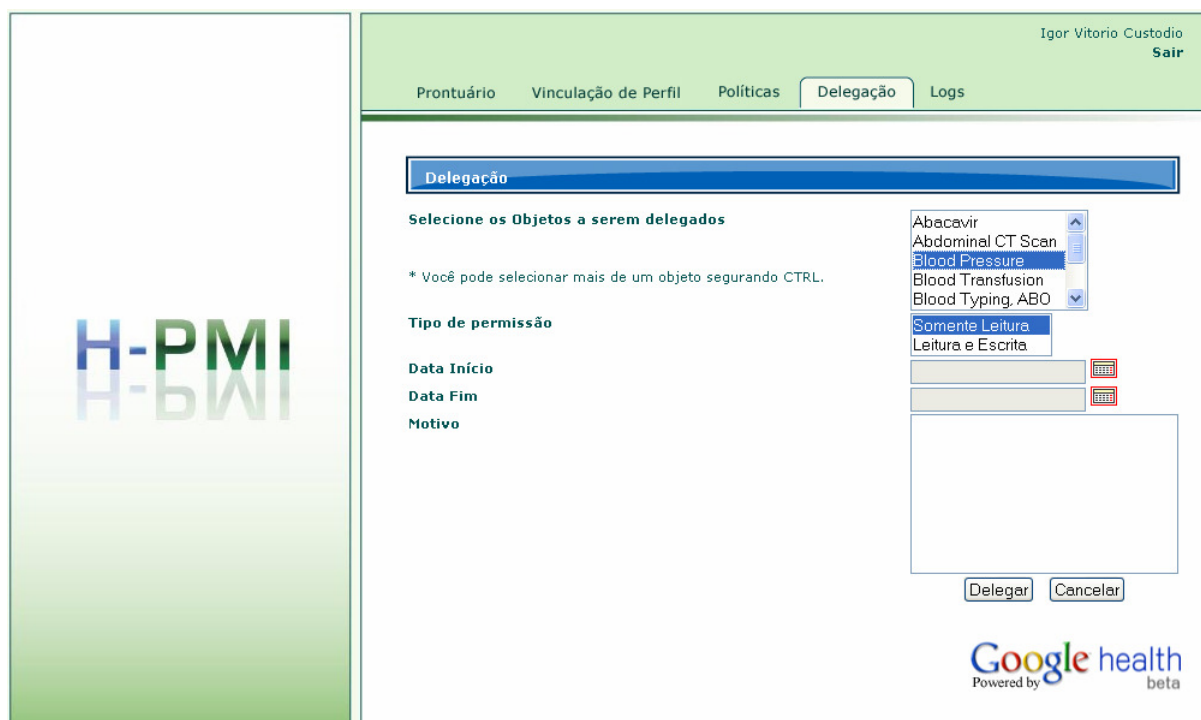
- Objetos a serem delegados;
- Tipo de permissão;
- Período de validade da delegação;
- Motivo da delegação.

Após o preenchimento destes campos, o usuário tem a opção de prosseguir com a delegação clicando sobre o botão “Delegar” (Figura 10-10) ou de abortar o procedimento, retornando a tela inicial, utilizando o botão “Cancelar”.



**Figura 10-9 - Página do menu de delegação do Web H-PMI ao se clicar sobre usuário que possui delegação**





**Figura 10-10 - Página do menu de delegação do Web H-PMI ao se clicar sobre opção Delegar**

Quando o usuário decide proceder a delegação, diversas operações são efetuadas a fim de possibilitar que este desejo do usuário seja transformado em políticas que serão aplicadas pelos sistemas do Web H-PMI.

Exemplo de processos executados:

- Criação das políticas XACML e armazenamento no SGBD;
- Registro de auditoria do processo.

Após as operações terem sido executadas com sucesso é apresentada uma tela que informa a finalização das operações ao usuário (Figura 10-11).



**Figura 10-11 - Página do menu de delegação do Web H-PMI sucesso na delegação**

A área de Delegação pode ser considerada um dos módulos do *Policy Administration Point* (PAP), já que é através dela que os usuários criam as políticas de acesso aos objetos.

#### **10.3.5.5 Página de políticas**

Outra parte do *Policy Administration Point* (PAP) é a página acessível através do menu “Políticas” (Figura 10-12).

Através desta tela é possível:

- Visualizar todas as políticas ativas;
- Verificar detalhes das políticas ativas;
- Verificar o XACML da política;
- Revogar política.

The screenshot displays the 'Políticas' menu in the Web H-PMI system. The user is logged in as 'Igor Vitorio Custodio' with a 'Sair' button. The navigation menu includes 'Prontuário', 'Vinculação de Perfil', 'Políticas', 'Delegação', and 'Logs'. The 'Políticas' section is active, showing a table of policies. The table has columns for policy ID, name, and actions (Detalhes, Visualizar, Revogar). The 'Google health beta' logo is visible in the bottom right corner.

Políticas		Nova Política		
w_DhALFK0Ls	Abacavir	Detalhes	Visualizar	Revogar
_JpN5m09IGw	Blood Typing, ABO	Detalhes	Visualizar	Revogar
Ouelrkq.6sE	Blood Pressure	Detalhes	Visualizar	Revogar
_JpN5m09IGw	Blood Typing, ABO	Detalhes	Visualizar	Revogar
Ouelrkq.6sE	Blood Pressure	Detalhes	Visualizar	Revogar
_JpN5m09IGw	Blood Typing, ABO	Detalhes	Visualizar	Revogar

Figura 10-12 - Página do menu de Políticas do Web H-PMI

Na Figura 10-12 verifica-se um exemplo da listagem de políticas ativas. Ao clicar em “Detalhes”, exibem-se os detalhes daquela política (Figura 10-13), como data da criação, motivo, receptor, validade.

Ao se seleccionar “Visualizar” é exibido o XACML correspondente à política visualizada (Figura 40).

Já com a opção “Revogar”, procede-se a revogação daquela política. Com isto, os usuários podem exercer um gerenciamento com alta granularidade das permissões de acesso aos objetos delegados.

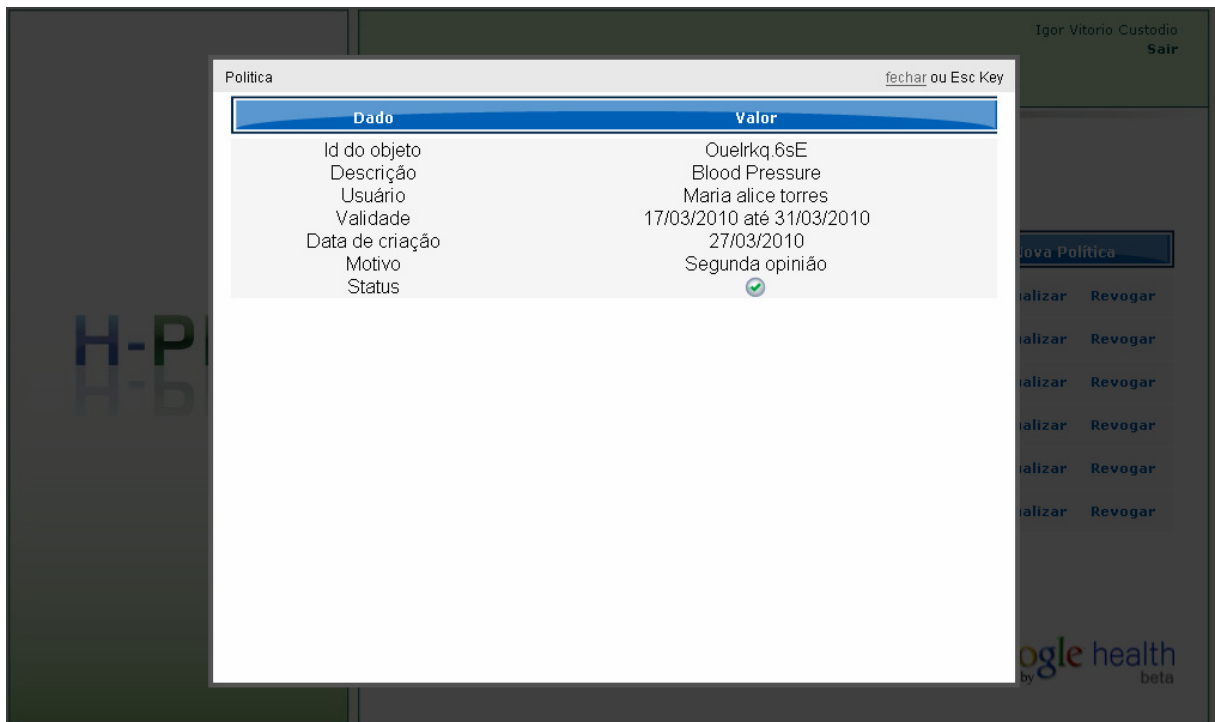


Figura 10-13 - Página do menu de Políticas do Web H-PMI ao se clicar "Detalhes"

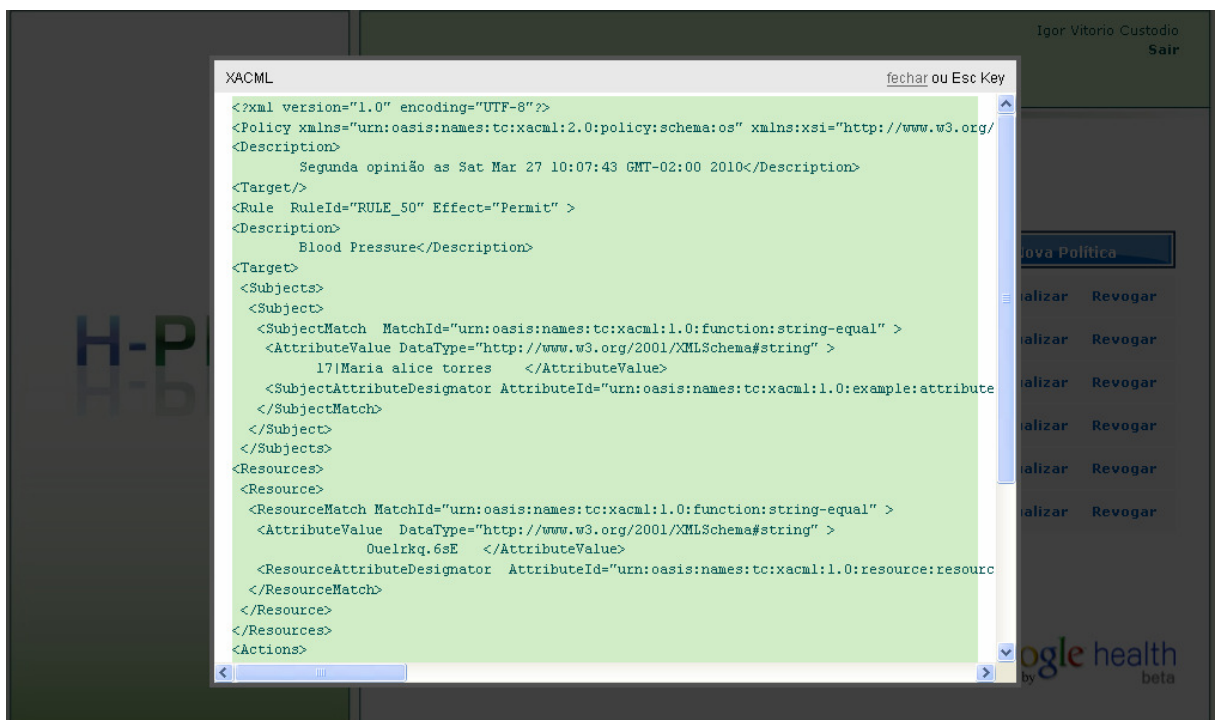


Figura 10-14 - Página do menu de Políticas do Web H-PMI ao se clicar "Visualizar"

### 10.3.5.6 Página de políticas

A página de prontuário é uma interface simplificada para a exibição dos registros presentes no ambiente do H9 (Figura 10-15).

Id	Tipo	Visualizar
w_DhALFK0Ls	Alerta	<a href="#">Detalhes</a> <a href="#">CCR</a>
GshdFtpEgFD	Procedimento	<a href="#">Detalhes</a> <a href="#">CCR</a>
Ouelrkq.6sE	Exame	<a href="#">Detalhes</a> <a href="#">CCR</a>
Sr5DpRuWUPE	Procedimento	<a href="#">Detalhes</a> <a href="#">CCR</a>
_jPn5m09lGw	Exame	<a href="#">Detalhes</a> <a href="#">CCR</a>
A_3OK.r5z0Y	Exame	<a href="#">Detalhes</a> <a href="#">CCR</a>
do94EQsRRc	Dados Pessoais	<a href="#">Detalhes</a> <a href="#">CCR</a>
_hGRRpKVahY	Dados Fisicos	<a href="#">Detalhes</a> <a href="#">CCR</a>
w_DhALFK0Ls	Alerta	<a href="#">Detalhes</a> <a href="#">CCR</a>
Ouelrkq.6sE	Exame	<a href="#">Detalhes</a> <a href="#">CCR</a>
_jPn5m09lGw	Exame	<a href="#">Detalhes</a> <a href="#">CCR</a>

Figura 10-15 - Página do menu de Prontuário do Web H-PMI

Utilizando esta interface, os usuários podem visualizar todos os seus registros no H9, como: exames, procedimentos, alertas, etc.

Além disto, são exibidos os registros delegados pertencentes a outros usuários.

Para a exibição destes registros é implementada toda a lógica do *Policy Enforcement Point* (PEP), do *Policy Decision Point* (PDP) e do *Policy Information Point* (PIP), bem como são efetuados os registros de auditoria.

O usuário pode também clicar na opção "Detalhes", exibindo dados do prontuário recebido diretamente do H9. Caso deseje verificar o CCR no formato XML (Figura 10-16), o usuário pode clicar na opção "CCR" (Figura 10-17).

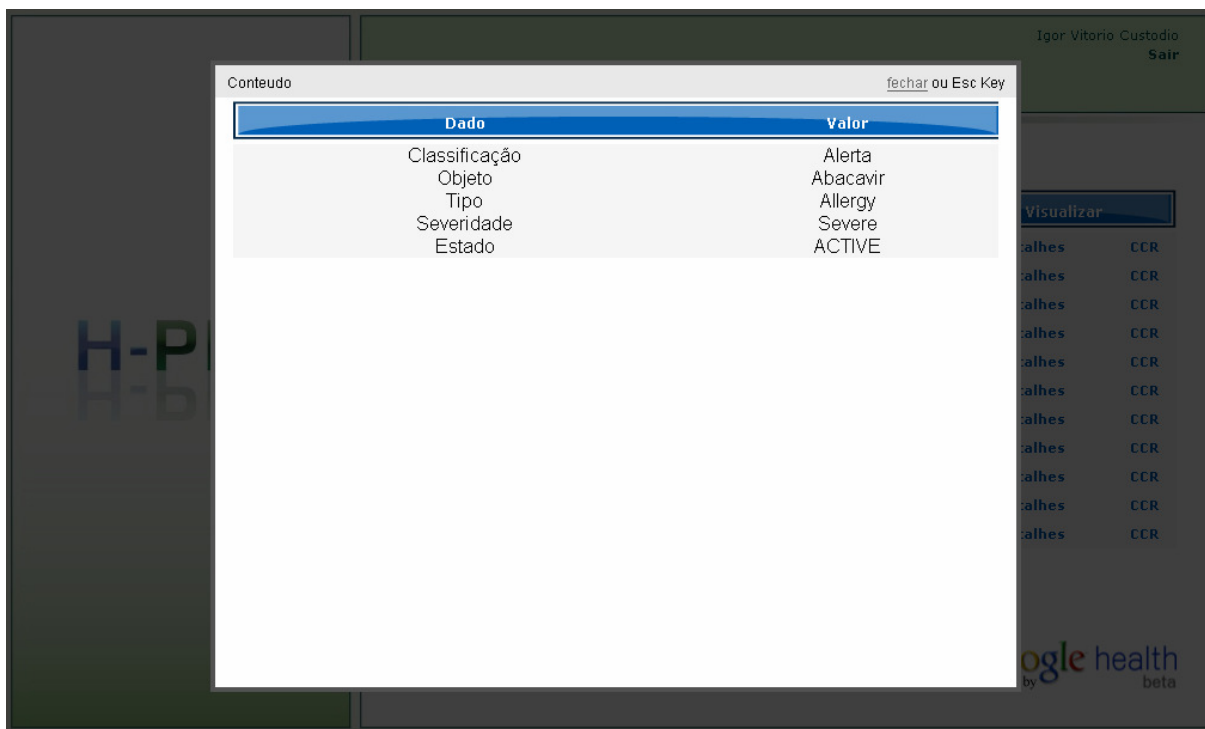


Figura 10-16 - Página do menu de Prontuário do Web H-PMI o se clicar "Detalhes"

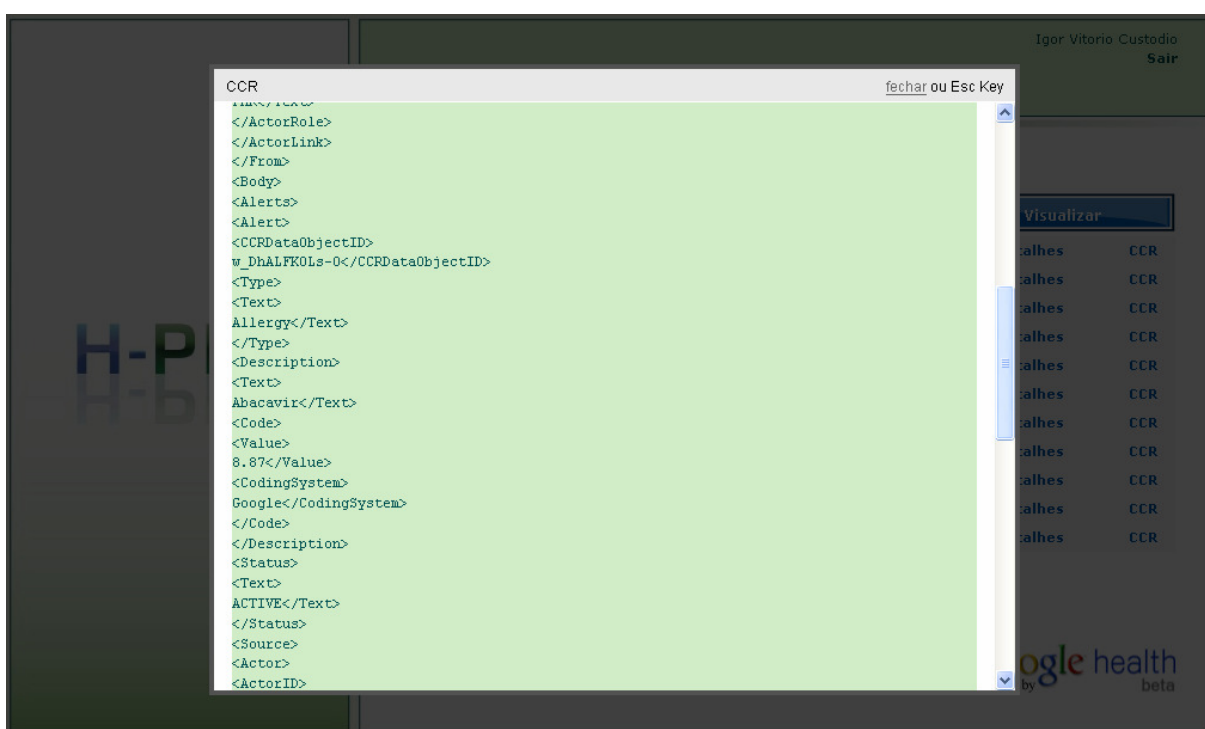


Figura 10-17 - Página do menu de Prontuário do Web H-PMI o se clicar "CCR"

### 10.3.5.7 Página de logs

A página de **logs** permite ao usuário visualizar todos os registros de auditoria realizados pela plataforma do Web H-PMI (Figura 10-18). Nela são exibidas todas as

atividades realizadas pelo usuário em questão ou realizadas utilizando algum objeto restrito do usuário.

Com esta funcionalidade, o usuário tem total conhecimento sobre as atividades executadas, quando foram executadas e quem as executou.

Data	Operação	Descrição	Autorização
Sun Jan 03 11:13:17 GMT-02:00 2010	Login	Login de Igor Vitorio Custodio na plataforma H-PMI IP: 127.0.0.1	✓
Sun Jan 03 11:13:23 GMT-02:00 2010	Acesso CCR	Acesso ao CCR de Igor Vitorio Custodio pela plataforma H-PMI IP: 127.0.0.1	✓
Sun Jan 03 11:13:23 GMT-02:00 2010	Acesso CCR	Acesso ao CCR de Igor Vitorio Custodio pela plataforma H-PMI IP: 127.0.0.1	✓
Sun Jan 03 11:13:23 GMT-02:00 2010	Acesso CCR	Acesso ao CCR de Igor Vitorio Custodio pela plataforma H-PMI IP: 127.0.0.1	✓
Sun Jan 03 11:13:23 GMT-02:00 2010	Acesso CCR	Acesso ao CCR de Igor Vitorio Custodio pela plataforma H-PMI IP: 127.0.0.1	✓
Sun Jan 03 11:13:23 GMT-02:00 2010	Acesso CCR	Acesso ao CCR de Igor Vitorio Custodio pela plataforma H-PMI IP: 127.0.0.1	✓
Sun Jan 03 11:13:24 GMT-02:00 2010	Acesso CCR Delegado	Acesso ao CCR de 12 pela plataforma H-PMI IP: 127.0.0.1	✓
Sun Jan 03 11:13:24 GMT-02:00 2010	Acesso CCR Delegado	Acesso ao CCR de 12 pela plataforma H-PMI IP: 127.0.0.1	✓

Figura 10-18 - Página do menu de Logs do Web H-PMI

#### 10.3.5.8 Web H-PMI Web service

O Web H-PMI também possui um **Web service** com uma única operação: getCCR. Com esta operação, sistemas de terceiros podem ter acesso aos dados armazenados no perfil do usuário que solicita ou que foi delegado o acesso (Figura 10-1).

O único parâmetro desta operação é o `id_usuario`. Esta identificação é única para cada cliente e deve ser fornecida a ele no momento de configuração e parametrização do ambiente dele.

A solicitação a este serviço deve seguir o indicado na especificação *WS-Security*, utilizando autenticação com certificados digitais X.509 com uma Autoridade Certificadora (AC) comum e confiável a ambos (cliente e servidor).

A informação de retorno do **Web service** é uma cadeia de caracteres contendo todos os CCRs aos quais o `id_usuario` tem acesso, ou uma mensagem de

erro, similar às informações visualizadas pelos usuários através da interface Web H-PMI de prontuário.

Este **Web service** implementa todas as lógicas de PEP, PDP, PIP e utiliza as regras em XACML criadas pela interface web do Web H-PMI (PAP). Além disto, ele registra traços de auditoria que podem ser visualizados pelos usuários afetados pelas operações através da página de **logs** do sistema.

O cumprimento de restrições (*enforcement*) é garantido uma vez que o acesso aos dados dos usuários presentes no H9 só pode ser realizado fornecendo-se o **token** de autorização, obtido durante a vinculação do perfil com o sistema Web H-PMI. Assim, caso algum usuário tente acessar diretamente os dados presentes na plataforma do Google, terá a permissão negada, pois o **token** de acesso nunca é fornecido para os clientes e somente está acessível através da plataforma do Web H-PMI.

### 10.3.6 Informações gerais de ambiente

Todo o Web H-PMI foi implementado em Java, utilizando-se a infraestrutura *Java Enterprise Edition* (JEE) através da utilização da tecnologia de *Java Server Pages* (JSP) e **Web services** estruturados e disponibilizados através do Servidor de Aplicações *GlassFish*<sup>10</sup> versão 2.

O Sistema de Gestão de Banco de Dados utilizado foi o PostgreSQL<sup>11</sup> versão 8.2 e o acesso e persistência dos dados realizados através da tecnologia *Java Persistence API*<sup>12</sup> (JPA).

Foi utilizado também como ferramenta de Desenvolvimento Rápido de Aplicação (*Rapid Application Development* (RAD)) Netbeans<sup>13</sup> versão 6.1.

Uma visão da integração entre os componentes utilizados pode ser vista na Figura 10-19.

---

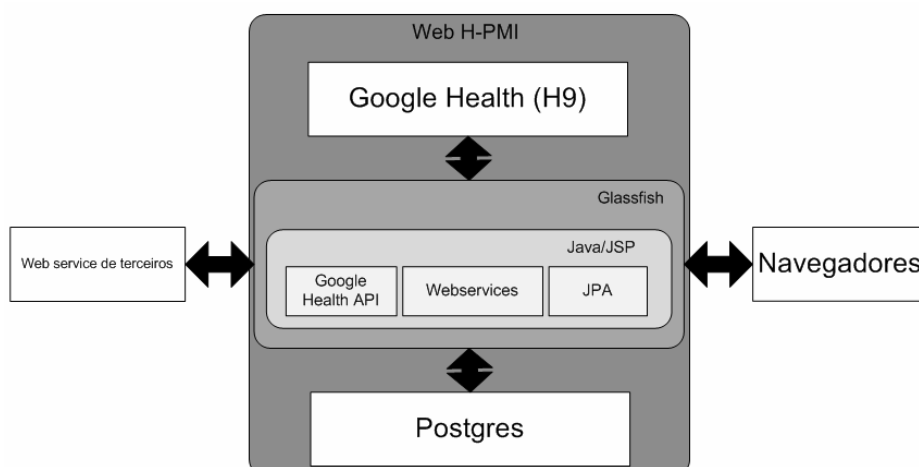
<sup>10</sup> Disponível em: <http://java.sun.com/javaee/community/glassfish/>

<sup>11</sup> Disponível em: <http://www.postgresql.org/>

<sup>12</sup> Disponível em: <http://java.sun.com/developer/technicalArticles/J2EE/jpa/>

<sup>13</sup> Disponível em: <http://www.netbeans.org>





**Figura 10-19: Integração entre as tecnologias utilizadas**

Como ferramenta de para a construção do diagrama de sequencia UML foi utilizada a ferramenta JUDE/Community<sup>14</sup> versão *Astah community* 6.0. Já o modelo do Banco de dados foi feito utilizando-se o Dia<sup>15</sup>.

O controle de versão foi feito utilizando-se o Sistema de Controle de Versão Concorrente e Distribuído (*Distributed Concurrent Versions System - DCVS*) Bazaar<sup>16</sup> versão 2.0.2.

Como sistema operacional base para os demais aplicativos foram utilizados dois, o Microsoft Windows XP SP2 e o Kubuntu 9.10, todos 64 bits.

A metodologia de desenvolvimento utilizada foi a Desenvolvimento Evolucionário (Sommerville, 2000), que especifica o andamento das fases de especificação, projeto e codificação e validação ocorrem simultaneamente, partindo-se de uma especificação preliminar, no caso a arquitetura proposta e evoluindo sua implementação, adicionando novas funcionalidades conforme vão evoluindo as fases de desenvolvimento.

Este método de desenvolvimento foi escolhido por ser recomendado para projetos onde há questões em aberto, de difícil solução, pois busca minimizar os riscos inerentes envolvidos (Philips, 2004).

<sup>14</sup> Disponível em: <http://jude.change-vision.com/jude-web/product/community.html>

<sup>15</sup> Disponível em: <http://live.gnome.org/Dia>

<sup>16</sup> Disponível em: <http://bazaar.canonical.com/en/>

## 10.4 Considerações Finais

O presente capítulo descreveu detalhadamente o ambiente web H-PMI, construído como prova de conceito para validar a arquitetura H-PMI proposta.

Definiram-se e demonstraram-se os módulos e as suas interfaces WWW constituintes da arquitetura implementada e suas inter-relações.

Um aspecto de destaque é a utilização do *Policy Enforcement Point* (PEP) como ponto de aplicação das regras e sua comunicação com o *Policy Decision Point* (PDP).

Apresentou-se também a utilização do *Policy Administration Point* (PAP), para a criação de políticas de acesso aos objetos, focando-se nos processos de delegação direta. Políticas estas, representadas em XACML e armazenadas no *Policy Information Point* (PIP).

Este capítulo descreveu também o módulo central do sistema, o PDP, responsável por decidir e autorizar, baseado nas informações enviadas pelo PDP e pelo PIP, o acesso ou não a determinado objeto.

Além disto, procurou-se demonstrar a aplicação e a integração destes módulos com o sistema Google Health no ambiente de testes, H9.

A interface **Web service** do Web H-PMI também foi apresentada, que possibilita a integração de tudo que foi implementado com outros sistemas independentes.

Por fim, apresentou-se as tecnologias utilizadas no desenvolvimento do Web H-PMI.

# Capítulo 11

## CONSIDERAÇÕES FINAIS

---

*Neste capítulo são apresentadas as conclusões e trabalhos futuros*

### 11.1 Considerações Finais

A Tecnologia da Informação aplicada aos Registros Eletrônicos em Saúde promove numerosas vantagens sobre a utilização em papel, porém trás outras preocupações como as maiores necessidades de segurança.

Com vista a prover mecanismos mais seguros de acesso aos dados em registros eletrônicos foi proposto o H-PMI, que se mostra flexível e seguro para uso em ambientes da área de saúde.

Através da proposta dos mecanismos de Delegações, direta e indireta, demonstram-se processos possíveis de serem implementados e que ampliam a segurança sem deixar de possibilitar a flexibilidade necessária para os sistemas da área de saúde.

Assim, com o a implantação do H-PMI é possível atingir um controle fino sobre os acessos aos registros eletrônicos em saúde.

A fim de exemplificar a implantação da arquitetura foi projetado, desenvolvido e testado um Sistema de Informação chamado Web H-PMI que aplica grande parte dos conceitos previstos na arquitetura proposta integrados a um Sistema de Informações médicas, no caso o H9 (ambiente de testes do Google Health).

Esta integração demonstra a aplicabilidade da arquitetura proposta em ambientes existentes agregando funcionalidades novas que podem ajudar a suprir necessidades de segurança e possibilitar o uso mais confiável por outros usuários.

Ou seja, ao implantar partes do H-PMI no sistema integrado com o Google Health foi possível prover maior controle sobre os dados lá armazenados, gerando inclusive informações de auditoria mais relevantes e completas, como definido pelo Manual de Certificação de Sistemas de Registros Eletrônicos em Saúde.

## 11.2 Trabalhos futuros

Como trabalho futuro a este trabalho verifica-se a possibilidade de integração de um sistema de análise de políticas XACML aplicadas ao Web H-PMI para a verificação de inconsistências de regras (Kolovski, Hendler *et al.*, 2007), através da utilização de lógica de primeira ordem, alertando aos usuários de inconsistências que podem levar o sistema a fornecer acesso a determinado objeto que não deveria ser acessado.

Outra funcionalidade que poderia ser trabalhada é a utilização de infraestrutura de Grade (Grids) para prover os mecanismos de autenticação, autorização aos objetos restritos utilizando-se como base a tecnologia de *Grid Services* (Ferreira, Thakore *et al.*, 2004), que são plenamente interoperáveis com **Web services**, transferindo-se assim a lógica de autorização para um ambiente distribuído e heterogêneo.

Pode-se também procurar a expansão das funcionalidades de segurança propostas aos sistemas como Google Docs<sup>17</sup> ou o sistema de Registro Eletrônico em Saúde da Microsoft, o *Microsoft HealthVault*<sup>18</sup>.

Por fim, é possível ampliar a pesquisa de mecanismos de delegações hierárquicas, bem como de outras formas de se executar a Delegação Indireta, mantendo-se o controle para evitar acessos indevidos.

---

<sup>17</sup> Disponível em: <http://docs.google.com/>

<sup>18</sup> Disponível em: <http://healthvault.com>

# REFERÊNCIAS BIBLIOGRÁFICAS

---

About Google Health. 2009 2009.

Anderson, A. Core and hierarchical role based access control (rbac) profile of xacml v2.0. OASIS2004-2005, p.23. 2005

Anderson, A. H. A comparison of two privacy policy languages: EPAL and XACML. Workshop On Secure Web Services. Alexandria, Virginia, USA ACM New York, NY, USA 2006, 2006. 53 - 60 p.

Ardagna, C. A., E. Damiani, *et al.* A Web Service Architecture for Enforcing Access Control Policies. First International Workshop on Views on Designing Complex Architectures (VODCA 2004) Itália. Janeiro, 2004. 47-62 p.

Atsm. E2369-05 Standard Specification for Continuity of Care Record (CCR). ASTM2005

AuthSub for Web Applications. 2009 2009.

Bacon, J., M. Lloyd, *et al.* Translating Role-Based Access Control Policy within Context. In: (Ed.). Lecture Notes in Computer Science: Springer Berlin / Heidelberg, v.1995, 2001. Translating Role-Based Access Control Policy within Context, p.107-119

Bacon, J. e K. Moody. Toward open, secure, widely distributed services. Communications of the ACM, v.45, n.6, 2002, p.59-64. 2002.

Bacon, J., K. Moody, *et al.* Access Control and Trust in the Use of Widely Distributed Services. IFIP/ACM International Conference on Distributed Systems Platforms Heidelberg: Springer-Verlag, 2001. 295-310 p.

\_\_\_\_\_. A model of OASIS role-based access control and its support for active security. ACM Transactions on Information and System Security (TISSEC), v.5, n.4, 2002, p.492-540. 2002.

Blaze, M., J. Feigenbaum, *et al.* The role of trust management in distributed systems security. In: (Ed.). Secure Internet programming: security issues for mobile and distributed objects. London, UK: Springer-Verlag, 1999. The role of trust management in distributed systems security, p.185-210

Bosworth, A. Developing Web Services. 17th International Conference on Data Engineering (ICDE'01), 2001, p.0477. 2001.

Burrows, M., M. Abadi, *et al.* A logic of authentication. ACM Transactions on Computer Systems (TOCS), v.8, n.1, 1990, p.18-36. 1990.

Conjunto Essencial de Informações do Prontuário para Integração da Informação em Saúde. PRC: PRC-1999-11-12 1999.

Curbera, F., M. Duftler, *et al.* Unraveling the Web Services Web: An Introduction to SOAP, WSDL, and UDDI. IEEE Internet Computing, v.6, p.86-93. 2002.

Etsi. TS 102 176-1: Eletronic Signatures and Infrastructures (ESI), algorithms and Parameters For Secure Electronic Signatures - Part 1: HAS functions and asymmetric algorithms. 2007. 2007

Farrell, S. e R. Housley. RFC: 3281 An Internet Attribute Certificate Profile for Authorization. 2002, p.40. 2002

Ferraiolo, D. F., R. Sandhu, *et al.* Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security (TISSEC), v.4, n.3, 2001, p.224-274. 2001.

Ferreira, L., V. Berstis, *et al.* Introduction to Grid Computing with Globus. 2003. 290 p.

Ferreira, L., A. Thakore, *et al.* Grid Services Programming and Application Enablement. 2004. 298 p.

Google Health Data API CCR Reference. 2009 2009.

The H9 Developer's Sandbox. 2009 2009.

Kolovski, V., J. Hendler, *et al.* Analyzing web access control policies. WWW '07: Proceedings of the 16th international conference on World Wide Web. Banff, Alberta, Canada, 2007. 677-686 p.

Leão, B. D. F., C. G. A. D. Costa, *et al.* Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES). Sbis/Cfm: 96 p. 2008.

Leite, F. R. M. Encontros Bibli. Universidade Federal de Santa Catarina: 53-70 p. 2006.

Linn, J. e M. Nyström. Attribute certification: an enabling technology for delegation and role-based controls in distributed environments. fourth ACM workshop on Role-based access control. Fairfax, Virginia, United States: ACM. 1999, 1999. 121-130 p.

Longstaff, J., M. Lockyer, *et al.* The tees confidentiality model: an authorisation model for identities and roles. Eighth ACM Symposium on Access Control Models and Technologies. Como, Italy: ACM. 2003, 2003. 125-133 p.

Marin, H. F., E. Massad, *et al.* Prontuário eletrônico do paciente: definições e conceitos. In: (Ed.). O prontuário eletrônico do paciente na assistência, informação e conhecimento médico. São Paulo: Organização Pan-Americana de Saúde, 2003. Prontuário eletrônico do paciente: definições e conceitos, p.213

Motta, G. H. M. B. Um modelo de autorização contextual para o controle de acesso ao prontuário eletrônico do paciente em ambientes abertos e distribuídos. Escola Politécnica, Universidade de São Paulo, São Paulo, 2003. 212 p.

Motta, G. H. M. B. e S. Furuie. MACA: Uma Ferramenta de Autorização e Controle de Acesso para o Prontuário Eletrônico de Pacientes. CBIS'2002 - VIII Congresso Brasileiro De Informática em Saúde. Natal-RN: 6 p. 2002.

Mykkänen, J., A. Riekkinen, *et al.* Designing web services in health information systems: From process to application level. International Journal of Medical Informatics, v.76, n.2-3, 2007, p.89-95. 2007.

Nadalin, A., C. Kaler, *et al.* Web Services Security: SOAP Message Security 1.0 (WS-Security 2004). OASIS2004, p.56. 2004

Neuman, B. C. e T. Ts'o. Kerberos: an authentication service for computer networks. Communications Magazine, IEEE IEEE. 32: 33-38 p. 1994.

OAuth for Web Applications. 2009 2009.

Oh, S. e S. Park. Enterprise Model as a Basis of Administration on Role-Based Access Control. CODAS '01: Third International Symposium on Cooperative Database Systems for Advanced Applications: IEEE Computer Society, 2001. 150-158 p.

Oppliger, R., G. Pernul, *et al.* Using Attribute Certificates to Implement Role-based Authorization and Access Controls. Sicherheit in Informationssystemen (SIS 2000), 2000. 169-184 p.

Papazoglou, M. P. Service -Oriented Computing: Concepts, Characteristics and Directions. The Fourth International Conference On Web Information Systems Engineering (Wise'03). Roma, Italia. 2003, 2003. 3-12 p.

Phillips, D. The Software Project Manager's Handbook: Principles That Work at Work: Wiley-IEEE Computer Society Pr. 2004. 504 p.

Power, D. J., E. A. Politou, *et al.* Securing web services for deployment in health grids. Future Generation Computer Systems, v.22, n.5, 2006, p.547-570. 2006.

Recommendations series X.509: Information Technology – Open Systems Interconnection - The Directory: Authentication Framework. International Telecommunication Union. 2001

Recordon, D. e D. Reed. OpenID 2.0: a platform for user-centric identity management. Second ACM Workshop on Digital Identity Management DIM'06. Alexandria, Virginia, USA: ACM, 2006. 11-16 p.

Resolução Conselho Federal de Medicina n. 1.638/2002a. Define prontuário médico e dá outras providências. Brasília. 2009 2002.

Resolução Conselho Federal de Medicina n. 1.639/2002b. Dispõe sobre as normas técnicas para uso de sistemas informatizados para guarda e manuseio do prontuário médico e dá outras providências. Brasília. 2009 2002.

Resolução Conselho Federal de Medicina n. 1.821/2007. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. 2009 2007.

Sandhu, R. S., E. J. Coyne, *et al.* Role-based access control models. Computer, v.29, n.2, p.38-47. 2006.

Sandhu, R. S. e P. Samarati. Access control: principle and practice. IEEE Communications Magazine, v.32, n.9, p.40-48. 1994.

Security and electronic signature standards. D. O. H. A. H. Services: Federal Register. 63: 43241-43280 p. 1998.

Sommerville, I. Software Engineering: Addison Wesley. 2000. 720 p.

Souza, J. N., C. C. Cunha, *et al.* Segurança nos processos de Autenticação e Autorização através de Certificados X.509. Sexto Simpósio Segurança Em Informática - SSI 2004. São José dos Campos/SP 2004.



Sucurovic, S. Implementing security in a distributed web-based EHCR. International Journal of Medical Informatics, v.76, n.5-6, p.491-496. 2007.

Waegemann, P. The Five Levels of Electronic Health Records. M.D.Computing, v.13, n.3,1996.

Wechsler, R., M. S. Anção, *et al.* A informática no consultório médico. Jornal de Pediatria, v.79, n.suppl.1, p.s3-s12. 2003.

Yuan, E. e J. Tong. Attributed Based Access Control (ABAC) for Web Services. IEEE International Conference on Web Services - ICWS 2005. Orlando, Florida, USA: IEEE, 2005. 569-578 p.

Zhang, L., G.-J. Ahn, *et al.* A role-based delegation framework for healthcare information systems. SACMAT '02: Seventh ACM Symposium on Access Control Models and Technologies. Monterey, California, USA: ACM, 2002. 125-134 p.

\_\_\_\_\_. A rule-based framework for role-based delegation and revocation. ACM Trans. Inf. Syst. Secur., v.6, n.3, p.404-441. 2003.

# Apêndice A

## 1. POLÍTICA EM XACML

---

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" xmlns:xsi=
"http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation=
"urn:oasis:names:tc:xacml:2.0:policy:schema:os access_control-xacml-2.0-policy-schema-os.xsd"
PolicyId="urn:oasis:names:tc:xacml:2.0:conformance-test:IIA002:policy" RuleCombiningAlgId=
"urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
<Description>
  A modified policy from the Draft XACML2.0 Conformance Test IIA002 Downloaded from:
  http://www.oasis-open.org/committees/download.php/14846/xacml2.0-ct-v.0.4.zip
</Description>
<Target/>
<Rule RuleId="urn:oasis:names:tc:xacml:2.0:conformance-test:IIA002:rule" Effect="Permit">
<Description>
  A subject with a role attribute of "Physician" can read specific Bart Simpson's CCR
  record.
</Description>
<Target>
<Subjects>
<Subject>
<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
  Physician
</AttributeValue>
<SubjectAttributeDesignator AttributeId=
"urn:oasis:names:tc:xacml:1.0:example:attribute:role"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</SubjectMatch>
</Subject>
</Subjects>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
  ha0zoLeLhQQBr61YhOuwXA0ue1rkq.6sE
</AttributeValue>
<ResourceAttributeDesignator AttributeId=
"urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>
</Policy>
```

## 2. EJEMPLO DE CONTINUITY OF CARE RECORD

```

<ContinuityOfCareRecord xmlns='urn:astm-org:CCR'>
  <CCRDocumentObjectID>ha0zoLeLhQQBr6iYhOuwXA0uelrkq.6sE</CCRDocumentObjectID>
  <Language>
    <Text>English</Text>
    <Code>
      <Value>en</Value>
      <CodingSystem>ISO-639-1</CodingSystem>
    </Code>
  </Language>
  <Version>V1.0</Version>
  <DateTime>
    <ExactDateTime>2009-10-27T18:38:57.029Z</ExactDateTime>
  </DateTime>
  <Patient>
    <ActorID>Google Health Profile</ActorID>
  </Patient>
  <From>
    <ActorLink>
      <ActorID>Google Health</ActorID>
      <ActorRole>
        <Text>PHR</Text>
      </ActorRole>
    </ActorLink>
  </From>
  <Body>
    <Results>
      <Result>
        <CCRDataObjectID>Ouelrkq.6sE-1</CCRDataObjectID>
        <Source>
          <Actor>
            <ActorID>bartsimpson@gmail.com</ActorID>
            <ActorRole>
              <Text>Patient</Text>
            </ActorRole>
          </Actor>
          <Actor>
            <ActorID>bartsimpson@gmail.com</ActorID>
            <ActorRole>
              <Text>Patient</Text>
            </ActorRole>
          </Actor>
        </Source>
        <Test>
          <CCRDataObjectID>Ouelrkq.6sE-0</CCRDataObjectID>
          <DateTime>
            <Type>
              <Text>Collection start date</Text>
            </Type>
            <ExactDateTime>2009-10-20</ExactDateTime>
          </DateTime>
          <Description>
            <Text>Blood Pressure</Text>
            <Code>
              <Value>36.1870</Value>
              <CodingSystem>Google</CodingSystem>
            </Code>
          </Description>
        </Test>
      </Result>
    </Results>
  </Body>
</ContinuityOfCareRecord>

```

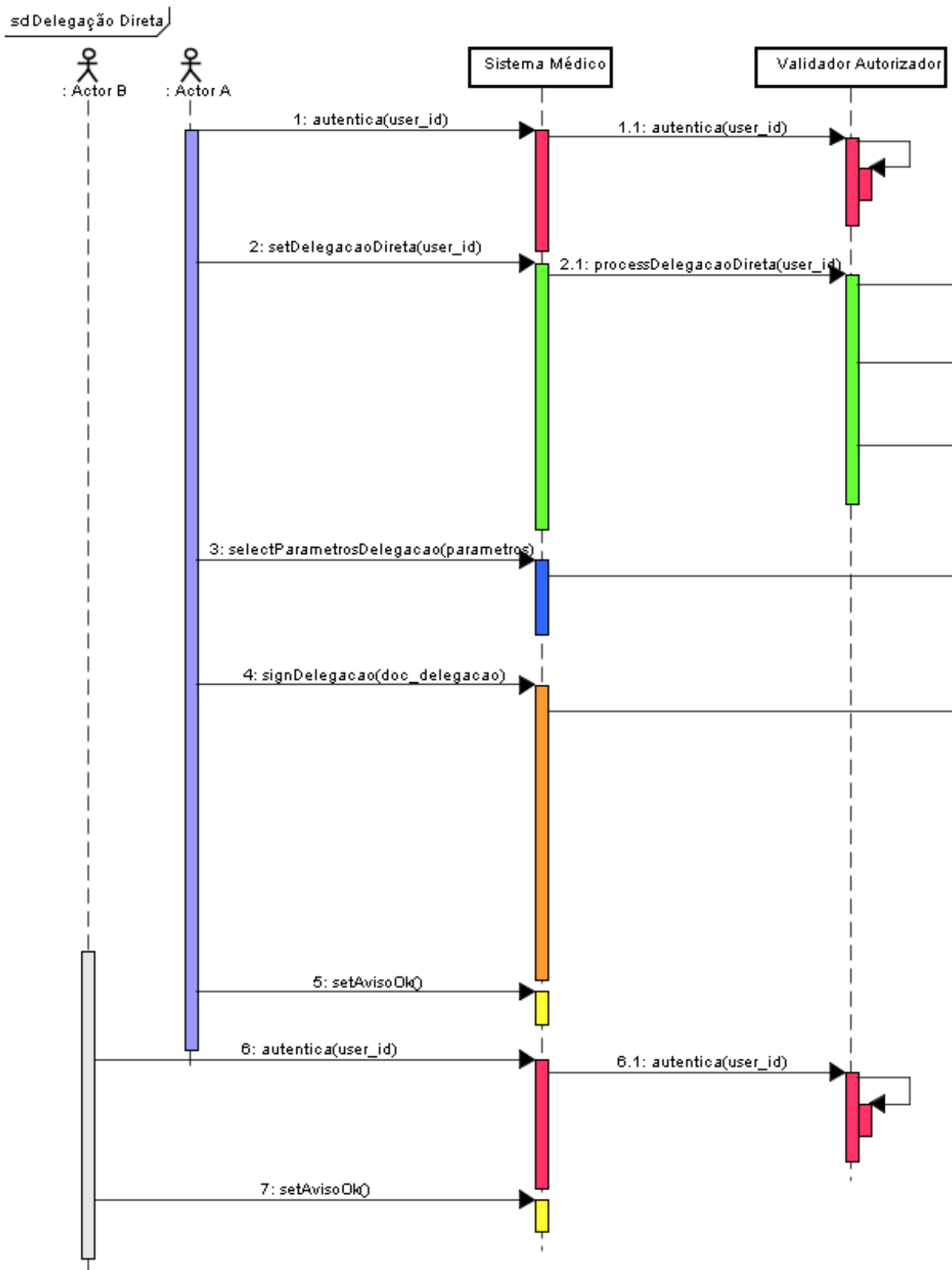
```
        <Source>
          <Actor>
            <ActorID>bartsimpson@gmail.com</ActorID>
            <ActorRole>
              <Text>Patient</Text>
            </ActorRole>
          </Actor>
        </Source>
      <TestResult>
        <Value>12/7</Value>
        <ResultSequencePosition>0</ResultSequencePosition>
      </TestResult>
    </Test>
  </Result>
</Results>
</Body>
<Actors>
  <Actor>
    <ActorObjectID>Google Health Profile</ActorObjectID>
    <Source>
      <Actor>
        <ActorID>bartsimpson@gmail.com</ActorID>
        <ActorRole>
          <Text>Patient</Text>
        </ActorRole>
      </Actor>
    </Source>
  </Actor>
</Actors>
</ContinuityOfCareRecord>
```

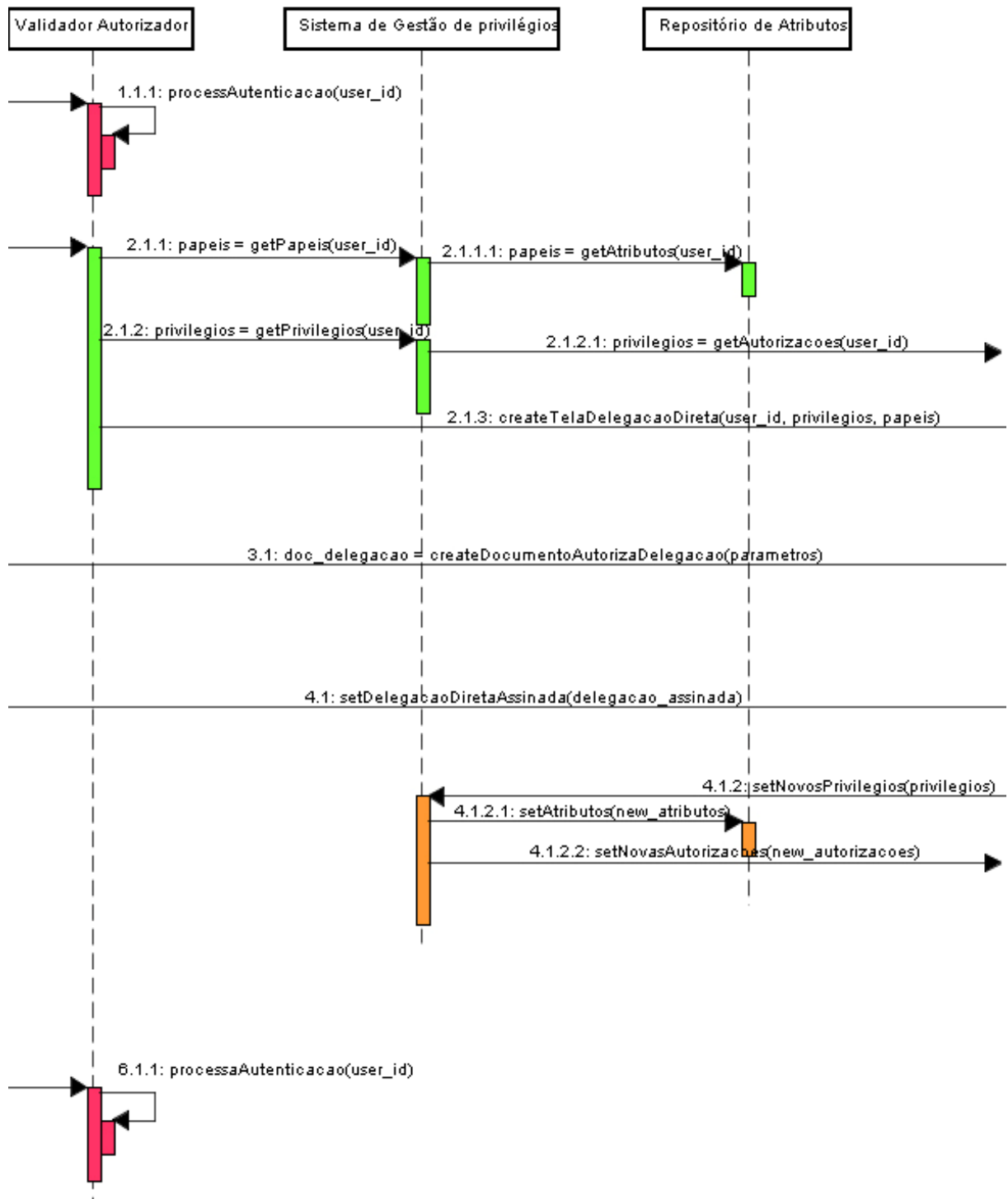
---

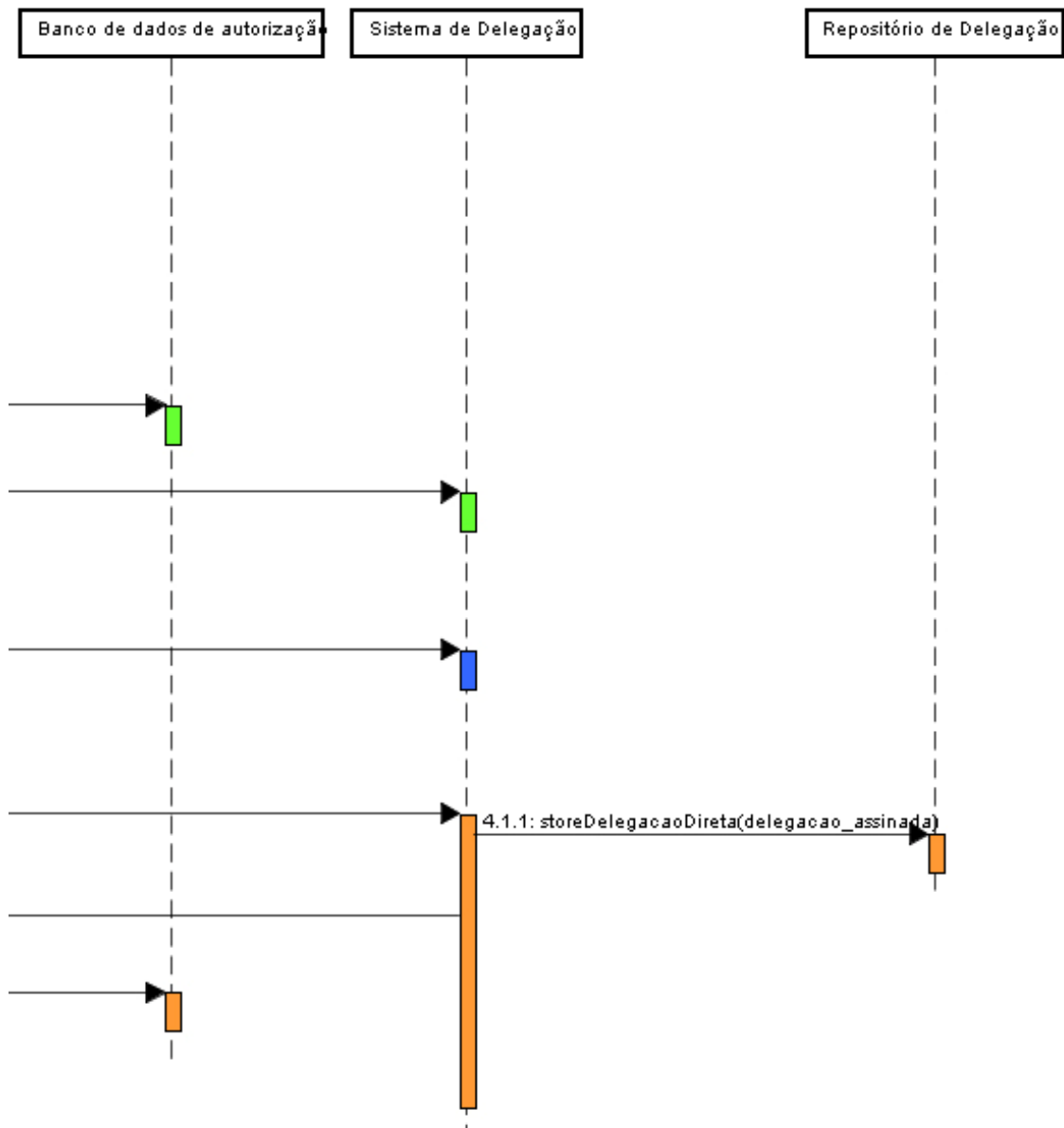
### **3. DIAGRAMA DE SEQUENCIA DO PROCESSO DE DELEGAÇÃO DIRETA**

---

---

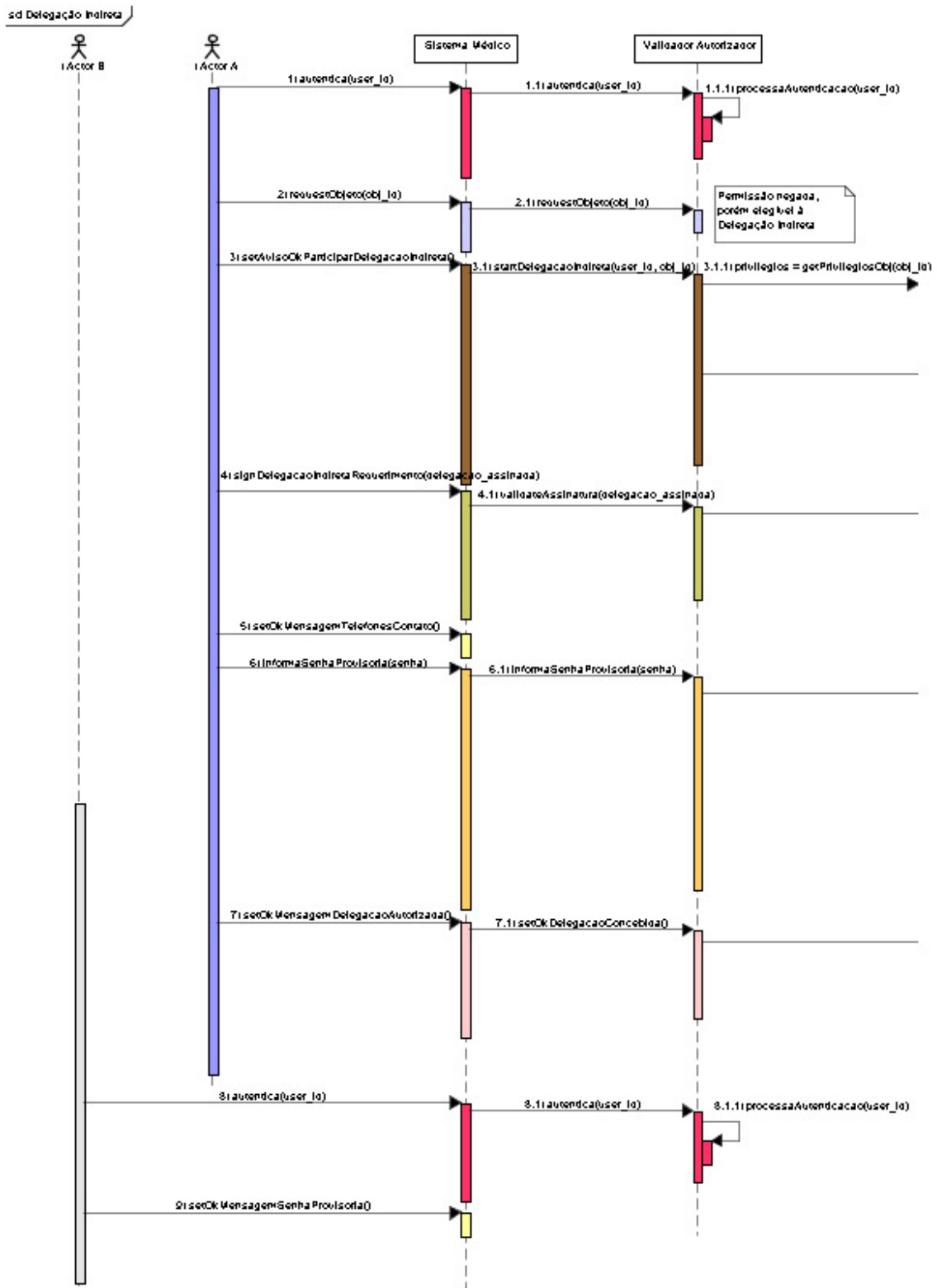


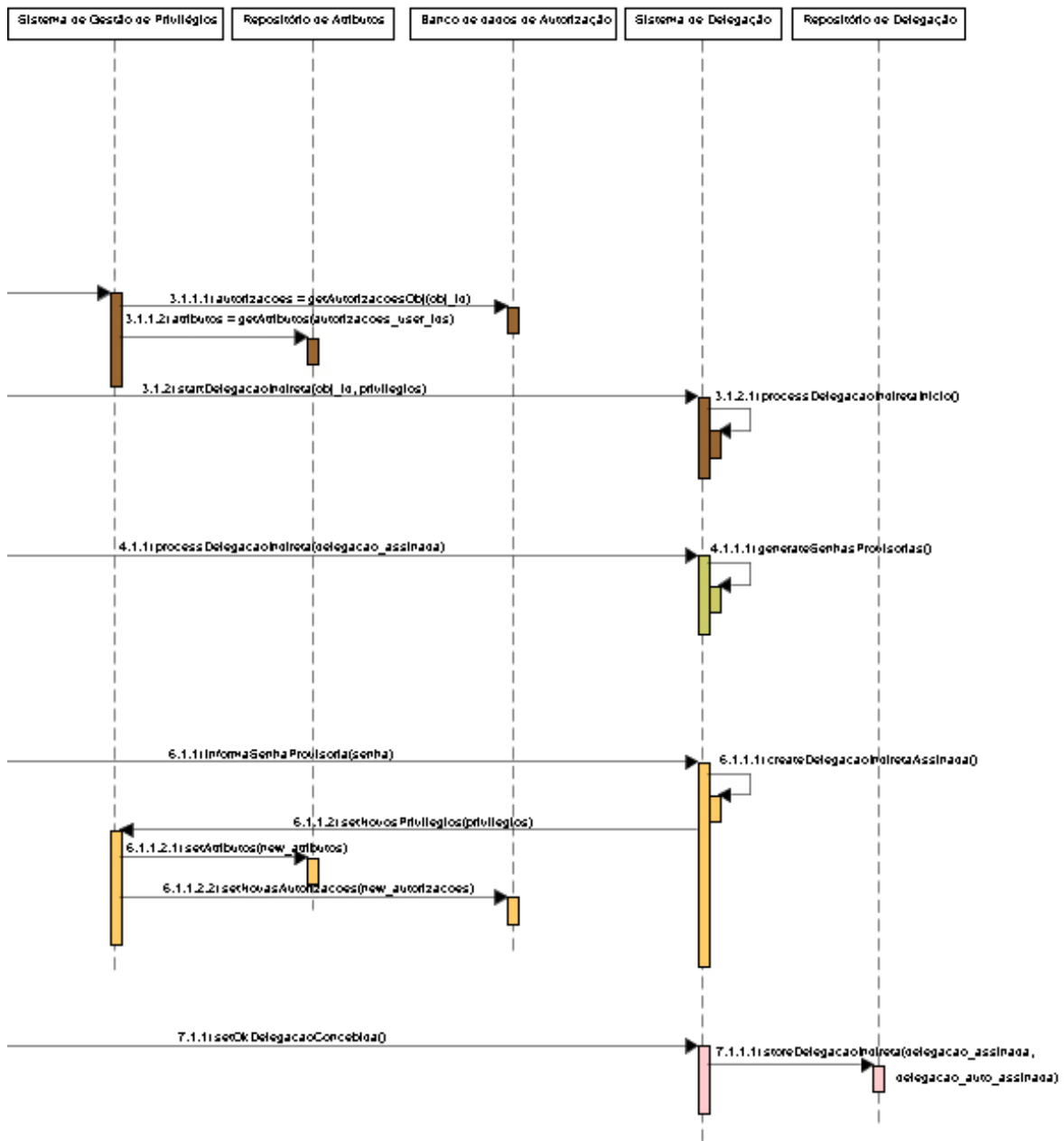






# 4. DIAGRAMA DE SEQUENCIA DO PROCESSO DE DELEGAÇÃO INDIRETA





# 5. DIAGRAMA DO BANCO DE DADOS

