Sistemas de Pagamento Eletrônico

Lucas de Carvalho Ferreira *Ricardo Dahab*

Relatório Técnico IC–98-20

Maio de 1998

Sistemas de Pagamento Eletrônico

Lucas de Carvalho Ferreira Ricardo Dahab*

Sumário

Neste trabalho, apresentamos um esquema que possibilita a análise e comparação de sistemas de pagamento eletrônico a partir de sua tipificação, dos requisitos para estes sistemas, seu modo de funcionamento e aspectos de implementação e apresentamos análises de alguns dos sistemas de pagamento eletrônico que consideramos mais importantes ou representativos.

Abstract

In this work we present a framework for the analysis and comparison of electronic payment systems. The following aspects are considered: typification, desirable requisites, functioning description and implementation issues. This framework is then used to analyze some of the most popular or representative payment systems that have been proposed so far.

*Instituto de Computação, Universidade Estadual de Campinas, 13081-970 Campinas, SP. Pesquisa desenvolvida com suporte financeiro parcial do CNPq — Conselho Nacional de Desenvolvimento Científico e Tecnológico.

Conteúdo

1 Introdução

A pesquisa e aplicação de sistemas criptográficos teve um grande impulso com a explosão do número de usuários da Internet e as primeiras aplicações comerciais desta rede. As necessidades de segurança destas aplicações ainda não foram supridas e novas propostas e padrões surgem a cada dia, tratando desde simples programas para cifrar mensagens ou autenticar usuários até complexos sistemas que permitem a realização de pagamentos pela rede.

Foram estes sistemas de pagamento que mais atraíram atenção nos últimos dois anos, após o surgimento do padrão SSL, que permite a transmissão segura de informações em redes TCP/IP. Com a ampla adoção do SSL como padrão seguro de transmissão de informações, o primeiro problema relacionado à segurança das transmissões pela Internet foi resolvido e os desenvolvedores e pesquisadores se voltaram para outro empecilho ao amplo desenvolvimento do comércio na Internet: a realização de transações de transferência de valores monetários através da rede. Neste ponto, então, começa o desenvolvimento de um sem número de sistemas e padrões para permitir a realização de pagamentos através de redes de computadores.

Muitos destes sistemas foram desenvolvidos e alguns já estão implementados, em fase de testes ou já em funcionamento comercial, mas não havia uma metodologia que permitisse comparar as características destes sistemas. Alguns trabalhos foram desenvolvidos neste sentido ([10, 2, 5, 22, 16, 1, 6, 17]), mas estes não tratam todos os aspectos do sistema, incluindo as suas características e seu modo de funcionamento.

Neste texto, apresentamos um esquema que possibilita a análise e comparação de sistemas de pagamento eletrônico a partir de sua tipificação, dos requisitos para estes sistemas, de seu modo de funcionamento e aspectos de implementação e apresentamos análises de alguns dos sistemas de pagamento eletrônico que consideramos mais importantes ou representativos. Na próxima seção, apresentamos o esquema de classificação e análise de sistemas de pagamento eletrônico. Em seguida, na seção 3, apresentamos as descrições de alguns sistemas com base no esquema apresentado na seção 2. No apêndice A encontra-se uma breve introdução à criptografia, com os conceitos necessários ao bom entendimento deste documento e no apêndice B apresentamos tabelas resumindo as análises da seção 3.

2 Descrição do esquema

Esta seção apresenta o esquema proposto para classificação de sistemas de pagamento eletrônico, primeiro caracterizando o tipo do sistema e estudando os requisitos gerais encontrados para sistemas de pagamento. Depois é apresentado o modelo de funcionamento destes sistemas, que permite uma melhor compreensão dos protocolos que compoem cada sistema, e enfim um resumo dos principais aspectos de implementação. A figura 1 apresenta este esquema graficamente.

2.1 Tipificação

Os sistemas de pagamento eletrônico apresentam certas características que nos permitem classificar e compreender seu funcionamento e aplicações. Estas características são:

- **Modelo de Troca**
  - **cupons (troca direta)**: Sistemas em que as transações ocorrem pela transferência de cupons de valor predeterminado. Estes cupons funcionam como num sistema de notas e moedas. Num sistema de cupons, o usuário deve "comprar" seus cupons de uma entidade emissora antes de poder realizar transações. Sistemas baseados em cupons são algumas vezes chamados de sistemas *cash-like*.

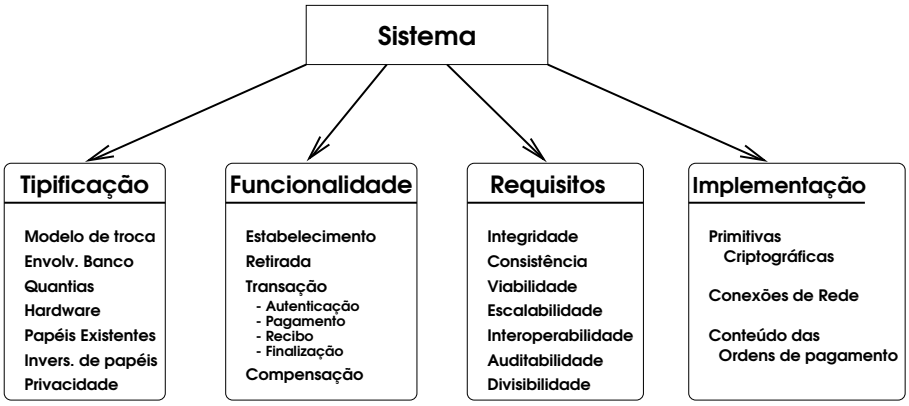

Figura 1: Os aspectos da caracterização dos sistemas de pagamento

- **notacional (troca indireta)**: São sistemas em que as transações ocorrem através da atualização de saldos em contas mantidas junto a uma instituição financeira. Nestes sistemas, os usuários trocam documentos que autorizam a transferência de valores entre suas contas, o valor da transferência sendo determinado pelo usuário. O cheque é um bom exemplo de um sistema notacional, assim como os cartões de crédito. Estes sistemas são algumas vezes chamados de sistemas de débito-crédito.
- **híbrido**: Sistemas que usam cupons e atualização de saldos. Um exemplo é o CAFé, que será citado mais adiante.

• **Envolvimento da Entidade Controladora**

- **on-line**: são os sistemas que necessitam do envolvimento da entidade controladora do sistema durante a realização da transação de transferência de valores. São sistemas adequados para a Internet, mas que incorrem em custos devidos às conexões adicionais necessárias. Alguns exemplos são os sistemas projetados especificamente para a Internet (e-cash, First Virtual, SET etc) e os sistemas de cartões de débito (Visa Electron, Cheque Eletrônico, B.I.S.).
- **off-line**: alguns sistemas não necessitam que a entidade emissora seja contactada no momento da transação. Esta entidade deverá ser contactada em algum momento do futuro para que a transação seja efetivada; o recebedor do pagamento é capaz de verificar a validade da transação por si só.

• **Quantias envolvidas**

- **micropagamentos**: pequenos valores são trocados, desde milésimos de dólares (ou reais) até alguns poucos dólares (reais), tipicamante até US$ 5,00.
- **pequenos e médios pagamentos**: valores que podem transitar na Internet com certa segurança, em geral de US$ 1,00 a US$ 500,00.
- **grandes pagamentos**: grandes quantias, geralmente acima de US$ 500,00, que exigem um nível de segurança maior do que se consegue hoje na Internet.

• **Hardware necessário**

- **dedicado**: faz uso de hardware especial, como *smart cards*.

  - **uso geral**: usa apenas computadores de uso geral. O usuário que já possui um computador não precisa adquirir nenhum equipamento especial.

- **Papéis envolvidos:** Os papéis a serem desempenhados pelos participantes das transações. Em geral são pagadores, recebedores, usuários ou bancos, embora alguns sistemas façam distinção entre compradores e vendedores.

- **Inversibilidade dos papéis**

  - **papeis fixos**: cada participante tem seu papel definido, seja vendedor, comprador ou banco. Para poder assumir dois papéis, o usuário tem que se cadastrar duas vezes, uma para cada papel desempenhado.
  - **papéis variáveis**: o sistema permite que o usuário desempenhe papéis diferentes dependendo da situação, podendo assumir o papel de pagador ou recebedor de acordo com sua conveniência. Estes esquemas permitem naturalmente a transferência de valores entre usuários. Em geral, os sistemas não permitem que um usuário assuma o papel de banco.

- **Privacidade**

  - **existente**: o sistema permite preservar a privacidade dos participantes, em situações como compras anônimas, transmissões seguras ou proteção de informações críticas. Alguns sistemas garantem que as informações só estarão disponíveis para as entidades que delas necessitarem.
  - **inexistente**: o sistema não faz uso de técnicas criptográficas que garantam a privacidade das informações transmitidas. Caso seja necessário, protocolos externos devem ser usados.

- **Divisibilidade** Deve ser possível substituir um cupom de valor alto por diversos cupons de menor valor. Estabelecemos quatro níveis de divisibilidade:

  1. o usuário é capaz de dividir os cupons.
  2. a entidade emissora pode ser contactada para trocar cupons pelo valor equivalente em cupons de menor valor.
  3. o sistema permite a devolução de troco.
  4. não há divisibilidade, ou trata-se de um sistema notacional.

2.2 Características Desejáveis

Considerando um modelo geral para sistemas de pagamento eletrônico, podemos estabelecer algumas características que poderiam ser desejadas nestes sistemas. Devemos ter ser em mente que a situação em que os sistemas serão usados deve ser levada em conta para determinar quais destas características são necessárias ou desejáveis.

Integridade O sistema deve ser capaz de impedir que informações sejam alteradas por descuido ou de forma não autorizada.

Consistência O sistema nunca deve estar num estado ilegal ou num estado em que os participantes tenham visões conflitantes do sistema. Uma maneira de garantir a consistência é fazer uso de transações ACID, que garantem:

- Atomicidade: a transação acontece completamente ou não acontece.
- Consistência: todos os participantes devem estar de acordo acerca dos fatos relevantes da transação.

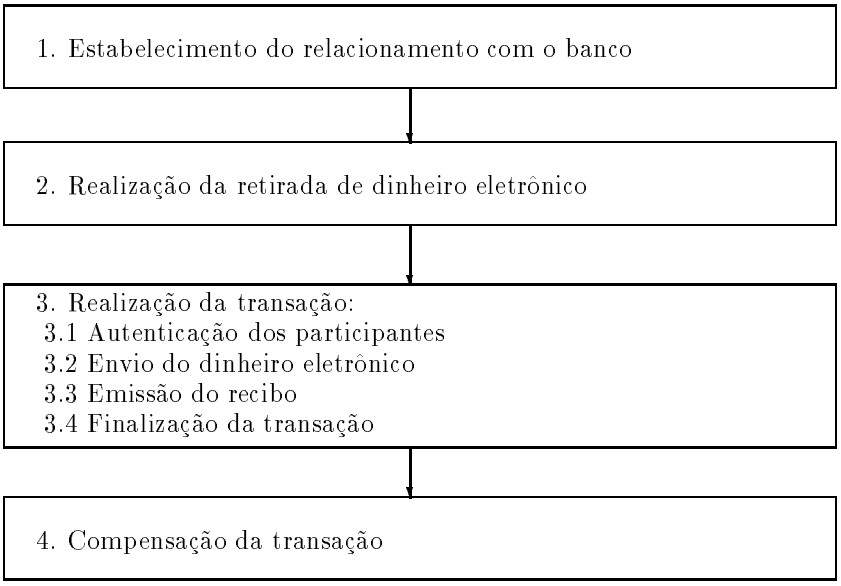

Figura 2: Esqueleto geral de funcionamento dos sistemas de pagamento

- Isolamento: uma transação não interfere em outras.
- Durabilidade: o sistema deve ser capaz de retornar ao último estado consistente.

Viabilidade econômica O custo das transações deve ser compatível com os valores trocados através do sistema.

Escalabilidade A inclusão de novos usuários no sistema não deve trazer uma queda de desempenho acentuada. O sistema deve permitir aumento do número de usuários e da quantidade de moeda envolvida sem que haja uma degradação acentuada de seu desempenho.

Interoperabilidade O sistema deve permitir a troca de moeda com outros sistemas. Por exemplo, deve ser possível trocar um cheque por papel moeda.

Auditabilidade O sistema deve permitir a realização de auditorias para detecção de falhas, fraudes ou comportamento inadequado de seus usuários.

2.3 Funcionamento

O funcionamento dos sistemas de pagamento eletrônico consiste, de forma geral, das seguintes etapas, ilustradas na figura 2. Estas etapas estão descritas de acordo com a visão do usuário que realiza um pagamento.

1. **Relacionamento**
   Consiste do estabelecimento do relacionamento entre o usuário e o banco ou entidade do sistema financeiro responsável pela administração do sistema de pagamentos. Esta é chamada de banco ou entidade emissora/controladora do sistema.

   O primeiro passo para que um usuário possa fazer uso de um sistema de pagamento eletrônico é se cadastrar com a entidade que controla o sistema, o que pode envolver a abertura de uma

conta, a aquisição de *software* ou a inicialização de mecanismos de autenticação, tais como a geração de chaves públicas.

2. **Retirada**
   Nesta etapa, o usuário deve contactar a entidade emissora que o habilitará a realizar transferências de valores. Isto pode se dar pela transferência de moedas eletrônicas, carga de um *smart-card* ou pela emissão de um certificado de crédito.

3. **Transação**
   Esta é a etapa principal do funcionamento dos sistemas, na qual ocorre a troca do dinheiro eletrônico por um recibo de pagamento. é durante esta etapa que ocorre a transferência de valor monetário.

   (a) **Autenticação**
   Pode ser necessário aos participantes ter a certeza de que estão em contato com outro usuário autorizado do sistema.

   (b) **Pagamento**
   O pagador envia o dinheiro eletrônico ao recebedor.

   (c) **Recibo**
   O recebedor envia ao pagador um recibo correspondente à transação.

   (d) **Finalização**
   Estando os participantes de acordo quanto ao resultado da transação, esta pode ser finalizada sem problemas. Caso contrário algum mecanismo de resolução de disputas pode ser acionado.

4. **Compensação**
   O recebedor deve levar o dinheiro eletrônico ao banco para que este seja convertido em moeda real ou depositado em sua conta. Em alguns casos, o recebedor pode optar por receber a quantia em dinheiro eletrônico do mesmo tipo ou solicitar sua conversão em outro tipo de dinheiro eletrônico.

2.4 Aspectos de Implementação

Alguns aspectos do projeto de um sistema de pagamento eletrônico estão intimamente ligados à sua implementação. Alguns destes sistemas foram especificados em detalhes, incluindo os aspectos de implementação, enquanto outros projetos não incluem este tipo de detalhamento. Nesta seção, apresentamos os aspectos de implementação mais importantes para a análise de um sistema de pagamento eletrônico:

Criptografia Descreve os algoritmos criptográficos a serem usados no sistema, detalhando os seguintes itens:

- Cifras simétricas
- Cifras assimétricas
- Assinatura digital
- Certificados
- *hashings*

Conexões de rede Quantidade e tipo das conexões de rede necessárias ao funcionamento do sistema.

Formato dos cupons ou ordens de pagamento O conteúdo e a organização dos cupons ou ordens de pagamento usados no sistema devem ser apresentados.

3 Análise dos Sistemas de Pagamento Eletrônico

Nesta seção, apresentamos alguns dos mais importantes e representativos sistemas de pagamento eletrônico, que são analisados de acordo com o esqueleto de funcionamento, as características, requisitos e aspectos de implementação descritos anteriormente. As descrições encontradas nesta seção estão sumarizadas nas tabelas do apêndice B.

3.1 Green Commerce Model da First Virtual

A First Virtual Holding Company foi uma das primeiras empresas a oferecer uma solução que permite a realização de transações pela Internet. O objetivo básico do sistema é eliminar a necessidade da transmissão de números de cartão de crédito pela rede. O sistema foi batizado Green Commerce Model [24], sendo o único sistema encontrado a não fazer uso de criptografia.

O Green Commerce foi projetado para a venda de informações pela rede, sendo que o vendedor assume os riscos de não receber o pagamento. O sistema funciona basicamente pela troca de mensagens de correio eletrônico, embora outros tipos de comunicação, como telnet, possam ser usados.

Como não faz uso de criptografia, os usuários do sistema não necessitam de *software* especial, e podem usar os programas navegadores e de envio de correio eletrônico que já possuírem. Os vendedores podem construir sistemas que automatizem o processo de venda ou usar os *softwares* prontos fornecidos pela *First Virtual*. A segurança do sistema está parcialmente baseada na segurança do sistema de correio eletrônico usado pelos participantes das transações.

3.1.1 Características

Modelo de troca: notacional
Sendo uma extensão ao método tradicional de compras por cartões de crédito, o sistema define contas especiais vinculadas a um cartão e que podem ser usadas para a realização de transações na Internet.

Envolvimento da entidade emissora: *on-line*
Numa transferência, o comprador informa ao vendedor o número de sua conta First Virtual, que tem de ser validado no momento da transação.

Quantias envolvidas: micropagamentos
O sistema foi projetado para venda de informações na Internet, e por isso não tem mecanismos de segurança, o que possibilitou uma redução nos custos. Assim, apenas micropagamentos podem ser efetuados com alguma segurança. O servidor central irá ajuntar diversas transações de cada usuário antes de processá-las junto à empresa de cartões de crédito, diminuindo assim o custo por transação.

Hardware necessário: uso geral
O *Green Commerce* foi projetado para fazer uso apenas de *hardware* e *software* disponíveis na maior parte das máquinas usadas para acesso à Internet.

Papéis envolvidos: comprador, vendedor e servidor central.
O servidor central, pertencente à First Virtual, é quem realiza a transferência de valor entre as contas dos compradores e vendedores. Cada vendedor deve estabelecer uma conta de

comprador no servidor central e solicitar a conversão desta conta em uma conta de vendedor, passando assim a poder receber pagamentos.

Inversibilidade de papéis: inexistente
O sistema distingue claramente entre contas de compradores e contas de vendedores.

Privacidade: inexistente
O sistema não prevê mecanismos para garantia de privacidade ou segurança das informações.

Divisibilidade: nível 4, o sistema é notacional.

3.1.2 Requisitos

Integridade O sistema confia nos mecanismos de integridade do TCP/IP e do SNMP, que são reconhecidamente fracos. Não há garantia da integridade das mensagens trocadas.

Consistência O mediador tenta garantir a consistência do sistema. Em caso de dúvida ou disputa, o mediador resolve a questão.

Viabilidade econômica O sistema está baseado nos protocolos mais usados na Internet, não agregando novos serviços de segurança. Sendo assim, apresenta um baixo custo de implantação e manutenção e pode ser considerado viável à realização de micropagamentos.

Escalabilidade O sistema é bem escalável, apesar de apresentar um gargalo no servidor central da entidade emissora. Uma freqüência muito grande de requisições pode comprometer o desempenho do sistema. Uma extensão ao sistema com o uso de várias entidades emissoras poderia melhorar este aspecto.

Interoperabilidade O sistema não prevê interoperabilidade.

Auditabilidade Todas as transações passam pelo servidor central que provê mecanismos de *logs*, extratos etc.

3.1.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   O usuário deve entrar em contato com o servidor central da First Virtual e estabelecer uma conta neste servidor. O usuário deverá fornecer o número de seu cartão de crédito, o que deve ser feito por telefone ou fax para maior segurança. Após ter se cadastrado, fornecendo nome, endereço, endereço de *e-mail* e o número do cartão de crédito, o usuário receberá um número de conta First Virtual. Este número de conta será usado na realização das transações. O cadastro não é feito pela Internet para aumentar a segurança do sistema.
2. **Retirada**: não há retirada já que o sistema atua pela transferência de valores entre contas.
3. **Transação**
   (a) **Autenticação**: não há autenticação dos participantes.
   (b) **Pagamento**
   Após a negociação do valor a ser pago, o comprador recebe as informações requisitadas e envia o número de sua conta First Virtual ao vendedor. O vendedor repassa este número, o número de sua conta, o valor da transação e a moeda usada na transação ao servidor central. Após esta etapa, o vendedor entrega as mercadorias.

(c) **Recibo**: não há emissão de recibo.

(d) **Finalização**
O servidor central envia um pedido de confirmação ao comprador, que pode responde SIM, NÃO ou FRAUDE. Caso o comprador responda SIM, o servidor envia uma confirmação ao vendedor e vai descontar o valor do cartão de crédito do comprador. Caso seja NÃO, o servidor informa ao vendedor que a transação não se completou. Se a resposta for FRAUDE, o servidor central inicia uma investigação.

4. **Compensação**
Após um prazo de 91 dias, a First Virtual deposita o valor na conta do vendedor. Este é o prazo que o comprador tem para receber a fatura do cartão de crédito e verificar se houve algum problema.

3.1.4 Aspectos de Implementação

Criptografia: não é usada.

Conexões de rede: 3 conexões.
O sistema prevê uma conexão entre comprador e vendedor, por onde se dará a transação, uma conexão do vendedor com o servidor central e uma conexão do servidor central com o comprador. Todas as conexões podem ser substituidas pela troca de correio eletrônico.

Formato das ordens de pagamento: As ordens de pagamento consistem apenas do número de identificação do comprador. O vendedor anexa a este sua identificação, valor e unidade monetária usada na transação.

3.2 GlobeID da GCTech

A empresa francesa GCTech desenvolveu o GlobeID [18] para ser um sistema completo para comércio eletrônico, sendo que este deve tratar desde a negociação do preço até o pagamento. O sistema foi projetado para ser usado em conjunto com métodos tradicionais de pagamento, através de uma conta especial vinculada a uma conta bancária ou a um cartão de crédito.

O ponto que difere o GlobeID dos outros sistemas estudados é que seus projetistas tentaram fazer dele mais que um sistema para a realização de pagamentos, mas um sistema em que haja um serviço de cartório, onde ficam armazenados os dados referentes às transações. Além disso, o serviço de cartório deve impedir que os usuários neguem a sua participação em uma transação (não repúdio).

3.2.1 Características

Modelo de troca: notacional
O sistema trabalha com contas especiais gerenciadas por uma entidade central, sendo que as transferências são feitas entre estas contas. Os autores argumentam que a criação de moeda eletrônica poderia ser ilegal em alguns países, além de apresentar problemas técnicos quanto ao armazenamento destas moedas com segurança.

Envolvimento da entidade emissora: *on-line*
Para que as transferências possam acontecer, a entidade que gerencia as contas deve ser acionada. O cliente repassa uma proposta de negócio ao banco que valida os dados e realiza a transação.

Quantias envolvidas: pequenos pagamentos
Os autores indicam um limite inferior de cerca de US$ 0,05 para as transações por este sistema, indo até algumas centenas de dólares na outra ponta. Valores da ordem de US$ 0,05 seriam classificados como micropagamentos, mas acreditamos que este sistema seja realmente eficiente na faixa dos pequenos pagamentos, a partir de US$ 1,00 .

Hardware necessário: uso geral
O sistema não faz uso de *hardware* específico e pode ser implementado em qualquer tipo de computador.

Papéis envolvidos: comprador, vendedor e servidor.
O sistema consiste de compradores, vendedores e de uma rede de servidores, que mantém as contas especiais dos usuários fornecendo os serviços de movimentação financeira e de cartório. Os compradores possuem uma senha, enquanto que os vendedores devem ter um par de chaves para uma cifra assimétrica. O servidor deve conhecer todas as senhas e todas as chaves públicas. O servidor deve atuar como intermediário em todas as transações. Podem existir vários servidores participando do sistema.

Inversibilidade de papéis: inexistente
Embora os autores não façam distinção entre contas de compradores e contas de vendedores, os programas usados são diferentes, assim como o tipo de informação que a entidade controladora deve ter a respeito de cada participante. Por exemplo, os vendedores devem registrar chaves públicas enquanto os compradores usam uma senha.

Privacidade: existente
Algumas mensagens são cifradas. é possível no entanto a um observador descobrir o que e por quanto um usuário está comprando. O banco tem informações sobre toda a operação. O cliente sabe quem é o vendedor embora o vendedor não saiba quem é o cliente. As mensagens cifradas e o mecanismo de *challenge-response* (ver seção A.5.1) usados impedem que um observador obtenha informações sobre a conta do usuário.

Divisibilidade: nível 4, o sistemas é notacional.

3.2.2 Requisitos

Integridade Assinaturas digitais e *hashings* são usados para garantir a integridade das mensagens. O usuário tem uma senha para permitir acesso a sua conta.

Consistência O mediador tenta garantir a consistência do sistema. Em caso de dúvida ou disputa, o mediador resolve a questão.

Atomicidade Depois que o comprador autoriza uma transação, não há mais possibilidade de revertê-la. Até este momento o comprador pode cancelar a transação.

Consistência O vendedor apresenta uma proposta que não pode ser alterada pelo comprador, sendo que esta proposta é o documento usado pelo banco para realizar a transferência. Assim, todos tem uma visão consistente da transação.

Isolamento Desde que o comprador tenha crédito, as transações são independentes. Se o comprador ultrapassar o limite que pode ser pré-estabelecido, as transações passam a ser negadas em função de transações anteriores.

Durabilidade A entidade emissora permite ao sistema estar sempre num estado consistente.

Viabilidade econômica Este sistema apresenta um custo de manutenção significativo, o que deve torná-lo eficiente para valores acima de US$ 1,00. No entanto, os autores afirmam que este sistema é adequado para transações acima de US$ 0,05.

Escalabilidade O sistema tem como gargalo o servidor da entidade controladora, embora sejam possíveis extensões para permitir a coexistência de diversas destas entidades.

Interoperabilidade O sistema não prevê interoperabilidade.

Auditabilidade Todas as transações passam pelo servidor central que pode prover mecanismos de *logs*, extratos etc. Além disto todas as transações são autenticadas com base em assinaturas digitais ou senhas.

3.2.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   O usuário deve estabelecer um relacionamento com um dos servidores de intermediação, fornecendo os dados do seu cartão de crédito, conta corrente ou de algum outro meio de pagamento que o servidor aceite. O servidor irá fornecer uma senha e um número de identificação ao usuário, assim como o *software* necessário à sua participação no sistema.

2. **Retirada**: não há retirada já que o sistema atua pela transferência de valores entre contas.

3. **Transação**

   (a) **Autenticação**
   O comprador deve entrar em contato com o vendedor e pedir uma cotação de preços. O vendedor enviará a cotação assinada com sua chave privada. O comprador irá repassar esta cotação ao servidor GlobeID, que irá efetuar a autenticação do comprador. A autenticação do comprador com o vendedor é feita via *challenge-response* (seção A.5.1), o que garante que a senha não trafega na rede. O vendedor é identificado pela assinatura na cotação.

   (b) **Pagamento**
   Quando envia o pedido de autenticação, o servidor informa ao comprador os detalhes da transação. Na resposta ao pedido de autenticação, o comprador deve confirmar seu desejo de continuar com a transação. Se for o caso, o servidor irá realizar a transferência entre a conta do comprador e a conta do vendedor.

   (c) **Recibo**
   O servidor emite uma prova de pagamento e envia ao comprador, que a repassa ao vendedor. O vendedor então entrega a mercadoria ou informação adquirida.

   (d) **Finalização**: não há etapa de finalização.

4. **Compensação**
   Não há etapa de compensação, já que a transferência ocorre quando o servidor recebe a confirmação de que o comprador aceita a transação.

3.2.4 Aspectos de Implementação

Criptografia: são usados os seguintes itens:

Cifras assimétricas: São usadas, embora o algoritmo não seja especificado.

Assinatura digital: O vendedor deve assinar a oferta de produtos/serviços.

Hashings: São usados como MACs no processo de *challenge-response*.

Conexões de rede: 2 conexões.
Uma conexão deve ser estabelecida entre o vendedor e o comprador e outra é necessária entre o comprador e o servidor do banco.

Formato das ordens de pagamento: Não especificado.

3.3 O Protocolo PayMe

O PayMe [19] foi desenvolvido no Trinity College, de Dublin, Irlanda e teve como objetivo melhorar os sistemas de pagamentos baseados em cupons, mantendo as qualidades dos sistemas mais conhecido e eliminando suas deficiências. Os principais sistemas que deram origem ao PayMe foram o E-cash (seção 3.8) e o NetCash (seção 3.12). O PayMe tentou manter o alto grau de privacidade oferecido pelo E-cash e oferecer a escalabilidade do NetCash[1], sem com isso diminuir a segurança do sistema.

O sistema tenta garantir o anonimato de maneira semelhante ao NetCash, ou seja, permitindo que a troca de moedas seja feita de forma anônima. Assim, um usuário que detém moedas dos sistema pode depositá-las em sua conta ou trocá-las por moedas que somem o mesmo valor total. Este mecanismo pode ser usado para obter as moedas necessárias à realização de pagamentos no valor exato ou para tentar mascarar o padrão das compras realizadas por um usuário.

3.3.1 Características

Modelo de troca: cupons
Os cupons deste sistema são chamados de moedas, sendo numerados e contendo uma identificação da entidade emissora, assim como a data de validade.

Envolvimento da entidade emissora: *on-line*
O banco que emite cada moeda deve ser contatado para confirmar a validade desta.

Quantias envolvidas: pequenos pagamentos
Os protocolos deste sistema foram projetados para uso na Internet, fazendo uso do TCP/IP como camada inferior, o que implica na possibilidade de exploração dos problemas de segurança do TCP para burlar o sistema. Além disso, uma das mensagens do protocolo não é criptografada, o que diminui a segurança do sistema. O uso de criptografia garante segurança suficiente à transferência de pequenos valores.

Hardware necessário: uso geral
O sistema não faz uso de *hardware* especial como *smart cards* ou outros mecanismos deste tipo, sendo passível de implementação em qualquer tipo de computador.

Papéis envolvidos: usuários e bancos.
Os usuários realizam transações pela rede, e os bancos emitem os cupons, ou moedas, usados no sistema.

[1] Acreditamos que o sistema tenha níveis de privacidade, escalabilidade e segurança semelhantes ao NetCash mesmo sendo mais simples.

Inversibilidade dos papéis: papéis variáveis.
Os usuários do sistema podem tanto atuar como pagadores quanto como recebedores. O único papel fixo é o papel do banco, ou entidade emissora.

Privacidade: existente
O sistema permite aos usuários a realização de trocas de moedas de forma anônima, o que possibilita a realização de transações em que a identidade do comprador é desconhecida. Apenas o banco é identificado por todos os participantes e o comprador sempre sabe a identidade do vendedor.

Divisibilidade: o protocolo prevê que os usuários podem trocar moedas com o banco, tanto para aumentar a privacidade das transações, já que a troca pode ser feita de forma anônima, quanto para obter moedas de menor valor.

3.3.2 Requisitos

Integridade: a integridade das moedas e das mensagens é garantida pelo uso de assinaturas e *hashings*.

Consistência: não é tratada de maneira explicita na especificação.

Viabilidade econômica: Este sistema apresenta um custo de operação por necessitar de conexões *on-line* e fazer uso de cifras assimétricas e certificados, o que o torna inadequado à realização de microtransações.

Escalabilidade: o sistema permite a existência de várias entidades emissoras e a incorporação de novos usuários é bastante fácil. O principal problema quanto à escalabilidade do sistema é a possibilidade do número de moedas válidas de um único banco crescer a ponto de inviabilizar a consulta aos números de série das moedas em circulação.

Interoperabilidade: o sistema prevê a existência de diversas entidades emissoras e a interoperabilidade com o sistema de contas bancárias. Sendo um sistema *on-line*, é possível a implantação de um serviço de conversão de moedas para outros sistemas.

Auditabilidade: as moedas contém a identificação da entidade emissora e um número de série. Nenhum outro mecanismo de auditoria é especificado.

3.3.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   O usuário deve manter uma conta corrente num dos bancos que participa do sistema. Desta conta, o usuário poderá realizar retiradas e depósitos de dinheiro eletrônico. Além disto, o usuário precisa receber e instalar o *software* de carteira eletrônica em seu computador.

2. **Retirada**
   O usuário informa ao banco o número de sua conta, sua senha e o valor da retirada. Esta mensagem é assinada e enviada ao banco. O banco irá responder enviando as moedas ou uma mensagem de erro. Se o usuário desejar realizar pagamentos anônimos, este deve trocar as moedas com algum banco de forma anônima.

3. **Transferência**

(a) **Autenticação**
O pagador só se identifica se quiser, e por meios fora do escopo do sistema. O recebedor deve enviar uma mensagem ao pagador requisitando o pagamento. Nesta mensagem vai a chave pública do recebedor.

(b) **Pagamento**
Se o pagador aceitar as condições do recebedor, este envia as moedas, cifradas com a chave pública do recebedor.

(c) **Recibo**
O recebedor verifica com o banco a validade das moedas recebidas e devolve um recibo. Esta verificação pode ser feita de duas maneiras: depositando as moedas em sua conta junto a um banco ou trocando as moedas por outras junto ao banco que as emitiu. Em qualquer destes casos, o banco indicará se as moedas são válidas.

(d) **Finalização**: não há.

4. **Compensação**
Os usuários podem depositar ou trocar os cupons a qualquer momento. O recebedor sempre deve realizar uma destas operações para verificar a validade das moedas recebidas.

Observações:

1. O sistema consegue atingir um alto grau de segurança se for usada uma infra-estrutura de certificação de chaves não prevista na especificação.

3.3.4 Aspectos de Implementação

Criptografia: as primitivas criptográficas usadas são:

Cifras simétricas: O protótipo usa o IDEA, embora outros algortimos possam ser usados.

Cifras assimétricas: O RSA foi escolhido para o protótipo. Outros sistemas poderiam ser usados se conveniente.

Assinatura digital: idem.

Conexões de rede: 2 conexões.
Uma conexão é necessária entre o comprador e o vendedor, e uma entre o vendedor e o banco.

Formato dos cupons: As moedas PayMe têm os seguintes campos:

- valor
- número de série
- identificação e endereço da entidade que emitiu a moeda
- validade

Cada moeda é assinada pelo banco que a emitiu.

3.4 Secure Electronic Transactions

O SET [25] é hoje o mais importante protocolo projetado para permitir a execução de pagamentos seguros pela Internet. Isto porque surgiu dos esforços conjuntos de grandes empresas da área financeira (Visa, MasterCard) e da área de informática (IBM, Netscape, Microsoft). é um protocolo destinado à realização de transações com cartões de crédito na Internet e pressupõe o uso da infra-estrutura já existente para compensação de transações com cartões de crédito. Assim, existem diversas empresas capacitadas a fornecer cartões e outras capacitadas a compensar as transações realizadas.

3.4.1 Características

Modelo de troca: notacional

O SET é uma extensão dos sistemas tradicionais de processamento de transações de cartões de crédito. Foi projetado como uma maneira segura de transferir números de cartões pela Internet. Portanto usa o modelo notacional.

Envolvimento da entidade emissora: *on-line*

é necessária a participação da entidade que processa as transações de cartões de crédito para o vendedor, já que apenas esta entidade está habilitada a validar a transação. Assim como no sistema tradicional de cartões de crédito, a tarefa de entidade emissora é repartida entre diversas entidades, congregadas sob a mesma marca (eg. VISA).

Quantias envolvidas: pequenos a grandes pagamentos

O custo das transações com cartões de crédito torna o sistema inadequado para a realização de micropagamentos. O limite estabelecido para cada cartão indica o teto para o valor das transações.

Hardware necessário: uso geral

O sistema não necessita do uso de nenhum tipo de maquinário dedicado ou especial.

Papéis envolvidos: comprador, vendedor e entidade controladora.

O protocolo trata a existência de um comprador, que deve ter um cartão de crédito, de um vendedor e de uma entidade controladora, que realiza as compensações para o vendedor.

Inversibilidade dos papéis: inexistente

Os papéis desempenhados no sistema são fixos, assim como em transações normais com cartões de crédito.

Privacidade: existente

O sistema não revela a identidade do comprador (número do cartão de crédito) ao vendedor e não revela o conteúdo do pedido à entidade controladora. Certificados e cifras são usados para garantir autenticação e a privacidade das mensagens trocadas, onde necessário. A entidade controladora deve ter acesso ao número do cartão de crédito do comprador, o que pode ser usado para identificá-lo.

Divisibilidade: nível 4, o sistema é notacional.

3.4.2 Requisitos

Integridade O sistema usa assinaturas digitais e certificados para proteger as mensagens e as implementações devem garantir a integridade dos dados críticos que sejam armazenados localmente.

Consistência O sistema é capaz de preservar a consistência das transações.

Atomicidade é garantida. A transação só é realmente processada pela entidade responsável pelo processamento de transações com cartões de crédito para o vendedor. Assim, se as informações chegam até ela corretamente a transação ocorre, senão a transação não acontece. As outras entidades envolvidas serão informadas e poderão verificar mais tarde se a transação foi processada.

Consistência O sistema inclui mecanismo para garantir que todos os participantes estejam de acordo quanto aos detalhes da transação, principalmente a quantia e o objeto ou serviço adquirido.

Isolamento A interferência entre transações só ocorre quando o usuário ultrapassar o limite de seu cartão, sendo que as próximas transações serão negadas por causa de transações anteriores.

Durabilidade O sistema tem um mediador, que é a entidade que processa as transações, e este é quem indica o estado do sistema. Assim, todos podem consultar o mediador e tomar conhecimento do estado atual. O sistema tradicional de processamento de transações de cartões de crédito provê mecanismos para garantir a durabilidade que devem ser usados quando do processamento através do SET.

Viabilidade econômica Como faz uso da infra-estrutura tradicional de transações com cartões de crédito, o sistema é viável economicamente apenas para transações cujos valores estejam na faixa daqueles normalmente usados em transações tradicionais com cartões de crédito.

Escalabilidade O sistema é tão escalável quanto o sistema tradicional de cartões de crédito.

Interoperabilidade O SET não prevê integração com outros sistemas de pagamento eletrônico.

Auditabilidade O uso de logs e assinaturas digitais permite verificar com bastante eficiência o funcionamento do sistema e detectar problemas, falhas ou uso indevido.

3.4.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   O usuário já deve ter um cartão de crédito, o que indica uma relação com uma empresa autorizada a emitir cartões. Esta entidade deve indicar a autoridade certificadora que emitirá os certificados de seus clientes. Já os vendedores devem estar habilitados a receber pagamentos com cartões de crédito e devem obter um certificado junto à autoridade certificadora indicada pela empresa que realiza as compensações de suas transações.

2. **Retirada**: não há.

3. **Transação**

   (a) **Autenticação**
   No inicio da transação, o usuário indica a marca de seu cartão de crédito e seu certificado e recebe o certificado do vendedor, que indica que o vendedor está habilitado a participar do sistema, e o certificado da entidade que vai realizar a compensação da transação.

   (b) **Pagamento**
   O usuário gera então uma ordem de pagamento e uma requisição de produtos ou serviços cifrada com a chave pública do vendedor. A ordem de pagamento é cifrada com a chave pública de uma entidade controladora. Estas duas mensagens são assinadas pelo processos de *dual signature*, que liga as duas informações. As assinaturas são enviadas junto com as mensagens para o vendedor. O vendedor deve repassar a ordem de pagamento à entidade controladora escolhida.

   (c) **Recibo:** não há emissão de recibo.

   (d) **Finalização**
   A entidade controladora vai receber uma ordem de pagamento e processá-la pela rede das empresas de cartões de crédito, obtendo uma resposta indicativa do crédito do usuário. Esta resposta, seja ela afirmativa ou não, será repassada ao vendedor. Se o usuário tiver

crédito, o vendedor recebe também um cupom para que possa realizar a compensação da transação.

O vendedor deve enviar uma resposta ao usuário indicando se a transação foi autorizada ou não, o que finaliza a transação.

4. **Compensação**
   Quando tiver entregue os bens ou serviços adquiridos pelo usuário, o vendedor deve pedir a compensação da transação, enviando uma requisição à entidade controladora junto com o cupom de compensação recebido anteriormente.

Observações:

1. O vendedor pode finalizar a transação assim que receber a ordem de pagamento, indicando ao comprador que a transação será autorizada mais tarde, e que o comprador deve verificar mais tarde se a autorização foi positiva.

2. O vendedor pode pedir a realização da compensação junto com a autorização da transação e, neste caso, as etapas de compensação e pagamento são condensadas numa única.

3.4.4 Aspectos de Implementação

Criptografia: as pimitivas usadas são:

Cifras simétricas: DES padrão de 56 bits.

Cifras assimétricas: RSA de 1024 bits para usuários e certificadores de usuários e RSA de 2048 bits para entidades de mais alto nível, que devem certificar chaves a serem usadas para emissão de certificados.

Assinatura digital: idem. Chaves diferentes são usadas para cifrar ou assinar mensagens.

Certificados: devem estar no formato X.509 versão 3.

Hashings: O algoritmo usado é o SHA.

Conexões de rede: 2 conexões.
Uma conexão é necessária entre o comprador e o vendedor, e uma entre o vendedor e a entidade controladora.

Formato das ordens de pagamento: As ordens de pagamento consistem de duas partes, chamadas de OI (*order information*), que contém dados que identificam os produtos serviços negociados, e PI (*payment instructions*), que autoriza a entidade controladora a efetuar o pagamento. O OI consiste do identificador da transação, identificador da marca do cartão, data e *nonces*. O PI consiste dos dados do cartão, identificação da transação, valor e de um *hashing* da descrição dos produtos/serviços.

OI e PI são assinados usando o processo de *dual signature* para garantir autenticidade e correspondêcia dos dois.

3.5 PayWord

O PayWord [21] é um sistema de micropagamentos projetado por R. Rivest e A. Shamir e é bem eficiente para a realização de pagamentos repetidos. O objetivo do sistema é reduzir o número de aplicações de cifras assimétricas, usando cifras simétricas e *hashings* (veja o apêndice A) sempre que possível.

O sistema é baseado em cadeias de *hashings* (seção A.4.1), que representam valor monetário.

3.5.1 Características

Modelo de troca: cupons
Cada usuário tem um certificado que o habilita a gerar séries de cupons (cadeias de *hashings*) que servem como forma de pagamento. As séries são específicas para um par comprador/vendedor.

Envolvimento da entidade emissora: *off-line*
A entidade emissora fornece a cada usuário um certificado que permite a confecção de séries de cupons. A emissão deste certificado e a aceitação e verificação das séries emitidas por cada usuário podem acontecer *off-line*.

Quantias envolvidas: micropagamentos
O sistema foi projetado para venda de informações na Internet, e para minimizar o custo devido ao uso de algoritmos criptográficos, principalmente algoritmos assimétricos. Assim, o nível de segurança foi reduzido.

Hardware necessário: uso geral
O sistema é todo baseado em *software*, não fazendo uso de *hardware* especial.

Papéis envolvidos: comprador, vendedor e corretor.
Os corretores gerenciam as contas dos usuários e emitem certificados aos usuários. Os vendedores devem se cadastrar com os corretores para poderem compensar os cupons recebidos.

Inversibilidade de papéis: inexistente
O sistema distingue claramente entre compradores e vendedores. O relacionamento com o corretor é diferente em cada caso.

Privacidade: inexistente
O sistema não prevê mecanismos para garantia de privacidade, sendo que o usuário é identificado em cada transação. As informações que trafegam na rede não são protegidas.

Divisibilidade Nível 4. O sistema não prevê divisibilidade, embora os autores sugiram que as cadeias possam ter um valor negociado entre comprador e vendedor.

3.5.2 Requisitos

Integridade O sistema usa assinaturas digitais para garantir a integridade dos certificados. Os cupons não usam mecanismos de proteção de integridade.

Consistência Não especificado.

Viabilidade econômica Os autores tiveram a preocupação de diminuir os custos do sistema, reduzindo o número de operações de aplicação e verificação de assinaturas digitais. Assim o protocolo tem custo compatível com a realização de micropagamentos.

Escalabilidade O sistema é bem escalável, principalmente porque as operação que envolvem a entidade controladora podem ser realizadas *off-line*.

Interoperabilidade O sistema não prevê interoperabilidade.

Auditabilidade As operações do sistema são identificadas, sendo necessário o uso de certificados para poder realizar transações.

3.5.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   O usuário deve escolher um corretor, que lhe emitirá um certificado. Este certificado dá direito ao usuário de gerar cadeias de *hashings* para a realização de pagamentos. O usuário se compromete a pagar o valor correspondente às cadeias que gerar.

2. **Retirada**
   O usuário deve gerar uma cadeia de *hashings* e assinar o último valor gerado. Esta assinatura é um comprometimento em pagar por cada um dos valores da seqüência, que são gastos na ordem contrária àquela em que foram gerados. Os comprometimentos são específicos para cada vendedor.

3. **Transação**

   (a) **Autenticação**
   O comprador deve se identificar, enviando o comprometimento e seu certificado para que o vendedor possa verificar a assinatura.

   (b) **Pagamento**
   Cada vez que o usuário for pagar algo, deve enviar um dos valores da cadeia gerada e uma indicação de sua posição na cadeia. O número de unidades monetárias em cada transferência corresponde à diferença entre a posição enviada e a última posição que o vendedor possuía. O vendedor deve verificar se o valor enviado faz parte da cadeia, gerando os *hashings* necessários até obter um valor conhecido.

   (c) **Recibo**: não há emissão de recibo.

   (d) **Finalização**: não existe etapa de finalização neste sistema.

4. **Compensação**
   O vendedor deve enviar ao corretor o comprometimento assinado pelo usuário e o último valor da cadeia que tenha recebido, indicando a posição deste valor na cadeia. O corretor irá gerar os *hashings* desta cadeia a partir do último valor recebido e verificar sua validade. Caso seja válido, o vendedor receberá o valor correspondente.

3.5.4 Aspectos de Implementação

Criptografia: as primitivas necessárias são:

Assinatura digital: é usada embora os autores não especifiquem qual algoritmo em particular.

Certificados: As chaves públicas dos usuários devem ser certificadas.

Hashings: São usados na geração da cadeia. O algoritmo não é especificado.

Conexões de rede: 1 conexão.
Apenas a comunicação entre comprador e vendedor precisa ocorrer durante cada transação.

Formato dos cupons: cadeias de hashings (ver seção A.4.1) com raiz assinada. Cada um dos valores da cadeia é um cupom.

3.6 MicroMint

Apresentado junto com o PayWord (seção 3.5), o MicroMint [21] também é um sistema para a realização de micropagamentos baseado em *hashings* (veja a seção A.4). O MicroMint tem a vantagem de não fazer uso de nenhum outro tipo de função criptográfica e permitir grande eficiência em pagamentos isolados a diferentes vendedores.

O sistema é baseado em colisões de *hashings* (ver seção A.4.2) e, se a função de *hashing* escolhida for criptograficamente forte, é difícil encontrar uma de suas colisões, o que torna o sistema seguro. Para gerar as moedas, a entidade emissora deve escolher valores aleatórios e aplicar a função nestes valores, se possível usando *hardware* dedicado, e ir armazenando os valores e o resultado da função. Quando, para um dado resultado, a entidade emissora já tiver armazenado valores suficientes, esta pode gerar um cupom válido. O fato de gerar colisões em larga escala permite à entidade emissora fazê-lo de forma econômica.

3.6.1 Características

Modelo de troca: cupons
O sistema é baseado em cupons gerados por uma entidade emissora. Os cupons correspondem a k-colisões de uma função de *hashing*.

Envolvimento da entidade emissora: *off-line*
Os cupons usados podem ser identificados e um usuário que gastar um cupom mais de uma vez pode ser identificado.

Quantias envolvidas: micropagamentos
O sistema foi projetado para venda de informações na Internet e sua segurança está em parte baseada no baixo valor unitário dos cupons, o que elimina o estímulo à fraude no sistema.

Hardware necessário: uso geral
O sistema é baseado em software e não faz uso de *hardware* específico. Os autores sugerem que a entidade emissora use *hardware* específico para poder aumentar o nível de segurança do sistema.

Papéis envolvidos: usuário e corretor.
O corretor emite cupons e os vende aos usuários que podem resgatá-los junto ao mesmo.

Inversibilidade de papéis: existente
Este sistema permite que qualquer usuário receba cupons, embora a entidade emissora possa limitar a capacidade dos usuários de trocarem cupons entre si, já que a troca indiscriminada de cupons entre os usuários pode dificultar a identificação dos usuários que cometerem fraudes.

Privacidade: inexistente
A entidade emissora é capaz de saber qual usuário comprou um determinado cupom, embora a troca indiscriminada de cupons entre os usuários possa aumentar o grau de privacidade do sistema. Nenhum tipo de proteção para as transmissões de cupons pela rede é especificado.

Divisibilidade: nível 4.
O sistema não prevê divisibilidade e os autores sugerem o uso de cupons cujo valor seja 1 centavo.

3.6.2 Requisitos

Integridade Não são especificados mecanismos de integridade.

Consistência Não especificado.

Viabilidade econômica A viabilidade econômica do sistema está baseada na economia de escala, ou seja, se a entidade emissora gerar muitos cupons, o sistema pode ser viável, já que o custo por cupom diminui.

Escalabilidade O número de cupons em circulação depende da capacidade da entidade emissora de gerar cupons a tempo e de gerenciar estes cupons. Assim, dados os custos e a tecnologia disponível, existe um limite na quantidade de cupons ou usuários do sistema.

Interoperabilidade O sistema não prevê interoperabilidade.

Auditabilidade Os cupons são identificados, o que permite à entidade emissora identificar usuários que estejam tentando fraudar o sistema.

3.6.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   O usuário deve entrar em contato com um corretor, que lhe venderá cupons, e negociar a forma de pagamento a ser usada.

2. **Retirada**
   Fazendo uso do sistema negociado na fase de estabelecimento de relacionamento, o usuário paga ao corretor, que lhe envia seus cupons já prontos para uso. Os cupons podem ser reconhecidos pelo corretor, que consegue verificar se o usuário está usando cada cupom mais de uma vez e lhe impor sanções.

3. **Transação**

   (a) **Autenticação**: não há autenticação.

   (b) **Pagamento**
   Os cupons são enviados em claro pela rede. Se for necessário cifrar os cupons, os usuários devem fazer uso de métodos externos ao sistema. Ao receber os cupons, o vendedor verifica sua validade calculando o resultado da função de *hashing* para os valores que o compõem.

   (c) **Recibo**: não há emissão de recibo.

   (d) **Finalização**: não existe etapa de finalização neste sistema.

4. **Compensação**
   O vendedor envia os cupons que recebeu ao corretor, que os reembolsará. O corretor irá verificar se os cupons não foram gastos duas vezes para poder tomar as providências cabíveis, como expulsar do sistema o comprador ou vendedor que estiver cometendo fraude. O depósito dos cupons pode acontecer *off-line*.

3.6.4 Aspectos de Implementação

Criptografia: a primitiva necessária é:

Hashings: Este sistema usa *hashings* como o único tipo de algoritmo criptográfico para fins de eficiência.

Conexões de rede: 1 conexão.
Apenas a comunicação entre comprador e vendedor precisa ocorrer durante cada transação.

Formato dos cupons: colisões de uma função de espalhamento (*hashing*, ver seção A.4). Os autores consideram viável o uso de 4-colisões, ou seja, quatro valores que a função mapeie sobre o mesmo valor. Os cupons tem valor único fixado pelo corretor.

3.7 CAFE

O projeto CAFE [3] foi um projeto europeu que tinha como objetivo a geração de tecnologia na área de permissões de usuários e controle de acesso. Seu resultado mais importante foi um dos mais avançados sistemas de pagamento eletrônico existentes hoje. Trata-se de um sistema *off-line*, anônimo e seguro.

3.7.1 Características

Modelo de troca: híbrido
Os cupons deste sistema são chamados de *slips*, sendo que o usuário determina o valor de cada *slip* quando da transação. Os *smart cards* contém contadores que indicam o valor armazenado no dispositivo. O valor total dos *slips* não pode ser superior a este valor armazenado.

Envolvimento da entidade emissora: *off-line*
No momento da transação, apenas o pagador e recebedor precisam se comunicar.

Quantias envolvidas: pequenos pagamentos
O sistema foi projetado para substituir a carteira de dinheiro tradicional, sendo adequado para valores pequenos a médios.

Hardware necessário: específico.
Parte da segurança do sistema depende de dispositivos *tamper-proof*, chamados de carteiras eletrônicas.

O CAFE permite o uso de dois tipos de dispositivos: *smart cards* e carteiras eletrônicas. Os *smart cards* são cartões plásticos semelhantes a cartões de crédito que têm um pequeno processador embutido, enquanto as carteiras eletrônicas são aparelhos mais sofisticados que possuem pequenos teclados e visores de cristal líquido. As carteiras usadas no CAFE são capazes de transferir ordens de pagamentos para os *smart cards*.

O CAFE funciona com o uso de observadores, que são dispositivos em que o banco confia e que ficam dentro da carteira ou *smart card* do usuário. O observador impede que o usuário faça algo que seja contrário aos interesses do banco, enquanto a carteira verifica se o observador está fazendo algo que seja contrário aos interesses do usuário. O observador é responsável, por exemplo, pelo controle do saldo do dispositivo.

Papéis envolvidos: pagador, recebedor e banco.
Os pagadores usam seus dispositivos para armazenar as ordens de pagamento em branco e para realizar pagamentos. Os recebedores possuem dispositivos capazes de receber as ordens

de pagamento, armazená-las e depois depositá-las em um banco. Os bancos assinam as ordens de pagamento emitidas pelos usuários e realizam a compensação dos pagamentos efetuados através do sistema.

Inversibilidade dos papéis: papéis variáveis.
Os usuários do sistema podem tanto atuar como pagadores quanto como recebedores. O único papel fixo é o papel do banco, ou entidade emissora.

Privacidade: existente
O sistema garante que o banco não será capaz de identificar as transações de um usuário se este respeitar as regras do sistema. Os dispositivos *tamper-proof* tornam a fraude mais difícil.

Divisibilidade: nível 1.
O usuário é capaz de determinar o valor dos *slips*.

3.7.2 Requisitos

Integridade O banco assina todos os *slips*, o que garante a integridade destes. O uso de dispositivos *tamper-proof* ajuda a manter a integridade do sistema.

Consistência Um mecanismo de recuperação de falhas tem o dever de garantir a consistência.

Atomicidade Os protocolos de comunicação garantem que as transações são atômicas.

Consistência O recebedor e o pagador negociam os parâmetros, garantindo a consistência de cada transação.

Isolamento As transações só interferem em outras se o usuário tentar usar o *slip* duas vezes. Neste caso a segunda transação não é válida.

Durabilidade O sistema implementa um mecanismo para recuperação de moedas perdidas.

Viabilidade econômica O sistema evita a necessidade de uma conexão *on-line* durante a transação, o que reduz os custos. Apesar disto, não é adequado para microtransações por ser bastante complexo e necessitar de *hardware* especial.

Escalabilidade O sistema é escalável já que os servidores centrais podem atuar *off-line*. Apenas a carga dos dispositivos deve ser feita *on-line*.

Interoperabilidade O sistema prevê a existência de vários bancos e pode funcionar com moedas de diferentes países.

Auditabilidade Os depósitos são registrados e o sistema é capaz de detectar múltiplos gastos da mesma moeda.

3.7.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   O usuário deve manter uma conta corrente num dos bancos que participa do sistema e obter deste banco um observador para sua carteira ou um *smart card*.

2. **Retirada**
   O usuário deve recarregar seu dispositivo junto a um caixa eletrônico especialmente adaptado ao sistema. O dispositivo do usuário entrará em contato com o seu banco através deste caixa eletrônico e irá gerar as ordens de pagamento em branco, que serão assinadas pelo banco. O dispositivo então armazenará estas assinaturas e o mínimo de informação necessária para gerar as ordens de pagamento novamente quando estas forem preenchidas. O dispositivo indica ao banco o valor total máximo que estas ordens de pagamento podem atingir, e este valor é adicionado ao contador de saldo do observador e retirado da conta do usuário .

3. **Transação**

   (a) **Autenticação**: Apenas o recebedor deve ser identificado.

   (b) **Pagamento**
   O pagador envia uma ordem de pagamento em branco ao recebedor, que verifica sua validade através da assinatura do banco. Depois o pagador preenche a ordem de pagamento. O pagador envia a ordem de pagamento preenchida ao recebedor.

   (c) **Recibo**: o sistema não prevê a emissão de recibo.

   (d) **Finalização**
   O recebedor verifica a se ordem de pagamento está de acordo com as informações recebidas anteriormente, e envia uma confirmação.

4. **Compensação**
   Após ter recebido a ordem de pagamento, o recebedor pode, a qualquer momento, enviar esta ordem de pagamento ao seu banco, que enviará a ordem de pagamento ao banco do pagador que verificará a validade da ordem de pagamento e se esta já não havia sido usada e então realizará a transferência do valor correto.

3.7.4 Aspectos de Implementação

Criptografia: é necessário o uso de:

Assinatura digital: O sistema usa assinaturas de schnorr, que requerem processamento menos intensivo que os métodos tradicionais.

Conexões de rede: 1 conexão.
Este sistema foi não desenvolvido para a realização de compras numa rede, e presume que os dispositivos do comprador e do vendedor se comunicam por contato direto ou infra-vermelho.

Formato das ordens de pagamento: Os *slips* em branco consistem de:

- PK_{Blind}: uma chave pública gerada a partir da chave secreta do usuário, mas que não permite sua identificação.
- Duas chaves públicas auxiliares, PK_1 e PK_2, que são desconhecidas do banco.

O *slip* preenchido consiste de:

- As chaves públicas PK_{Blind} e PK_i, onde i indica se o *slip* está sendo usado pela primeira ou segunda vez.
- Identificação do vendedor
- Data
- Valor

- Valor aletório para garantir que a mensagem é única.

Este *slip* é assinado pelo comprador usando sua chave secreta e um string aleatório, o que impede que o usuário seja identificado.

3.8 O E-cash da Digicash

O E-CASH [9] da DIGICASH é um dos mais conhecidos sistemas de pagamento na Internet. Este sistema permite a realização de transações na qual o pagador permanece anônimo perante o recebedor e a entidade emissora. Isto se dá pelo uso de *blind signatures* (veja a secao A.3.1) quando a entidade emissora valida os cupons gerados pelo usuário.

Este sistema já vem sendo utilizado na Internet por bancos dos Estados Unidos, Alemanha e Finlândia. Até o momento da redação deste documento, a DIGICASH não havia publicado a especificação do sistema, e a análise abaixo baseou-se em informações extra-oficiais.

3.8.1 Características

Modelo de troca: cupons
Os cupons deste sistema são chamados de moedas, sendo numerados e com data de validade. O valor do cupom é indicado pela chave usada pelo banco para assiná-lo, já que o banco não terá acesso aos dados que está assinado por causa do processo de *blind signatures*.

Envolvimento da entidade emissora: *on-line*
O banco que emite cada moeda deve ser contatado para confirmar a validade da mesma.

Quantias envolvidas: pequenos pagamentos
O sistema foi projetado para uso na Internet, e as moedas devem ser armazenadas nos computadores dos usuários . Apesar do sistema de pagamento fazer uso de criptografia forte o suficiente para permitir a realização de pagamentos de centenas de dólares ou mais, os computadores nos quais este deve ser usado não apresentam, em geral, segurança suficiente para tanto.

Hardware necessário: uso geral.
O sistema não faz uso de *hardware* especial como *smart cards* ou outros mecanismos deste tipo, sendo passível de implementação em qualquer computador.

Papéis envolvidos: usuário e banco.
Os usuários podem comprar e resgatar cupons emitidos pelo banco.

Inversibilidade dos papéis: papéis variáveis.
Os usuários do sistema podem tanto atuar como pagadores quanto como recebedores. O único papel fixo é o papel do banco, ou entidade emissora.

Privacidade: existente
O sistema está baseado em *blind signatures* (veja A.3.1) e garante o anonimato do pagador, embora este deva se identificar em caso de disputa. O banco e o recebedor são identificados. O sistema não especifica que as moedas ou pedidos devam ser enviados criptografados pela rede, o que permite que um observador possa obter algumas informações sobre as transações.

Divisibilidade Nível 2.
Para dividir uma moeda, é necessário trocá-la no banco, realizando um depósito e retirando as moedas de valor menor.

3.8.2 Requisitos

Integridade A integridade das moedas é garantida pelo uso de assinaturas[2].

Consistência Não é tratada de maneira explicita.

Viabilidade econômica A necessidade de contato com o banco durante a transação e o uso de cifras assimétricas para o processo de assinatura tornam o sistema inviável para micropagamentos. Apesar disto, o sistema é perfeitamente adequado à realização de pequenas ou médias transações.

Escalabilidade O sistema prevê que os usuários que quiserem realizar transações devem ter contas no mesmo banco. Assim, os servidores dos bancos são os pontos críticos do sistema. A lista de moedas usadas pode ser outro problema se crescer muito.

Interoperabilidade O sistema não prevê interoperabilidade, sendo que cada banco opera independentemente, emitindo e recebendo apenas suas próprias moedas.

Auditabilidade é possível ao usuário provar sua participação em transações, sacrificando seu anonimato. O banco mantém registros das moedas depositadas e pode identificar o usuário que as depositou ou trocou.

3.8.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   O usuário deve manter uma conta corrente num dos bancos que participa do sistema e requisitar a este banco a instalação de uma conta E-CASH. Desta conta E-CASH, o usuário poderá realizar retiradas e depósitos de E-CASH. Além disto, o usuário precisa receber e instalar o *software* de carteira eletrônica em seu computador.

2. **Retirada**
   O usuário deve gerar as moedas eletrônicas e enviá-las ao banco para que este as valide pela aplicação de uma *blind signature*. O banco recebe as moedas e uma indicação do valor que o usuário deseja associar a cada uma delas. O banco aplica a assinatura com a chave correspondente ao valor solicitado e debita este valor da conta do usuário. A seguir o banco devolve as moedas ao usuário, que retira o *blinding factor* e já pode utilizá-las.

3. **Transação**

   (a) **Autenticação**: não há

   (b) **Pagamento:** O pagador deve enviar os cupons ao recebedor, que deve entrar em contato com o banco que os emitiu. O recebedor envia os cupons ao banco para verificação. O recebedor deve proceder então à etapa de depósito dos cupons.

   (c) **Recibo**: não há

   (d) **Finalização**: não existe etapa de finalização neste sistema.

4. **Compensação**
   Após o banco ter confirmado a validade dos cupons, o recebedor tem duas alternativas: depositar os cupons em sua conta ou gerar novos cupons no mesmo valor total que serão validados pelo banco.

[2] Algum esquema com redundância deve ser usado para garantir que as moedas assinadas pelo banco com uma chave correspondente a um valor baixo sejam verificadas por uma chave de valor alto e sejam válidas.

3.8.4 Aspectos de Implementação

Criptografia: as pimitivas necessárias são:

Cifra simétrica: Triplo-DES, usando em conjunto com a cifra assimétrica para tornar o processo mais eficiente, usando o modelo do envelope seguro.

Cifra assimétrica: RSA.

Assinatura digital: RSA, usado para assinar *hashings* das mensagens.

Hashing: SHA.

Conexões de rede: duas conexões.
Uma conexão é necessária entre pagador e recebedor, e uma entre o recebedor e o banco para verificação da validade das moedas.

Formato dos cupons: Os cupons usados consistem de um número de série, uma data de validade e da assinatura do banco. O número de série tem um formato especial para permitir a identificação dos números válidos.

3.9 Internet Keyed Protocol

A divisão de pesquisas da IBM desenvolveu o iKP [10] para ser um sistema adequado à realização de transações pela Internet usando contas bancárias ou cartões de crédito. No fundo, trata-se de um sistema adequado para a transmissão de números de contas pela Internet.

O sistema faz uso de criptografia forte, com cifras simétricas e assinaturas digitais e consiste em três níveis distintos. No primeiro nível, apenas as entidades controladoras possuem um certificado vinculando sua identidade a uma chave pública. No segundo nível, o vendedores já devem ter um tal certificado, e consequentemente, um par de chaves para uso em assinaturas. No terceiro nível, todos os envolvidos, inclusive os compradores, devem ter cada um seu par de chaves e o certificado correspondente. Esta hierarquia permite a implantação gradual do sistema, com um aumento da segurança a medida que a infra-estrutura se torna disponível.

3.9.1 Características

Modelo de troca: notacional
O iKP é baseado nos sistemas tradicionais de processamento de transações de cartões de crédito ou débito. Foi projetado como uma maneira segura de transferir números de cartões ou contas bancárias pela Internet. Portanto usa o modelo notacional.

Envolvimento da entidade emissora: *on-line*
é necessária a participação da entidade que processa as transações de cartões de crédito ou banco responsável pela conta, já que apenas esta entidade está habilitada a validar a transação. Esta entidade fará a interface entre o sistema iKP e o sistema bancário tradicional, que gerencia as contas usadas nas transações.

Quantias envolvidas: pequenos a grandes pagamentos
O custo das transações com cartões de crédito torna o sistema inadequado para a realização de micropagamentos. O limite estabelecido para cada cartão indica o teto para o valor das transações. Foi proposta uma variação do iKP para lidar com micropagamentos.

Hardware necessário: uso geral
O sistema não necessita do uso de nenhum tipo de maquinário dedicado ou especial.

Papéis envolvidos: pagador, recebedor e entidade controladora.
A entidade controladora é a entidade habilitada a processar pagamentos realizados com cartões de crédito.

Inversibilidade dos papéis: inexistente
Os papéis desempenhados no sistema são fixos, assim como em transações normais com cartões de crédito. Uma entidade cadastrada como vendedor não pode participar como comprador, a não ser que se cadastre como tal. Um sistema de nível 3, ou 3KP, poderia permitir inversibilidade de papéis para transações com números de contas bancárias.

Privacidade: existente
O sistema protege a identidade do usuário (número do cartão de crédito ou conta) do vendedor. Além disso, o conteúdo do pedido não é informado à entidade emissora. O uso extensivo de criptografia e certificados garante a segurança e privacidade das mensagens trocadas. O sistema não permite transações totalmente anônimas por fazer uso de cartões de crédito ou contas bancárias.

Divisibilidade: nível 4, o sistema é notacional.

3.9.2 Requisitos

Integridade O sistema usa assinaturas digitais e certificados para proteger as mensagens e as implementações devem garantir a integridade dos dados críticos que sejam armazenados localmente. A mensagem inicial do protocolo não é cifrada, o que permitiria que intrusos alterassem a proposta de negócio que o vendedor manda ao comprador. Entretanto, nos níveis 2 e 3 do protocolo, o vendedor deve ter um par de chaves e um certificado, o que permitiria que esta primeira mensagem já fosse cifrada.

Consistência O sistema é capaz de preservar a consistência das transações.

- **Atomicidade** é garantida. A transação só é realmente processada pela entidade responsável pelo processamento de transações com cartões de crédito para o vendedor, assim, se as informações chegam até ela corretamente a transação ocorre, senão a transação não acontece. As outras entidades envolvidas serão informadas. As implementações deveriam permitir que os participantes verifiquem mais tarde se a transação for processada.
- **Consistência** O sistema inclui um mecanismo para garantir que todos os participantes estejam de acordo com os detalhes da transação: quantia e objeto ou serviço adquirido.
- **Isolamento** A interferência entre transações só ocorre quando o usuário ultrapassar o limite de seu cartão ou saldo em conta, sendo que as próximas transações serão negadas por causa de transações que já ocorreram.
- **Durabilidade** O sistema tem um mediador, que é a entidade que processa as transações, e este é quem indica o estado do sistema. Assim, todos devem poder consultar o mediador e tomar conhecimento do estado atual. O sistema tradicional de processamento de transações de cartões de crédito provê mecanismos para garantir a durabilidade que devem ser usados quando do processamento através do iKP.

Viabilidade econômica O sistema é viável economicamente para transações cujos valores estão na faixa daqueles normalmente usados em transações tradicionais com cartões de crédito ou cheques, já que deve usar os canais de processamento já implantados para estes instrumentos.

Escalabilidade O sistema é tão escalável quanto o sistema tradicional de cartões de crédito. Podem participar vários bancos ou companhias de cartões de crédito, fazendo uso de uma infra-estrutura de certificação comum.

Interoperabilidade O iKP não prevê integração com outros sistemas de pagamento eletrônico. O sistema poderia ser usado como ponto de partida para alguns sistemas de micropagamentos, que necessitam da realização de macropagamentos para que o usuário use o sistema.

Auditabilidade O uso de logs e assinaturas digitais permite verificar com bastante eficiência o funciomento do sistema e detectar problemas, falhas ou uso indevido. O sistema foi projetado de maneira que, em seu nível 3, garanta registros de transações que não permitam disputas.

3.9.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   O usuário deve escolher uma das entidades controladoras participantes do sistema e estabelecer um relacionamento comercial com esta. Os vendedores devem se habilitar a receber através do sistema e os compradores devem se habilitar à realização de pagamentos. Caso o sistema esteja operando nos níveis 2 ou 3, os usuários podem ter de gerar um par de chaves e obter um certificado para a chave pública. Os usuários recebem uma cópia da chave mestra da hierarquia de certificação, que é usada para verificar a validade dos certificados recebidos. Nesta etapa o usuário deve adquirir o *software* necessário ao uso do sistema. O iKP pressupõe que o usuário já fazia uso do sistema de pagamentos tradicional usado como base para o sistema, como por exemplo o sistema de cartões de crédito ou de contas bancárias.
2. **Retirada**: não há.
3. **Transação**
   (a) **Autenticação**
   Nos níveis mais avançados de funcionamento, o usuário deve enviar seu certificado ao outro participante da transação, que verificará sua validade. No nível 1, os participantes trocam apenas os dados necessários à inicialização do sistema, como uma identificação de transação e uma fatura. Nesta fase, o vendedor informa ao comprador a entidade controladora escolhida para processar a transação e envia o certificado desta entidade controladora.
   (b) **Pagamento**
   O usuário recebe a fatura, verifica sua validade e gera uma ordem de pagamento, que contém o valor, um *hashing* da descrição dos produtos ou serviços comprados, o número de sua conta ou cartão de crédito e, opcionalmente, uma senha. Esta fatura é cifrada com a chave pública da entidade controladora escolhida pelo vendedor.
   (c) **Recibo**: não há emissão de recibo.
   (d) **Finalização**
   Após ter recebido a ordem de pagamento, o vendedor entra em contato com a entidade controladora para verificar a validade da transação. A entidade controladora informa se a transação foi válida ou não e o vendedor passa esta informação ao comprador.
4. **Compensação**
   A entidade controladora realiza a compensação automaticamente quando o vendedor valida a transação. Assim sendo, o vendedor não precisa tomar nenhuma atitude para que a transação seja compensada após ter sido informado de que a transação foi validada.

3.9.4 Aspectos de Implementação

Criptografia: são necessários:

Cifra assimétrica: RSA.

Assinatura digital: usa as mesmas chaves que a cifra assimétrica.

Certificados: do tipo PKCS.

Hashing: MD5.

Conexões de rede: duas conexões.
Uma conexão é necessária entre pagador e recebedor, e uma entre o recebedor e o banco para verificação da validade do pagamento e compensação.

Formato das ordens de pagamento: Cada ordem de pagamento contém:

- valor
- *hashing* de informações de indentificação que são do conhecimento do comprador e do vendedor.
- número da conta do pagador
- número aleatório escolhido pelo comprador
- opcionalmente a senha da conta do comprador

Estas informações são cifradas com a chave pública da entidade controladora.

3.10 Millicent

O Millicent [13] é um sistema para a realização de micropagamentos projetado pela Digital Equipment Corporation. é um sistema otimizado para a realização de compras repetidas de pequenos valores. O sistema pressupõe a existência de um ou mais corretores, que vendem cupons em nome das entidades que estão vendendo produtos ou serviços. Estes corretores tem a função de agrupar as diversas compras dos usuários, sejam em um ou mais vendedores, de tal modo a tornar viável o uso de sistemas para a realização de macropagamentos.

Os cupons usados são específicos para cada vendedor, que deve emitir os cupons e vendê-los ao corretor, ou autorizar o corretor a emitir cupons em seu nome. Os cupons tem um valor fixo, mas o sistema permite que o vendedor devolva troco caso o valor do cupom seja maior que o valor do produto ou serviço.

3.10.1 Características

Modelo de troca: cupons
Cada vendedor emite cupons que tem um determinado valor monetário. O usuário compra estes cupons e pode então realizar transações com este vendedor.

Envolvimento da entidade controladora: *off-line*
Os cupons são emitidos por ou em nome de um vendedor, sendo que este é capaz de identificar e validar seus próprios cupons. Assim, a entidade controladora, ou corretor, não precisa ser contactada durante a transação.

Quantias envolvidas: micropagamentos
O sistema foi projetado para venda de informações na Internet, e para minimizar o custo apresentado pelo uso de algoritmos criptográficos. Assim, o nível de segurança foi reduzido e o sistema é adequado apenas para transferências de valores entre US$ 0,001 e US$ 5,00.

Hardware necessário: uso geral
O sistema é todo baseado em software, não fazendo uso de hardware especial.

Papéis envolvidos: comprador, vendedor e corretor.
O comprador adquire cupons junto ao corretor e pode então realizar transações com o vendedor.

Inversibilidade de papéis: inexistente
O sistema distingue claramente entre compradores e vendedores. O vendedor deve emitir cupons e ter um relacionamento com um corretor que se encarrega de vender os cupons aos compradores.

Privacidade: existente
O sistema prevê um mecanismo para proteger as informações e cupons em transito pela rede. Se for usado um sistema anônimo para compra de cupons, a privacidade do comprador é protegida. O vendedor é sempre identificado, já que os cupons lhe são específicos.

Divisibilidade nível 3.
Não há necessidade de trocar cupons por outros de menor valor já que o sistema prevê a devolução de troco.

3.10.2 Requisitos

Integridade O sistema usa *hashings* para garantir a integridade dos cupons.

Consistência O sistema não possui um mecanismo que garanta sua consistência. Como as transações envolvem apenas duas entidades, o questionamento sobre o estado do sistema é bastante eficaz.

Viabilidade econômica Os autores tiveram a preocupação em diminuir os custos do sistema, reduzindo o número de operações criptográficas e usando apenas *hashings*. Assim o protocolo tem custo compatível com a realização de micropagamentos. Testes divulgados com implementações deste sistema confirmam sua viabilidade.

Escalabilidade O sistema é bem escalável, sendo que os testes mostram que o principal problema de desempenho pode ser a realização das conexões de rede.

Interoperabilidade O sistema não prevê interoperabilidade.

Auditabilidade Cada vendedor controla seus próprios cupons, sendo capaz de identificar fraudes ou outros problemas no uso do sistema.

3.10.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   O usuário deve escolher um corretor de quem comprará os cupons válidos para um determinado vendedor. O corretor deve ser habilitado pelo vendedor em questão. O estabelecimento do relacionamento consiste basicamente em definir que tipo de sistema de macropagamentos será usado. O usuário deve então comprar deste corretor um cupom válido para trocas com o próprio corretor. Este cupom tem um valor monetário e será gasto quando da compra de cupons para uso com os vendedores.

2. **Retirada**
   O usuário envia o cupom do corretor e indica o vendedor e o valor do cupom desejado para este vendedor. O corretor irá obter o cupom do vendedor (ele pode já ter comprado do vendedor ou então estar habilitado a gerar cupons) no valor correto e devolver ao usuário o cupom do vendedor e um cupom com o troco, se houver.

3. **Transação**

   (a) **Autenticação**: o pagador só se identifica se quiser, e por meios fora do escopo do sistema, enquanto o vendedor é sempre identificado, já que os cupons lhe são específicos.

   (b) **Pagamento**
   O usuário envia o cupom e uma requisição, indicando o produto ou serviço desejado, pela rede. O sistema prevê o uso de conexões seguras com dois níveis: uso de cifras simétricas, cuja chave é informada ao usuário pelo corretor, ou uso de um esquema simplificado de assinaturas, baseado em *hashing* usando como segredo a chave já citada. Os cupons podem também ser enviados pela rede sem nenhum tipo de proteção.

   (c) **Recibo**: O sistema não faz uso de recibos.

   (d) **Finalização**
   O vendedor deve devolver o troco ao usuário. O troco é enviado pela rede com o mesmo nível de segurança que o pagamento, consistindo de um cupom comum que pode ser usado em outras compras.

4. **Compensação** : não há necessidade de etapa de depósito, já que o vendedor é responsável pela geração dos seus próprios cupons. O vendedor e o corretor devem concordar num método para realização do acerto referente aos cupons vendidos.

3.10.4 Aspectos de Implementação

Criptografia: o sistema faz uso de:

Hashing: MD5, é o único tipo de algoritmo criptográfico usado, o que permite aumentar a eficiência do sistema.

Conexões de rede: uma conexão.
Apenas o vendedor e o comprador precisam se comunicar durante a transação.

Formato dos cupons: cada cupom consiste dos seguintes campos:

- indentificação do vendedor.
- valor
- identificador do cupom
- identificador do comprador que não precisa ter ligação com a identidade real do comprador, mas é necessário para permitir a transmissão segura dos cupons. Este identificador é usado para gerar as chaves que permitem a transmissão segura dos cupons pela rede.
- data de validade
- informações extras opcionais
- certificado de autenticidade, que é gerado como um *hashing* do cupom concatenado com um segredo escolhido pelo vendedor.

3.11 NetBill

O NetBill [14] foi desenvolvido na Carnegie Mellon University e é um esquema para venda de informações ou programas pela Internet. é um protocolo completo, que inclui uma fase de negociação de preços e a entrega dos bens é garantida. Neste sistema, um servidor central é responsável pelas contas dos usuários, e pode creditar estas contas a partir de contas correntes em bancos conveniados ou a partir de cartões de crédito. Neste sistema existem os compradores, os vendedores e o servidor central (entidade controladora), cada um com seu papel bem definido.

O sistema faz uso de um mecanismo de autenticação chamado *Public Key Kerberos*, que é uma variação do sistema *Kerberos* (seção A.5.2) onde não há necessidade de um servidor *Kerberos* para autenticar os usuários. Em compensação é necessária uma infra-estrutura para emissão de certificados e todos os participantes devem ter um par de chaves para uma cifra assimétrica.

3.11.1 Características

Modelo de troca: notacional
O sistema trabalha com contas especiais gerenciadas por uma entidade central, sendo que as transferências são feitas entre estas contas.

Envolvimento da entidade emissora: *on-line*
Para que as transferências possam acontecer, a entidade que gerencia as contas deve ser acionada. O vendedor repassa uma ordem de pagamento ao banco que valida os dados e realiza a transferência entre as contas.

Quantias envolvidas: micro e pequenos pagamentos
O sistemas foi projetado para venda de informações *on-line*, o que envolve tipicamente quantias na faixa dos micropagamentos. Pelo nível de segurança apresentado, acreditamos que o sistema seja capaz de lidar também com pequenos pagamentos.

Hardware necessário: uso geral
O sistema não faz uso de *hardware* específico e pode ser implementado em qualquer tipo de computador.

Papéis envolvidos: comprador, vendedor e entidade controladora.
A entidade controladora age como um mediador em caso de disputa entre comprador e vendedor.

Inversibilidade de papéis: inexistente
O sistema faz uma clara distinção quanto a vendedores e compradores e o *software* usado deve prover funções bem distintas. Para participar do sistema nos dois papéis, um usuário deve se cadastrar duas vezes.

Privacidade: existente
O uso de criptografia em todas as mensagens e o sistema de autenticação permitem que as mensagens e informações sejam mantidas secretas quando necessário.

Divisibilidade: nível 4, o sistema é notacional.

3.11.2 Requisitos

Integridade Assinaturas digitais e *hashings* são usados para garantir a integridade das mensagens.

Consistência O mediador tenta garantir a consistência do sistema. Em caso de dúvida ou disputa, o mediador resolve a questão.

Atomicidade Depois que o comprador envia a ordem de pagamento, não há mais possibilidade de reverter a transação. Até este momento o comprador pode cancelar a transação.

Consistência Após uma fase de negociação, o vendedor faz uma proposta ao comprador que deve enviar uma ordem de pagamento no valor correto. Caso contrário o vendedor pode cancelar a transação.

Isolamento Desde que o comprador tenha crédito, as transações são independentes. Se o comprador ultrapassar o seu saldo, novas transações passam a ser negadas em função de transações anteriores.

Durabilidade Garantida pela entidade controladora.

Viabilidade econômica O custo de operação do sistema permite que sejam realizados micro ou pequenos pagamentos. Apesar disto, este é um dos mais caros sistemas de micropagamentos encontrado por usar bastante as cifras assimétricas.

Escalabilidade O sistema tem como gargalo o servidor da entidade controladora, embora sejam possíveis extensões para permitir a coexistência de diversas destas entidades.

Interoperabilidade O sistema não prevê interoperabilidade.

Auditabilidade Todas as transações passam pelo servidor central que pode prover mecanismos de *logs*, extratos etc. Além disto todas as transações são autenticadas com base em assinaturas digitais ou *hashings*.

3.11.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   O usuário que quiser fazer uso do NetBill deve se cadastrar com o servidor central e obter deste um número de conta. é necessário obter também um par de chaves e um certificado para a chave pública. Neste momento o usuário precisa também obter o *software* necessário ao uso do sistema.

2. **Retirada**: não há.

3. **Transação**

   (a) **Autenticação**
   Antes de poder participar de transações, o usuário deve se autenticar, usando o *public key Kerberos* com o vendedor e o servidor central. O vendedor também deve se autenticar com o servidor central. Em outras palavras, para iniciar a transação, o comprador e o vendedor já devem ter obtido seus tíquetes.

   (b) **Pagamento**
   A transação se inicia quando o comprador requisita um orçamento e o vendedor indica o preço do item escolhido. Tendo recebido o preço, o comprador envia uma requisição de compra e o vendedor devolve os bens negociados cifrados com uma chave de seção. O comprador verifica se os bens foram recebidos íntegros, e assina e envia uma ordem de pagamento. A partir deste momento o comprador não pode mais cancelar a transação. O vendedor recebe a ordem de pagamento e a envia ao servidor central juntamente com a chave de seção usada para cifrar os bens enviados ao comprador.

(c) **Recibo**
O recibo é gerado pelo servidor central quando este realiza a transferência do valor da transação entre as contas do comprador e do vendedor. O recibo contém a chave para decifrar os bens que o comprador recebeu.

(d) **Finalização**
O servidor central informa ao vendedor se a transação foi bem sucedida e, caso afirmativo, envia também o recibo, que o vendedor deve repassar ao comprador. O servidor central mantém um *log* dos recibos para verificação em caso de disputa.

4. **Compensação**
A compensação é feita assim que o servidor central recebe a ordem de pagamento.

Observações:

1. Este método pode ser adaptado para venda de bens físicos se for retirada a etapa de envio dos bens criptografados.

2. Se o vendedor não enviar o recibo ao comprador, este último pode requisitar ao servidor central uma cópia do recibo, bastando indicar a identificação da transação.

3.11.4 Aspectos de Implementação

Criptografia: o sistema necessita dos seguintes itens:

Cifra simétrica: DES.

Cifra assimétrica: RSA.

Certificados: formato não especificado.

Hashing: SHA.

Conexões de rede: duas conexões.
O comprador deve enviar a ordem de pagamento ao vendedor, que irá repassá-la à entidade controladora para compensação.

Formato das ordens de pagamento: As ordens de pagamento consistem de duas partes: a primeira contendo a identificação do comprador, identificação e preco das mercadorias, identidade do vendedor e um código de verificação dos produtos cifrados pode ser lida pelo vendedor e pela entidade controladora. A Segunda, contendo um tíquete, que autentica o comprador, o número de sua conta e um campo de informações extras, só pode ser lido pela entidade controladora.

3.12 NetCash

O grupo de comércio eletrônico da USC desenvolveu dois sistemas de pagamento: o NetCash [11] e o NetCheque (seção 3.13). O primeiro funciona por cupons e o segundo é um sistema notacional. O NetCheque é usado principalmente como método de compensação para o NetCash.

O NetCash é um sistema de cupons com anonimato restrito, o que significa que é possível rastrear os pagamentos de um usuário. O principal mecanismo usado para melhorar o nível de privacidade do comprador é a troca de cupons, que pode ser realizada de forma anônima. Assim, um usuário pode tentar trocar seus cupons para tornar mais difícil a identificação de seus gastos. Claramente, este processo não garante anonimato total.

3.12.1 Características

Modelo de troca: cupons
Os cupons deste sistema são chamados de moedas, sendo numerados e contendo uma identificação da entidade emissora, assim como a data de validade e seu valor.

Envolvimento da entidade emissora: *on-line*
O banco que emite cada moeda deve ser contatado para confirmar a validade da moeda. Os bancos devem manter registros dos números das moedas em circulação.

Quantias envolvidas: pequenos pagamentos
Os cupons usados no sistema são assinados pela entidade emissora, o que garante certa segurança. O uso de assinaturas digitais em cada moeda pode inviabilizar o seu uso para micropagamentos.

Hardware necessário: uso geral
O sistema não faz uso de *hardware* especial como *smart cards* ou outros mecanismos deste tipo, sendo passível de implementação em qualquer tipo de computador.

Papéis envolvidos: comprador, vendedor e servidor de moeda.
Os usuários podem assumir tanto o papel de comprador quanto o papel de vendedor, o que permite que quaisquer dois usuários transfiram valores entre si. Podem existir diversos servidores de moeda, que formam uma rede de compensações. Os usuários pode trabalhar com qualquer servidor de moeda do sistema.

Inversibilidade dos papéis: papéis variáveis.
Os usuários do sistema podem tanto atuar como pagadores quanto como recebedores. O único papel fixo é o papel do banco, ou entidade emissora.

Privacidade: existente
O anonimato oferecido pelo sistema é parcial, já que o banco seria capaz de identificar as transações realizadas por determinados usuários. Os autores indicam que isto seriam anti-econômico e que a existência de vários bancos faria com que a garantia da privacidade do usuário se tornasse um diferencial de mercado. Uma maneira indicada para melhorar o nível de anonimato do comprador é trocar as moedas em vários bancos antes de usá-las. Assim apenas um acordo entre todos os bancos permitiria a identificação do usuário. O vendedor pode tentar manter sua privacidade trocando as moedas que receber, ao invés de depositá-las.

Divisibilidade: nível 2.
para obter cupons de menor valor, o usuário deve trocá-los no banco.

3.12.2 Requisitos

Integridade: a integridade das moedas é garantida pelo uso de assinaturas digitais.

Consistência: não é tratada de maneira explicita.

Viabilidade econômica: O servidor de moeda pode gerar cupons *off-line* e precisa apenas verificar a sua assinatura e a validade de um número de série *on-line*. Assim acreditamos que o sistema é viável economicamente. Talvez possa ser implementado de forma a tornar viáveis as microtransações.

Escalabilidade: o sistema permite a existência de várias entidades emissoras e a incorporação de novos usuários é bastante fácil. O principal problema quanto à escalabilidade do sistema é a possibilidade do número de moedas válidas de um único banco crescer a ponto de inviabilizar a consulta aos números de série das moedas em circulação.

Interoperabilidade: o sistema prevê a existência de diversas entidades emissoras e a interoperabilidade com o sistema NetCheque. Sendo um sistema on-line, é possível a implantação de um serviço de conversão de moedas para outros sistemas.

Auditabilidade: as moedas contém a identificação da entidade emissora e um número de série. Nenhum outro mecanismo de auditoria é especificado.

3.12.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   O usuário deve escolher o servidor de moeda com quem deseja trabalhar e negociar qual método de pagamento será usado para a compra de cupons NetCash. O usuário deve também obter o *software* necessário ao uso do sistema, além do certificado com chave pública do servidor de moeda.

2. **Retirada**
   O usuário deve usar o método escolhido quando do estabelecimento do relacionamento com o servidor de moeda para comprar cupons NetCash. O usuário envia o pagamento e uma requisição, que indica os valores dos cupons que deseja, cifrados com a chave pública do servidor. Quando o servidor recebe o pagamento e a requisição de cupons, este vai gerar os cupons requisitados, assiná-los e enviá-los ao usuário, cifrados com uma chave de seção escolhida pelo usuário.

3. **Transação**

   (a) **Autenticação**: O pagador não precisa se identificar, enquanto que o recebedor deve enviar uma chave pública certificada para o pagador.

   (b) **Pagamento**
   O pagador envia os cupons, uma indicação dos itens adquiridos, e duas chaves de seção, todos cifrados com a chave pública do vendedor. O vendedor decifra os cupons e os envia ao seu servidor de moeda. O servidor de moeda vai verificar a validade dos cupons com o servidor que os emitiu e retorna ao recebedor um cheque eletrônico ou uma quantidade de cupons correspondente ao valor da transação.

   (c) **Recibo**
   Se o servidor indica uma transação válida, o recebedor emite um recibo, assina este recibo e o envia ao pagador. Uma indicação de transação válida ocorre quando o servidor envia ao recebedor os novos cupons ou o cheque no valor correto.

   (d) **Finalização**: não existe etapa de finalização neste sistema.

4. **Compensação**
   O depósito dos cupons recebidos ocorre no momento da verificação de sua validade.

3.12.4 Aspectos de Implementação

Criptografia: Os algoritmos não são especificados, sendo que o sistema faz uso de:

Cifra simétrica

Cifra assimétrica

Assinatura digital

Certificados

Hashing

Conexões de rede: duas conexões.
Uma conexão é necessária para que o comprador pague ao vendedor e outra para que o vendedor entre em contato com o servidor de moeda para verificar a validade das moedas que recebeu.

Formato dos cupons: cada cupom consiste de:

- nome do servidor que emitiu a moeda
- endereço deste servidor
- data de validade
- número de série
- valor

Cada moeda é assinada pelo servidor que a emitiu.

3.13 NetCheque

O NetCheque [15] é um dos sistemas de pagamento desenvolvidos na USC. O NetCheque é um sitema que imita o funcionamento dos cheques tradicionais e usa a autenticação baseada no Kerberos, não fazendo uso de cifras assimétricas. Para assinar um cheque, o usuário deve obter um tíquete com o servidor Kerberos e usar a informação contida neste tíquete para gerar sua assinatura. Todas as entidades devem ser cadastradas nos servidores Kerberos.

3.13.1 Características

Modelo de troca: notacional
O sistema imita o funcionamento dos cheques bancários, sendo então um sistema notacional.

Envolvimento da entidade emissora: *on-line*
O uso de servidores baseados no *Kerberos* obrigam o sistema a funcionar *on-line*.

Quantias envolvidas: pequenos pagamentos
A segurança do sistema depende da segurança dos servidores e dos algoritmos criptográficos usados. O sistema é adequado para pequenos pagamentos, embora seu custo possa vir a ser pequeno o suficiente para viabilizar micropagamentos.

Hardware necessário: uso geral
O sistema não faz uso de *hardware* especial como *smart cards* ou outros mecanismos deste tipo, sendo passível de implementação em qualquer tipo de computador.

Papéis envolvidos: comprador, vendedor e banco.
O sistema prevê a existência de vários bancos, que mantêm as contas dos usuários do sistema e se comunicam para compensar os cheques emitidos.

Inversibilidade dos papéis: papéis variáveis.
Os usuários do sistema podem tanto atuar como pagadores quanto como recebedores. O único papel fixo é o papel do banco, ou entidade emissora.

Privacidade: inexistente
Não são previstos mecanismos para garantir a privacidade dos usuários ou dos dados trocados.

Divisibilidade: nível 4, o sistema é notacional.

3.13.2 Requisitos

Integridade: a integridade dos cheques é garantida pelo uso de *hashings* criptografados e tickets *Kerberos*.

Consistência: não é tratada de maneira explicita.

Viabilidade econômica: O sistema só prevê o uso de cifras simétricas e deve ser usado para transações de valores próximos aos valores de transações com cheques. Assim, acreditamos que seja viável economicamente.

Escalabilidade: A existência do servidor *Kerberos* central pode atrapalhar a escalabilidade do sistema, embora a última versão do *Kerberos* já permita o uso de vários servidores.

Interoperabilidade: é prevista e interoperabilidade com o NetCash.

Auditabilidade: todas as transações são identificadas e devem passar pelo servidor que pode manter *logs*.

3.13.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   Os usuários devem abrir contas especiais nos bancos que participam do sistema, sendo que estas contas serão usadas nas transferências feitas através do NetCheque. Os usuários devem também obter o *software* necessário ao uso do sistema.

2. **Retirada**: não há.

3. **Transação**

   (a) **Autenticação**
   Os usuários devem obter tíquetes junto a um servidos Kerberos, antes da transação ou a medida em que forem necessários.

   (b) **Pagamento**
   O pagador obtém um tíquete para uso dos serviços do banco e usa a chave de seção contida no tíquete para cifrar um *hashing* dos dados do cheque. O pagador envia este cheque ao vendedor que vai obter um tíquete para si, endossar o cheque e enviá-lo ao banco para compensação.

   (c) **Recibo**: este sistema não prevê emissão de recibo.

   (d) **Finalização**: não há fase de finalização.

4. **Compensação**
   O banco do recebedor deve entrar em contato com o banco do pagador e realizar a compensação do cheque. Quando a compensação for completada, o banco credita o valor na conta do recebedor. O sistema não prevê que o banco avise ao recebedor que o valor foi creditado em sua conta.

Observações:

1. Se os participantes da transação quiserem se comunicar de forma cifrada, o pagador deve obter junto ao servidor KERBEROS um tíquete para que tenha uma chave de seção com o recebedor.

3.13.4 Aspectos de Implementação

Criptografia: Os algortimos não são especificados, sendo que o sistema faz uso de:

Cifra simétrica

Hashing

Conexões de rede: uma conexão.
Durante a transação apenas o comprador e o vendedor precisam se comunicar.

Formato das ordens de pagamento: os seguintes campos devem ser preenchidos:

- valor
- unidade monetária
- data
- número da conta
- identificação do recebedor
- assinatura do pagador

3.14 Cybercash

A CYBERCASH, INC. foi uma das primeiras empresas a oferecer serviços de pagamento na Internet através do sistema que leva o nome da companhia. Este é hoje o mais popular sistema de pagamento seguro na Internet, sendo usado por importantes empresas da área de comércio eletrônico e com mais de meio milhão de cópias do seu programa de carteira eletrônica distribuídas.

O CYBERCASH é um sistema baseado em cartões de crédito que pode ser considerado como uma etapa intermediária entre a coleta de números de cartões pelos comerciantes e os sistemas a serem implantados pelas empresas de cartões de crédito, como o SET. A cybercash vem anunciando que passará a usar o SET, o que permitirá a integração com sistemas de outros fabricantes.

3.14.1 Características

Modelo de troca: notacional
é um sistema baseado no sistema de cartões de crédito, que pode ser visto como uma maneira segura de comunicar números de cartões.

Envolvimento da entidade emissora: *on-line*
O servidor deve ser contactado para que este processe o pagamento junto às administradoras de cartões.

Quantias envolvidas: pequenos a médios pagamentos
A faixa de valores é determinada pelas empresas de cartões de crédito. Em geral, os custos das transações são altos demais para micropagamentos e os limites de crédito não permitem transações de grandes valores.

Hardware necessário: uso geral
O sistema não faz uso de *hardware* especial como *smart cards* ou outros mecanismos deste tipo, sendo passível de implementação em qualquer tipo de computador. Existem implementações para PCs, *MacIntoshes* e estações UNIX.

Papéis envolvidos: comprador, vendedor e servidor central.
Os papéis são fixos e o sistema prevê a existência de apenas um servidor central, com o qual os compradores e vendedores deve se registrar.

Inversibilidade dos papéis: papéis fixos.
Assim como no sistema de cartões de crédito, os papéis são fixos.

Privacidade: existente.
Embora não permita transações anônimas, o sistema não permite que o vendedor veja o número do cartão do comprador e não permite que o banco tenha conhecimento dos ítens adquiridos.

Divisibilidade: nível 4, o sistema é notacional.

3.14.2 Requisitos

Integridade: As mensagens são assinadas e o servidor central garante a integridade do sistema.

Consistência: As trasações são realizadas pelo servidor central, que deve se encarregar de garantir a consistência do sistema. As mensagens trocadas garantem que o comprador e o vendedor tem uma visão consistente da transação.

Viabilidade econômica: O sistema está em operação desde 1995 e têm demonstrado ser viável e lucrativo.

Escalabilidade: O sistema é dependente de um servidor central, o que impõe um limite na quantidade de usuários e transações que este é capaz de atender.

Interoperabilidade: Este sistema não prevê interoperabilidade.

Auditabilidade: As mensagens são assinadas e as transações são registradas pelo servidor central.

3.14.3 Funcionamento

As etapas do funcionamento são:

1. **Relacionamento**
   O usuário deve adquirir o *software* que permite o uso do sistema, e deve também registrar uma identificação junto ao servidor CyberCash e escolher uma senha. Após ter se registrado, o usuário deve registrar seus cartões de crédito, o que permite à CyberCash realizar uma verificação prévia junto às empresa de cartões de crédito quanto à validade destes cartões.

2. **Retirada**: não há.

3. **Transação**

(a) **Autenticação**: não há.

(b) **Pagamento**
Após escolher os ítens, o comprador inicia a transação. O vendedor assina e envia ao comprador a descrição dos bens e seu preço. O comprador verifica esta descrição e escolhe o cartão a ser usado na transação. O número deste cartão é cifrado com a chave pública do servidor CyberCash e é assinado junto com um *hashing* da descrição dos bens e do preço total. Esta mensagem é enviada ao vendedor, que a repassa ao servidor central juntamente com um novo *hashing* da descrição do pedido assinada com sua chave secreta.

(c) **Recibo**: O servidor CyberCash verifica se os *hashings* da descrição são iguais, verifica as assinaturas e processa a transação junto às empresas de cartões de crédito. Após a realização da transação, o servidor envia ao vendedor dois recibos: um fica com o vendedor e o outro deve ser repassado ao comprador.

(d) **Finalização**: não há fase de finalização.

4. **Compensação**: Não há etapa de conpensação.

3.14.4 Aspectos de Implementação

Criptografia: são necessários:

Cifra simétrica: DES.

Cifra Assimétrica: RSA com chaves de 1024 bits.

Assinatura Digital: RSA com chaves de 1024 bits

Hashing: MD5.

Conexões de rede: duas conexões.
O comprador e o vendedor devem se comunicar e o vendedor deve entrar em contado com o servidor CyberCash.

Formato das ordens de pagamento: O comprador envia os seguintes dados, assinados com sua chave secreta:

- número do cartão cifrado com a chave pública do servidor central
- valor
- *hashing* da descrição das mercadorias

O vendedor acrescenta um *hashing* assinado da descrição das mercadorias.

3.15 Outros Sistemas

Existem no mercado outros sistemas de pagamento que não pudemos analisar por diversos motivos. Em geral são sistemas proprietários, cujos detalhes são difíceis de obter, como Visa Cash, Visa Electron, MasterCard Cash, NetChex, ou mesmo sistemas cujos detalhes de funcionamento são mantidos secretos, como Mondex, CyberCoin, Proton.

Alguns destes sistemas já estão em uso comercial, outros estão em fase de testes, enquanto outros parecem detinados a não saírem do papel. De qualquer maneira, é difícil analisar ou comparar estes sistemas sem que as companhias que os desenvolveram apresentem os detalhes de seu funcionamento.

Existem também diversos sistemas propostos que consideramos "sistemas acadêmicos" porque são difícil compreensão e implementação, embora apresentem características que os tornem importantes. São, em geral, sistemas que consistirão na base para desenvolvimentos futuros. Alguns exemplos podem ser encontrados em [17, 4, 8, 20].

4 Contribuições e Conclusões

Este trabalho a presenta um esquema que permite sistematizar a análise e comparação dos sistemas de pagamento eletrônico, tendo em vista a tipificação, a análise das características desejáveis, o funcionamento e implementação destes sistemas.

Tendo em vista que não deve haver apenas um único sistema de pagamento no mercado, mesmo no futuro, é necessário encontrar fórmulas que nos permitam decidir qual o sistema de pagamento mais adequado a nossa necessidades. Assim, acreditamos que uma das importantes contribuições deste trabalho seja oferecer uma sistemática que permita, após um levantamento detalhado dos requisitos da aplicação, analisar a adequabilidade de um sistema ou comparar, dentre os sistemas existentes, qual é o mais indicado. Assim, acreditamos que a análise e comparação de sistemas de pagamento eletrônico devem sempre ocorrer tendo em vista a aplicação desejada, por exemplo: venda de informações, venda de bens físicos, *pay-per-view* etc.

Outro ponto que consideramos importante neste trabalho foi sistematizar o funcionamento dos sistemas de pagamento de um maneira bastante ampla, o que pode ajudar quando do projeto de novos sistemas. As diferentes etapas de funcionamento que caracterizamos para os sistemas de pagamento devem ser levadas em conta quando do projeto de novos sistemas, o que permite ao projetista verificar se deixou de incluir algum ponto importante para o sistema. Além disto, a caracterização do sistema permite que o projetista elimine algum ítem do sistema cuja inclusão revelou-se desnecessária em vista da aplicação desejada.

Como não acreditamos na possibilidade de contrução de um sistema universal, ou seja, que possa substituir com eficiência qualquer outro sistema de pagamento, acreditamos que analise e comparação levando em conta o contexto de aplicação do sistema são imprecindíveis a um bom entendimento e ao uso correto dos sistemas de pagamento.

Referências

[1] N. Asokan, Michael Steiner, and Michael Waidner. The state of the art in electronic payment systems. *IEEE Computer*, pages 28–35, September 1997.
Apresenta uma classificacao dos sistema de pagamento eletronico e descreve alguns sistemas para micropagamentos.

[2] Anish Bhimani. Securing the commercial internet. *Communications of the ACM*, 39(6):29–35, June 1996.
Este artigo apresenta diversos requisitos necessarios a realizacao de comercio na Internet e as tentativas existentes de tornar esta rede segura.

[3] Jean Paul Boly, Antoon Bosselaers, Ronald Cramer, Rolf Michelsen, Stig Mjolsnes, Frank Muller, Torben Pedersen, Birgit Pfitzmann, Peter de Rooij, Berry Schoenmakers, Matthias Schunter, Luc Vallee, and Michael Waidner. The esprit project CAFE: High security digital payment systems. In *ESORICS 94, LNCS 875*, pages 217–230. Springer-Verlag, 1994.
Apresenta o sistema CAFE.

[4] Stefan Brands. Untraceable off-line cash in wallets with observers. In *Proceedings of Crypto 93*. Springer-Verlag, 1994.

[5] L. Jean Camp and Marvin Sirbu. Critical issues in internet commerce. *IEEE Communications Magazine*, pages 58–62, May 1997.
Apresenta os aspectos (confiabilidade, privacidade e seguranca) do comercio eletronico que os autores consideram criticos.

[6] L. Jean Camp, Marvin Sirbu, and J. D. Tygar. Token and notational money in electronic commerce. In USENIX Association, editor, *Proceedings of the first USENIX Workshop of Electronic Commerce: July 11–12, 1995, New York, New York, USA*, pages 1–12, Berkeley, CA, USA, July 1995. USENIX.
Apresenta as propriedades consideradas importantes em sistemas de pagamento eletronico. Introduz a notacao usada: sistemas notacionais ou de cupons.

[7] David Chaum. Achieving electronic privacy. *Scientific American*, pages 96–101, August 1992.
Este artigo apresenta a *blind signature*, que permite o projeto de sistemas de pagamento eletrônico com privacidade.

[8] David Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In S. Goldwasser, editor, *Proceedings of Crypto 88*, LNCS 403, pages 319–327, Santa Barbara, CA, USA, August 1990. Springer-Verlag.
Apresenta um sistema off-line com privacidade total para os usuarios que nao tentarem trapacear o sistema.

[9] Digicash web site.
URL: http://www.digicash.com, 1997.

[10] P. Janson and M. Waidner. Electronic payment systems. Activity Paper 211ZR018, Semper/IBM Zurich Research Lab, May 1996.
Este artigo apresenta uma classificação dos esquemas de pagamento eletrônico via Internet e dá detalhes do *iKP*, que foi desenvolvido pela IBM. Uma comparação dos diversos métodos de pagamento eletrônico para a Internet é apresentada, com base em diversos parâmetros, como uso de criptografia, privacidade, etc. Este artigo está disponível eletronicamente na URL: http://semper.zurich.ibm.com/info/211ZR018.ps.

[11] Gennady Medvinsky and B. Clifford Neuman. Netcash: A design for practical electronic currency on the internet. In *Proceedings of the First ACM Conference on Computer and Communications Security*. ACM, November 1993.

[12] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, October 1996.
Um livro bem completo sobre criptografia, técnicas criptográficas e aplicações.

[13] Millicent web site.
URL: http://www.millicent.digital.com, 1997.

[14] Netbill web site.
URL: http://www.ini.cmu.edu/netbill/, 1997.

[15] Netcheque web site.
URL: http://nii.isi.edu/info/netcheque/documentation.html, 1997.

[16] B. Clifford Neuman. Security, payment and privacy for network commerce. *IEEE Journal on Selected Areas in Communications*, 13(8):1523–1531, october 1995.
Apresenta os requisitos para sistemas de pagamento eletronico e algumas tecnicas para atingi-los.

[17] T. Okamoto and K. Ohta. Universal electronic cash. In J. Feigenbaum, editor, *Proceedings of Crypto 91, LNCS 576*, pages 324–337. Springer-Verlag, 1992.
Apresenta um sistema de pagamento off-line com transferibilidade e indica 6 caracteristicas que os sistemas de pagamento por cupons devem ter para serem considerados universais.

[18] Paul-André Pays and Fabrice de Comarmond. An intermadiation and payment system technology. In *Fifth International World Wide Web Conference*. GC Tech, May 1996.
Apresenta o sistema Globe ID para comercio eletronico.

[19] Michael Peirce and Donal O'Mahony. Scaleable, secure cash payment for WWW resources with the PayMe protocol set. In *Fourth International Conference on the World-Wide Web*, MIT, Boston, December 1995.
Apresenta o protocolo Payme, para pagamentos na Internet.

[20] Birgit Pfirtzmann and Michael Waidner. Strong loos tolerance of electronic coin systems. *ACM Transactions on Computer Systems*, 15(2):194–213, May 1997.

[21] Ronald L. Rivest and Adi Shamir. Payword and micromint: Two simple micropayment schemes. disponivel em http://theory.lcs.mit.edu/ rivest/RivestShamir-mpay.ps, 1995.

[22] Andreas Schoter and Rachel Willmer. Digital money online: A review of some existing technologies. Technical report, Intertrader Ltd., February 1997.
Apresenta rapidamente os sistemas de pagamento eletronico mais comuns e os classifica de acordo com o trabalho do grupo que desenvolveu o NetBill.

[23] Jennifer G. Stein, Clifford Neuman, and Jeffrey L. Schiller. Kerberos: An authentication service for open network systems. In *USENIX Conference Proceedings*, pages 203–211, Winter 1988.
Este artigo apresenta o famoso sistema Kerberos, do M.I.T. O Kerberos permite autenticação e troca de mensagens cifradas numa rede.

[24] Lee H. Stein, Einar A. Stefferud, Nathaniel S. Borenstein, and Marshall T. Rose. The green commerce model. Internet Draft Internet Draft, First Virtual Holdings Inc., May 1995.
Este artigo apresenta uma classificação dos esquemas de pagamento eletrônico via Internet e dá detalhes do *iKP*, que foi desenvolvido pela IBM. Uma comparação dos diversos métodos de pagamento eletrônico para a Internet é apresentada, com base em diversos parâmetros, como uso de criptografia, privacidade, etc. Este artigo está disponível eletronicamente na URL: http://semper.zurich.ibm.com/info/211ZR018.ps.

[25] Visa and Mastercard. *Secure Electronic Transactions (SET) Specification - Book 1: Business Description*, June 1996.
Especificação do SET. Este primeiro volume apresenta uma visão de alto nível do protocolo, que foi projetado para permitir transações com cartões de crédito via Internet.

A Conceitos Básicos de Criptografia

A.1 Funções Usadas em Criptografia

Alguns tipos de funções são necessários na implementação das técnicas criptográficas. Dentre estes podemos destacar:

função unidirecional: é uma função de um conjunto X em um conjunto Y para a qual é *fácil* calcular $y = f(x)$, mas é *difícil* calcular $x = f^{-1}(y)$, $y \in Y$, $x \in X$, para a maior parte dos elementos em Y.

função unidirecional com porta de escape: é uma função unidirecional $f : X \rightarrow Y$ com a propriedade adicional de que, dada certa informação extra, torna-se *fácil* achar um $x \in X$ para um $y \in Y$, tal que $f(x) = y$.

permutação: Seja S um conjunto finito. Uma permutação p em S é qualquer bijeção de S em si mesmo: $p : S \rightarrow S$.

involução: Seja S um conjunto finito e f uma bijeção de S em S ($f : S \rightarrow S$). A função f é chamada de involução se $f = f^{-1}$, ou seja, $f(f(x)) = x$, $\forall x \in S$.

As permutações e involuções são usadas nas cifras de chave privada e as funções unidirecionais são usadas nas cifras de chave pública.

A.2 As Cifras

Uma cifra é uma maneira de garantir a confidencialidade dos dados, ou seja, de codificar uma informação de forma a impedir que esta chegue ao conhecimento de pessoas não autorizadas. Nas seções abaixo apresentamos os dois tipos de cifras existentes: as cifras de chave privada e as de chave pública.

Uma cifra consiste de duas transformações: uma para cifrar e outra para decifrar. As duas transformações podem algumas vezes ser iguais. A segurança das cifras está ligada ao fato de um adversário ser incapaz de descobrir qual foi a transformação usada.

Em geral, estas transformações são funções que requerem o uso de chaves, ou seja, de parâmetros adicionais. Neste caso, apenas as chaves precisam ser tratadas como segredo. A figura 3 mostra como funcionam as cifras de maneira geral.

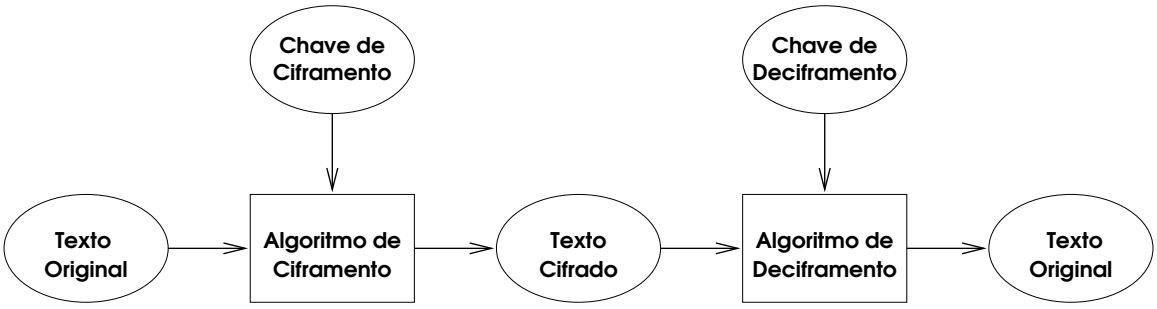

Figura 3: Funcionamento de uma cifra

A.2.1 Chave Secreta

Uma cifra de chave privada ou cifra simétrica é uma cifra para a qual é *fácil* determinar a chave de deciframento a partir da chave de ciframento; em muitos casos as duas chaves são iguais. Portanto, as chaves devem ser mantidas em segredo. As cifras simétricas são classificadas em dois grupos principais: as cifras de blocos (block ciphers) e as cifras de fluxo (stream ciphers).

As cifras de blocos são aquelas que quebram o texto de entrada em blocos menores e cifram cada bloco separadamente. A transformação aplicada para cifrar os blocos é a mesma em todos eles. As principais cifras simétricas usadas atualmente são cifras de blocos.

As cifras de fluxo são cifras que usam blocos de tamanho unitário, mas que variam a transformação aplicada à entrada a cada bloco. Isto significa que cada bloco é cifrado com uma chave diferente. Este tipo de cifra é útil porque permite que os dados sejam processados um símbolo de cada vez, mantendo a segurança, sendo então úteis para cifrar as comunicações oriundas de dispositivos como teclados.

Uma consideração importante para avaliar a segurança de cifras simétricas é o tamanho do espaço de chaves, ou seja, quantas chaves diferentes podem ser usadas com uma determinada cifra. Uma condição necessária, mas não suficiente, para que uma cifra seja segura é que seu espaço de chaves seja grande o suficiente para dificultar uma busca exaustiva.

Em geral, as cifras simétricas são permutações da entrada, principalmente as cifras de blocos. Nestas, o bloco de saida pertence ao mesmo universo que o bloco de entrada, o que na prática quer dizer que os blocos de entrada e saída têm o mesmo número de bits. Algumas cifras são também involuções, no sentido de que o texto cifrado deve passar pelo mesmo algoritmo novamente para ser decifrado.

Alguns exemplos de cifras simétricas são: DES, IDEA, Lucifer, BlowFish.

A.2.2 Chave Pública

Uma cifra de chave pública ou cifra assimétrica é aquela na qual é *difícil* determinar a mensagem original se soubermos apenas a mensagem cifrada e a chave de ciframento. Isto implica que dada a chave de ciframento é *difícil* obter a chave de deciframento. Assim, a função de ciframento de uma cifra assimétrica é uma função unidirecional com porta de escape (a chave de decifração).

Em geral, num sistema onde cifras assimétricas são usadas, cada entidade tem duas chaves: uma é secreta e deve ser guardada com cuidado e a outra é pública e deve ser publicada. As mensagens destinadas a uma entidade devem ser cifradas com sua chave pública. No recebimento, a entidade usa a chave secreta para decifrar a mensagem. Como todos que forem se comunicar nesse sistema devem ter acesso às chaves públicas existentes, deve haver uma maneira de autenticar a origem destas chaves.

As cifras assimétricas também são suscetíveis a ataques por busca exaustiva em seu espaço de chaves, embora, normalmente, existam ataques mais eficientes que obriguem ao uso de um espaço de chaves maior. Por exemplo, o esquema RSA é uma cifra assimétrica baseado na dificuldade de fatoração de números grandes. Neste esquema, ataques que usem fatoração são mais eficientes que busca exaustiva de chaves e já obrigam o espaço de chaves a ser bastante grande.

Alguns exemplos de cifras assimétricas são: RSA e ElGamal.

A.3 Assinaturas Digitais

As assinaturas digitais são importantes para que se possa realizar autenticação, autorização e não-repúdio. O objetivo de uma assinatura digital é prover um mecanismo para que uma entidade associe sua identidade a alguma informação.

Um esquema de assinatura digital deve prover: um mecanismo para que alguém gere uma assinatura e um mecanismo para verificar esta assinatura. Qualquer outra entidade, de posse desta assinatura e da informação original, deve conseguir verificar a assinatura, sabendo assim que a informação não foi alterada e que a entidade que assinou tem conhecimento desta informação. Assim, dado um esquema de assinatura digital, devemos tem uma função de assinatura $ass : M \rightarrow A$ e uma função de verificação $ver : M \times A \rightarrow Verdadeiro, Falso$, onde M é a mensagem e A é a assinatura. A aplicação da função *ass* gera uma assinatura que, em conjunto com a mensagem original, leva a função de verificação a emitir um resultado Verdadeiro ou Falso.

Uma maneira simples de conseguir uma assinatura digital é o uso de cifras assimétricas em que a ordem de aplicação das chaves não é relevante, ou seja, $D_A(C_A(X)) = C_A(D_A(X)) = X, \forall X$, sendo que C_A é a aplicação da cifra usando a chave pública de A e D_A é a aplicação da cifra usando a chave secreta de A. Assim, se A "cifra" a mensagem com sua chave secreta, qualquer entidade que tenha acesso a sua chave pública pode verificar que a mensagem foi enviada por A e não foi alterada, já que somente A conhece sua chave secreta. Se a mensagem tivesse sido alterada, o resultado da tentativa de verificação usando a chave pública de A seria um texto ininteligível.

A.3.1 Blind Signatures

Algumas vezes é necessário um mecanismo que permita a uma entidade assinar uma mensagem sem tomar conhecimento de seu conteúdo. Um destes mecanismos se chama *blind signature* [7] e consiste em aplicar uma transformação no valor a ser assinado de tal forma que, após a aplicação da assinatura, seja possível inverter esta transformação e obter o valor original assinado. Desta maneira, a entidade que assina o valor não é capaz de identificar o que assinou. A transformação aplicada é chamada *blinding factor*.

A.4 Funções de Espalhamento

Uma função de espalhamento, ou função de *hashing*, é uma função computacionalmente eficiente que mapeia cadeias de tamanho arbitrário em cadeias de tamanho predeterminado. A probabilidade de uma cadeia ser mapeada sobre um valor de saída deve ser uniforme entre os possíveis valores de saída.

Outra propriedade importante para que uma função de espalhamento seja usada em criptografia é que deve ser computacionalmente difícil gerar duas cadeias que tenham o mesmo valor de saída. Deve também ser difícil encontrar qual cadeia corresponde a uma dada saída.

Funções de espalhamento são usadas para:

- gerar assinaturas digitais compactas: normalmente, para assinar um documento, gera-se um *hash* deste documento. Este *hash* é então assinado. Para verificar a assinatura, gera-se um novo *hash* do documento original que é comparado com o *hash* assinado. Se a função de espalhamento usada for adequada não será possível encontrar outro documento que gere o mesmo *hash*. Então a assinatura será segura.

- garantir a integridade de dados: um *hash* da mensagem é enviado juntamente com a mensagem original. O receptor pode então verificar se a mensagem recebida tem o mesmo *hash* da original.

- protocolos com acordos a priori: a verificação da informação trocada a priori pode ser feita sem que a informação tenha que transitar numa rede. Para isso cada participante envia um *hash* da informação aos outros.

Alguns exemplos de funções de espalhamento são: MD5, MD4, SHA.

A.4.1 Cadeia de Hashings

Se pegarmos um número aleatório e aplicarmos a função de *hashing* neste número e em cada um dos valores obtidos pela aplicação da função sucessivamente, obteremos uma seqüência criptograficamente forte. Se divulgarmos apenas o último valor obtido, ninguém será capaz de obter facilmente qualquer outro valor da seqüência, já que seria necessário reverter a função de *hashing* usada. Esta seqüência, usada na ordem contrária àquela em que foi gerada é chamada de cadeia de *hashing*.

A.4.2 Colisões de Hashings

Uma colisão de uma função de *hashing* é um conjunto de valores que, quando usados como entrada para a função, resultam no mesmo resultado. Por exemplo: x_1 e x_2 formam uma colisão da função $h(x)$ se $h(x_1) = h(x_2) = y$, para um y qualquer.

A.5 Protocolos Criptográficos

Um protocolo criptográfico é um algoritmo distribuído que descreve as ações necessárias para que duas entidades atinjam um determinado objetivo de segurança. [12]

Os principais protocolos criptográficos são aqueles projetados para permitir:

Estabelecimento de chaves: permitir que uma chave secreta fique disponível para duas ou mais entidades sem contudo ser acessível a entidades não autorizadas.

Gerência de chaves: os processos que permitem o estabelecimento de chaves e a manutenção das relações entre as entidades que envolvem o transporte e armazenamento de chaves.

Certificação de chaves: garantia de que a chave recebida provém da origem correta e de que a chave não foi alterada sem autorização.

Autenticação: garantia da identidade da entidade com a qual se estabeleceu a comunicação.

A.5.1 o Protocolo Challenge-Response

Uma das maneiras da autenticar um usuário é o uso de senhas secretas. No protocolo básico de autenticação por senhas, o usuário envia a senha pela rede e o servidor irá verificar se a senha está correta e então permitir ao usuário acesso a seus serviços. Este protocolo é falho no sentido de que um adversário poderia escutar as transmissões que circulam na rede e interceptar a senha. A partir daí, o adversário poderia personificar o usuário, tendo acesso não-autorizado aos serviços do servidor.

Para corrigir esta falha, usa-se o protocolo challenge-response, que consiste em enviar um pedido de inicio de conexão ao servidor, que irá enviar um desafio ao usuário. Este desafio é, normalmente, um número aleatório. O usuário irá usar um programa para cifrar este desafio usando sua senha como chave (alguns sistemas invertem e usam o desafio como chave para cifrar a senha) e devolvê-lo ao servidor. O servidor então verifica se a resposta ao desafio foi correta e informa ao usuário que a autenticação foi bem sucedida.

A.5.2 O Sistema Kerberos

O *Kerberos* [23] é um dos mais famosos sistemas de segurança da atualidade. O Kerberos foi baseado num sistema de estabelecimento de chaves com servidor confiável e permite realizar autenticação e estabelecimento de chaves para comunicação segura entres duas entidades de uma rede.

No *Kerberos*, participam entidades, que podem ser programas ou pessoas, e um servidor central. Sempre que alguma entidade (cliente) deseja solicitar um serviço a outra entidade (servidor), este cliente deve enviar uma solicitação de autenticação ao servidor *Kerberos*, que irá verificar a identidade deste cliente através de *challenge-response* lhe enviará um tíquete e uma chave de seção. Com este tíquete, o cliente pode estabelecer comunicação com o servidor e se autenticar. O servidor aceitará esta autenticação e poderá usar a chave de seção para estabelecer um canal seguro com o cliente. Para que este processo possa acontecer, o servidor *Kerberos* deve conhecer a senha de cada um dos participantes.

O sistema *Kerberos* faz uso de cifras simétricas e senhas, sendo que as senhas nunca trafegam na rede. Algumas variações já foram propostas, inclusive para permitir a uso de cifras assimétricas e eliminar a necessidade de um servidor central.

A.5.3 Public key Kerberos

Para eliminar a necessidade de um servidor *Kerberos* central, foi desenvolvida uma variação do *Kerberos* que faz uso também de cifras assimétricas. Cada usuário deve ter um par de chaves pública/privada.

Quando um cliente deseja entrar em contato com um servidor, este deve obter a chave pública do servidor e enviar a este uma requisição de um tíquete cifrada com a chave pública do servidor. Quando recebe esta requisição, o servidor retorna ao cliente o tíquete solicitado. Após esta etapa, o protocolo funciona como o *Kerberos* tradicional.

B Resumo das características dos sistemas

B.1 Tipificação

	Mod. de troca	Env. Banco	Quantias	Hardware
Fisrt Virtual	notacional	*on-line*	micro	geral
Globe ID	notacional	*on-line*	pequenas	geral
Payme	cupons	*on-line*	pequenas	geral
SET	notacional	*on-line*	pequ. a grandes	geral
PayWord	cupons	*off-line*	micro	geral
MicroMint	cupons	*off-line*	micro	geral
CAFE	híbrido	*off-line*	pequenas	específico
E-cash	cupons	*on-line*	pequenas	geral
iKP	notacional	*on-line*	pequ. a grandes	geral
Millicent	cupons	*off-line*	micro	geral
NetBill	notacional	*on-line*	micro	geral
NetCash	cupons	*on-line*	pequenas	geral
NetCheque	notacional	*on-line*	pequenas	geral
CyberCash	notacional	*on-line*	pequ. a médias	geral

	Papéis	Invers.	Privacidade	Nível de divisib.
Fisrt Virtual	CVS	não	não	4
Globe ID	CVS	não	sim	4
Payme	UE	sim	sim	2
SET	CVE	não	sim	4
PayWord	CVE	não	não	4
MicroMint	UE	sim	não	4
CAFE	PRE	sim	sim	1
E-cash	UB	sim	sim	2
iKP	PRE	não	sim	4
Millicent	CVE	não	sim	3
NetBill	CVE	não	sim	4
NetCash	CVE	sim	sim	2
NetCheque	CVB	sim	não	4
CyberCash	CVS	não	sim	4

Legenda: na colunais **papéis envolvidos (papéis)**, as letras representam:

C	comprador	**V**	vendedor
S	servidor central	**U**	usuário
E	entidade controladora	**P**	pagador
R	recebedor	**B**	banco

B.2 Características Desejáveis

	Integridade	Consistência	Viabilidade	Escalab.	Interoper.	Audit.
Fist Virtual		√	√	√		√
Globe ID	√	√	√			√
Payme	√		√	√		
SET	√	√	√	√		√
PayWord			√	√		√
MicroMint			√	√		√
CAFE	√	√	√	√	√	√
E-cash	√		√			√
iKP	√	√	√	√		√
Millicent	√		√	√		√
NetBill	√	√	√			√
NetCash	√		√	√	√	
NetCheque	√	?	√		√	√
CyberCash	√	√	√			√

B.3 Aspectos de implementação

	Primitivas Criptográficas	Conexões de Rede	Cont. Ordens de Pagamento
Fist Virtual		3	número de conta
Globe ID	Cifra assimétrica Assinatura *hashing*	2	não especificado
Payme	Cifra simétrica (IDEA) Cifra assimétrica (RSA) Assinatura digital (RSA)	2	valor do cupom número de série identificação do banco data de validade assinatura do banco
SET	Cifra Simétrica (DES) Cifra assimétrica (RSA) Assinatura digital (RSA) Certificado (X.509) *Hashing*	2	dados do cartão de crédito ID da transação valor da transação *hashing* da descrição do produtos
PayWord	Assinatura digital Certificados *Hashings*	1	valor de cadeia de *hashings*
MicroMint	*Hashing*	1	colisão de *hashing*
CAFE	Assinatura digital (Schnorr)	1	chaves públicas ID do vendedor data da transação valor da tarnsaçao
E-cash	Cifra simétrica (Triplo-DES) Cifra assimétrica (RSA) Assinatura digital *Hashing* (SHA)	2	número de série do cupom data de validade assinatura do banco
iKP	Cifra assimétrica (RSA) Assinatura digital (RSA) Certificados (PKCS) *Hashing* (MD5)	2	*hashing* de informações gerais número da conta número aleatório
Millicent	*Hashing* (MD5)	1	ID do vendedor valor do cupom número de série ID do comprador data de validade certificado de autenticidade
NetBill	Cifra simétrica (DES) Cifra assimétrica (RSA) Certificados *Hashing* (SHA)	2	tíquete *Kerberos* número da conta
NetCash	Cifra simétrica Cifra assimétrica Assinatura digital Certificado *Hashing*	2	ID do emissor do cupom Endereço do emissor data de validade número de série valor do cupom assinatura do emissor
NetCheque	Cifra simétrica *Hashing*	1	valor da transação unidade monetária data da transação número da conta do comprador ID do vendedor assinatura do comprador
CyberCash	Cifra simétrica (DES) Cifra assimétrica (RSA) Assinatura digital (RSA) *Hashing*	2	número do cartão valor *hashing* da desc. das mercadorias

Índice