Certificados Digitais: Uma ferramenta desenvolvida com base no padrão SET

Tommy Jakobsen

Profª Drª Maria Janilce B. Almeida (orientador)

(tommy, janilce)@inf.ufrgs,br

Universidade Federal do Rio Grande do Sul

Instituto de Informática

Av. Bento Gonçalves, 9500 - Bloco IV - Campus do Vale

CEP 91501-970 - Tel.: +55.51.316.6168 - Fax.: +55.51.316.7029

Resumo

O comércio eletrônico será uma das mais importantes maneiras de fazer negócios no futuro, porém seu crescimento tem sido lento devido a problemas de segurança. O padrão SET, criado em 1996 por um consórcio de empresas e entidades, oferece um alto grau de segurança às transações eletrônicas[1], contudo ainda não se tornou um padrão de fato devido a sua grande complexibilidade. O padrão SET é basicamente dividido em 2 partes: sistemas de pagamento e gerenciamento de certificados [2]. Nesse artigo teremos uma visão geral do SET, seu funcionamento, objetivos e características, bem como o gerenciamento de certificados, objeto do trabalho que esta sendo desenvolvido no momento.

O grande número de processos criptográficos utilizando diversos algoritmos diferentes, como DES [14] e RSA [13], a necessidade de um modelo distribuído eficiente para emissão, renovação e revogação de certificados, e a grande complexibilidade envolvida no desenvolvimento de soluções compatíveis com o SET, são os principais fatores que tem inibido sua aceitação.

Neste contexto, em 1998 na UFRGS, foi desenvolvido um conjunto de aplicações denominado SET-F [3], cujos principais objetivos são: facilitar o uso do sistema de pagamento baseado no padrão SET, garantindo a sua compreensão, e também fornecer ao mercado do comércio eletrônico uma ferramenta de segurança a baixo custo para empresas de pequeno e médio porte. Dando continuidade a esse trabalho, agora estão sendo desenvolvidas aplicações para permitir o gerenciamento de certificados, ainda não contemplado pelo SET-F. Estas aplicações, além de facilitar a utilização de um sistema para gerenciar certificados digitais(obtenção, renovação e revogação) fornecerão maior grau de segurança ao SET-F através da autenticação das partes envolvidas na transação.

Abstract

E-Commerce will be one of the most important way to do business in the early future, however its growth has been slow because of security problems. The SET (Secure Electronic Transaction) standard, created in 1996 by a group of enierprises and entities, provides a high level of security in electronic transactions over Internet, however it isn't a standard in fact yet due to its high complexibility. SET is divided into two parts: the first defines the payment

6. CONCLUSÕES

Apesar da arquitetura proposta pelo SET ser muito eficiente nos aspectos relacionados ao atendimento dos requisitos necessários para o processamento seguro de transações eletrônicas em redes abertas, como a *Internet*, uma série de fatores atualmente ainda inibem a sua aceitação no mercado como uma solução definitiva para os problemas de segurança. Sendo alguns deles, talvez os maiores, a alta complexibilidade do padrão e alto custo de implementação para empresas de pequeno e médio porte.

Um dos maiores desafios que enfrentados na implementação do protótipo, para o gerenciamento de certificados, é a alta complexibilidade e falta de informações precisas na especificação fornecida pelo SETCo. A utilização do padrão depende de uma série de requisitos que devem ser observados e corretamente seguidos pelos desenvolvedores. Alguns deles são: obedecer a rígida seqüência de passos para a obtenção ou renovação dos certificados digitais; observar a correta utilização dos inúmeros algoritmos de criptografia, dos métodos de assinaturas, e rotinas de encapsulamento envolvidos no processo de obtenção, renovação revogação de certificados digitais, e a preocupação com o correto funcionamento destes mecanismos em um ambiente distribuído. Além disso, há a preocupação com o adequado armazenamento das chaves secretas/privadas e dos certificados, ponto onde reside uma das maiores fragilidades do padrão, que até o momento não apresentou nenhuma solução deixando o problema a cargo dos desenvolvedores [15].

Desta forma, a dificuldade de acesso a informações sobre implementações bem sucedidas do modelo, bem como a ausência de bibliotecas que visem facilitar o desenvolvimento de aplicações baseadas no padrão SET, constituem os principais fatores para a evolução do SET como um padrão de fato, para o processamento de transações seguras na *Internet*.

O presente trabalho tem como meta principal, desenvolver um sistema de gerenciamento de certificados com o objetivo fundamental de reduzir, a medida do possível, a complexibilidade inerente ao padrão SET, aumentando assim a sua utilização por parte de comerciantes e proprietários de cartão de crédito, e por conseqüência, contribuir para o crescimento do comércio eletrônico. Através da incorporação do protótipo, do sistema de gerenciamento de certificados desenvolvido, ao SET-F, será possível aumentar seu grau de segurança, visto que de posse de seus certificados os proprietários de cartão de crédito e comerciantes poderão ser autenticados.

pronto. Assim que esse processamento estiver concluído, o proprietário do cartão terá em seu poder o seu certificado digital e, a partir deste momento, estará apto comprovar sua identidade onde necessário.

A figura 5 ilustra os passos seguidos pelo protocolo para informar à consumidores, comerciantes o estado atual de seu pedido de certificado digital. [6].

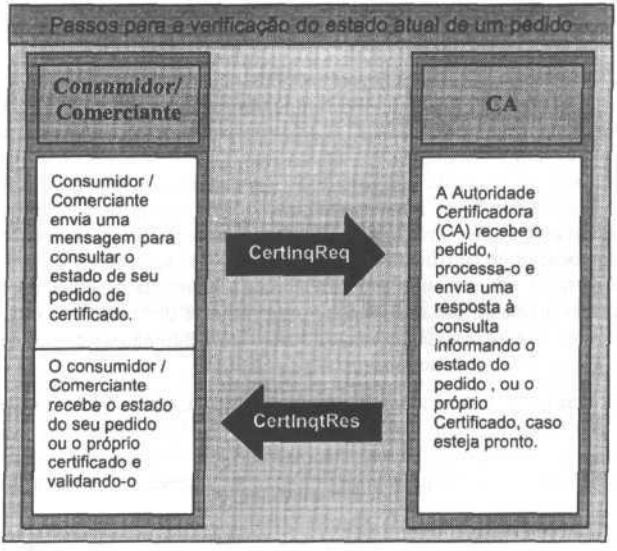

FIGURA 5 - Passos do protocolo para consultar o estado do pedido.

• A CA então responde com a mensagem MeAqCInitRes (*Merchant Acquirer CertificateInitiation Response)*, que por sua vez, contém o modelo do formulário apropriado a ser preenchido pelo comerciante. Esta mensagem contém as seguintes informações: os certificados e parâmetros necessários para a realização de procedimentos de criptografia e assinatura; o conjunto de regras ou políticas com as quais o comerciante deve concordar, e o formulário apropriado.

• A partir deste ponto o protocolo segue os mesmos passos do processo anterior, ou seja, o comerciante envia um CertReq , recebe um CertRes, assim por diante.

Urna das diferenças entre os dois protocolos é que comerciantes necessitam de dois pares de chaves pública/privada, uma utilizada somente para assinatura e outra utilizada para intercâmbio de mensagens criptografadas. Assim sendo, quando o processo for disparado, comerciantes devem estar aptos a gerar dois pares de chaves assimétricas e envias as duas chaves públicas à CA.

A figura 4 ilustra o protocolo seguido pelos comerciantes e CAs para a requisição e obtenção de novos certificados [6].

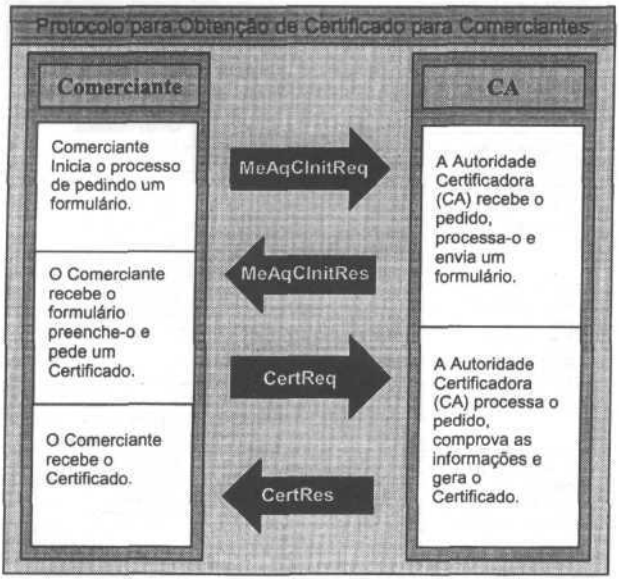

FIGURA 4 - Protocolo para obtenção de certificados para comerciantes

Em algumas implementações, pode não ser possível para a CA fazer o envio imediato dos certificados a seus solicitantes. Neste caso, é possível para consumidores (proprietário de cartão) e comerciantes, realizar consultas que lhe permitam receber informações sobre o *status* da sua requisição. Este procedimento é realizado através do envio de uma mensagem CertInqReq (*CertificateInquiry Request*), que é respondida pela CA com a mensagem CertInqRes *(Certificate Inquiry Response).* A mensagem CertInqRes conterá informações relativas ao *status* atual da emissão do certificado ou o próprio certificado digital, caso esteja

• A CA valida as informações do formulário, número da conta, e gera o certificado, assinado com sua chave privada, e envia-o ao consumidor na mensagem CertRes (*Certificate Response).*

• O consumidor recebe o novo certificado da CA e o armazena em seu computador, para ser utilizado mais tarde para transações de comércio eletrônico. O SET sugere que o Certificado outras informações sensíveis devem ser armazenadas de forma segura, não define como esse certificado deve ser feito o armazenado.

A figura 3 ilustra o protocolo seguido pelos consumidores / proprietários de cartão de crédito e autoridades de certificação para emissão de novos certificados [6].

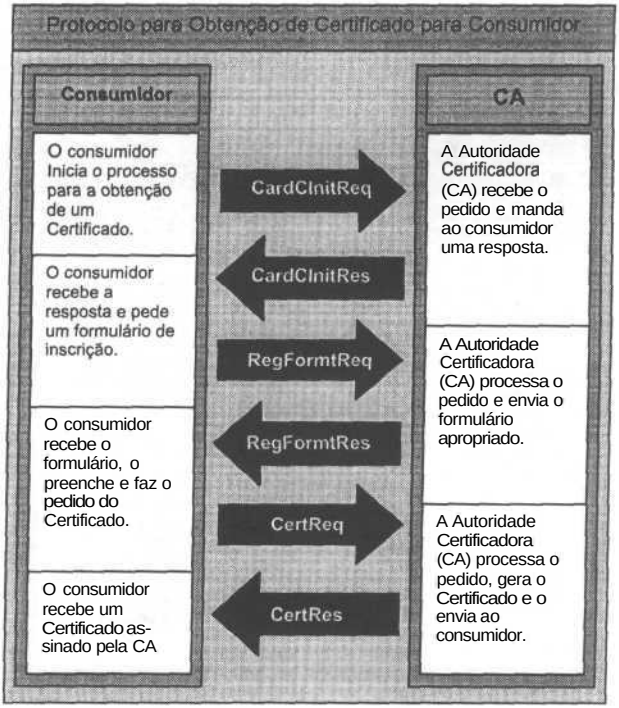

FIGURA 3 - Protocolo para obtenção de certificados para consumidores

O protocolo para a obtenção ou renovação de certificados novos para um comerciante, e seguido no desenvolvimento da ferramenta, é semelhante ao processo anterior e percorre os passos:

• O comerciante inicia o processo enviando uma mensagem MeAcCInitReq (*Merchant-AcquirerCertificate Initiation Request*), contendo a lista de certificados aceitos e demais parâmetros necessários no processo.

desenvolvedores. Por exemplo, quando a especificação trata da revogação de certificados digitais, ela apenas define os motivos pelos quais um certificado deve ser revogado, deixando por conta dos desenvolvedores a maneira de fazer isso. Como não existem definições de mensagens para realizar essa operação, perde-se a padronização dos sistemas baseados no SET.

Dentro da especificação do SET existem dois tipos de mensagens: mensagens de pedido de certificados (escopo do trabalho que esta sendo desenvolvido atualmente) e as mensagens do sistema de pagamentos (escopo do *framework* SET-F e não serão apresentadas aqui).

Em adição as mensagens de pedido de certificados e mensagens do sistema de pagamentos, temos as mensagens de erro. Estas mensagens são usadas para avisar a quem enviou uma requisição que o destinatário não conseguiu, por algum motivo, processar a mensagem ao recebe-la.

No sistema gerenciador de certificados, baseado no especificação do padrão SET, os consumidores deverão possuir as seguintes requisitos antes de se tornarem aptos a pedir e obter um certificado digital a uma CA: uma conta válida com alguma operadora de cartões de crédito; habilidade de gerar um par de chave pública; uma URL *(Universal Resource Locator)*; e um *browser* compatível com o SET.

Igualmente comerciantes deverão possuir os seguintes requisitos: uma identificação válida perante um banco; habilidade de gerar pares de chaves públicas; uma URL; e um *browser* compatível com o SET.

O processo de obtenção de novos certificados pelos consumidores/proprietários de cartão de crédito (tratado pelo SET como *Cardholder*), e seguido no desenvolvimento da ferramenta, se dá percorrendo os passos do protocolo:

- O processo inicia quando o consumidor envia uma mensagem CardCInitReq *(Cardholder CertificateInitiation Request)* à CA.

- A CA então recebe a mensagem e gera a resposta, enviando a mensagem CardCInitRes *(Cardholder Certificate Initiation Response),* contendo os seus certificados e demais parâmetros necessários para a verificação de assinaturas e criptografia de informações nos próximos passos. O certificado de criptografia da CA fornece ao *software* do consumidor informações necessárias para proteger o número do cartão de crédito no pedido de formulário de registro.

- Consumidor recebe o CardCInitRes, verifica assinaturas, armazena o certificado enviado pela CA, cria e envia uma mensagem RegFormReq *(Registration Form Request)*, solicitando o formulário que será preenchido com seus dados. Neste ponto é utilizado o conceito de envelope digital para criptografar o número da conta ou cartão.

- A CA recebe o RegFormReq identifica a instituição financeira com a qual o consumidor mantém uma conta, seleciona o formulário adequado de registro e então responde com a mensagem RegFormRes *(Registration Form Response),* contendo o formulário e um modelo de preenchimento, para que o proprietário do cartão possa efetivar a requisição.

- Ao receber o RegFormRes *software* do consumidor gera um par de chaves pública/privada, preenche o formulário, e envia as informações (chave pública, formulário e número do cartão) criptografadas através de uma mensagem CertReq *(Certificate Request),* informando à CA que está pronto para receber o certificado.

5. O DESENVOLVIMENTO DO PROTÓTIPO

O ambiente genérico para o funcionamento do modelo consiste dos seguintes componentes: o *browser* do consumidor (ou proprietário do cartão de crédito), o *browser* do comerciante e o servidor *Web* da autoridade certificadora.

A figura *2* apresenta a arquitetura do modelo proposto.

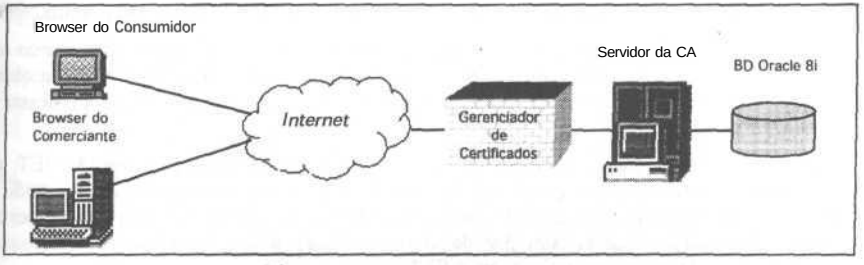

FIGURA *2* - Arquitetura do Modelo Proposto

Uma vez acionada a aplicação através browser do Consumidor ou do Comerciante, será então estabelecida uma conexão TCP/IP com o *deamon* do protótipo instalado no servidor da CA, que fornecerá os serviços, como emissão ou renovação de certificados, que estão sendo requisitados. Na CA será utilizado um BD Oracle 8i para o armazenamento de certificados e chaves. O sistema Gerenciador de Certificados esta sendo desenvolvido na linguagem de programação Java 1.2, visto que esta possui pacotes de segurança com uma ampla diversidade de classes e métodos que podem ser usados para criptografar, assinar, verificar assinaturas, armazenar e recuperar chaves e certificados. Por ser o Java uma linguagem de programação voltada para a *Internet,* foi criada de maneira que fosse independente de plataforma ou sistema operacional, sendo essa uma das principais vantagens na sua utilização.

Um dos problemas enfrentados na implementação da ferramenta foi conseguir, gratuitamente, bibliotecas capazes de fornecer mecanismos de criptografia fortes como por exemplo, a geração de chaves criptográficas grandes o suficientes para não serem quebradas por intrusos. Esse problema tem origem na política oficial do governo norte-americano em restringir a exportação de *software* que gerasse tal (tamanho) chave.

A extensão de criptografia da linguagem Java (JCE) fornece, entre outras coisas, vários mecanismos para realizar a codificação e decodificação de dados arbitrários, não esta disponível no *Kit* de desenvolvimento Java (JDK). Como a Sum Microsystems, desenvolvedor do Java, tem um centro de operações nos Estados Unidos, a exportação do JCE fica estritamente limitado pelas restrições impostas pelo governo norte-americano. Devido a essa implementação ser capaz de uma codificação forte, os únicos países onde pode ser utilizada são nos Estados Unidos e no Canadá. Porém todas estas restrições não evitaram que diversas empresas ou grupos implementassem novamente, fora dos Estados Unidos, suas próprias APIs do JCE, e atualmente existem diversos provedores de segurança disponíveis fora dos Estados Unidos [8].

Outro problema com relação a implementação dos protocolos baseados no padrão SET, é que alguns pontos da especificação ficam obscuros, não sendo bem definidos aos

Um dos requisitos de segurança sugeridas pelo padrão SET, e ainda não é contemplada no *framework* SET-F, é a autenticação de todas as partes envolvidas em uma transação eletrônica, realizada através de certificados digitais.

Na segunda fase deste projeto iniciado em 1998, esta sendo desenvolvido o protótipo de uma ferramenta cuja finalidade é gerenciar os certificados de identidade digital e chaves secretas, das entidades que participam de transações eletrônicas baseadas no padrão. Dentro do gerenciamento de certificados digitais baseado no padrão SET encontramos atividades como: processamento de pedidos e obtenção de certificados digitais, a renovação de certificados (ex: quando expira a data de validade de um Certificado), e revogação ou cancelamento de certificados (ex: quando chaves privadas são comprometidas).

A validação do sistema será realizada através do protótipo da ferramenta que estamos desenvolvendo, que incorporado ao *Framework* SET-F, fornecerá uma maneira de: gerenciar os certificados das entidades participantes, o que deverá garantir os requisitos básicos de segurança para transações comerciais eletrônicas; oferecer a necessária facilidade de uso, quer seja no desenvolvimento, quer seja na utilização efetiva da tecnologia; e finalmente, permitir um alto grau de padronização e conformidade com o conceito de sistemas abertos. A incorporação deste aplicativo ao SET-F garantirá um alto nível de segurança às transações, já que todas as partes, de posse de seus certificados, poderão ser autenticadas.

sofisticado cartão de visitas, que propicia que entidades remotas se apresentem, de modo que uma, tome ciência da identidade das demais;

2. Permitir que terceiros transmitam arquivos, mensagens, etc, criptografados (privados e seguros) endereçados ao proprietário do certificado, tendo ambos a certeza que ninguém mais, além do próprio proprietário, poderá ter acesso aos seus conteúdos originais. O remetente deverá utilizar a chave pública de criptografia constante no certificado digital para criptografar os dados destinados ao seu proprietário;

3. Permitir que terceiros verifiquem as assinaturas digitais geradas e postas em arquivos, mensagens, etc. pelo proprietário do certificado digital, com uso da sua chave privada de criptografia. A assinatura digital substitui a uma assinatura escrita, e fornece uma ligação legal do autor com o documento que foi assinado e transmitido.

A CA assina os certificados digitalmente com sua chave privada, de forma que essa assinatura poderá ser confirmada, por qualquer pessoa, com a chave pública, que deverá ser amplamente distribuída. Ao assinar um certificado, a CA garante sua validade. No entanto, um problema ainda persiste: como a chave pública da CA é distribuída? Existem muitas estratégias para tratar esse problema. Uma delas, se a CA é bem conhecida, como no caso do serviço postal americano, ela poderia divulgar amplamente sua chave pública. Outro método seria se a CA tivesse seu próprio certificado assinado por uma outra CA, também reconhecida pelo destinatário. Essa é a idéia de encadeamento de certificação e pode avançar ainda mais, com várias CAs organizadas em uma hierarquia, onde cada CA subordinada valida sua assinatura com a assinatura de uma CA de mais alta hierarquia. Obviamente as CAs de nível mais alto deverão reverter para o método de divulgação direta.

Para utilizar o protocolo SET, todas as partes envolvidas em uma transação (consumidores, comerciantes e bancos) precisam de uma prova de identidade, que garanta estarem habilitados a executarem tal transação. Essa prova de identidade é conhecida como "Certificado Digital".

Este esquema de certificação baseia-se na confiança comum entre uma CA ou cadeia de CAs, cada uma certificando a outra de mais baixo nível. A legitimidade de um certificado pode ser verificada descriptogranfando-o com a chave pública da CA que o assinou. Esta chave pública deve estar amplamente disponível e deve ser obtida de fonte idônea. Através dos certificados digitais, o consumidor pode ter certeza de que está diante de um comerciante legítimo, devidamente identificado por uma CA, e não um impostor fazendo-se passar por ele. Da mesma forma, o comerciante pode ter a garantia de que o consumidor é realmente quem afirma ser, pois confia na CA que emitiu o certificado deste. Todo esse processo é transparente ao usuário.

As funções básicas de uma autoridade certificadora e contempladas na ferramenta que esta sendo desenvolvida são: receber pedidos para obtenção de certificados; processar estes pedidos e aprovar ou nega-los; e finalmente emitir e enviar o certificado digital a quem fez a requisição.

A segurança do SET depende em última instância da autenticidade dos certificados digitais utilizados no sistema. Estes certificados são verificados, conferindo a cadeia de certificados até o Certificado da Autoridade Certificadora Raiz. Apenas por meio da confiança no certificado raiz a confiança no sistema SET poderá ser mantida.

1) Todos os participantes envolvidos numa transação SET devem obter certificados digitais de uma Autoridade Certificadora (CA) idônea (foco do trabalho);
2) O comerciante envia seu certificado digital ao consumidor;
3) O consumidor verifica a autenticidade do comerciante, e envia o pedido de compra e seu certificado digital ao comerciante;
4) O comerciante verifica a autenticidade do consumidor e repassa a solicitação de pagamento ao banco com o qual ele tem relação;
5) O banco verifica o crédito do consumidor e confirma/não a transação ao comerciante;
6) O comerciante processa o pedido de compra e envia os bens/serviços ao consumidor.

4. CERTIFICADO DIGITAL

Mas como saber que a pessoa com quem nos comunicamos via *Internet* realmente é quem diz ser? Entre um consumidor e um comerciante por exemplo, é muito importante para o consumidor confiar que o comerciante, a quem ele esta fornecendo informações de pagamento sensíveis (número do cartão de crédito), é legítimo. Por outro lado é importante para um comerciante que vende artigos ou serviços assegurar que o consumidor, que forneceu as informações de pagamento, esta realmente autorizado a fazer o pagamento. Depois que a transação for consumada, é importante para ambas as partes provar que participaram da transação e que cada um é responsável por suas respectivas obrigações.

Existem vários meios de solucionar este tipo de problema. Um deles é trocar chaves públicas através de um meio direto, como uma reunião ou um telefonema por exemplo. Infelizmente este método não funciona bem quando existem muitas pessoas envolvidas. Uma outra opção seria a utilização de certificados digitais e dos serviços das autoridades de certificação digital (CAs).

O certificado é um documento digital contendo informações de identificação e uma chave pública. Em geral, os certificados tem um formato comum, normalmente baseado no padrão ITU X-509. Mas ainda não podemos ter certeza de que o certificado é genuíno, ou seja, que não *é* falso. Uma forma de descobrir isso é utilizar autoridades de certificação ou CAs (*CertificatuAuthority*). As CAs são os órgãos, semelhantes aos cartórios, que emitem os certificados digitais.

O certificado digital é um documento eletrônico emitido por um agente idôneo e confiável, denominado "Autoridade Certificadora", declarando que a chave pública de quem fez o pedido do certificado tem determinado valor. O certificado digital é então emitido, assinado (chancelado), e garantido por essa Autoridade Certificadora, que comprova as informações fornecidas pelo solicitante em cartórios e outros estabelecimentos. O certificado digital poderá então ser apresentado como prova de identidade onde seja necessária a comprovação de identidade [5], evitando assim que uma pessoa ou empresa se passe por outra.

O SET utiliza 2 tipos de certificados digitais, os certificados utilizados somente para assinatura de documentos ou informações e certificados de criptografia.

Os certificados digitais tem três finalidades:

1. Transmitir, de forma confiável, os dados de identificação e a chave pública do seu proprietário (identificado no campo *subject* do certificado digital) a terceiros, com os quais ele venha a se comunicar remotamente. Simplificando, um certificado digital seria um

virtualmente impossível de alterar uma mensagem sem que o seu *hash* se altere. Isso possibilita que o destinatário, recebendo uma mensagem, possa verificar a sua integridade recalculando o *hash* da mensagem e comparando-o com o valor original, recebido junto com a mensagem. O *hash* deve ser criptografado antes de sua transmissão ao destinatário para que não seja passível de alterações durante o trajeto.

O SET utiliza dois métodos consagrados, o algoritmo de chave pública RSA, que tem como nome as iniciais de seus criadores, Rivest, Shamir e Adleman, e o algoritmo DES (*Data Encryption Standard),* desenvolvido pela IBM, ambos com mais de 20 anos de existência. Além disso, o SET utiliza-se de técnicas mais recentes, como o algoritmo de *Hashing* SHA-1 (*Secure Hash Algorithm*), a otimização pré-RSA OEAP (*Optimal Asymmetric Encryption Padding*), além de uma versão mais leve do DES denominada de CDMF (*Cryptographic Data Masking Facility*). Cada um destes algoritmos desempenha um papel importante dentro do protocolo, e são utilizados nesse caso para alcançar a segurança necessária sem no entanto comprometer o desempenho global da solução.

O elevado custo computacional do algoritmo RSA e o problema do gerenciamento das chaves simétricas, quando aplicada à transações em larga escala na *Internet*, são equacionados pelo SET, aproveitando o melhor dos dois algoritmos ao utilizar o conceito de "envelope digital". Com esse conceito, o SET utiliza, por motivos de desempenho, os algoritmos simétricos DES e CDMF para criptografar a mensagem. Já o problema da distribuição de chaves simétricas é solucionado "envelopando-a" dentro de uma mensagem, criptografada com o sistema de chave pública RSA, ou seja, a chave simétrica utilizada para criptografar a mensagem é criptografada com a chave pública (RSA) do destinatário. Como somente o destinatário possui a chave privada correspondente e a mantém em segredo, somente ele poderá decifrar e recuperar a chave simétrica, que por sua vez será utilizada para decifrar a mensagem. Como o tamanho da chave simétrica é pequeno o processo assimétrico é relativamente rápido.

Com o uso das técnicas descritas anteriormente o SET consegue uma comunicação segura a baixo custo, com autenticação da fonte (RSA), confidencialidade na entrega (DES) e verificação da integridade do conteúdo (SHA-1). Estas técnicas estão sendo disponibilizadas no protótipo da ferramenta que esta sendo desenvolvida.

Em uma transação típica, que utiliza padrão SET, o consumidor entra em contato com o comerciante, via *Internet,* escolhe os produtos deseja adquirir, e faz o pedido. A figura 1 apresenta resumidamente as etapas percorridas pelo protocolo.

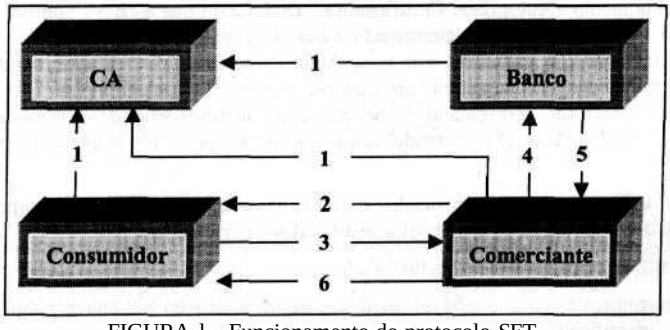

FIGURA 1 - Funcionamento do protocolo SET

A operação inversa é:

M = Descriptografa(C,X)

Onde:

C = Chave, M = Mensagem, X = Mensagem Criptografada.

O grande problema desse tipo de criptografia é a distribuição das chaves quando o número de usuários é muito grande.

Outra forma de criptografia, chamada de assimétrica, tem como diferencial o fato de requerer o uso de um par de chaves para cada parte envolvida na transação, onde uma das chaves é chamada privada e é mantida em segredo, e a outra, chamada de pública, é livremente divulgada. Daí a denominação de criptografia de chave pública. Este tipo de criptografia utiliza uma função matemática que garante que uma mensagem criptografada com a chave pública de alguém somente poderá ser decifrada utilizando-se a correspondente chave privada do par. Da mesma forma, uma mensagem criptografada com a chave privada somente pode ser decifrada com a chave pública correspondente.

Os relacionamentos entre as operações de criptografar e descriptografar com as duas chaves pode ser expressa através da seguinte fórmula:

M = Descriptografa(C_Publ, Criptografa(C_Priv, M))
M = Descriptografa(C_Priv, Criptografa(C_Publ, M))

Onde:

C_Publ = Chave pública do par (Chave Pública, Chave Privada);
C_Priv = Chave Privada do par (Chave Pública, Chave Privada);
M = Mensagem.

Deste relacionamento concluímos que se criptografarmos uma mensagem com a chave pública de alguém somente este, com a correspondente chave privada, poderá decifrá-la. Logo, assegura-se a confidencialidade das informações na comunicação.

Da mesma forma, se alguém criptografar uma mensagem usando sua chave privada, esta mensagem somente poderá ser decifrada com a correspondente chave pública do par. No entanto, qual a vantagem neste procedimento, já que a chave pública é amplamente divulgada e qualquer pessoa pode ter acesso a esta chave e decifrar a mensagem? A resposta é que com esse procedimento asseguramos a autenticidade da mensagem, funcionando como uma assinatura digital, pois ninguém mais poderia ter a chave privada senão o seu legítimo dono/ remetente, que a mantém em absoluto segredo.

Como a chave privada gerada pelo algoritmo assimétrico não pode ser divulgada nunca, não existe problema em enviar a chave pública por canais inseguros e passível de ser interceptada. Isso facilita muito a tarefa de gerenciamento e distribuição de chaves. A grande desvantagem em utilizar criptografia de chave pública é a alta demanda de recursos computacionais, diretamente proporcional ao tamanho da mensagem a ser criptografada e ao tamanho da chave a ser utilizada.

Comparativamente a criptografia assimétrica à criptografia simétrica oferece vantagens quanto a sua velocidade de processamento, porém há um sério problema quando se trata do gerenciamento das chaves.

Adicionalmente o SET utiliza outra função criptográfica, denominada *hash*, que produz uma espécie de impressão digital da mensagem, algo como um dígito verificador para aquele conteúdo. O motivo que caracteriza uma boa função de *hash* reside no fato de ser

O SET tem os principais objetivos: oferecer confidencialidade sobre as informações relacionadas a pagamentos e pedidos de compra; assegurar a integridade das informações; oferecer a autenticação de que o proprietário do cartão é um usuário de uma conta legítima em uma administradora de cartões; oferecer a autenticação de que o comerciante está habilitado a aceitar pagamentos de determinada marca de cartão, através do seu relacionamento com uma instituição financeira; assegurar o uso das melhores práticas de segurança e técnicas de projeto de sistemas para proteger todas as partes envolvidas na transação de compra eletrônica; criar um protocolo que não dependa de mecanismos de segurança no nível de transporte e não "impeça seu uso"; facilitar e encorajar a interoperabilidade entre provedores de *software* e serviços de rede.

Através de operadores de encapsulamento, combinando criptografia com assinaturas digitais, o SET fornece um alto grau de segurança na integridade das informações, bem como na autenticação das entidades finais. O encapsulamento é utilizado em quase todas as mensagens SET [7]. Se por um lado o encapsulamento fornece um alto grau de segurança do protocolo, por outro, contribui para o aumento da sua complexibilidade.

O padrão SET utiliza criptografia de chave pública e secreta (assimétrica e simétrica) para garantir a segurança das transações, através da verificação de assinaturas e confidencialidade das informações. Isso fornece os requisitos necessários para a existência de elementos importantes e desejáveis, tais como a confidencialidade das informações de pagamentos e pedidos, a verificação de integridade das mensagens e a autenticação das partes envolvidas em uma transação (consumidores, comerciantes e bancos).

No SET, bem como na ferramenta que esta sendo desenvolvida, cada parte envolvida na transação, tem acesso somente às informações necessárias ao desempenho de seu papel na transação, ou seja, o comerciante não tem acesso ao número do cartão de crédito do consumidor e a operadora do cartão não tem acesso ao objeto da transação, desta forma os hábitos proprietários de cartão de crédito ficam livres do escrutínio indesejável, e o número do cartão de crédito fica resguardado de olhos alheios à instituição de crédito. Isso oferece uma segurança maior do que aquela proporcionada com o uso tradicional do cartão em um estabelecimento comercial, onde o comerciante obtém o número do cartão de crédito e a operadora de cartões obtém dados sobre a transação efetuada.

Para garantir a confidencialidade da mensagem na *Internet*, mesmo que ela seja interceptada por um ***intruso***, esta deve ser criptografada. Basicamente, a criptografia "mistura" os bits de uma mensagem, tornando-a ilegivel, de forma que o destinatário pode restaurar a mensagem a sua forma legível novamente. Mesmo que alguém que consiga interceptar a mensagem durante a transmissão não poderá decifra-la, a menos que possua a chave necessária para tal.

Existem diversas técnicas de criptografia. Em uma delas, dita simétrica ou de chave secreta, o remetente e o destinatário da mensagem compartilham a mesma chave, que é mantida em segredo pelos dois. O remetente utiliza a chave para **criptografar** a mensagem, que é então enviada ao destinatário através de um canal de comunicação não necessariamente seguro, como a *Internet.* O destinatário, ao receber a mensagem, utiliza a chave que possui para decifrá-la.

Matematicamente, a operação de criptografia simétrica pode ser expressa pela fórmula:

$$X = \text{Criptografa}(C,M)$$

Enquanto Tensa Systems e o CommerceNet Consortium buscavam a consolidação do S-HTTP *(Secure* HTTP) frente ao crescente uso do SSL (*Secure Socket Layer*) criado pela Netscape e endossado pela VeriSign, a Microsoft anunciava o PCT (*Private Communication Tecnology*),cuja implementação muito se assemelhava ao SSL. Nesse interin, as duas maiores administradoras de cartão de crédito, Visa e Mastercard desenvolviam em parceria com outras empresas, suas próprias soluções para comércio seguro. Assim, Mastercard se associava à Cibercash, IBM, GTE e Netscape no desenvolvimento do protocolo SEPP *(Secure Electronic Payment Protocol).* Por outro lado a Visa se juntava à Microsoft no desenvolvimento do STT *(Secure Transaction Tecnology).*

2.0 SURGIMENTO DO PADRÃO SET

Em fevereiro de 1996 Visa e Mastercard, após desistirem de empreender esforços paralelamente em busca de um solução segura para o comércio eletrônico, consolidaram uma parceria que viria a resultar no desenvolvimento de um padrão único, simples e seguro para transações eletrônicas. Esse padrão foi denominado SET *(Secure Electronic Transaction).* Aderiram ao SET empresas de peso como a IBM, GTE, RSA, Tensa Systems *e* VeriSign.

Em dezembro de 1997 foi criada a SETCo (SET Consortium), uma entidade com a finalidade de providenciar a infra-estrutura de certificação necessária ao estabelecimento do padrão SET, bem como fomentar e divulgar a especificação.

O padrão SET é basicamente dividido em dois grandes blocos: o sistema de pagamento e o gerenciamento de certificados. O primeiro bloco trata as mensagens com informações relacionados a compra propriamente dita, já o segundo bloco trata mensagens para obtenção, renovação e revogação de certificados.

Em 1998, foi desenvolvido por [2], na UFRGS um conjunto de aplicações denominado SET-F, cuja finalidade é facilitar a utilização dos sistemas de pagamento em comércio eletrônico, baseadas no padrão SET e oferecer as empresas pequenas e de médio porte uma ferramenta a baixo custo. O SET-F é constituído por um grupo de três aplicações desenvolvidas e reunidas de forma cooperativa na forma de um *framework,* que trata especificamente de sistemas de pagamento em transações *on-line* com cartões de crédito, modalidade esta que concentra o maior volume de pagamentos na *Internet.* Em virtude da grande complexibilidade no desenvolvimento de um *framework* que envolvesse todos os participantes no sistema de processamento de transações eletrônicas baseadas no SET, o SET-F limitou-se unicamente ao desenvolvimento das aplicações relativas ao processamento de transações entre o consumidor (proprietário do cartão de crédito) e o comerciante. Por não possuir um sistema para gerenciamento de certificados, foco deste trabalho, deixou para mais tarde a autenticação de consumidores e comerciantes.

3. FUNCIONAMENTO E CARACTERÍSTICAS DO PADRÃO SET

O SET é a especificação de um protocolo destinado a oferecer segurança em transações de pagamento, bem como autenticar todas as partes envolvidas nessa transação, em qualquer tipo de rede. A especificação foi criada com a finalidade de fornecer a confiança necessária para que os consumidores e comerciantes sintam-se seguros em usar seus cartões de pagamento na *Internet.* Com base em estudos da especificação, esta sendo desenvolvida uma ferramenta para a certificação digital, cujo objetivo é oferecer aos seus usuários maior segurança.

systems and the second defines the certificates management. In this paper will give an overview of the SET standard, its working, goals and features, as well as, the certificates management, the subject of thework which has been in developing in this moment.

The large number of cryptographic processes, using algorithms like DES and RSA, the need of an efficiendistributed certificate issuance, renewal and revocation model, and SET-compliant solution development complexity, are the main factors which had inhibited the faster and definitiveSET's acceptance

In this context, in 1998, at UFRGS, was develop a set of applications named SET-F, which the main objective is ensuring the standard comprehension and provide an easy way to use the payment systems. At this way, allowing the development of solutions based in it. Continuing this work, the next step is develop a new set of applications which will allow the certificates management, not within SET-F yeí. This applications, will easy the use of a certificate management system and will provide a high levei of security to the SET-F framework, through authenticating all parties involved in the transaction.

\. INTRODUÇÃO

Nos últimos anos o progresso do comércio eletrônico tem sido lento em relação ao número de usuários da *Internet*, estima-se que isto vem acorrendo devido a falta de mecanismos seguros para efetuar pagamentos via *Internet*, ou seja, a falta de confiança do consumidor na segurança oferecida pelos diversos *sites* que estão realizando transações eletrônicas via *Internet*. Os serviços de computação e indústrias de *software*, em conjunto com setores financeiros e outros, tem trabalhado arduamente para oferecer ao *E-Commerce* uma solução real para os problemas relacionados à segurança.

Enquanto os *firewalls* tem um valioso propósito de fornecer segurança em conexões de redes à *Internet*, eles não fornecem segurança em transações fim-a-fim, e não podem ser considerados soluções adequadas para transações comerciais sob a *Internet*. Outras soluções tais como senhas, que podem ser utilizadas apenas uma vez, resolvem parte do problema e não o problema inteiro. Uma solução segura, considerada robusta, para transações comerciais deve satisfazer as seguintes requisitos fundamentais: confidencialidade, autenticação, integridade dos dados e não repúdio.

Confidencialidade é geralmente oferecida através de criptografia, enquanto autenticação, integridade dos dados e não-repúdio são geralmente oferecidos através de assinaturas digitais e uso de certificados de identidade digital.

Muitos sistemas de pagamento e de criptografia como CyberCash, Electonic Cheque, First Virtual Accounts, PGP [9], S-HTTP [10], S/MIME [11], SSL [12] tem sido propostos com a finalidade de solucionar os problemas de segurança em transações comerciais. Cada sistema apresenta uma série de vantagens e desvantagens, mas nenhum deles consegue atender de forma simultânea todos os requisitos necessários para garantir a segurança do processo como um todo, sendo esta uma das principais razões para o estágio que se encontra o comércio na *Internet*, que apesar de significativo em números absolutos, ainda é pequeno frente ao seu potencial [4].

Sob esse pano de fundo que se desenrolava até 1996 uma das mais acirradas batalhas tecnológicas, na busca de um padrão de comércio seguro para a *Internet*, que assegurasse ao seu desenvolvedor uma boa fatia do filão do comércio no ciberespaço.

REFERÊNCIAS

[1] SECURE ELECTRONIC TRANSACTIONS. SET Specification- Book 1. MasterCard Visa. 23 de fevereiro de 1996.

[2] SECURE ELECTRONIC TRANSACTIONS. SET Specification- Book 2. MasterCard Visa. 23 de fevereiro de 1996.

[3] ROCKENBACH, Alexis. SET-F Um Framework para sistemas de Transações Eletrônicas Seguras Baseadas no Padrão SET. Rio Grande do Sul: Dissertação de Mestrado - CPGCC-UFRGS, 1999, 113p.

[4] GUROVITS, Hélio et al. Planeta E. In: Revista EXAME. Ed. 690, No 12, Junho 1999. Pp. 148-159.

[5] CERTISIGN, Central de Informações. CERTIFICADOS DIGITAIS. Disponível por www em http://www.certisign.com.br/. 11 de março de 1999.

[6] LOEB, Larry. Secure Electronic Transaction: Introduction and Technical Reference. Artech House, Inc., 1998. 341p.

[7] MERKOW, Mark S. BREITHAUPT, Jim; WHEELER, Ken L. Building SET applications for secure transactions. New York: Wiley, 1998. 403p.

[8] OAKS, Scott. Segurança de dados em Java. Rio de Janeiro. Editora Ciência Moderna Ltda, 1999. 431p

[9] PRETTY GOOD PRIVACY. What is PGP? Disponível por WWW em http://www.rsa.com/rsalabs/faq/html/5-2-6.html. 9 de dezembro de 1998.

[10] SECURE HYPER TEXT TRANSFER PROTOCOL. What is Secure HyperText Transfer Protocol? Disponível por WWW em http://www.iks-jena.de/mitarb/lutz/security/cryptfaq/q133.html. 10 de dezembro de 1998.

[11] SECURE MULTIPURPOSE INTERNET MAIL EXTENSIONS. What is S/MIME? Disponível por WWW em http://www.rsa.com/smime/html/faq.html#gnrl.2. 9 de dezembro de 1998.

[12] SECURE SOCKETS LAYER. What is SSL? Disponível por www em http://www.rsa.com/rsalabs/faq/html/5-1-2.html. 11 de dezembro de 1998.

[13] RIVEST, SHAMIR, and ADLEMAN. What is RSA? Disponível por WWW em http://www.rsa.com/rsalabs/faq/html/3-1-1.html. 9 de dezembro de 1998

[14] DATA ENCRYPTION STANDARD. What is DES? Disponível por WWW em http://www.rsa.com/rsalabs/faq/html/3-2-1.html. 9 de dezembro de 1998

[15] GARFINKEL, Simson; SPAFFORD, Gene. Web security & commerce. Cambridge: O'Reilly, 1997. 483p.