SMMM – Um Sistema de Correio Eletrônico Multimídia Seguro

Marcel Stanley A. de Moura ①② Guido Lemos de Souza ② Thaís V. Batista ② Luiz Fernando G. Soares ③

① Programa Especial de Treinamento - Curso de Ciências da Computação - UFRN

② DIMAp - UFRN
Campus Universitário, Lagoa Nova
59072-970 - Natal-RN, Brasil

③ Lab. Telemídia - DI, PUC-Rio
R. Marquês de São Vicente, 225
22453-900 - Rio de Janeiro, Brasil

e-mail: {msam, guido, thais}@dimap.ufrn.br, lfgs@telemidia.puc-rio.br.

Resumo

O correio eletrônico tem se mostrado como a mais importante das aplicações de comunicação usadas na Internet. A necessidade de intercâmbio de mensagens complexas, compostas de várias mídias fez surgir os sistemas de correio eletrônico multimídia. Com a modernização e a popularização das aplicações de comunicação, diversas ameaças às mensagens intercambiadas via e-mail surgiram. Dentro deste contexto, este artigo apresenta o Secure MultiMedia Mail, um sistema de correio eletrônico multimídia seguro.

Abstract

Nowadays, e-mail is the most important communication application used inside Internet. With the necessity of interchange of complex messages, composed by different medias, multimedia e-mail systems have arisen. However these systems aren't perfect; with the advance of the computer's technology and the popularity of e-mail systems, a lot of threats against them have arisen. In that context, this paper presents the Secure MultiMedia Mail, a secure multimedia e-mail system.

Palavras-chave: Correio Eletrônico, Java, Multimídia em Redes, Segurança.

1 INTRODUÇÃO

O avanço e a disseminação da tecnologia de redes de computadores possibilitou o surgimento de várias aplicações, muitas destas, utilizando o potencial de comunicação à distância provido pela plataforma de rede. Dentre essas aplicações, destaca-se, por sua vasta utilização, o correio eletrônico (*e-mail*).

O correio eletrônico oferece um sistema de troca de mensagens de forma assíncrona com suporte computacional entre usuários localizados remotamente. Em um serviço de correio eletrônico, todo o processo de intercâmbio de mensagens ocorre sem a necessidade da presença física do usuário de destino, ficando a cargo do servidor de correio, que o realiza em *background*, após a solicitação de envio por parte do remetente [Comer93, Lynch93].

A facilidade de integração de dados multimídia oferecida pelo surgimento de sofisticadas ferramentas para edição e exibição de voz, vídeo e imagens, determinou um mudança no perfil das aplicações. Neste contexto, surgiram novas aplicações de comunicação, dentre elas alguns sistemas de correio eletrônico com suporte à transmissão de informações multimídia [Thomas85, Edwards91, Soares94a, Ouhyoung94][1].

Em sistemas de correio eletrônico multimídia é importante que os documentos intercambiados possam ser apresentados de forma estruturada, de acordo com uma especificação feita pelo seu autor. A especificação desses documentos pode conter relacionamentos, de espaço (disposição dos componentes na apresentação do documento) e/ou de tempo (ordem, sincronismo da apresentação dos componentes), entre as suas diversas partes. Relações semânticas desse tipo são fornecidas por sistemas de documentos multimídia/hipermídia que, portanto, podem servir de base para a composição (autoria) de mensagens intercambiadas por

[1]Exemplos de *softwares* comerciais recentes que lidam com o intercâmbio de mensagens multimídia são o CVideo-Mail (www.cvideomail.com) e o E-Mail PossaLink (www.bravomail.com/possalink.htm).

esses sistemas. Adicionalmente, questões como tráfego na rede e espaço de armazenamento devem ser consideradas. Deste modo, sistemas de correio eletrônico devem evitar ao máximo o envio desnecessário de informação (componentes multimídia/hipermídia) através da rede, assim como a sua replicação indevida nos servidores de correio.

A facilidade de comunicação oferecida pela interconexão das redes de computadores do mundo inteiro, vem suscitar a aparição da questão segurança no que se refere à transmissão de dados e informação. Nessa situação, o correio eletrônico, por se tratar da mais utilizada aplicação de comunicação, é alvo das mais diversas ameaças [Soares97]. Nos últimos anos, alguns modelos de intercâmbio seguro de mensagens via correio eletrônico foram definidos. Pode-se citar o *Pretty Good Privacy* (PGP) [Schneier95] e o *Privacy Enhanced Mail* (PEM) [Schneier95].

Este artigo apresenta o SMMM (*Secure MultiMedia Mail*), um sistema de correio eletrônico multimídia seguro, implementado em Java™, onde são considerados todos os requisitos levantados anteriormente. Este sistema trata de forma eficaz a transmissão segura de mensagens multimídia (as mensagens intercambiadas via SMMM são estruturadas utilizando um modelo de edição de documentos multimídia) via correio eletrônico, diferentemente de outros trabalhos existentes que somente tratam do quesito segurança quanto ao correio eletrônico convencional [Cavalcanti97], não considerando a transmissão de informações multimídia; ou que não tratam a segurança de documentos complexos, preocupando-se apenas com a segurança dos diversos componentes de forma separada, sem uma estruturação lógica definida entre eles [Elkins96].

O presente artigo encontra-se organizado da seguinte forma: a segunda seção traz o detalhamento do sistema de correio eletrônico, produto deste trabalho, onde são mostradas a arquitetura e a implementação do sistema; a terceira expõe as conclusões do trabalho e descreve alguns possíveis trabalhos futuros.

2 O SECURE MULTIMEDIA MAIL

O Secure MultiMedia Mail (*SMMM*) é um sistema de correio eletrônico seguro que oferece tratamento a mensagens Multimídia/Hipermídia (M/H). Sua base conceitual é derivada do MMM [Batista96], sistema de correio eletrônico multimídia idealizado como parte do projeto HyperProp [Soares95]. Neste sistema, o NCM (*Nested Context Model*) [Soares94b] é o modelo utilizado para a criação de mensagens M/H.

Nesta seção, são introduzidos conceitos básicos sobre o modelo utilizado pelo sistema, assim como o formato dos dados intercambiados pelo sistema de correio. Após isso, a arquitetura e a implementação do sistema são descritas, detalhando-se todos os seus componentes.

2.1 O Modelo Conceitual dos Documentos M/H Intercambiados

O NCM é o modelo utilizado para a composição de mensagens multimídia/hipermídia no SMMM. Como forma de introduzir alguns conceitos que serão utilizados durante este trabalho, uma breve explanação sobre o modelo é dada nesta seção.

Um documento hipermídia é definido no modelo NCM a partir dos conceitos usuais de nós e elos. Os nós são constituídos de fragmentos de informação e os elos são usados para exprimir todas as possíveis relações entre os diferentes nós que constituem o documento. Existem duas classes básicas de nós: os nós terminais e os nós de composição, sendo estes últimos o ponto central do modelo.

Um nó terminal (ou nó de conteúdo) contém um conjunto de dados, cuja estrutura interna é dependente da aplicação, como no caso dos nós hipermídia tradicionais. A classe de nós terminais pode ser especializada em outras classes (por exemplo., texto, gráfico, áudio,

vídeo), conforme requerido pelas aplicações. Um nó de composição contém uma coleção de elos e nós, de conteúdo ou de composição, interrelacionados.

Informações adicionais sobre o modelo podem ser encontradas em [Rodrigues98, Soares94b, Soares95].

2.2 O Formato dos Dados Intercambiados

No SMMM, qualquer nó de composição ou de conteúdo é chamado de *documento-M/H*. Uma mensagem multimídia/hipermídia intercambiada via SMMM é representada por um tipo específico de documento-M/H, chamado *mensagem-M/H*. Uma mensagem-M/H é um nó de composição composto por um **envelope**, semelhante ao cabeçalho de uma mensagem de correio eletrônico convencional (definido na RFC 822 [Crocker82]) e pelo **corpo da mensagem**, um documento M/H qualquer (Figura 1).

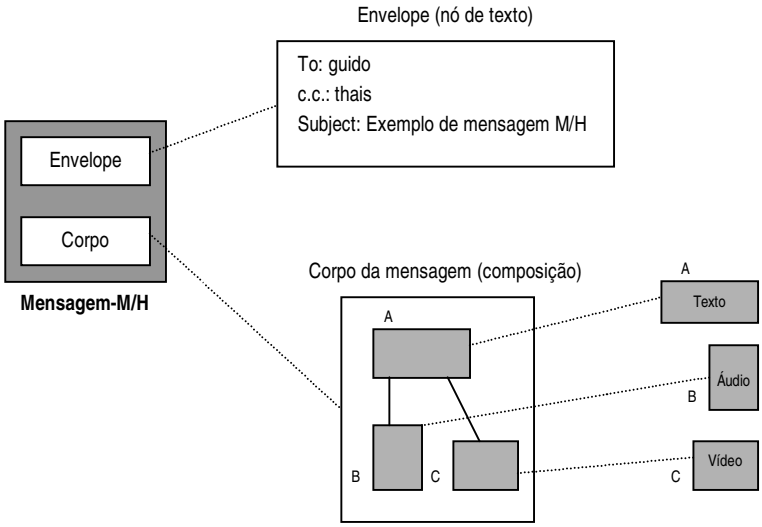

Figura 1 - *Uma mensagem M/H no SMMM.*

O SMMM define um modelo de dados para a descrição das mensagens-M/H por ele transmitidas/recebidas. Este formato é representado por uma mensagem ASCII comum, resultante da inclusão implícita[2] dos componentes da mensagem original (Figura 2).

O modelo de mensagens M/H utilizado pelo SMMM fornece uma notável flexibilidade. Ele permite que um nó esteja contido em um ou mais nós de composição. Assim:

- o corpo de uma mensagem-M/H pode ou não ser compartilhado, total ou parcialmente, com outros usuários, obedecendo os direitos de acesso definidos pelo proprietário;
- uma mensagem-M/H pode estar contida no corpo de qualquer outra mensagem-M/H.

Outra vantagem é a de que o corpo da mensagem pode ser criado externamente, sendo incorporado depois à mensagem-M/H.

---

[2] Tendo em vista a heterogeneidade dos sistemas na Internet, onde os recursos são limitados, é interessante que os componentes multimídia de uma mensagem sejam incluídos implicitamente no seu corpo. Desta forma, a mensagem transmitida é pequena (alguns sistemas possuem restrição quanto ao tamanho das mensagens por eles intercambiadas) e, além disso, permite que o sistema de destino, como ainda será visto durante este trabalho, somente receba os componentes que ele puder tratar, o que evita uma sobrecarga desnecessária da rede. [Batista96a,b]

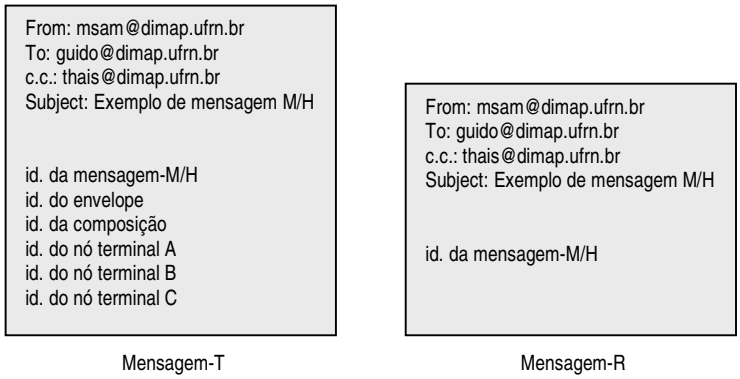

Figura 2 - *Mensagens utilizadas pelo SMMM.*

Na composição da mensagem, seus componentes são selecionados. Adicionalmente, são definidos aqueles onde serão aplicados serviços de segurança. Para esses, são escolhidos os serviços a serem empregados. Após a composição e a solicitação do envio de uma mensagem-M/H, o usuário passa as informações necessárias à execução dos serviços de segurança selecionados para o sistema. Então, é criada uma mensagem ASCII correspondente à original, denominada *mensagem-T temporária*.

A mensagem-T temporária é enviada ao servidor SMMM (seção 2.3) onde é realizado seu tratamento. No servidor SMMM, é gerada a *mensagem-T final* (ou somente *mensagem-T*), que segue o formato definido na RFC 822 para mensagens textuais transmitidas via Internet. Para identificar uma mensagem-M/H gerada pelo SMMM, é adicionado ao cabeçalho da mensagem-T o campo **X-SMMM** com o valor **TRUE**. Feito isso, a mensagem é enviada normalmente através de um servidor de correio convencional, utilizando-se o protocolo SMTP (*Simple Mail Transfer Protocol*) [Postel82].

Quando da chegada da mensagem ao servidor de destino, o sistema é capaz de separar as mensagens-M/H geradas pelo SMMM das mensagens convencionais, efetuando as ações necessárias para que elas possam ser disponibilizadas nas caixas postais do(s) destinatário(s) na forma de *mensagens-R*. Isto só ocorre após o sistema de correio de destino garantir que os componentes principais da mensagem tenham sido recuperados, observando-se as mídias que o sistema consegue tratar (seção 2.4.1). Uma mensagem-R diferencia-se de uma mensagem-T apenas pela exclusão de todas referências aos componentes da mensagem, existindo somente uma referência (identificador) à mensagem-M/H. Mais detalhes a respeito dos processos de envio e recepção de mensagens-M/H podem ser encontrados na seção 2.4.

Na seção seguinte é apresentada a arquitetura do SMMM, onde são descritos todos os componentes presentes e responsáveis pelo seu funcionamento.

2.3 Arquitetura do Sistema

Utilizando-se de um cenário de configuração, onde uma rede utiliza o protocolo SMTP para a transferência de mensagens ASCII, é descrita nesta seção a arquitetura do Secure MultiMedia Mail.

Na figura 3, duas redes, A e B, possuem a mesma configuração: uma estação do servidor SMTP, uma estação do servidor M/H e uma ou mais estações de usuário.

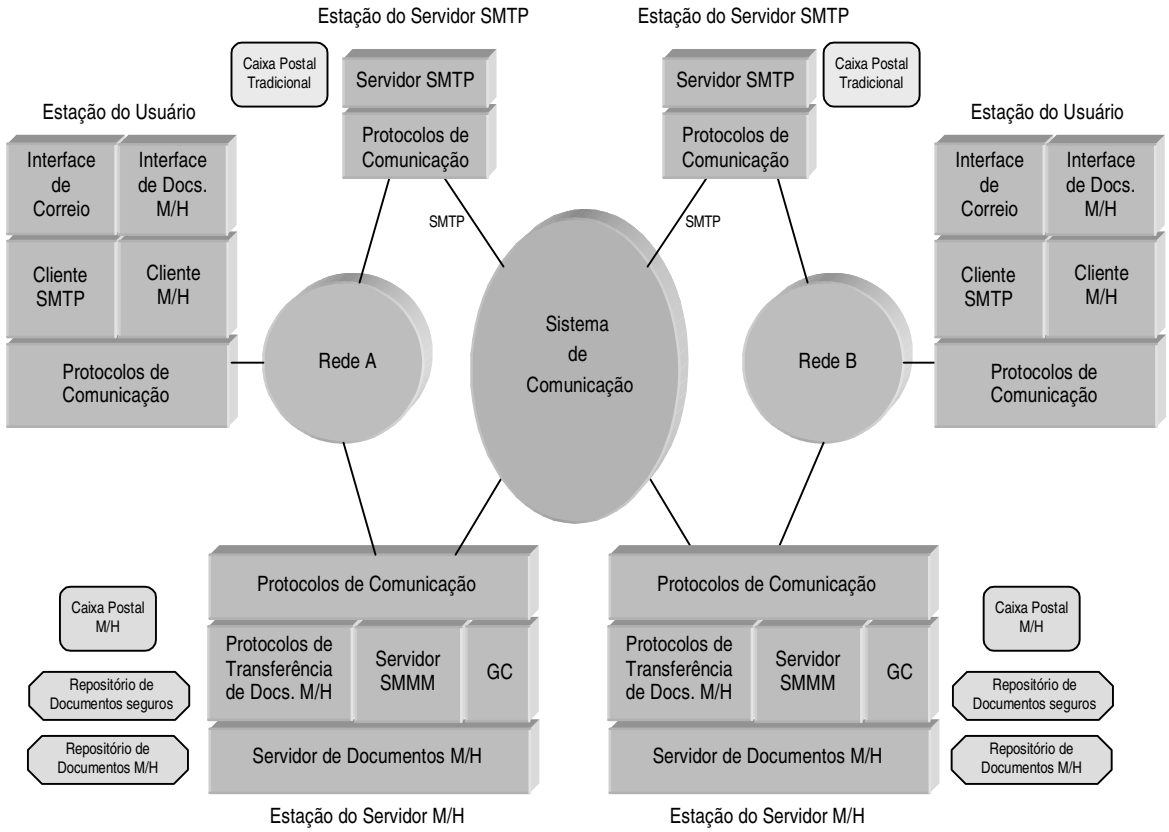

Figura 3 - *Arquitetura do Secure MultiMedia Mail em um sistema distribuído.*

Na estação do servidor SMTP é executado um servidor de correio convencional, utilizando o protocolo SMTP. Este servidor é responsável pelo envio de mensagens via Internet. Nele estão armazenadas as caixas postais dos usuários (correio convencional).

A estação do servidor M/H é composta por três módulos: o Servidor de documentos M/H (ou, somente, Servidor M/H), o Servidor SMMM (Gerente de Mensagens) e o GC (Gerenciador de Chaves). O Servidor de documentos M/H é responsável pelo armazenamento e recuperação de documentos-M/H na rede, tendo acesso aos repositórios onde os documentos M/H são armazenados (Repositórios de documentos M/H e de documentos M/H seguros). O Servidor SMMM é responsável pelo tratamento das mensagens M/H enviadas/recebidas pela rede. Esse servidor é subdivido em dois módulos. Ao primeiro módulo são atribuídas as funções de, quando da recepção de uma mensagem M/H: identificação dos componentes das mensagens, solicitação do envio daqueles não situados localmente a um servidor M/H remoto e geração da mensagem-R, que será armazenada na caixa postal convencional do destinatário pelo servidor SMTP. O segundo módulo é responsável pela aplicação dos serviços de segurança selecionados pelo usuário às mensagens-M/H geradas através da interface de correio. Por fim, o GC é responsável pelo gerenciamento, armazenamento e recuperação das chaves de cada usuário, usadas na execução dos serviços de segurança do sistema.

A estação do usuário é uma estação típica a qual um usuário teria acesso para a composição e envio de mensagens. É composta por dois módulos: a Interface de Correio e a Interface de Documentos M/H. São funções da Interface de Correio: acessar o correio convencional (o acesso aos serviços de correio eletrônico convencional oferecidos pelo servidor SMTP é feito através de um cliente SMTP); dar suporte à transmissão de documentos M/H; e comunicar-se

com o servidor SMMM, de forma a serem aplicados os serviços de segurança selecionados pelo usuário. A Interface de Documentos M/H é responsável pela composição e exibição das mensagens-M/H (o acesso ao servidor de Documentos M/H é feito através de um cliente M/H)[3].

Na seção seguinte é apresentada a atual implementação do Secure MultiMedia Mail. Nela, o funcionamento do sistema e detalhes de implementação, assim como a Interface de correio, são descritos.

2.4 Implementação do Sistema

Em sua atual versão, o Secure MultiMedia Mail encontra-se implementado na Linguagem Java™. A razão da escolha dessa linguagem se deveu a sua capacidade intrínseca de prover portabilidade. Desta forma, o SMMM pode ser executado em qualquer plataforma onde a máquina virtual Java esteja instalada.

Após ter sido apresentada a arquitetura do sistema (seção 2.3), nesta seção é explicado o seu funcionamento, detalhando-se o papel de cada um dos módulos. Primeiramente são apresentados alguns dos requisitos do sistema, então, é mostrada a interface de correio utilizada pelo sistema. Após isso, é feita a descrição do processo padrão de composição/envio/recepção de uma mensagem-M/H no SMMM, onde os demais componentes da arquitetura são detalhados.

2.4.1 Requisitos do Sistema

Independentemente do modelo de documentos M/H utilizado ou do sistema de transporte, alguns aspectos, no que concerne ao tratamento de documentos M/H, devem ser considerados. Quando da implementação de um sistema de correio eletrônico multimídia baseado na mesma filosofia do MMM, alguns requisitos devem ser atendidos:

- nenhum nó deve ser replicado no servidor M/H. Se um nó pertence a mais de uma mensagem, ele deve ser referenciado, não replicado. Isto visa minimizar o espaço necessário ao armazenamento das mensagens;
- o SMMM deve funcionar mesmo em sistemas que não forneçam suporte a todas as mídias. No pior caso, o SMMM deve funcionar como um sistema de correio eletrônico convencional. Além disso, nós que o sistema do usuário não consiga tratar não devem ser transmitidos através da rede. Para tanto, no SMMM, devem ser definidas as mídias suportadas pelo sistema (perfil).

Com o atendimento desses requisitos, o SMMM minimiza o tráfego de informações na rede, uma vez que não há a replicação de nós, assim como não são transmitidos nós que o sistema de destino não seja capaz de tratar.

Além dos requisitos básicos já apresentados, outros devem ser satisfeitos:

- o sistema deve ser o mais flexível possível em relação aos tipos de mídia que possam ser utilizados;
- o SMMM deve aproveitar ao máximo os padrões para a composição e transmissão de documentos M/H.

Quanto às questões de segurança, outros requisitos devem ser atendidos pelo sistema [Soares97]:

---

[3] A composição de mensagens também pode ser realizada pela IC, como poderá ser visto posteriormente, na seção 2.4.3.

- mecanismos de segurança que não sejam sujeitos às restrições de controle de exportação ou patentes devem ter preferência;
- deve-se dar preferência às tecnologias de segurança que possam compartilhar uma infra-estrutura de segurança comum;
- os serviços de segurança somente devem ser aplicados às partes sensíveis de uma mensagem, evitando-se, assim, processamento desnecessário;
- os algoritmos de segurança selecionados devem ser amplamente conhecidos, devendo-se dar preferência àqueles que tiverem sido amplamente testados.

2.4.2 Interface de Correio do SMMM

A **Interface de correio do SMMM (IC)** é uma aplicação Java *stand-alone*, necessitando apenas da máquina virtual Java para funcionar.

Ao ser executada, a IC tenta se conectar a um servidor de correio comum, configurado pelo usuário (Janela *Preferences*, aba *Mail*), para recuperar as mensagens contidas na caixa postal do usuário. O acesso ao servidor só é permitido mediante a passagem do nome do usuário e a senha correspondente. Após a validação da senha, é iniciada a IC.

A IC é semelhante a outras interfaces de correio convencional já existentes. Ela possui um menu de opções e uma barra de ferramentas, onde operações, como a composição de mensagens, a recuperação de mensagens no servidor, *forward's* e *reply's* de mensagens, podem ser executadas[4]. O usuário também pode acessar, através do menu, a janela *Preferences*, onde são editadas as preferências do usuário (menu *Edit*, opção *Preferences*).

Na janela *Preferences*, o usuário configura suas preferências com relação ao correio e à segurança das transmissões.

Na aba *Mail* são solicitadas informações sobre os servidores de envio (*outgoing*) e recepção (*incoming*) de mensagens. Para ambos os servidores devem ser informados o nome do usuário, o endereço do servidor e o protocolo a ser utilizado para se conectar a cada um deles. Especialmente para o servidor de saída, é solicitado o endereço eletrônico do usuário, a ser usado no campo *From* de todas as mensagens compostas/enviadas pela IC.

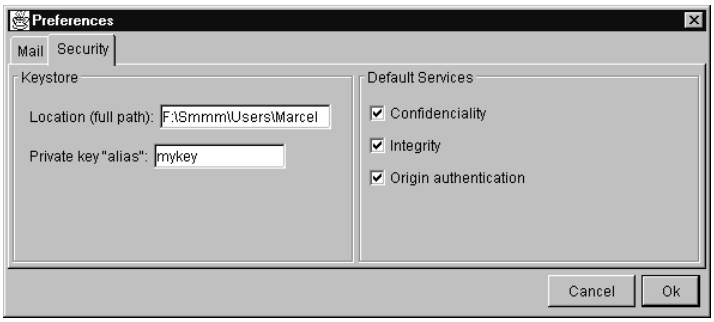

Figura 4 - *Janela "Preferences" (preferências de segurança).*

Na aba *Security* (Figura 4) são solicitados dados referentes à aplicação dos serviços de segurança às mensagens compostas (as mensagens também podem ser compostas externamente, como ainda será visto) e enviadas pela IC. Nesta aba deve-se fornecer dados sobre o gerenciador de chaves utilizado (a localização do *keystore* e o *alias* da chave privada

[4] Na Interface de Correio do SMMM uma ajuda, onde o usuário pode obter explicações sobre o funcionamento do sistema, assim como outras operações (no menu) são disponibilizadas.

utilizada pelo usuário[5]) e selecionar os serviços de segurança *default* a serem aplicados a uma mensagem e seus componentes (quando existirem). Os serviços de segurança podem ser configurados em separado para uma mensagem e seus nós componentes quando da composição da mensagem, caso necessário.

O usuário, após realizada a configuração adequada, pode passar à composição de mensagens. Este processo é apresentado na seção seguinte.

2.4.3 Composição de uma mensagem-M/H no SMMM

Na Interface de correio, o usuário, ao clicar o botão *Compose* (ou selecionar o item File-New-Message do menu), solicita a criação de uma nova mensagem.

O usuário pode, então, preencher os dados do envelope da mensagem (os campos *To*, *Subject* e *c.c.*). Caso o usuário apenas queira compor uma mensagem textual, ele pode assim fazê-lo, editando o conteúdo da mensagem normalmente; caso o usuário deseje compor uma mensagem M/H, ele tem duas opções para a criação do seu corpo:

- selecionar um nó de composição da base de documentos M/H (arrastar da Interface/base de documentos M/H e soltar na janela de composição);
- editar o corpo da mensagem.

A composição da mensagem prossegue com a configuração dos serviços de segurança a serem aplicados. Devem ser considerados pelo remetente quais os nós da mensagem são merecedores da aplicação de serviços de segurança. Esses são os chamados **nós sensíveis**[6] de uma mensagem.

Os serviços[7] disponibilizados pelo SMMM são:

- confidencialidade;
- integridade; e
- autenticação da origem da mensagem.

Caso o usuário deseje editar "manualmente" o corpo da mensagem-M/H, ele deve selecionar o botão *Components* na janela de composição de uma nova mensagem. Com isso, a janela *M/H Composition* é exibida (Figura 5).

Nessa janela, o usuário pode escolher os nós que comporão a mensagem. Na caixa de edição *Node*, o remetente entra com a URL de um nó. Caso o usuário entenda que esse nó deve ser enviado de forma segura ao destinatário (nó sensível), ele deve definir quais os serviços de segurança serão aplicados ao nó. Após isso o usuário pode adicionar o nó à mensagem (botão *Add*). Para a inserção de outros nós, procede-se da mesma forma.

Após a adição dos nós, caso o usuário deseje, ele pode removê-los da mensagem. Isto é feito selecionando o(s) nó(s) na lista de nós e clicando no botão *Remove*.

Os nós sensíveis da mensagem e os serviços de segurança aplicados podem ser modificados a qualquer momento, através da seleção do(s) nó(s) e a alteração dos serviços na caixa de serviços.

---

[5] Tanto o *keystore* quanto as chaves nele armazenadas só são acessadas mediante a apresentação das suas respectivas senhas. Estas só são solicitadas ao usuário no momento de envio da mensagem, como poderá ser visto adiante.

[6] Os nós sensíveis de um documento-M/H podem ser diferentes com relação a vários usuários.

[7] Os serviços de segurança oferecidos pelo SMMM seguem as orientações definidas pelo documento ISO 7498-2, adequados às características das comunicações feitas via Internet (TCP/IP). [Lynch93]

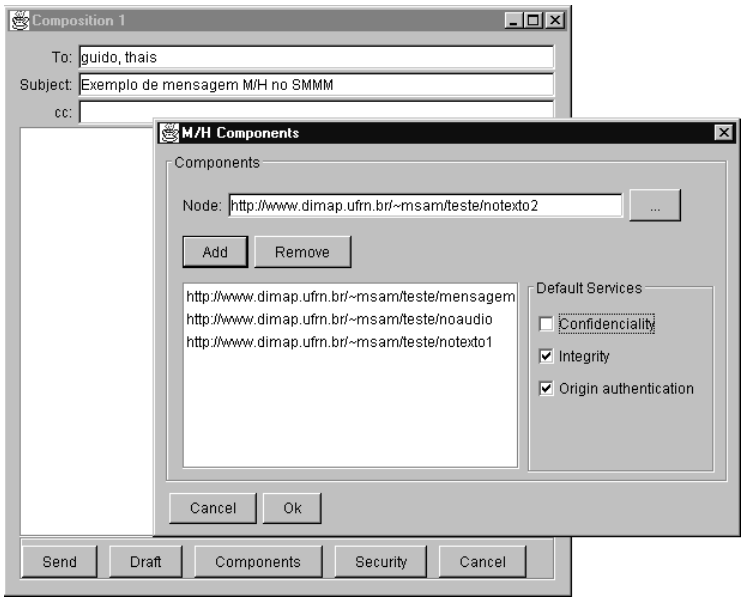

Figura 5 - *Composição "manual" de uma mensagem-T.*

Após a seleção dos componentes da mensagem e a configuração dos serviços de segurança para cada um dos seus nós (além da própria mensagem), o usuário pode solicitar o seu envio. A IC, neste momento, gera automaticamente a mensagem-T temporária (Figura 6). Nesta mensagem são postas informações sobre os nós que a compõem e os serviços de segurança selecionados para cada um deles, incluindo a própria mensagem. Então, a mensagem-T temporária é repassada para o servidor SMMM, responsável pelo envio das mensagens.

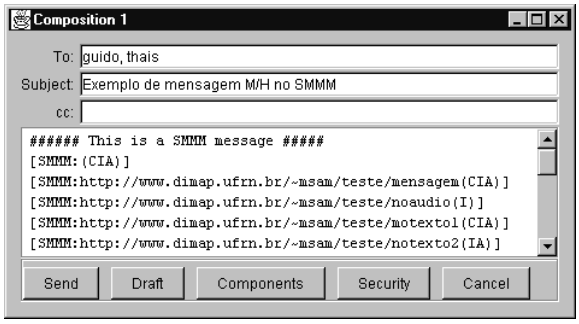

Figura 6 - *Mensagem-T temporária gerada pela IC.*

2.4.4 Envio de uma mensagem-M/H no SMMM

Após a geração da mensagem-T temporária pela IC, esta é repassada para o servidor SMMM.

O Servidor SMMM, como dito anteriormente (seção 2.3), possui um módulo responsável, na ocasião do envio de uma mensagem (seja uma mensagem textual ou mensagem-M/H), pela aplicação dos serviços de segurança, determinados pelo usuário, à mensagem e aos seus componentes.

Os serviços de segurança disponibilizados no SMMM são implementados com o auxílio de mecanismos de segurança, tais como: funções geradoras de *hash* (MD5) e mecanismos de criptografia simétrica (DES) e assimétrica (RSA) [Schneier95, Soares97]. Os mecanismos de criptografia necessitam de chaves para funcionar, que devem estar armazenadas em algum

banco de dados de chaves. Cada usuário do sistema possui um arquivo, *keystore*, onde são armazenadas sua(s) chave(s) privada(s), sua(s) chave(s) pública(s) e as chaves públicas de outras pessoas[8]. Em um *keystore*, cada chave é identificado por um *alias*. Cada uma das chaves só pode ser acessada através da passagem de uma senha, individual para cada chave.

O acesso a *keystore* é realizado através do **gerenciador de chaves (GC)** (na atual implementação do SMMM, o gerenciador de chaves utilizado é o *KeyTool*™, ferramenta provida pela plataforma Java 2™).

Para que o servidor SMMM possa aplicar os serviços de segurança à mensagem, ele necessita de algumas informações, como a senha e a localização (caminho completo) do *keystore* do usuário[9].

Além dessas informações, outras, referentes a cada um dos serviços de segurança implementados pelo servidor, devem ser a ele fornecidas[10]. O SMMM, como visto anteriormente, provê serviços de confidencialidade, integridade e autenticação da origem de uma mensagem. De acordo com o serviço a ser aplicado, informações distintas são necessárias.

Na implementação do serviço de confidencialidade são usados mecanismos de criptografia assimétrica e criptografia simétrica. Para executar o serviço de confidencialidade, o servidor SMMM precisa recuperar a chave pública do destinatário no *keystore*. Para isso, através da IC, no momento da solicitação do envio da mensagem, são solicitados ao usuário o nome dessa chave no *keystore* e a senha de acesso dela. Estas informações são então remetidas para o servidor SMMM.

O servidor SMMM gera uma chave de sessão *k*. Com essa chave, ele criptografa a mensagem e/ou seus componentes (conforme configuração do usuário). Além disso, o servidor criptografa a chave de sessão com a chave pública do destinatário. Então, cada um dos componentes criptografados, é unido à chave de sessão criptografada e disponibilizado como um novo documento (seguro) no repositório de documentos seguros. No caso da mensagem, o seu corpo é substituído pelo resultado da sua criptografia, adicionado da chave de sessão devidamente criptografada.

Para a provisão do serviço de integridade são usados mecanismos de criptografia assimétrica e funções geradoras de *hash*. Da mesma forma que no serviço de confidencialidade, neste serviço, o servidor SMMM utiliza a chave pública do destinatário, que, portanto, deve ser recuperada do *keystore*. Para que isso seja realizado, faz-se necessária a solicitação das mesmas informações requeridas para execução do serviço de confidencialidade ao usuário, pela IC, que as repassa para o servidor SMMM.

O servidor SMMM gera um *hash* para a mensagem e/ou seus componentes (conforme configurado pelo remetente). Cada um dos *hashs* gerados é assinado (criptografado) com chave pública do destinatário. No caso dos componentes, estes são adicionados de seus respectivos *hashs*, devidamente assinados, e disponibilizados no repositório de documentos seguros. Para a mensagem, ao seu corpo é adicionado o seu *hash* assinado.

Na implementação do serviço de autenticação da origem utiliza-se os mesmos mecanismos que o serviço de integridade. Para que esse serviço seja executado, o servidor SMMM

---

[8] É importante que todas as chaves armazenadas no *keystore* estejam certificadas (assinadas por entidades certificadoras ou outras pessoas).

[9] Estas informações são recuperadas do arquivo de configuração do usuário, gerado a partir das configurações feitas na janela *Preferences*, como visto na figura 6 (seção 2.4.2).

[10] Tais informações são solicitadas ao usuário, pela IC, quando este requer o envio de uma mensagem de forma segura e, depois, repassadas ao servidor SMMM, através de um canal seguro (implementado com chave de sessão).

necessita que a chave privada do remetente seja recuperada do *keystore*. Para tanto, a IC solicita ao usuário, quando da solicitação do envio, o nome e a senha de acesso do alias dessa chave no *keystore* do usuário. Tais informações são repassadas ao servidor SMMM.

O servidor SMMM gera um *hash* para cada um dos componentes da mensagem, como no serviço de integridade. Após isso, cada um dos *hashs* é assinado com a chave privada do usuário remetente. Aos componentes são adicionados os seus *hashs*, e os documentos resultantes são armazenados no repositório de documentos seguros. No caso da mensagem, esta tem seu corpo modificado de forma a conter também o seu respectivo *hash* criptografado.

Como o mais comum é utilizar mais de um dos serviços disponíveis, o conjunto de informações solicitado ao usuário pela IC e transmitido para o servidor SMMM deve comportar a união dos dados necessários a cada um dos serviços requeridos.

Quando diversos serviços são solicitados para um mesmo componente, a seguinte ordem é respeitada pelo servidor SMMM, quando da execução dos serviços: primeiro confidencialidade; depois, integridade; e, por último, autenticação da origem. Dessa forma, a confidencialidade dos documentos é sempre respeitada, quando este serviço é solicitado.

Devido à sua importância, todas os dados intercambiados entre a IC e o servidor SMMM são transmitidos por canais de comunicação seguros, implementados com mecanismos de criptografia assimétrica com chave de sessão (assim como quaisquer outras transmissões de dados internos que necessitem de segurança), haja vista a possibilidade de ataque aos processos de comunicação internos ao sistema.

Após a aplicação dos serviços de segurança selecionados à mensagem, é gerada a mensagem-T final[11]. A ela são adicionadas as datas de modificação dos documentos e, caso algum serviço de segurança tenha sido aplicado, as URLs dos componentes são alteradas, de forma a representar a sua nova localização, no repositório de documentos seguros (desta forma, quando da chegada da mensagem-T ao servidor SMMM de destino, este acessará os documentos referenciados em sua localização correta). Após isso, a mensagem-T é repassada ao servidor SMTP que se encarrega de enviá-la normalmente pela Internet.

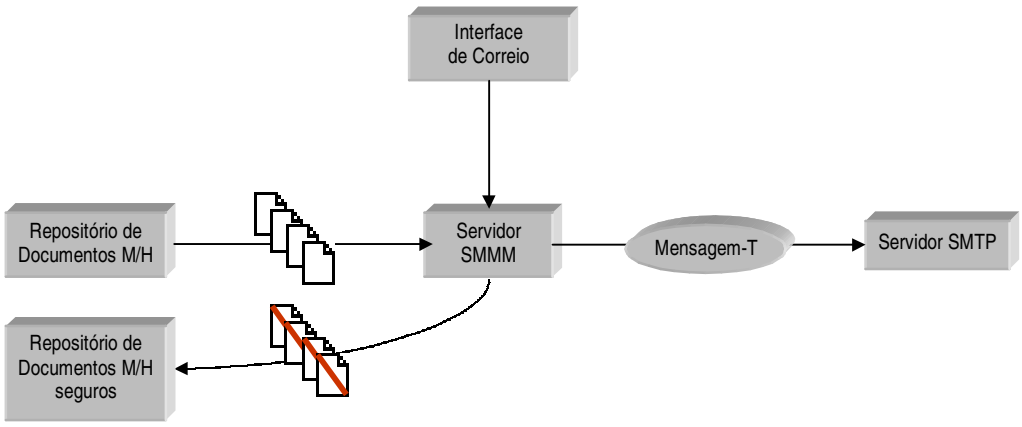

Figura 7 - *Processo de envio de uma mensagem-M/H no SMMM.*

Ao mesmo tempo em que é acionado o envio da mensagem-T, é disparada a aplicação dos serviços de segurança selecionados aos seus componentes. O servidor SMMM verifica a lista de componentes no servidor de documentos M/H. Aqueles localizados no servidor são recuperados e são neles aplicados os serviços de segurança selecionados. Os documentos

[11] No caso de não ser selecionada a aplicação de nenhum serviço de segurança a mensagem como um todo, a mensagem-T final é a mesma da mensagem-T temporária.

seguros são, então, enviados para o servidor de documentos M/H que os armazena no repositório de documentos-M/H seguros para que possam ser recuperados, posteriormente, pelo servidor SMMM de destino.

Todo o processo de envio de uma mensagem no SMMM pode ser visualizado na Figura 7.

Ao chegar ao servidor de correio de destino, as mensagens são processadas, como poderá ser visto na seção seguinte.

2.4.5 Recepção de uma mensagem-M/H no SMMM

O processo de recepção de uma mensagem pelo SMMM divide-se em duas etapas: a recepção da mensagem-T e a recuperação dos componentes da mensagem (nós) que estejam localizados remotamente.

As mensagens são recebidas normalmente no Servidor de Correio convencional pelo programa **sendmail**. Este programa pode disparar automaticamente a execução de processos quando da recepção de uma mensagem. No SMMM, o sendmail redireciona cada mensagem recebida para o programa **procmail**, que é incumbido de verificar o tipo da mensagem antes de colocá-la na caixa postal do destinatário. O procmail detecta as mensagens-M/H geradas pelo SMMM através do campo X-SMMM. Quando esse campo tem o valor TRUE ele a redireciona para o servidor SMMM; caso contrário (X-SMMM=FALSE) ou quando não for detectado o campo X-SMMM, a mensagem é depositada normalmente na caixa postal do usuário de destino.

O servidor SMMM realiza uma varredura no corpo da mensagem-T, devidamente recebida do servidor de correio, procurando pelas referências aos componentes da mensagem. Para cada um dos elos encontrados, o servidor verifica se o documento encontra-se no servidor de documentos M/H local[12]. Caso haja componentes que não estejam no servidor local, este são recuperados via algum protocolo de transferência de arquivos multimídia (no caso, o HTTP) e armazenados no repositório correspondente (os documentos seguros no repositório de documentos M/H seguros; os demais no de documentos M/H).

No servidor de documentos M/H é mantida uma **Tabela de Documentos (TD)** para realizar o controle dos documentos situados localmente. Essa tabela associa os nomes dos documentos locais com os seus nomes originais. É através da TD que o servidor SMMM verifica a existência dos documentos no servidor M/H. A pesquisa é realizada a partir do nome original de cada um dos componentes. No caso de o componente não ser encontrado, uma nova "tupla" <*nome original, nome local, data de modificação, número de ocorrências*> é inserida na tabela. Mesmo quando o documento referenciado na mensagem é encontrado, sua data (fornecida no corpo da mensagem-T) é confrontada com a data do documento existente no servidor (campo *data de modificação* na TD). Caso as datas sejam diferentes (versões diferentes de um mesmo documento[13]), aquele referenciado na mensagem é recuperado e armazenado no repositório conveniente.

Para que seja garantida a atomicidade do processo de inserção ou atualização da tupla, as funções que mantém a TD são implementadas através do mecanismo de RMI (*Remote Method Invocation*) provido pela plataforma Java™.

---

[12] O servidor de documentos M/H tem acesso ambos os repositórios de Documentos M/H e de Documentos M/H Seguros. Em virtude disso a verificação é realizada nos dois repositórios, respeitando-se a natureza dos componentes (seguros ou não).

[13] A utilização dos mecanismos de controle de versão pelo SMMM não faz parte do escopo deste trabalho, sendo tema de um trabalho futuro.

A disponibilização no servidor local dos componentes remotos referenciados na mensagem-T deve respeitar as restrições de *hardware*/*software* disponíveis do *site* do usuário de destino. Para tanto, é mantido no servidor SMMM um arquivo de configuração (perfil), onde são listadas as extensões de arquivo suportadas, descrevendo as mídias que o sistema é capaz de tratar. Entre outras coisas, este arquivo de configuração permite ao servidor não solicitar componentes que estejam representados em mídias não tratáveis, eliminando tráfego desnecessário na rede.

Após o término com sucesso do processo, quando todos os documentos referenciados na mensagem-T tiverem sido recuperados e armazenados no servidor de documentos M/H (ou detectados como locais), o servidor SMMM gera a mensagem-R e a disponibiliza na caixa postal do usuário. A mensagem-R contém as mesmas informações da mensagem-T, com exceção das referências aos componentes secundários da mensagem.

Como uma mensagem pode ser enviada a vários destinatários localizados em um mesmo domínio, a TD também mantém um campo "número de ocorrências" com o número de vezes que cada componente é referenciado pelas diversas mensagens armazenadas no servidor. Este campo é utilizado como mecanismo de "coleta de lixo", sendo incrementado sempre que é criada uma nova referência a um componente e decrementado quando da exclusão de referências ao mesmo componente. Desta forma, quando não houver mais referências a um dado documento, ao servidor é permitido exclui-lo.

O processo de recepção de uma mensagem no SMMM pode ser visto na Figura 8.

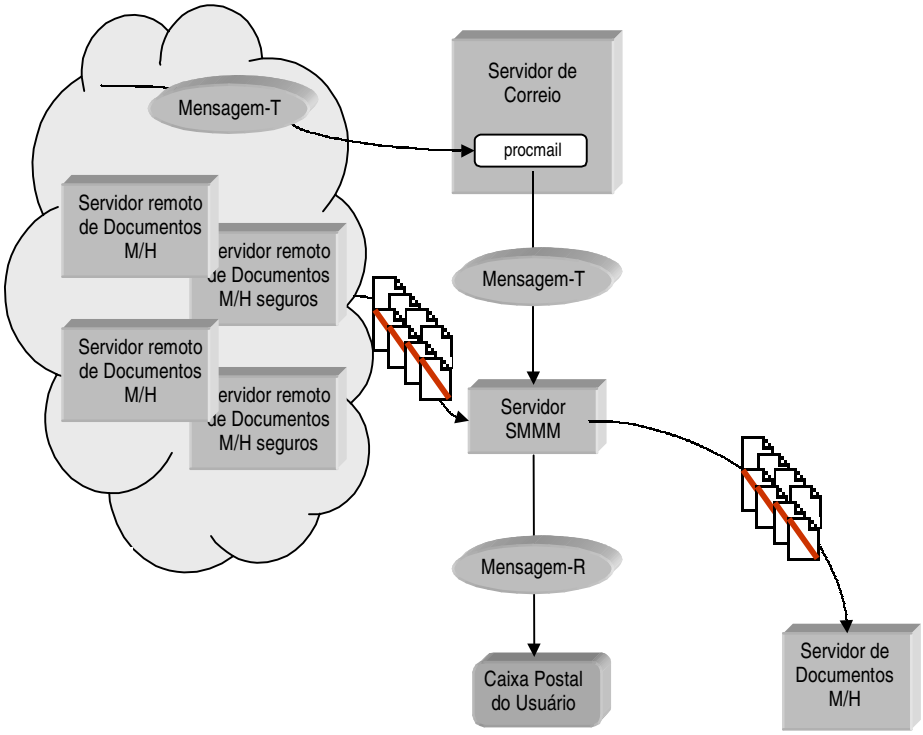

Figura 8 - *Processo de recepção de uma mensagem-M/H no SMMM.*

Após a disponibilização das mensagens-R na caixa postal do usuário, pode-se, então, passar ao processo de visualização, através da IC.

2.4.6 Visualização de uma mensagem no SMMM

Como dito anteriormente, durante a inicialização da interface de correio, esta se conecta ao servidor de correio, configurado previamente pelo usuário (Seção 2.4.2). Após isso, são recuperadas as mensagens disponíveis na caixa postal do usuário[14]. De posse das mensagens, a IC as disponibiliza ao usuário na forma de uma tabela, onde podem ser visualizadas as principais informações sobre as mensagens (endereço do remetente, assunto, data e hora do envio). Para o SMMM, o campo de maior importância, visto através da IC é o campo M/H (correspondente ao campo X-SMMM da mensagem-R em ASCII), que identifica para o usuário as mensagens M/H.

O usuário pode visualizar uma mensagem (Figura 9) através da sua seleção na tabela (cada linha da tabela representa uma mensagem recuperada pela IC). Caso ela seja uma mensagem textual comum, seu conteúdo é exibido normalmente em uma janela de texto; caso seja uma mensagem-M/H, um visualizador de documentos-M/H apropriado é aberto, com o conteúdo da mensagem. Após isso, o destinatário da mensagem pode visualizar normalmente a mensagem, acessando cada um dos seus componentes. Para que o usuário possa ver o conteúdo de componentes seguros, algumas informações são a ele solicitadas.

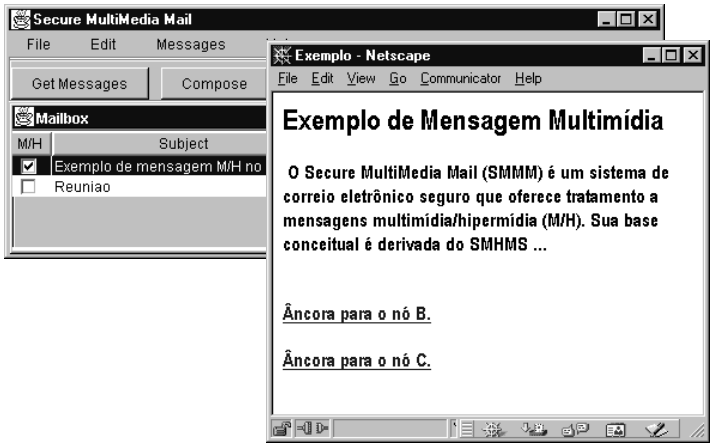

Figura 9 - *Visualização de uma mensagem-M/H no SMMM.*

Quando é solicitada a visualização de componentes confidenciais, para que esses possam se abertos, o servidor SMMM pede, através da interface de documentos M/H, o nome do alias e a senha de acesso da chave privada do destinatário no *keystore* deste usuário. De posse da desta chave privada, o servidor SMMM extrai a chave de sessão (criptografada com a chave pública do destinatário) e, com ela, decripta o documento, que, então pode ser visualizado. Para o caso de mensagens confidenciais, essas informações são solicitadas ao usuário pela IC logo que ele solicita a sua abertura.

Para documentos onde foram aplicados o serviço de integridade, o servidor SMMM solicita ao usuário, através da interface de documentos, o nome do alias e a senha de acesso de sua chave privada no seu *keystore* (destinatário). Com a chave privada do destinatário, o servidor SMMM extrai o *hash* de cada um dos componentes, ao mesmo tempo em que gera novos *hashs* para cada um dos deles[15]. Os *hashs* gerados são, então, comparados com aqueles extraídos dos componentes recuperados pelo servidor SMMM. Quando o resultado for

[14] A recuperação das mensagens do servidor também é possível através do botão "*Get Messages*".

[15] É usada a mesma função geradora de *hash* utilizada pelo remetente da mensagem. A função é definida no corpo da mensagem, ao lado do componente.

positivo, o documento é liberado para a visualização, caso contrário, uma mensagem de erro é exibida ao usuário. Para mensagens transmitidas de forma íntegra, a solicitação do *alias* e da senha é feita através da IC.

Quando é requerida a visualização de documentos autenticados, o processo executado é semelhante ao feito para documentos íntegros. A única diferença é que a chave utilizada para autenticar a mensagem, extraindo os *hashs* íntegros, é a chave pública do remetente. Esta chave deve ser recuperada do *keystore* do destinatário através de seu alias e de sua senha.

É importante dizer que, ao "navegar" em um documento-M/H, é possível que o usuário acesse (solicite a visualização) nós que não tenham sido referenciados na mensagem-T, editada pelo seu remetente. Esses documentos não estarão localizados nos repositórios de documentos M/H locais. Nesse caso, tais nós serão solicitados ao servidor remoto (através de sua URL), o que acarretará uma queda na performance da visualização.

3 CONSIDERAÇÕES FINAIS

O Secure MultiMedia Mail é um sistema de correio eletrônico independente de plataforma implementado na Linguagem Java. Esse sistema introduz novos conceitos, dos quais, destaca-se o conceito de nós sensíveis. No SMMM é permitido ao usuário, na composição de uma mensagem, definir quais os componentes que serão transmitidos de forma segura (nós sensíveis), não sendo assim necessária a aplicação dos serviços de segurança a todos os componentes da mensagem (segurança em bloco). Além disso, podem ser definidos diferentes serviços de segurança para cada um dos nós sensíveis. Dentre os serviços definidos para sistemas de correio eletrônico [Soares97], o único não oferecido pelo SMMM é o de não repúdio, ficando pendente para novas versões do sistema.

O SMMM encontra-se em fase avançada de testes. Até o presente momento, encontram-se implementadas a interface de correio, o servidor SMMM . Na fase atual da implementação, a integração com o servidor e a interface de documentos[16] está sendo realizada [Muchaluat98, Rodrigues98].

A arquitetura do sistema foi definida a partir da arquitetura original do MMM. Devido aos requisitos de segurança, adicionados à idéia original de um sistema de correio eletrônico multimídia, foram incluídos ou modificados alguns dos módulos da arquitetura.

A atual implementação do SMMM oferece serviços de segurança que utilizam o DES como padrão (algoritmos) de criptografia simétrica, o RSA para a criptografia assimétrica e o MD5 como função geradora de *hash*.

A arquitetura do SMMM é aberta. No futuro, outras opções de algoritmos de criptografia serão incorporadas ao sistema.

Durante a implementação do SMMM, pôde-se constatar que, devido às questões de segurança envolvidas no seu funcionamento (transmissão de mensagens), os requisitos de economia de espaço de armazenamento e de redução do tráfego na rede, citados na seção 2.4.1, estavam sendo prejudicados, pois a adição de segurança ao intercâmbio de mensagens multimídia, exige que a partir de um mesmo documento sejam gerados, para cada um dos destinatários de uma mensagem-M/H, vários arquivos com o mesmo conteúdo, mas criptografados diferentemente, e depositados no repositório de documentos seguros[17]. Para resolver tal

[16] O servidor e a interface de documentos M/H foram implementados separadamente (também em Java). Ambos fazem parte da implementação do modelo NCM, como parte do projeto HyperProp. Tal implementação continua sendo realizada no laboratório Telemídia da PUC-Rio.

[17] Por exemplo, quando uma mensagem é enviada íntegra a vários destinatários, um mesmo arquivo tem seu *hash* criptografado com as chaves públicas de todos os destinatários, e disponibilizado no repositório de documentos seguros em vários arquivos diferentes.

problema, foi elaborada uma política de níveis de acesso para o SMMM, onde existirão chaves de usuário, de grupo e de domínio (algo semelhante ao usado no sistema operacional UNIX para o acesso a arquivos). Assim, um usuário poderá enviar uma mensagem para um grupo e não, várias mensagens para destinatários diferentes. Isso resultará na economia de espaço de armazenamento tanto no *site* de origem, onde os arquivos são armazenados até que sejam recuperados, quanto no *site* de destino. Este problema está sendo estudado e sua solução deverá ser futuramente acrescida ao sistema.

4 BIBLIOGRAFIA

[Batista96] Batista, T.; Rodriguez, N. L. R.; Soares, L. F. G. & Resende, M. C. "MMM: Um Correio Eletrônico Multimídia sobre o WWW", *Anais do 14º Simpósio Brasileiro de Redes de Computadores (SBRC)* , Fortaleza - CE, Maio de 1996.

[Cavalcanti97] Cavalcanti, E. C.; Cirne Filho, W. C; Brasileiro, F.V. "Introduzindo Segurança no Correio Eletrônico Internet" *Anais do 15º Simpósio Brasileiro de Redes de Computadores (SBRC)*, São Carlos - SP, Maio de 1997.

[Crocker82] Crocker, D.H. "Standard for the Format of ARPA Internet Text Messages". *RFC 822*. Agosto 1982

[Comer93] Comer, D. *Internetworking with TCP/IP - Volume III*. Prentice-Hall Inc. 1993

[Edwards91] Edwards, W.K. "The Design and Implementation of the Montage Multimedia Mail System". *Proceedings of TRICOMM'91*. Chapel Hill, NC, USA. Abril 1991. pp. 47-57.

[Elkins96] Elkins, M. "MIME Security with Pretty Good Privacy (PGP)", *RFC 2015*, Outubro de1996.

[Halasz94] Halasz, F.; Schwartz, M. "The Dexter Hypertext Reference Model". *Communications of the ACM*, 37 (2), Fevereiro de 1994. pp. 30-39.

[Kaufman95] Kaufman, C.; Perlman, R. & Speciner, M. *Network Security - PRIVATE Communication in a PUBLIC World*. Prentice-Hall Inc. 1995

[Ouhyoung94] Ouhyoung, M. et al. "The MOS Multimedia E-mail System" IEEE 1994

[Postel82] Postel, J.B. "Simple Mail Transfer Protocol", *RFC 821*, Agosto de 1982.

[Prabhu96] Prabhu, M. & Raghavan, S. "Security in computer networks and distributed systems", *Computer Communications*, No. 19, (1996).

[Lynch93] Lynch, D. C.; Rose, M. T. *Internet System Handbook*. Addison-Wesley Publishing Company, Inc., 1993.

[Muchaluat98] Muchaluat, D. C.; Rodrigues, R. F.; Soares, L. F. G. *Navegação e Consulta no WWW Através de Browser Gráfico Usando Visões Olho-de-Peixe*. XXV Seminário Integrado de Software e Hardware, Anais do XVIII Congresso da Sociedade Brasileira de Computação, 1998.

[Rodrigues98] Rodrigues, R. F.; Soares, L. F. G. *Integração dos Sistemas HyperProp e WWW*. Simpósio Brasileiro de Multimídia SBMIDIA'98.

[Schneier95] Schneier, B. E-Mail Security — How to Keep your Electronic Messages Private. John Wiley & Sons. 1995.

[Soares93] Soares, L. F. G.; Rodriguez, N. L. R.; Colcher, S. "An Architecture for Hypermedia Systems Using MHEG Standard Objects Interchange". *Proceedings of the Workshop on Hypermedia and Hypertext Standards*. Amsterdam, The Netherlands. Abril de 1993.

[Soares94a] Soares, R.A.M.; Soares, L.F.G. "SMHMS: Um Correio Eletrônico Multimídia/Hipermídia", *Anais do 12º Simpósio Brasileiro de Redes de Computadores (SBRC)*, Curitiba - Pr, Maio de 1994.

[Soares94b] Soares, L. F. G.; Rodriguez, N. L. R.; Casanova, M. A. "Modelo de Contextos Aninhados: um Modelo Conceitual Hipermídia". *Revista Brasileira de Computação*, 7(2). Janeiro de 1994.

[Soares95] Soares, L.F.G. "Hyperprop: Uma Visão Geral". *I Workshop em Sistemas Hipermídia Distribuídos*, São Carlos, São Paulo. Julho de 1995.

[Soares97] Soares, L.F.G; Lemos, G.; Colcher, S. *Redes de Computadores – Das LANs, MANs e WANs às Redes ATM*. Segunda Edição — Rio de Janeiro: Campus, 1997.

[Thomas85] Thomas, R. H.; Forsdick, H. C.; Crowley, T. R.; Schaaf, R. W.; Tomlinson, R.S.; Travers, V.M.; Robertson, G.G. "DIAMOND: A Multimedia Message System Built on a Distributed Architecture". *IEEE Computer Magazine*, Dezembro de 1985, Vol.23, Nº 12, pp.65-77.