UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Carlos Eduardo Mazzi

Emissor de Cupom Fiscal Virtual

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de mestre em Ciência da Computação.

Ricardo Felipe Custódio, Dr.
Orientador

Florianópolis, março de 2005

Emissor de Cupom Fiscal Virtual

Carlos Eduardo Mazzi

Esta Dissertação foi julgada adequada para a obtenção do título de mestre em Ciência da Computação, área de concentração Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Raul Sidnei Wazlawick, Dr.
Coordenador do Curso

Banca Examinadora

Ricardo Felipe Custódio, Dr.
Orientador

Joni da Silva Fraga, Dr.

Luiz Carlos Zancanella, Dr.

Sérgio Peters, Dr.

Ofereço esta dissertação a meus tios Geraldo Mazzi e Maria das Graças Cabral Mazzi como expressão de minha gratidão e apreço.

Agradecimentos

Agradeço ao professor Dr. Ricardo Felipe Custódio, pela orientação, motivação e incentivo. Agradeço aos funcionários da Secretaria de Estado da Fazenda, nas pessoas de Rogério Mello, Sérgio Pinetti e Ernesto Warnecke pelos diversos esclarecimentos prestados. Agradeço aos colegas do LabSEC que contribuíram de forma direta ou indireta, especialmente ao Eduardo dos Santos pela importante colaboração no desenvolvimento do protótipo proposto.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas

$ICMS$	Imposto sobre Circulação de Mercadorias e Serviços
$UFSC$	Universidade Federal de Santa Catarina
$LabSEC$	Laboratório de Segurança em Computação
NF	Nota Fiscal
ECF	Emissor de cupom fiscal
$ECF - IF$	Emissor de cupom fiscal - Impressora Fiscal
$ECF - PDV$	Emissor de cupom fiscal - Ponto de Venda
$ECF - MR$	Emissor de cupom fiscal - Máquina Registradora
SEF	Secretaria de Estado da Fazenda
EC	Estabelecimento Comercial
CI	Centro de Informática
$ECFV$	Emissor de Cupom Fiscal Virtual
CFV	Cupom fiscal virtual
ICP	Infra-estrutura de chave pública
GCP	Gerador de chaves privadas
XML	*Extensible Markup Language* ou Linguagem de Marcação Extensível
DTE	Diagrama de Transição de Estados
$CONFAZ$	Conselho Nacional de Política Fazendária
PCF	Placa Controladora Fiscal
MT	Memória de Trabalho
MF	Memória Fiscal

MFD	Memória de Fita-Detalhe
DOU	Diário Oficial da União
GT	Grande Totalizador
SB	Software Básico
AC	Autoridade Certificadora
AR	Autoridade de Registro
$W3C$	*World Wide Web Consortium* ou Consórcio para Rede Mundial
DTD	*Document Type Definition* ou Definição de Tipo de Documento
$LCMI$	Laboratório de Controle e Microinformática
API	*Application Program Interface* ou Interface para Programas Aplicativos
$COTEPE$	Comissão Técnica Permanente do ICMS

Resumo

Estabelecimentos comerciais emitem cupons fiscais nas operações de venda a consumidores. Tal procedimento é realizado através da utilização de um equipamento de impressão fiscal (ECF) auditado e autorizado pela Secretaria de Estado da Fazenda. Esta dissertação propõe alternativas para a emissão de cupons fiscais eletrônicos através da Internet dispensando a utilização de impressoras fiscais; ao invés disto utilizam-se impressoras comuns com as mesmas garantias de segurança do processo. Palavras-Chave: protocolos criptográficos, delegação de assinaturas digitais, documentos eletrônicos.

Abstract

Commercial establishments issue fiscal documents after commercial transactions. Such fiscal documents are usually printed over paper by a hardware device (ECF) audited and homologated by the Treasure Department. This Masther's Thesis proposes an alternative way to generate electronic fiscal documents on the Internet without any homologated hardware; instead, any printer may be used to print the document. Keywords: cryptographic protocols, proxy signature schemes, electronic documents.

Capítulo 1

Introdução

A arrecadação de um governo nas economias contemporâneas, de modo geral, compõe-se quase exclusivamente da cobrança de impostos de diversas naturezas [WAR 03]. Dentre a gama de impostos existentes, estará no escopo desta dissertação o ”imposto estadual sobre operações relativas à circulação de mercadorias”, descrito na lei federal número 5.172 [BRA 66], de 25 de outubro de 1966, que dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios.

Em nosso estado (Santa Catarina), tal imposto é regulamentado pelo decreto 2.870/01 que aprova o Regulamento do ICMS, publicado no Diário Oficial do Estado em 28/08/01. O ICMS (Imposto sobre Operações Relativas à Circulação de Mercadorias e sobre Prestação de Serviços de Transporte Interestadual e Intermunicipal e de Comunicação) é um imposto sobre valor agregado e não cumulativo [WAR 03]. Particularmente interessa para esta dissertação o procedimento de cobrança do ICMS do consumidor final feito pelo estabelecimento comercial no ato da venda.

Será sugerida nesta dissertação uma nova alternativa para emissão do documento fiscal denominado protocolo **Emissor de Cupom Fiscal Virtual** (ECFV), cujo objetivo é substituir a máquina Emissor de Cupom Fiscal (ECF) por um computador conectado a uma rede para realizar a emissão de documentos fiscais. A geração do documento fiscal será feita através de técnicas de criptografia e certificação digital as quais

propiciarão todos os requisitos de segurança necessários para garantir total controle do Estado sobre o processo de emissão.

As informações tratadas nesta alternativa serão codificadas na forma de documentos eletrônicos, beneficiando-se das vantagens destes sobre documentos em papel para as partes envolvidas: Estado, comércio e consumidor final. O Estado é beneficiado porque terá um maior controle sobre a emissão dos cupons fiscais diminuindo a sonegação. O comércio será beneficiado porque não será obrigado a adquirir equipamentos de impressão fiscal e diminuirá a concorrência desleal (quando um concorrente sonega impostos consegue praticar preços mais baixos). O consumidor terá benefícios diretos e indiretos. Por benefícios diretos entende-se que pode haver uma política de incentivos, como sorteios premiados; o benefício indireto é o aumento de arrecadação do Estado, que torna-se mais forte para investir em áreas como saúde, educação e segurança. A solução proposta ao longo desta dissertação pode ser estendida para todo o tipo de relação Estado/contribuinte.

Nesta dissertação o **Estado** é representado pela **Secretaria de Estado da Fazenda** (SEF) ou pelo **Fisco** (conjunto de órgãos públicos responsáveis pela determinação e arrecadação de impostos [WAR 03]).

1.1 Objetivos

O objetivo desta dissertação é a elaboração de um protocolo criptográfico que viabilize a emissão de documentos fiscais em meio digital e em papel no processo de venda direta a consumidores utilizando plataformas computacionais comuns com acesso à Internet. Os documentos fiscais devem atender a requisitos específicos de segurança da informação, tais como a comprovação eficiente de sua autenticidade e integridade.

Entretanto, o protocolo que será proposto neste trabalho apresenta alguns problemas que necessitam ser adequadamente tratados:

- Emissão do documento fiscal a distância;
- Impressão do documento fiscal;

- Emissão de documento fiscal na ausência de comunicação com a Secretaria de Estado da Fazenda (SEF);
- Possibilidade de conferir a autenticidade do documento fiscal impresso.

1.1.1 Objetivos Gerais

É objetivo desta dissertação conceber e validar um protocolo criptográfico para emissão segura de documentos fiscais em meios digital e papel.

1.1.2 Objetivos Específicos

Os objetivos específicos desta dissertação são:

- Oferecer uma alternativa de geração de documentos fiscais aos estabelecimentos comerciais e prestadores de serviços dispensando-os da obrigatoriedade da aquisição de equipamentos de impressão fiscal e toda burocracia envolvida, bastando-lhes utilizar plataformas computacionais comuns com acesso à Internet;
- Diminuir os custos envolvidos no processo de arrecadação de tributos;
- Propor um sistema menos vulnerável a fraudes de sonegação fiscal;
- Proporcionar à SEF mecanismos precisos e confiáveis de apuração de impostos devidos;
- Proporcionar ao consumidor final de mercadorias e serviços meios que possibilitem verificar a autenticidade do documento fiscal gerado.
- Possibilitar à SEF gerar documentos fiscais digitais remotamente, mesmo em situações em que não haja conexão à Internet;
- Possibilitar a impressão de documentos fiscais a partir de impressoras comuns, garantindo-se no mínimo os requisitos de segurança obtidos com uso de impressoras fiscais.

1.2 Justificativa e motivação

Quando alguém compra um produto em uma loja ou supermercado, está pagando além do valor do produto propriamente dito os impostos associados tais como o ICMS. É obrigação do estabelecimento comercial repassar ao Estado o valor do imposto pago pelo cliente. Desta forma, pode-se dizer que os clientes de estabelecimentos comerciais são de fato os contribuintes do Fisco enquanto os estabelecimentos comerciais desempenham o papel de guardiães e devem receber esta quantia e repassá-la ao Estado. Infelizmente esse processo é burlado freqüentemente pelos estabelecimentos comerciais que, ao invés de repassar para o Estado o imposto pago pelos contribuintes, apropriam-se indevidamente deste valor, enriquecendo ilicitamente e contribuindo para o empobrecimento do Estado. Trata-se do crime da sonegação fiscal.

Há várias tentativas técnicas que buscam diminuir este crime. Uma delas é a fiscalização de porta em porta, no entanto, atualmente a SEF não dispõe de fiscais em número suficiente para fiscalizar a emissão de documentos fiscais nos milhares de estabelecimentos comerciais existentes no estado de Santa Catarina. Visando aumentar a capacidade de fiscalização da SEF sobre as operações de venda a consumidores, esta dissertação traz propostas para melhorar o processo de emissão de documentos fiscais, contribuindo para o fortalecimento do Estado.

1.3 Caracterização do problema

Enquanto o documento em papel é naturalmente visualizado, o documento eletrônico precisa ser interpretado por um sistema computacional para que então possa ser visto e entendido pelas pessoas. Caso o sistema esteja corrompido ou não seja confiável, a visualização do documento ficaria comprometida. Surge então o problema de como garantir que um documento eletrônico expresse a vontade de quem o assinou e não outro conteúdo manipulado pela plataforma computacional.

A legitimidade de uma assinatura manuscrita no papel é comprovada através de comparação por semelhança, mais precisamente por reconhecimento de firma

em cartório (o cartório é uma entidade de fé pública) [BOR 02]. Além disso, quando uma pessoa assina um documento em papel confere características biométricas ao documento assinado. Tais características são vestígios importantes para eventuais perícias caso seja questionada a validade do documento.

A assinatura digital [STI 02] de um documento eletrônico é realizada através de um processo muito diferente de assinaturas manuscritas de documentos em papel. Documentos eletrônicos são seqüencias de números binários (zeros e uns); a entidade que o assina não é uma pessoa e sim um sistema computacional e não há como rastrear vestígios biométricos em uma assinatura digital de documento eletrônico. O reconhecimento da assinatura também não é feito por comparação e semelhança, há algoritmos específicos para tal atividade; no entanto há uma entidade que desempenha função equivalente ao cartório no processo de assinatura manuscrita: a autoridade certificadora. A confiança na autoridade certificadora é importante para garantir a identidade do titular.

Considerando-se resolvida a questão da confiabilidade do documento eletrônico, ainda restam alguns problemas a serem resolvidos:

- Garantir que a impressão em papel seja o mais fiel possível ao conteúdo do documento eletrônico (ou da vontade daquele que o produziu);
- Garantir que a impressão em papel traga a identificação da entidade que a assinou digitalmente;
- Garantir que as características impressas do documento eletrônico sejam facilmente reconhecidas (ou ao menos que seja possível automatizar o processo de reconhecimento destas características).

A argumentação exposta acima pode ser resumida através do seguinte desafio: garantir que a impressão de um documento eletrônico possa ser validada do ponto de vista dos requisitos de segurança. Para dificultar ao máximo falsificações, a impressão de documentos fiscais precisa conter elementos que possibilitem identificar sua legitimidade e garantir o correto registro de operações comerciais tributáveis. Somente desta forma garante-se que os tributos devidos ao Estado provenientes destas operações

comerciais cheguem aos cofres públicos de forma correta. Quanto maior a sofisticação das técnicas empregadas na geração de documentos fiscais, maior será a dificuldade de falsificá-los e portanto maior será o controle do Estado sobre o processo de arrecadação de tributos. Historicamente buscou-se aperfeiçoar o registro de operações comerciais com uso de diferentes tecnologias buscando garantir o correto registro de operações comerciais tributáveis:

- **Papel Único:** O Estado controla o fornecimento de formulários de Notas Fiscais aos estabelecimentos comerciais através de gráficas credenciadas. Cada Nota Fiscal (NF) possui um número seqüencial e é composta de quatro vias, que devem conter os mesmos dados, sendo que cada uma delas tem diferente destino. Para garantir que as quatro vias contenham os mesmos dados, utiliza-se papel carbono, intercalando-as. Desta forma, o estabelecimento comercial preenche os dados da primeira via da NF de forma manual ou mecânica (seja por datilografia ou impressão matricial) e as demais vias são automaticamente preenchidas graças ao papel carbono. Todavia, esta técnica é muito frágil e pode ser facilmente burlada; basta o estabelecimento comercial registrar valores diferentes nas diversas vias dos documentos fiscais pois não há como o Estado saber se foi utilizado ou não este mecanismo. Além disso, perde-se muito tempo preenchendo os valores da nota fiscal, o que representa um inconveniente para o estabelecimento comercial que a emite.

- **Equipamento de Impressão:** Esta é uma alternativa a tecnologia exposta no item anterior: ao invés de emitir NF em quatro vias, em um processo geralmente lento e suscetível a falhas de preenchimento dos valores, o estabelecimento comercial pode optar por um procedimento automatizado: trata-se do Emissor de Cupom Fiscal (ECF), equipamento de impressão de documentos fiscais controlado pelo Estado. O cupom fiscal gerado é equivalente a uma NF. Dependendo do ECF utilizado, a impressão do documento fiscal pode ocorrer em 1 ou 2 vias, além do registro dos dados na memória fiscal do equipamento. O ECF é composto por hardware e software e é fornecido por empresas credenciadas pelo Estado, sendo que sua liberação para comercialização está sujeita a homologação pelo Estado. Apesar de

apresentar vantagens em relação ao bloco de NF, o ECF também apresenta falhas de segurança que possibilitam fraudes de comerciantes mal intencionados. Maiores detalhes a respeito do ECF são apresentados no capítulo 2, página 14.

Nesta dissertação busca-se uma tecnologia alternativa às expostas no parágrafo anterior para o desafio de registrar os impostos devidos ao Estado provenientes de transações comerciais de venda à consumidores: trata-se de um enfoque sobre as **características de impressão do documento**. A partir deste enfoque busca-se agregar informações que permitam verificar a idoneidade do documento impresso, independente do papel utilizado para sua impressão ou mesmo do equipamento que o gerou. Tais características devem ser detectadas visualmente ou através de algum dispositivo, como sugerido na tabela 1.1.

Tabela 1.1: Propostas para impressão de documento fiscal

SOLUÇÃO	VANTAGENS	DESVANTAGENS
Impressão de um código alfanumérico.	facilidade de geração do código.	validação do cupom fiscal depende de uma consulta à Internet.
Hardware seguro: utilização de impressora fiscal (atual sistema).	facilidade de utilização.	possibilita fraudes ou utilização de impressoras fiscais irregulares. Necessidade de fiscalização ostensiva. Custo elevado.
Papel único, a ser fornecido pela Casa da Moeda.	dificuldade de falsificação do papel. Reconhecimento visual do papel.	alto custo na aquisição do papel proveniente da casa da moeda.
Documento eletrônico + papel.	maior dificuldade de fraudes.	necessidade do comprador possuir mídia ou dispositivo digital para armazenar o documento eletrônico.
Selo do Estado para conferir autenticidade ao papel impresso.	dificuldade de falsificação do selo. Reconhecimento visual do selo.	custo da obtenção do selo; pode tornar o processo de emissão de cupons fiscais lento.
Impressão de um código de barras, contendo a assinatura digital da SEF e outras informações.	facilidade de verificação do documento fiscal impresso. Dificuldade de falsificação do código de barras.	repetição de códigos de barras existentes.

O processo de geração de documentos fiscais, inicialmente controlado pelo uso de **papel único** (bloco de NF), evoluiu para o controle sobre o **equipamento de**

impressão (ECF), e agora propõe-se nova evolução: o controle sobre a **informação** que compõe o documento fiscal.

Dentre as propostas apresentadas para impressão de documento fiscal na tabela 1.1, a alternativa que parece ser mais promissora é a impressão de código de barras no documento fiscal contendo a assinatura digital da SEF; esta técnica será adotada para que se alcance o objetivo principal desta dissertação, descrito na seção 1.1.

1.3.1 Sonegação Fiscal

No processo de venda a consumidores, quando o cupom fiscal (ou nota fiscal) não é emitido de forma correta, ou as informações referentes a venda de produtos ou serviços são omitidas do Fisco, ocorre o crime de **sonegação fiscal** de acordo com a lei federal 8.137/90 [BRA 90] (define crime contra a ordem tributária, econômica e contra as relações de consumo). Mais precisamente, o inciso quinto do artigo segundo diz: *"utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública"*. Pena: detenção, de 6 (seis) meses a 2 (dois) anos, e multa. A sonegação fiscal enfraquece o Estado, enriquece ilicitamente o comerciante e engana o consumidor final, que paga pelo imposto que não é repassado ao Estado como deveria.

No ramo de sonegação de impostos pode-se observar dois tipos básicos de fraudes:

1. A que é realizada sobre os documentos ou livros fiscais propriamente ditos, ou seja, a que indica adulteração ou registro fora das especificações legais;

2. Ou aquela que é realizada sobre outros documentos, ou seja, que se referem a operações realizadas sem a emissão dos documentos fiscais respectivos.

Dentre as formas de sonegação do ICMS conhecidas, algumas se enquadram na adulteração dos registros fiscais e outras na omissão dos documentos fiscais. Eis algumas das formas de sonegação mais comuns:

- Clonagem de ECFs que operam sem a devida autorização do Fisco, portanto sem o lacre de segurança. Neste caso, o cupom fiscal emitido não tem valor algum e as informações fiscais são omitidas do Fisco;

- Alteração de funcionalidades do software básico do equipamento ECF, de forma a manipular os totalizadores do equipamento. Neste caso, os cupons fiscais emitidos são válidos, o equipamento ECF possui autorização de operação e um lacre válido, porém a totalização dos registros fiscais internos ao ECF não ocorre de forma correta;

- O Software Aplicativo que realiza comunicação com o equipamento ECF (ver capítulo 2, página 20) é alterado para contabilizar apenas alguns registros de vendas, é a chamada operação *by pass*. A cada n vendas realizadas apenas x são totalizadas, sendo $n > x$. Novamente, os cupons fiscais emitidos são válidos, o equipamento ECF possui autorização de operação e um lacre válido, porém ocorre ainda a sonegação;

- Finalmente a mais trivial das sonegações, a não emissão do cupom fiscal. Neste caso, embora o equipamento ECF esteja em situação regular, e mesmo que não haja nenhuma alteração nas funcionalidades do mesmo, o fato de não emitir o cupom fiscal deixa de atualizar os registros fiscais e portanto o Fisco deixa de receber o que lhe é devido.

Para descobrir e comprovar a sonegação fiscal de um estabelecimento na era da informática, passa-se a fazer, além da busca física por fichas, anotações, cadernos e outros meios utilizados para registrar as vendas realizadas, também uma busca nos meios informatizados do contribuinte, como arquivos, disquetes ou documentos eletrônicos utilizados para o registro de vendas realizadas tanto eletronica quanto convencionalmente [WAR 03]. E mesmo assim há um problema quanto a vestígios eletrônicos (planilhas e arquivos) pois estes são facilmente manipulados, portanto não apresentam valor jurídico, a menos que estejam assinados digitalmente e a assinatura seja válida. Ainda assim há

uma série de fatores que podem tornar questionáveis esses vestígios eletrônicos, os quais podem ser escassos ou mesmo inexistir fisicamente no local.

A forma mais simples de combater a sonegação fiscal é exigir o cupom fiscal (ou nota fiscal) a cada compra realizada. Entretanto, é sabido que isto não acontece com muita freqüência, por alguns motivos:

- O consumidor final não é multado por não exigir documento fiscal;
- O procedimento de compra de produtos e/ou serviços não é inviabilizado pelo fato do consumidor não solicitar o documento fiscal;
- O consumidor em geral não tem consciência da importância de exigir o documento fiscal;
- Geralmente os estabelecimentos comerciais adotam uma postura de não oferecer espontaneamente o documento fiscal, e, mesmo quando o consumidor solicita documento fiscal o processo torna-se mais demorado (na opinião do autor desta dissertação para desestimular o consumidor);

Além disso, mesmo que o consumidor exija o cupom fiscal não estará apto a identificar com precisão se o cupom entregue é válido ou não, ou então se o equipamento ECF está autorizado a emití-lo, e muito menos se há alguma fraude interna ao ECF.

O Fisco conta apenas com um número reduzido de fiscais que esporadicamente visitam os estabelecimentos comerciais em busca de irregularidades. Se for levado em consideração o número de estabelecimentos comerciais do estado de Santa Catarina e o número de fiscais disponíveis, constata-se facilmente que o sistema atual de detecção de fraudes é ineficiente e inviável.

Portanto, ao que tudo indica o Estado está em desvantagem nessa guerra contra a sonegação fiscal.

1.4 Trabalhos Correlacionados

O enfoque desta dissertação é o processo de venda a consumidores, o qual ocorre em estabelecimentos comerciais e prestadores de serviços. Neste cenário, o ICMS é cobrado dos consumidores e posteriormente repassado ao Estado. Entretanto, há outros cenários em que há controle sobre ICMS:

- Comércio entre empresas. Ernesto Warnecke [WAR 03] trata deste cenário em sua dissertação de mestrado entitulada ”G-DEF - Protocolo Criptográfico para Geração de Documento Eletrônico Fiscal nas Operações entre Empresas”;

- Empresas fornecedoras de energia ou prestadora de serviços domiciliares, individualizados, em larga escala, equacionado pelo convênio ICMS 115/03 em dezembro de 2003.

O Conselho Nacional de Política Fazendária (CONFAZ) [CON 04] criou um Grupo de Trabalho com a intenção de propor melhorias aos equipamentos de impressão fiscal. Este grupo, denominado GT-46 da COTEPE (Comissão Técnica Permanente do ICMS), possui participantes espalhados por diversos estados brasileiros, inclusive em Santa Catarina.

Há uma iniciativa da Secretaria de Estado da Fazenda do Rio Grande do Sul chamada ICMS Eletrônico [RS 05]. Esta iniciativa criou um Grupo de Trabalho, através da Portaria n 07/2003 DRP de 31/03/2003, para a criação e implantação do ICMS Eletrônico, com o objetivo de criar uma sistemática de apuração do ICMS segura e ágil, que possibilite o acompanhamento, em tempo real, de todas as transações eletrônicas efetuadas pelos contribuintes, otimizando o controle dos recursos arrecadados pelo Estado.

1.4.1 Experiência do Grupo

O Laboratório de Segurança em Computação (LabSEC) da Universidade Federal de Santa Catarina (UFSC) conta com um grupo de pesquisa na linha de Segurança em Computação; tal grupo, formado por professores e alunos de graduação,

mestrado e doutorado tem produzido diversos trabalhos científicos (incluindo esta própria dissertação) sendo que muitos deles com áreas afins. Além da dissertação de mestrado de Ernesto H. Warnecke [WAR 03] já citada, há os seguintes trabalhos que de alguma forma estão relacionados a esta dissertação:

- Tese de doutorado de Júlio Dias da Silva [DIA 04], entitulada ”Confiança no Documento Eletrônico”, a qual traz aspectos acerca da utilização de documentos eletrônicos em substituição a documentos em papel.

- Dissertação de mestrado de Dejane Luiza Bortoli [BOR 02] entitulada ”O Documento Eletrônico no Ofício de Registro Civil de Pessoas Naturais”traz contribuições para o advento de documentos eletrônicos em um cenário específico: os cartórios, mais especificamente os Ofícios de Registro Civil de Pessoas Naturais.

- Luciane Jussara Bezerra Kusbick [KUS 02] analisa o impacto da desmaterialização de documentos em papel em conseqüência da crescente utilização de documentos eletrônicos em sua monografia de especialização entitulada ”A Desmaterialização de Documento em Papel: Análise do Requisito Segurança para Validade Legal de Documentos Eletrônicos”

1.5 Conteúdo da Dissertação

Esta dissertação está organizada da seguinte forma:

O capítulo 2 apresenta a atual situação de controle de arrecadação de tributos sobre vendas realizadas a consumidores e como seria a situação ideal. Esta contextualização serve como motivação para o protocolo proposto nesta dissertação. São detalhadas as características do equipamento Emissor de Cupom Fiscal (ECF) e características do documento Cupom Fiscal.

O capítulo 3 apresenta o embasamento teórico necessário para a implementação do protocolo criptográfico ECFV. São apresentadas diferenças entre documentos papel e eletrônico, características de protocolos criptográficos, esquemas de assinatura

digital por delegação, conceitos de criptografia baseada em identidade e criptografia incremental além da padrões de código de barras.

O capítulo 4 apresenta o protocolo criptográfico ECFV: a infra-estrutura necessária à sua implementação, as entidades envolvidas em sua execução, contextualização do cenário proposto à sua utilização, além de características do Cupom Fiscal Virtual (CFV). Os problemas e deasafios tecnológicos do protocolo ECFV são descritos e possíveis soluções são sugeridas. Neste capítulo, os objetivos geral e específicos, listados na seção 1.1 são atendidos através das propostas apresentadas. O protocolo é formalizado e validado através de um Diagrama de Transição de Estados (DTE).

O capítulo 5 apresenta características, requisitos funcionais e procedimentos relacionados ao aplicativo ECFV, necessário à execução do protocolo criptográfico proposto nesta dissertação. É apresentado um protótipo desenvolvido para demonstrar algumas funcionalidades do aplicativo ECFV.

O capítulo 6 fecha a dissertação apresentando algumas considerações acerca do resultados obtidos com este trabalho, confrontando-os com os objetivos traçados na seção 1.1. Além disso, sugestões de trabalhos futuros são apresentadas.

Capítulo 2

Emissor de Cupom Fiscal

2.1 Introdução

Quando o consumidor adquire produtos em estabelecimentos comerciais, ele paga além do valor do produto propriamente dito, os impostos associados, dentre os quais o ICMS. O estabelecimento comercial tem a obrigação de registrar todas as suas vendas realizadas para poder repassar os impostos devidos ao Estado. O registro das vendas faz-se necessário para documentar o processo de vendas e fornecer ao estabelecimento comercial informações de quanto deve ser repassado ao Estado e ao Estado maneiras de fiscalizar e auditar todo o processo.

Em um cenário ideal, o consumidor compraria um produto pagando o valor deste ao estabelecimento comercial e pagaria diretamente ao Estado os impostos devidos, como ilustra a Figura 2.1. Esta situação é impraticável em nosso país por questões culturais e tecnológicas. Não há, por exemplo, uma infra-estrutura que possibilite, no momento da compra, que o comprador deposite concomitantemente ao valor do produto, o valor do imposto.

Fiscalizar toda a população de consumidores seria tarefa impraticável; ao invés disso, o Estado optou por fiscalizá-la através dos estabelecimentos comerciais. Em alguns casos, como automóveis, o Estado cobra os impostos diretamente das fábricas, o que simplifica e facilita o controle fiscal. No entanto a solução geralmente adotada

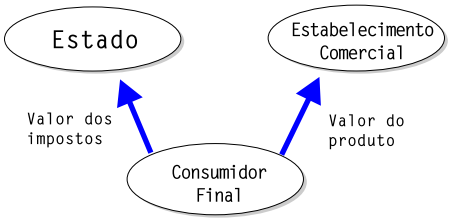

Figura 2.1: Situação ideal: consumidor adquire produtos e/ou serviços e paga ao estabelecimento comercial o valor destes; além disso, o consumidor paga diretamente ao Estado os impostos devidos.

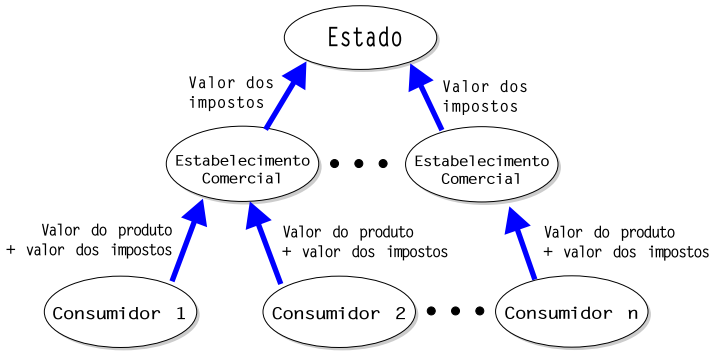

Figura 2.2: Situação atual: consumidor adquire produtos e/ou serviços e paga ao estabelecimento comercial o valor destes mais os valores dos impostos. Os estabelecimentos comerciais fazem o registro destes impostos e os repassam ao Estado.

pelo Estado é forçar o estabelecimento comercial a cobrar os impostos do consumidor, registrá-los e repassá-los ao Estado, como ilustra a Figura 2.2.

A tecnologia mais difundida para tal registro, inicialmente, foi o bloco de notas fiscais. Cada nota fiscal emitida possui um número sequencial para controle do Estado, e deve ser emitida em quatro vias, com auxílio de papel carbono, como ilustra a Figura 2.3. Este procedimento, conforme discutido na seção 1.3, página 4, apresenta alguns inconvenientes tais como o tempo de preenchimento dos valores da nota fiscal e a fragilidade desta tecnologia em relação a fraudes de sonegação fiscal.

Buscando oferecer maior agilidade e precisão ao processo de registro de vendas realizadas, surge uma alternativa ao uso das notas fiscais: trata-se de um dis-

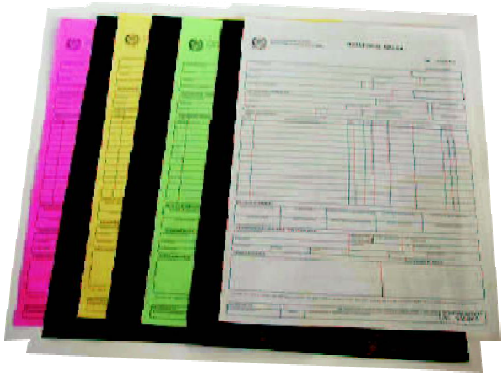

Figura 2.3: Nota Fiscal com papel carbono: quatro vias de uma nota fiscal avulsa, onde foram intercaladas folhas de papel carbono, visando transmitir os dados de uma via para a seguinte. Fonte: [WAR 03]

positivo de hardware e software integrado chamado Emissor de Cupom Fiscal (ECF), o qual será visto em detalhes na seção 2.2. O Cupom Fiscal, registro de venda em papel impresso pelo ECF, que possui valor equivalente a uma nota fiscal de venda a consumidor é apresentado na seção 2.3. A seção 2.4 fecha o capítulo.

2.2 Equipamento Emissor de Cupom Fiscal

De acordo com Ernesto Warnecke [WAR 03], ECF é um equipamento de automação comercial com capacidade de emitir documentos fiscais em papel e realizar controles de natureza fiscal referentes a operações de circulação de mercadorias ou prestações de serviços. Em equipamentos ECF o registro das vendas é feito no papel e também mediante a gravação em um dispositivo semicondutor de memória não volátil que não possui recursos de apagamento por sinais elétricos. Lá ocorre o armazenamento da chamada ”Memória Fiscal”, com capacidade para armazenar, no mínimo, dados referentes as vendas realizadas em um período de 5 anos, separadas por alíquota do imposto, além de outros dados [WAR 03].

O primeiro mecanismo de segurança do ECF é uma cópia da fita de papel onde são impressos os cupons fiscais. Esta cópia, chamada de **fita-detalhe**, é a

Figura 2.4: Lacre de Emissor de Cupom Fiscal: detalhe do lacre numerado instituído com o objetivo de impedir a abertura de ECF por terceiros não autorizados pela SEF. Fonte: [WAR 03]

segunda via do cupom fiscal e sua obtenção ocorre através de papel carbonado, ocorrendo a transmissão dos dados para a segunda via no momento da geração da primeira via do documento fiscal. A fita detalhe fica localizada dentro do equipamento ECF para possibilitar auditorias realizadas por técnicos da Secretaria de Estado da Fazenda (SEF). Os valores dos impostos, no entanto, são armazenados dentro dos registradores somadores que encontram-se dentro do ECF. Para evitar acesso indiscriminado aos componentes eletrônicos dos somadores que poderia resultar no zeramento dos mesmos, instituiu-se um controle baseado em lacres numerados como observamos na Figura 2.4, apenas abertos pelo Fisco ou por empresas credenciadas para tal ação. A seção 2.2.1 traz mais detalhes a respeito do lacre de proteção do ECF.

2.2.1 Lacre de proteção do ECF

Os dispositivos físicos chamados lacres são peças compostas por um corpo externo de policarbonato translúcido, um corpo interno composto de acrílico (chamado inserto rotativo) e um arame de lacração, com o objetivo de impossibilitar a abertura do ECF. A Figura 2.5 mostra um lacre aberto.

Uma vez fechado o lacre, não existe maneira de abrí-lo, senão através do

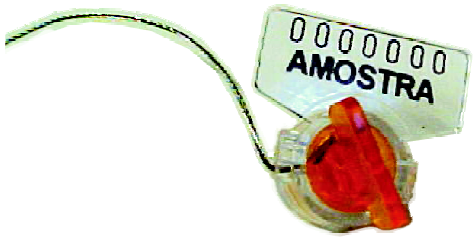

Figura 2.5: Lacre aberto para proteção de equipamento ECF: este dispositivo é composto por um corpo externo de policarbonato translúcido, um corpo interno composto de acrílico (chamado inserto rotativo) e um arame de lacração. Enquanto o lacre está aberto, uma das extremidades do arame de lacração está livre.

Figura 2.6: Lacre fechado para equipamento de ECF: após ser fechado, lacre não pode ser aberto.

seu rompimento. O procedimento para fechamento do lacre é muito simples: introduz-se a extremidade do arame de lacração que está livre no orifício do corpo externo do lacre. Então, gira-se o corpo de acrílico interno (inserto rotativo) tracionando-se o arame de lacração em um único sentido. Uma vez inserido no orifício do corpo do lacre não é possível puxar o arame de lacração para soltá-lo. A Figura 2.6 ilustra um lacre de proteção ECF fechado.

O arame de lacração presente no lacre de proteção de equipamentos ECF é composto por 6 a 8 fios de aço inox, com características físicas que evidenciam seu rompimento. Portanto, se o arame de lacração for cortado será visualmente detectável seu rompimento, como ilustra a Figura 2.7.

O lacre de proteção de equipamentos ECF deve ser único, por isso cada lacre recebe um número sequencial para que seja possível rastreá-lo. Sua produção é controlada, sendo que em Santa Catarina apenas a empresa ”Brooks Selos de Segurança

Figura 2.7: Lacre rompido para equipamento de ECF

do Brasil Ltda", sediada no Rio de Janeiro, está credenciada a fornecê-los a SEF[1].

Caso haja suspeita de que um lacre seja falso, este deve ser encaminhado para perícia a ser realizada exclusivamente pela empresa fornecedora de lacres credenciada pela SEF. Somente esta empresa tem competência para emitir laudo técnico confirmando ou desmentindo uma suposta falsificação. Em situações em que haja necessidade de realizar intervenções técnicas em algum equipamento ECF lacrado, apenas os técnicos da SEF estão autorizados a romper o lacre de proteção.

As características técnicas detalhadas dos lacres de proteção de equipamentos ECF são apresentadas pela tabela 2.1.

2.2.2 Tipos de Emissores de Cupom Fiscal

Antes de classificar os tipos de equipamentos ECF, é importante mencionar que as características destes equipamentos são definidas através de convênios celebrados pelo Conselho Nacional de Política Fazendária (CONFAZ) [CON 04]. Tais convênios, chamados convênios ICMS são publicados no Diário Oficial da União (DOU) e tem força de lei em todo o território nacional. Dentre os vários convênios existentes, é de interesse para esta dissertação os convênios que especificam as características dos equipamentos ECF.

Há três tipos de equipamentos ECF, sendo que a escolha do tipo de equipamento a ser utilizado fica a critério do estabelecimento comercial. A seguir, uma

[1]Esta informação é válida para o ano de 2004, época em que foram realizadas visitas a SEF para esclarecimentos acerca de equipamentos ECF

Tabela 2.1: Características do lacre de proteção de equipamento ECF.

CARACTERÍSTICA	DESCRIÇÃO
Modelo	Roto Seal II - Toolless Roto Seal.
Tipo	Corpo e Inserto Rotativo.
Material	Corpo em policarbonato translúcido resistente a ação de raios ultra-violeta e Inserto Rotativo em acrílico de alto impacto.
Sistema de Lacração	Corpo externo e Inserto interno rotativo capaz de tracionar o arame de lacração em um único sentido.
Local das Gravações	Personalização e Numeração seqüencial gravadas em lâmina localizada no Corpo do lacre.
Tipo de Gravação	Hot Stamp indelével em baixo relevo.
Fixação do Arame de Lacração	Transpassado por orifício localizado no Corpo externo do lacre, atinge o Inserto interno rotativo capaz de tracioná-lo.
Tipo do Arame de Lacração	Arame de lacração em cordoalha de aço inox evidenciadora de fraude, por meio de efeito de abertura ao ser cortada, composta de 6 a 8 fios de aço inox 304L em espiral continua, com diâmetro de cada fio entre 0,21mm e 0,30mm e o diâmetro total da cordalha entre 0,60mm e 0,95mm.

breve descrição de cada um dos tipos de ECF disponíveis.

2.2.2.1 ECF - Máquina Registradora (ECF-MR)

ECF com funcionamento independente de programa aplicativo externo, de uso específico, dotado de teclado e mostrador próprios. As características deste equipamento estão descritas nos convênios ICMS 24/86 [BRA 86] e ICMS 156/94 [BRA 94]. A Figura 2.8 mostra um exemplo de ECF-MR;

2.2.2.2 ECF - Impressora Fiscal (ECF-IF)

Este equipamento é implementado na forma de impressora com finalidade específica, que recebe comandos de computador externo. Ou seja, este equipamento precisa estar ligado a um computador munido de um Software Aplicativo que comunica-se com o Software Básico do ECF-IF para que sejam feitos os registros de venda nos somadores do ECF-IF; não é possível acessar os componentes eletrônicos registradores do ECF-IF senão através do Software Básico. O Software Aplicativo do computador ligado ao ECF-IF também realiza as funções de exibição dos itens de venda, comunicação

Figura 2.8: Máquina Registradora (ECF-MR)

com operadoras de cartão de crédito para pagamento, controle de estoque, entre outras.

Equipamentos ECF-IF podem estar de acordo com o convênio ICMS 156/94 [BRA 94] publicado no DOU de 15 de dezembro de 1994 ou convênio ICMS 85/01 [BRA 01a] publicado no DOU de 4 de outubro de 2001. A principal diferença entre as duas especificações diz respeito ao modo de armazenamento da segunda via dos documentos fiscais emitidos: o convênio ICMS 156/94 [BRA 94] determina que o registro seja feito em papel (**fita-detalhe**) enquanto o convênio ICMS 85/01 [BRA 01a] determina que o registro seja feito de forma eletrônica (**Memória Fita-Detalhe**).

Os principais componentes do ECF-IF, ilustrados pela Figura 2.9, são:

Placa Controladora Fiscal (PCF): conjunto de recursos de hardware, internos ao ECF, que concentra as funções de controle fiscal;

Software Básico (SB): conjunto fixo de rotinas, residentes na Placa Controladora Fiscal, que implementa as funções de controle fiscal do ECF e funções de verificação do hardware da Placa Controladora Fiscal;

Memória Fiscal (MF): conjunto de dados, internos ao ECF, que contém a identificação do equipamento, a identificação do contribuinte usuário e, se for o caso, a identificação do prestador do serviço de transporte quando este não for o usuário do

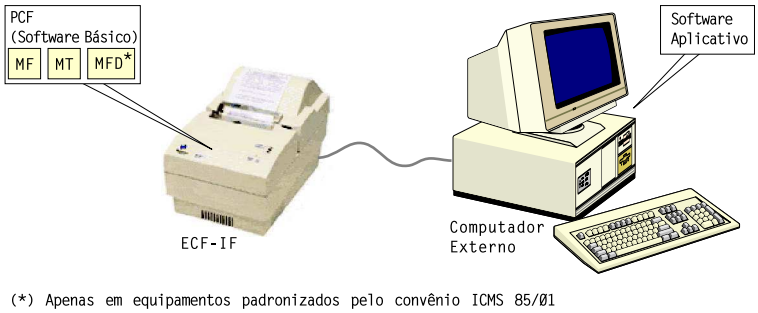

Figura 2.9: Estrutura física e lógica de um ECF-IF: o equipamento ECF-IF possui os componentes eletrônicos Memória Fiscal(MF), Memória de Trabalho(MT), Memória Fita-Detalhe (opcionalmente); tais componentes encontram-se localizados na da Placa Controladora Fiscal (PCF), controlada pelo Software Básico do ECF-IF.

ECF, o Logotipo Fiscal, o controle de intervenção técnica e os valores acumulados que representam as operações e prestações registradas diariamente no equipamento;

Memória de Trabalho (MT): área de armazenamento modificável, na Placa Controladora Fiscal, utilizada para registro de informações do equipamento e de parâmetros para programação de seu funcionamento, do contribuinte usuário, acumuladores e identificação de produtos e serviços;

Memória de Fita-detalhe (MFD): recursos de hardware, da Placa Controladora Fiscal, para armazenamento dos dados necessários à reprodução integral de todos os documentos emitidos pelo equipamento, dispensada a Leitura da Memória Fiscal, e que adicionalmente: a) não permitam o apagamento e a modificação de dados; b) permitam a reprodução dos dados armazenados para arquivo em meio eletrônico; c) permitam a impressão de segundas vias dos documentos originalmente emitidos; d) imprimam, em cada Redução Z, informações que permitam a recuperação de dados referentes a todos os documentos emitidos após a Redução Z anterior, inclusive a Redução Z que contenha as informações desta alínea;

Os equipamentos ECF-IF precisam ainda disponibilizar um modo de operação chamado **Modo de Intervenção Técnica (MIT)**, através do qual permite-se o

acesso direto aos componentes registradores do ECF-IF, exclusivamente, para: a) alteração de conteúdo da Memória de Trabalho; b) inserção de informações do estabelecimento comercial na Memória Fiscal; c) ajuste do relógio interno; d) no caso de ECF com Memória de Fita-detalhe, iniciação da Memória de Fita-detalhe e impressão de Fita-detalhe;

Figura 2.10: ECF-IF atendendo às especificações do convênio ICMS 156/94 [BRA 94].

O ECF-IF é o equipamento de registro de vendas adotado em maior escala pelos estabelecimentos comerciais no estado de Santa Catarina, segundo técnicos da SEF. A Figura 2.10 mostra um exemplo de equipamento ECF-IF que atende ao convênio ICMS 156/94 [BRA 94].

O convênio ICMS 85/01 [BRA 01a] traz algumas melhorias aos equipamento ECF-IF. A já mencionada substituição da fita-detalhe em papel por um dispositivo de memória (MFD) facilita a leitura dos dados do ECF-IF realizada pelos técnicos da SEF; além disso, a impressão do cupom fiscal passa a ser térmica ao invés de matricial, o que confere maior qualidade ao documento fiscal impresso. Todavia, equipamentos ECF-IF que atendem ao convênio ICMS 85/01 [BRA 01a] são mais caros que os que atendem ao convênio ICMS 156/94 [BRA 94]. A Figura 2.11 mostra um exemplos de ECF-IF dentro das especificações do convênio ICMS 85/01 [BRA 01a].

2.2.2.3 ECF - Terminal Ponto de Venda (ECF-PDV)

ECF que reúne em um sistema único o equivalente a um ECF-IF e o computador que lhe envia comandos. Suas características são definidas pelo convênio

Figura 2.11: ECF-IF atendendo às especificações do convênio 85/01 [BRA 01a].

ICMS 44/87 [BRA 87] A Figura 2.12 ilustra um conjunto ECF-PDV.

Figura 2.12: Conjunto ECF-PDV

2.2.3 Informações registradas

Os componentes eletrônicos internos ao ECF tem a função de totalizar e somar informações relativas às vendas realizadas, com o objetivo de apurar os impostos devidos ao Estado. A seguir, uma breve descrição das informações registradas pelos equipamentos ECF.

2.2.3.1 Leitura X

A Leitura X é um documento fiscal que mostra os valores acumulados nos contadores e totalizadores fiscais do equipamento ECF. A principal função deste documento é fornecer informações acerca de todos os registros de vendas realizadas desde o início da operação do ECF naquele dia até o momento da emissão da Leitura X; sua emissão deve ocorrer nas seguintes situações:

1. Antes da primeira venda do dia;
2. Durante a manutenção do ECF: sempre que possível, deve-se emitir a Leitura X antes e depois da intervenção para preenchimento do Atestado de Intervenção, documento que registra a intervenção no equipamento;
3. Tempo de operação do ECF no dia e tempo gasto com emissão de documentos fiscais, para os equipamentos ECF-IF e ECF-PDV.

2.2.3.2 Redução Z

A Redução Z é um documento fiscal que deve ser impresso obrigatoriamente no final do dia. Ao ser emitido, envia para a Memória Fiscal as seguintes informações:

- Data e a Hora da Redução Z;
- Contador de Reduções Z incrementado em uma unidade;
- Valor da Venda Bruta Diária;
- Tempo de operação do ECF no dia e tempo gasto com emissão de documentos fiscais, para os equipamentos ECF-IF e ECF-PDV.

Após a emissão da Redução Z, todos os totalizadores parciais do ECF são zerados e novas vendas só poderão ser iniciadas a partir das 00:00h do dia seguinte (para este controle o ECF utiliza-se de seu relógio interno). Empresas que operam 24

horas dispõem de um período de tolerância entre 00:00h e 02:00h, para poder realizar a redução Z sem haver problemas de travamento do ECF. Os dados impressos são os mesmos da Leitura X.

2.2.3.3 Registros Totalizadores

Os principais totalizadores de um ECF são o Totalizador Geral e os Totalizadores Parciais, que guardam as informações mais relevantes das operações efetuadas no ECF e que são necessários para os relatórios fiscais gerados para a SEF.

O **Totalizador Geral** ou Grande Total é o acumulador irreversível, destinado a acumular todos os registros de operações sujeita ao ICMS até atingir a capacidade máxima, quando então é automaticamente reiniciado. Seu valor acumulado deve constar na impressão de Leitura X e Redução Z, e também deve estar disponível na fita-detalhe (seja em papel ou eletrônica).

Os **Totalizadores Parciais** são os acumuladores líquidos dos registros de valores efetuados pelo equipamento de uso fiscal, com especificações de situação tributária das mercadorias vendidas, dos serviços prestados, das operações de descontos e cancelamentos ou de operações não sujeitas ao ICMS, redutíveis quando ocorre a emissão da Redução Z.

O Contador de Reduções é um acumulador irreversível incrementado de uma unidade sempre que for efetuada a Redução Z. O Contador de Leitura X também é irreversível e será incrementado em uma unidade quando ocorrer Leitura X.

Caso algum dos totalizadores ou contadores seja perdido, o ECF deve bloquear sua operação automaticamente.

2.2.4 Preços de equipamentos ECF

A tabela 2.2 apresenta os modelos de equipamentos de emissão de cupom fiscal e respectivos preços de venda.[2].

[2]Os modelos e preços foram obtidos em http://www.hardstand.com.br e http://www.zanthus.com.br/

Tabela 2.2: Modelos e preços de equipamentos ECF

FABRICANTE	MODELO	PREÇO
Quattro	Impressora Fiscal EASY IIF 1E	R$ 1.185,00
Daruma	Impressora Fiscal ECF-IF FS345	R$ 1.475,00
Bematech	Impressora Fiscal MP-20 FI II	R$ 1.697,80
Bematech	Impressora Fiscal Térmica MP-2000THFI	R$ 3.170,00
Bematech	Impressora Fiscal MP-40 FI II c/ Impressão de Cheques	R$ 4.168,00
Bematech	Impressora Fiscal Térmica MP 6000 TH FI c/ Impressão de Cheques	R$ 10.810,00

2.3 Cupom Fiscal

O cupom fiscal é o documento fiscal emitido pelo ECF que substitui a nota fiscal para vendas ao consumidor desde que esteja de acordo com as formalidades legais impostas pelo Fisco.

O Cupom Fiscal, entregue ao consumidor, deve conter alguns ítens obrigatórios, que devem ser impressos pelo próprio ECF. Estes ítens são:

- A expressão ”Cupom Fiscal”no topo do cupom;
- Denominação, firma, razão social, endereço e números de inscrição, Estadual e Federal, do estabelecimento que está efetuando a venda;
- Endereço do estabelecimento;
- O número de inscrição no CNPJ identificado pela expressão ”CNPJ”;
- A data de emissão, obtida do relógio interno do ECF;
- Dados de identificação do equipamento, que devem constituir o rodapé do documento;
- Para cada item da venda, os seguintes dados:
  - Número do item registrado;
  - O código do produto ou do serviço;

- A descrição do produto ou do serviço;

- A quantidade comercializada;

- A unidade de medida do produto;

- O valor unitário do produto ou serviço;

- A situação tributária do item registrado, que pode ser feita por meio de códigos ou por extenso, obedecendo a codificação:

a) T - Tributada;

b) F - Substituição Tributária;

c) I - Isenta;

d) N - Não-Incidência;

- Valor total do produto ou serviço, que é a multiplicação da quantidade comercializada pelo valor unitário do produto ou serviço;

- Número e registro de item;
- registro de operação de cancelamento, desconto ou acréscimo, se for o caso;
- O subtotal dos itens e ou operações registradas, se for o caso;
- O total dos itens e das operações registradas, precedida da expressão ”TOTAL”;
- O meio de pagamento utilizado;

Além desses itens, se o ECF for do tipo ECF-PDV ou ECF-IF, outros itens deverão ser adicionados obrigatoriamente ao cupom:

- O código da mercadoria ou serviço de acordo com o a legislação;
- Um símbolo que deve indicar a acumulação do valor do Totalizador Geral. Este símbolo deve ser uniforme por fabricante do respectivo produto;
- O valor acumulado no Totalizador Geral atualizado. Pode-se fazer sua codificação, desde que o algoritmo de decodificação seja fornecido ao fisco, quando este fizer o pedido de uso.

2.3.1 Registro de item

Cada item comercializado deverá possuir um Registro de Item no cupom. Um registro de item é o conjunto de dados referentes a registro, em documento fiscal, de produto comercializado ou de serviço prestado. Ele é composto por:

- Código alfanumérico do produto ou serviço;
- Descrição do produto ou serviço;
- A quantidade comercializada;
- A unidade de medida do produto;
- O valor unitário do produto ou serviço;
- A indicação do símbolo de situação tributária do produto ou serviço;
- O valor total do produto ou do serviço, que é a multiplicação da quantidade comercializada pelo valor unitário do produto ou serviço.

2.4 Conclusão

Os equipamentos de emissão de cupons fiscais devem obedecer as especificações expressas nos diversos convênios ICMS celebrados pelo Conselho de Política Fazendária Nacional (CONFAZ). Há três tipos de equipamentos ECF à escolha dos estabelecimentos comerciais (ECF-MR, ECF-IF e ECF-PDV), embora a grande maioria dos equipamentos ECF atualmente em uso seja o ECF-IF.

O ECF é um dispositivo de hardware controlado por um software interno, chamado Software Básico, que controla todos os registradores internos ao ECF nos quais os valores das vendas e impostos são armazenados.

O ECF apresenta dispositivos de segurança tais como lacre de proteção e fita-detalhe(em papel ou em memória fiscal). No entanto, vários fatores contribuem para a sonegação fiscal do imposto ICMS: há diversas maneiras de fraudar os equipamentos

ECF, a população em geral não está apta a identificar cupons fiscais falsos, o Fisco dispõe de poucos recursos para fiscalizar os estabelecimentos comercias e a legislação em vigor prevê penas leves para os sonegadores. Considerando-se este cenário, novas tecnologias são bem-vindas e necessárias no sentido de ajudar o Estado a combater a sonegação fiscal. No entanto, implementar novas propostas tecnológicas implica, a curto prazo, em custos para os cofres públicos.

Capítulo 3

Fundamentos Criptográficos

3.1 Introdução

Há muito tempo a humanidade tem utilizado a escrita para construir sua história, manifestar a arte, difundir conhecimentos, estabelecer tratados comerciais, registrar as leis que regem a sociedade, enfim, para armazenar toda e qualquer informação de forma eficiente. Por muito tempo a escrita tem sido utilizada sobre diferentes substratos: pedra, argila, papiros. No entanto, o substrato mais conhecido e utilizado é o papel.

Nas últimas décadas a consagrada técnica de escrita sobre o papel tem cedido espaço a uma novidade tecnológica que tem mudado de forma considerável a maneira como a sociedade tem tratado a informação ao longo de sua história: trata-se do surgimento do documento eletrônico. Facilidades de edição, armazenamento, disponibilização e replicação são algumas das vantagens deste sobre o documento convencional em papel.

Graças a outra tecnologia revolucionária que surgiu nas últimas décadas, a Internet, a humanidade tem experimentado um poder de comunicação jamais visto anteriormente. Ao interligar e disponibilizar documentos eletrônicos em uma rede de cobertura mundial, a sociedade passa a escrever um importante marco na história: trata-se da era da informação.

Apesar das vantagens dos documentos eletrônicos sobre os documentos

em papel, ainda existem barreiras para sua adoção de forma a substituir em determinadas situações os documentos em papel.

Este capítulo traz tecnologias que podem ser empregadas para viabilizar a construção de um protocolo criptográfico que atenda aos objetivos propostos para esta dissertação, mencionados no capítulo 1, seção 1.1, página 2.

A seção 3.2 discute as diferenças entre documentos papel e eletrônico e os requisitos de segurança que devem ser atendidos por documentos, independente do meio que o suporte (papel ou eletrônico). A seção 3.3 traz definições acerca de protocolos criptográficos. Técnicas de assinatura digital por delegação são apresentadas na seção 3.4. A seção 3.5 traz definições acerca de criptografia baseada em identidade. Outra técnica criptográfica é apresentada pela seção 3.6, trata-se de criptografia incremental. A seção 3.7 traz padrões de códigos de barras e a seção 3.8 fecha o capítulo.

3.2 Documentos papel e eletrônico

Faz-se necessário definir claramente o significado da palavra documento para que seja possível confrontar as diferenças entre documentos tradicionais em papel e documentos eletrônicos. Segundo o dicionário Houaiss da língua portuguesa [HOU 01], a palavra documento do latim *documentum* apresenta os seguintes significados:

*"**1** Qualquer escrito para esclarecer determinada coisa **1.1** qualquer objeto de valor documental (fotografias, peças, papéis, filmes, construções etc.) que elucide, instrua, prove ou comprove cientificamente algum fato, acontecimento, dito etc. **1.2** atestado, escrito etc. que sirva de prova ou testemunho **2** cada uma das escrituras que se referem à vida de uma pessoa (diz-se esp. de certidão [nascimento, casamento etc.], diploma, título etc.), a um objeto ou a uma instituição **3** qualquer registro escrito **4** qualquer título, declaração, testemunho etc. que tenha valor legal para instruir e esclarecer algum processo judicial."*

Pelas definições acima expostas e considerando-se o levantamento realizado em [DIA 04] pode-se concluir que documentos são registros que podem ter o propósito de: a) ser fonte de informações para fins de consulta, aprendizagem, comprova-

ção científica de fatos; b)ser declaração de fatos ou acontecimentos de natureza jurídica.

Segundo Warnecke [WAR 03], documento em suas diversas definições é independente do meio físico utilizado para a sua divulgação ou guarda. O fato de o documento ser produzido em papel ou qualquer outro meio que sirva para o seu suporte, não o torna mais ou menos autêntico - a determinação precisa de sua origem é que precisa ser levada em consideração. Uma vez comprovado que o documento é proveniente de um autor específico, tem-se a prova legal, passível de sustentação em juízo, de que as idéias e os fatos nele relatados espelham a vontade do autor e a realidade de uma situação.

A dificuldade em abandonar o documento físico de papel para utilizar o documento eletrônico reside em atribuir-lhe segurança comparável à que se obtém nos documentos em papel. Enquanto os documentos tradicionais (impressos ou escritos em papel) podem ser vistos e entendidos pelas pessoas através de seus sentidos tais como a visão e o tato, os documentos eletrônicos não podem. O documento eletrônico nada mais é do que uma seqüência de números binários (isto é, zeros ou uns) que, reconhecidos e traduzidos adequadamente pelo computador, representam uma informação. Além disso, documentos eletrônicos podem ser facilmente alterados, sem deixar vestígios em seu suporte.

O documento em papel tem sua validade jurídica reconhecida, por ser de fácil identificação e em princípio inalterável. Além disso, o papel traz características próprias identificáveis por meio de perícia (idade do papel, composição química da tinta utilizada, etc). Documentos eletrônicos tem sua validade jurídica [CAS 01] garantida pelo artigo primeiro da Medida Provisória 2.200-2 de 28 de junho 2001 [BRA 01b]. A única maneira reconhecidamente segura de atribuir autenticidade e a integridade a documentos eletrônicos é o uso de assinaturas digitais produzidas por criptografia assimétrica [OAB 04].

Considerando-se as características do documento tradicional em papel e as características do documento eletrônico, conclui-se que não é possível substituir a utilização de um pelo outro de forma simples. Júlio Dias [DIA 04] explora a dificuldade em abandonar o documento em papel e o desafio de agregar confiança ao documento eletrônico. Para Júlio Dias é necessária a adoção de técnicas e protocolos criptográficos

que permitam agregar confiança ao documento eletrônico de forma a atender à requisitos de segurança tais como autenticidade (certeza quanto a autoria) e integridade (não adulteração).

3.2.1 Requisitos de segurança

Embora documentos eletrônicos apresentem inúmeras vantagens sobre documentos em papel, encontra-se ainda muita resistência em sua utilização em situações delicadas e que requeiram alto grau de confiança, tais como testamentos, contratos de compra e venda, recibos, etc. Tal resistência pode ser atribuída a questões culturais mas também à dificuldade dos documentos eletrônicos em atender aos nossos requisitos de segurança que podem ser identificados nos documentos em papel.

De acordo com Júlio Dias [DIA 04], através da utilização de técnicas criptográficas busca-se agregar confiança aos documentos eletrônicos de forma a atender aos seguintes requisitos de segurança:

- **Autenticidade**: deve ser possível para quem recebe um documento eletrônico identificar de forma inequívoca o autor do mesmo;

- **Integridade**: deve ser possível verificar que um documento eletrônico não tenha sido indevidamente alterado ao longo de sua existência.

- **Tempestividade**: possibilidade de comprovação da existência do documento em determinado instante no tempo.

- **Irrefutabilidade**: quem produz um documento eletrônico não pode negar tal fato em um momento futuro.

- **Confidencialidade**: somente quem for autorizado pode ter acesso às informações, garantindo-se a privacidade de quem produz o documento eletrônico.

3.3 Protocolos Criptográficos

Criptografia por si só não resolve problemas relacionados à comunicação entre duas entidades. Apesar de oferecer técnicas úteis, é necessário a utilização de protocolos para resolver problemas práticos que envolvam autenticação, segredo e integridade - apenas para citar alguns requisitos de segurança desejáveis.

Um protocolo consiste de uma série de passos, envolvendo duas ou mais entidades, com o objetivo de realizar alguma tarefa [SCH 96]. Os passos necessários e estipulados para um protocolo precisam ser executados seqüencialmente, respeitando-se a ordem de execução prevista. Por definição, considera-se que ao menos duas entidades estejam envolvidas no protocolo, e que este possa alcançar algum objetivo prático - caso estas premissas não sejam atendidas não caracteriza-se um protocolo.

Segundo Bruce Schneier [SCH 96], protocolos possuem ainda as seguintes características:

- As entidades envolvidas no protocolo precisam saber antecipadamente todas etapas que deverão realizar dentro do protocolo;
- As entidades envolvidas no protocolo precisam concordar em seguí-lo a risca;
- Não são permitidas ambigüidades em protocolos.

O protocolo deve ser completo, ou seja, deve prever todas as situações alcançáveis durante sua execução.

Protocolos criptográficos são protocolos que utilizam criptografia. As entidades envolvidas podem ser hostis ou amigáveis, honestas ou desonestas. Geralmente o propósito de um protocolo criptográfico vai além da pura confidencialidade da informação: pode-se compartilhar segredos, realizar operações matemáticas sobre valores desconhecidos, garantir autoria e/ou integridade de informações, entre outros.

Um protocolo criptográfico deve prever quais requisitos de segurança devem ser atendidos durante sua execução: em um protocolo criptográfico de votação digital, anonimato é um requisito fundamental, enquanto em um protocolo criptográfico para transação bancária eletrônica a autenticação deve ser atendida em detrimento do anonimato.

3.4 Esquemas de assinatura digital por delegação

Assinatura digital por delegação é um esquema no qual uma entidade (assinante original) delega sua capacidade de realizar assinaturas digitais para outra entidade (assinante delegado), geralmente através da cessão de algum segredo. A entidade que recebe a delegação passa a assinar digitalmente em nome do assinante original. Pode-se fazer uma analogia a situação na qual uma pessoa delega autorização para outra representá-la em uma situação qualquer através de uma procuração. Uma vez de posse da procuração, o procurador passa a responder pela pessoa em questão, podendo inclusive assinar documentos em nome desta.

De acordo com a literatura [MAM 96, LAL 03], esquemas de assinatura digital por delegação são classificados, de acordo com o tipo de delegação, nas seguintes categorias:

- **Delegação total**: ocorre quando o assinante original entrega sua chave criptográfica privada para o assinante delegado. Neste caso, não há como diferenciar se a assinatura digital foi gerada pelo assinante delegado ou pelo assinante original. Esta é a modalidade de delegação menos utilizada por expor a chave criptográfica privada do assinante original; apesar de ser o assinante delegado quem realiza a assinatura, não há como provar que foi ele de fato, prejudicando o não-repúdio;

- **Delegação parcial**: ocorre quando o assinante original computa uma chave criptográfica σ a partir de sua própria chave criptográfica privada e a entrega para o assinante delegado. Neste caso é possível diferenciar uma assinatura digital gerada pelo assinante original de uma assinatura gerada pelo assinante delegado;

- **Delegação por procuração**: por procuração entende-se um certificado composto por uma mensagem que restringe as autorizações cedidas ao assinante delegado (por exemplo, que tipos de mensagem ele pode assinar e em qual período), além de uma chave criptográfica pública correspondente à chave criptográfica privada do assinante delegado. Este certificado é assinado digitalmente pelo assinante original;

- **Delegação parcial com procuração**: ocorre quando o assinante original computa uma chave criptográfica σ a partir de sua própria chave privada e a entrega ao assinante delegado juntamente com uma mensagem restringindo as autorizações cedidas a este.

- **Delegação parcial descartável**: nesta proposta de Kim [KIM 01] o assinante original entrega parâmetros ao assinante delegado, que utiliza além dos parâmetros sua própria chave privada para construir um par de chaves delegadas. Este par de chaves é utilizado para assinar uma única mensagem, sob pena de revelar o segredo do assinante delegado.

Além das classificações expostas quanto ao tipo de delegação, a literatura [LEE 01] traz as seguintes classificações quanto às características da assinatura realizada por delegação:

- Quanto ao vínculo da assinatura e dos assinantes (original e delegado):
  - **delegação forte**: representa tanto a assinatura do assinante original quanto a assinatura do assinante delegado. Por conter características do assinante delegado, este não pode negar ter realizado a assinatura;
  - **delegação fraca**: representa apenas a assinatura do assinante original. Por não conter características do assinante delegado, este pode negar ter realizado a assinatura;

- Quanto a designação concedida pelo assinante original ao assinante delegado:
  - **delegação designada**: o assinante original especifica explicitamente quem é o assinante delegado;
  - **delegação não designada**: o assinante original não especifica quem será o assinante delegado, apenas quais as restrições para as mensagens a assinar.

Tomando como exemplo uma situação em que Alice, assinante original, entrega sua chave privada diretamente para Beto assinar em nome de Alice, é possível identificar as seguintes características:

- **tipo**: assinatura por delegação total;
- **vínculo**: assinatura por delegação fraca;
- **designação**: assinatura por delegação não designada.

Portanto, quando Beto assina com a própria chave privada de Alice diz-se que esta é uma assinatura digital por delegação total, fraca e não designada.

O primeiro esquema de assinatura digital por delegação foi proposto por Mambo, Usuda e Okamoto [MAM 96] cuja proposta permite que um assinante original delegue autoridade para um assinante delegado que passa a produzir assinaturas digitais em nome do assinante original. A proposta é baseada no problema do logaritmo discreto[1] e oferece três modalidades de assinatura por delegação: a) delegação total; b) delegação parcial; c) delegação por procuração.

A delegação por procuração é baseada no trabalho de Neuman [NEU 93] que propôs um esquema de delegação por procuração buscando aperfeiçoar a autenticação de usuários em redes de computadores. Kim, Park e Won [KIM 97] baseiam-se nos trabalhos de [MAM 96, NEU 93] para criar a delegação parcial de assinatura digital por procuração, na qual o assinante original deriva uma chave delegada σ a partir de sua própria chave privada, utilizando um fator aleatório K. O assinante original cria uma procuração M_w (uma mensagem contendo restrições acerca da realização de assinaturas delegadas) e finalmente entrega para o assinante delegado o conjunto (M_w, σ, K). O assinante delegado verifica a procedência das informações e passa a utilizar a chave σ para realizar assinaturas digitais delegadas. Uma assinatura delegada realizada pelo assinante delegado sobre uma mensagem M_p é composta por: $M_p, assinatura_\sigma(M_p), K, M_w$. A verificação desta assinatura é realizada a partir da chave pública do assinante original, através de simples operações matemáticas realizadas sobre a mesma.

[1]Muitos sistemas criptográficos baseiam-se no problema do logaritmo discreto, definido da seguinte forma: dados um número primo p e números inteiros g, t tais que $0 < g, t < p$, calcular um inteiro s tal que $t = g^s mod_p$. Para números pequenos, é possível calcular s pelo método conhecido como força bruta (atribui-se valores ao s até obter-se o resultado desejado). A medida que os números envolvidos crescem, torna-se computacionalmente inviável encontrar s.

Os requisitos de segurança dos esquemas de assinatura digital por delegação propostos por [MAM 96] e mais tarde estendidos por [LEE 01] são:

- **Verificabilidade**: deve ser possível verificar, a partir da assinatura digital por delegação, a concordância do assinante original com a mensagem assinada;

- **Forte inforjabilidade**: entidades não autorizadas não podem produzir assinaturas digitais por delegação válidas;

- **Forte identificabilidade**: deve ser possível identificar a identidade do assinante delegado que realizou a assinatura por delegação;

- **Forte irretratabilidade**: uma vez gerada a assinatura digital por delegação, o assinante delegado não pode negar que a tenha gerado;

- **Prevenção ao mau uso**: uma chave criptográfica delegada deve ser utilizada somente para gerar assinaturas digitais por delegação.

Um esquema de assinatura por delegação de uso único para agentes móveis é proposto por [KIM 01], baseado em um esquema de assinatura sensível a falha [HEY 93]. Na proposta de Kim et al [KIM 01], o assinante delegado é altamente desencorajado a assinar mais de uma mensagem com as chaves delegadas, sob pena de comprometer sua própria chave privada criptográfica. Isto acontece porque a chave delegada é calculada a partir de parâmetros do assinante original e da própria chave privada do assinante delegado. Caso o assinante delegado assine duas mensagens diferentes com as mesmas chaves delegadas, pode-se montar um sistema de equações a partir do qual é possível descobrir a chave privada do assinante delegado. Outra proposta envolvendo agentes móveis e assinatura digital por delegação é descrita em [dCF 01]. Nesta proposta o assinante original entrega sua chave privada - protegida por um fator de ocultação - a um agente móvel, o qual está apto a assinar em nome do assinante original. No entanto este esquema exige uma terceira entidade confiável que exerce o papel de tabelião, contendo as políticas de restrições das assinaturas delegadas.

Herranz et al [HER 02] propõe um esquema de multi-delegação total, no qual tanto a entidade assinante original quanto a entidade assinante delegada são compostas por conjuntos de assinantes. Os próprios autores revisam sua proposta em 2003 [HER 03], baseados no trabalho de [BOL 03], produzindo um novo esquema de multi-delegação total formalmente seguro. Chen [CHE 02] propõe um esquema de assinatura digital por delegação com a utilização de curvas elípticas possibilitando melhor desempenho para a realização das operações criptográficas; no entanto este esquema sofreu ataques bem sucedidos em [WAN 02]. Lal [LAL 03] propõe um esquema que permite a obtenção de uma mensagem de procuração a partir da assinatura digital por delegação, eliminando-se a necessidade de anexar tal mensagem explicitamente à assinatura gerada. Desta forma poupa-se largura de banda na transmissão e espaço de armazenamento, em contrapartida é necessário maior capacidade de processamento. Os mesmos autores propõem um novo esquema de multi-delegação parcial por procuração em [LAL 02]. Wang [WAN 03] traz um novo esquema de delegação por assinatura, no qual apenas uma entidade previamente escolhida pode fazer a verificação da assinatura digital gerada por delegação. Um esquema de assinatura digital por delegação em anel é proposto por Zhang et al. em [ZHA 03]. Nesta proposta há um conjunto de assinantes delegados, sendo que qualquer um destes pode realizar uma assinatura sem que seja possível distinguir quem dentro deste conjunto realizou a assinatura. Tan et. al [TAN 04a] demonstram que esquemas de delegação de assinatura em conjunto - em um conjunto de n elementos é necessário que t elementos concordem em cooperar para realizar a assinatura - são vulneráveis à determinados tipos de ataques. Os mesmos autores [TAN 04b] apontam fragilidades nos esquemas de assinatura digital por delegação com certificados em ataques de mensagem escolhida, propondo um modelo a prova deste tipo de ataque.

Tanta pesquisa sobre esquemas de assinatura digital por delegação acaba trazendo alguma confusão para o entendimento deste tema, pois a cada nova publicação algum esquema anterior é derrubado e um novo esquema é proposto. São poucos os que não tenham sido derrubados, e mais raros os garantidamente seguros. Boldyreva, Palacio e Warinschi [BOL 03] inovam neste cenário ao propor um esquema de assinaturas digitais por delegação formalmente seguro baseado no trabalho de [KIM 97]. A contribuição

de Boldyreva et al. [BOL 03] é a formalização de aspectos de segurança para esquemas de delegação de assinatura digital; após sutis mudanças em um conhecido esquema de delegação [KIM 97] obtiveram um esquema de delegação cuja segurança é justificada através de provas formais de teoremas.

Um resumo das propostas encontradas na literatura acerca de esquemas de assinatura digital por delegação classificadas de acordo com o tipo de delegação é apresentado pela tabela 3.1.

Tabela 3.1: Esquemas de assinatura digital por delegação

DELEGAÇÃO	ESQUEMAS PROPOSTOS
Total	Mambo et al. [MAM 96], Ferreira et al. [dCF 01]
Parcial	Mambo et al. [MAM 96]
Por procuração	Mambo et al. [MAM 96], Tan et al. [TAN 04b]
Parcial por procuração	Kim et al. [KIM 97], Lal et al. [LAL 03], Wang [WAN 03], Zhang et al. [ZHA 03], Lal et al. [LAL 02], Boldyreva et al. [BOL 03]
Descartável	Kim et al. [KIM 01]

Dentre todos os esquemas de assinatura digital por delegação disponíveis na literatura, o que parece mais adequado às necessidades do protocolo proposto nesta dissertação é o esquema de Kim et al. [KIM 01]. Por este motivo, tal esquema será descrito a seguir.

3.4.1 Esquema de assinaturas digitais por delegação parcial descartável

O esquema de assinatura por delegação parcial descartável inicialmente proposto por Kim et al [KIM 01] caracteriza-se pelo fato do assinante delegado não poder assinar duas mensagens diferentes com as chaves delegadas. Um possível cenário para este esquema caracteriza-se por um agente móvel pesquisando preços de passagens aéreas na Internet. Se o agente encontrar uma proposta que atenda às expectativas do consumidor, o agente entrega parâmetros para que o próprio vendedor das passagens aéreas realize uma assinatura digital em nome do consumidor sobre um pedido de compra . Este é um caso típico de delegação de autoridade para realização de assinatura digital. A inovação

da proposta reside na garantia de que a assinatura por delegação ocorrerá uma única vez. Conforme mencionado anteriormente, o assinante delegado é altamente desencorajado a assinar mais de uma mensagem com as chaves delegadas sob pena de comprometer sua própria chave privada.

A proposta consiste das seguintes etapas:

1. O assinante original calcula parâmetros que servirão para a geração das chaves delegadas. Estes parâmetros são derivados da chave privada do assinante. Entretanto, não é possível obter a chave privada do assinante a partir destes parâmetros. O assinante entrega ao agente móvel os parâmetros calculados, além de uma mensagem com restrições quanto a delegação concedida ao agente. O agente móvel navega livremente pela rede até encontrar o sítio especificado pelo assinante original;

2. Chegando ao servidor de destino, o agente móvel entrega os parâmetros para que as chaves de delegação possam ser calculadas pelo próprio servidor, baseando-se nos parâmetros do assinante original e na chave privada do servidor. Após gerar as chaves delegadas, o servidor realiza duas assinaturas delegadas sobre uma mesma mensagem utilizando-se das chaves delegadas calculadas. Este par de assinaturas, a mensagem e os pares de chaves calculadas são entregues ao agente móvel;

3. Chegando ao assinante original, o agente móvel entrega os valores recebidos do servidor. O assinante verifica a procedência dos dados recebidos e finalmente verifica o par de assinaturas recebidas.

3.5 Sistemas Criptográficos baseados em identidade

Esta seção traz características da tecnologia de criptografia baseada em identidade: a estrutura necessária para sua implementação, as possíveis formas de utilização além das vantagens e desvantagens desta tecnologia.

3.5.1 Introdução

Os Sistemas criptográficos baseados em identidade oferecem uma alternativa ao tradicional modelo de infra-estrutura de chave pública (ICP), no qual é necessário haver uma complexa estrutura de Autoridades de Certificação (AC) e Autoridades de Registro (AR) para garantir a emissão de certificados digitais. Em sistemas criptográficos baseados em identidade o processo de obtenção de pares de chaves é simplificado: qualquer string pode ser uma chave criptográfica pública, a partir da qual uma entidade Geradora de Chaves Privadas (GCP) gera a chave privada correspondente. Este modelo apresenta vantagens e desvantagens e será descrito a seguir.

Em 1984 Shamir [SHA 84] propôs o conceito de criptografia baseada em identidade. Neste novo esquema, a chave pública do usuário pode ser um texto arbitrário, como por exemplo o nome completo ou o endereço de correio eletrônico. O objetivo desta proposta é facilitar o uso da criptografia, eliminando a necessidade de utilização de diretórios e certificados digitais, reduzindo a complexidade e o custo operacional da manutenção de uma infra-estrutura de chaves públicas (ICP) [BAE 04]. Além disso, chaves criptográficas tradicionalmente são compostas por centenas de dígitos, enquanto em sistemas criptográficos baseados em identidade uma chave pública pode ser um texto muito mais simples e significativo, facilitando sua memorização.

Graças à criptografia baseada em identidade dois usuários quaisquer podem se comunicar de forma segura sem a necessidade de troca de segredos ou utilização de certificados digitais. Em contrapartida, há a necessidade de uma entidade confiável chamada GCP, cuja principal função é gerar uma chave privada baseada em uma identidade (qualquer string) e seus próprios parâmetros públicos (a própria chave criptográfica pública do GCP). Uma vez gerada a chave privada, esta é transmitida ao usuário que a solicitou através de um canal de comunicação seguro. A utilização das técnicas cifrar/decifrar e assinar/verificar através de criptografia por identidade são apresentadas na seção 3.5.2.

3.5.2 Utilização de sistemas criptográficos baseado em identidade

De acordo com Gagne [GAG 03], o processo de cifrar/decifrar com criptografia baseada em identidade é composta por quatro etapas:

1. **Configuração**: o GCP (gerador de chaves privadas) cria sua chave mestra (privada) e sua respectiva chave pública. A chave pública é utilizada como parâmetro do sistema, e é disponibilizada para todos os usuários, enquanto a chave mestra é mantida em sigilo;

2. **Extração da chave privada**: o usuário Beto autentica-se perante o GCP e obtém uma chave privada associada com sua identidade;

3. **Cifração**: utilizando-se da identidade de Beto e a chave pública do GCP, Alice cifra a mensagem M obtendo o criptograma C.

4. **Decifração**: ao receber o criptograma C de Alice, Beto decifra-o utilizando sua chave privada e recupera a mensagem M original.

De forma equivalente, o processo de assinar/verificar mensagens utiliza-se das seguintes etapas:

1. **Configuração**: o GCP (gerador de chaves privadas) cria sua chave mestra (privada) e sua respectiva chave pública. A chave pública é utilizada como parâmetro do sistema, e é disponibilizada para todos os usuários, enquanto a chave mestra é mantida em sigilo;

2. **Extração da chave privada**: o usuário Alice autentica-se perante o GCP e obtém uma chave privada associada com sua identidade;

3. **Geração da assinatura**: utilizando-se da sua chave privada, Alice cria uma assinatura σ sobre a mensagem M.

4. **Verificação da assinatura**: ao receber σ e a mensagem M de Alice, Beto verifica a assinatura σ utilizando-se da identidade de Alice e a chave pública do GCP.

Além de simplificar a utilização das técnicas criptográficas cifrar/decifrar e assinar/verificar, há outras vantagens na utilização de sistemas criptográficos baseados em identidades:

- Não há necessidade de um diretório de chaves públicas;
- Qualquer entidade que possua um par de chaves padrão pode fazer o papel de GCP. Esta característica ameniza a necessidade de uma estrutura complexa para o gerenciamento de chaves públicas, envolvendo entidades externas como AC e AR;
- Pode-se enviar mensagens cifradas para uma entidade que ainda não tenha chaves criptográficas;
- Em uma comunicação entre Alice e Beto, não é necessário obter certificados digitais.

Apesar das vantagens expostas, os sistemas criptográficos baseados em identidades são alvos de sérias críticas. Jon Callas [CAL 04] expõe algumas delas:

- Considerando que qualquer texto pode ser uma identidade (chave pública), um texto digitado incorretamente também é uma chave válida. Beto acidentalmente pode ter cifrado uma mensagem para **Alicia** ao invés de **Alice**, e neste caso não há como Alice ter acesso à mensagem;
- O GCP tem conhecimento das chaves privadas geradas. Isso implica que o GCP precisa ser uma entidade confiável neste modelo, de forma análoga à confiança depositada em uma AC na estrutura de ICP convencional;
- Todas as chaves privadas criadas pelo GCP são baseadas em sua própria chave mestra. Caso esta chave seja comprometida, todas as chaves privadas geradas também estarão comprometidas.

3.6 Criptografia Incremental

Esta seção traz características de uma tecnologia cujo objetivo é aumento de desempenho durante o processamento de conhecidas técnicas criptográficas, tais como como cifrar/decifrar e assinar/verificar. Considera-se que tais procedimentos sejam aplicados a documentos eletrônicos que sofram pequenas alterações em seus conteúdos ou que apresentem uma estrutura padrão, havendo pouca variação de conteúdo.

Uma das principais características de documentos eletrônicos é a facilidade de edição. Considerando um documento eletrônico que tenha sido submetido a uma operação de assinatura digital e/ou cifragem e venha sofrer alguma alteração, seria mais eficiente atualizar o resultado do procedimento criptográfico (assinatura digital e/ou cifragem) apenas sobre as alterações feitas no documento ao invés de refazer o procedimento sobre todo o documento novamente.

Tomando como exemplo a assinatura digital de um documento, o objetivo da criptografia incremental é ter uma assinatura que seja de fácil atualização a partir das modificações realizadas sobre o documento em questão. Por exemplo, assinando uma mensagem M temos como resultado uma assinatura σ. Ao realizar alterações sobre M (inclusão de um novo bloco de texto, por exemplo) tem-se a mensagem M'. Seria interessante poder atualizar a assinatura σ para a assinatura σ' em tempo proporcional à quantidade de modificações feitas a M para se obter M', ao invés de simplesmente refazer a assinatura σ' de M'.

Para atingir tais objetivos um novo esquema criptográfico é proposto por [BEL 94], trata-se da Criptografia incremental. Em sua proposta, Bellare et al. [BEL 94] utiliza-se de uma função resumo criptográfica de atualização e de um algoritmo de assinatura de atualização para obter um procedimento de assinar/verificar incremental, ou seja, aplicado somente às alterações do documento ao invés do documento completo.

3.7 Código de Barras

Esta seção apresenta a tecnologia de impressão de códigos de barras sobre papel, necessária ao protocolo proposto nesta dissertação. Serão apresentados os principais padrões de código de barras disponíveis na literatura e algumas de suas características.

3.7.1 Introdução

A impressão de código de barras é uma representação visual que possibilita obter informações do papel de forma automatizada. Inicialmente só haviam códigos de barras expressos através de linhas paralelas de largura variável intercaladas por espaços em branco. Atualmente, há uma grande variedade de padrões de código de barras disponíveis: pontos, círculos concêntricos, matrizes contendo elementos de formas geométricas e outras representações gráficas [WIK 04].

3.7.2 Tipos de código de barras

Códigos de barras podem ser lidos por scanners óticos conhecidos como leitores de código de barras ou se o código estiver em uma imagem digital pode ser reconhecido por software apropriado. De acordo com o padrão de representação de informações, os códigos de barra são classificados em três categorias:

- **Linear**: primeiro padrão de código de barras a surgir, esta categoria representa informações através de linhas verticais de larguras diferentes, intercaladas por espaços em branco, conforme ilustrado na Figura 3.1.

  Portanto, a variação da informação ocorre na linha horizontal, Graças a esta característica, este padrão de código de barras é otimizado para leitura pois o feixe de laser do leitor ótico precisa ”cortar”o código impresso uma única vez. Em contrapartida, este padrão apresenta baixa capacidade para representar informações. O código de barras linear que apresenta maior capacidade de representar informações

Figura 3.1: Código de barras linear: As informações são representadas por linhas verticais de larguras diferentes, intercaladas por espaços em branco.

é o padrão ”EAN UCC Reduced Space Symbology” [Ide 04], o qual comporta até 74 caracteres numéricos.

- **Bidimensional**: este padrão representa uma evolução dos códigos de barra lineares, pois representa maior quantidade de informações. Ao invés de barras separadas por espaços em branco, este padrão é formado por uma grade contendo formas geométricas diversas (quadrados, círculos, pontos). A Figura 3.2 traz os seguintes exemplos de códigos de barras bidimensionais:

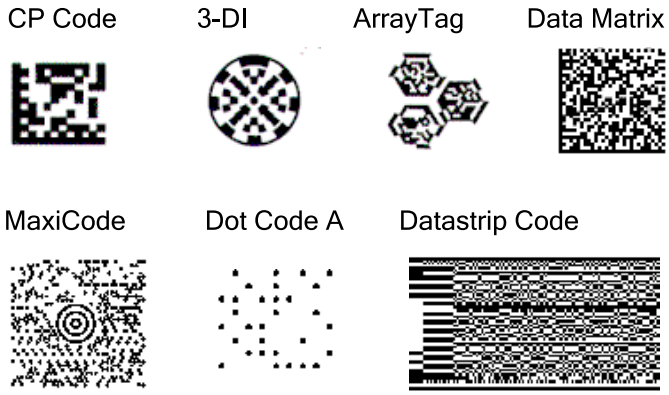

Figura 3.2: Código de barras bidimensional: grade contendo formas geométricas capaz de armazenar grande quantidade de informações. No entanto, leitores óticos convencionais não reconhecem estes códigos.

CP Code: código de barras proprietário composto por uma matriz de quadrados com marcas em branco em forma de ”L”;

3-DI: código de barras proprietário composto por pequenos símbolos circulares. Indicado para identificação de instrumentos cirúrgicos metálicos;

ArrayTag: este padrão é proprietário e é composto por símbolos hexagonais com bordas complementares. Este código de barras é otimizado para leitura a distância (pode ser lido a uma distância de até 50 metros) e ambientes com variações luminosas;

Data Matrix: código de barras proprietário, projetado para armazenar grande quantidade de informações em espaço reduzido. É composto por símbolo em formato quadrado, sendo que cada símbolo pode representar entre 1 e 500 caracteres alfanuméricos. Se o símbolo for reduzido ao seu tamanho mínimo ($1mm^2$), teoricamente pode-se obter até 50.000 caracteres alfanuméricos por cm^2. Em contrapartida, são requeridos equipamentos de alta precisão para impressão e leitura deste código de barras;

MaxiCode: código proprietário composto por cadeias de hexágonos interligados e uma figura circular ao centro para direcionar o leitor ótico que faz sua leitura.

Dot Code A: conhecido por código Philips, é composto por combinações de pontos e é utilizado para identificação única de objetos. Possibilita bilhões de possíveis diferentes combinações;

DataStrip Code: este foi o primeiro código de barras bidimensional, formado por pequenas áreas retangulares brancas e pretas, conhecidas por DiBits. Este código é proprietário e pode representar grande quantidade de informações, porém, sua leitura só pode ser feita por leitores produzidos pela empresa que o desenvolveu.

Leitores óticos convencionais utilizam-se de um estreito feixe de laser horizontal para capturar informações de códigos de barras. São indicados para leitura de código de barras linear, porém incapazes de capturar informações de código de barras em padrão bidimensional devido a geometria irregular deste padrão. Para obter informações representadas por um código de barras bidimensional é necessário fazer uma varredura do mesmo através de dispositivos para captura de imagem.

- **Empilhado**: este padrão é um meio termo entre os padrões linear e o bidimensional. O padrão de código de barras empilhado concilia o que há de melhor nos padrões

anteriores: tem capacidade de armazenar grande quantidade de informações (pode armazenar milhares de caracteres alfanuméricos) e apresenta facilidade de leitura [2]. O código de barras empilhado consiste de códigos lineares repetidos verticalmente em múltiplas linhas. A Figura 3.3 traz os seguintes exemplos de códigos de barras empilhados:

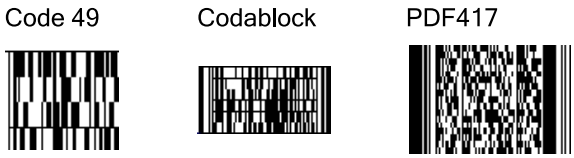

Figura 3.3: Código de barras empilhador: As informações são expressas por códigos de barra lineares repetidos verticalmente em n linhas.

Code 49: este código é de domínio público e é composto por 2 a 8 linhas de código de barras lineares empilhadas, cada um delas composta por 18 barras e 17 espaços;

Codablock: em sua última versão, este código de barras é composto por 2 a 44 linhas de código de barras lineares empilhadas, cada uma delas comporta até 62 símbolos. O número de caracteres representado por este código de barras é variável de acordo com as dimensões do mesmo. Este padrão é utilizado em bancos de sangue na Alemanha para identificação de sangue;

PDF417: este código de barras é de domínio público, composto por 3 a 90 linhas de código de barras lineares empilhados. Pode representar até 1860 caracteres alfanuméricos ou 2710 números;

A tabela 3.2 traz exemplos dos códigos de barras mais comuns em cada uma das três categorias existentes.

Dentre os tipos de códigos de barras disponíveis na literatura, o que atende de forma mais satisfatória aos requisitos do protocolo proposto nesta dissertação

[2] embora o padrão de código de barras empilhado seja de fácil leitura, o padrão de código de barras que possibilita a leitura de suas informações de forma mais otimizada é o código de barras linear.

Tabela 3.2: Padrões de códigos de barra.

LINEAR	EMPILHADO	BIDIMENSIONAL
Plessey	Codablock	3-DI
UPC	Code 16k	ArrayTag
EAN-UCC	Code 49	Aztec Code
Codabar	PDF417	CP Code
Interleaved 2 of 5	Data Matrix	QR Code
Code 39	Micro PDF417	DataStrip Code
Code 93		Dot Code A
Code 128		Snowflake Code
Code 11		UltraCode

é o código de barras empilhado PDF417, cujas características são apresentadas na seção 3.7.3.

3.7.3 PDF417

O padrão de código de barras PDF417 pertence a categoria de código de barras empilhado, portanto apresenta grande capacidade de representação de informações. Sua estrutura é composta por várias linhas (mínimo de 3, máximo de 90), sendo que cada uma destas é um código de barras linear reduzido, como pode ser visto na Figura 3.3.

O processo de codificação de informações para o formato PDF417 consiste de duas etapas: primeiro, os dados são convertidos para palavras-código (codificação de alto nível); em seguida as palavras-código são convertidas para padrões de barras e espaços (codificação de baixo nível). Cada palavra-código é representada por 4 barras e 4 espaços em branco, sendo que o comprimento total de cada palavra-código é 17 vezes a largura mínima que uma barra pode assumir. Destas características deriva-se o 417 presente no nome do código. O processo de leitura de informações representadas pelo código de barras PDF417 é realizado com o uso de dispositivos físicos apropriados, ilustrados pela Figura 3.4. O leitor ótico modelo ”P300 PRO”, ilustrado na Figura 3.4, custa US$ 1.120,00 [3].

As características do código de barras padrão PDF417 [WIK 04] são:

[3] valor obtido do sítio web http://www.okey.com.br em novembro de 2004.

Figura 3.4: Leitores óticos modelo ”P300 PRO”e ”DS6600”[TEC 04]. Estes dispositivos oferecem facilidade e rapidez de leitura para código de barras padrão PDF417.

- Capacidade de armazenamento de até 2710 números ou 1860 caracteres alfanuméricos;
- Detecção e correção de erros;
- Rapidez de leitura comparável aos padrões de código de barras lineares;
- Facilidade de leitura: o código pode ser lido de baixo para cima ou de cima para baixo. Não é necessário que o leitor varra o código de forma horizontal;
- Formato de domínio público.

3.8 Conclusão

Documentos eletrônicos possuem características muito diferentes dos documentos tradicionais em papel. Através da utilização de protocolos e técnicas criptográficas é possível compensar algumas limitações de documentos eletrônicos, agregando-se confiança a estes. Desta forma documentos eletrônicos passam a atender a requisitos de segurança atualmente atendidos por documentos tradicionais em papel e viabilizam sua utilização em situações onde até então apenas documentos em papel eram aceitos.

Criptografia por si só não resolve problemas relacionados à comunicação entre duas entidades(autenticação, integridade, irretratabilidade). Nestas situações o mais indicado é a utilização de um protocolo (seqüencia de passos bem definidos executados

rigorosamente pelas entidades envolvidas) aliado a técnicas criptográficas: desta forma é estabelecido um protocolo criptográfico.

Através de assinatura digital por delegação uma entidade recebe delegação para produzir assinaturas digitais em nome de outra entidade. Há diversos esquemas de assinatura digital disponíveis na literatura, categorizados em: delegação total, delegação parcial, delegação por procuração, delegação parcial por procuração e delegação descartável.

Uma alternativa a infra-estruturas de chaves públicas convencionais pode ser obtida com uso de criptografia baseada em identidade. Desta forma, reduz-se a complexidade da geração e gerenciamento de chaves públicas, pois como visto na seção 3.5 qualquer string pode ser utilizada como chave pública, a partir da qual uma entidade Geradora de Chaves Privadas (GCP) gera a chave privada correspondente. Em contrapartida, o GCP tem acesso às chaves privadas geradas.

A Criptografia incremental traz ganho de desempenho em operações criptográficas simples, tais como cifrar/decifrar e assinar/verificar, quando aplicadas a documentos eletrônicos que sofram poucas alterações.

Código de barras é uma forma de representação visual que possibilita obter informações do papel de forma automatizada, através de utilização de dispositivos chamados leitores óticos. Há três tipos de código de barras: linear, bidimensional e empilhado. Em geral, a quantidade de informações representadas e a facilidade de leitura das mesmas são características inversamente proporcionais nos diversos padrões de código de barras existentes.

Capítulo 4

Protocolo ECFV

4.1 Introdução

Neste capítulo é proposto o protocolo criptográfico ECFV que viabiliza a emissão de documentos fiscais virtuais, em uma operação envolvendo a Secretaria de Estado da Fazenda (SEF), o estabelecimento comercial (EC) responsável pela venda, um centro de informática (CI), subordinado à SEF, responsável pelo processamento dos dados e o consumidor final (C).

Há desafios tecnológicos que precisam ser solucionados para a implementação do protocolo proposto por esta dissertação; tais desafios são caracterizados e possíveis soluções são apresentadas ao longo deste capítulo. Inicialmente, é apresentada a infra-estrutura tecnológica necessária para a implementação do protocolo ECFV na seção 4.2. As entidades do protocolo e suas respectivas responsabilidades são apresentadas na seção 4.3. Na seção 4.4 é apresentado um cenário que contextualiza o protocolo ECFV. Uma proposta alternativa ao cupom fiscal impresso por equipamento ECF, o cupom fiscal virtual (CFV) é descrito em detalhes na seção 4.5. Finalmente, o protocolo Emissor de Cupom Fiscal Virtual é apresentado na seção 4.6; sua formalização ocorre na seção 4.7, através de utilização de Diagrama de Transição de Estados (DTE), mais especificamente uma Rede de Petri [IEE 89]. A seção 4.8 fecha o capítulo.

4.2 Infra-estrutura necessária para o Protocolo ECFV

A discussão levantada no capítulo 3, seção 3.2, página 32 remete à necessidade de utilização de assinaturas digitais sobre arquivos eletrônicos para que estes tenham alguma confiança e valor jurídico agregados.

É necessário haver uma infra-estrutura de chaves públicas (ICP) para gerenciar os certificados digitais utilizados nos procedimentos de assinatura digital de documentos. Para a implementação de uma ICP, faz-se necessário a adoção de um módulo de segurança criptográfico (MSC) para proteger a chave privada da AC-Raiz [MAR 04].

Outros requisitos de infra-estrutura requeridos pelo protocolo ECFV são:

- as entidades envolvidas precisam estabelecer um canal de comunicação no mínimo esporádico para troca de mensagens;
- é necessário haver um aplicativo a ser executado pelos estabelecimentos comerciais para criação do cupom fiscal virtual;
- o centro de informática precisa ter poder de processamento suficiente para centralizar o fluxo de mensagens trocadas na execução do protocolo, além de armazenar e disponibilizar informações processadas.

4.3 Entidades do protocolo ECFV

Em um protocolo criptográfico, duas ou mais entidades precisam relacionar-se, através do estabelecimento de um canal de comunicação para realizar troca de mensagens. Além disso, as entidades envolvidas precisam saber previamente quais os passos a serem seguidos e os possíveis estados alcançados pela execução do protocolo. As seguintes entidades fazem parte do protocolo ECFV:

- **Secretaria de Estado da Fazenda (SEF)**: entidade governamental responsável por arrecadar e gerenciar o imposto ICMS. É a SEF que assina os cupons fiscais virtuais

gerados. Além disso, a SEF tem acesso às informações processadas pelo Centro de informática (CI).

- **Estabelecimento Comercial (EC)**: Empresa devidamente cadastrada junto a SEF, autorizada a emitir documentos eletrônicos fiscais. É responsável por repassar à SEF todas as informações de vendas realizadas.

- **Centro de informática (CI)**: Entidade subordinada à SEF, responsável por disponibilizar o aplicativo ECFV, receber os cupons fiscais gerados e manipulá-los de forma a disponibilizar à SEF as informações necessárias. O CI pode estar localizado na própria SEF.

- **Consumidor (C)**: Entidade de papel fundamental dentro do protocolo. A exemplo do que ocorre atualmente, é o consumidor final quem será responsável por exigir seu cupom fiscal após a compra de produtos ou serviços. Além disso, o protocolo ECFV traz uma inovação: o consumidor estará apto a conferir a autenticidade do cupom fiscal impresso de forma automatizada, submetendo o código de barras impresso no cupom fiscal a um leitor ótico.

4.4 Cenário proposto

O Protocolo ECFV propõe-se a alterar o atual cenário de transações comerciais para venda de produtos e serviços a consumidores. Atualmente a comunicação entre Estado, comércio e consumidores apresenta deficiências que dificultam o controle da arrecadação de tributos devidos aos cofres públicos. No sentido de diminuir esta deficiência de comunicação, o protocolo criptográfico ECFV propõe o cenário ilustrado pela Figura 4.1 para realização de transações comerciais.

No cenário ilustrado pela Figura 4.1 o EC gera o cupom fiscal virtual a partir de uma plataforma computacional convencional (etapa 1) e passa a ter uma forte ligação com a SEF, transmitindo informações referentes às suas vendas em tempo real (etapa 2). Os valores do cupom fiscal virtual são contabilizados pela SEF, que produz

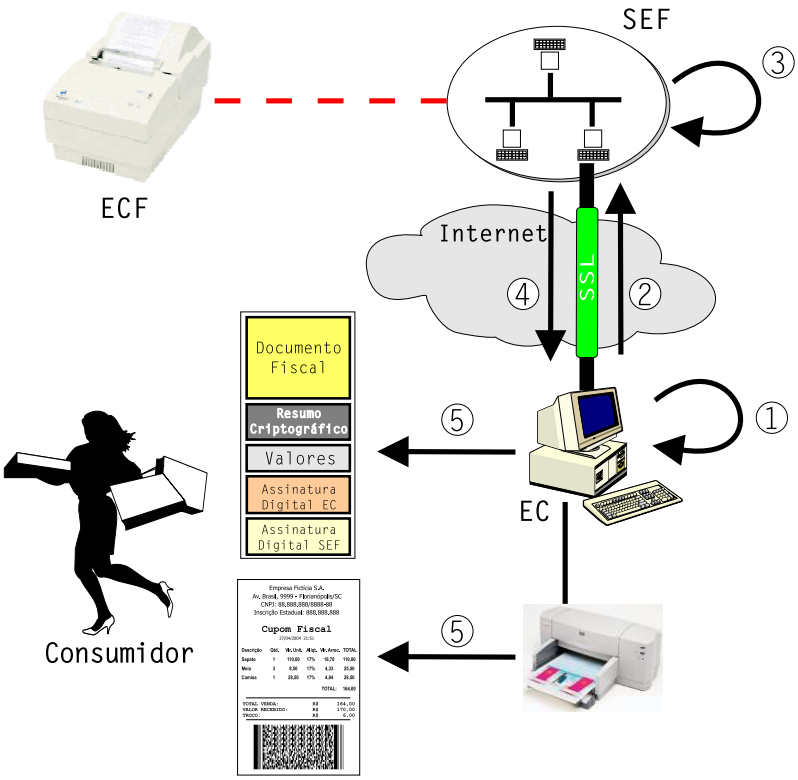

Figura 4.1: Cenário proposto para utilização do Protocolo ECFV

uma assinatura digital sobre o cupom fiscal (etapa 3) e o devolve ao EC (etapa 4) para ser entregue ao consumidor em meio digital e/ou meio papel (etapa 5). A impressão do documento fiscal pode ser feita por uma simples impressora.

Este cenário apresentado pela Figura 4.1 serve como motivação e contextualiza a proposta do protocolo criptográfico ECFV, a qual será tratada em detalhes na seção 4.6.

O equipamento ECF-IF presente na Figura 4.1 e sua ligação com a SEF através da linha tracejada representa o atual método de controle do Estado sobre as transações comerciais de venda a consumidores. A linha que liga o ECF-IF à SEF está tracejada para enfatizar que tal dispositivo não permite comunicação em tempo real com a SEF; ao invés disso utilizam-se métodos burocráticos de envio de documentos fiscais (ver capítulo 2, página 14) periodicamente.

4.5 O Cupom Fiscal Virtual

Esta seção descreve características do documento fiscal virtual em meio digital e impresso em papel. Inicialmente, o cupom fiscal virtual (CFV) é um documento eletrônico e sofre operações de edição (extração de valores) e criptográficas (assinatura digital e verificação). Após estar completo, o cupom fiscal é impresso em papel com características visuais que permitem sua leitura de forma automatizada.

4.5.1 Introdução

O cupom fiscal virtual (CFV) é gerado pelo EC em meio digital através da utilização de um aplicativo disponibilizado pelo CI. No entanto, as informações das vendas realizadas pelo EC são estratégicas e não devem ser tornadas públicas [1]. Portanto, embora o CFV contenha todas as informações da venda realizada ao consumidor, apenas parte destas informações, os valores totais agrupados por alíquota de imposto e um resumo criptográfico do documento fiscal completo, são repassadas às entidades CI e SEF. Desta forma, protege-se a privacidade do EC quanto às suas informações. Em caso de suspeita de fraude, o Estado pode exigir o CFV completo ao EC, calcular o resumo criptográfico do mesmo e comparar com o resumo criptográfico enviado previamente pelo EC. Caso a comparação falhe, constata-se uma tentativa de sonegação fiscal.

Para que seja possível atender aos requisitos expostos no parágrafo anterior, a estrutura do CFV é ilustrada pela Figura 4.2. A geração do CFV é explicada na seção 4.5.2.

4.5.2 Geração do Cupom Fiscal Virtual

A tecnologia XML (*extensible markup language* ou linguagem de marcação extensível) é uma meta linguagem de marcação desenvolvida pela W3C [CON 05] que define um padrão para representação e transferência de dados em redes de comuni-

[1] exceto quando o Estado as solicita para fiscalização por meio de intervenção técnica de fiscais autorizados

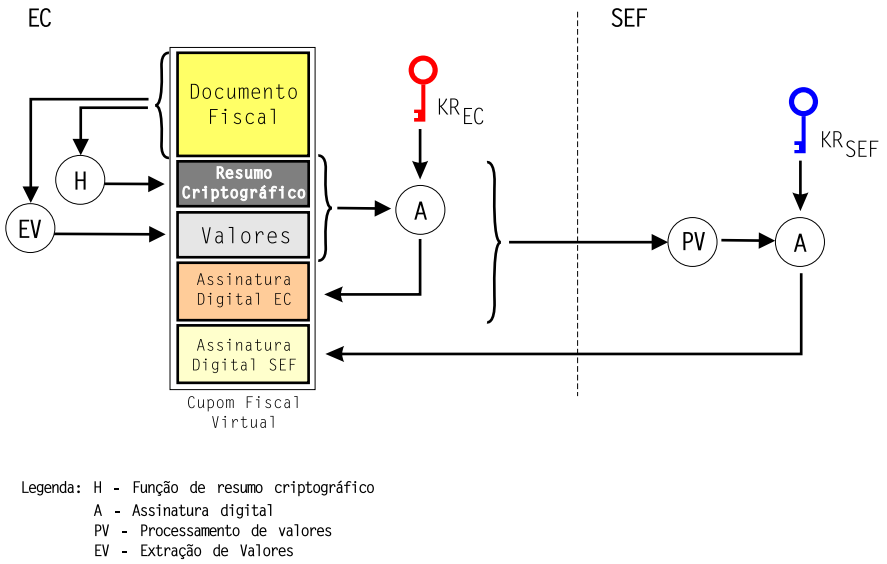

Figura 4.2: Cupom fiscal virtual é composto pelo documento fiscal (XML), os valores da venda categorizados por alíquota de imposto, além das assinaturas do EC e da SEF

cação. A geração de documentos XML é regida por um conjunto de regras gramaticais conhecida por DTD (*Document Type Definition* ou Definição de Tipo de Documento). Após gerado, o documento pode ser validado para seu DTD com a utilização de um analisador léxico.

Pelas características apresentadas pela tecnologia XML o cupom fiscal virtual (CFV) será gerado neste formato. O DTD para geração do CFV é apresentado na Figura 4.3.

A Figura 4.4 ilustra um exemplo de documento XML gerado de acordo com o DTD especificado na Figura 4.3. No entanto, a geração do documento XML é apenas uma etapa da geração do cupom fiscal virtual. A estrutura completa do cupom fiscal virtual ilustrada pela Figura 4.2 é formada pelos procedimentos listados a seguir:

1. EC gera um documento em formato XML contendo todos os ítens da venda, além de informações do próprio EC;
2. A partir do documento fiscal são extraídos os valores referentes à venda, agrupados por alíquota de imposto;
3. EC gera um resumo criptográfico do documento fiscal;

```
<!ELEMENT documentoFiscal(item+, totalVenda, totalImposto, formaPagamento)>
<!ELEMENT item (aliquota, descricao, precoUnitario)>
<!ATTLIST item numero CDATA #REQUIRED>
<!ATTLIST item codigo CDATA #REQUIRED>
<!ATTLIST item quantidade CDATA #REQUIRED>
<!ELEMENT aliquota EMPTY>
<!ATTLIST aliquota id CDATA #REQUIRED>
<!ATTLIST aliquota valor CDATA #REQUIRED>
<!ELEMENT descricao (#PCDATA)>
<!ELEMENT precoUnitario EMPTY>
<!ATTLIST precoUnitario valor CDATA #REQUIRED>
<!ATTLIST precoUnitario imposto CDATA>
<!ELEMENT totalVenda EMPTY>
<!ATTLIST totalVenda valor CDATA #REQUIRED>
<!ELEMENT totalImposto EMPTY>
<!ATTLIST totalImposto valor CDATA #REQUIRED>
<!ELEMENT formaPagamento EMPTY>
<!ATTLIST formaPagamento id CDATA #REQUIRED>
```

Figura 4.3: DTD para geração do documento fiscal virtual em formato XML

4. EC envia os valores calculados nos ítens **2** e **3**, assinados digitalmente pelo próprio EC, para a SEF;
5. SEF contabiliza os impostos sobre os valores informados. Em seguida, assina digitalmente o conjunto de informações recebidas e as devolve para o EC.

Gerado o cupom fiscal virtual, o consumidor pode optar por recebê-lo em formato digital (armazenando-o em um notebook ou outro dispositivo móvel), em formato impresso ou em ambos formatos. Pelo fato do CFV ser um documento eletrônico, apresenta características e problemas levantados no capítulo 3, seção 3.2, página 32. Deve-se considerar ainda que o CFV está digitalmente assinado, portanto é desejável que sua impressão em papel traga elementos que transponham para o papel suas características eletrônicas, especificamente sua assinatura digital. Uma possível maneira de obter tais característica na impressão do documento fiscal é tratada na seção 4.5.3.

4.5.3 Impressão do Cupom Fiscal Virtual

Como visto na seção anterior, o cupom fiscal virtual (CFV) pode ser entregue ao consumidor em meio digital e/ou impresso. A impressão do CFV deve conter os elementos descritos no capítulo 2, seção 2.3, página 27, exceto as informações do

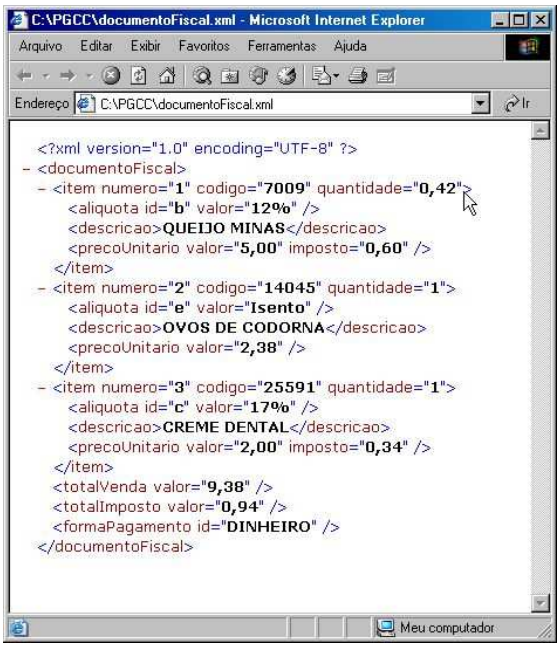

Figura 4.4: Documento fiscal em formato XML

equipamento de impressão fiscal. Uma sugestão de leiaute para a impressão do CFV é apresentada pela Figura 4.5.

É necessário agregar características à impressão do CFV que possibilitem identificar sua assinatura digital. Para tanto, vislumbra-se a inclusão de dois códigos de barras no rodapé do CFV impresso: enquanto um código de barras contém as informações dos itens da venda realizada o outro contém as seguintes informações:

- Assinatura digital da SEF;
- Valor total da venda realizada;
- Data da realização da venda (expressa em milisegundos [2]);
- Identificação do estabelecimento comercial que realizou a venda.

Considerando-se a quantidade de informações que devem ser representadas e os padrões de código de barras existentes, conforme levantamento do capítulo 3, seção 3.7, página 47, optou-se por adotar o padrão de código de barras empilhado,

[2]a data é armazenada é o tempo em milisegundos que se passou desde 1/1/1970 00:00:00. Este padrão confere maior precisão e facilidade de armazenamento

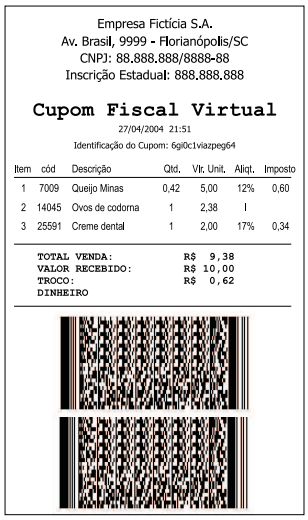

Figura 4.5: Leiaute sugerido para impressão do cupom fiscal virtual. O primeiro código de barras contém a assinatura digital emitida pela SEF, além da data da venda, o valor total e identificação do estabelecimento comercial. O segundo código de barras contém informações da venda. Além disso, é impresso um código de identificação alfanumérico sobre o cupom fiscal, para possibilitar consultas através da Internet.

categoria PDF417, devido às suas características: grande capacidade para representar informações (até 2710 caracteres numéricos ou 1860 alfanuméricos), praticidade de leitura, formato de domínio público.

O conjunto de informações do CFV representado pela impressão do código de barras (data, valor total da compra, identificação do estabelecimento comercial e assinatura digital da SEF) possibilita ao consumidor verificar, de forma automatizada, requisitos de segurança citados na seção 3.2.1, página 34, tais como a autoria e integridade do documento. Um estabelecimento comercial mal intencionado poderia gerar um CFV, imprimir o código de barras e tentar repetí-lo para falsificar documentos fiscais. Para evitar esse tipo de fraude foram incluídas na impressão do código de barras as informações data e valor total da compra.

Além disso, é impresso um código alfanumérico sobre o cupom fiscal para possibilitar uma consulta aos dados do cupom através da Internet, sendo esta consulta disponibilizada pela SEF. Ao acessar a tela de consulta ilustrada pela Figura 4.6, o

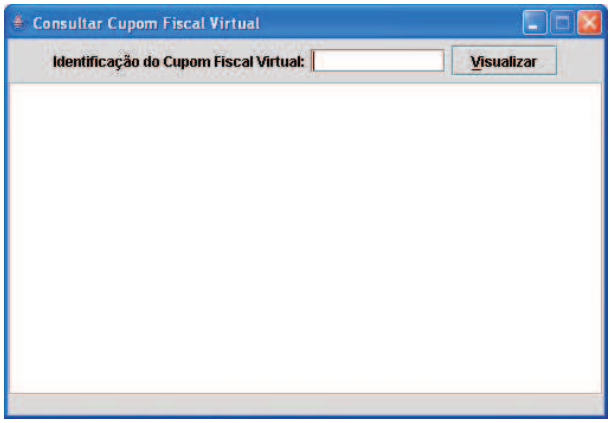

Figura 4.6: Tela de consulta ao Cupom Fiscal Virtual, disponibilizada através da Internet.

consumidor digita o código alfanumérico no campo indicado e pressiona o botão ”Visualizar”. O resultado da pesquisa é demonstrado pela Figura 4.7. Aliando-se a verificação do código de barras ao código alfanumérico, elimina-se a possibilidade de fraude de clonagem de um documento fiscal válido.

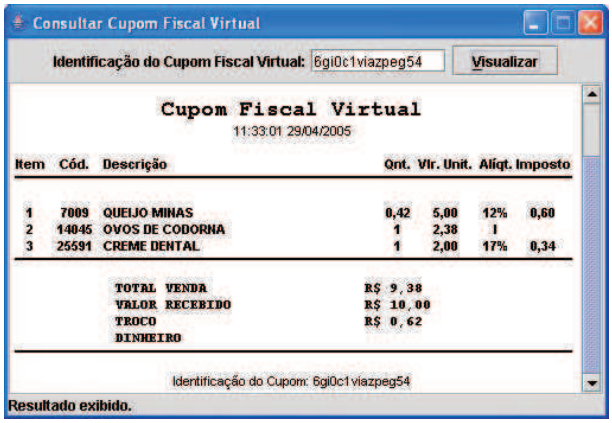

Figura 4.7: Resultado da consulta ao cupom fiscal virtual: após digitar o código alfanumérico, o cupom é montado para verificação dos dados.

A atual infra-estrutura adotada pelo Estado para controle e registro das operações de venda a consumidores, com utilização de equipamentos ECF, não possibilita aos consumidores diferenciar um cupom fiscal falso de um verdadeiro. O CFV traz um grande avanço neste sentido, pois viabiliza a verificação de sua veracidade de forma efi-

ciente. Para que seja possível verificar a autenticidade de um CFV impresso é necessário utilizar dispositivos capazes de realizar a leitura de código de barras, como ilustrado na Figura 3.4, ligados a uma plataforma computacional para processar as informações obtidas da leitura do código de barras. Pode-se adotar uma política que incentive os consumidores a realizar a verificação de seus documentos fiscais virtuais impressos, tal como sorteios premiados no momento da leitura do código de barras.

O procedimento de verificação de um CFV impresso é descrito a seguir:

- O consumidor compra mercadorias e/ou serviços e solicita a impressão de seu CFV;
- De posse do CFV, o consumidor dirige-se a algum leitor ótico de códigos de barra para validar a impressão. Opcionalmente, o consumidor pode optar por entregar seu CFV impresso à SEF, através de caixas coletoras, para que a verificação seja feita de forma automatizada;
- Ao submeter o código de barras do cupom fiscal ao leitor ótico acoplado a uma plataforma computacional equipada com visor, será realizada uma validação da assinatura digital impressa: se a assinatura for válida são exibidas no visor informações do cupom fiscal (a data, o valor total e o estabelecimento comercial que realizou a venda) para que o consumidor faça a verificação dos dados. Além disso, é impresso no cupom fiscal virtual um código alfanumérico a ser utilizado para consultar a unicidade do documento fiscal. Esta consulta será disponibilizada pela SEF através da Internet. Em situações que as informações do documento fiscal não estejam corretas, sugere-se ao consumidor entrar em contato com a SEF e proceder a denúncia.

Desta forma, a SEF consegue estabelecer uma forte ligação com os consumidores, que passarão a exercer o papel de fiscais ativos do complexo sistema de arrecadação tributária, podendo ter a certeza que seu tributo irá efetivamente para o Estado.

4.5.4 Análise da geração de Cupom Fiscal Virtual

O processo de geração do cupom fiscal virtual é composto por várias etapas (geração do documento XML, extração de determinados valores do documento,

geração de resumo criptográfico, assinatura digital e verificação), algumas das quais são realizadas no EC e outras são realizadas pela SEF. Considerando a arquitetura cliente-servidor adotada para o protocolo ECFV, no lado cliente (EC) não há, em princípio, nenhum gargalo que comprometa a execução do protocolo, uma vez que um computador de uso pessoal equipado com um processador Intel de 1.8GHz, comum atualmente, é capaz de realizar até 40 assinaturas digitais por segundo [DES 02]. No lado servidor (SEF) pode haver um gargalo que comprometa a escalabilidade do protocolo. No que diz respeito a geração de assinaturas digitais em documentos eletrônicos, mesmo adotando-se um módulo de segurança criptográfico (MSC), consegue-se com os modelos atualmente disponíveis um máximo de 1200 assinaturas digitais por segundo [COR 04].

Considerando-se a quantidade de estabelecimentos comerciais (milhares) existentes apenas no estado de Santa Catarina, surge a necessidade de adotar alguma estratégia para conferir maior escalabilidade ao protocolo ECFV, possibilitando seu uso em grande escala. Existem alternativas lógicas e físicas para contornar esse gargalo de desempenho na realização de assinaturas digitais pela SEF. Uma delas é o uso de Criptografia Incremental [BEL 94]. Como visto no capítulo 3, seção 3.6, 46, esta técnica criptográfica busca acelerar o processo de geração de assinaturas digitais. Outra alternativa é a criação de uma arquitetura descentralizada hierárquica de Centros de Informática (CI) para distribuir o processamento computacional necessário à execução do protocolo.

4.6 Visão do protocolo ECFV

O protocolo ECFV é constituído por entidades que interagem entre si através de trocas de mensagens. Algumas mensagens são submetidas a processos criptográficos tais como assinatura digital e verificação, para que hajam garantias quanto a integridade e procedência das mesmas. A Figura 4.8 traz uma visão do protocolo ECFV, cujas etapas são descritas a seguir:

1. O EC gera o documento fiscal virtual, cujas características estão descritas na seção 4.5, contendo as informações referentes à venda ou prestação de serviço;

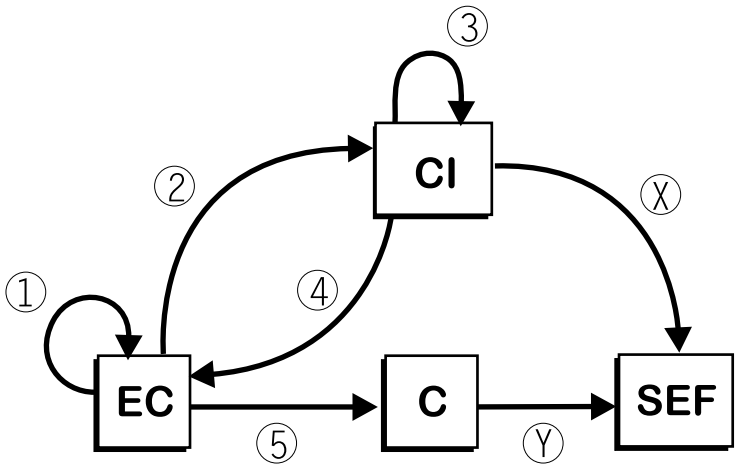

Figura 4.8: Protocolo ECFV

2. São extraídos os valores totais do documento fiscal virtual, agrupados por alíquota. É calculado um resumo criptográfico do próprio documento fiscal. Estas informações são assinadas digitalmente pelo EC e enviadas ao CI para o cálculo de impostos devidos ao Estado;

3. O CI, ao receber as informações geradas no passo anterior, verifica a assinatura digital do EC: caso a verificação falhe o protocolo tem sua execução interrompida; caso a verificação esteja correta, os valores recebidos são contabilizados para apuração de impostos devidos. A SEF produz sua assinatura digital sobre o documento recebido.

4. A assinatura digital da SEF é devolvida ao EC, para que seja concatenada ao cupom fiscal virtual;

5. O cupom fiscal virtual é impresso e entregue a entidade C;

- X: A entidade SEF recebe os valores dos impostos devidos;

- Y: A entidade C pode verificar a validade de seu cupom fiscal impresso através de uma consulta a dispositivos de leitura de códigos de barras, que não precisam estar ligados à SEF, e reportar possíveis irregularidades.

4.6.1 Modos de operação do protocolo ECFV

O documento fiscal virtual deve sempre ser assinado pela SEF, independente de haver ou não comunicação com o CI. Quando há comunicação com o CI o documento fiscal virtual é gerado no EC e assinado pela própria SEF (o leiaute do documento fiscal assume a forma apresentada pela Figura 4.2). Quando não há comunicação com o CI o documento fiscal virtual é gerado no EC e deveria ainda ser assinado pela SEF. Atender a este requisito de segurança é o maior desafio do protocolo ECFV. Deve-se garantir que os documentos fiscais virtuais gerados durante o período em que não há comunicação com o CI atendam aos mesmos requisitos de segurança daqueles gerados durante o período em que há comunicação com o CI.

Para atingir este objetivo será utilizado um esquema de assinatura digital por delegação. Esquemas de assinatura digital por delegação permitem que uma entidade assine mensagens digitais em nome de outra entidade, como visto no capítulo 3, seção 3.4, página 36. Desta forma a entidade EC pode assinar digitalmente os documentos fiscais em nome da SEF nos períodos em que não haja comunicação entre as entidades do protocolo ECFV, como ilustrado na Figura 4.9.

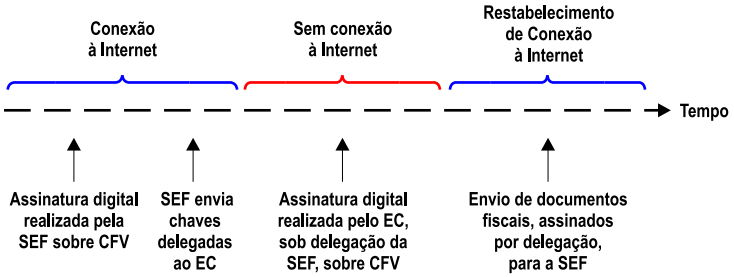

Figura 4.9: Modos de operação do protocolo ECFV: de acordo com a disponibilidade de comunicação entre as entidades do protocolo ECFV, sua execução assume diferentes modos de operação.

Dentre os esquemas de assinatura digital por delegação disponíveis na literatura, uma alternativa que atende de forma satisfatória Às necessidades do protocolo ECFV é o esquema de delegação parcial descartável proposto por [KIM 01]. Tal esquema, ilustrado pela Figura 4.10, é composto pela seguintes etapas:

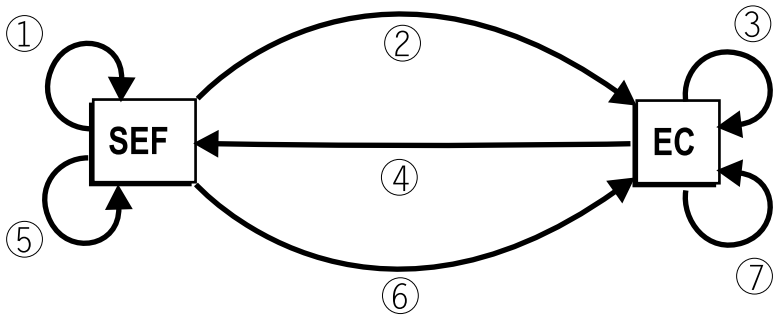

Figura 4.10: Esquema para delegação parcial descartável de assinaturas digitais proposto para o protocolo ECFV.

1. SEF gera parâmetros derivados a partir da própria chave privada;

2. SEF envia para EC os parâmetros calculados;

3. EC verifica a procedência dos parâmetros recebidos: se houver falha nesta verificação o protocolo é encerrado. Caso a verificação esteja correta, são calculadas os pares de chaves delegadas, a partir dos parâmetros da SEF e da chave privada do EC;

4. EC envia os pares de chaves delegadas para a SEF;

5. SEF cria procurações para as chaves delegadas. Cada procuração é composta por uma mensagem de texto contendo restrições quanto ao uso das chaves delegadas, tais como período de validade e categorias de documentos que podem ser assinados. Além disso, a procuração também contém a chave pública correspondente à chave privada delegada. A procuração é assinada pela SEF;

6. As chaves e as respectivas procurações são entregues ao EC.

7. EC está apto a realizar assinaturas digitais em nome da SEF. Cada chave delegada é utilizada para assinar uma única mensagem; caso mais de uma mensagem seja assinada com a mesma chave, a própria chave privada do EC fica comprometida [KIM 01].

Pode-se criar um esquema de assinatura digital por delegação utilizando-se de criptografia baseada em identidade (ver seção 3.5, página 42), considerando que a SEF realizaria a função de Gerador de Chaves Privadas (GCP). A idéia básica consiste em gerar uma chave privada associada a uma determinada identidade (mensagem de texto) e entregar a chave diretamente ao EC. O EC, utilizando-se desta chave recebida, assina documentos fiscais em nome da SEF. Para verificar a assinatura digital gerada pelo EC deve-se utilizar a chave pública da SEF e a identidade correspondente à chave utilizada pelo EC para realizar a assinatura. O esquema é composto das seguintes etapas:

1. Inicialmente é realizada a configuração do Gerador de Chaves Privadas (SEF): é gerado um par de chaves, sendo que uma delas é tornada pública (parâmetro público) e outra é mantida em segredo (chave mestra);

2. SEF gera uma chave privada associada a uma identidade escolhida. Esta identidade é um texto com informações sobre a utilização da chave gerada. Um exemplo de identidade poderia ser ”SEF - Nome do Estabelecimento - 16/12/2004”, restringindo a utilização da chave privada a um determinado estabelecimento durante determinado período (no exemplo, dia 16 de dezembro de 2004);

3. SEF entrega a chave privada e a identidade associada ao EC por meio de um canal de comunicação seguro;

4. EC passa a realizar assinaturas digitais em nome da SEF, dentro do período determinado pela identidade.

A tabela 4.1 traz um comparativo dos dois possíveis esquemas de assinatura digital por delegação apresentados nesta seção.

4.7 Formalização do protocolo ECFV

Modelar um protocolo criptográfico exige algum formalismo, para que se possa ao menos garantir propriedades estruturais do protocolo proposto. Para formalizar o protocolo ECFV foi escolhida a técnica de redes de petri. Este método formal

Tabela 4.1: Comparativo dos esquemas de assinatura digital por delegação propostos.

ESQUEMA	VANTAGENS	DESVANTAGENS
Delegação Parcial Descartável.	• Proporciona controle sobre o uso da chave criptográfica delegada; • Há vínculo do assinante delegado sobre a assinatura produzida, evitando possível repúdio de autoria da mesma.	• Dificuldade de implementação; • Necessidade de realização de um par de assinaturas digitais sobre o mesmo documento eletrônico; • necessidade de troca de parâmetros para estabelecimento de chaves delegadas.
Delegação por Criptografia Baseada em Identidade.	• Simplicidade de geração de chaves delegadas; • A chave pública (mensagem de texto) contém as restrições de uso da chave delegada.	• Não proporciona controle sobre o uso da chave criptográfica delegada; • Não há vínculo do assinante delegado sobre a assinatura produzida, podendo haver repúdio de autoria da mesma.

enquadra-se na categoria dos Diagrams de Transições de Estado (DTE) e tem sido utilizado para especificação e validação de sistemas discretos e complexos. Através desta formalização pode-se verificar propriedades estruturais do modelo [IEE 89], tais como **alcançabilidade**, **limites de marcas**, **reinicialização**, **reversibilidade**, **cobertura** e eventuais impasses ou *dead-locks*. Opcionalmente, pode-se modelar através de redes de petri formas de ataques que possam ameaçar o funcionamento do protocolo [LEE 97].

As representações montadas através de redes de petri utilizam-se de três primitivas [CAR 97]: a)**lugar**: o conjunto de lugares representa o estado do sistema; b)**transição**: representa um evento que causa uma mudança de estado do sistema; c) **condição**: representada por uma ficha em um lugar (item a); quando o número de fichas requerido por uma transição é atendido, a transição é disparada e ocorre uma mudança de estado do sistema, em caso contrário o evento fica suspenso aguardando recursos (fichas).

A Figura 4.11 mostra o protocolo ECFV modelado através de uma rede

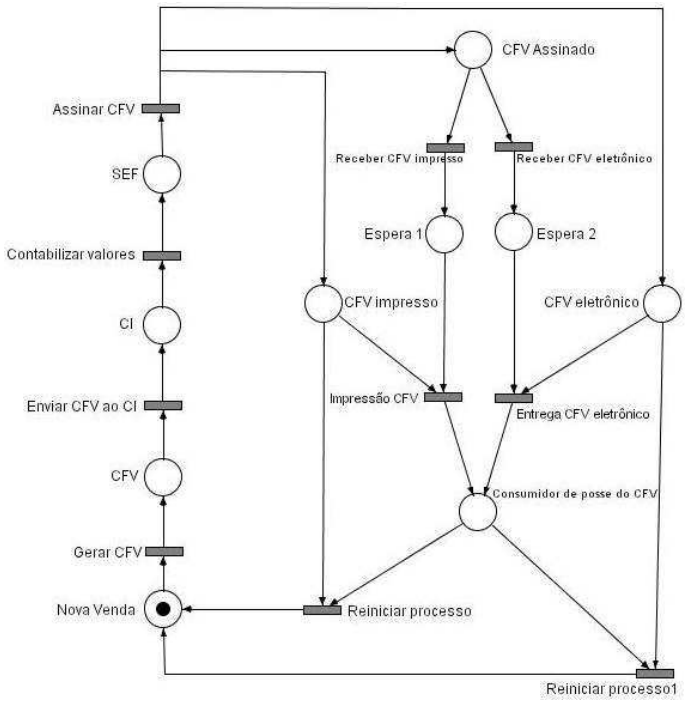

Figura 4.11: Protocolo ECFV modelado por uma rede de petri

de petri.

Utilizou-se o programa ARP v2.4, desenvolvido pelo LCMI do departamento de Engenharia Elétrica da UFSC, para analisar as propriedades da rede de petri proposta. A análise, ilustrada pela Figura 4.12, traz os seguintes resultados:

- A rede de petri é binária, ou seja, para cada um dos lugares o número de fichas será 0 ou 1;
- Todos os lugares podem ser alcançados a medida que as transições são disparadas;
- A rede de petri não é estritamente conservativa, ou seja, o número de fichas varia a medida que as transições são disparadas;
- A rede de petri é viva, ou seja, todas as transições podem ser disparadas;
- A rede é reinicializável, ou seja, o estado inicial sempre pode ser alcançado;
- Não há situações de impasse.

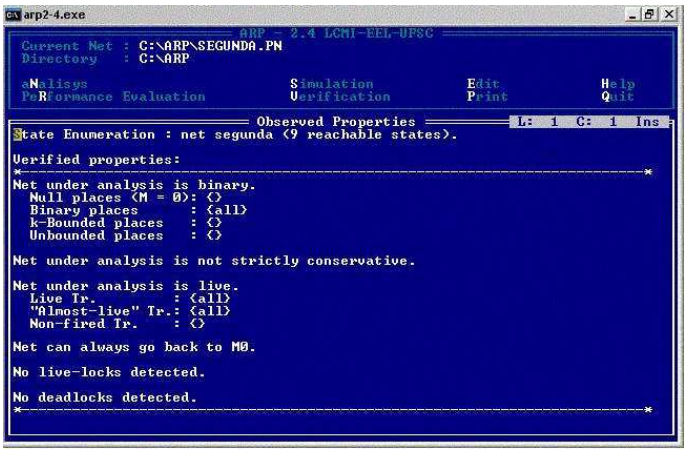

Figura 4.12: Análise de propriedades da rede de petri que modela o protocolo ECFV através do programa ARP v2.4

Conforme visto ao longo deste capítulo, o documento fiscal virtual sempre é assinado pela SEF, havendo ou não comunicação entre as entidades do protocolo ECFV. Esta situação está modelada através da rede de petri da Figura 4.13, cujas propriedades foram verificadas pelo programa ARP v2.4, como ilustra a Figura 4.14. Alguns comentários a respeito das propriedades verificadas:

- A rede de petri é limitada[3], ou seja, o número de fichas que pode estar ocupando um lugar é maior que 1;
- Todos os lugares podem ser alcançados a medida que as transições são disparadas;
- A rede de petri não é estritamente conservativa, ou seja, o número de fichas varia a medida que as transições são disparadas;
- A rede de petri não é viva pois, pois em determinadas circunstâncias algumas transições não podem ser disparadas;

[3]Embora na Figura 4.13 o lugar ”Chaves delegadas pela SEF”esteja representado com 50 fichas, para efeito de validação do modelo reduziu-se de 50 para 5 fichas (para evitar uma explosão de estados no mecanismo de validação da rede de petri). Tal redução, no entanto, não altera os resultados da análise - apenas reduz o número de repetições de execuções completas do DTE. Isto explica porque a análise da Figura 4.14 cita lugares k-limitados, com k=5 e não 50.

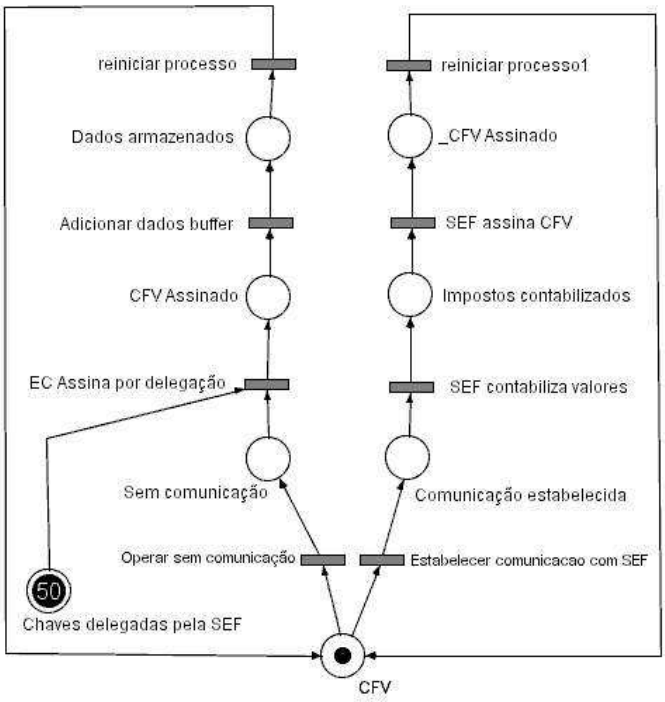

Figura 4.13: Procedimento de assinatura do CFV modelado por uma rede de petri

- A rede não é reinicializável;
- Há situações de impasse.

Propriedades indesejáveis tais como presença de impasses foram encontradas nesta rede de petri que modela o processo de assinatura do documento fiscal virtual. Isto ocorre porque o sistema modelado através da rede de petri depende de chaves delegadas pela SEF. Tal característica reflete esta necessidade do protocolo. Em uma situação em que não há comunicação entre SEF e EC e não há chaves delegadas pela SEF, não há como assinar documentos fiscais e portanto a execução do protocolo não pode prosseguir.

4.8 Conclusão

Neste capítulo é apresentado um protocolo criptográfico para emissão de documentos fiscais virtuais, trata-se do protocolo ECFV, uma alternativa à emissão convencional de documentos fiscais no processo de venda de produtos e/ou serviços ao

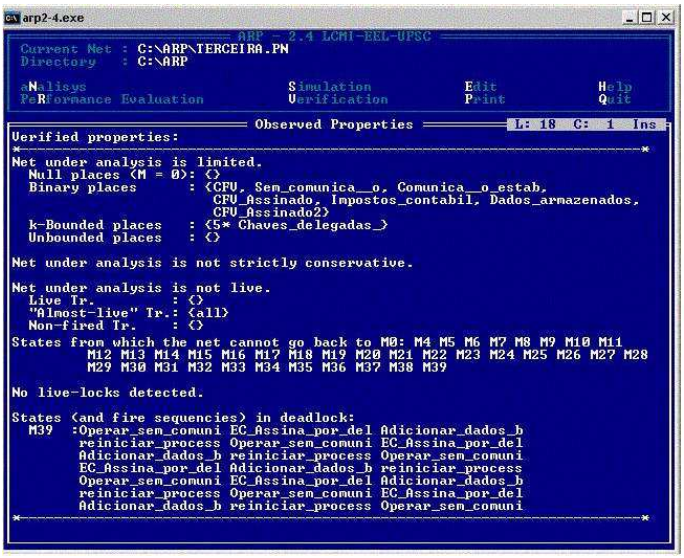

Figura 4.14: Análise de propriedades da rede de petri que modela o protocolo ECFV através do programa ARP v2.4

consumidor final. As entidades envolvidas neste protocolo são: SEF (Secretaria de Estado da Fazenda), EC (Estabelecimento Comercial), CI (Centro de Informática) e C (Consumidor).

O protocolo ECFV prevê a criação do CFV, um documento fiscal eletrônico cuja impressão pode ser realizada por qualquer impressora. Para a viabilização desta proposta, faz-se necessário construir uma infra-estrutura física e lógica para a criação, manipulação e gerenciamento dos documentos fiscais gerados: hardware criptográfico seguro (HSM) [MAR 04], Infra-estrutura de chaves públicas, redes de comunicação de dados, aplicativos específicos e técnicas de armazenamento de dados. A entidade CI tem importância estratégica dentro desta proposta, pois centraliza o fluxo de informações trocadas entre as demais entidades.

Há um fator muito importante a ser considerado, a possível perda de conexão com a Internet no momento da operação do aplicativo na entidade EC. Duas propostas são sugeridas para possibilitar uma operação híbrida do sistema (havendo ou não comunicação entre as entidades do protocolo), através de esquemas de assinatura digital por delegação. A primeira proposta baseia-se em esquemas de assinatura digital

por delegação descartável [KIM 01] e a segunda proposta é uma adaptação de criptografia baseada em identidade para possibilitar delegação para realização de assinaturas digitais. Cada proposta apresenta vantagens e desvantagens, listadas pela tabela 4.1, página 70.

O Cupom Fiscal Virtual (CFV) traz as informações exigidas pela atual legislação [BRA 94], e em sua forma impressa apresenta características que permitem verificar de forma automatizada seus requisitos de segurança (requisitos de segurança de documentos são discutidos no capítulo 3, seção 3.2.1, página 34). A impressão de características do CFV é realizada através de utilização de código de barras. Dentre os padrões de códigos de barras existentes (ver capítulo 3, seção 3.7, página 47) optou-se pelo código de barras PDF417, por suas características e por ser de domínio público.

A formalização do protocolo ECFV é construída através de um Diagrama de Transição de Estados (DTE), representado por uma Rede de Petri [IEE 89]. A validação deste modelo formal foi automatizada com o uso do programa ARP v2.4, desenvolvido pelo LCMI do departamento de Engenharia Elétrica da UFSC. A análise das propriedades do modelo formal foi apresentada na seção 4.7, página 69.

Capítulo 5

Protótipo do protocolo ECFV

5.1 Introdução

É objetivo desta dissertação propor soluções para as dificuldades tecnológicas de emissão, validação e impressão de cupons fiscais virtuais. No entanto, sabe-se que a implementação destas propostas não é trivial. A implementação do protocolo ECFV envolve, além da criação do aplicativo propriamente dito, a disponibilização de serviços de diversas naturezas (autenticação, consulta, auditoria, etc.) para as entidades envolvidas.

Este capítulo descreve os procedimentos necessários ao estabelecimento comercial (EC) para utilização do aplicativo ECFV, além de demonstrar a implementação de um protótipo com algumas funcionalidades básicas para a implementação do protocolo criptográfico proposto nesta dissertação.

O capítulo está organizado da seguinte maneira: a seção 5.2 descreve as funcionalidades do aplicativo ECFV além dos procedimentos para sua obtenção e utilização. A seção 5.3 traz as funcionalidades do aplicativo ECFV demonstradas através da implementação do protótipo desenvolvido. A seção 5.4 fecha o capítulo.

5.2 Características do Aplicativo ECFV

A implementação do protocolo ECFV requer uma infra-estrutura física e lógica, de acordo com a seção 4.2, página 55 do capítulo 4. Um dos requisitos de infra-estrutura requeridos para o funcionamento do protocolo ECFV é o aplicativo ECFV, a ser executado pelo estabelecimento comercial (EC) em substituição ao equipamento ECF utilizado atualmente. O aplicativo ECFV deve ser implementado em uma arquitetura cliente-servidor e disponibilizar as seguintes funcionalidades:

- Gerar o cupom fiscal virtual (CFV);
- Realizar assinatura do EC sobre o CFV;
- Verificar se há comunicação em rede:

  - Havendo comunicação, o aplicativo ECFV deve formatar os dados do CFV para submissão ao centro de informática (CI) para apuração dos impostos devidos e geração da assinatura digital da SEF sobre o CFV;

  - Não havendo comunicação, o aplicativo ECFV deve assinar o CFV com uma chave delegada pela SEF e adicionar os dados do CFV em um buffer de transmissão para posterior envio ao CI;
- Imprimir o CFV;
- Gerar log de todas as operações realizadas para fins de auditoria;
- Disponibilizar o CFV em meio digital para o consumidor.

5.2.1 Autenticação do EC e obtenção do aplicativo ECFV

Antes de poder utilizar o aplicativo ECFV, o EC precisa obtê-lo. Para isso, é necessário que o EC autentique-se perante o CI e solicite o aplicativo. Caso a autenticação falhe, o EC recebe um aviso e é sugerido a fazer/atualizar seu cadastro junto à SEF. Se a autenticação for bem sucedida, o EC obtém o aplicativo para emissão de Cupom Fiscal Virtual (CFV). Todo o procedimento descrito neste parágrafo está ilustrado pelo fluxograma da Figura 5.1.

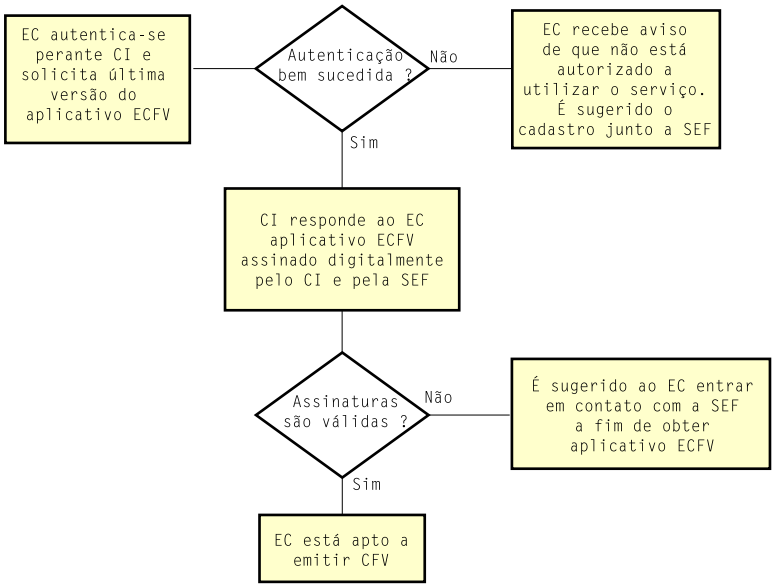

Figura 5.1: Processo de obtenção do aplicativo ECFV.

5.2.2 Utilização do aplicativo ECFV

Após obtenção do aplicativo ECFV, o estabelecimento comercial (EC) está apto a realizar a emissão de Cupom Fiscal Virtual (CFV). O CFV poderá ser entregue em meio digital e/ou papel ao consumidor, como discutido ao longo do capítulo 4. Para gerar o CFV, o EC deverá seguir algumas etapas, ilustradas pelo fluxograma da Figura 5.2.

Inicialmente o EC realiza a abertura do CFV, registrando itens de venda de produtos ou serviços. Após finalizar o CFV, o aplicativo formata os dados do CFV para envio à SEF. A formatação destes dados está descrita no capítulo 4, seção 4.5, página 58. Então, o aplicativo ECFV verifica se há comunicação em rede, conforme ilustrado pelo fluxograma 5.3.

Havendo comunicação em rede, o aplicativo ECFV envia os dados referentes à venda realizada para a SEF para serem contabilizados e assinados pela SEF. Caso não haja comunicação em rede, os dados de registro da venda realizada são assinados com utilização de chave criptográfica delegada pela SEF. Os dados deste CFV são adicionados a um buffer de espera para transmissão, tão logo o aplicativo ECFV detecte

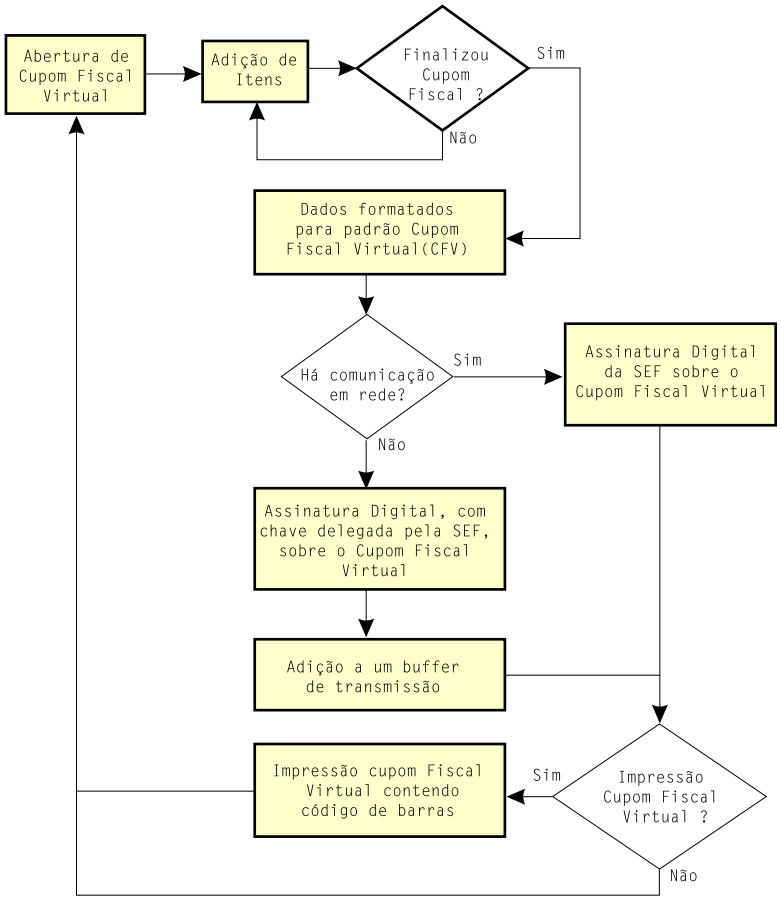

Figura 5.2: Processo de emissão de Cupom Fiscal Virtual.

o restabelecimento de comunicação em rede, como ilustra o fluxograma da Figura 5.3. O CFV está pronto e pode ser entregue ao consumidor, seja em meio papel ou meio digital.

5.3 Aplicativo ECFV

Para demonstrar algumas funcionalidades básicas do aplicativo ECFV foi desenvolvido um protótipo que será apresentado nesta seção. O aplicativo apresenta arquitetura cliente-servidor e foi desenvolvido com uma linguagem de programação multiplataforma - Java - o que confere portabilidade à sua execução. O número de rotinas implementadas neste protótipo é restrito a algumas funcionalidades que queremos demonstrar. Estas funcionalidades são:

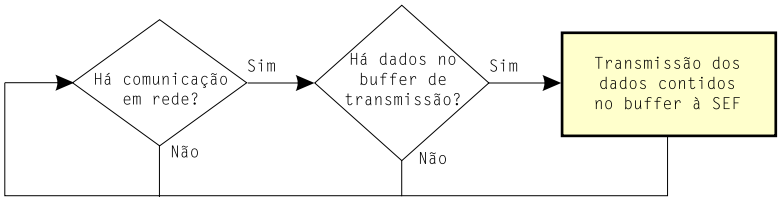

Figura 5.3: Verificação de disponibilidade de comunicação em rede

- Derivação de chave criptográfica delegada a partir de chave privada mestra[1];
- Derivação de chave pública delegada a partir de chave pública mestra[2];
- Geração de assinatura digital delegada;
- Verificação de assinatura digital delegada;
- Verificação de possibilidade de comunicação em rede;
- Troca de mensagens assinadas digitalmente entre cliente e servidor.

A Figura 5.4 ilustra o cenário de utilização do protótipo desenvolvido e suas funcionalidades. A aplicação servidora é ilustrada pela entidade SEF enquanto a aplicação cliente é ilustrada pela entidade EC.

A seção 5.3.1 traz detalhes a respeito da implementação do protótipo do aplicativo ECFV, apresentado por um aplicação cliente-servidor.

5.3.1 Protótipo do aplicativo ECFV

O protótipo do aplicativo ECFV, desenvolvido em linguagem de programação multi-plataforma (Java) foi desenvolvido de acordo com a arquitetura cliente-servidor. A aplicação servidora é um programa Java que representa a entidade SEF do protocolo ECFV. A aplicação cliente representa a entidade EC do protocolo ECFV, sendo um applet Java assinado. Para implementar as funções criptográficas de assinatura digital

[1]A expressão ”chave privada mestra”será utilizada para identificar a chave criptográfica privada de um assinante original que delega chaves para um assinante delegado.

[2]A expressão ”chave pública mestra”será utilizada para identificar a chave criptográfica pública de um assinante original que delega chaves para um assinante delegado.

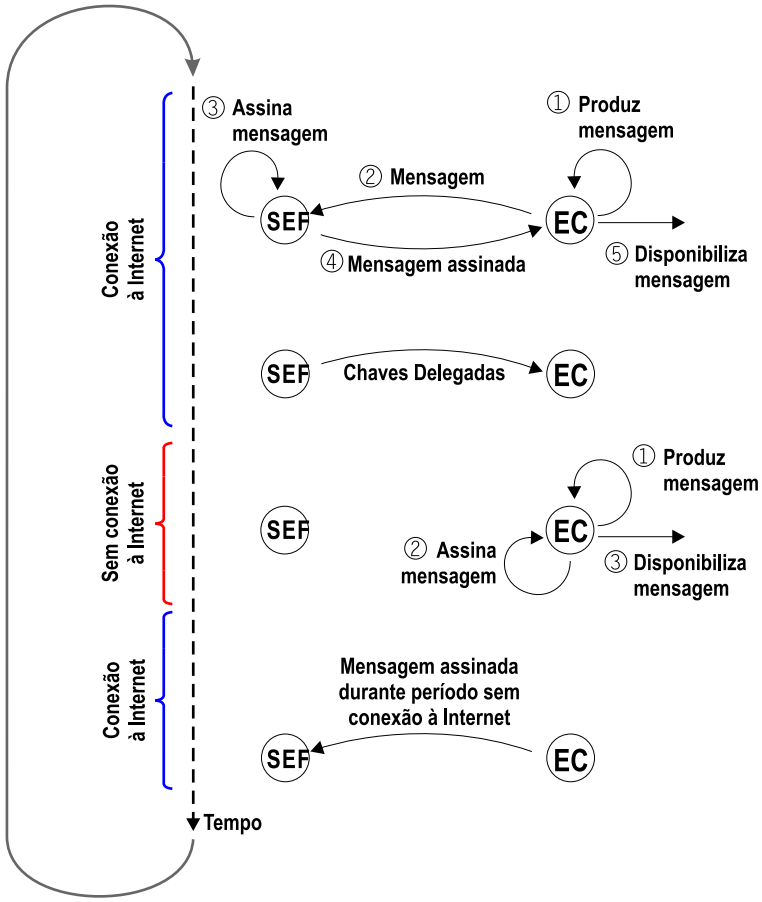

Figura 5.4: Cenário de utilização do protótipo do aplicativo ECFV

e verificação, utilizou-se uma API do provedor criptográfico El Gamal disponibilizada em [CAT 05]. Tanto a aplicação servidora quanto a aplicação cliente inicializam este provedor em seus métodos construtores, como ilustra o seguinte fragmento de código:

```
...
java.security.Provider provedor = new ecfv.compartilhamento.elgamal.Provider();
Security.addProvider(provedor);
...
```

A aplicação servidora, ao ser iniciada, procura pela sua chave privada mestra localizada em um arquivo texto [3]. Se for encontrada a chave criptográfica ela é

[3] O protótipo do protocolo ECFV armazena chaves criptográficas em arquivos texto para simplificar sua implementação. Em situações reais de uso, deve-se considerar mecanismos para armazenamento de chaves criptográficas, tais como cartões inteligentes.

carregada, senão é gerada uma nova chave. Esta chave criptográfica representa a chave privada da SEF no processo de assinatura de documentos fiscais virtuais. A rotina que procura pela chave mestra é apresentada a seguir:

```
public boolean leChaveMestra(){
    try{
        if (!arquivoChaveMestra.exists()) {
            servidor.addTextoLog("Arquivo da chave mestra nao encontrado.");
            return false;
        }

        // Inicializa o ObjectInputStream.
        entrada = new ObjectInputStream(new FileInputStream(arquivoChaveMestra));

        chaveMestra = (KeyPair) entrada.readObject();
        chavePrivada = (ElGamalPrivateKey) chaveMestra.getPrivate();
        chavePublica = (ElGamalPublicKey) chaveMestra.getPublic();
        entrada.close();
        return true;
    }
    // Caso ocorra uma IOException, o programa cria nova chave mestra.
    catch ( IOException excecao ){
        servidor.addTextoLog( "Erro na manipulacao do arquivo da chave mestra." );
        return false;
    }catch ( ClassNotFoundException excecao ){
        servidor.addTextoLog( "Nao foi possivel carregar a chave mestra." );
        return false;
    }catch ( ClassCastException excecao ){
        servidor.addTextoLog( "Nao foi possivel carregar a chave mestra." );
        return false;
    }
}
```

Caso não seja possível ler a chave mestra por algum motivo (erro de manipulação do arquivo que contém a chave ou mesmo inexistência do arquivo), a rotina `leChaveMestra()` retorna o valor booleano falso. Neste caso, é acionada uma rotina para geração de uma nova chave privada para a aplicação servidora. O fragmento de código para criar nova chave criptográfica é apresentado a seguir:

```
    // Inicializa KeyPairGenerator
    geraChave = new ElGamalKeyPairGenerator();
```

```
geraChave.initialize(keysize,new SecureRandom());
// Gera a chave mestra
chaveMestra = geraChave.generateKeyPair();
servidor.addTextoLog("Chave mestra gerada.");
```

Assim que a aplicação servidora consegue carregar (ou criar) suas chaves criptográficas, passa a aguardar a conexão da aplicação cliente em uma determinada porta lógica, como ilustra a Figura 5.5.

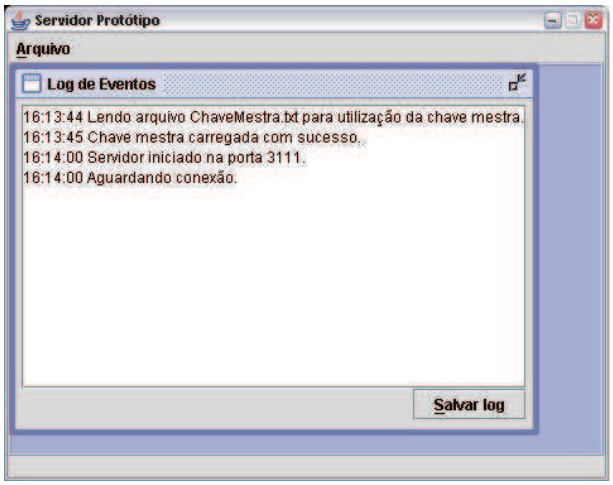

Figura 5.5: Inicialização do protótipo servidor

Ao iniciar, a aplicação cliente carrega uma chave criptográfica utilizada para a realização de assinatura digital dos documentos eletrônicos enviados à aplicação servidora. Esta chave criptográfica representa a chave privada do EC. A rotina para leitura de chave criptográfica na aplicação cliente é apresentada a seguir:

```
public void leChaves(){
    if (!arquivoChaves.exists()) {
        cliente.addTextoLog("Nenhuma chave foi encontrada.");
        this.criaChaves();
        return;
    }try{
        ObjectInputStream entrada =
        new ObjectInputStream(new FileInputStream(arquivoChaves));
        if (!isChaveCriada){
            cliente.addTextoLog("Lendo arquivo " +
            arquivoChaves.getPath() + " para utilizacao da chave.");
```

```
            }
            KeyPair parChaves = ( KeyPair ) entrada.readObject();
            chavePrivada = ( ElGamalPrivateKey ) parChaves.getPrivate();
            chavePublica = ( ElGamalPublicKey ) parChaves.getPublic();
            cliente.addTextoLog( "Chave carregada com sucesso." );
            entrada.close();
        }catch ( ClassNotFoundException excecao ) {
            cliente.addTextoLog( "Objeto de tipo desconhecido." );
            this.criaChaves();
        }catch ( IOException excecao ) {
            cliente.addTextoLog( "Ocorreu um erro durante a leitura da chave." );
            this.criaChaves();
        }
    }
```

Um aspecto muito importante do protocolo ECFV é sua capacidade de gerar documentos fiscais havendo ou não comunicação entre o EC e a SEF. Como visto no capítulo 4, a emissão de documento fiscal virtual em uma situação que não haja comunicação entre o EC e a SEF só é possível graças ao uso de técnicas de assinatura digital por delegação (ver capítulo 3, seção 3.4, página 36). É sugerido no capítulo 4 o uso de uma técnica para assinatura digital delegada descartável, baseada no trabalho de Kim et al. [KIM 01], para o protocolo ECFV. No entanto, o artigo que traz este esquema de delegação de assinatura digital não apresenta de que forma pode-se implementá-lo; ao invés disso, apenas a fundamentação matemática necessária ao esquema é apresentada. Portanto, para a implementação do protótipo do aplicativo ECFV optou-se pela utilização de um esquema de assinatura digital por delegação baseado no trabalho de Mambo et al. [MAM 96].

A derivação da chave delegada a partir da chave privada, de acordo com Mambo et al. [MAM 96], ocorre através da escolha de um inteiro $k \in_R, Z^*_{p-1}$. Após, computa-se $K = g^k \ mod \ p$. Finalmente, a chave delegada é calculada pela equação $\sigma = s + kK \, mod \ p - 1$, sendo s a chave privada original. O fragmento de código utilizado para realizar esta operação é listado abaixo:

```
public KeyPair derivaChaves() {
   BigInteger um = BigInteger.ONE;
   BigInteger p = chavePrivada.getP();
```

```
    BigInteger pMenosUm = p.subtract(um);
    BigInteger g = chavePrivada.getG();
    BigInteger k;
    do{
       // Cria um novo k de tamanho p - 1.
       k = new BigInteger(p.bitLength() - 1, new SecureRandom());
    }while(k.gcd(pMenosUm).equals(um) == false);

    BigInteger K = g.modPow(k,p);

    // Calcula o valor de sigma passo-a-passo.
    BigInteger sigma1 = K.mod(pMenosUm);
    BigInteger sigma2 = k.multiply(sigma1);
    BigInteger sigma = chavePrivada.getX().add(sigma2);
    BigInteger v = chavePublica.getY().multiply(K.modPow(K,p));
    ElGamalPrivateKey chavePrivadaDerivada= new ElGamalPrivateKey(sigma,g,p);
    ElGamalPublicKey chavePublicaDerivada = new ElGamalPublicKey(
                                  v,chavePublica.getG(),chavePublica.getP());
    return new KeyPair(chavePublicaDerivada, chavePrivadaDerivada);
}
```

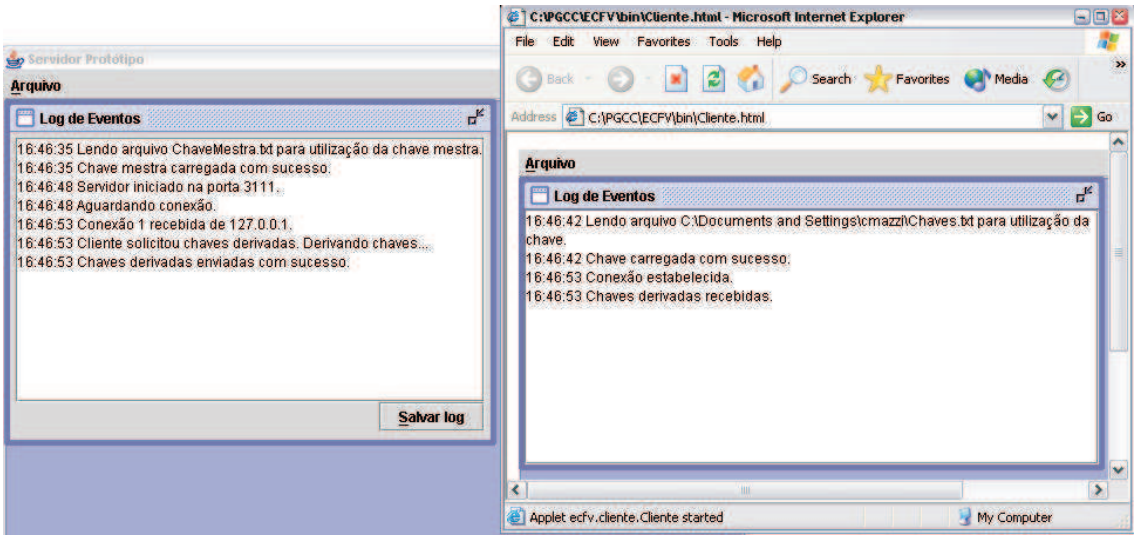

Figura 5.6: Comunicação entre protótipos do servidor e cliente

Estabelecida a comunicação entre a aplicação cliente e o servidor, ilustrada pela Figura 5.6, a aplicação cliente verifica se possui chaves derivadas da chave privada mestra do servidor. Caso não possua chaves derivadas, a aplicação cliente as solicita ao servidor. Toda comunicação que parte do cliente para o servidor é tratada pela

rotina `run()` do servidor, caracterizada pelo seguinte fragmento de código:

```
public void run(){
    Thread threadAtual = Thread.currentThread();
    while ( servidorThread == threadAtual ){
        try{
            this.recebeConexao();
            this.processaConexao();
            this.fechaConexao();
        }catch ( EOFException excecao ){
        ...
        //tratamento de diversas excecoes
        ...
        }
    }
}
```

A rotina `processaConexao()` é a responsável por processar e responder às requisições realizadas pelo cliente ao servidor. Portanto, ao receber uma requisição do cliente solicitando chaves derivadas, o servidor as processa através do seguinte fragmento de código da rotina `processaConexao()`:

```
...
else if (recebido.toString().equals("Requisicao de chaves
derivadas.")){
    // Deriva o par de chaves.
    this.addTextoLog( "Cliente solicitou chaves derivadas. Derivando chaves..." );
    KeyPair parChavesDerivadas = processamento.derivaChaves();
    // Envia o par de chaves ao cliente.
    this.envia( parChavesDerivadas );
    this.addTextoLog( "Chaves derivadas enviadas com sucesso." );
}
...
```

A aplicação cliente, ao receber as chaves derivadas do servidor utiliza-se da rotina `salvaChavesDerivadas(KeyPair)` para armazená-las em arquivo. Estas chaves derivadas somente serão utilizadas pela aplicação cliente em situações que não haja comunicação entre esta e o servidor. A rotina utilizada pelo cliente para armazenar as chaves derivadas é apresentada a seguir:

```
public void salvaChavesDerivadas(KeyPair parChaves) {
    try{
        if (!arquivoChavesDerivadas.exists()){
            arquivoChavesDerivadas.createNewFile();
        }
        ObjectOutputStream saida =
        new ObjectOutputStream(new FileOutputStream(arquivoChavesDerivadas));
        saida.writeObject( parChaves );
        saida.flush();
        saida.close();
        this.leChavesDerivadas();;
    }
    catch ( IOException excecao ) {
        cliente.addTextoLog("Ocorreu um erro ao salvar as chaves derivadas.");
    }
}
```

O Documento fiscal gerado na aplicação cliente deve ser assinado pela própria aplicação cliente e também pela aplicação servidora. A aplicação cliente, após gerar o documento, assina-o através da rotina `assinaOnLine(...)`. Esta rotina cria um objeto `assinarDocumento` da classe `Assinar` utilizado para o transporte, pela rede, do documento fiscal gerado até o servidor. A rotina `assinaOnLine(...)` é apresentada pelo seguinte fragmento de código:

```
public void assinaOnLine(byte[] bytesArquivo) {
   tarefaPendente = true;
   // Recebe os bytes do arquivo a ser assinado.
   byte[] bytesArquivoAssinar = bytesArquivo;
   // Instancia um objeto Assinar para o transporte das informacoes pela rede.
   Assinar assinarDocumento = new Assinar(bytesArquivoAssinar, this.getChavePublica());
   // Acrescenta ao objeto Assinar a assinatura realizada com chave do cliente.
   assinarDocumento.setAssinaturaCliente(this.realizaAssinatura(
                               this.getChavePrivada(), bytesArquivoAssinar));
   // Envia o documento para o servidor
   cliente.envia(assinarDocumento);
}
```

A aplicação servidora, ao receber o documento fiscal, verifica a procedência deste (verificando a assinatura digital do EC sobre o documento) e produz sua própria assinatura digital sobre o documento. O procedimento de verificação de assinatura

digital é realizado através da rotina `verificaAssinatura(...)`, cujo fragmento de código é apresentado a seguir:

```
public boolean verificaAssinatura(ElGamalPublicKey chavePublica,
                            byte[] arquivo, byte[] bAssinatura){
    byte[] bytesArquivo = arquivo,
            bytesAssinatura = bAssinatura;
    boolean verificado;
    ElGamalPublicKey chavePublicaVerificar = chavePublica;
    bytesArquivo = arquivo;
    bytesAssinatura = bAssinatura;
    chavePublicaVerificar = chavePublica;
    try{
        assinatura = Signature.getInstance(algoritmoAssinatura);
        assinatura.initVerify(chavePublicaVerificar);
        //Atualiza os bytes da assinatura, ainda os bytes originais do arquivo.
        assinatura.update(bytesArquivo);
        //O resultado da verificacao (true/false) eh armazenado em verificado.
        verificado = assinatura.verify(bytesAssinatura);
    }catch (NoSuchAlgorithmException excecao) {
        ...
        \\tratamento de diversas excecoes
        ...
    }
    return verificado;
}
```

Enquanto há comunicação entre as aplicações cliente e servidor, a assinatura digital do servidor sobre o documento fiscal é realizada pelo própria aplicação servidora, através da rotina `realizaAssinatura(...)`. Nesta rotina, são passados como parâmetros a chave criptográfica uitilizada para realizar a assinatura, além de um array de bytes que representa o documento a ser assinado. O retorno deste método é um novo array de bytes, contendo a assinatura digital produzida. O fragmento de código apresentado a seguir demonstra a rotina `realizaAssinatura(...)`:

```
public byte[] realizaAssinatura(ElGamalPrivateKey
chavePrivada,byte[] arquivo){
    byte[] bytesArquivo = arquivo, c;
    ElGamalPrivateKey chavePrivadaAssinar = chavePrivada;
    try{
        //Pega uma instancia do algoritmo especificado.
```

```
        assinatura = Signature.getInstance(algoritmoAssinatura);
        assinatura.initSign(chavePrivadaAssinar);
        //Define os bytes a assinar (array de bytes).
        assinatura.update(bytesArquivo);
        //Assina o documento, passando o resultado para o array de bytes c.
        c = assinatura.sign();
    }catch(NoSuchAlgorithmException excecao){
        ...
        \\tratamento de excecoes
        ...
    }
    return c;
}
```

Quando não houver comunicação entre o servidor e o cliente, o protótipo cliente assina o documento eletrônico com sua própria chave criptográfica e gera uma assinatura com a chave delegada pela SEF. O fragmento de código a seguir ilustra este procedimento:

```
public void assinaOffLine(byte[] bytesArquivo) {
   tarefaPendente = true;
   byte[] bytesArquivoAssinar = bytesArquivo;
   byte[] assinaturaCliente = this.realizaAssinatura(
                   this.getChavePrivada(), bytesArquivoAssinar);
   byte[] assinaturaDerivada = this.realizaAssinatura(
                   this.getChaveDerivadaPrivada(), bytesArquivoAssinar);
   boolean b = this.verificaAssinatura(this.getChaveDerivadaPublica(),
                               bytesArquivoAssinar, assinaturaDerivada);
   String derivadaAutenticado = b ? "AUTENTICADO" : "NAO AUTENTICADO";

   // Texto de autenticacao a ser anexado ao documento.
   String textoAutenticacao = "<!-- Assinatura Cliente:\n" +
                       this.byteParaHexa(assinaturaCliente) + " -->\n" +
                       "<!-- Assinatura com chaves derivadas do Servidor:\n" +
                       this.byteParaHexa(assinaturaDerivada) +
                       "\n" +
                       derivadaAutenticado + " -->\n";

   // Anexa o texto de autenticacao ao documento.
   StringBuffer buffer = new StringBuffer(textoAutenticacao);
   buffer.append(new String(bytesArquivoAssinar));

   // Salva o texto final.
```

```
        this.salvaDocumento(buffer.toString());
        tarefaPendente = false;
    }
```

A assinatura digital delegada realizada pela aplicação cliente sobre o documento fiscal pode ser verificada com o uso da chave criptográfica pública mestra da aplicação servidora, através da rotina `verificaAssinatura(...)`, apresentada anteriormente nesta seção.

5.4 Conclusão

O protocolo ECFV propõe a emissão de documentos fiscais virtuais no processo de venda à consumidores. Para a geração, impressão e disponibilização destes documentos é necessário haver o aplicativo ECFV, cujas funcionalidades, procedimentos necessários à sua obtenção e operação são descritos neste capítulo.

Foi desenvolvido um protótipo para implementar algumas funcionalidades do aplicativo ECFV. O protótipo, desenvolvido em linguagem de programação multi-plataforma (Java), é composto por uma aplicação servidora e uma aplicação cliente (applet).

O principal objetivo do protótipo apresentado é demonstrar a viabilidade técnica da realização de assinaturas digitais por delegação, possibilitando a geração remota de documentos fiscais eletrônicos em situações em que não haja comunicação entre as entidades que compõem o protocolo ECFV.

Capítulo 6

Considerações Finais

O atual sistema de controle da arrecadação tributária do imposto ICMS adotado pelo Estado é realizado sobre documentos fiscais em papel gerados para registrar as vendas realizadas aos consumidores. Historicamente diferentes tecnologias tem sido utilizadas para garantir o correto registro de operações comerciais tributáveis.

Esta dissertação propõe o protocolo criptográfico ECFV, buscando oferecer uma alternativa ao atual sistema de emissão de documentos fiscais nas vendas de produtos e/ou serviços a consumidores. Não há, inicialmente, a ambição de substituir o atual sistema de registro de operações comerciais pelo ECFV; ao invés disso, considera-se possível utilizar o protocolo ECFV em contextos específicos. Possivelmente com o amadurecimento da tecnologia, sua adoção em larga escala possa tornar-se uma realidade.

Haviam alguns problemas expostos inicialmente no capítulo 1 para os quais foram desenvolvidas as seguintes soluções ao longo desta dissertação:

- **Problema:** Emissão do documento fiscal a distância;

  Solução: Utilização do aplicativo ECFV que possibilita a geração e assinatura do documento fiscal de forma remota;

- **Problema:** Impressão do documento fiscal;

  Solução: Utilização de código de barras para impressão de características de identificação, dispensando a necessidade de impressora fiscal controlada pelo Es-

tado;

- **Problema:** Emissão de documento fiscal na ausência de comunicação com a Secretaria de Estado da Fazenda (SEF);

  Solução: Utilização de esquemas de assinatura digital por delegação, permitindo a assinatura de documentos fiscais pela SEF através do EC (assinante delegado);

- **Problema:** Possibilidade de conferir a autenticidade do documento fiscal impresso;

  Solução: Graças à utilização de código de barras, torna-se possível imprimir características que são lidas de forma automatizada para garantir a autenticidade do documento fiscal impresso.

Além dos problemas solucionados, os objetivos específicos listados no capítulo 1 foram atendidos com as seguintes propostas:

- **Objetivo:** Oferecer uma alternativa de geração de documentos fiscais aos estabelecimentos comerciais e prestadores de serviços dispensando-os da obrigatoriedade da aquisição de equipamentos de impressão fiscal e toda burocracia envolvida, bastando-lhes utilizar plataformas computacionais comuns com acesso à Internet;

  Proposta: Com a utilização do aplicativo ECFV, a emissão de documentos fiscais pode ser realizada a partir de qualquer plataforma computacional, desde que tenha acesso à Internet esporadicamente. Não é necessário adquirir equipamento específico para impressão fiscal. Não há burocracia envolvida no processo: basta o contribuinte estar previamente cadastrado junto à SEF para possibilitar a utilização do aplicativo ECFV;

- **Objetivo:** Diminuir os custos envolvidos no processo de arrecadação de tributos;

  Proposta: Eliminando-se a necessidade de aquisição de equipamento emissor de cupom fiscal (ECF), há uma diminuição de custos para o contribuinte. O Estado tem o benefício de ganho de tempo, pois não precisará controlar as dezenas de empresas fabricantes de equipamentos fiscais. Cabe ao Estado somente disponibilizar

uma infra-estrutura tecnológica adequada ao funcionamento do protocolo ECFV, o que pode significar despesas aos cofres públicos em um primeiro momento;

- **Objetivo:** Propor um sistema menos vulnerável a fraudes de sonegação fiscal;

  Proposta: Considerando que todo documento fiscal virtual gerado é assinado pela SEF, e considerando que o procedimento de verificação da assinatura digital gerada pode ser automatizado, diminui-se as possibilidade de falsificação de documentos fiscais com o uso do protocolo ECFV;

- **Objetivo:** Proporcionar à SEF mecanismos precisos e confiáveis de apuração de impostos devidos;

  Proposta: Os valores registrados no momento da emissão do documento fiscal são enviados imediatamente à SEF para apuração de impostos devidos, considerando a diponibilidade de comunicação entre as entidades do protocolo ECFV. Mesmo não havendo comunicação no momento da geração do documento fiscal, tão logo seja restabelecida a comunicação das entidades os valores são automaticamente enviados para a SEF. Além disso, todas as operações realizadas pelo aplicativo ECFV são registradas em log, possibilitando auditorias fiscais;

- **Objetivo:** Proporcionar ao consumidor final de mercadorias e serviços meios que possibilitem verificar a autenticidade do documento fiscal gerado, conseqüentemente assegurando-lhe que o imposto por ele pago será repassado ao Estado.

  Proposta: Esta é um dos maiores benefícios oferecidos pelo protocolo ECFV. De posse do documento fiscal virtual impresso, o consumidor pode submetê-lo a um procedimento de leitura dos dados para verificação de autenticidade do documento fiscal. O atual sistema utilizado não oferece recursos neste sendido;

- **Objetivo:** Possibilitar à SEF gerar documentos fiscais digitais remotamente, mesmo em situações em que não haja conexão à Internet;

  Proposta: Graças ao uso de técnicas de geração de assinatura digital por delegação, mesmo que não haja comunicação entre a SEF e o EC que registra a venda

realizada, o documento fiscal é gerado pela SEF remotamente através do aplicativo ECFV;

- **Objetivo:** Possibilitar a impressão de documentos fiscais a partir de impressoras comuns, garantindo-se no mínimo os requisitos de segurança obtidos com uso de impressoras fiscais.

  Proposta: O Cupom Fiscal Virtual (CFV) atende aos requisitos exigidos pela legislação através de suas características impressas. O enfoque dos requisitos de segurança, no entanto, não concentram-se mais sobre o equipamento de impressão e sim sobre as informações do documento fiscal virtual;

Deve-se enfatizar uma característica importante proporcionada pelo protocolo ECFV: ocorre o fortalecimento da comunicação entre o consumidor e a Secretaria de Estado da Fazenda. Busca-se desta forma uma aproximação de um modelo ideal de controle sobre os tributos fiscais, como ilustrado pela Figura 2.1, página 14. Conseqüentemente, cada consumidor passa a contribuir de forma ativa no controle do correto registro das operações comerciais realizadas, compensando o baixo número de fiscais empregados pela SEF para esta tarefa. Na guerra do Estado contra a sonegação fiscal, o cidadão pode e deve ser um aliado. É sugerido que algum tipo de benefício, como sorteios premiados, seja oferecido ao consumidor que exige o cupom fiscal virtual e confere sua veracidade.

6.1 Trabalhos futuros

A proposta deste trabalho é a utilização de um protocolo criptográfico que dispensa o uso de equipamentos específicos para emissão de documentos fiscais, agregando benefícios a este processo, como visto no início deste capítulo.

No entanto, vislumbra-se a possibilidade de adicionar ao protocolo ECFV um equipamento de impressão fiscal com características que possibilitem a assinatura digital remota da SEF sobre os documentos fiscais emitidos. Esta proposta, simplificaria o protocolo ECFV, porém os resultados obtidos com esse trabalho continuam sendo interessantes, pois possibilitam ao Estado, entre outras coisas, um controle a distância sobre

os equipamentos de emissão de cupom fiscal. Aos consumidores continuaria sendo oferecido o benefício de verificar a autenticidade do documento fiscal impresso.

Referências Bibliográficas

[BAE 04] BAEK, J. et al. **A Survey of Identity-Based Cryptography**.

[BEL 94] BELLARE, M.; GOLDREICH, O.; GOLDWASSER, S. Incremental cryptography: The case of hashing and signing. 1994. Lectures Notes in Computer Science, 1994.

[BOL 03] BOLDYREVA, A.; PALACIO, A.; WARINSCHI, B. **Secure proxy signature schemes for delegation of signing rights**.

[BOR 02] BORTOLI, D. L. **O Documento Eletrônico No Ofício de Registro Civil de Pessoas Naturais**. Universidade Federal de Santa Catarina, 2002. Dissertação de Mestrado.

[BRA 66] BRASIL. **Lei 5172/66**. Diário Oficial. Dispõe sôbre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios - Brasília (DF) 25 de outubro de 1966.

[BRA 86] BRASIL. **Convênio ICMS 24/86**. Diário Oficial. Dispõe sobre o uso de máquinas registradoras por contribuintes do ICM - Brasília (DF) 19 de junho de 1986.

[BRA 87] BRASIL. **Convênio ICMS 44/87**. Diário Oficial. Dispõe sobre o uso de Terminal Ponto de Venda - PDV por contribuinte do ICM - Brasília (DF) 20 de agosto de 1987.

[BRA 90] BRASIL. **Lei 8137/90**. Diário Oficial. Define crimes contra a ordem tributaria, economica e contra as relações de consumo, e da outras providencias - Brasília (DF) 28 de dezembro de 1990.

[BRA 94] BRASIL. **Convênio ICMS 156/94**. Diário Oficial. Dispõe sobre o uso de Equipamento Emissor de Cupom Fiscal-ECF por contribuintes do ICMS - Brasília (DF) 15 de dezembro de 1994.

[BRA 01a] BRASIL. **Convênio ICMS 85/01**. Diário Oficial. Estabelece requisitos de hardware, de software e gerais para desenvolvimento de equipamento Emissor de Cupom Fiscal (ECF), os procedimentos aplicáveis ao contribuinte usuário de ECF e às empresas credenciadas, e dá outras providências - Brasília (DF) 4 de outubro de 2001.

[BRA 01b] BRASIL. **Medida Provisória 2.200**. Diário Oficial. Institui a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - Brasilia (DF) - 28 de junho de 2001.

[CAL 04] CALLAS, J. **Identity-Based Encryption**. www.pgp.com/resources/ctocorner/identitybased.html.

[CAR 97] CARDOSO, J.; VALLETE, R. **Redes de Petri**. 1a. ed. Editora da UFSC, 1997.

[CAS 01] CASTRO, A. A. **Validade Jurídica de Documentos Eletrônicos. Considerações Sobre O Projeto de Lei Apresentado Pelo Governo Federal**. [Internet] http://www.ambito-juridico.com.br/aj/int0010.htm - data de acesso: 6/4/2004.

[CAT 05] CATALOG, O. O. **Java Cryptography**. [Internet] http://www.oreilly.com/catalog/javacrypt - data de acesso: 5/02/2005.

[CHE 02] CHEN, T. S.; LIU, T. P.; CHUNG, Y. F. A proxy-protected proxy signature scheme based on elliptic curve cryptosystem. In: IEEE TENCOM'02, 2002. [s.n.], 2002. p.184–187.

[CON 04] CONFAZ. **Conselho Nacional de Política Fazendária - CONFAZ**. Disponível em <http://www.fazenda.gov.br/confaz - data de acesso: 10/11/2004.

[CON 05] CONSORTIUM, W. W. W. **Extensible Markup Language (XML)**. Disponível em <http://www.w3c.org/XML/ - data de acesso: 13/02/2005.

[COR 04] CORPORATION, S. **Secure Identity Management**. [Internet] http://www.bizforum.org/whitepapers/safenet.htm.

[dCF 01] DE CARVALHO FERREIRA, L.; DAHAB, R. Blinded-key signatures: securing private keys embedded in mobile agents. Instituto de Computação - Universidade Estadual de Campinas, 2001. Relatório técnico.

[DES 02] DESMOND, P. **Forum Systems Appliance Secures XML Web Services**. [Internet] http://www.esecurityplanet.com/prodser/article.php/1368941.

[DIA 04] DIAS, J. D. S. **Confiança No Documento Eletrônico**. Universidade Federal de Santa Catarina, 2004. Tese de Doutorado.

[GAG 03] GAGNÉ, M. Identity-based encryption: A survey. RSA Laboratories Cryptobyte, 2003. Relatório Técnico1.

[HER 02] HERRANZ, J.; ET AL. **Fully Distributed Proxy Signature Schemes**.

[HER 03] HERRANZ, J.; SAEZ, G. **Revisiting Fully Distributed Proxy Signature Schemes**.

[HEY 93] HEYST, E. V.; PEDERSEN, T. How to make efficient fail stop signatures. In: ADVANCES IN EUROCYPT'92, 1993. Springer-Verlag, 1993. p.366–377.

[HOU 01] HOUAISS, A. **Dicionário Houaiss Da Língua Portuguesa**. Editora Objetiva Ltda., 2001.

[Ide 04] **Association for Automatic Identification and Mobility - Reduced Space Symbology**. [Internet] http://www.aimglobal.org/standards/symbinfo.

[IEE 89] IEEE. **Petri Nets: Properties, Analysis and Applications**, v.77, April, 1989.

[KIM 97] KIM, S.; PARK, S.; WON, D. Proxy signatures, revisited. In: ICICS, 1997. [s.n.], 1997. p.223–232.

[KIM 01] KIM, H. et al. Secure computation with secrets for mobile agent using one-time proxy signature. In: PROC. OF SCIS, 2001. [s.n.], 2001.

[KUS 02] KUSBICK, L. J. B. **A Desmaterialização de Documentos Em Papel: Análise Do Requisito Segurança Para Validade Legal de Documentos Eletrônicos**. Universidade Federal de Santa Catarina, 2002. Dissertação de Mestrado.

[LAL 02] LAL, S.; AWASTHI, A. K. **A New Multi-Proxy Signature Scheme for Partial Delegation with Warrant**.

[LAL 03] LAL, S.; AWASTHI, A. K. **A Scheme for obtaining a Warrant Message from the delegated Digital Proxy Signatures**.

[LEE 97] LEE, G.-S.; LEE, J.-S. Petri net based models for specification and analysis of criptographic protocols. **J. Systems software**, [S.l.], p.141–159, 1997.

[LEE 01] LEE, B.; KIM, H.; KIM, K. Strong proxy signature and its applications. In: PROC. OF SCIS, 2001. [s.n.], 2001.

[MAM 96] MAMBO, M.; USUDA, K.; OKAMOTO, E. Proxy signatures for delegating signing operation. In: CCS'96, 1996. ACM Press, 1996. p.48–57.

[MAR 04] MARTINA, J. E.; CUSTÓDIO, R. F. Módulo de hardware criptográfico HSM LabSEC. Universidade Federal de Santa Catarina, 2004. Relatório técnico.

[NEU 93] NEUMAN, B. C. Proxy-based authorization and accounting for distributed systems. In: INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS, 1993. [s.n.], 1993. p.283–291.

[OAB 04] OAB/SP. **Documentos Eletrônicos**. [Internet] http://cert.oabsp.org.br/info01.htm - data de acesso: 6/4/2004.

[RS 05] RS, S. D. F. **eICMS - ICMS Eletrônico.** [Internet] http://www.sefaz.rs.gov.br/EICMS/.

[SCH 96] SCHNEIER, B. **Applied Cryptography: Protocols, Algorthms, and Source Code in**. second. ed. Wiley Computer Publishing, John Wiley Sons, Inc., January, 1996.

[SHA 84] SHAMIR, A. Identity-based cryptosystems and signature schemes. In: ADVANCES IN CRYPTOLOGY - CRYPTO'84, 1984. [s.n.], 1984. p.47–53.

[STI 02] STINSON, D. R. **Cryptography: Theory and Practice**. second. ed. Chapman Hall/CRC, 2002.

[TAN 04a] TAN, Z.; LIU, Z. **On the Security of some Nonrepudiable Treshold Proxy Signature Schemes with Known Signers**.

[TAN 04b] TAN, Z.; LIU, Z. **Provably Secure Delegation-by-Certification Proxy Signature Schemes**.

[TEC 04] TECHNOLOGIES, S. **PDF417 - Products**. [Internet] http://www.pdf417.com/products.htm.

[WAN 02] WANG, S. et al. **Cryptanalysis of A Proxy-Protected Proxy Signature Scheme Based on Elliptic Curve Cryptosystem**.

[WAN 03] WANG, G. **Designated-Verifier Proxy Signatures for e-Commerce**.

[WAR 03] WARNECKE, E. **G-DEF - Protocolo Criptográfico Para Geração de Documento Eletrônico Fiscal Nas Operações Entre Empresas**. Universidade Federal de Santa Catarina, 2003. Dissertação de Mestrado.

[WIK 04] WIKIPEDIA, T. F. E. **PDF417**. [Internet] http://en.wikipedia.org/wiki/PDF417 - data de acesso: 12/11/2004.

[ZHA 03] ZHANG, F.; SAFAVI-NAINI, R.; LIN, C.-Y. **New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairings**.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo