Análise dos Sistemas Comerciais Emergentes na Internet

Grupo de Sistemas e Serviços Telemáticos
INESC - Instituto de Engenharia de Sistemas e Computadores
Rua Alves Redol, Nº 9
Apartado 13069
1000 Lisboa - Portugal
Telefone Geral: + 351-1-3100 000
Fax: + 351-1-52 58 43

José Filipe Costa
Universidade de Évora
Email: jcosta@Uevora.pt
Telefone: +351-66-25572 (Ext. 253)

Alberto SIlva
Email: Alberto.Silva@inesc.pt
Telefone Directo: +351-1-3100307

José Delgado
Email: José.Delgado@inesc.pt
Telefone Directo: +351-1-3100211

Palavras Chave:

Sistemas Comerciais, Segurança, Dinheiro Electrónico, Internet, WWW.

Resumo:

Este documento faz uma análise da tecnologia existente e emergente que permite suportar a existência de sistemas comerciais sobre a Internet, que de algum modo verifiquem um conjunto de requisitos por vezes incompatíveis entre si: segurança (privacidade, autenticidade, integridade e não repudiação), robustez, anonimato, extensibilidade, flexibilidade, eficiência, facilidade de utilização e facilidade de integração com as aplicações finais e com outros sistemas comerciais.

A tecnologia necessária para suporte de sistemas comerciais baseia-se em geral sobre três pilares: mecanismos e algoritmos de criptografia; protocolos de transferência de informação; e sistemas de bases de dados para manutenção e gestão de informação de controlo.

O documento descreve com detalhe sistemas e projectos de sistemas comerciais, os quais se dividem genéricamente em três categorias ou modelos diferenciados: baseados em Dinheiro Electrónico; em Contas de Crédito/Débito; ou na Apresentação de Cartão de Crédito.

Por fim é realizado uma análise crítica e comparativa dos diferentes modelos e projectos de sistemas comerciais.

1. Introdução

Com a actual explosão de utilizadores e de fornecedores de informação na Internet, assiste-se a mudanças profundas nos seus objectivos e propósitos iniciais. Apesar das conhecidas críticas de falta de segurança na Internet começa-se a assistir à sua utilização com fins comerciais, designadamente a transações de bens ditos electrónicos (*software*, revistas, informação especializada resultante de acessos a determinadas bases de dados, etc) e como substituição de venda de artigos por catálogo.

Genericamente o problema das transacções comerciais envolve as seguintes entidades: o cliente (ou comprador), o fornecedor (ou vendedor), o banco virtual (sistema computacional com suporte de segurança, etc), o banco real (de modo a poderem ser realizadas as operações de compensação entre moeda virtual/electrónica e moeda real), e por fim o intruso (ou bandido), que de algum modo pode potenciar fraudes. O presente documento concentra-se apenas nas interacções entre o cliente, o fornecedor e o banco virtual.

O documento apresenta com detalhe a problemática da implementação de sistemas comerciais numa rede aberta de grande utilização que é a Internet. É dado ênfase aos mecanismos e protocolos de segurança e também aos protocolos transaccionais realizados entre os diferentes intervenientes.

São descritos sistemas e projectos de sistemas comerciais, os quais se dividem genéricamente em três categorias ou modelos diferenciados: baseados em Dinheiro Electrónico; em Contas de Crédito/Débito; ou na Apresentação de Cartão de Crédito.

Por fim o documento apresenta uma análise crítica e comparativa dos diferentes modelos e projectos de sistemas comerciais.

2. Tecnologia

2.1 Segurança

A segurança, é um requisito fundamental exigido pelos protocolos de pagamento. Divide-se em várias componentes, ou características:

- **Privacidade**. A privacidade consiste na realização de transacções sem que terceiros acedam à informação trocada entre os intervenientes.
- **Autenticação.** Garante que a mensagem foi criada por quem diz ter sido, eliminando a possibilidade de alguém forjar mensagens em nome de terceiros. É a garantia de que não existe fraude no que respeita à verdadeira entidade dos intervenientes.
- **Integridade.** É a garantia de que os dados em circulação não podem ser alterados sem que essa alteração seja detectada.
- **Não repudiação.** É a impossibilidade de o emissor de uma mensagem invocar a ocorrência de qualquer tipo de fraude para negar que foi o seu emissor. É a prova de origem e de recepção de uma mensagem. A autenticidade é a prova de criação da mensagem. A não repudiação é a prova de transmissão da mensagem.

2.2 Criptografia

A ciência e arte de criptar (ou codificar) baseia-se em métodos e algoritmos de transformação de informação de modo que esta possa ser trocada ou transmitida de modo seguro entre diferentes intervenientes sem que possa ser reconhecida por partes terceiras. Existem duas operações associadas: a operação de criptação, que consiste em transformar a informação para um formato ilegivel; e a operação inversa, denominada decriptação.

2.2.1 Algoritmos

Os algoritmos que interessam para os mecanismos de pagamento são os reversíveis e dividem-se em dois tipos: simétricos e assimétricos. Todos eles utilizam uma chave para criptar e decriptar a informação. Conforme o algoritmo utilize a mesma chave para as duas funções ou não, ele diz-se simétrico ou assimétrico.

Ambos os tipos de algoritmos apresentam vantagens e desvantagens e são normalmente usados em conjunto de modo complementar.

2.2.1.1 Algoritmos Simétricos ou de Chave Secreta

Os algoritmos de chave secreta utilizam uma chave para cada par de utilizadores. Cada um tem que ter armazenado no seu sistema a sua, e todas as chaves de utilizadores com quem tem necessidade de comunicar com segurança. A vantagem destes algoritmos é a sua rapidez. A desvantagem destes algoritmos é o problema da troca inical da chave secreta.

O algoritmo mais conhecido e usual deste tipo, utilizado nos mecanismos de pagamento é o **DES** (*Data Encryption Standard*). Existem variantes do DES. A mais simples, ECB (*Electronic CodeBook*) cripta cada bloco de 64 *bits* um após o outro com a mesma chave. Outras variantes são o triplo DES, o CBC (*Ciber Block Chaining*), e o EDE (*Encrypt-Decrypt-Encrypt*).

Outros algoritmos existentes são o **IDEA** (*Internacional Data Encryption Algorithm*), RC2, RC4 e Skipjack.

2.2.1.2 Algoritmos Assimétricos ou de Chave Pública

Os algoritmos de chave pública utilizam duas chaves, uma pública e outra privada. Estes algoritmos tem a vantagem de que com um único par de chaves, qualquer utilizador pode trocar mensagens seguras. Nestes algoritmos a chave pública é colocado num servidor público e seguro, a Autoridade de Certificação (AC). Na transmissão de informação, o emissor cripta previamente a informação com a sua chave pública do receptor (consultando eventualmente a AC para obter essa informação). Na recepção o receptor decripta a informação recebida com a sua chave privada.

As vantagens destes algoritmos são: o suporte para utilização de assinaturas digitais e a utilização das chaves em segurança, sem necessidade de serem trocadas. A principal desvantagem é o considerável tempo de processamento para criptar/decriptar.

Uma **assinatura digital** é um conjunto, não forjável, de dados digitais que atestam que uma determinada pessoa escreveu ou concorda com um documento ao qual a assinatura está ligada. Para fazer uma assinatura digital o emissor gera um **código de integridade de mensagem** (CIM) da mensagem a transmitir e de seguida cripta-o com a sua chave privada. O receptor após receber uma mensagem com assinatura digital pode verificar a assinatura.

Os algoritmos de geração de CIMs são utilizados para gerar pequenas sequências de caracteres representativas de documentos de tamanho variável. As funções *MD2 (Message*

Digest 2), MD4, MD5 e SHS (*Secure Hash Standard*"), são exemplos de funções de *hash* seguras.

O algoritmo do tipo de chave pública mais conhecido é o **RSA** (Rivest, Shamir, Adleman). As chaves deste algoritmo consistem em dois pares de valores inteiros (*e*,*n*) e (*d*,*n*), respectivamente chave pública e privada. A segurança deste sistema de criptografia deriva de ser dificil obter o valor *d* a partir da chave pública (*e*,*n*). Para isso é necessário factorizar *n* em dois números primos.

Outros algoritmos existentes são o **Elgamar**, menos eficente; o **Diffie-Helleman**, que é um sistema unicamente para troca de chaves; e o **DSS** (*Digital Signature Standard*) unicamente para assinaturas digitais.

2.2.2 Aplicações

A criptografia é utilizada para proporcionar segurança na transmissão de mensagens nas quatro componentes expostas em 2.1, **Privacidade** do conteúdo da mensagem, **Autenticidade** do emissor da mensagem, **Integridade** do conteúdo da mensagem e **Não Repudiação** (origem) da mensagem. É possível obter-se qualquer uma das três primeiras componentes ou combinação destas com os dois tipos de algoritmos. Por exemplo se um utilizador só pretende garantir a autenticação ou integridade da mensagem, deve-se utilizar apenas o mecanismo de assinaturas digitais o que torna o sistema computacionalmente mais rápido. A não repudiação só pode ser obtida com criptografia assimétrica.

2.2.3 Sistemas

- **O Kerberos** é um sistema de autenticação que permite a um programa cliente, executado por um utilizador, provar a sua identidade perante um verificador (servidor). O sistema Kerberos garante ao verificador que o cliente detém uma chave de criptação que só é conhecida pelo utilizador e pelo servidor de autenticação. O sistema Kerberos usa criptografia simétrica e combina-a com a utilização de CIM*s* para garantir integridade e privacidade para as suas mensagens.
- **O PEM** (*Privacy Enhanced Mail*) é uma norma, para facultar correio electrónico seguro na Internet. Trabalha com os formatos de email existentes na Internet e inclui facilidades de privacidade, autenticação, integridade e não repudiação utilizando algoritmos criptográficos de chave pública e chave secreta. O PEM consiste basicamente num filtro que funciona entre um editor e um sistema de correio electrónico.
- **O PGP** (*Pretty Good Privacy*) é também um sistema para proporcionar facilidades de segurança para o email. O PGP proporciona, similarmente ao PEM, opção de criptar o texto da mensagem. O PGP utiliza também os dois tipos de criptografia combinados.
- **O SSL** (*Secure Sockets Layer*) é um protocolo que oferece facilidades de segurança na Internet, criando um canal seguro configurável. O protocolo garante privacidade, autenticação e integridade às comunicações entre aplicações cliente e servidor. A sua vantagem principal é ser independente do protocolo de transferência de informação.

2.3 Transferência de Informação

Os protocolos de transferência de informação, quer de controlo quer da informação própriamente comercializada, são os disponíveis na Internet. Basicamente FTP, E-Mail e HTTP, ou quaisquer outros derivados ou de algum modo especializados. Alguns dos

protocolos de transferência de informação já incluiem também extensões para segurança como é o caso do S-HTTP.

2.4 Controlo e gestão da informação critica envolvida nas transacções

Por fim, o terceiro grupo tecnológico consiste no controlo e na manutenção da informação inerente das operações comerciais. Algumas das operações tipicas são a criação/remoção de contas de clientes, registo (inventariação) das transacções realizadas, ou transferências de dinheiro e consolidação financeira entre diferentes parceiros e instituições financeiras. Em geral recorre a sistemas de bases de dados centralizadas ou distribuidas e implica sistemas transaccionais de modo a controlar todas as operações envolvidas.

Este documento não focará os problemas inerentes ao controlo e gestão da informação dos sistemas comerciais, nem a questões de suporte, do tipo escolha de sistemas de bases de dados e análise dos requisitos transaccionais.

3. Requisitos

Existem, segundo vários autores, diferentes requisitos considerados importantes para a concretização de um sistema de pagamento na Internet. Algums destes requisitos, como por exemplo o anonimato, são mais importantes em determinadas comunidades, ou para certos tipos de transacções, do que o são para outras. Estes requisitos são uma forma de comparação dos vários sistemas e serão utilizados (aqueles considerados dependentes do mecanismo de pagamento) no capítulo 6, como critério de comparação entre os vários sistemas.

3.1 Requisitos Dependentes do Mecanismo de Pagamento

Segurança. Uma vez que os pagamentos envolvem dinheiro (ou formas de dinheiro) e bens reais, os sistemas de pagamento são concerteza potenciais alvos de crimes. Por outro lado, como a Internet é uma rede aberta, as escutas e modificações de mensagens são fáceis de realizar pelo que a infraestrutura de suporte ao comércio electrónico deve ser segura e resistente aos ataques. A segurança pode ser dividida em três sub-requisitos:

- Segurança contra crimes perpetuados por terceiros;
- Segurança contra crimes perpetuados pelos intervenientes; e
- Privacidade, autenticação, integridade e não repudiação.

Anonimato. Para algumas transacções, a identidade dos intervenientes deve ser protegida. Não deve ser possível portanto controlar o tipo de despesas de um consumidor, nem determinar a fonte de receitas de um comerciante.

Escalabilidade. Com o crescimento do comércio na Internet, aumentará também o acesso aos servidores de pagamentos. A infraestrutura de pagamentos deverá suportar múltiplos servidores espalhados pela Internet para permitir o aumento de consumidores e comerciantes sem que se verifiquem perdas importantes de *performance*.

Eficiência. As taxas de acesso à informação poderão frequentemente gerar pagamentos de pequenas quantidades, os micropagamentos. As aplicações deverão suportar os micropagamentos sem acusarem degradação de *performance*. Os custos, da utilização da

infraestrutura, por transacção devem ser suficientemente reduzidos quando comparados com os valores dos bens a transaccionar.

Aceitabilidade. Um instrumento de pagamento deve ser abrangente em termos de aceitação. Quando o mecanismo de pagamento for suportado por múltiplos servidores, os utilizadores dos vários servidores devem poder interactuar transparentemente.

Base de Consumidores. O sucesso de um mecanismo de pagamento é afectado pelo número de consumidores que o podem usar. Os comerciantes querem vender produtos, e sem uma base de consumidores suficientemente grande a utilizar um mecanismo de pagamento, poderá não valer a pena ao comerciante aceitar o mecanismo.

Flexibilidade São necessárias formas de pagamento alternativas, dependendo das garantias exigidas pelas partes envolvidas numa transacção, a altura do pagamento, requisitos para verificações de contas, requisitos de performances, e o valor do pagamento.

Interoperacionalidade. Os utilizadores da Internet escolherão os instrumentos financeiros que melhor se adaptarem às suas necessidades para uma dada transacção. Será importante que os valores representados por um mecanismo sejam facilmente convertidos em valores representados por outros sistemas.

Atomicidade. Toda a transacção deverá ser atómica, ou seja, a qualquer momento da execução do protocolo de pagamento ou ela se realizou ou não, e se se realizou então o comerciante tem o dinheiro em seu poder e o comprador o bem (caso este seja electrónico).

3.1.1 Requisitos Só Para Sistemas de Dinheiro Electrónico

Operação *off-line*. Quando um comprador adquir algo com dinheiro electrónico, o protocolo de pagamento deve poder ser executado *off-line*, ou seja, o comerciante não deverá ter necessidade de estar ligado ao servidor de dinheiro.

Transferabilidade. O dinheiro electrónico deverá poder ser transferido entre utilizadores sem a intervenção de qualquer entidade central.

Independência física. Uma moeda electrónica não deverá depender de qualquer componente físico do sistema. Nem do servidor de dinheiro, nem do computador do utilizador nem de qualquer tipo de porta moedas electrónico.

Divisibilidade. Uma moeda de dinheiro electrónico, deverá poder ser dividida em outras de menor valor, até valores considerados razoáveis.

3.2 Requisitos Não dependentes do Mecanismo de Pagamento

Características como a robustez, a facilidade de integração nas aplicações e a facilidade de uso, embora não constituam o mecanismo de pagamento em si são também importantes para o desenvolvimento e divulgação destes mecanismos.

4. Mecanismos de Pagamento

Os mecanismos de pagamento na Internet podem ser agrupados, segundo o modo de pagamento, em três classes genéricas: sistemas de **dinheiro electrónico**, sistemas de **crédito/débito** e sistemas que suportam a apresentação segura de números de **cartões de crédito**.

Segundo o modo de pagamento podem-se estabelecer três modelos de protocolos. Todos eles pretendem evitar em geral os seguintes problemas:

- O cliente receber o bem e interromper a comunicação sem pagar;
- O vendedor receber o dinheiro e não fornecer o bem;
- A utilização em duplicado da ordem de compra ou do dinheiro; e
- Alteração do valor da transacção por um dos intervenientes sem o conhecimento do segundo.

Para simplificar a descrição, e visto que é uma fase óbvia e requerida para os três modelos, não é descrita a fase de troca de informação para escolha do produto e do comerciante que o vende. Cada modelo é descrito a partir do momento em que o cliente seleccione conceptualmente a opção "comprar".

Todos os meios de pagamento têm uma ligação a um banco para movimentação de dinhero real. A descrição dessas ligações e seus protocolos sai fora do interesse deste documento.

4.1 Dinheiro Electrónico

4.1.1 Meio de pagamento

Nestes sistemas, os utilizadores clientes adquirem dinheiro electrónico nos servidores de dinheiro, que garantem a usabilidade desse dinheiro. Os clientes pagam o dinheiro electrónico através de uma conta previamente estabelecida nesse servidor ou através de cartões de crédito, cheques electrónicos, ou ainda com dinheiro real, via uma instituição financeira, por meio de um sistema electrónico ou não.

O dinheiro electrónico consiste em sequências especiais de *bits*, geralmente números grandes. A criação e representação do dinheiro electrónico difere de sistema para sistema, como se constata pela análise dos exemplos descritos em 5.1.

Uma vez emitido, o dinheiro electrónico representa um valor, e pode ser gasto no comércio ligado ao mesmo sistema. Os comerciantes depositam o dinheiro electrónico num servidor para o transformarem em real, ou gastam-no, por sua vez, no sistema.

4.1.2 Modelo do Protocolo de Pagamento

O modelo de protocolo de pagamento para utilização de dinheiro electrónico consiste em três fases concretas (conforme ilustrado na Figura 1) e utiliza criptografia de chave pública conjugada com criptografia simétrica.

O modelo assume que o cliente pode determinar a chave pública do vendedor e que este pode determinar a chave pública do banco virtual.

Podemos considerar 3 fases na aplicação do modelo:

1. O cliente requer ao vendedor um determinado bem, enviando-lhe para isso dinheiro electrónico que possui, no seu computador. A mensagem contém o dinheiro

electrónico, o descritor do bem pretendido e uma chave simétrica do cliente. A mensagem vai criptada com a chave pública do vendedor.

2. O vendedor envia o dinheiro ao servidor, que, após certificar-se da autenticidade do mesmo, autoriza a operação. A mensagem que o vendedor envia ao banco virtual contém o dinheiro electrónico e uma chave secreta do vendedor, e vai criptada com a chave pública do banco virtual. Após verificar a autenticidade do dinheiro, isto é, que não se trata de dinheiro duplicado ou não emitido pelo banco virtual, este retorna ao vendedor novo dinheiro, resultante da transacção, selado com a chave secreta que tinha recebido.
3. O vendedor transfere o bem para o cliente. O vendedor envia ao cliente um recibo criptado com a chave simétrica que lhe tinha sido transmitida na 1ª fase. O recibo inclue a descrição do valor pago, a data e um identificador que será utilizado para obter o bem pretendido.

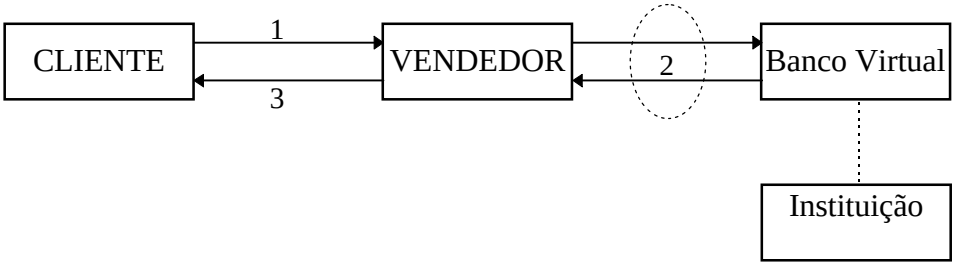


Figura 1. Modelo de pagamento com dinheiro electrónico

Este modelo tem como vantagens o potencial para o anonimato, para utilização *off-line* e para segurança contra fraude por parte dos dois intervenientes na transacção.

Os sistemas DigiCash e NetCash são dois exemplos de utilização de dinheiro electrónico na Internet. O sistema *DigiCash* criou uma extensão às técnicas de criptografia para obter anonimato incondicional. Um cliente mantém o anonimato mesmo que exista cruzamento da informação de cada uma das partes intervenientes na transacção. Se o cliente tentar gastar duas vezes o mesmo dinheiro, então perde o anonimato e consequentemente é identificado. No NetCash se houver cruzamento de informação, o anonimato é perdido. O sistema *NetCash* propõe uma variante ao protocolo para proteger ambas as partes de fraude.

Por fim, o maior problema deste modelo é a não transferabilidade do dinheiro electrónico devido à facilidade de duplicação do dinheiro. Para evitar o uso duplicado o banco virtual mantém uma base de dados com o dinheiro gasto ou por gastar.

4.2 Contas de Débito/Crédito

4.2.1 Meio de Pagamento

Nestes sistemas os consumidores registam-se em servidores de pagamentos ficando com uma conta corrente que é suportada por ligação a uma conta bancária ou um cartão de crédito. Quando procede ao registo o consumidor acorda com o sistema de pagamento a

forma de compensação da conta e a altura em que a compensação é feita. Nas contas de débito o consumidor mantém um saldo financeiro positivo. Nas contas de crédito o consumidor não precisa de ter saldo, tendo sim crédito para gastar até um determinado montante, sendo posteriormente cobrado. A conta é debitada, quando o consumidor adquire algo, por meio de cheques electrónicos ou autorizações de débito.

4.2.2 Modelo do Protocolo de Pagamento

O modelo de protocolo de pagamento para utilização de contas de crédito/débito difere do anterior principalmente em dois aspectos: por ser o cliente a comunicar com o servidor e por existir mais um par de mensagens trocadas entre o cliente e o servidor ou o vendedor. A Figura 2 ilustra este modelo. Este modelo é composto por 4 fases:

1. O cliente envia a informação sobre a sua conta, o bem que pretende adquirir e sobre o vendedor. A mensagem inclui uma assinatura digital do cliente, para o autenticar. Toda a mensagem é criptada com a chave pública do servidor.
2. O servidor, após registar a transacção, envia ao cliente dois certificados, um dos quais criptado com a chave pública do vendedor. A mensagem inclui ainda uma assinatura digital para verificar o conteúdo da mensagem.
3. O vendedor recebe o certificado com a indicação de que a transferência foi efectuada, autorizando a entrega do bem. Conjuntamente com o certificado, o cliente envia uma chave simétrica e uma assinatura digital para o autenticar. A mensagem vai criptada com a chave pública do vendedor.
4. O vendor transmite o bem, ou uma cópia das instruções de entrega, ao cliente. A mensagem vai criptada com a chave simétrica que o cliente lhe enviou.

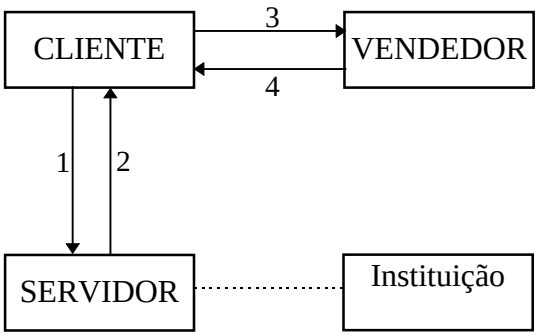


Figura 2. Modelo de pagamento para contas de débito/crédito

As vantagens deste modelo são o risco reduzido devido à auditabilidade e atomicidade das transacções, e a flexibilidade (micropagamentos). As desvantagens deste modelo situam-se ao nível financeiro: na versão conta de débito o consumidor é obrigado a confiar no sistema transferindo previamente dinheiro para a conta, na versão conta de débito o consumidor tem que esperar pela transferência bancária antes de utilizar o sistema e na versão conta de crédito o consumidor paga taxas mais elevadas por transacção. Outra característica deste modelo é que não suporta facilmente o anonimato.

As características deste meio de pagamento, possibilidade do controlo efectivo do que é adquirido, fazem com que este sistema seja o que mais agrada às empresas e instituições em geral, tornando-o num sistema rentável.

Alguns sistemas que utilizam este meio de pagamento são o NetBill, o NetCheque, o OpenMarket e o First Virtual.

4.3 Apresentação Segura de Cartão de Crédito

4.3.1 Meio de Pagamento

O terceiro meio de pagamento é a utilização directa e segura de um cartão de crédito. De cada vez que um consumidor pretende adquirir algo, ele transmite os dados do cartão de crédito ao servidor, criptados.

4.3.2 Modelo do protocolo

A diferença mais relevante deste modelo em relação aos anteriores consiste no facto de que para todas as transacções existe uma ligação efectiva à instituição financeira. O modelo encontra-se ilustrado na Figura 3, consistindo nas seguintes fases:

1. O cliente envia os dados do cartão de crédito, a identificação do vendedor, a identificação do produto que pretende e o valor da transacção criptados com a chave pública do servidor. Envia também uma chave simétrica para ser utilizada no fase 4. A mensagem é assinada e contém uma marca de tempo.
2. O servidor procede à transacção junto da instituição financeira.
3. O servidor transmite ao vendedor a identificação do cliente e do produto que este pretende, o valor e número da transacção e a chave simétrica que recebeu na fase 1. Esta informação é toda criptada com uma chave simétrica que ambos partilham.
4. O vendedor cripta a informação do cliente com a chave simétrica que este lhe enviou e transmite-a.

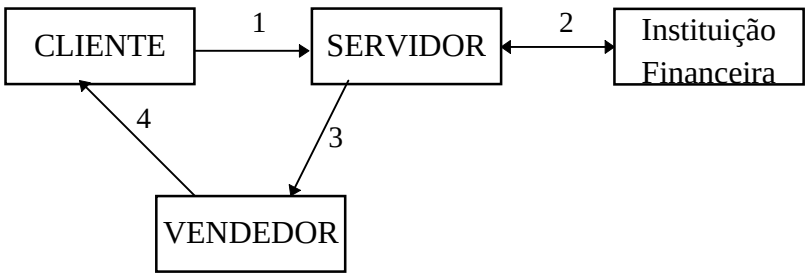


Figura 3. Modelo de pagamento para apresentação cartão crédito

Este modelo protege o cliente de utilização abusiva do cartão de crédito por parte do vendedor, mas não o protege da não entrega do bem. Este facto não pode ser impedido e não se consegue provar neste modelo que o bem não foi enviado. Neste modelo a confiança no vendedor é essencial.

A principal vantagem deste modelo é o consumidor não necessitar de proceder a qualquer registo antes ou depois de adquirir um bem. A principal desvantagem são os custos inerentes ao facto de se tratar de uma transacção de cartão crédito.

5. Sistemas

5.1 Sistemas de Dinheiro Electrónico

5.1.1 Digicash

Neste sistema quer os consumidores quer os comerciantes têm que ter uma conta, registando-se, no banco *First Digital Bank* criado para permitir a conversão de dinheiro real para *ecash* e aceder ao software *ecash*.

A Digicash criou dois tipos de sistemas, um baseado em hardware e outro em software. Nos sistemas baseados em hardware, não discutidos neste trabalho, existe um componente físico especifico para a função no sistema, que controla o dinheiro electrónico.

David Chaum, que desenvolveu o sistema da Digicash, apresenta duas soluções por software para o comércio com dinheiro electrónico, ambas com anonimato, uma em modo *on-line* e outra em *off-line*. No primeiro modo o sistema permite detectar a tentativa de gastar o dinheiro electrónico em duplicado e no segundo o sistema revela a identidade do utilizador quando este gasta o dinheiro em duplicado. D. Chaum utiliza três personagens, que são normalmente utilizadas na ilustração de mecanismos deste género, para explicar as suas propostas, a Alice, o Bob e o Charles, que utilizar-se-á também neste e noutros mecanismos. Os dois modos funcionam da seguinte forma:

⇒ Modo *On-Line*

Este sistema utiliza uma extensão ao mecanismo de assinatura digital a que chama "assinatura às cegas", que garante anonimato incondicional.

O mecanismo de assinatura às cegas tira partido do facto da técnica de criptamento RSA ser associativa, ou seja, o resultado de dois criptamentos RSA é o mesmo seja qual for a ordem em que os criptamentos são realizados.

- **Aquisição da moeda**

Quando a Alice pretende adquirir dinheiro electrónico ela gera um número aleatório x, de pelo menos 100 bits, e calcula sobre este um código de integridade de mensagem (CIM), f(x) utilizando o algoritmo MD4 ou MD5 descritos em 2.2.1.2. Antes de enviar o resultado f(x) para o banco assinar, a Alice multiplica-o por um factor aleatório N, assinando o resultado com a sua chave privada. A Alice indica também o valor da nota que pretende e a sua identificação.

O banco verifica e remove a assinatura do número, debita a conta da Alice e assina o valor f(x)*N com a sua chave privada para o valor pretendido. O banco pode emitir moedas de vários valores, utilizando para esse efeito assinaturas diferentes. Assim com uma assinatura ele cria moedas de 1 dolar, com outra assinatura moedas de 2 dolares, com outra, de 5 dolares, etc. Da moeda enviada pelo banco à Alice também faz parte uma data de validade para esta.

A Alice divide o número assinado pelo banco e obtém o CIM f(x), mas assinado pelo banco. O par $(x, [f(x), \text{validade}]_{\text{ass. banco}})$ formam a moeda que a Alice usará para adquirir bens na loja do Bob.

O banco pode debitar a conta do consumidor por que sabe quem é que lhe apresenta a moeda para ele assinar, mas quando aparece essa moeda como pagamento ele não a consegue associar com nenhum cliente, pois após remover a sua assinatura, que lhe garante que a nota é autentica, obtem um número não conhecido por si.

O número que o consumidor apresenta ao banco tem, pelo menos, 100 digitos, para que as probabilidades de outro consumidor apresentar o mesmo número no mesmo periodo de vida sejam completamente despreziveis.

Para autenticar o número que o cliente envia, ele é assinado com a chave privada do consumidor, previamente estabelecida para utilização com a sua conta.

- **Protocolo Pagamento**

O protocolo de pagamento corresponde ao ilustrado em 4.1.2. A Alice envia ao vendedor, Bob, a moeda electrónica. Antes de entregar o bem, o Bob verifica a assinatura do banco e envia a moeda ao banco para que este verifique se ela já foi utilizada. O banco mantém uma base de dados das moedas gastas para confrontar com os novos pedidos de verificação. Assim, após verificar a sua assinatura e que a moeda ainda não foi gasta, o banco acrescenta a moeda à base de dados, credita a conta do Bob e informa-o sobre a validade da moeda. Após o banco responder o Bob actua em concordância.

Este mecanismo detecta a tentativa de utilização duplicada de uma moeda. Como todas as moedas, têm um prazo de validade, findo o qual nem os vendedores nem o banco as aceitarão, ao fim desse prazo elas podem ser removidas da base de dados, o que impede que esta cresça indefinidamente.

⇒ **Modo *Off-Line***

Este modo tem duas variantes, ambas com o mesmo resultado. Descreve-se uma e explica-se as diferenças para a segunda.

- **Aquisição da moeda**

Uma moeda é o produto de k/2 números, sendo cada número da forma $f(x_i,y_i)$. x_i e y_i são dois números calculados para cada i de 0 a k/2 da seguinte forma: $x_i = g(a_i,c_i)$ e $y_i = g(a_i$ xor <info>$,d_i)$, sendo f e g funções de dois argumentos aplicando um algoritmo como o MD4 ou o MD5. a_i, c_i e d_i são números aleatórios, também gerados para cada i de 0 a k/2, e <info> uma chave que identifica a conta da Alice.

Repare-se que (a_i xor <info>) não revela quem a Alice é, mas que, para o mesmo i, (a_i xor (a_i xor <info>)) revela.

O protocolo funciona assim:

A Alice começa por enviar ao banco k números, da forma $f(x_i,y_i)$, ocultos, pelo mecanismo de assinatura às cegas, com um factor aleatório r_i. O banco escolhe, aleatoriamente, k/2 dos números e pede à Alice que revele para eles o factor aleatório r_i, os números aleatórios a_i, c_i e d_i, e o resultado (a_i xor <info>). Com esta informação o banco verifica que a Alice gerou correctamente os números $f(x_i,y_i)$ e que a chave <info> é correcta.

Os restante k/2 números mantidos ocultos formarão a moeda. Nesta fase existe uma penalização desincentivadora aplicada pelo banco à Alice em caso de tentativa de fraudes por esta. Quando maior for o número k, maiores serão as probabilidades de uma tentativa de fraude ser descoberta. Por outro lado para ter probabilidades, ainda assim remotas, de fazer um pagamento com dinheiro duplicado com sucesso é necessário que o campo <info> esteja falsificado em pelo menos 50% dos números que constituem a moeda.

Nesta fase a variante consiste em o valor da moeda não ser definido pela assinatura que o banco utiliza, mas sim por um campo que indica o valor da moeda. Também na variante, a

Alice envia 100 moedas ao banco para este lhe devolver uma; as restantes 99 servem para o banco verificar se elas foram geradas corretamente. Para isso a Alice gera por cada moeda 100 pares do tipo (a_i, (a_i xor <info>)) e dá-os a conhecer ao banco para as 99 moedas que ele solicitar. Estas 99 moedas não chegam a ser usadas como dinheiro, pois servem exclusivamente para o banco desinibir qualquer tentativa de fraude.

- **Protocolo Pagamento**

Sendo em *off-line*, o protocolo vê eliminada a ligação ao banco digital para autorizar a transacção. Em vez disso existe mais uma troca de informação entre o cliente, a Alice, e o vendedor, o Bob.

A primeira fase é idêntica à do modo "on-line": a Alice envia ao Bob o dinheiro bem como indicação do que pretende aquirir, tudo protegido, como indicado pelo modelo. O Bob começa por verificar a assinatura do banco e de seguida pede à Alice que lhe indique, para cada i de 0 a k/2, conforme ele gere aleatoriamente um 1 ou um 0, os números a_i, c_i e y_i, ou os números (a_i xor <info>), d_i e x_i, respectivamente.

A Alice envia-lhe os números e o Bob verifica então se a moeda foi gerada com estes números. Depois envia-lhe os bens que este adquirio.

Periodicamente, por exemplo semanalmente ou diariamente, o Bob deposita todas as moedas que recebeu no banco. Conjuntamente com as moedas envia todos os números a_i, c_i, y_i, (a_i xor <info>), d_i e x_i que a Alice lhe transmitiu.

Em relação à variante a diferença é que o Bob gera 100 números aleatórios, e por cada um a Alice envia-lhe um ou outro dos elementos que formam o par conforme o número gerado seja 0 ou 1.

Com este protocolo, os três intervenientes estão protegidos contra qualquer tentativa desonesta por parte dos outros dois, quer separadamente, quer em concluio. A Alice mantém o anonimato incondicional, o banco não é burlado nem pela alice nem pelo Bob e este não é burlado pela Alice.

Como para cada i a Alice só revela o a_i ou o (a_i xor <info>), mesmo que o banco e o Bob cruzem a informação de que dispõem não conseguem descobrir a identidade da Alice.

Se a Alice copiar a moeda e a utilizar em dois pagamentos distintos, quer sejam ambos na loja de Bob quer seja um com o Bob e outro na loja do Charles, vai revelar com toda a certeza para vários iis o a_i e o (a_i xor <info>), o que vai permitir conhecer a sua identidade. A probabilidade de serem geradas pelos comerciantes duas sequências idênticas de uns e zeros é de 1 em 2^k, ou para a variante, de 1 em 2^{100}.

Esta probabilidade vai desinibir o Bob de tentar depositar mais do que uma vez a mesma moeda, pois ao receber duas moedas com sequências idênticas o banco vai concluir que o Bob está a cometer fraude.

5.1.2 NetCash

O NetCash, proposto por Gennady Medvinsky e B. Clifford Neuman, tem vários estágios de segurança contra fraudes. Um primeiro que não contém qualquer espécie de segurança deste tipo, e que por isso não vamos analisar, um segundo que corresponde de um modo geral ao modelo apresentado e um último estágio que oferece segurança contra a duplicação de dinheiro e contra a fraude por parte do vendedor. Será este último estágio que será aqui mais detalhado.

- **Representação da moeda**

A infraestrutura NetCash é constituida por Servidores de Dinheiro (SD), geridos independentemente. Existe uma autoridade central, denominada *Federal Insurance*

Corporation, FIC, que emite certificados de segurança para que os SDs possam emitir moedas. Assim uma moeda consiste na seguinte informação, toda criptada com a chave privada do SD: o nome do SD, o endereço na Internet do SD, uma data de expiração da moeda, um número de série e o valor da moeda.

A moeda é acompanhada por um certificado emitido pela FIC que autentica o SD. Esse certificado, criptado com a chave privada da FIC, contém a seguinte informação: um identificador único do SD, o nome do SD, a chave pública do SD e uma data de expiração do certificado.

Esta estrutura possibilita que uma moeda emitida por um qualquer SD seja aceite em todos os outros SD.

- **Aquisição da moeda**

Este sistema não prevê a aquisição de dinheiro electrónico directamente com os meios existentes na sociedade. Para adquirir moedas neste sistema o utilizador tem que estar registado num sistema que lhe permita aceder a formas de dinheiro como cheques electrónicos, duma forma não anónima. Para isto, o NetCash prevê a ligação ao sistema NetCheque, dos mesmos autores, e a outros sistemas. A Alice ou o Bob trocam cheques por dinheiro electrónico NetCash, ou vice-versa, que detenham da seguinte forma:

1. Enviando ao SD uma mensagem criptada com a chave pública deste que contém o instrumento de pagamento a utilizar (moeda NetCash ou cheque), uma chave simétrica gerada por si e a indicação do tipo de transacção que pretende.
2. O SD devolve-lhe criptado com a chave simétrica que recebeu o instrumento de pagamento solicitado.

- **Protocolo Pagamento**

No modelo do protocolo de pagamento com dinheiro electrónico, o comprador fica exposto a fraude por parte do vendedor, pois este após receber o dinheiro pode não entregar o bem. O sistema NetCash tem um estágio do seu protocolo semelhante ao do modelo. Cada SD mantém uma base de dados com os números de série das moedas que emitiu. Quando uma moeda é gasta, ela é eliminada da base de dados. Se surgir uma moeda com um número de série não existente, então trata-se de fraude, ou seja, de uma moeda duplicada. Quando o SD_A recebe, para efectuar um pagamento, uma moeda emitida por SD_B, ele estabelece uma ligação com SD_B para se certificar de que a moeda é valida.

O NetCash estende o modelo apresentado em 4.1.2, com o objectivo de proteger o consumidor contra fraude por parte do vendedor. Para isso é alargada a definição de moeda e melhorado, com mais 2 passos, o modelo de protocolo proposto para troca de dados entre o cliente e o banco virtual.

Uma moeda passa a poder ser adaptada para uma transacção específica, isto é, ser preparada para só poder ser utilizada pela Alice durante um determinado intervalo de tempo, na loja de Bob. Para isso a Alice obtem do SD, em troca de uma moeda ou cheque, um triplo de moedas, $<M_B, M_A, M_X>$, todas com o mesmo número de série e valor. Cada uma destas moedas só pode ser gasta num determinado intervalo de tempo, exclusivamente. No 1º intervalo de tempo somente a moeda M_B pode ser gasta no SD, no 2º somente a moeda M_A e no 3º a moeda M_X . Isto é implementado com marcas de tempo, "time stamps", em cada uma das moedas do triplo.

As moedas M_B e M_A só podem ser gastas no SD respectivamente pelo Bob ou pela Alice, tendo para isso cada uma, um código chave criptado com a chave pública respectiva. Assim quando, por exemplo, o Bob quiser trocar a sua moeda, junto do SD ele terá que enviar o código chave decriptado. Isto prova a origem da moeda, com não repudiação. A

moeda M_X não tem este código chave de segurança, e só pode ser utilizada pela Alice se nenhuma das outras duas o for.

Na transacção com o Bob, a Alice envia a moeda M_B e guarda as restantes. Se o Bob não lhe der o recibo, ela pode indagar junto do SD se o Bob gastou a moeda. Se a resposta for afirmativa então o SD emite um recibo à Alice especificando o valor da moeda que Bob utilizou, senão a Alice pode utilizar a sua moeda M_A, durante o intervalo de tempo em que ela é válida, para recuperar o dinheiro.

Para que a Alice não tente gastar em duplicado a moeda M_B, o Bob deve manter uma cópia dela enquanto que não terminar o seu período de utilização. A Figura 4 ilustra o desenrolar deste protocolo de pagamento.

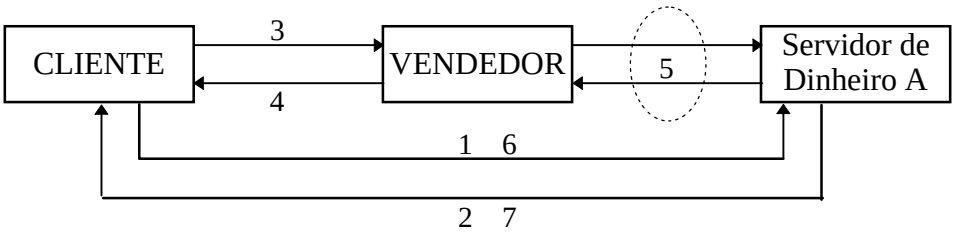


Figura 4. Protocolo de pagamento contra fraude do sistema NetCash

As 5 (ou 7 em caso de tentativa de fraude) fases consistem no seguinte:

1. A Alice envia ao SD numa mensagem criptada com a chave pública deste, as moedas que pretende trocar por triplos, uma chave simétrica gerada por si, os intervalos de tempo que pretende para as moedas MB e MA e a quantia que pretende em triplos.
2. O SD devolve, criptados com a chave simétrica que a Alice lhe enviou, os triplos e possivelmente o troco num triplo unicamente com uma moeda M_X.
3. A Alice envia a Bob a moeda M_B, uma chave simétrica nova, uma chave simétrica de sessão e a indicação do bem ou serviço que pretende. Toda a informação vai criptada com a chave pública de Bob. A chave de sessão vai servir para Bob fazer a ligação da entrega do bem com o pagamento.
4. O Bob envia um recibo à alice. O recibo consiste no valor pago, num identificador para a Alice obter o bem e na data, tudo criptado com a chave privada de Bob. O Recibo vai criptado com a chave simetrica que a Alice enviou em 4.
5. O Bob troca a moeda M_B por uma normal enquanto que ela é válida. Não corresponde a uma operação de autorização porque o Bob neste protocolo tem capacidade para verificar a autenticidade da moeda.

Caso o Bob não cumpra a 4ª fase, então a Alice origina uma 6ª e 7ª fases:

6. A Alice envia ao SD indicação de que Bob não respeitou a fase 4, conjuntamente com a moeda M_A. A informação vai criptada com a chave pública de SD.
7. SD retorna à Alice o recibo ou uma moeda conforme Bob tenha ou não utilizado a sua moeda M_B.

Note-se que as fase 4 e 5 podem ser executadas pela ordem inversa.

O NetCash faz parte de um projecto do Instituto de Ciências de Informação da Universidade do Sul da Califórnia de que também faz parte o sistema, de contas de débito/crédito, NetCheque, descrito no ponto 5.2.1., no qual os intervenientes utilizam cheques electrónicos. Este projecto prevê que os dois sistemas possam ser utilizados interligados. Por exemplo, um vendedor quando recebe dinheiro electrónico de um cliente pode querer que o banco virtual lhe retorne um cheque electrónico à sua ordem. Para que este tipo de operação seja possível os servidores de dinheiro electrónico têm contas no servidores dos cheques electrónicos.

Este sistema verifica anonimato, mas não incondicional, da seguinte forma: A Alice pode adquirir moedas no SD A, e trocá-las por outras no SD B e assim sucessivamente. Quanto maior for a cadeia mais dificil é o cruzamento de informação para seguir o seu rasto. Os autores do sistema dizem que quando uma moeda é trocada por outra, não fica registada a correspondência entre elas.

5.2 Sistemas de Contas de Débito/Crédito

5.2.1 NetCheque

A principal característica deste sistema é que os seus utilizadores podem passar cheques electrónicos, via email ou outro protocolo de transferência de informação, entre intervenientes com contas em servidores diferentes, procedendo a compensações entre os vários servidores.

Este sistema funciona similarmente ao sistema tradicional com informação adicional: um consumidor registado escreve documentos electrónicos, que incluem o seu nome, o seu número de conta, o nome do banco, o sacador do cheque, o valor, a moeda de pagamento e a data de expiração. O cheque inclue uma assinatura electrónica e deve ser endossado, com a assinatura electrónica do sacador, antes de ser depositado.

O modelo de protocolo de pagamento utilizado pelo NetCheque é o de conta de débito/crédito ilustrado na Figura 2, só que o servidor é um servidor de autenticação Kerberos e as duas mensagens trocadas correspondem às mensagens de pedido e fornecimento do bilhete Kerberos como descrito em 2.2.3, Sistemas - Kerberos.

Para escrever um cheque, o cliente utiliza a função *write _cheque*. Esta função, para além de permitir a inserção de toda a informação normal do cheque, obtém um bilhete Kerberos, que será utilizado para autenticar o cliente junto do seu servidor, e gera um CIM para autenticar a informação contida no cheque e coloca ambos no campo assinatura do cheque. O cheque é codificado em base 64 e enviado ao vendedor que lhe retorna o bem.

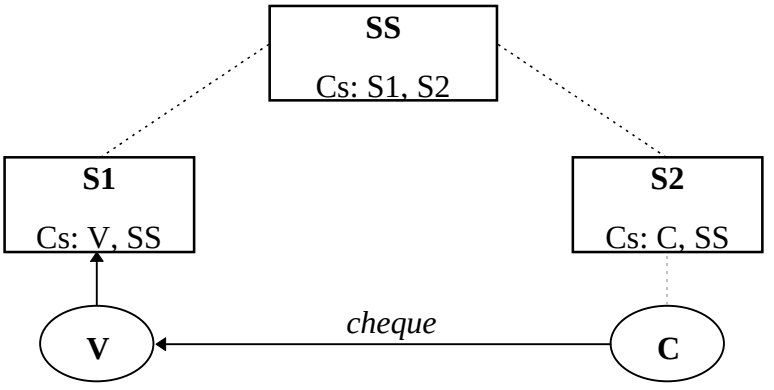
Para depositar o cheque o comerciante obtém um bilhete Kerberos para o autenticar no seu servidor, e gera um autenticador que endossa o cheque em seu nome, juntando-o ao cheque. O cheque é então enviado ao servidor do comerciante para depósito na sua conta.

A Compensação é, normalmente, realizada posteriormente, como no sistema tradicional, reduzindo assim os custos por transacção. Contudo existe a possibilidade de o vendedor requer compensação em tempo real, ou seja, antes de entregar o bem, mediante o pagamento de uma taxa.

Quando o cliente e comerciante tem a conta no mesmo servidor, a compensação restringe-se à transferência de fundos entre as duas contas.

Os servidores estão todos ligados hierarquicamente a um servidor de servidores, que funciona como uma central de compensação (Figura 5). Quando a compensação deve ser

feita entre servidores diferentes, o cheque percorre a hierarquia existente até atingir o servidor que mantem a conta referenciada no cheque. Em cada servidor o cheque é depositado na conta de quem (vendedor ou servidor) depositou o cheque e endossado ao próximo servidor. Por fim o servidor final aceita ou rejeita o cheque sendo essa informação transmitida em cascata no sentido contrário. Para evitar a tentativa de duplicação de um cheque, o servidor final guarda-o até este expirar.



SS: Servidor de Servidores S#: Servidor

V: Vendedor C: Cliente Cs: Contas

Figura 5. Protocolo de pagamento do sistema NetCheque

O NetCheque pretende ser um sistema seguro, resistente, escalonável e eficiente, usando para isso criptografia e vários servidores. Graças à utilização do sistema Kerberos, o sistema pode garantir autenticação dos intervenientes, autenticação da informação trocada, privacidade e autorização. Não suporta anonimato.

5.2.2 NetBill

O protocolo de pagamento do sistema NetBill tem duas diferenças significativas em relação ao modelo apresentado em 4.2.2. Modelo do Protocolo de Pagamento. A primeira diferença é que o interlocutor do cliente é o comerciante. A segunda é que com a troca de mais um par de mensagens entre o cliente e o comerciante, ambos ficam completamente livres de riscos de problemas como a não entrega da informação ou o não pagamento. A Figura 6 ilustra o funcionamento do protocolo.

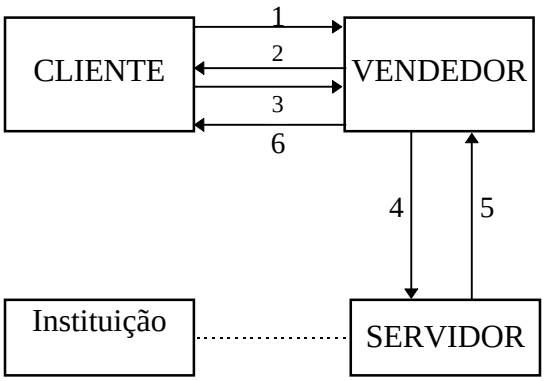


Figura 6. Protocolo de pagamento do sistema NetBill

Este sistema assume que o cliente e o vendedor partilham uma chave simétrica, assim como o vendedor e o servidor NetBill. Na descrição que se segue todas as mensagens são criptadas com estas chaves para garantir privacidade.

Na mensagem 1, autenticada com a sua assinatura digital, o cliente indica ao comerciante qual o bem que pretende adquirir. Este, retorna através da mensagem 2 o bem solicitado criptado com uma chave simétrica gerada aleatoriamente. Entretanto calculou um CIM sobre a mensagem. Após receber o bem, o software do cliente grava-o num disco estável, onde não exista risco de o perder, e calcula um CIM, que envia, mensagem 3, conjuntamente com o identificador do produto, o preço do produto e um valor de *timeout*, ao comerciante com uma assinatura digital. Esta informação constitue uma ordem de pagamento electrónica. Neste momento o cliente tem a informação, mas criptada, e o comerciante a ordem de pagamento. Antes de continuar o protocolo, o comerciante compara os dois CIM: se estiverem de acordo continua, senão volta a repetir o passo 2 ou aborta a transacção. Para continuar o protocolo o comerciante cria uma nota de débito consistindo no preço do bem, no seu CIM, e na chave de decriptamento para o bem, e envia-a, mensagem 4, ao servidor NetBill conjuntamente com uma assinatura digital para autenticar e garantir a integridade dos dados e a ordem de pagamento electrónica. O servidor após verificar que os dados constantes na nota de débito coincidem com os da ordem de pagamento electrónica procede à transferência dos fundos, regista a transacção num ficheiro de transacções e grava uma cópia da chave de decriptação. Por fim retorna, mensagem 5, ao comerciante uma mensagem com assinatura digital a indicar o sucesso da transacção, que por sua vez a repete, 6, para o cliente conjuntamente com a chave de decriptamento.

O NetBill tem custos de transacção muito baixos, na ordem das unidades de escudos para produtos de dezenas de escudos, possibilitando a compra, como, por exemplo, de um único artigo de jornal. A existência desta característica, micropagamentos, conjuntamente com a atomicidade, escalabilidade, segurança, autenticação e privacidade são as grandes apostas do sistema NetBill.

O NetBill usa um único protocolo que suporta transacções numa grande variedade de serviços. O comprador e vendedor comunicam usando aplicações/protocolos adequados para o tipo de informação que pretendem (por exemplo, video, documentos, resultados de pesquisas em bases de dados). Quando o comprador inicia o processo de compra, entra em acção o protocolo de pagamento do NetBill. Isto permite que o NetBill trabalhe com mecanismos de transferência de informação desde o WWW ao FTP.

Para o suporte da transacção o comprador e o vendedor têm cada um uma biblioteca que se integram com a aplicação usada. As biblioteca incorporam os mecanismos de segurança e pagamento. A biblioteca do cliente denomina-se *checkbook* e a do vendedor *till*.

5.2.3 Open Market

Um comutador de pagamentos é um serviço de rede que autoriza e executa ordens digitais de pagamento baseadas em contas bancárias. A ordem de pagamento é autenticada, a cobertura ou crédito da conta verificada e depois a transacção de transferência de fundos originada de modo a completar a ordem de pagamento. O comutador de pagamentos confirma a aceitação ou rejeição de uma ordem de pagamento.

Pode existir mais do que um comutador de pagamentos numa dada rede, e o comutador de pagamentos pode operar em mais do que um *host*, para aumentar a fiabilidade, disponibilidade e velocidade do sistema.

Este sistema segue o modelo descrito em 4.2.2, com a diferença de que baseado no tipo e valor da transacção o comutador decide que nível de segurança a utilizar, desde a utilização única de uma *password* até esquemas de criptamento como descrito no modelo. Isto permite que o equilibrio entre a segurança e a conveniência do cliente seja ajustado ao perfil de risco da transacção e do vendedor e obriga à troca de mais um ou dois pares de mensagens, em relação ao modelo, entre o comutador e o cliente antes de a transacção se verificar.

Este sistema pretende utilizar HTTP seguro como meio de providenciar um canal de comunicação seguro.

Sobre cada pagamento fica registada a informação correspondente num *Smart Statement*. A qualquer momento um utilizador pode consultar os seus *Smart Statements* para ver toda a informação sobre as transacções que efectuou, de bens electrónicos ou fisicos. Se ocorrer uma falha durante uma transacção, o *Smart Statement* contém o estado em que ficou a transacção.

Existem facilidades acrescentadas para conveniência do utilizador. Por exemplo, um comprador pode ir simplesmente adicionando os itens que pretende adquirir a uma lista e no fim, depois de rever a lista retirando ou acrescentando itens, finalizar o processo de aquisição simultâneo de todos os itens escolhidos.

O comutador de pagamento também permite ao comprador e ao vendedor aceder a uma lista com as respectivas transacções cometidas. No caso dos *smart statements* existe um URL que retorna ao comprador o produto comprado.

O sistema tem também facilidades de detecção de compras duplicadas e de controlo de contas. Por exemplo, uma conta pode ser parametrizada com critérios que limitam o tipo de compras ou o valor total de uma transacção pelo comprador ou vendedor. Existem ainda facilidades como descontos.

Os métodos suportados e a usar conforme o nível da transacção são:

- nome de utilizador e palavra chave;
- desafios - o sistema utiliza informação pessoal sobre o utilizador para lhe fazer perguntas de modo a o autenticar;
- dispositivos de autenticação - o sistema faz perguntas cujas respostas dependerão de dispositivos como o *Secure Net Key* (SNK) e o *Secure ID* que o utilizador deve possuir;

O SNK é um dispositivo, tipo calculadora de bolso, que permite autenticar um utilizador e autorizar uma transacção. O SNK tem uma chave secreta DES interna. Quando o desafio aleatório é enviado pelo servidor o utilizador activa o SNK com um pino e introduz o

desafio. Como o servidor sabe qual a resposta correcta, compara-a para decidir sobre a autenticação e autorização da transacção.

Os requisitos verificados por este sistema são segurança, atomicidade, escalabilidade, fiabilidade e eficiência.

5.2.4 First Virtual

Os responsáveis pelo desenvolvimento do First Virtual partem de várias permissas para justificarem a existência do seu sistema e o modo como ele funciona. A primeira premissa é que um sistema de comércio na Internet para funcionar tem que ser simples de usar. A segunda é que o número de clientes aumenta se estes puderem consultar a informação antes de a pagar. A terceira é que qualquer cliente, após analisar a informação, e se esta lhe agradar a pagará. Dizem ainda que por os custos de venda de informação serem praticamente nulos os vendedores de informação não arriscam nada em permitir o seu acesso sem garantias de pagamento. Ou seja, após a informação estar criada vender uma, dez, n ou nenhuma cópia tem os mesmos custos.

Este método funciona do seguinte modo: O cliente tem um código identificador, que transmite quando compra algum bem. O vendedor dá conhecimento da transacção para o sistema, que envia *email* ao cliente a pedir a confirmação da transacção. O cliente pode aprovar, recusar o pagamento, ou declarar que existe fraude. O vendedor corre algum risco porque o cliente pode negar-se a pagar.

O First virtual não disponibiliza confirmações em tempo real, devido ao seu sistema baseado no *email*, pelo que não pode ser utilizado para vendas em tempo real de software ou documentos informatizados. Entretanto permite que o comprador se aperceba da qualidade da informação antes de a pagar.

5.3 Sistemas de Cartão de Crédito

5.3.1 Cybercash

O Cybercash é outro sistema de comércio electrónico na Internet que possibilita transacções com pagamento imediato entre consumidores e vendedores via instituição financeira. As transacções são baseadas em cartões de crédito estando previsto o alargamento a cartões de débito e a dinheiro electrónico. A função do Cybercash é garantir a eficiência, segurança e baixo custo para a realização de transacções comerciais.

O sistema segue também o modelo apresentado em 4.3.2.

O sistema utiliza criptoanálise baseado em chave pública para garantir segurança e privacidade ao cliente.

Para funcionar com o WWW os consumidores e os vendedores recebem software cliente gratuito que comunicam directamente com os servers Cybercash, que por sua vez estão ligados às redes privadas das instituições financeiras.

5.3.2 iKP

O iKP (*i-Key-Protocol*) é uma famila de protocolos constituida por três protocolos 1KP, 2KP e 3KP, representando diferentes níveis de segurança. Este conjunto de protocolos desenvolvido por investigadores da IBM usa criptografia RSA e canais seguros (SHTTP ou SSL) para oferecer segurança aos seus utilizadores. O iKP chama ao servidor do sistema de

gateway porque este passa as transacções do sistema electrónico para o sistema financeiro usual.

Em relação ao modelo proposto para este sistema de pagamento o iKP é fisicamente diferente mas logicamente idêntico pois embora a ordem de compra seja transmitida ao *gateway* via vendedor, ela vai protegida contra qualquer acção do vendedor. Na versão, 1KP, a menos segura, a ordem contém o valor, a identificação do vendedor e do produto, o número do cartão, a data de expiração, um pino associado ao cartão, uma marca de tempo e um CIM. Toda a informação vai criptada com a chave pública do *gateway*.

O iKP garante anonimato em relação a terceiros e opcionalmente em relação ao comerciante.

Este protocolo pode ser implementado em software ou hardware e utiliza a criptografia de modo a não verificar as habituais restrições de exportação do governo dos EUA.

6. Comparação

6.1 Segundos os Requisitos

6.1.1 Requisitos em geral

Requisito / Sistema	Contra Terceiros	Contra Interven	Ano-nimato	Escala-bilidade	Efici-ência	Aceita-bilidade	Inter-operac.	Flexi-bilidade	Atomi-cidade
Digicash	✓	p	✓						
NetCash	✓	✓	f	✓		✓	✓	p	
NetCheque	✓	✓		✓	✓	✓	✓	p	✓
NetBill	✓	✓		✓	✓				✓
Open Market	✓	✓		✓	✓				✓
First Virtual					✓				
CyberCash	✓	f							
iKP	✓	f	p	✓					

✓ - Verifica

f - Verifica, mas de um modo fraco

p - Verifica parcialmente

Se não considerar-mos o sistema First Virtual observa-se que todos se preocupam com a segurança, quer contra terceiros quer contra os intervenientes na transacção. Os sistemas que não verificam são os sistemas de apresentação segura de cartão de crédito que têm associados dois motivos para não preocupar o cliente: a confiança do servidor na boa fé destes e os contratos de exploração de cartões de crédito.

Depois de um modo geral verifica-se que os sistemas de conta de débito/crédito se preocupam com a escalabilidade, eficiência e atomicidade.

A interoperacionalidade só se comecará a verificar quando os sistemas entrarem numa fase estável, ou seja, quando começarem a ser usados com normalide e frequência. Então serão

os utilizadores a exigir esta característica. Entretanto os sistemas NetCash e NetCheque são os primeiros a verificarem este requisito. Repare-se que conjuntamente estes dois sistemas verificam todos os requisitos, faltando apenas a base de consumidores, não representada no quadro.
No que respeita à base de consumidores o que se constata é que os sistemas de apresentação segura de cartão de crédito são os únicos em que não é tudo novo para os utilizadores. Todo o potencial utilizador destes mecanismos sabe qual o funcionamento normal do cartão de crédito e a confiança que pode depositar nele. Por esta razão, no futuro próximo o mecanismo de apresentação segura de cartão de crédito será o mais popular.

6.1.2 Requisitos dos Sistemas de Dinheiro Electrónico

Requisito / Sistema	Operação *off-line*	Transferabilidade	Independência Física	Divisibilidade
DigiCash	✓		✓	
NetCash			✓	✓

Este quadro representa correctamente a dificuldade de implementar sistemas de dinheiro electrónico em que a moeda ou nota tenham as características às homólogas reais. A passagem de uma moeda de um utilizador para outro, que a possa utilizar directamente é para já impossível. A divisibilidade observada pelo sistema NetCash obriga a recorrer ao servidor.

6.2 Segurança

6.2.1 Segurança nos Sistemas

Sistema	Privacidade	Autenticação	Integridade	Não* Repudiação
Digicash	✓	✓	✓	✓
NetCash	✓	✓	✓	✓
NetCheque	✓	✓	✓	✓
NetBill	✓	✓	✓	✓
Open Market	✓	✓	✓	✓
First Virtual				
CyberCash	✓	✓	✓	✓
iKP	✓	✓	✓	✓

* da origem

Este quadro ilustra a utilização dos serviços de segurança que permitem observar no quadro apresentado em 6.1.1.Requisitos em geral, a verificação de segurança contra terceiros e intervenientes.

6.2.2 Análise de Problemas

Esta tabela ilustra a resolução, em cada um dos sistemas, dos seguintes problemas:

A - o cliente receber o bem e interromper a comunicação sem pagar;

B - o vendedor receber o dinheiro e não fornecer o bem;

C - a utilização em duplicado da ordem de compra ou do dinheiro;

D - alteração do valor da transacção por um dos intervenientes sem o conhecimento do segundo.

Sistema	A	B	C	D
Digicash	i	p	d	i
NetCash	i	i	i	i
NetCheque	i	p	i	i
NetBill	i	p	i	i
Open Market	i	p	i	i
First Virtual		i		
CyberCash	i		i	i
iKP	i		i	i

i - impede a ocorrência

d - detecta a ocorrência posteriormente

p - prova a ocorrência

Deste quadro conclui-se que os sistemas consideram em geral os vendedores como intervenientes de confiança. Em regra, com a excepção do First Virtual, os vendedores recebem o valor e só depois entregam o bem ou o acesso a este. Esta confiança faz sentido na medida em que se um vendedor não entregar os bens, então os clientes queixar-se-ão, levando o servidor a agir. No mínimo, tendo em conta o sistema "democrático" da Internet, os clientes comunicarão entre si a ocorrência resultando num boicote generalizado ao vendedor.

6.3 Bens Transaccionados

Sistema	Electrónicos	Fisícos
Digicash	✓	
NetCash	✓	
NetCheque	✓	
NetBill	✓	
Open Market	✓	✓
First Virtual	✓	
CyberCash	✓	✓
iKP	✓	✓

6.4 Utilização de Criptografia

Na elaboração deste quadro considero que um sistema utiliza criptografia desde que a sua segurança dependa da criptografia utilizada a qualquer nível: canal seguro, bilhete Kerberos, etc.

Sistema	**Assimétrica**	**Simétrica**
Digicash	✓	
NetCash	✓	
NetCheque	✓	✓
NetBill	✓	✓
Open Market	✓	✓
First Virtual		
CyberCash	✓	✓
iKP	✓	

Na generalidade os algoritmos utilizados são o RSA e o DES, oferecendo alguns a possibilidade de escolher o algoritmo.

O iKP é o primeiro sistema a ter uma preocupação especial com as restrições de exportação de algoritmos de criptografia impostas pelo governo dos E.U.A.. A criptografia é utilizada neste sistema de modo a que este possa ser utilizado legalmente fora dos E.U.A..

O facto de todos, com excepção do First Virtual, utilizarem criptografia assimétrica permite-lhes verificarem não repudiação da origem.

A criptografia simétrica é utilizada especialmente para proporcionar privacidade e eficiência na criptagem dos bens electrónicos.

7. Considerações Finais

Os três meios de pagamentos têm características que os levam a ser mais indicados para determinados tipos de aquisições e de utilizadores. Por outro lado a sua utilização depende da confiança que neles depositem os potenciais clientes e comerciantes.

Os sistemas de apresentação segura de cartão de crédito são os que suscitam mais confiança em relação ao modo de funcionamento. Como referido atrás, todo o utilizador sabe de um modo geral como funcionam os cartões de crédito e tem confiança nos seus mecanismos de segurança próprios. Julga-se que o utilizador deste sistema o utilizará para fazer compras não muito frequentes.

Os sistemas de conta de débito/crédito estão num nível intermédio em relação à base de clientes e dificuldade de manter. O facto de haver registos das operações realizadas ajuda a criar confiança neste sistema, e torna-o indicado para utilizadores que por terem necessidade de adquirirem muitos bens no dia-a-dia o utilizarão como meio de aumentar a eficiência nas compras mantendo o controlo do que é adquirido. As empresas e instituições em geral serão concerteza os utilizadores comuns deste sistema.

Os sistemas de dinheiro electrónico são os mais complexos. Para já, nenhum verifica um conjunto de requisitos suficientemente lato que leve a sua utilização frequente. É o sistema que apresenta mais conceitos diferentes daqueles com que lidamos no dia a dia. O anonimato é neste momento a sua principal vantagem.

8. Bibliografia

Bellare, Mihir, *iKP - A Family of Secure Electronic Payment Protocols*, IBM, Maio de 1995

Chaum, David, *Achieving Electronic Privacy*, Scientific American, Agosto de 1992

Comer, Douglas E., *Internetworking With TCP/IP Volume I Second Edition*, Prentice - Hall, 1991

Cox, Benjamin T. H., *Maintaining Privacy in Electronic Transactions*, Carnegie Mellon University, Pennsylvania, Agosto de 1994

Fahn, Paul, *FAQ About Today's Cryptography*, RSA Laboratories, Redwood City, Setembro de 1993

Gifford, David K., Stewart, Lawrence C., Payne, Andrew C., Treese, G. Winfield, *Payment Switches for Open Networks*, Open Market, Inc., 1994

Kent, Stephen T., *Internet Privacy Enhanced Mail*, Communications of the ACM, Agosto de 1993

Medvinsky, Gennady, Neuman, B. Clifford, *Electronic Currency for the Internet*, Electronic Markets , Outubro 1993

Medvinsky, Gennady, Neuman, B. Clifford, *NetCash: A Design for Pratical Electronic Currency on the Internet,* Information Sciences Institute, University of Southern California, Novembro 1993

Neuman, B. Clifford, *Proxy-Based Authorization and Accounting for Distributed Systems*, Information Sciences Institute, University of Southern California, Maio1993

Neuman, B. Clifford, Medvinsky, Gennady, *Requirements for Network Payment: The NetCheque Perspective,* Information Sciences Institute, University of Southern California, 1995

Neuman, B. Clifford, Ts'o, Theodore, *Kerberos: An Authentication Service for Computer Networks*, IEEE Communications Magazine, Setembro 1994

O'Toole, Kevin, *Transaction Protocol Alternatives*, Carnegie Mellon University, Pennsylvania, Abril de 1994

Simmons, Gustavus J., *Cryptanalysis and Protocol Failures*, Communications of the ACM, Novembro de 1994

Sirbu, Marvin, Tyger, J. D., *NetBill:An Internet Commerce System Optimized for Network Delivered Services*, Carnegie Mellon University, 1994