Modelo Federado Distribuído para Autorização e Comunicação Multilateral Segura entre Instituições de Saúde

João F. M. Figueiredo[1], Gustavo H. M. B. Motta[1], Eduardo P. Serafim[1], Diego S. A. Pizzol[1], Rodrigo C. M. Duarte[1]

[1]Departamento de Informática – Universidade Federal da Paraíba (UFPB)
João Pessoa – PB – Brasil

{joaomatosf, gustavo, eduardops, diegopizzol, rodrigo}@di.ufpb.br

Abstract. *This paper proposes a model of network and distributed application capable of satisfy the security needs required for clinical information systems as demanded by the Federal Council of Medicine - CFM and recommendations of the Health Insurance Portability and Accountability Act - HIPAA. The architecture deals with a multilateral model, where different health institutions may utilize the resources collaboratively in a federative environment. We used technologies such as ContextuAl Access Model (MACA), Virtual Private Networks (VPN), Lightweight Directory Access Protocol (LDAP), smartcards, besides the development of modules for abstraction of the "all-online" model.*

Resumo. *Este trabalho propõe um modelo de rede e de aplicação distribuída, capaz de prover as necessidades de segurança requeridas para sistemas de informações clínicas, conforme exigências do Conselho Federal de Medicina – CFM e recomendações do Health Insurance Portability and Accountability Act – HIPAA. A arquitetura contempla um modelo multilateral, onde diferentes instituições de saúde possam usufruir colaborativamente dos recursos em um ambiente federativo. Foram utilizadas tecnologias de Modelo de Acesso ContextuAl (MACA), Redes Virtuais Privadas (VPN), Lightweight Directory Access Protocol (LDAP), smartcards, e outros mecanismos, além do desenvolvimento de módulos para abstração do modelo "tudo-online".*

1. Introdução

À medida que os sistemas clínicos avançam, a exemplo do Registro Eletrônico de Saúde *(Electronic Health Record – EHR)*, cresce a necessidade de integração destes com demais serviços hospitalares, tais como sistemas de comunicação e arquivamento de imagens (*PACS*) que se comunicam via protocolo no padrão *DICOM* (*Digital Imaging Communications in Medicice*), contribuindo na qualidade do atendimento ao paciente. Desta forma, o *EHR* viabiliza a troca de informações sensíveis entre profissionais de saúde [Chang 2004], possibilitando, inclusive, interações entre diferentes instituições por intermédio de redes de comunicação, a exemplo da internet.

Neste contexto, mecanismos que promovam a segurança, no que tange ao sigilo, autenticação, não-repúdio, controle de integridade e irretroatividade, são indispensáveis, além de medidas impostas pelos órgãos reguladores, para permitir e promover o uso imperativo da tecnologia nos registros eletrônicos de saúde, potencializando, assim, os benefícios advindos deste meio em detrimento do uso tradicional do registro em papel [CFM 2007]. Não obstante, novos desafios focam-se na possibilidade de distribuir e intercomunicar dados de pacientes de diferentes centros de saúde, a fim de possibilitar o

compartilhamento destes recursos de maneira federada [Putman 2001], onde cada instituição detém autonomia para decidir, contextualmente, suas próprias políticas de acesso e autorização, de maneira a não ir de encontro com as políticas das demais. Desta forma, tem-se um modelo cooperativo multilateral, capaz de localizar e recuperar, dinamicamente, dados de pacientes em um aglomerado de hospitais, independentes do seu local de origem.

Assim, este trabalho propõe um modelo adequado aos requisitos de segurança especificados pelo CFM, além de considerar uma gama de outros padrões e tecnologias, de forma a conceber uma camada de segurança para abstração da complexidade envolvida nas soluções mais emergentes de gerenciamento de identidades federadas que, em sua maioria, baseiam-se em especificações recentemente lançadas ou ainda em desenvolvimento [Camargo 2007]. Com isso, propicia-se a comunicação distribuída, conforme proposto, tendo como foco as fortes exigências de segurança particulares dos sistemas de informação em saúde.

2. Metodologia e Arquitetura Proposta

Para permitir a comunicação entre instituições de saúde distintas, de maneira que estas se comportem, virtualmente, como um único aglomerado de recursos, usufruiu-se de *VPNs*, com recursos adicionais, de modo a disponibilizar pontos de regulamentação de regras e processos, concebendo, desta forma, o órgão Federativo.

Neste enlace, os centros de saúde comunicar-se-ão por intermédio do órgão regulador, denotando flexibilidade quanto às relações de confiança, que se estabelecerão com cardinalidade simples de *um* para *um* entre o hospital e a federação e *um* para *n* entre a federação e os centros de saúde. Como consequência, hospitais federados, e seus respectivos sistemas clínicos, inserir-se-ão no domínio multilateral com baixa impedância (despendendo pouco esforço), através de um único elo virtual com a federação. Este relacionamento de confiança proporcioná-los-á dispor dos recursos de todos os demais, inerentemente submetidos às regras federativas. A Figura 1 esboça esta proposta, enquanto a Figura 2 exemplifica o fluxo da troca de dados por intermédio da federação.

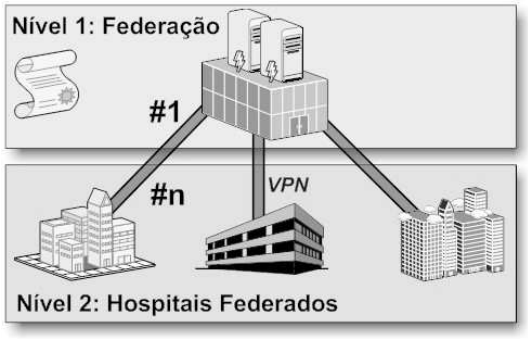

Figura 1. Enlaces entre hospitais e federação.

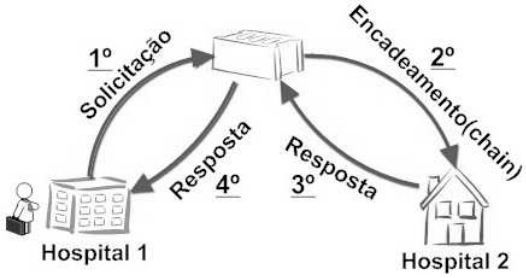

Figura 2. Fluxo do encadeamento de dados entre hospitais.

Percebe-se que os elos de comunicação, por intermediação da federação, concebem um modelo análogo a uma topologia de rede Parcialmente Ligada [Tanenbaum 2003], embora com custo simples de uma rede ponto-a-ponto.

Uma notável vantagem deste modelo é que cada órgão federado terá autonomia para definir suas próprias políticas de relacionamentos externos, com as quais

determinará as permissões de acesso aos recursos clínicos com base nos papeis dos usuários [Ferraiolo 2003], bem como no contexto do momento da solicitação [Motta 2002]. A exemplo cita-se a situação onde um médico precise resgatar informações do *RHE*, porém de um segundo hospital, onde não desfruta de vínculo. A autorização para o acesso será determinada pela permissão do papel médico externo na instituição detentora do recurso, que poderá, por padrão, negar o acesso em situações rotineiras, porém autorizá-lo se o médico externo, na sua instituição de origem, encontre-se em uma sala de cirurgia, caracterizando um contexto emergencial. Este recurso é atingível por meio do *MACA* [Motta 2002], que sofrerá customizações, seja diretamente ou por intermédio de uma camada de software externa, tendo em vista adaptá-lo para o contexto federativo.

O serviço de diretórios *LDAP*, requerido pelo *MACA*, assumirá a característica de diretórios distribuídos com recurso de encadeamento automático. Isto promoverá a abstração para as camadas superiores da distribuição física dos recursos. Chaves públicas e privadas de pacientes e de profissionais de saúde estarão acessíveis, respectivamente, na árvore de diretórios e em *smartcards*/*tokens*. Ressalta-se que as chaves públicas hão de compor certificados digitais devidamente assinados por uma Autoridade Certificadora reconhecida [MP 2200-2/2001]. Os *smartcards*/*tokens* hão de oferecer segurança máxima para à proteção das chaves privadas.

O uso destes mecanismos de criptografia proporcionará maior flexibilidade no cenário de *RHEs*, possibilitando autenticação segura, protocolação, assinatura digital e inserção de timbre de tempo. Logo, atingem-se os requisitos de autenticação, sigilo, integridade, não-repúdio e irretroatividade, conferindo validade jurídica aos documentos digitais [CFM 2007]. Ao prescrever, por exemplo, um profissional de saúde deverá fornecer o seu *smartcard*/*token* a fim de assinar o resumo (*hash*) do documento com sua chave privada, a qual é conhecida apenas pelo seu dispositivo de segurança. Além da assinatura do resumo, também será agregado o timbre de tempo assinado. Em outra ocasião, um paciente poderá fornecer o seu dispositivo de segurança para autorizar o profissional de saúde a resgatar o seu *EHR* de outro hospital que o negava acesso. Isso é possível uma vez que a chave pública do paciente encontra-se no serviço de diretórios distribuído, garantindo a sua autenticação em qualquer dos enlaces federativos.

A descentralização da federação, o órgão regulador, é outro fator crítico que deve ser assegurado. Sua distribuição física irá contribuir para redução da sobrecarga em um único ponto e elevará a eficiência entre as relações de confiança [Figueiredo 2008]. Um modelo que permita a delegação física da infra-estrutura federativa, de maneira a possibilitar disponibilizá-la arbitrariamente em quaisquer hospitais que assim desejem, é de propriedade essencial no cenário multilateral. A Figura 3 ilustra a arquitetura que contempla este modelo, onde um nó da federação pode ser observado fisicamente em um hospital. A Figura 4 explana a topologia virtual em forma de grafo.

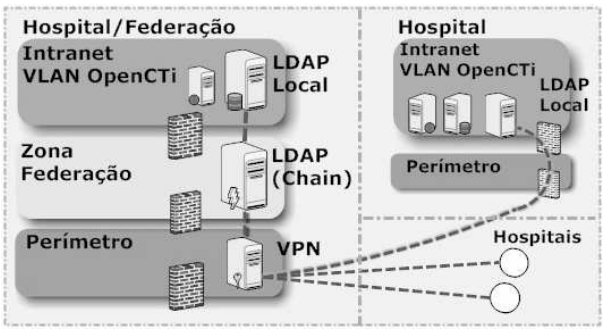

Figura 3. Modelo da arquitetura dos hospitais e federação distribuída.

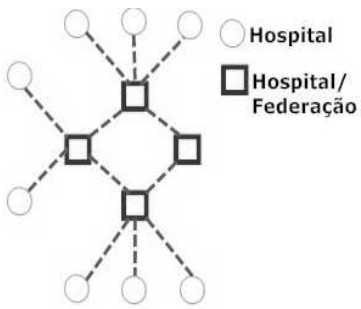

Figura 4. Grafo da topologia.

Salienta-se que os enlaces de comunicação entre os envolvidos têm custos desprezíveis por se tratarem de ligações virtuais (*VPNs*). Um plano de gerência de segurança pró-ativa, de perímetro e em profundidade, permitirá oferecer garantias quanto à segurança dos *hosts*, ainda que o ingresso de novas estações à federação se dê estocasticamente.

Servidores compatíveis com tecnologias *Network Access Protection – NAP* e *Netwok Policy Server – NPS* permitirão criar e impor, automaticamente, políticas de segurança aos *hosts* que ingressarem na *VPN* federativa. Os *hosts* serão inspecionados e avaliados, constantemente, de maneira que se possa decidir quanto a necessidade de isolamento e remediação, caso apresentem incompatibilidade com as políticas estabelecidas.

4. Discussão e perspectivas

Este modelo vem sendo desenvolvido no âmbito do projeto *OpenCTI*[1], visando dar suporte a sua implantação em hospitais regionais circunvizinhos. O modelo enfatiza a segurança, no que tange a alta-disponibilidade, integridade e sigilo das informações, além de alta flexibilidade, de maneira que viabilize sua implantação em centros de saúde arbitrariamente, tornando irrelevantes as barreiras geográficas e culturais. Todo modelo vem sendo desenvolvido sobre uma plataforma de virtualização, promovendo TI Verde e reduzindo os custos de implantação.

A separação de responsabilidades inter-institucionais, possibilitando localização e acesso aos dados no ambiente distribuído, é uma notável vantagem deste modelo. Pretende-se, também, aprofundar as pesquisas quanto à integração com o Sistema do Cartão Nacional de Saúde, a fim de se elevar os benefícios e almejando adequar-se a um padrão susceptível de implantação em todo território nacional.

Agradecimentos

Este trabalho recebeu apoio financeiro da FINEP (Financiadora de Estudos e Projetos).

Referências

Conselho Federal de Médicina – Brasil. (2007). “Resolução CFM Número 1.821/2007”, Brasília, DF: CFM.

Putman J. (2001) “Architecting with RM-ODP”, Prentice Hall.

Camargo, E., et al. (2007) “Autenticação e Autorização em Arquiteturas Orientadas a Serviço através de Identidades Federadas”, In Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. Belém.

Tanenbaum, A. S. (2003) “Redes de Computadores”, 4ª Ed. Rio de Janeiro: Elsevier.

Ferraiolo D. F., Kuhn, D. R., Chandramouli, R. (2003). “Role-Based Access Control”, Boston: Artech House.

Motta, G. H. M. B. and Furuie, S. S. (2002). Um modelo de autorização contextual para o controle de acesso baseado em papéis. In 22o Simpósio Brasileiro de Redes Computadores.

Medida Provisória 2200-2/01 – Brasil (2001). "Institui a intra-estrutura de chaves públicas Brasileira – ICP-BRASIL", Casa Civil, Brasil.

Figueiredo, J. F. M, et al. (2008) “Modelo conceitual de segurança para uma arquitetura multidomínio em telemedicine”, in XI Congresso Brasileiro de Informática em Saúde, Campos do Jordão. São Paulo.

[1]OpenCTI: Software de uma Central de Telemedicina para Apoio à Decisão Médica em Medicina Intensiva. Projeto financiado pela FINEP nº 01.08.0533.00.