JHI JOURNAL OF HEALTH INFORMATICS

Infraestrutura de segurança para comunicação, autenticação e autorização transparentes em hospitais federados

Security infrastructure for transparent communication, authentication and authorization in federated hospitals

Infraestructura de seguridad para la comunicación, autenticación y autorización transparentes en hospitales federados

João Filho Matos Figueiredo[1], Diego Santos de Andrade Pizzol[1], Luciano Carvalho de Medeiros Junior[2], Andrea Fernanda Fontes Bezerra[3], Gustavo Henrique Matos Bezerra Motta[4]

Descritores: Telemedicina; Sistemas Computadorizados de Registros Médicos; Segurança (computação)

RESUMO

A interação entre sistemas e profissionais de saúde de diferentes instituições, por meio da tecnologia, permite que recursos, tais como dados clínicos, transpassem barreiras geográficas e contribuam, desta forma, no cuidado ao paciente. Todavia, este ambiente se depara com os desafios da autenticação e autorização em ambientes distribuídos e autônomos e, ainda, com outras questões de segurança divididas nas seguintes áreas interligadas: sigilo, autenticação, disponibilidade, não-repúdio e controle de integridade. Assim, este trabalho define um modelo capaz de abstrair parte da complexidade na comunicação distribuída, entre centros de saúde, com ênfase na segurança, de maneira a oferecer uma base confiável e transparente para autenticação e autorização federada neste cenário. Padrões de Segurança para Serviços Web, como SAML e XACML, foram utilizados para promover a interoperabilidade e transposição de atributos dos usuários e das políticas de controle de acesso entre os Hospitais Federados. Redes Virtuais Privadas e o protocolo *Lightweight Directory Access* (LDAP) formaram a base para o estabelecimento dos elos de comunicação, de forma escalável e distribuída. A combinação dos padrões, protocolos e ferramentas possibilitou a elaboração de um modelo capaz de localizar dados de pacientes, espalhados por diversos hospitais, com tratamento dinâmico do controle de acesso as dados.

Keywords: Telemedicine; Medical Records Systems; Computerized; Computer Security

ABSTRACT

The interaction between health systems and professionals from different institutions, through technology, allows resources such as clinical data, to overcome geographical barriers and thus, contribute in patient care. However, this environment is faced with the challenges of authentication and authorization in distributed and autonomous environments, and also with security issues divided into the following interrelated areas: confidentiality, authentication, availability, non-repudiation and integrity control. So, this paper defines a model capable of abstracting part of the complexity in distributed communication between health centers, with emphasis on safety, to provide a reliable and transparent basis for authentication and federated authorization in this scenario. Security Standards for Web Services, such as SAML and XACML, were used to promote interoperability and implementation of attributes of users and access control policies among federal hospitals.Virtual Private Networks and the Lightweight Directory Access Protocol (LDAP) formed the basis for the establishment of communication links, in a scalable and distributed way. The union of these standards, protocols and tools made possible the development of a model able to locate patient data, scattered across several hospitals, treated with dynamic access control.

Descriptores: Telemedicina; Sistemas de Registros Médicos Computarizados; Seguridad Computacional

RESUMEN

La interacción entre los sistemas y profesionales de salud de diferentes instituciones, a través de la tecnología, permite que recursos como datos clínicos, superen las barreras geográficas y contribuan, por lo tanto en la atención al paciente. Sin embargo, este ambiente enfrenta a los desafíos de autenticación y autorización em ambientes distribuídos y autónomos, y también con otros problemas de seguridad divididas en las siguientes áreas interrelacionadas: la confidencialidad, la autenticación, la disponibilidad, no repudio y control de la integridad. Por lo tanto, el presente documento define un modelo capaz de abstrair parte de la complejidad en la comunicación distribuida entre los centros de salud, com énfasis en la seguridad con el fin de proporcionar una base confiable y transparente para la autenticación y la autorización federada en este escenario. Padrões de Seguridad para Servicios Web, SAML y XACML fueron utilizados para promover la interoperabilidad y la transposición de los atributos de los usuarios y las políticas de control de acceso entre los hospitales federales. Redes Virtuales Privadas y el Lightweight Directory Access Protocol (LDAP) sirvieron de base para el establecimiento de vínculos de comunicación, en una solución escalable y distribuida. La combinación de padrões, protocolos y herramientas hizo posible el desarrollo de un modelo capaz de localizar los datos del paciente, dispersos en vários hospitales, con tratamiento dinámico del control de acceso a los mismos.

[1] Mestrando em Ciência da Computação, Universidade Federal da Paraíba (UFPB), João Pessoa (PB) Brasil.
[2] Graduando em Ciência da Computação, Universidade Federal da Paraíba (UFPB), João Pessoa (PB) Brasil.
[3] Graduação em Sistemas para Internet, Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB), João Pessoa (PB) Brasil.
[4] Professor Adjunto, Departamento de Informática, Universidade Federal da Paraíba (UFPB), João Pessoa (PB) Brasil.

Autor Coorespondente: **João Filho Matos Figueiredo**
e-mail: **joaomatosf@di.ufpb.br**

Artigo recebido: **22/03/2011**
Aprovado: **12/06/2011**

INTRODUÇÃO

Com a tecnologia cada vez mais presente no processo de cuidado ao paciente, a exemplo dos Registros Eletrônicos em Saúde (RES) e dos Sistemas de Comunicação e Arquivamento de Imagens (PACS), tem crescido a demanda pelo compartilhamento colaborativo de recursos clínicos e da experiência dos profissionais de saúde, tendo em vista elevar os benefícios no atendimento ao paciente. Mediante a colaboração, profissionais de saúde podem resgatar importantes informações clínicas dos seus pacientes, distribuídas em diferentes centros de saúde, desfrutando de acesso prévio a diagnósticos, exames, tratamentos e demais dados relevantes para o contexto do cuidado atual ao paciente. Esta cooperação tem o potencial de elevar a qualidade no cumprimento dos cuidados à saúde, de auxiliar na tomada de decisão e de reduzir os seus custos. Neste ambiente, cresce, também, a demanda por meios íntegros e eficientes, que atendam as exigências de segurança impostas pelos órgãos reguladores, a fim de permitir e promover o uso da tecnologia em beneficio do paciente, porém resguardando a sua privacidade[1] e garantindo, desta forma, o uso adequado destes recursos. Entretanto, a interoperabilidade, principalmente no que tange aos processos de autenticação e autorização interdomínios, tem se mostrado um grande desafio, haja vista a diversidade cultural e tecnológica de cada domínio em particular.

Com a popularização do protocolo SOAP[2], diversas abordagens, com base nas suas especificações e outras associadas, têm surgido como propostas para os problemas da autenticação federada. Todavia, nos modelos mais emergentes[3-4], identifica-se um elevado grau de complexidade arquitetural, principalmente em consequência do emprego de um grande número de especificações, as quais ou foram recentemente lançadas ou ainda continuam em desenvolvimento[5]. Tais soluções, na grande maioria, estabelecem-se sobre os padrões XACML[6], SAML[7], WS-Security, WS-Policy, WS-Trust e WS-Federation que, em suma, definem formas adequadas de comunicar serviços para concepção de domínios de segurança interoperáveis, com portabilidade de políticas de acesso e credenciais de usuários. Entretanto, dado o vasto escopo das especificações, cresce, paralelamente, o risco de falhas críticas de segurança perdurarem, como demonstrado em[8], que revela uma falha crítica na solução de *Single Sign-On* (SSO) em serviços do *Google Apps*, em consequência de uma implementação simplificada do protocolo de SSO do SAML. O padrão SAML 2.0 tem conquistado espaço nas atuais soluções de SSO em serviços *Web* e no gerenciamento de identidades federadas, entretanto o seu uso em larga escala ainda se restringe a grandes instituições, a exemplo da *Sun Microsystems, Novell, Google e Max Planck Institute.*

Cabe salientar que essas abordagens mantêm o foco na transposição dos atributos de autenticação, porém em cenários incompatíveis com as particularidades e fortes exigências de segurança dos ambientes que lidam com informações sensíveis de saúde, como nos hospitais, pressupondo ainda que as relações de confiança entre eles estejam previamente estabelecidas. Ademais, não prevêem soluções para a localização e resgate dinâmico dos recursos distribuídos, a exemplo do RES, e seu respectivo controle de acesso com base no relacionamento "profissional de saúde/paciente". Ressalva-se que o termo hospital, no escopo desde trabalho, é colocado em um sentido amplo, podendo ser entendido como uma organização de saúde qualquer.

Diante dessas dificuldades, este trabalho propõe um modelo capaz de suportar os requisitos para concepção de domínios federados seguros para comunicação, autenticação e autorização entre hospitais, porém de maneira a abstrair a complexidade do cenário distribuído, principalmente através do uso da tecnologia de Redes Virtuais Privadas (VPNs), do protocolo *Lightweight Directory Access* (LDAP) e de especializações nos padrões *Security Assertion Markup Language* (SAML), *eXtensible Markup Language Access Control* (XACML), WS-Security e WS-Trust. Dada a particular combinação dessas e de outras tecnologias, construiu-se uma camada de abstração de segurança, de maneira a disponibilizar um ambiente virtual dos recursos distribuídos. Assim, as camadas superiores podem atuar nos aspectos de autorização local, enquanto o modelo trata das questões relativas à gerência de identidades federadas e à segurança. As relações de confiança estabelecer-se-ão dinamicamente, de forma transparente e escalável, através de um elemento mediador e de tecnologias de criptografia que possibilitarão a distribuição deste elo com respectiva delegação de responsabilidades[9].

METODOLOGIA E MODELO PROPOSTO

Na arquitetura do modelo, preocupou-se em prover um serviço adaptável a diferentes tecnologias de autorização nas camadas superiores, além de disponibilizar meios eficientes para localização de objetos distribuídos. Algumas características foram essenciais para proporcionar a confiabilidade neste contexto, como a definição de um escopo, restrito a organizações de saúde, auxiliado pelos seguintes *Security Patterns*: Canais Seguros, *Known Partners* (Parceiros Conhecidos), Zona Desmilitarizada (DMZ), *Protection Reverse Proxy, Integration Reverse Proxy e Intrusion Detection System*[10]. Este conjunto de padrões contribuiu na elaboração de um modelo especializado em segurança na comunicação e em perímetro.

Outras importantes restrições que norteiam a construção de sistemas distribuídos de alta confiabilidade são: 1) disponibilidade: o sistema deve funcionar mesmo em caso de desligamentos pontuais; 2) sigilo: a confidencialidade e a integridade dos dados devem ser asseguradas; 3) delegação: cada domínio deve ser capaz de gerenciar seus próprios recursos[11]. Observou-se, conjuntamente, a escalabilidade, a flexibilidade, a segurança dinâmica e a confiança mútua.

Com objetivo de garantir a interoperabilidade e a segurança multilateral, fez-se larga adoção de especificações de segurança para Serviços *Web,* introduzindo especializações a fim de alcançar as funcionalidades adequadas ao estudo de caso de organizações de saúde. Tais padrões formam a base para a concretização da autenticação e autorização transparentes dos profissionais de saúde nos diferentes hospitais pertencentes à federação. A seguir comenta-se sobre os principais padrões empregados:

SAML: é um padrão aberto e extensível, que oferece um mecanismo universal para transmissão de informações

relacionadas com segurança entre diversos segmentos de um sistema de controle de acesso. As informações são expressas em asserções de segurança, podendo ser de três tipos: 1) autenticação – afirma que um usuário foi autenticado por algum meio, em algum sistema. 2) autorização – indica direitos que um usuário detém sobre determinados recursos, normalmente com base em atributos. 3) atributo – afirma sobre detalhes do usuário, como papéis em um modelo RBAC[12], permissões locais de acesso, etc. O padrão também especifica protocolos de pedido/resposta de tais asserções, com base em XML, que podem ocorrer dentro de um modelo SOAP, sobre o protocolo *Hyper Text Transfer Protocol* (HTTP). Em outras palavras, uma asserção SAML pode ser entendida como um *ticket* que os usuários utilizam para comprovar sua identidade e seus direitos no ambiente distribuído;

XACML: é um padrão aberto, baseado em XML, que permite criar políticas complexas de controle de acesso, que derivam uma decisão de acesso com base na análise dos atributos do usuário, do recurso solicitado, da ação desejada sobre este recurso e do contexto da solicitação, tal como hora e local do pedido. Assim, esse padrão é suficientemente flexível para ambientes distribuídos, oferecendo um controle de acesso de granularidade fina. Em suas últimas versões, os padrões SAML 2.0 e XACML foram projetados para complementarem um ao outro. Por exemplo, políticas XACML podem especificar o que deve ser feito quando uma instituição receber asserções SAML, enquanto que, por sua vez, atributos de políticas XACML podem ser expressas por asserções SAML, tornando-se portáveis[13];

WS-Security: especifica como aplicar criptografia fim-a-fim nas mensagens SOAP, garantindo a confidencialidade e integridade destas. A criptografia das mensagens é efetuada através de *token profiles,* que descrevem como realizar o mapeamento entre diferentes tecnologias de autenticação (*Kerberos*, X.509, etc.), com objetivo de garantir a interoperabilidade entre várias tecnologias;

WS-Trust: fornece extensões para o WS-Security, definindo um serviço para emissão, troca, renovação e validação de *tokens* de segurança;

WS-Federation: fornece uma abstração dos padrões WS-Security e WS-Trust, de maneira a combiná-los e definir mecanismos para autenticação e autorização entre domínios.

Os requisitos citados, que permeiam os princípios de segurança em sistemas distribuídos, os *Security Patterns* e as respectivas estratégias e ferramentas utilizadas para conceber as bases do modelo, bem como a abstração do cenário, serão abordados na subseção 2.1. Na subseção 2.2 apresentar-se-á o modelo de autenticação e autorização no ambiente federado, com uso dos Padrões de Segurança para Serviços Web, os quais fornecerão os alicerces para concretização da interoperabilidade entre as organizações de saúde.

Requisitos e *Security Patterns*

Para fornecer um meio de consulta eficiente e acessível aos participantes, através do qual possam divulgar chaves públicas, certificados digitais, persistir objetos distribuídos, atributos, ou outras informações importantes relativas à segurança, elaborou-se uma árvore de diretórios distribuída. O protocolo LDAP oferece uma visão unificada dos dados em forma de árvore e é normalmente utilizado para compor diretórios altamente distribuídos, tendo como um dos principais objetivos a robustez das consultas e a segurança das informações[14]. Utilizou-se, portanto, uma implementação livre deste protocolo, o OpenLDAP, de maneira a se construir a estrutura de diretórios distribuída exposta na Figura 1.

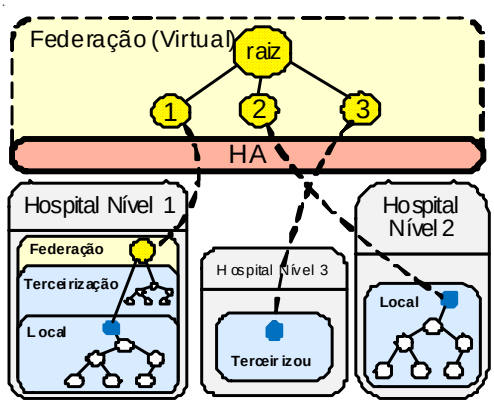

Figura 1 – Estrutura de diretórios distribuídos entre os hospitais federados

Observa-se na Figura 1 a utilização de uma tecnologia de *High-Availability* (HA), que exerce função de um *cluster* de altíssima disponibilidade. O *HA* permite que os clientes se comuniquem com um único endereço virtual que, por sua vez, referencia o servidor físico com maior disponibilidade naquele instante (*Integration Reverse Proxy*). Esse é mais um fator coadjuvante para os requisitos de disponibilidade e balanceamento de carga e tolerância a falhas.

A abordagem replicada do LDAP como serviço de nomes, disponibilizando informações que podem ser utilizadas para autenticação e autorização baseada em papéis[12] (*Role-Based Access Control* – RBAC) e em atributos (*Attribute-Based Access Control* – ABAC), é capaz de atender aos requisitos de disponibilidade, enquanto que a distribuição dos ramos do diretório, entre as diferentes instituições, permite a descentralização e delegação da gerência. O *Simple Authentication and Security Layer* (SASL), utilizado pelo LDAP, assegura a confidencialidade e integridade na comunicação, além de prover autenticação mútua entre servidores, clientes e clientes-servidores. Ainda, a API SASL fornece fácil integração com diversos mecanismos, como o *Kerberos e Radius,* fornecendo autenticação unificada, em sistemas heterogêneos, sendo esta mais uma recomendação de segurança para acesso ao RES. Mais detalhes observados na Figura 1 serão melhor colocados adiante.

Com uso de VPNs, estabeleceu-se a segurança dinâmica, que além de permitir a comunicação segura através de meios não confiáveis, como a internet, possibilitou a criação de um grande domínio virtual, interligando todos os hospitais federados por intermédio de uma terceira parte confiável (também virtual e distribuída). O domínio virtual é um fator relevante para a concepção final do modelo, o qual tornou praticável

que as partes usufruam e compartilhem, através deste, dos recursos de todos os participantes (RES, usuários, papéis, etc.), haja vista a integração dos ramos distribuídos da árvore de diretórios em uma única unidade lógica, onde cada instituição terá autonomia para definir as suas próprias políticas de controle de acesso. O mecanismo de encadeamento automático do LDAP introduziu flexibilidade quanto ao ingresso dos hospitais à federação, aos quais, ao estabelecerem relações de confiança com um único órgão regulador, disponibilizar-se-á comunicação e interação com todos os demais. A Figura 2 ilustra o fluxo de comunicação por meio do encadeamento automático e via VPNs.

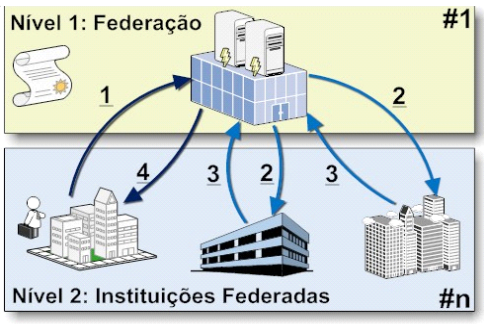

Figura 2 – Fluxo de comunicação por intermédio da Federação, via VPN

Na Figura 2, um médico, por exemplo, realiza a busca de um RES (1), que é replicada (concorrentemente) para os todos participantes (2), os quais respondem à federação (3) que, por fim, responde ao solicitante (4). Caso o hospital não disponha de link com a rede, apenas o nó local é consultado.

Com esta estratégia, em um ambiente com N Hospitais, esses comunicar-se-ão com um custo simples de N canais seguros, um para cada. Tais canais estabelecem-se dinamicamente durante o ingresso do hospital no domínio federativo. Em um modelo tradicional, cada participante precisaria de um elo com todos os demais, elevando o custo total de N para $(N^2 - N)/2$. Por exemplo, em termos quantitativos, para 100 hospitais haverá 100 canais seguros (VPNs), enquanto que em abordagens clássicas esse número seria de 4.950 relacionamentos, o que tornaria a gerência das relações extremamente complexa.

Neste ambiente, clínicas menores que assim desejem, ou necessitem, podem terceirizar a infraestrutura de autenticação / autorização para outro hospital da federação, de maneira a usufruírem dos serviços em um ambiente de *Cloud Computing*. A complexidade de projetar, instalar, configurar, implantar e apoiar o sistema com recursos internos pode ser minimizada com este tipo de metodologia[15]. Desta forma, hospitais com maior disponibilidade de infraestrutura podem prover os serviços federativos (Zona Federação na Figura 3) e, ainda, os demais serviços, em nuvem, para os participantes que assim necessitem (Zona Terceirização na Figura 3).

A descentralização da federação (Zona Federação na Figura 3), de forma transparente, reduz a sobrecarga em um único ponto e eleva a eficiência entre as relações de confiança, correspondendo adequadamente ao modelo distribuído. Na camada de perímetro estão os padrões de segurança, com destaque para o Sistema de Detecção de Intrusão (IDS), *Firewalls* e serviços de VPN.

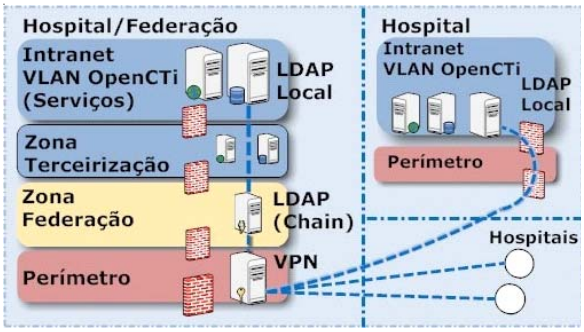

Figura 3 – Distribuição da federação e terceirização de infraestrutura

Um plano de gerência de segurança pró-ativa, de perímetro e em profundidade, permitirá oferecer garantias quanto à segurança no lado dos clientes, ainda que o ingresso destes à federação se dê estocasticamente. Servidores e clientes com tecnologias compatíveis com *Network Access Protection* (NAP) e *Network Policy Server* (NPS) agregarão proteção dinâmica aos *hosts* que tentem ingressar na rede Federativa. Os *hosts* serão avaliados com base nos critérios de integridade ditados pelo NPS, a fim de se decidir sobre a liberação de acesso à rede ou isolamento para possíveis remedições, a exemplo de atualizações críticas de segurança.

Padrões Para Interoperabilidade de Serviços Web

O Middleware de Autenticação e Controle de Acesso (MACA)[17], com uso de um módulo para suporte ao modelo aqui proposto, gerenciará a autenticação e autorização local, com base nos papéis dos usuários e no contexto da solicitação. Internamente usar-se-á asserções SAML para permitir a interoperabilidade entre diferentes tecnologias de autorização, aplicadas nas camadas superiores. Para isso, uma API padronizada proverá a interface de ligação entre as camadas, estendendo a tecnologia de autorização local para o ambiente distribuído. O encapsulamento da complexidade em um modelo especializado eleva a confiabilidade, eximindo esta dos usuários e, consequentemente, reduzindo o escopo sujeito a falhas humanas, entre outras vantagens provindas do reuso. Ressalta-se que para a completa eliminação do RES em papel, o modelo, nas camadas superiores, deve incorporar uma Infraestrutura de Chaves Públicas (ICP/PKI), sendo esta uma determinação legal do CFM que, com isso, confere validade jurídica aos documentos digitalmente assinados, desde que se estabeleça uma Autoridade Certificadora com base na raiz ICP-Brasil[16]. Entretanto, uma alternativa mais escalável, econômica e com portabilidade de políticas de autorização, porém que não possibilitará a eliminação do RES em papel (por questões legais), alcança-se com o Simple Public Key Infrastructure/Simple Distributed Security Infrastructure (SPKI/SDSI). Em síntese, a união dessas infraestruturas de chaves públicas resulta em um sistema de autenticação e autorização distribuída, o qual

define certificados de nomes e autorização, simplificando a concessão de permissões entre os principais[2] e isentando a necessidade de centralização em uma única raiz confiável.

Internamente à camada de abstração, por "baixo" do MACA, implantar-se-á os padrões que proverão a autenticação SSO e autorização dinâmica entre serviços de diferentes domínios. Uma interface padronizada realizará o mapeamento local, expressando permissões do modelo RBAC no modelo ABAC, de maneira a transpor os papéis dos usuários entre os diferentes domínios por meio das asserções SAML. Assim, pode-se aplicar políticas de controle de acesso complexas, construídas dinamicamente com base nas definições XACML de ambas as instituições envolvidas na requisição, bem como nos atributos do usuário, do recurso e no contexto. A Figura 4 ilustra este processo.

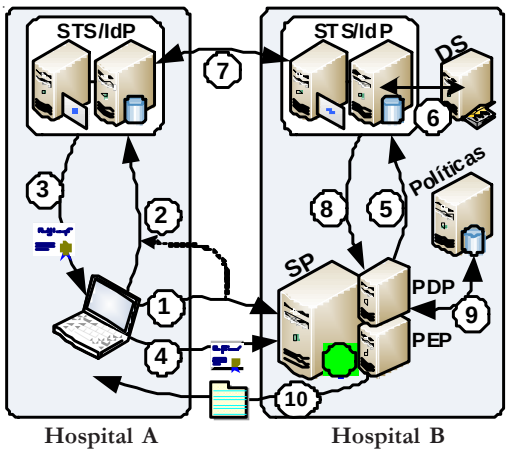

Figura 4 – Processo de autenticação SSO e autorização dinâmica no ambiente federado

Os passos de (1) a (4), na Figura 4, são o protocolo de pedido/resposta definido no *Perfil Web Browser* do padrão SSO SAML 2.0. Tal implementação está disponível na ferramenta OpenSAML. O elemento *Security Token Service* (STS) é definido pelo *WS-Trust* e tem função de emitir, trocar e validar as credenciais. A *WS-Federation* adiciona ao STS as funcionalidades de Provedor de Identidades (IdP), o qual é responsável por armazenar as credenciais dos usuários. Juntos, o STS/IdP realizam autenticação com respectiva emissão do *ticket*(asserção) com os atributos do usuário autenticado. Entretanto, no modelo aqui proposto, cada instituição tem o seu próprio STS/IdP. A comunicação entre estes elementos é realizada por meio dos canais seguros, enquanto o Serviço de Descoberta (DS) indica o caminho correto na árvore de diretórios onde as políticas e atributos necessários para uma dada negociação poderão ser resgatados. O Provedor de Serviço (SP) é o elemento que disponibiliza os recursos, como o RES dos pacientes. O XACML define o *Policy Decision Point* (PDP) e o *Policy Enforcement Point* (PEP), onde são feitas trocas pedido/resposta para acesso aos recursos. O PEP delega a decisão sobre um acesso ao PDP, que por sua vez recorre às autoridades de atributos (STS/IdP), obtém as políticas locais e, por fim, decide se aceita ou nega o acesso, informando sua resposta ao PEP. O PEP então cumpre a decisão do PDP, liberando ou negando o acesso ao recurso solicitado.

Na Figura 4, após ocorrer o SSO (passos 1 a 4), o serviço requisitado pelo usuário pode precisar de mais atributos para decidir quanto à liberação do acesso. Assim, o PDP recorre ao STS/IdP local (5), e este, por sua vez, consulta o DS (6) a fim de determinar onde os atributos podem ser encontrados. Com isso, o STS/IdP solicita os atributos do usuário ao STS/IdP seu domínio (7). Ao obter os dados necessários, o STS/IdP os devolve ao PDP (8), que já pode consultar as políticas locais (9), onde irá cruzar os dados(atributos do usuário, recurso, políticas XACML, contexto e etc.) e finalmente aplicar o controle de acesso sobre a solicitação. Por fim, o PEP cumpre a política, liberando ou negado o recurso solicitado (10).

DISCUSSÃO E CONCLUSÃO

A combinação e a especialização dos padrões em questão proporcionam às facilidades SSO, onde médicos e outros profissionais de saúde podem se autenticar uma única vez no seu próprio domínio e, com essa autenticação, localizar e solicitar acesso às informações disponíveis nos outros hospitais. Todo o processo é realizado de forma transparente ao usuário e ao desenvolvedor da aplicação. A decisão de autorização é determinada com base nos atributos do solicitante (profissional de saúde), nos atributos do recurso (RES), no relacionamento médico/paciente (também expresso em forma de atributos), no contexto do ambiente (hora, local) e, por fim, nas políticas locais do hospital fiel depositário do recurso e do hospital onde o usuário mantém um papel institucional. Todos esses atributos são combinados para, por fim, uma política ser atribuída.

Este trabalho vem sendo desenvolvido no âmbito do projeto OpenCTI*, visando dar suporte a sua implantação em hospitais regionais no Estado da Paraíba. Atualmente um protótipo segue evoluindo, juntamente com o OpenCTI, que já desfruta da autenticação com base no modelo RBAC e está em funcionamento em um ambiente distribuído, via VPN, entre o Hospital Universitário Lauro Wanderley e o Laboratório de Arquitetura e Sistemas de Software, ambos na Universidade Federal da Paraíba (UFPB). O uso de bibliotecas livres, que implementam boa parte das especificações abordadas, está sendo avaliado, de maneira que se possa usufruir de modelos já consagrados, apenas especializando-os para o nosso contexto. A infraestrutura foi montada sobre uma plataforma de virtualização, contribuindo para redução de custos capitais, ao mesmo tempo em que introduziu importantes funcionalidades de *Cloud Computing*. Pretende-se, ainda, convergir a um modelo suscetível de implantação em território nacional, dando suporte a necessidades do Sistema Cartão Nacional de Saúde, sobre uma ampla infraestrutura de comunicação, a exemplo da rede Ipê, da RNP.

AGRADECIMENTOS

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

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

REFERÊNCIAS

1. Brasil. Conselho Federal de Medicina. Resolução Nº 1.821 de 11 de julho de 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. Brasília: Conselho Federal de Medicina; 2007.
2. W3C. Simple Object Access Protocol. [cited 2007 apr 27]. Available from: http://www.w3.org/TR/soap12-part1
3. Tom Barton, Jim Basney, Tim Freeman, Tom Scavo, Frank Siebenlist, Von Welch, Rachana Ananthakrishnan, Bill Baker, Monte Goode and Kate Keahey. Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, GridShib, and MyProxy. In 5th Annual PKI R&D Workshop. NIST Gaithersburg MD, USA; 2006.
4. Field, M. Cardea: dynamic access control in distributed systems. NASA Advanced Supercomputing. 2003. p. 1-31.
5. Camargo E, Fraga JS, Wangham MS, Mello ER. Autenticação e autorização em arquiteturas orientadas a serviço através de identidades federadas. In: Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos; 2007 mai 28; Belém. Pará, Brasil; 2007.
6. Oasis. eXtensible Access Control Markup Language (XACML). OASIS standard [Online]. [cited 2005 fev 1]. Available from: http://www.oasis-open.org.
7. Oasis. Security Assertion Markup Language (SAML). Oasis standard [Online]. [cited 2005 mar 15]. Avaiable from: http:// / www.oasis-open.org.
8. Armando A, Carbone R, Compagna L, Cuellar J, Abad LT. Formal analysis of SAML 2.0 web browser single sign-on Breaking the SAML-based Single Sign-On for Google Apps. 6th ACM workshop on Formal methods in security engineering. 2008 Oct 27; Virginia, USA; 2008.
9. Carrião DA, Santin CM. Integrando o modelo de segurança SPKI/SDSI ao ambiente de gerência WBEM. I Workshop em Segurança de Sistemas Computacionais; 2001 mar 5-6; Florianópolis. Santa Catarina. 2001. p.1-12.
10. Schumacher M, Buglioni EF, Hybertson D, Buschmann F, Sommerlad P. Security patterns: integrating security and systems engineering. England: John Wiley & Sons; 2006.
11. N Dagorn, N Bernard, S Varrette. Practical authentication in distributed environments. IEEE International Computer Systems and Information Technology Conference (ICSIT'05); 2005 Jul 19-21. Algerie. 2005.
12. Ferraiolo DF, Kuhn DR, Chandramouli R. Role-based access control. Boston: Artech House; 2003.
13. Schläger C, Priebe T, Liewald M, Pernul, G. Enabling attribute-based access control in authentication and authorisation infrastructures. 20th Bled eConference eMergence: Merging and Emerging Technologies, Processes and Institutions; 2007 Jun 4 - 6; Bled, Slovenia. 2007. p. 814-26.
14. Carter G. LDAP Administração de sistemas. Rio de Janeiro: Alta Books; 2009.
15. Lewis KD, Lewis JE. Web single sign-on authentication using SAML. IJCSI. 2009;2:41-8.
16. Brasil. Ministério da Justiça. Casa Civil. Medida Provisória 2200-2/01. Institui a intra-estrutura de chaves públicas brasileira – ICP-BRASIL; 24 de agosto 2001.
17. Motta GHMB. Um modelo de autorização contextual para o controle de acesso ao prontuário eletrônico do paciente em ambientes abertos e distribuídos. [tese] São Paulo: Escola Politécnica da Universidade de São Paulo; 2004.