UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Bruno Imhof

CONTROLE DE MEDICAMENTOS UTILIZANDO PRESCRIÇÕES DIGITAIS SEGURAS

Florianópolis

2012

Bruno Imhof

CONTROLE DE MEDICAMENTOS UTILIZANDO PRESCRIÇÕES DIGITAIS SEGURAS

Trabalho de conclusão de curso submetido ao Curso de Bacharelado em Ciências da Computação para a obtenção do Grau de Bacharel em Ciências da Computação.
Orientador: Ricardo Felipe Custódio, Dr.
Coorientador: Eduardo Dos Santos

Florianópolis

2012

Catalogação na fonte elaborada pela biblioteca da
Universidade Federal de Santa Catarina

A ficha catalográfica é confeccionada pela Biblioteca Central.

Tamanho: 7cm x 12 cm

Fonte: Times New Roman 9,5

Maiores informações em:
http://www.bu.ufsc.br/design/Catalogacao.html

Bruno Imhof

CONTROLE DE MEDICAMENTOS UTILIZANDO PRESCRIÇÕES DIGITAIS SEGURAS

Este Trabalho de conclusão de curso foi julgado aprovado para a obtenção do Título de "Bacharel em Ciências da Computação", e aprovado em sua forma final pelo Curso de Bacharelado em Ciências da Computação.

Florianópolis, 4 de junho 2012.

Ricardo Felipe Custódio, Dr.
Orientador

Eduardo Dos Santos
Coorientador

Banca Examinadora:

Jean Everson Martina, Ph.D.
Presidente

Luciana Tricai Cavalini, Dra

Aos pais pelo amor na criação, ao irmão pela amizade, à família pelo suporte e aos amigos pela convivência.

AGRADECIMENTOS

Aos colegas do LabSEC da UFSC, cujas críticas e análises possibilitaram o aperfeiçoamento do modelo.

Ao professor Ricardo Felipe Custódio, por me acolher em seu laboratório e por sempre ter apoiado o projeto.

RESUMO

Instituído pela Portaria344/98, o sistema de controle de medicamentos atual apresenta diversos problemas. A ilegibilidade e a imprecisão das informações prescritas manualmente pode acarretar em prejuízos para pacientes e governo. Além disso, o monitoramento que é feito da dispensação destas substâncias no âmbito nacional é sujeito a falhas, pois transcrição das informações das prescrições para o meio digital ocasiona em erros. Recentemente, com a instituição do Sistema Nacional de Controle de Medicamentos, o Governo Federal estabeleceu um novo modelo para o rastreamento de medicamentos. Mas existem desafios quanto a identificação de pacientes e agentes de saúde. A utilização de identidades digitais possibilita a autenticação dos usuários com mais segurança, e sua difusão no cenário nacional viabiliza o desenvolvimento de novos sistemas de controle.

Deparando-se com os novos recursos e a necessidade de novas soluções para o rastreamento de medicamentos, esse trabalho foca-se na criação de um protocolo que tem por objetivo garantir a integridade, autenticação e sigilo das informações referentes ao seu controle. São propostos um conjunto de três protocolos em um modelo construtivo. O intuito é tornar o sistema flexível permitindo que o processo de implantação aconteça em diferentes etapas. Finalizando, é desenvolvido uma prova de conceito para mostrar a viabilidade dos protocolos propostos. O protótipo utiliza os padrões brasileiros para assinatura digital em uma estrutura independente de aplicação, multiplataforma e livre.

Palavras-chave: Política Nacional de Medicamentos, Medicamentos de Controle Especial, Prescrição Eletrônica, Protocolo de Segurança, Assinatura Digital.

ABSTRACT

The drug control established by the Normative Decree SVS/MS 344/98 presents several problems. The illegibility and the inaccuracy of the information prescribed manually can result in harm to patients and government. In addition, monitoring of the dispensing is done these substances nationally is prone to failure, since transcription of information from prescriptions for digital media leads to errors. Recently, the institution of National Drug Control, the Federal Government established a new model for the drug tracking. But there are challenges in identifying patients and health workers. The use of digital identities enables the authentication of users with more security, and its dissemination on the national stage enables the development of new control systems.

Faced with the need for new resources and new solutions for the screening of drugs, this work focuses on creating a protocol that aims to ensure the integrity, authentication and confidentiality of information relating to their control. We propose a set of three protocols in a constructive model. The aim is to make the system flexible allowing the deployment process occurs in different steps. Finally, it developed a proof of concept to show the feasibility of the proposed protocols. The prototype uses Brazilian standards for digital signature on an independent structure of application, platform and free.

Keywords: National Drug Policy, Drugs of Special Control, Electronic Prescription, Computerized Medical Records Systems, Digital Signature

LISTA DE FIGURAS

Figura 1 Notificação Receita A 33
Figura 2 Notificação Receita B 34
Figura 3 Descrição dos passos do controle de medicamentos 35
Figura 4 Notificação Receita Azul 36
Figura 5 Notificação Receita Branca 37
Figura 6 Exemplo do uso da chave simétrica 46
Figura 7 Exemplo do uso da chave assimétrica 48
Figura 8 Exemplo do processo de assinatura e validação 50
Figura 9 Certificado X.509(STALLINGS, 2010) 52
Figura 10 Lista de Certificados Revogados(STALLINGS, 2010) 54
Figura 11 CRM-Digital 59
Figura 12 Certificado digital emitido pela Receita Federal 59
Figura 13 Registro de Identidade Civíl 60
Figura 14 Casos de uso do sistema. 61
Figura 15 Exemplo da notação utilizada. 63
Figura 16 Versão simplificada do protocolo. 65
Figura 17 Notação formal da proposta simpleficada do protocolo. 65
Figura 18 Versão completa do protocolo. 67
Figura 19 Notação formal da proposta do protocolo completa. 68
Figura 20 Versão completa do protocolo com autenticação multi-fator . . 69
Figura 21 Notação formal da proposta completa englobando autenticação com biometria. 70
Figura 22 Tabelas do banco de dados 72
Figura 23 Camadas de processamento para assinatura de documentos eletrônicos médicos 73
Figura 24 Estrutura do componente SCiPhOEr 74

LISTA DE ABREVIATURAS E SIGLAS

AC	*Autoridade Certificadora*
ANVISA	*Agência Nacional de Vigilância Sanitária*
CAdES	*CMS Advanced Electronic Signatures*
CFM	*Conselhor Federal de Medicina*
ICP	*Infra-Estrutura de Chaves Públicas*
ICP-Brasil	*Infra-Estrutura de Chaves Públicas Brasileira*
IUM	*Identificador Único do Medicamento*
LCR	*Lista de Certificados Revogados*
LRE	*Livro de Registro Específico*
ONU	*Organização das Nações Unidas*
SNCM	*Sistema Nacional de Controle de Medicamentos*
SNGPC	*Sistema Nacional de Gerenciamento de Produtos Controlados*
SSL/TLS	*Secure Sockets Layer/Transport Layer Security*
XAdES	*XML Advanced Electronic Signatures*

SUMÁRIO

1 INTRODUÇÃO 23
1.1 JUSTIFICATIVA 24
1.2 OBJETIVOS DO TRABALHO 25
1.2.1 Objetivo Geral 25
1.2.2 Objetivos Específicos 25
1.3 ESTRUTURA DO TRABALHO 25
2 CONTROLE DE MEDICAMENTOS 27
2.1 MEDICAMENTO COMO POTENCIAL CAUSADOR DE DANO 27
2.2 ASPECTOS LEGAIS 28
2.2.1 Restrição de Substância pelo Estado 28
2.2.1.1 Sistema Nacional de Gerenciamento de Produtos Controlados . 29
2.2.1.2 Sistema Nacional de Controle de Medicamentos 29
2.2.2 Legislação relacionada ao uso de registros eletrônicos 30
2.3 CONTROLE DE MEDICAMENTOS 31
2.3.1 Classificação dos Medicamentos 31
2.3.2 Mecanismos de Controle 32
2.3.2.1 Notificação de Receita 32
2.3.2.2 Livro de Registro Específico 33
2.3.2.3 Dispensação 34
2.3.3 Fluxo de Controle 34
2.4 DEFICIÊNCIAS DO PROCESSO 35
2.4.1 Erros Envolvendo Medicamentos 35
2.4.2 Má Utilização de Prescrições e Aquisição Irregular 36
2.4.3 Remarcação de Consultas para Emissão de Segunda Via 38
2.4.4 Tratamentos Contínuos ou de Longo Prazo 38
2.4.5 Adulterabilidade e Legitimidade do Documento 39
2.4.6 Dispensação Manual 39
2.4.7 Custos 39
2.5 POSSÍVEIS MELHORIAS COM A INFORMATIZAÇÃO DO PROCESSO 40
2.5.1 Sistemas de Prescrição Eletrônica 40
2.5.2 Automatização do Controle e da Dispensação dos Medicamentos 40
2.5.3 Integridade e Autenticidade do Documento 41
2.5.4 Acesso à Segunda Via da Prescrição 41
2.5.5 Documento Digital 41
2.5.6 Incorporação de Novas Tecnologias 41

2.5.7 Custos ... 42
2.6 CONSIDERAÇÕES ... 42
3 FUNDAMENTOS DA ASSINATURA DIGITAL ... 45
3.1 CRITPOGRAFIA ... 45
3.1.1 Criptografia Simétrica ... 46
3.1.2 Criptografia Assimétrica ... 47
3.1.3 Função de Resumo Criptográfico ... 49
3.1.4 Assinatura Digital ... 49
3.1.5 Protocolos Criptográficos ... 51
3.1.6 Autenticação ... 51
3.2 CERTIFICAÇÃO DIGITAL ... 52
3.2.1 Certificado Digital ... 52
3.2.2 Autoridade Certificadora ... 53
3.2.3 Revogação de Certificados ... 53
3.2.4 Infraestrutura de Chaves Públicas ... 54
3.2.5 Política de Assinatura ... 55
3.2.6 ICP - Brasil ... 56
4 PROPOSTA DE PROTOCOLO ... 57
4.1 ANALISE DO CONTROLE DE MEDICAMENTOS ... 57
4.2 ATORES DO SISTEMA ... 58
4.2.1 CRM-Digital ... 58
4.2.2 e-CPF ... 59
4.2.3 CRF-Digital ... 60
4.2.4 Registro de Identidade Civíl (RIC) ... 60
4.3 REQUISITOS DO PROJETO ... 60
4.4 DOCUMENTO ELETRÔNICO ... 61
4.4.1 Prescrição ... 61
4.4.2 Dispensação ... 62
4.5 CENTRAL DE PRESCRIÇÕES ... 62
4.6 PROJETO PROCESSO ELETRÔNICO ... 63
4.6.1 Notação Formal ... 63
4.6.2 Protocolo Médico-Farmacêutico ... 64
4.6.3 Protocolo Médico-Farmacêutico-Paciente ... 66
4.6.4 Protocolo Multifator Médico-Farmacêutico-Paciente ... 68
5 PROTOTIPO DO PROJETO ... 71
5.1 TRABALHOS RELACIONADOS ... 71
5.2 ESTRUTURA DA APLICAÇÃO ... 72
5.3 TECNOLOGIAS UTILIZADAS ... 74
5.3.1 Signer-SCiPhOEr ... 74
5.3.2 Central-SCiPhOEr ... 75
6 CONCLUSÃO ... 77

7 TRABALHOS FUTUROS 79
REFERÊNCIAS 81

1 INTRODUÇÃO

Com o avanço dos sistemas computacionais registrado nas últimas décadas, diversos setores passaram a contar com sistemas de informação para gestão. Na área da saúde, em particular, diversos motivos contribuíram neste sentido. O primeiro deles é a inviabilidade do arquivamento de grande quantidade de registros de pacientes, em especial, prontuários médicos. A dificuldade de realização desta tarefa aumenta exponencialmente ao considerarmos um país populoso como o Brasil. Além disso, fatores como a obrigatoriedade da manutenção destes documentos por longos períodos de tempo, a necessidade de redução de custos por estabelecimentos de saúde e a consequente otimização de espaço físico, impulsionaram o registro e processamento em meio eletrônico dessas informações (CFM, 2002a).

Considerando as diferenças geográficas e epidemiológicas em um país tão extenso e diversificado como o Brasil, torna-se praticamente impossível de se estabelecer um sistema de informação verticalizado de gestão de saúde pública.

A necessidade de adequação dos sistemas médicos às características locais específicas, juntamente à carência da centralização e transmissão das informações clínicas do paciente, gera demandas para o desenvolvimento de modelagem de dados multi-nível. O desafio é convergir as diferentes tecnologias para tornar a informação acessível, inteligível e semânticamente coerente (EICHELBERG et al., 2005).

No Brasil, existem algums tipos de medicamentos que só podem ser vendidos à população com a apresentação de uma prescrição assinada por um médico autorizado. São confeccionados talões de receitas e distribuídos aos médicos pela Agência Nacional de Vigilância Sanitária.

Além dos custos que são gerados com as ferramentas manuais, segundo (GHALEB et al., 2005), anualmente, muitos pacientes são prejudicados por erros de medicamentos, sendo que cerca de um terço desses erros podem ser evitados. Como conseqüência, iniciativas políticas têm sido implementadas em uma tentativa de reduzir os eventos adversos a medicamentos. Erros de medicação são uma das causas mais comuns de eventos adversos, incluindo a prescrição, transcrição, dispensação e erros na administração.

Não bastecem os prejuízos que podem ser acarretados ao paciente pelo uso incorreto das prescrições, ainda existem problemas quanto aos remédiso. O relatório anual da Organização das Nações Unidas (ONU), traz o alerta para o risco que os mediamentos falsificados podem trazer à saúde dos pacientes e as implicações que o comércio ilícito trazem à sociedade. Os danos à saúde se referem ao consumo de um medicamento falso, prejudicando o tratamento do

paciente, e o consumo desavisado e ou abusivo de substâncias que podem ser nocivas. O perigo é real e de tamanho considerável. A Organização Mundial da Saúde (OMS) estima que 25% a 50% dos remédios consumidos em países em desenvolvimento sejam falsificados(ONU, 2006).

Visando aumentar a segurança dos pacientes com os medicamentos comercializados no país, em 2009, o Governo Federal instituiu o Sistema Nacional de Controle de Medicamentos (SNCM) (BRASIL, 2009). Este novo sistema tem como objetivo monitorar todas as etapas que envolvem o ciclo de vida de um medicamento, cobrindo desde sua fabricação e transporte até sua dispensação e consumo pelo população.

Diante de todas estas iniciativas de automatização, ficam claros os primeiros indícios de que o processo de controle de medicamentos precisa de uma revisão.

Atualmente, apenas a primeira etapa do SNCM, responsável pelo monitoramento de indústrias e fornecedores de medicamentos, está em vigor. As demais etapas, correspondentes ao rastreamento do médico, farmacêutico, paciente, além da própria prescrição, ainda não entraram em funcionamento.

A proposta deste trabalho é a análise de um sistema, junto com a formalização de um protocolo, para controle de medicamentos que envolva as partes cuja interação não é coberta pelo estágio atual do SCNM, ou seja, médicos, farmacêuticos, pacientes, prescrição e dispensação.

1.1 JUSTIFICATIVA

A ilegibilidade e a imprecisão das prescrições feitas a mão é um problema gravíssimo em todo o mundo. Pacientes são diretamente prejudicados se o farmacêutico interpretar erroneamente as informações sobre seu tratamento, ou medicamento prescrito. Além desses prejuízos diretos a sua saúde, há casos em que os pacientes que utilizam medicamentos controlados precisam retornar ao médico para emissão de uma segunda via desnecessariamente. Diferentes são os motivos: ter perdido ou violado a prescrição,se ela estiver vencida, não adquirir todos os itens simultaneamente, entre outros. A informatização do processo de controle resolve todos esses problemas.

O intuito deste trabalho é propor um novolo modelo para o controle de medicamentos. O meio digital permite aumentar a segurança das prescrições, podendo melhorar a qualidade do tratamento medicamentoso. A utilização de prescrições eletrônicas busca reduzir os gastos, trazer facilidades ao paciente, aprimorar o monitoramento da distribuição das substâncias dispensadas, e se enquadrar dentro das normas de rastreamento das informações que foram recentemente instituídas com o SNCM. Este trabalho, é uma iniciativa de

unir a confiança das identidades digitais a as etapas do novo monitoramento instituído.

1.2 OBJETIVOS DO TRABALHO

1.2.1 Objetivo Geral

Propor estratégias para a forma como são controladas as prescrições e as dispensações dos medicamentos controlados no Brasil. O sistema projetado utiliza tecnologias estabelecidas, e tem como foco oferecer um melhor tratamento ao paciente, prezando pela segurança e a rastreabilidade de todas as informações necessárias para o modelo estabelecido pelo SNCM.

1.2.2 Objetivos Específicos

- Estudar a legislação vigente relacionada ao controle de medicamentos pelo Estado.
- Conceber um protocolo que seja capaz de garantir a autenticidade e a confidencialidade das informações trocadas no processo do controle de medicamentos adequando-se as etapas de implantação do SNCM.
- Projetar um sistema que seja capaz de suportar o protocolo desenvolvido, levantando casos de uso, funcionalidades, e requisitos.
- Desenvolver uma prova de conceito das operações definidas no protocolo simulando uma parte do sistema.

1.3 ESTRUTURA DO TRABALHO

No segundo capítulo são descritos o processo de venda e distribuição de medicamentos no Brasil contextualizando com a legislação vigente. Tem como objetivo contextualizar o leitor fazendo uma descrição de como cada etapa do processo se organiza explorando seus desafio e apontando motivos para sua informatização. No capítulo seguinte, são descritos os aspectos pertinentes à criptografia e a segurança das informações. O capítulo quatro apresenta os protocolos que são concebidos no trabalho e o projeto do sistema. O quinto capítulo trata o protótipo do projeto, o sistema SCiPhOEr. No sexto capítulo são trazidas as conclusões alcançadas com a elaboração e

do protótipo do sistema. Por último, o capítulo sete, trata sobre os trabalhos futuros que podem ser realizados a partir deste.

2 CONTROLE DE MEDICAMENTOS

Este capítulo descreve o processo de prescrição, venda e distribuição de medicamentos em âmbito nacional. Primeiramente é trazido o contexto histórico aonde se começou a entender a necessidade do uso racional de medicamentos. Em seguida, é tratada toda a parte de legal referente as responsabilidades dos envolvidos no processo, desde a prescrição por parte do médico, até dispensação por parte dos farmacêuticos e como o governo atua no seu papel de fiscalizador. Ainda são abordados os erros mais comuns envolvendo medicamentos, estes que acontecem justamente na hora de sua prescrição. Ao final deste capítulo é feita uma retrospectiva trazendo os principais pontos levantados e algumas das abordagens que serão posteriormente desenvolvidas.

2.1 MEDICAMENTO COMO POTENCIAL CAUSADOR DE DANO

Segundo (Weatherall, 1990), para os gregos, phármakon era aquilo que poderia trazer tanto o bem quanto o mal, manter a vida ou causar a morte.

O potencial causador de danos dos medicamentos só passou a chamar a atenção no século XX, inicialmente em função de inúmeros relatos de mortes súbitas durante anestesia com clorofórmio(Grahame-Smith, Aronson, 2002).

Com as constantes descobertas sobre novos fármacos terapêuticos, o número de acidentes relacionados a tratamentos farmacológicos também foi aumentando. Neste cenário, foram iniciados os primeiros estudos com enfoque na utilização racional de medicamentos, em resposta à necessidade de se conhecer e relatar os problemas relacionados à medicação e da elevada morbidade e mortalidade associada ao uso inadequado dos medicamentos (OMS, 1969).

Assim o conceito da “pílula milagrosa”,que beneficia a saúde do homem, foi sendo contraposto pelos riscos e prejuízos causados pelos medicamentos(Lefevre, 1991). Dessa forma, iniciou-se a discussão de algumas questões relevantes, como o uso indiscriminado e incorreto do medicamento e os possíveis efeitos adversos e interações relacionadas ao tratamento medicamentoso(Mant, 1994).

2.2 ASPECTOS LEGAIS

Nesta seção, serão abordados os aspectos legais referente ao controle de medicamentos no Brasil. Primeiro são apresentadas as leis que envolvem a venda e a distribuição de medicamentos, juntamente com os mecanismos governamentais criados para o monitoramento. Em seguida, são esclarecidos os aspectos da legislação que tratam dos prontuários eletrônicos. Por último, são feitas considerações respectivas ao trabalho que será proposto.

2.2.1 Restrição de Substância pelo Estado

O controle especial foi estabelecido porque determinados medicamentos, apesar de eficazes, podem oferecer riscos elevados à saúde se o consumo não for racional e adequado. As autoridades sanitárias tem como meta o equilíbrio entre o acesso de quem precisa utilizar medicamentos controlados e a restrição ao uso abusivo(ANVISA, 2012).

No Brasil, a lei vigente que regula a venda e distribuição dos medicamentos sujeitos a controle é a Portaria 344/98 do Ministério da Saúde. Esta portaria contempla a venda e distribuição através do processo manuscrito(BRASIL, 1998), o médico preenche uma notificação de receita que junto da prescrição medicamentosa autoriza a aquisição do medicamento pelo paciente junto ao farmacêutico. Após a dispensação do medicamento, o farmacêutico é encarregado de gerenciar os dispensários para fins de fiscalização. Na próxima seção são apresentadas modelos de notificação de receita, diagramando o fluxo e os mecanismos utilizados para o controle.

Com a evolução dos sistemas informatizados, foi aumentado em mais um passo o caminho para dispensação final dos medicamentos. O lançamento do Sistema Nacional para Gerenciamento de Produtos Controlados (SNGPC), agregou ao farmacêutico a responsabilidade de transcrever as informações do Livro de Registro Específico (LRE) para o sistema digital semanalmente(ANVISA, 2012).

Posteriormente é criado o Sistema Nacional Controle de Medicamentos (SNCM), e o SNGPC é incorporado ao novo sistema. O novo cenário trás a necessidade de informatização das outras etapas junto com o rastreamento dos medicamentos.

2.2.1.1 Sistema Nacional de Gerenciamento de Produtos Controlados

O Sistema Nacional de Gerenciamento de Produtos Controlados (SNGPC) foi instituído pela Agência Nacional de Vigilância Sanitária(ANVISA) no ano de 2007. Farmácias e drogarias que dispensam medicamentos controlados devem aderir à nova solução, que capta dados de todo o ciclo destes tipos de produtos(ANVISA, 2012)

O comunicado ao SNGPC é semanal e feito pela internet. Anteriormente, o anúncio da venda de medicamentos controlados era feito a mão, posteriormente enviado à Vigilância Sanitária Municipal, para então os dados serem repassados a ANVISA a cada trimestre(ANVISA, 2012).

2.2.1.2 Sistema Nacional de Controle de Medicamentos

Em 2009 foi decretada uma nova lei que tem prazo de homologação de até 3 anos e por isso, ainda não foi totalmente implementada. Segundo a nova Lei 11903, de 22/04/2009(BRASIL, 2009) no seu Art. 2o

> "Todo e qualquer medicamento produzido, dispensado ou vendido no território nacional será controlado por meio do Sistema Nacional de Controle de Medicamentos. Parágrafo único. O controle aplica-se igualmente às prescrições médicas, odontológicas e veterinárias."

A nova Lei prevê implementação do sistema, mas ainda não apresenta mecanismos definidos. O terceiro artigo especifica as informações que agora deverão ser rastreadas eletronicamente.

> "O controle será realizado por meio de sistema de identificação exclusivo dos produtos, prestadores de serviços e usuários, com o emprego de tecnologias de captura, armazenamento e transmissão eletrônica de dados.
> § 1o Os produtos e seus distribuidores receberão identificação específica baseada em sistema de captura de dados por via eletrônica, para os seguintes componentes do Sistema Nacional de Controle de Medicamentos:
> I – fabricante (autorização de funcionamento, licença estadual e alvará sanitário municipal dos estabelecimentos fabricantes);
> II – fornecedor (atacadistas, varejistas, exportadores e importadores de medicamentos);
> III – comprador (inclusive estabelecimentos requisitantes de produtos não aviados em receitas com múltiplos

> produtos);
> IV – produto (produto aviado ou dispensado e sua quantidade);
> V – unidades de transporte/logísticas;
> VI – consumidor/paciente;
> VII – prescrição (inclusive produtos não aviados numa receita com múltiplos produtos);
> VIII – médico, odontólogo e veterinário (inscrição no conselho de classe dos profissionais prescritores).”(BRASIL, 2009)

Ainda no mesmo decreto, ficam estipulados diferentes etapas de implantação e seus respectivos prazos.

> ”O órgão de vigilância sanitária federal competente implantará o sistema no prazo gradual de 3 (três) anos, sendo a inclusão dos componentes referentes ao art. 3o desta Lei feita da seguinte forma:
> I – no primeiro ano, os referentes aos incisos I e II do § 1o;
> II – no segundo ano, os referentes aos incisos III, IV e V do § 1o;
> III – no terceiro ano, os referentes aos incisos VI, VII e VIII do § 1o;”(BRASIL, 2009)

Atualmente a implantação do sistema ainda está na primeira etapa. Apenas a tecnologia utilizada para a identificação individualizada dos medicamentos foi definida. A escolhida em comum acordo com a indústria foi o Datamatrix. O Datamatrix é um código de barras bidimensional composto por células brancas e pretas em um formato quadrado(ISO/IEC, 2006).

A proposta desse trabalho vai ao encontro da nova Lei, que visa dar mais segurança ao consumidor e realizar um rastreamento completo do processo de venda e distribuição de medicamentos controlados.

2.2.2 Legislação relacionada ao uso de registros eletrônicos

Com a aprovação da (CFM, 2002b), abriu-se o caminho para a utilização dos sistemas informatizados. As validade e a segurança das informações referentes aos prontuários eletrônicos dos pacientes ficam asseguradas pela utilização dos certificados emitidos pela ICP-Brasil.

Posteriormente, a resolução 1.821, de 11 de julho de 2007, do Conselho Federal de Medicina, considera que as unidades de serviços de apoio diagnóstico e terapêutico têm documentos próprios, mas que fazem parte dos prontuários eletrônicos, autorizando a eliminação do papel e a troca de

informação em saúde. (CFM, 2007).

2.3 CONTROLE DE MEDICAMENTOS

Apenas algumas categorias de substâncias são sujeitas a um controle especial. Uma parcela menor ainda necessita que as dispensas sejam registradas e informadas posteriormente a entidade reguladora. Mas para esta parcela, fica estabelecido que toda a sua movimentação deve ser registrada, e que as autoridades tenham acesso a estas informações.

Como o tema deste trabalho são os medicamentos controlados, esta seção apresenta as categorias restritas, os mecanismos junto com o fluxo do processo atual e as entidades responsáveis atuantes.

2.3.1 Classificação dos Medicamentos

Os medicamentos são divididos em categorias e organizados em listas, sendo necessário o controle em cima de algumas substâncias específicas. Estas categorias estão dispostas da seguinte maneira:

- A1 - Lista das substâncias entorpecentes
- A2 - Lista das substâncias entorpecentes
- A3 - Lista das substâncias psicotrópicas
- B1 - Lista das substâncias psicotrópicas
- B2 - Lista das substâncias psicotrópicas anorexígenas
- C1 - Lista das outras substâncias sujeitas a controle especial
- C2 - Lista de substâncias retinóicas
- C3 - Lista de substâncias imunodepressoras
- C4 - Lista das substâncias anti-retrovirais
- C5 - Lista das substâncias anabolizantes
- D1 - Lista de substâncias precursoras de entorpecentes e/ou psicotrópicos
- D2 - Lista de insumos químicos utilizados como precursores para frabricação e síntese de entorpecentes e/ou psicotrópicos

- E - Lista de plantas que podem originas substâncias entorpecentes e/ou psicotrópicas.
- F1 - Lista das substâncias entorpecentes
- F2 - Lista das substâncias psicotrópicas

2.3.2 Mecanismos de Controle

As ferramentas utilizadas para se fazer uma restrição dessas substâncias, serão abaixo descritas.

2.3.2.1 Notificação de Receita

A Notificação de Receita é o documento que acompanhado de receita autoriza a dispensação de medicamentos, a base de substâncias constantes das listas “A1” e “A2” (Entorpecentes), “A3”, “B1” e “B2” (Psicotrópicos) “C2” (Retinóicas para uso sistêmico) “C3” (Imunossupressoras).(BRASIL, 1998)

O artigo 36 define o documento utilizado para a prescrição do tratamento medicamentoso.

”A Notificação de Receita deverá conter os itens referentes as alíneas a, b e c devidamente impressos e apresentando as seguintes características:

a) sigla da Unidade da Federação;

b) identificação numérica: a seqüência numérica será fornecida pela Autoridade Sanitária competente dos Estados, Municípios e Distrito Federal;

c) identificação do emitente: nome do profissional com sua inscrição no Conselho Regional com a sigla da respectiva Unidade da Federação; ou nome da instituição, endereço completo e telefone;

d) identificação do usuário: nome e endereço completo do paciente, e no caso de uso veterinário, nome e endereço completo do proprietário e identificação do animal;

e) nome do medicamento ou da substância: prescritos sob a forma de Denominação Comum Brasileira (DCB), dosagem ou concentração, forma farmacêutica, quantidade (em algarismos arábicos e por extenso) e posologia;

f) símbolo indicativo: no caso da prescrição de retinóicos deverá conter um símbolo de uma mulher grávida, recortada ao meio, com a seguinte advertência: ”Risco de graves defeitos na face, nas orelhas, no coração e no sistema nervoso do feto”;

g) data da emissão;

h) assinatura do prescritor: quando os dados do profissional estive-

Figura 1: Notificação Receita A

rem devidamente impressos no campo do emitente, este poderá apenas assinar a Notificação de Receita. No caso de o profissional pertencer a uma instituição ou estabelecimento hospitalar, deverá identificar a assinatura com carimbo, constando a inscrição no Conselho Regional, ou manualmente, de forma legível;

i) identificação do comprador: nome completo, número do documento de identificação, endereço completo e telefone;

j) identificação do fornecedor: nome e endereço completo, nome do responsável pela dispensação e data do atendimento;

l) identificação da gráfica: nome, endereço e C.N.P.J./ C.G.C. impressos no rodapé de cada folha do talonário. Deverá constar também, a numeração inicial e final concedidas ao profissional ou instituição e o número da Autorização para confecção de talonários emitida pela Vigilância Sanitária local;

m) identificação do registro: anotação da quantidade aviada, no verso, e quando tratar-se de formulações magistrais, o número de registro da receita no livro de receituário."

As figuras 1 e 2 são imagens das Notificações de Receita A e B.

2.3.2.2 Livro de Registro Específico

Segundo (BRASIL, 1998) os LRE é destinado à anotação, em ordem cronológica, de estoques, de entradas, de saídas e de perdas de medicamentos sujeitos ao controle especial.

A instituição do SNGPC simplificou o LRE a um mecanismo de controle manual da farmácia, podendo ser substituído por sistemas informatizados. O cadastramento de informações nesse livros ou sistemas, é uma

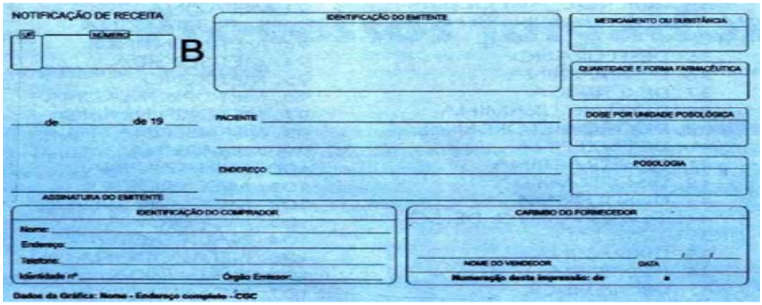


Figura 2: Notificação Receita B

etapa abstraída para os efeitos deste trabalho, sendo tratada apenas o envio das informações ao serviço disponibilizado pela ANVISA.

2.3.2.3 Dispensação

Todo estabelecimento, entidade ou órgão oficial que comercializar, distribuir, beneficiar, vender, comprar substância ou medicamento de que trata a (BRASIL, 1998), com qualquer finalidade deverá escriturar e manter no estabelecimento para efeito de fiscalização e controle.

(BRASIL, 1998)A Notificação é retida pela farmácia ou drogaria e a receita devolvida ao paciente devidamente carimbada, como comprovante do aviamento ou da dispensação.

Além de alimentar os livros de escrituração, os estabelecimentos também são obrigados a manter os livros, balanços, e os demais documentos comprovantes da movimentação do estoque das substâncias “C3” (Imunossupressoras) por 5 anos.

As informações que são transcritas ao SNGPC, são todas as que estão registradas nos LREs. O farmacêutico é o responsável por alimentar o sistema, acrescentando mais uma etapa no controle dos medicamentos(ANVISA, 2012).

2.3.3 Fluxo de Controle

A figura 3 descreve as etapas do processo.

No primeiro passo, o médico prescreve uma receita e entrega ao paciente, na segunda etapa, o paciente munido da prescrição dirige-se a uma dro-

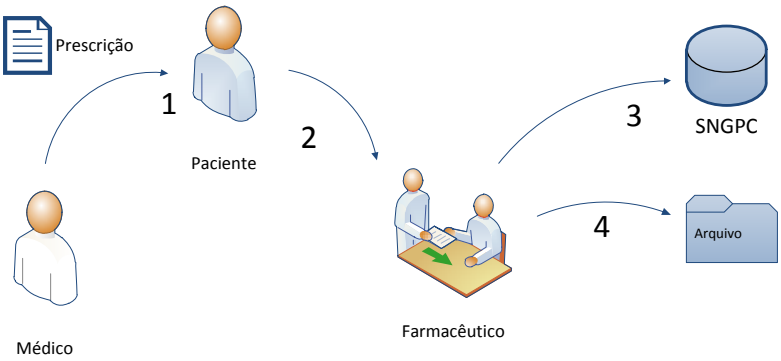


Figura 3: Descrição dos passos do controle de medicamentos

garia. O farmacêutico verifica a identidade do paciente e fornece o medicamento. As duas vias apresentadas são então assinadas ambos farmacêutico e paciente. Uma via fica com o paciente, pois ali também constam informações do tratamento farmacológico enquanto a outra via fica de posse do farmacêutico responsável, para fins de dispensação. Semanalmente ele precisa transcrever as informações para o SNGPC, terceiro estado do protocolo. Por último, todos os documentos envolvidos no trâmite de algumas categorias de medicamentos, precisam ser armazenados por 5 anos.

2.4 DEFICIÊNCIAS DO PROCESSO

Nesta seção serão descritas deficiências do processo de controle de medicamentos.

2.4.1 Erros Envolvendo Medicamentos

Segundo (KAWANO et al., 2006), os erros na medicação têm relação com o aumento do número de medicamentos disponíveis no mercado, com as várias vias de administração, com os regimes terapêuticos complexos e com as dificuldades dos profissionais em atualizarem os seus conhecimentos quanto às características do medicamento (indicações, efeitos colaterais etc.).

A prescrição manuscrita aumenta a probabilidade de apresentar pro-

Figura 4: Notificação Receita Azul

blemas de legibilidade, quando a letra do prescritor não é clara. Isso incrementa a chance de erros de medicamentos(AGUIAR; SILVA; FERREIRA, 2006). As figuras 4 e 5 são prescrições medicamentosas utilizando notificação de receita. Observa-se claramente que a ilegibilidade afeta diretamente a interpretação das informações referentes ao tratamento farmacológico.

Entende-se que as prescrições incompletas, ilegíveis ou com rasuras impedem a eficiência da dispensação, colocando em risco a qualidade da assistência farmacêutica ao paciente, levando ao comprometimento no tratamento medicamentoso e erros de medicação(BENJAMIN, 2003).

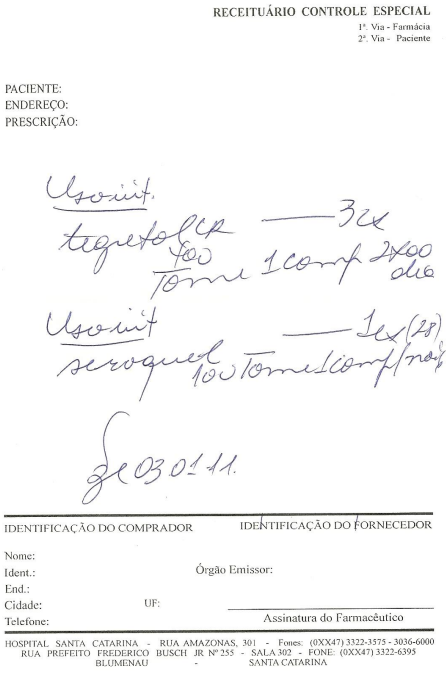
No caso dos medicamentos psicoativos, tema deste trabalho devido ao controle especial (BRASIL, 1998), a prescrição incompleta ou ilegível pode levar ao uso inadequado e até mesmo o uso abusivo dessas substâncias(NOTO, 2002).

Como a prescrição do medicamento pelo médico é parte processo do controle de medicamentos, os erros envolvendo o preenchimento incorreto, ilegível ou indevido caracterizam-se como deficiências.

2.4.2 Má Utilização de Prescrições e Aquisição Irregular

O processo manual de prescrição da notificação de receita leva vários médicos a uma má utilização do controle. Frequentemente apenas uma receita é preenchida, diferentes medicamentos e quantidades referentes a um período estendido são todas concentradas no mesmo documento. A não individualização dos medicamentos em receitas respectivas, abre possibilidades para aquisição irregular, e ocasiona na necessidade do paciente de requerer uma segunda via.

Há casos de pacientes que não consomem a quantidade total dos itens descritos na receita, gerando uma espécie de “gordura” de prescrições. Em



RECEITUÁRIO CONTROLE ESPECIAL

1ª. Via - Farmácia
2ª. Via - Paciente

PACIENTE:
ENDEREÇO:
PRESCRIÇÃO:

Usoint. —— 3cx
Neuleptil 100 Tomar 1 comp 2x100 dia
Usoint —— 1cx (28)
Seroquel 100 Tomar 1 comp/noite

Jc 03-01-11.

IDENTIFICAÇÃO DO COMPRADOR — IDENTIFICAÇÃO DO FORNECEDOR

Nome:
Ident.: Órgão Emissor:
End.:
Cidade: UF:
Telefone: Assinatura do Farmacêutico

HOSPITAL SANTA CATARINA - RUA AMAZONAS, 301 - Fones: (0XX47) 3322-3575 - 3036-6000
RUA PREFEITO FREDERICO BUSCH JR Nº 255 - SALA 302 - FONE: (0XX47) 3322-6395
BLUMENAU - SANTA CATARINA

Figura 5: Notificação Receita Branca

outras situações, o paciente compra alguns de seus remédios em diferentes farmácias, como o farmacêutico precisa ficar de posse da prescrição, o paciente irá precisar de outra via para os outros medicamentos, a mesma ”gordura”é gerada nesta situação. Esses dois cenários dão margem para venda ou distribuição irregular, aproveitando-se da ”gordura”acumulada, pois para a fiscalização, as baixas nos estoques estão devidamente justificadas.

2.4.3 Remarcação de Consultas para Emissão de Segunda Via

Além da má utilização do sistema de controle, existem outros motivos que podem levar um paciente a precisar de uma segunda via da prescrição. O paciente pode ter perdido a receita, o documento pode ser considerado violado se estiver rasgado em algum lugar, inválido se apresentar rasuras, ou ainda vencido se já tiverem passados os 30 dias a partir de sua emissão(BRASIL, 1998).

A remarcação de consultas apenas para tirar uma segunda via de uma prescrição é uma das maiores deficiência do processo de controle. O paciente perde tempo e dinheiro para se locomover até o hospital e o médico precisa atendê-lo para prescrever novamente a mesma receita.

2.4.4 Tratamentos Contínuos ou de Longo Prazo

No estudo realizado em (MASTROIANNI, 2009), (52,8%) das prescrições que estavam com a data de validade expirada, era por se tratarem de medicamentos de uso crônico, no entanto o seu uso deve ser determinado nas informações referentes ao tempo de tratamento ou vinculado a próxima consulta.

A validade das notificações de receita são de 30 dias(BRASIL, 1998), isto implica à pacientes de tratamentos contínuo ou de longo prazo, são submetidos a precisarem retornar ao médico mensalmente para obtenção de uma nova prescrição em cenário as vezes similar a aquisição da segunda via.

Outra atitude ainda praticada por médicos, é a de prescrever documentos com datas posteriores de emissão. Esta definitivamente não é uma boa prática para o acompanhamento de um tratamento farmacológico.

2.4.5 Adulterabilidade e Legitimidade do Documento

Em(MASTROIANNI, 2009), as ausências de nome do paciente (0,2%), assinatura (0,1%), carimbo do prescritor (15,9%) e data de emissão (12,6%) podem levar a fraudes e falsificação de prescrições ou notificações. Não se trata apenas de uma preocupação por uso incorreto, mas também de uso ilícito e/ou abusivo de medicamentos.

(NOTO, 2002), identificou prescrições de médicos que não estavam na lista do conselho de classe do estado em que exerciam a profissão. Outro problema foram os documentos que tinham a numeração oficial repetida, houve caso do mesmo número de série aparecer nove vezes, o que sugere fraude.

2.4.6 Dispensação Manual

> "O SNGPC faz a captura de dados essenciais referentes à prescrição e à dispensação de medicamentos e de substâncias controladas. No entanto, a necessidade da inclusão do número do lote de cada unidade dispensada no sistema acarreta algumas dificuldades operacionais, podendo gerar algumas falhas, como erros de digitação, por exemplo"(ANVISA, 2012)

é o que explica o gerente substituto responsável pelo monitoramento da qualidade de medicamentos e produtos da ANVISA, Tiago Rauber.

Além de precisar transcrever as informações do LRE para o SNGPC, é obrigação do farmacêutico reter a prescrição por 5 anos, prazo que ele fica sujeito a vistoria da ANVISA.

2.4.7 Custos

(AGUIAR; SILVA; FERREIRA, 2006), descreve que o uso inadequado de medicamentos é um importante problema de saúde pública em todo o mundo, com grandes consequências econômicas. É estimado que a prescrição incorreta pode acarretar gastos de 50 a 70 por cento a mais nos recursos governamentais destinados a medicamentos.

Além dos erros que podem ser ocasionados no preenchimento, a nomenclatura utilizada para os medicamentos também pode trazer prejuízos ao paciente. A política de medicamento(BRASIL, 1998) estabelece à adoção do nome genérico nas prescrições medicamentosas, apesar disto, em (MASTROIANNI, 2009) 43,3% das prescrições não apresentavam o nome da substância

ativa, demonstrando uma falha na divulgação e conscientização na adesão aos padrões estabelecidos e consequentemente um comprometimento no acesso a medicamentos, pois o paciente fica sem a opção da intercambiabilidade de um medicamento mais barato e de mesma segurança, qualidade e eficácia que o medicamento referência de marca.

2.5 POSSÍVEIS MELHORIAS COM A INFORMATIZAÇÃO DO PROCESSO

A criação de mecanismos mais eficazes para o rastreamento de medicamentos é parte integrante do Plano Nacional de Prevenção e Combate à Falsificação de Medicamentos da Anvisa e do Ministério da Saúde(ANVISA, 2012).

A proposta deste trabalho segue na mesma linha, oferecendo uma diversificada gama de aplicações e vantagens ao estado e ao usuário final. Estão elas aqui compreendidas assim:

2.5.1 Sistemas de Prescrição Eletrônica

Os sistemas de prescrição eletrônica são alvo de estudo em todo o mundo. As principais vantagens adquiridas com a implantação desses sistemas são, a legibilidade e a integridade das informações referentes ao tratamento medicamentoso.

Em um hospital de Belo Horizonte, das prescrições escritas (totalmente escritas à mão) constatou-se um risco 6,3 vezes maior de problemas, enquanto que as mistas (composta por prescrição digitada e escrita à mão) apresentaram um risco 3,5 vezes maior de problemas, quando comparadas às digitadas (computadorizadas e impressas).(AGUIAR; SILVA; FERREIRA, 2006)

2.5.2 Automatização do Controle e da Dispensação dos Medicamentos

O controle da emissão da prescrição por meio de um documento de papel deixa de ser suportado pelo estado e passa a ser gerenciando no sistema. A aquisição dos medicamentos junto as farmácias fica automatizado, sendo o dispensário gerenciando automatizadamente.

O cadastramento de produtos no SNGPC não precisaria mais ser feito pelo farmacêutico, pois o gerenciamento do dispensário seria automatizado.

O estado teria um melhor controle para aonde vão os remédios e como

a distribuição se da em território nacional com maior precisão.

2.5.3 Integridade e Autenticidade do Documento

A integridade é uma das principais características do documento eletrônico, uma vez assinado, não é possível validar o documento se ele sofrer alguma tipo de alteração sem um novo processo de assinatura.

O próximo capítulo deste trabalho, apresenta todas as fundamentações envolvendo estes aspectos de segurança da informação.

2.5.4 Acesso à Segunda Via da Prescrição

A remarcação de consultas, apenas para a retirada de uma segunda via, dependendo da especialidade chega a representar quase cinquenta por cento das consultas, diminuir o fluxo de pessoas em hospitais, que não precisariam efetivamente estar ali, é uma decisão estratégica.

2.5.5 Documento Digital

A desmaterialização do documento é um dos avanços conquistados pela tecnologia, alem do espaço economizado, volume de papel, tempo de consulta, levantamento informações, a questão da facilidade do documento a pessoa que usa a prescrição, é fundamental para que isso deixe de ser um problema.

2.5.6 Incorporação de Novas Tecnologias

A centralização das informações dos pacientes gera um registro de todos os remédios que determinado paciente já tivesse retirado na farmácia. Esse histórico tem uma valiosa informação sobre substâncias que possivelmente foram ingeridas pelo paciente.

A incorporação de novas tecnologias como sistemas especialistas de recomendação de medicamentos, precisa de informações sobre o histórico do paciente para poder sugerir um tratamento medicamentoso. Essas informações são importantes para prevenir quantidades errôneas de medicamentos ou interações medicamentosas.

2.5.7 Custos

A partir da resolução que estabelece o prazo mínimo de 20 (vinte) anos, a partir do último registro, para a preservação dos prontuários médicos em suporte de papel Art. 4o – Estabelece o prazo mínimo de 20 (vinte) anos, a partir do último registro, para a preservação dos prontuários médicos em suporte de papel(CFM, 2002b).

O tratamento das informações no meio digital torna o armazenamento das informações muito mais barato além de outros custos gerados por todas as etapas falhas ou ineficientes. Todas estas despesas podem ser reduzidos com a adoção de uma politica de informatização.

2.6 CONSIDERAÇÕES

Considerando que maioria dos erros de medicação ocorre no estágio de prescrição do medicamento, a adoção de sistemas de prescrição eletrônica de medicamentos, com suporte à decisão clínica, pode reduzir significativamente os eventos adversos relacionados aos medicamentos, melhorando a qualidade e a eficiência do tratamento farmacológico, com redução de custos para o sistema de saúde(KAWANO et al., 2006).

Conhecendo as possíveis causas de erros de medicação, poderão ser desenvolvidos sistemas de prescrição mais seguros, que agreguem qualidade ao processo de utilização de medicamentos não apenas nos hospitais, mas também nas drogarias e farmácias, favorecendo a racionalização dos custos do sistema de saúde(FRANKLIN et al., 2007).

A análise de prescrições medicamentosas permite identificar erros e problemas, implantar medidas corretivas e educativas e avaliar o impacto da adoção dessas medidas. As deficiências nas informações nas prescrições são responsáveis por grande parte dos erros de medicação(BENJAMIN, 2003).

Espera-se, assim, que sistemas de detecção de erros evitáveis pelos profissionais de saúde possam melhorar a segurança dos pacientes e reduzir os custos de eventos adversos a medicamentos. Deste modo, o custo-benefício da implantação de tais sistemas tem sido suficiente para gerar uma multiplicidade de iniciativas de desenvolvimento de sistemas informatizados de prescrição de medicamentos(BEMT et al., 2002).

No estudo de (NOTO, 2002), os resultados confirmam a ocorrência de uso irracional e uma série de práticas inadequadas que envolvem a prescrição desses medicamentos no Brasil, indicando a necessidade de uma ampla revisão no atual sistema de controle dessas substâncias no país.

Este capitulo descreveu o que são os medicamentos controlados, por-

que seu controle é necessário, e como ele é feito o no Brasil. Apontou deficiências inerentes ao processo de prescrição manuscrita, erros no controle, e outros problemas decorrentes deste modelo. Por último, foram apresentados dados que incentivam os investimentos em soluções de prontuários eletrônicos.

A partir da contextualização do cenário nacional, é definida a proposta deste trabalho que é: tornar digital todo o processo de controle de medicamentos, fornecer as informações ao SNGPC, e se enquadrar ao modelo de rastreamento estabelecido pelo SNCM.

A informatização pode melhorar o processo e trazer beneficícios a todas as partes envolvidas, governo população e gestão de saúde. Todavia, um aspecto muito importante precisa ser bem definido, a segurança da informação. Neste contexto, as técnicas de criptografia representam um importante papel, pois é o correto uso destas que garantirá um sistema confiável.

3 FUNDAMENTOS DA ASSINATURA DIGITAL

3.1 CRITPOGRAFIA

Segundo (SCHNEIER, 1996), criptografia resolve problemas que envolvem sigilo, autenticação, integridade, e pessoas desonestas.

O intuito é ter a uma maneira de armazenar e transmitir dados de modo que somente aqueles a quem os dados são destinados possam ler e processar. É considerada a ciência da proteção da informação através da codificação da mensagem para um formato ilegível. A criptografia é um meio efetivo de proteger informação sensível tanto como é armazenada em mídias ou é transmitida através de redes de comunicação não seguras(HARRIS, 2010).

Os primeiros métodos de criptografia datam de mais de 4000 anos atrás e eram mais considerados um formato de arte ou uma linguagem de comunicação. Posteriormente a criptografia foi remodelada e foi adaptada como uma nova ferramenta para ser usada em guerra, comércio, governo, e em outros lugares aonde segredos precisam ser guardados.

Com o nascimento da Internet, criptografia ganhou uma novo enfoque como ferramenta vital nas transações de todos os dias. Ao longo da história, a criptografia foi sendo usada e desenvolvida por indivíduos e gorvenos para proteger sua comunicação. Como resultado, algorítmos de criptografia e os dispositivos que utilizam dos mesmos, tem aumentado em complexidade, novos métodos e algorítmos tem sido continuamente introduzidos, e a criptografia se tornou parte integrante do mundo da computação.(HARRIS, 2010)

A criptografia computacional é capaz de fornecer sistemas de informação com as seguintes características:

- Confidencialidade: Torna a informação ilegível exceto para as partes autorizadas;
- Integridade: O dado não foi alterado de forma não autorizada desde que foi criado, transmitido ou armazenado;
- Autenticação: Verifica a identidade do usuário do sistema, ou o sistema que criou a informação;
- Autorização: Perante comprovação da identidade, é fornecido uma chave ou senha que da acesso a algum recurso ao indivíduo.
- Não-Repúdio: Garante que o emitinte não possa negar que emitiu a mensagen.(HARRIS, 2010)

Para duas partes serem capazes de se comunicar de utilizando criptografia, elas precisam estar usando o mesmo algorítmo e, muitas vezes, a mesma chave. Em algumas tecnologias de criptografia, o remetente e o destinatário usam a mesma chave, e em outras, eles precisam usar chaves diferentes, mas relacionadas entre si(HARRIS, 2010).

Existem dois tipos de algoritmos de criptografia são ou algoritmos simétricos, que utilizam chaves simétricas (também chamadas de chaves secretas), ou algorítmos assimétricos, que utilizam chaves assimétricas (também chamadas de chaves públicas de privadas).

3.1.1 Criptografia Simétrica

Algorítmos Simétricos, as vezes chamados de algorítmos convêncionais, são algorítmos aonde a chave usada para cifrar pode ser calculada a partir da chave de decifragem e vice-versa. Na maior partes dos algorítmos simétricos, a chave de cigrafem e a chave de decifragem são as mesmas. Esse tipo de algorítmo também é chamado de chave secreta, chave única, ou uma chave. A segurança do algorítmo fica na chave; divulgar a chave, significa que qualquer um pode cifrar e decifrar mensagens. Enquanto a comunicação precisar permanecer secreta, a chave precisa permanecer secreta.(SCHNEIER, 1996)

Cifragem simétrica transforma um texto simples em texto cifrado utilizando a chave secreta e o algorítmo de cifragem. Utilizando a mesma chave e o algorítmo de decifragem, o texto simples é recuperado a partir do texto cifrado(STALLINGS, 2010). A figura 6 é um exemplo desse processo.

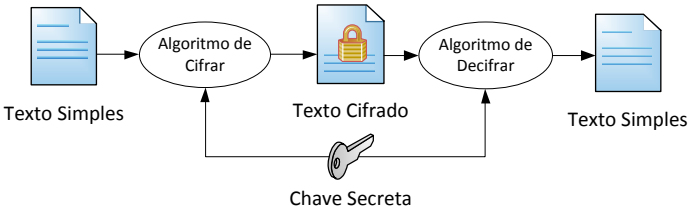


Figura 6: Exemplo do uso da chave simétrica

Podemos citar como exemplos: o DES e o AES como algoritmos bem populares.

Apesar do grande uso e da importância da criptografia simétrica junto com a evolução dos povos, esta técnica de criptografica não consegue suportar a demanda de sistemas computacionais complexos. Três aspectos importantes

que precisam ser resolvidos de outra maneira são:

- Serviços de segurança: Criptografia simétrica prove confidencialidade apenas, autenticação e não-repúdio não podem ser garantidos.
- Escalabilidade: Como o número de pessoas que precisam se comunicar cresce, o número de chaves simétricas nescessárias também, isso significa que mais chaves precisam ser gerenciads.
- Distribuição Segura da Chave: A chave simétrica deve ser entregue as partes através de um canal seguro.(HARRIS, 2010)

Criptografia simétrica era o único tipo de criptografia em uso antes do desenvolvimento da criptografia por chaves públicas na década de 1970. Mesmo com as novas técnologias, ela continua sendo de longe o mais usado dos dois tipos de criptografia graças ao seu alto desempenho(STALLINGS, 2010). É sobre uma nova técnica desenvolvida na década de 70 conhecida como criptografia assimétrica, ou criptografia de chave pública que tratamos na próxima seção.

3.1.2 Criptografia Assimétrica

O desenvolvimento da criptografia de chave pública é a maior e talvez a única verdadeira revolução em toda a história da criptografia.(STALLINGS, 2010)

O primeiro modelo apresentado utilizando o modelo assimétrico foi publicado em 1976 e ficou conhecido por acordo de chaves de Diffie-Hellman em homenagem a seus autores. A força deste algoritmo era baseado na dificuldade de calcular logaritmos discretos. Mais tarde Hellman sugeriu que o nome fosse aumentado para Diffie-Hellman-Merkle em reconhecimento a Ralph Merkle pela sua igual contribuição no desenvolvimento da criptografia de chave pública(HELLMAN, 2002).

Em sistemas de criptografia assimétrica, a cifragem e a decifragem são feitas com chaves diferentes. Uma é a chave pública e a outra é a chave privada. A chave pública como o próprio nome já diz, é de conhecimento público, e é usada para cifrar. A outra chave, a privada, é usada para decifrar e só é conhecida pelo possuidor. O compartilhamento da chave pública não compromete a chave privada. Uma chave não pode ser calculada a partir outra(pelo menos em qualquer período de tempo razoável).

Esta característica permite que qualquer entidade possa enviar uma mensagem cifrada para outro entidade, e só o destinatário terá acesso ao conteudo protegido. É possivel se comunicar com outros indivíduos de maneira

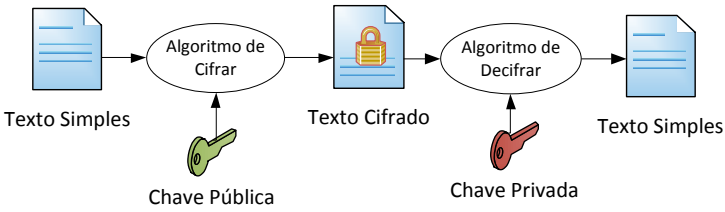


Figura 7: Exemplo do uso da chave assimétrica

cifrada e autenticada sem nunca tê-los conhecido. Cada parte cifra as mensagens que deseja enviar para a outra com a chave pública do destinatário, e o receptor das mensagens decifra com sua chave privada(HELLMAN, 1976). A figura 7 é um exemplo deste processo.

O desempenho da criptografia assimpetrica não é dos melhores, estima-se que ela seja 1000 vezes mais lenta que a simétrica. Além disso, como a chave pública é de conhecimento de todos, isso torna inseguro seu uso para troca de mensagens. A idéia é que ela seja utilizada para combinar uma chave de sessão entre as partes, e a partir dai a cifragem dos dados da comunicação acontece pela técnica simétrica.(SCHNEIER, 1996)

O modelo proposto por (HELLMAN, 1976) é entendido até hoje como uma revolução dentro do mundo da criptografia. A estratégia de usar duas chaves na troca de mensagens foi inspiradora para muitos pesquisadores. A proposta com logaritmos era boa e é utilizada até hoje, mas ainda existiam lacunas a serem preenchidas. Segundo o algoritmo, para toda a comunicação entre duas partes, se fazia nescessário estabelecer um novo par de chaves. O problema é que não há garantia quanto a identidade da outra parte, uma vez que pode haver um intermediário entre as partes.

O algoritmo proposto em por (RIVEST; SHAMIR; ADLEMAN, 1978),entre todos os algorítmos de chave assimétrica, é o mais popular. Leva o nome de RSA em homenagem a seus inventores, Ron Rivest, Adi Shamir e Leonard Adleman. O RSA é um padrão mundial e pode ser usado para assinaturas digitais, troca de chaves e criptografia. Foi desenvolvido em 1978 no MIT, ao contrário da abordargem do Diffie-Hellman, o par de chaves é gerado apenas uma vez. A segurança deste algoritmo vem da dificuldade de fatorar números primos grandes.(RIVEST; SHAMIR; ADLEMAN, 1978)

Este algoritmo se tornou popular pela vantagem de se trabalhar computacionalmente a geração de dois números primos grandes e multiplicar um com o outro.

A criptografia de chave pública nos permite trocar mensagens, gantindo nossa identidade e a de quem estamos nos comunicando. O comércio eletrônico é realizado em cima dessa confiança de identidade.

Agora que entendemos como nos autenticar perante outras partes, é preciso entender como podemos obter integridade de documentos e mensagens. Este é o assunto da próxima seção.

3.1.3 Função de Resumo Criptográfico

Funções de resumo são funções matemáticas não inversíveis. Portanto, uma vez calculado o valor desta função, não é possível obter novamente sua entrada original a partir do valor do resumo.

São peças importantes na construção de muitos protocolos e fundamentais na criptografia moderna(SCHNEIER, 1996). A aplicação destas funções está diretamente relacionada às propriedades de integridade e autênticidade da criptografia.

Estas funções de resumo mapeiam uma mensagem de tamanho variável em um valor de tamanho fixo que representa seu resumo(STALLINGS, 2010). Podemos citar como exemplos o: Secure Hash Algorithm (SHA) e o Message Diggest 5 (MD5) como funções de resumo bem populares.

O valor da função de resumo é como a impressão digital de um arquivo. A idéia é ter uma identificação única.

Como exemplo de aplicações práticas destas funções de resumo temos a verificação de integridade de arquivos. Uma vez que se tenha acesso ao algoritmo usado e o valor do resumo do arquivo original, se a cadeia de bytes do arquivo que for usada para calcular o novo resumo não for a mesma, o valor resumo irá divergir indicando que o arquivo ou pode estar corrompido ou foi alterado.

3.1.4 Assinatura Digital

Segundo (HELLMAN, 1976), em qualquer lugar que usamos assinaturas, precisamos transmitir e armazenar os documentos. Se quisermos substituir os documentos de papel para o meio digital precisamos de uma assinatura digital. Cada usuário precisa ser capaz de criar uma mensagem e que a autenticidade desta possa ser verificada por qualquer outra entidade. Outro ponto crucial é que esta mensagem não pode ser criada por mais ninguém no ambiente.

Segundo (STALLINGS, 2010) a assinatura digital é uma aplicação

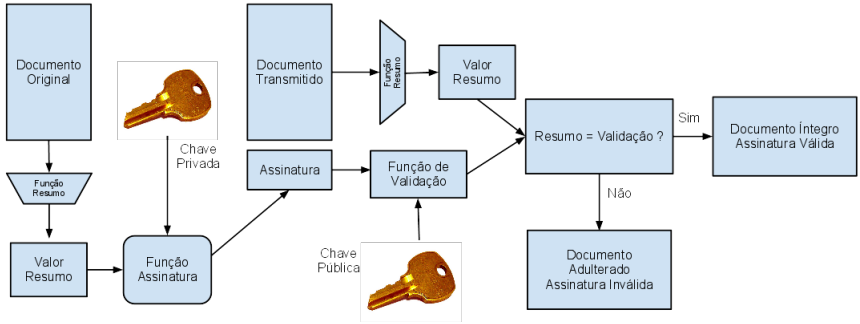


Figura 8: Exemplo do processo de assinatura e validação

importante muito parecida com a autenticação de mensagem. Esse serviço é suportado através a criptografia por chaves públicas. A chave privada é usada para gerar assinaturas, e a chave pública é usada para validá-las.

Nas aplicações do mundo real, as assinaturas não são geradas diretamente a partir do documento original, ao invés disso, é primeiro calculado o resumo através das funções de resumo, e em cima do valor do resumo é gerada a assinatura do documento utilizando a chave privada(HOUSLEY; POLK, 2001).

A função de resumo garante a integridade do texto, e a assinatura desse resumo garante autênticidade e não-repúdio. O ato de assinar, é um processo criptográfico utilizando o valor do resumo e a chave privada(HARRIS, 2010).

Uma vez que o documento tenha sido assinado, para este poder ser alterado e a sua assinatura se manter integra, é nescessario gerar uma nova assinatura. E para isso ser possível, só estando de posse da chave privada(STALLINGS, 2010).

Uma vez que todos conhecem a chave pública, é possível validar se o detentor da chave privada foi quem gerou a assinatura.

A Figura 8 é um exemplo do processo de assinatura e validação. Se ao final do envio de um documento o valor da assinatura puder ser comparado ao valor do resumo, a integridade e a autenticidade estão garantidos, caso contrário a assinatura não é daquele documento ou não é daquela chave privada correspondente.

No Brasil, as aplicações que trabalham com assinaturas digitais são cada vez mais presentes. Exemplos dessas aplicações encontram-se no Judiciário e no Colégio Notarial. Juízes assinam sentenças, advogados gerenciam seus processos, cartórios emitem declarações, contratos são assinados, etc, e tudo isso no meio digital. Não há a nescessidade de papel impresso nem

de longos trâmites de documentos. Estas e outras facilidades que são trazidas pela criptografia, só podem ser entendidas como confiáveis, uma vez que se tenha um padrão que nos diga como podemos confiar nas chaves públicas espalhadas pelo mundo. É pensando nessa nescessidade que foi criado o conceito da certificação digital utilizado a infraestrutura de chaves públicas, tema da proxima seção.

Como neste trabalho estamos propondo um modelo de assinatura de documentos digital. É importante termos conhecimentos dos modelos de assinatura e as informações que elas contemplam. As estruturas exploradas são o CAdES e o XAdES. Vale lembrar que estes padrões são idenpentes de certificados, trabalham diretamente com a assinatura e seus campos.

3.1.5 Protocolos Criptográficos

Protocolo nada mais é que uma sequencia de passos, executada por duas ou mais entidades, que tem como intuito a execução de uma tarefa. Computadores não são flexíveis, logo, precisam de regras para poder executar algum tipo de comportamento. Protocolos são as descrições de todas as possibilidades e ações que evolvem a execução da tarefa(SCHNEIER, 1996).

Protocolos de segurança são pontos críticos na infraestrutura que suporta a comunicação e o processamento de informações de maneira segura. A segurança das aplicações se dá através de um conjunto de elementos criptográficos, que trabalhando de maneira interligada, permitem entidades autênticarem umas as outras, estabelecer novas chaves de sessão para se comunicar confidencialmente e garantir a autênticidade de informações, serviços e assim por diante(RYAN; SCHNEIDER, 2001).

3.1.6 Autenticação

Pode-se ser utilizado um sistema de autenticação multifator para o aumento da segurança na utilização do sistema porém, em particular, o uso de dispositivos biométricos deve proporcionar subsídios ao reconhecimento do indivíduo e não serem unicamente responsáveis pela tomada de decisão Sendo que os fatores existentes podem ser entendidos em frases como: aquilo que eu sei, algo que possuo e o que sou. Conhecimento, material, característica física(ANDERSON, 2008).

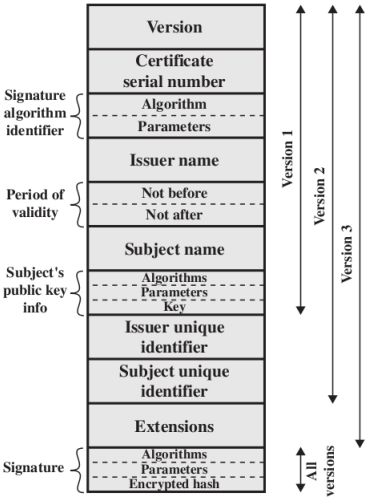


Figura 9: Certificado X.509(STALLINGS, 2010)

3.2 CERTIFICAÇÃO DIGITAL

3.2.1 Certificado Digital

O certificado é a identidade digital de um indivíduo. Esta identidade tem informações como chave pública, AC que a emitiu, datas de emissão e expiração e os algoritmos usados para gerar e assinar o certificado.

Como os algoritmos que foram utilizados na sua emissão são declarados na sua estrutra, qualquer entidade que deseje verificar a validade da assinatura, pode faze-lo de maneira independente.

O X.509 é um padrão que estabelece formato para certificados para Infraestrutura de Chaves Públicas (ICP). Estabelece o formato mas não dita os algoritmos que precisam ser utilizados. Cada certificado possui uma chave pública e é assinado com a chave privada de uma Autoridade Certificadora (AC)(STALLINGS, 2010). A figura 9 nos trás o certificado X.509 detalhado.

Esse tipo de certificado é utilizado em muitos tipos de protocolos criptográficos. O SSL é um exemplo de uso(HARRIS, 2010).

É importante entender que um certificado no formato X.509 não é nescessariamente confiável. A sua principal característica é precisar ser gerado e assinado por uma AC. Sendo este o assunto da nossa próxima seção.

3.2.2 Autoridade Certificadora

A Autoridade Certificado (AC) é a entidade que emite, assina e gerência o ciclo de vida de um certificado digital. Existem duas características que identificam um AC, seu nome e sua chave privada.(HOUSLEY; POLK, 2001)

É importante entender que o certificado de uma AC pode ser auto-assinado. Isso é a mesma coisa que dizer que um certificado de um usuário final pode ser gerado pelo mesmo, a partir de uma AC própria.

Quando uma AC assina um certificado, ela na verdade, está ligando sua chave pública a assinatura do certificado do usuário final. Além de gerar novos certificados, quando é dito que uma AC também é responsável por gerenciar o ciclo de vida dos certificados, estamos querendo saber se podemos confiar em um determinado certificado. A AC precisa manter e publicar certificados que precisaram ser revogados, e suas as datas de revogação. Mas isto é assunto da nossa próxima seção. Por hora basta entender que é a partir da AC que vamos confiar ou não em um certificado.

A autênticidade do certificado pode ser comprovada, mas é preciso poder confiar na AC.

Com o intuito de estabelecer uma rede de ACs confiávies, foi concebido o modelo de Infraestrutura de Chaves Públicas. Este é o assunto que será tratado após a seção de Revogação de Certificados

3.2.3 Revogação de Certificados

A revogação de certificados é uma medida a ser tomada quando alguém perde a posse confidencial da sua chave secreta ou quando há alterações dos dados associados aquele certificado. Cabe a AC que emitiu o certificado revogá-lo também. Para saber se um certificado está válido ou revogado, é nescessario consultar a AC emissora.

Existem algumas maneiras de se verificar se o certificado foi revogado junto a AC que o emitiu. A mais comum de todas é através da Lista de Certificados Revogados (LCR). A LCR é uma lista com os números dos certificados emitidos por aquela AC, que ainda não estão expirados, mas, que não podem mais ser considerados como confiávies(HOUSLEY; POLK, 2001).

A figura 10 é a lista de certificados revogados no padrão X.509.

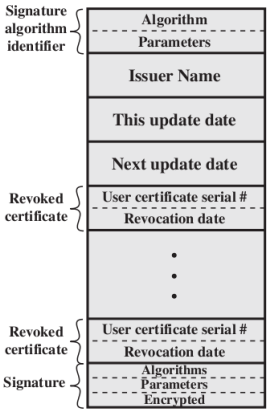


Figura 10: Lista de Certificados Revogados(STALLINGS, 2010)

3.2.4 Infraestrutura de Chaves Públicas

Segundo (HARRIS, 2010) uma Infraestrutura de Chaves Públicas (ICP) é um conglomerado de programas, padronizações, procedimentos, protocolos de comunicação, políticas de segurança e mecanismos de criptografia de chave pública trabalhando concomitantemente para disponibilizar comunicação segura e autenticada entre uma gama dispersa de pessoas. A proposta de uma ICP é a de estabelecer um nível de confiança dentro de um ambiente. A ICP é um framework ISO que usa de criptografia de chave pública e o padrao adotado é o X.509.

Este é um sistema híbrido de métodos e algoritmos simétricos e assimétricos que pode fornecer autenticação, confidecialidade, não-repúdio e integridade nas mensagens trocadas(HARRIS, 2010).

A Autoridade Certificado (AC) é a entidade que sustenta a confiança no esaquema da ICP.(HOUSLEY; POLK, 2001)

Existem diversos modelos de ICP, mas o maios comum e a estrutura hieraquica. Estaestrutura é similar a uma estrutura de dados do tipo árvore, sendo o nó mais ao topo da cadeia conhecido como AC Raiz. As ACs que estaçao abaixo da AC Raiz podem ser ACs Intermediárias ou Finais. As Intermediárias emitem certifivados para outras ACs. As Finais emitem certificados para entidades, pessoas e empresas afim de participar da rede de confiança.

Este ambiente tem como objetivo possibilitar a autenticação através de diferentes redes e da Internet. Protocolos e algoritmos não são especificados, e é por isso que a ICP é um padrão e não uma tecnologia específica.(HARRIS,

2010)

O principal objetivo deste sistema é permitir a aquisição do par de chaves de maneira segura, conveniente e eficiente(STALLINGS, 2010).

Para um indivíduo, poder fazer parte do sistema, ele precisa de um certificado. Este certificado contém uma chave pública e varias outras informações. O propósito é que as informações tornem única a identificação dentro do sistema.(HOUSLEY; POLK, 2001)

Segundo (HARRIS, 2010) o certificado é uma das peças mais importantes da ICP. É através dele que vamos identificar e autenticar as partes com quem desejamos nos comunicar. É a confiança em cima da AC que traz a credibilidade e a segurança ao sistema.

Dentro deste ambiente, podemos identificar o detentor da chave privada de duas maneiras, o certificado que contém a chave pública, e a Lista de Certificados Revogados (LCR). O certificado associa a chave pública a privada, e a LCR nos diz se o possuidor do certificado precisou revogálo ou se a autoridade não certifica mais aquele indivíduo.(HOUSLEY; POLK, 2001)

A identidade das partes é garantida através dos certificados e que o algoritmo assimétrico toma conta de todo o resto do processo efetuando a troca de chaves. Por sua vez, a infraestrutura se faz de ferramentas que irão identificar os usuários, criar e distribuir os certificados, revogar e manter os certificados, distribuir e manter as chaves criptográficas. Todo este artefato de entidades trabalhando concomitantemente possibilita fornecer uma comunicação criptografada e autênticada(HARRIS, 2010).

No Brasil, por intermédio da medida provisória 20022, foi instucionalizada a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). A partir desta, todos os documentos assinados por indivíduos que fazem parte da cadeia, tem validade legal e jurídica no território nacional.(BRASIL, 2001)

3.2.5 Política de Assinatura

Uma politica de assinatura é um conjunto de normas estabelecidas por uma entidade a fim de determinar quando uma assinatura pode ser considerada válida ou não. Existem parametros e condições que precisam ser especificados para que a assinatura possa ser aceita. São estes que caracterizam uma política de assinatura.(HOUSLEY; POLK, 2001)

3.2.6 ICP - Brasil

No dia 24 de agosto de 2001, foi institítuida a Infra-Estrutura de Chaves Públicas Brasileira (ICP-BRASIL). A medida provisória tem como intuito garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras(BRASIL, 2001)

A ICP-Brasil é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação do cidadão quando transacionando no meio virtual, como a Internet. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raíz única, sendo que o ITI além desempenhar o papel de Autoridade Certificadora Raiz - AC Raiz, também, tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos(INSTITUTO. . . , 2012).

4 PROPOSTA DE PROTOCOLO

Neste capítulo, será proposto um protocolo para prescrições eletrônicas de medicamentos. Da emissão pelo médico, a obtenção do medicamento com um farmacêutico e dispensação do mesmo perante as autoridades competentes. Aqui estão descritas as etapas do processo, bem como as partes devem interagir para atingir a execução da tarefa.

Em virtude dos problemas apontados em 2.4, é proposto um novo modelo informatizado, no intuito de corrigir deficiências inerentes ao processo de controle manual. Os conceitos apresentados no capítulo 3, fornecem meios técnologicos suficientes, para automatizar esse processo. A utilização das identidades digitais agrega recursos muito interessantes para o gerencimento deste tipo de informação. como por exemplo:

- Não Repúdio - O Médico não poderia refutar que assinou uma prescrição, assim como o farmacêtico não poderia negar que deu baixa na compra de um medicamento.

- Autênticidade - A assinatura digital garante que aquela assinatura só pode ter sido gerada por aquele par de chaves.

- Integridade - A integridade documento seria garantida atraves do processo de validaçao da assinatura, garantindo que a prescrição não possa ser adulterada nem violada.

As identidades digitais, permitem a identificação e reconhecimento de um indivíduo dentro de uma estrura. O controle de medicamentos demanda a autenticação das várias partes envolvidas. São apresentados protocolos que objetivam proteger as informações e rastrear o controle de medicamentos, utilizando soluções de abrangência nacional.

4.1 ANALISE DO CONTROLE DE MEDICAMENTOS

Analisando o processo de controle de medicamentos, fica claro que existem pelo menos três papéis distintos, médico, farmacêutico e paciente. A identificação destas partes serão discorricas na próxima seção, neste momento, para fins de modelagem, será utilizada esta abstração.

Na primeira etapa, o médico prescreve o medicamento ao paciente, neste momento, o paciente apenas interage como transportador da mensagem. A prescrição emitida pelo médico tem como objetivo autorizar o farmacêutico

a venda de medicamentos controlados. Para informatizar este passo, o médico precisa ser capaz de assinar uma prescrição digital e torná-la disponível para o farmacêutico.

No segundo estado, o paciente e farmacêutico interagem diretamente. O paciente recebe uma via da prescrição, pois ali constam as informações do tratamento medicamentoso. O farmacêutico, por sua vez, é responsável pela averiguação da identidade do paciente e da retenção de uma das vias da receita. O sistema proposto precisa permitir ao farmacêutico acessar a prescrição que havia sido disponibilizada pelo médico, estabelecer as identidades do paciente e do farmacêutico para satisfazer as nescessidades do mundo real.

O último passo, é de responsabilidade do farmacêutico que precisa transcrever as informações das prescrições para o SNGPC. A informatização do processo, elimina a nescessidade desta etapa, pois as informações são capturadas durante as outras etapas do processo.

Para atender a essa demanda, existe a nescessidade da construção de um sistema que

- Emita prescrições eletrônicas assinadas digitalmente por médicos autorizados.
- Emita baixas de medicamentos assinadas digitalmente por farmacêuticos autorizados, referentes a prescrições válidas.
- Centralize o recebimento e genrenciamento de prescrições e dispensações, e em cima deste histórico, gere relatórios, para alimentar o SNGPC.

4.2 ATORES DO SISTEMA

Os papéis estabelecidos para o controle de medimantos são: Médico, Farmacêutico e Paciente. A prototipação do protocolo, independe da técnologia utilzada para sua implementação sempre que este método forneça os mecanismos de autenticação e assinatura.

Este protocolo contempla a identificação das partes através de diferentes mecanismos estabelecidos pelo estado brasileiro.

4.2.1 CRM-Digital

(CFM, 2012) estabele o e-CRM, esta nova identificação do médico, agora provê meios para autenticação em sistemas digitais, permitindo também a assinatura de documentos eletrônicos com validade legal.

Figura 11: CRM-Digital

Figura 12: Certificado digital emitido pela Receita Federal

O e-CFM é um certificado digital, portanto atende as demandas de identifição para o Médico. A figura 11 é um exemplo desta identidade.

4.2.2 e-CPF

O e-CPF, é um certificado digital que é emitido pela Receita Federal. Contém informações que são relevantes ao ministério da fazenda. Este certificado tem validade de autenticação em todo o território brasileiro. Todos os três atores do sistema, poderiam utilizar de e-CPFs pois ele não restringe uma categoria profissional, ao contrário do e-CFM.A figura 12 é um exemplo desta identidade.

Figura 13: Registro de Identidade Civíl

A decisão do médico pelo e-cpf ou e-cfm, é apenas de caráter político, afinal, ambos provêm os meios nescessários para execução das tarefas.

4.2.3 CRF-Digital

Não existe hoje, no Brasil, um certificado somente para farmacêuticos. Uma nova Autoridade Certificadora, nos mesmos moldes da e-OAB e e-CFM, dentro da hierárquia da ICP-Brasil, seria uma solução elegante em um cenário no qual os médicos e pacientes utilizam e-CFM e e-CPF respectivamente.

4.2.4 Registro de Identidade Civíl (RIC)

De modo análogo ao e-CPF, o RIC não é restrito a nenhuma categoria de profissional. Adicionalemte ele apresenta uma vantagem para os fins deste protocolo, a autenticação dos atores do sistema é suportada em nível multi-fator (BRASIL, 2010b). Isto caracteriza este dispositivio dentre todos os outros que foram apresentados, como aquele que fornece o maior nível de segurança. A figura 13 é um exemplo desta identidade.

4.3 REQUISITOS DO PROJETO

Existe a nescessidade de um sistema que:

1. Emita prescrições eletrônicas assinadas digitalmente por médicos au-

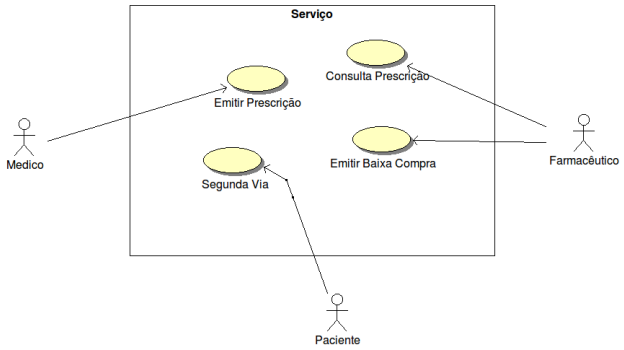


Figura 14: Casos de uso do sistema.

torizados.

2. Emita dispensações de medicamentos eletrônicas assinadas digitalmente por farmacêuticos autorizados, referentes a prescrições válidas.
3. Possibilite ao paciente consultar as informações referentes ao seu tratamento medicamentoso, a partir de casa, sem a necessidade de voltar ao hospital.
4. Centralize o recebimento e gerenciamento de prescrições e dispensações
5. Com base nos históricos, gere relatórios, para alimentar o SNGPC.
6. Evite erros no preenchimento.
7. Suporte a baixa parcial da receita.

Todas as questões abordadas são técnicas, e focam na solução técnologica do problema.

A figura 14 é a representação das interações com o servidor remoto.

4.4 DOCUMENTO ELETRÔNICO

4.4.1 Prescrição

Como em(DUTCH, 2011), as informações listadas a seguir, são essências para um sistema de prescrições eletrônicas.

- Médico
- Paciente
- Medicamento
- Posologia
- Quantidade
- Dosagem
- Data
- Codigo

4.4.2 Dispensação

- Médico
- Farmacêutico
- Paciente
- Medicamento
- Posologia
- Quantidade
- Dosagem
- Data
- Codigo

Em adicção a estas, informações, o protocolo proposto ainda contempla o DataMatrix contido no medicamento.

4.5 CENTRAL DE PRESCRIÇÕES

As prescrições seriam submetidas a um sistema central administrado pela ANVISA. A submissão das prescrições poderia ser feita através de uma interface grafica no portal da web ou então através de um webservice assim se tornando aberto a interação com sistemas de terceiros. A Central de

Prescrições seriam responsável por armazernar a prescrição enquanto nescessária ao uso e após o seu efetivo consumo, o sistema ainda seria responsável pelo controle de baixas e pela alimentação das informações ao SNGPC.

4.6 PROJETO PROCESSO ELETRÔNICO

Nesta seção serão apresentadas os protocolos que foram produzidos com este trabalho. A notação formal destes é o artefato mais importante que é concebido. Através desta, é possível verificar formalmente a funcionabilidade dos protocolos.

O primeiro passo para a verificação de protocolos é sua conversão para um formato mais estrito e formal. Desse modo, diminui-se a ocorrência de processos paralelos e evita-se ambigui- dades na descrição(RYAN; SCHNEIDER, 2001)

4.6.1 Notação Formal

A figura 15 é um exemplo de como será feita a notação dos protocolos que serão especificados posteriormente. O número 1 indica a etapa do protocolo, no caso, representa a primeira mensagem. A primeira letra maiúscula representa a entidade que envia as mensagens, esta entidade é a representação de um médico, farmacêutico, paciente, ou ainda o servidor da Central de Prescrições. A seta direcionada indica o sentido em que a mensagem está sendo enviada, e a letra maiúscula seguinte por fim representa a entidade destinatária da mensagem correspondente. As informações contidas na troca das mensagens é representada dentro do conjunto representado pelas chave, no caso $\{texto\}_{eKu_S}$ siginifica um texto que é cifrado pela chave pública de S e $\{mensagem\}_{sKr_M}$e uma mensagem assinada pela chave privada de M.

$$1. \quad M \quad \rightarrow \quad S \quad : \qquad \{\{Med, Q, Pos, Dos, T, D, M, P\}_{sKr_M}\}_{eKu_S}$$

Figura 15: Exemplo da notação utilizada.

Para poder representas estes modelos formalmente, as informações contidas dentros das mensagens precisam ser especificadas, são elas:

- P - Paciente

- M - Médico
- F - Farmacêutico
- S - Servidor
- Q - Quantidade.
- Med - Medicamento - Inclui dosagem e forma farmacêutica
- Tinfo - Informações do tratamento medicamentoso(posologia, duração)
- D - Data
- R - Requisição de prescrição
- Dmatrix - Identificador único do medicamento - $\{$Dmatrix$\}$ representa um conjunto para dispensação com quantidade maior que 1
- Nonce - Número aleatório usado para identificar a sessão.

4.6.2 Protocolo Médico-Farmacêutico

Das três propostas de protocolo apresentadas neste trabalho, este pode ser encarado como o mais simples. O processo envole a atuação de apenas duas partes e tem um número menor de passos.

As etapas nescessárias para a execução deste protocolo são:

- 1. O médico prescreve um medicamento, assina e submete a nova entrada para a central.
- 2. O farmacêutico envia uma solicitação das prescrições pendentes do paciente, ele assina esta requisição para garantir sua identidade.
- 3. A central envia as precrições do paciente solicitadas, cifrando os dados com a chave pública do farmacêutico.
- 4. O farmacêutico, junto com o paciente presente no mesmo recinto, escolhem a prescrição desejada. O medicamento é fornecido ao paciente, e o farmacêutico envia uma dispensa desta medicação assinada por ele e envia a central.

A figura 16 é uma representação dos passos do processo.

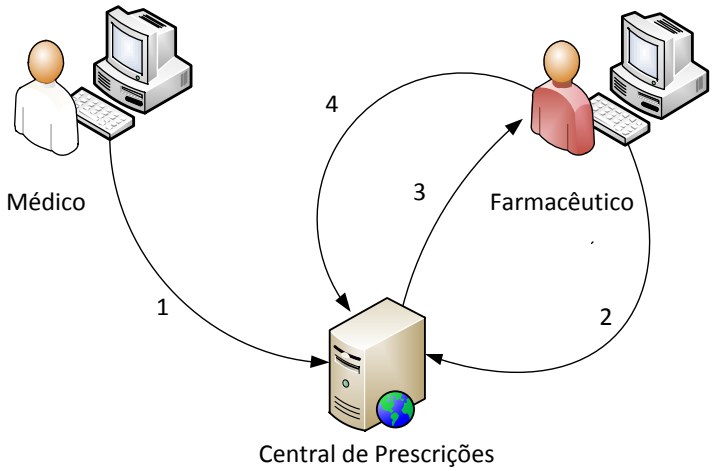


Figura 16: Versão simplificada do protocolo.

1.	M	$\rightarrow$	S	:	$\{\{P,Med,Q,V,M,D,Tinfo\}_{sKr_M}\}_{eKu_S}$
2.	F	$\rightarrow$	S	:	$\{Request(P,Nonce)_{sKr_F}\}_{eKu_S}$
3.	S	$\rightarrow$	F	:	$\{\{P,Med,Q,V,D,M,Tinfo\}_{sKr_M},Nonce\}_{eKu_F}$
4.	F	$\rightarrow$	S	:	$\{\{P,Med,Q,D,M,\{Dmatrix\}\}_{sKr_F}\}_{eKu_S}$

Figura 17: Notação formal da proposta simpleficada do protocolo.

A figura 17 é a notação formal do protocolo.

A ausência do paciente caracteriza este como um protocolo de transição. A verificação da idêntidade do paciente é responsabilidade do farmacêutico na hora em que a compra estiver acontecendo. Este procedimento é análogo ao processo atual, a diferenca entre os dois, é que não seria armazenada a assinatura do paciente.

Soluções como o e-CPF e o RIC ainda tem um longo caminho até serem largamente utilizados pela população em geral, aumentando a importância de uma versão simplificado. A utilização das identidades digitais por médicos e farmacêuticos, é a primeira etapa para a informatização total do controle de medicamentos.

O estabelecimento dessas novas tencnologias de identidade, permite a incorporação do paciente ao processo, aumentando a seguranca do controle. Sob esta perperctiva, outro protocolo, um mais completo é proposto.

4.6.3 Protocolo Médico-Farmacêutico-Paciente

A participação do paciente no processo completa a cadeia de fabricação, comercialização e dispensação de medicamentos. Das três etapas de implantação do SNCM (BRASIL, 2009), este protocolo não contempla apenas a primeira, fabricante e fornecedor. Todas as outras informações que são descritas nas duas ultimas etapas estão contempladas nesta versão completa.

As etapas nescessárias para a execução desta versão do protocolo são:

- 1. O médico prescreve um medicamento, assina e submete a entrada para a central.

- 2. O farmacêutico envia uma solicitação das prescrições pendentes do paciente, ele assina esta requisição para garantir sua identidade.

- 3. A central envia as precrições do paciente solicitadas, cifrando os dados com a chave pública do paciente.

- 4. O farmacêutico, encaminha as precrições para o paciente escolher qual delas é a desejada.

- 5. O paciente, no intuito de adquirir o medicamento, assina a baixa do mesmo, referindo a quantidade desejada, e envia ao farmacêutico.

- 6. O farmacêutico, também assina a baixa que acabou de ser gerada pelo paciente, e submete esta com as 2 assinaturas a central.

A figura 18 é uma representação dos passos do processo.

A figura 19 é a notação formal do protocolo.

A configuração de médicos,farmacêuticos e pacientes utilizarem todos e-CPFs ou e-CFM, e-CPF e e-CFF respectivamente, atende as nescessidades de segurança para execução desta tarefa.

No intuito de tornar o sistema ainda mais seguro, pode ser exigidos mais do que um fator de autenticação. A seguir é proposta o mesmo protocolo, mas utilizando o suporte fornecido pelo RIC para verificar as impressões digitais.

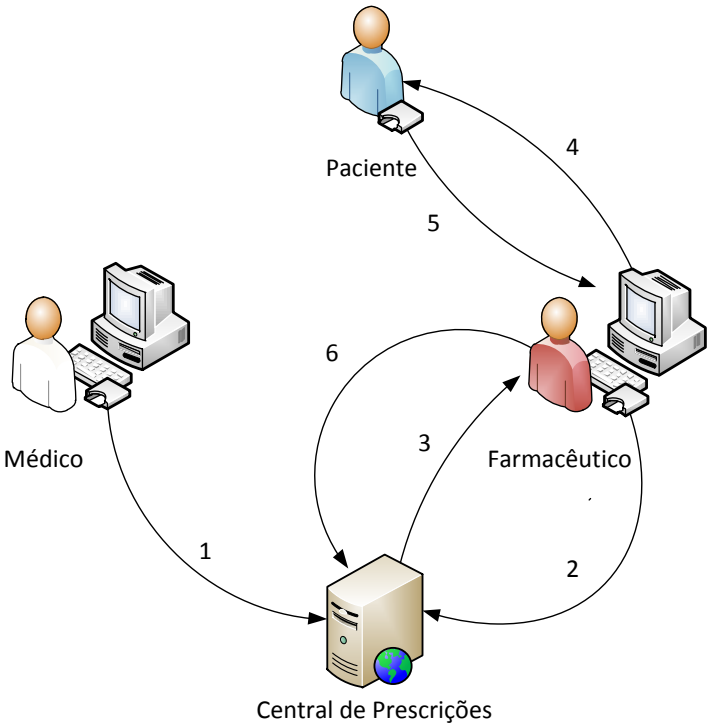


Figura 18: Versão completa do protocolo.

1.	M	$\rightarrow$	S	:	$\{\{P,Med,Q,V,M,D,Tinfo\}_{sKr_M}\}_{eKu_S}$
2.	F	$\rightarrow$	S	:	$\{Request(P.Nonce)_{sKr_F}\}_{eKu_S}$
3.	S	$\rightarrow$	F	:	$\{\{\{P,Med,Q,V,D,M,Tinfo\}_{sKr_M}\}_{eKu_P},Nonce\}_{eKu_F}$
4.	F	$\rightarrow$	P	:	$\{\{P,Med,Q,V,D,M,Tinfo\}_{sKr_M}\}_{eKu_P}$
5.	P	$\rightarrow$	F	:	$\{\{P,Med,Q,D,M\}_{sKr_P}\}_{eKu_F}$
6.	F	$\rightarrow$	S	:	$\{\{\{P,Med,Q,D,M\}_{sKr_P},\{Dmatrix\}\}_{sKr_F}\}_{eKu_S}$

Figura 19: Notação formal da proposta do protocolo completa.

4.6.4 Protocolo Multifator Médico-Farmacêutico-Paciente

Uma vantagens da RIC além de suportar certificados digitais, é sua capacidade de fazer match-on-card de impressão digital(BRASIL, 2010a). Essa ferramenta permite a construção de sistemas onde não é nescessário ter a impressão digital do usuário cadastrada previamente para fazer autenticação. Outra vantagem é que o dado biométrico fica de posse do usuário, impossibilitando a sua utilização indevida.

Desta maneira, é possível fazer autenticação-multifator em todas as etapas que envolvem a assinatura dos documentos eletrônicos. A aplicação ganha mais segurança e a versão completa do procolo não precisa de alterações formais.

Os passos que envolvem o protocolo continuam os mesmos da versão apresentada em 4.6.3, são eles:

- 1. O médico prescreve um medicamento, assina e submete a entrada para a central.
- 2. O farmacêutico envia uma solicitação das prescrições pendentes do paciente, ele assina esta requisição para garantir sua identidade.
- 3. A central envia as precrições do paciente solicitadas, cifrando os dados com a chave pública do paciente.
- 4. O farmacêutico, encaminha as precrições para o paciente escolher qual delas é a desejada.
- 5. O paciente, no intuito de adquirir o medicamento, assina a baixa do mesmo, referindo a quantidade desejada, e envia ao farmacêutico.
- 6. O farmacêutico, também assina a baixa que acabou de ser gerada pelo paciente, e submete esta com as 2 assinaturas a central.

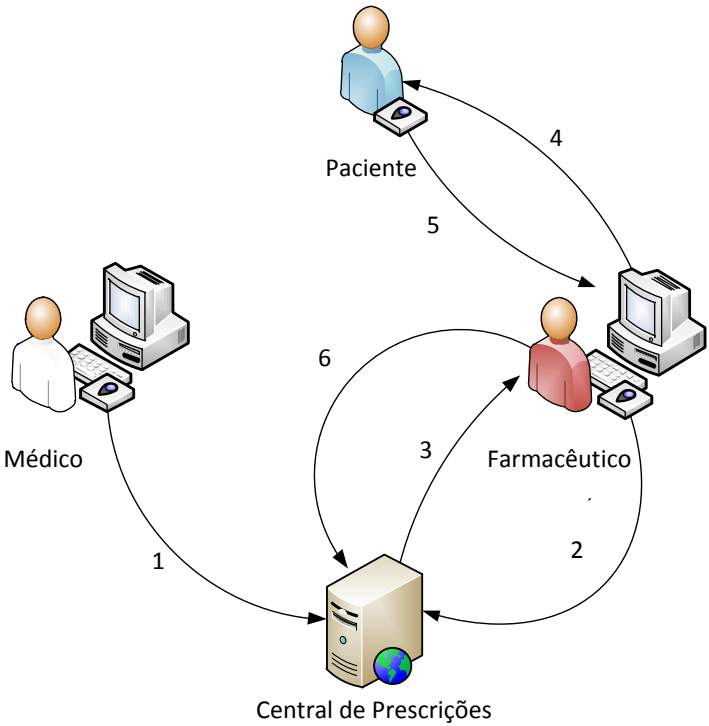


Figura 20: Versão completa do protocolo com autenticação multi-fator

A figura 21 representa formalmente as mensagens do protocolo descrito. Como já citado anteriormente, não existem diferenças formais entre os protocolos concebidos em 4.6.3 e nesta seção.

1.	M	$\rightarrow$	S	:	$\{\{P,Med,Q,V,M,D,Tinfo\}_{sKr_M}\}_{eKu_S}$
2.	F	$\rightarrow$	S	:	$\{Request(P.Nonce)_{sKr_F}\}_{eKu_S}$
3.	S	$\rightarrow$	F	:	$\{\{\{P,Med,Q,V,D,M,Tinfo\}_{sKr_M}\}_{eKu_P},Nonce\}_{eKu_F}$
4.	F	$\rightarrow$	P	:	$\{\{P,Med,Q,V,D,M,Tinfo\}_{sKr_M}\}_{eKu_P}$
5.	P	$\rightarrow$	F	:	$\{\{P,Med,Q,D,M\}_{sKr_P}\}_{eKu_F}$
6.	F	$\rightarrow$	S	:	$\{\{\{P,Med,Q,D,M\}_{sKr_P},\{Dmatrix\}\}_{sKr_F}\}_{eKu_S}$

Figura 21: Notação formal da proposta completa englobando autenticação com biometria.

5 PROTOTIPO DO PROJETO

A sigla SCiPhOEr é a abreviação de Secure Prescription Electronic Order Entry, que em português fica ”Prescrições Eletrônicas Seguras”. A segurança é suportada através das caracaterísticas fornecidas pelas ferramentas com as quais o sistema é construído e trabalha.

O sistema consiste de dois componentes

- Signer-SCiPhOEr: Aplicativo Applet que emite e submete os documentos de prescrição e dispensação.
- Central-SCiPhOEr: Serviço Web que recebe e gerencia prescrições e dispensações, e emite relatórios deste histórico.

5.1 TRABALHOS RELACIONADOS

Em (SONG; AHN; KIM, 2002), é proposto um sistema para transmissão de prescrições eletrônicas, através da internet, fazendo a comunicação entre hospitais(prescritores) e as farmácias(dispensadores). O formato do projeto coreano, centraliza as prescrições em um servidor remoto, gerenciando o disposório das mesmas. As características busca a identificação do paciente, através do certificado contido dentro de um smart card. O sistema ainda preve comunicação cifrada entre as partes, para fins de confidencialidade. Por se tratarem de sistemas, com finalidades praticamente idênticas, o projeto referido serve como referência, para construção deste novo sistema.

Outro software que esta diretamente relacionado a este projeto é o Dispensação Individualizada de Medicamentos (DIM). O DIM é uma ferramenta que gerencia a dispensação de medicamentos, é uma solução de grande porte, que propoe-se a atender, 20.000 dispensações por dia. O sistema controla em cada operação o lote e a validade dos medicamentos disponibilizados aos pacientes e identificando univocamente cada paciente, garantindo desta maneira a rastreabilidade(DISPENSACAO. . . , 2012).

Na próxima seção, é descrita a arquitetura do protótipo do SCiPhOER. São apresentados os contextos de processamento de informação, junto com sua organização estrutural. Depois que forem apresentadas as camadas que o sistema opera, fica claro que o DIM e o SCiPhOEr podem trabalhar juntos. O SCiPhOER é uma camada de software que pode ser ajustada as nescessidades do DIM, trazendo a confiança da assinatura digital para este software. A integração dos dois sistemas, é uma das propostas, de trabalhos futuros, apresentadas neste documento.

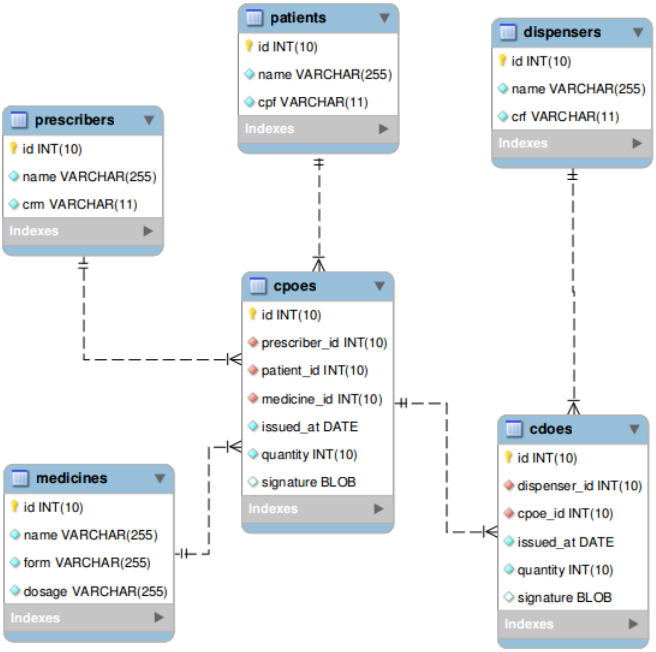


Figura 22: Tabelas do banco de dados

5.2 ESTRUTURA DA APLICAÇÃO

O sistema proposto, podem ser entendidos como um compenente de software, e sua abstração trás diversas vantagens. O aplicativo de assinatura dos documentos eletrônicos, é uma camada que fica abstraida do sistema clínico e a plataforma computacional.

A figura 22 é o modelo do banco de dados do Central-SCiPhOEr.

O Signer-SCiPhOEr, é a camada que fica destacada na figura abaixo. Sua implementação na verdade, é uma interface em cima de outras duas bibliotecas. O PBAD fornece as estruturas de para se trabalhar com os documentos eletrônicos, enquanto a LibCrytoDev, prove os recursos nescessários para os processos criptográficos envolvendo a assinatura digital.

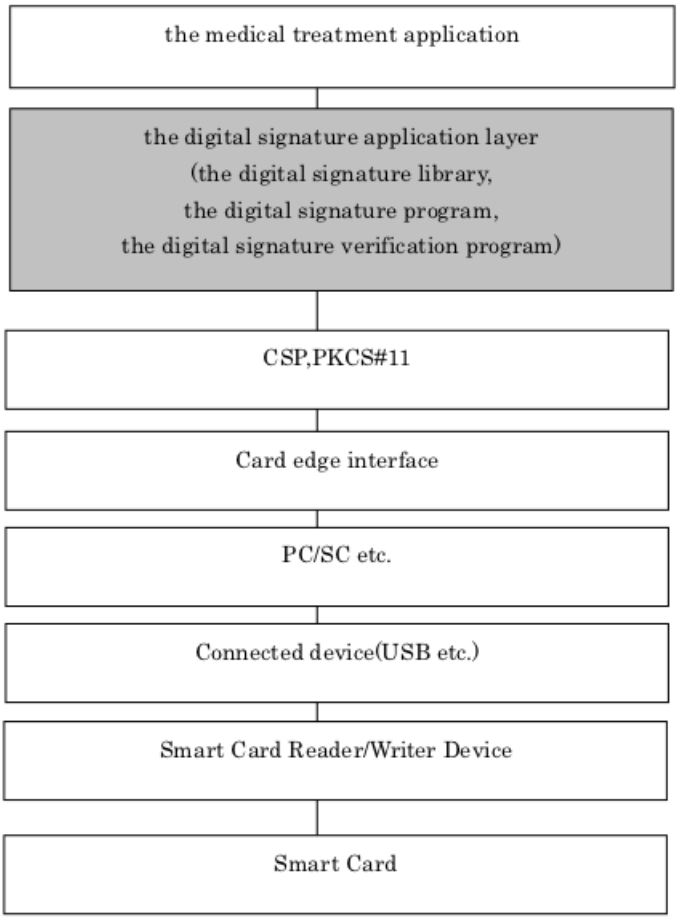


Figura 23: Camadas de processamento para assinatura de documentos eletrônicos médicos

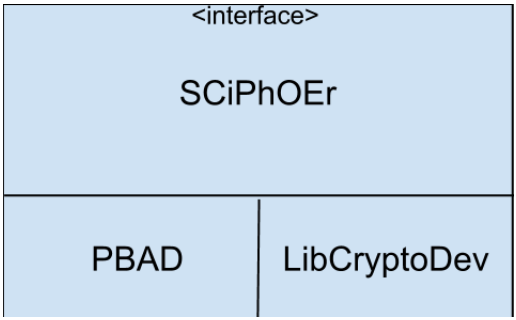


Figura 24: Estrutura do componente SCiPhOEr

5.3 TECNOLOGIAS UTILIZADAS

A seguir, são descritas as técnologias que foram utilizadas para implementação deste trabalho. O sistema consiste basicamente de dois softwares bem distintos, um é o assinador de prescrições e dispensações (Signer), e o outro é um serviço web (Central). São apresentadas algumas noções de suas funcionalidades e como estas foram arquitetadas para alcançar as funcionalidades desejadas.

Todas as técnologias utilizadas são distribuídas livremente.

5.3.1 Signer-SCiPhOEr

O Signer-SCiPhOEr é o aplicativo descrito na figura 23. As características incoporadas através das tecnologias utilizadas permite que os dados da prescrição sejam como paramêtros, ou escolhidos a partir de uma interface gráfica fornecida pelo software.

- Java SE Applet - O Java é uma plataforma de execução multi-plataforma. Programas são compilados a partir desta linguagem, e geram os Byte-CodesJava que então são interpretados pela sua máquina virtual. O Applet é uma solução muito popular para Web, é suportada pela solução Java e tem como foco a execução de tarefas que dependem do acesso á maquina, indisponíveis para os navegadores(JAVA. . . , 2012). Para este projeto, o Applet é a técnologia que permite o acesso ao smart-card dos atores do sistema.

- PBAD - O Padrão Brasileiro de Assinaturas Digitais, é um formato

para documentos eletrônicos que precisam se comunicar dentro da infra estrutura da ICP-BRASIL(INSTITUTO..., 2012).

- LibCryptoDev - A LibCryptoDev é uma biblioteca que foi desenvolvida como projeto interno do LabSEC. Esta biblioteca é na verdade uma camada de abstração para o acesso aos chaveiros que contem os certificados e as chaves privadas das entidade. Além de assumir algumas configurações que facilitam o desenvolvimento, a camada de separação permite que a biblioteca trabalhe com diversas plataformas computacionais. Atualmente suporta Windows e Linux(LABSEC..., 2012).

5.3.2 Central-SCiPhOEr

O Central-SCiPhOEr é um serviço instanciado em um servidor remoto. É responsável por verificar as assinaturas das prescrições e dispensações que lhe são submetidas, controlar as quantidades dos medicamentos que são fornecidos e pendentes, e por emitir os relatórios para o SNGPC.

- Java EE - O Java Enterprise é uma solução web construída em cima da plataforma Java. Esta especificação trata o lado do servidor da aplicação. Através desta infra estrutura, o Central-SCiPhOEr adquiri a portabilidade entre diferente plataformas. Outro motivo, para a escolha desta técnologia, é o suporte nativo a biblioteca Codigos-de-Referencia, implementação do PBAD.

- MySQL - O MySQL é um Sistema de Gerenciamento de Banco de Dados que utiliza a linguagem SQL como interface. Esta técnologia provê suporte a praticamente todas a plataformas e é atualmente um dos bancos de dados mais populares, com mais de 10 milhões de instalações pelo mundo. Dentre suas características este software ainda provê excelente desempenho e estabilidade, contraponto a pouca exigência quanto aos recursos de hardware(MYSQL, 2012).

- Apache Tomcat - A Apache é uma empresa que trabalha com soluções web em diversas prataflormas. O Tomcat é uma implementação de Container Web para a Plataforma Java. Da suporte a execução da especificação Java EE.

- TLS - A camada de transporte seguro, é uma implementação da utilização de certificados digitais para autentição e estabelecimento de chave de sessão(RFC5246..., 2008). Em todas as etapas deste protótipo que se

precisou utilizar de um canal seguro para a comunicação dos dados, esta foi a tecnologia utizada.

6 CONCLUSÃO

O trabalho proposto pode ser ampliada para o todos os tipos de medicamento. As facilidades providas com a informatização do sistema descritos em 2.5, são importante para outros tipos de medicamentos além dos controlados.

Assim como em (BARBOSA, 2011), a maioria dos estudos pertinentes a área de saúde, demonstraram a redução de erros pela implementação de Registros Eletrônicos de Saúde (RES), Sistemas de Prontuário Eletrônico (SPE) e Sistemas de Apoio à Decisão (SAD), sendo que a ilegibilidade foi eliminada.

A analise do processo de controle de medicamentos resultou na notação formal de um protocolo e a prototipação deste sistema mostrou-se prática, alcançando os objetivos do trabalho.

As evidências geradas com este estudo, servem como roteiro para a gestão pública sobre possíveis caminhos para a implantação do SNCM. A adoção da identificação unívoca de pessoas, é um requisito essencial para a implementação de registros eletrônicos em saúde que sejam verdadeiramente longitudinais e centrados no cidadão.

7 TRABALHOS FUTUROS

1. Integração com SNCM - Emissão automatizada de relatórios ao SNGPC, disponibilização das informações do rastreamento.

2. Proposta Offline - Uma necessidade em todos os sistemas que dependem de conexão com a internet, é um fluxo alternativo para quando a conexão esta indisponível. Para as prescrições, uma opção offline é desejada para trazer mais facilidades ao paciente. A materializaçao do documento através de códigos bidimensionais, armazenamento em cartões inteligentes pessoais ou temporários, juntamente mecanismos de sincronização com repositoórios assim que a conexão fosse restabelecida são propostas para um modelo offline.

3. Comprador não é o paciente - Estender a versão completa do protocolo permitindo a adição de um quarto ator. O comprador do medicamento precisa de uma autorização poder adquirir os medicamentos, isso pode se dar através de um cadastro prévio, ou então utilizando outras técnologias como Certificados de Atributos.

4. Sistema de Prevenção de Erros e Interações Medicamentosas - As informações envolvendo os medicamentos consumidos, são pertinentes ao prontuário eletrônico do paciente. Estas poderiam ser fornecidas a um sistema terceiro para acompanhamentos longitudinais e análise para diagnósticos.

5. Canal de comunicação Farmacêutico-Médico - Em havendo necessidade, o farmacêutico deve entrar em contato com o profissional prescritor para esclarecer eventuais problemas que tenha detectado.

6. Lembretes para tomar remédio - Aplicativos que utilizam das informações sobre o tratamento medicamentoso para enviar mensagens aos pacientes lembrando o horário correto de tomar o medicamento.

REFERÊNCIAS

AGUIAR, G.; SILVA, L.; FERREIRA, M. Ilegibilidade e ausência de informação nas prescrições médicas: fatores de riscos relacionados a erros de medicação. *Rev Bras Prom Saúde*, n. 19, p. 84–91, 2006.

ANDERSON, R. *Security Engineering*. 2nd. ed. [S.l.]: Wiley, 2008.

ANVISA, A. N. de V. S. *Site Oficial da Anvisa*. 2012. Acesso em 25 junho. <http://portal.anvisa.gov.br/>.

BARBOSA, N. da Silva de O. *Desempenho dos Sistemas de Prescrição Eletrônica e dos Sistemas de Apoio à Decisão na Pediatria: Uma Revisão Sistemática.* Dissertação (Mestrado) — Universidade Federal Fluminense, 2011.

BEMT, P. et al. Cost-benefit analysis of the detection of prescribing errors by hospital pharmacy staff. *Drug Saf*, n. 25, p. 135–143, 2002.

BENJAMIN, D. Reducing medication errors and increasing patient safety: case studies in clinical pharmacology. *J Clin Pharmacol*, n. 43, p. 768–83, 2003.

BRASIL. *Medida Provisória No 2.200-2*. 21 DE Agosto 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

BRASIL. *Lei n. 11903*. 14 DE JANEIRO 2009. Dispõe sobre o rastreamento da produção e do consumo de medicamentos por meio de tecnologia de captura, armazenamento e transmissão eletrônica de dados.

BRASIL, M. da J. *Decreto nº 7.166, de 5 DE maio*. 2010. Cria o Sistema Nacional de Registro de Identificação Civil, institui seu Comitê Gestor, regulamenta disposições da Lei no 9.454, de 7 de abril de 1997, e dá outras providências.

BRASIL, M. da J. *Resolução nº 2, DE 10 DE SETEMBRO*. 2010. Dispõe sobre as especificações técnicas básicas do documento de Registro de Identidade Civil.

BRASIL, M. da Saúde. Secretaria de Vigilância em S. *Portaria n. 344*. 1998. Dispõe sobre o Regulamento Técnico sobre substâncias e medicamentos sujeitos a controle especial.

CFM, C. F. de M. *Processo-Consulta CFM nº 1401 PC/CFM nº 30*. 2002.

CFM, C. F. de M. *Resolução 1.638*. 2002. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde.

CFM, C. F. de M. *Resolução 1.821*. 2007. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes , autorizando a eliminação do papel e a troca de informação identificada em saúde.

CFM, C. F. de M. *Resolução N 1.983*. 2012. Normatiza o CRM Digital para vigorar como cédula de identidade dos médicos inscritos nos Conselhos Regionais de Medicina.

DISPENSACAO Individualizada de Mendicamentos. 2012. <http://www.softwarepublico.gov.br/dotlrn/clubs/dim>.

DUTCH. *Health Informatics - Messages - Electronic exchange of messages on prescriptions and dispensations*. [S.l.], jan. 2011.

EICHELBERG, M. et al. A survey and analysis of electronic healthcare record standards. *ACM Comput. Surv.*, ACM, New York, NY, USA, v. 37, n. 4, p. 277–315, dez. 2005. ISSN 0360-0300. <http://doi.acm.org/10.1145/1118890.1118891>.

FRANKLIN, B. et al. The impact of a closed-loop electronic prescribing and administration system on prescribing errors, administration errors and staff time: a before-and-after study. *Qual Saf Health Care*, n. 16, p. 279–284, 2007.

GHALEB, M. et al. What constitutes a prescribing error in paediatrics? *Qual Saf Health Care*, n. 14, p. 352–357, 2005.

HARRIS, S. *CISSP All in One Exam Guide*. 5. ed. [S.l.: s.n.], 2010.

HELLMAN, M. E. An overview of public key criptography. *IEEE Transactions on Information Theory*, v. 40, p. 42–49, maio 2002.

HELLMAN, W. D. . M. E. New directions in cryptography. *IEEE Transactions on Information Theory*, v. 22, nov. 1976.

HOUSLEY, R.; POLK, T. *Planning for PKI Best Practices Guide fir Deploying Public Key Infrastructure*. 4th. ed. [S.l.]: John Wiley & Sons, 2001.

INSTITUTO Nacional de Técnologia. 2012. <http://www.iti.gov.br>.

ISO/IEC. *16022:Data Matrix bar code symbology specification*. [S.l.], 2006.

JAVA Technology. 2012. <http://www.java.com>.

KAWANO, D. F. et al. Acidentes com os medicamentos: como minimizá-los? *Revista Brasileira de Ciências Farmacêuticas*, scielo, v. 42, p. 487–495, 12 2006. ISSN 1516-9332. <http://www.scielo.br>.

LABSEC - Laboratório de Segurança em Computação. 2012. <http://www.labsec.ufsc.br/>.

MASTROIANNI, P. Análise de prescrição de medicamentos. *Revista de Ciências Farmacêuticas Básica e Aplicada*, n. 30, 2009.

MYSQL. 2012. <www.mysql.com>.

NOTO, A. R. et al. Analysis of prescription and dispensation of psychotropic medications in two cities in the state of são paulo, brazil. *Rev. Bras. Psiquiatr.*, v. 24, n. 2, jun. 2002.

ONU, J. I. D. F. D. E. *Risco dos Medicamentos Falsos*. 2006.

RFC5246 - The Transport Layer Security (TLS) Protocol. [S.l.], 2008. Http://tools.ietf.org/html/rfc5246.

RIVEST, R.; SHAMIR, A.; ADLEMAN, L. Method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, v. 21, p. 120–126, fev. 1978.

RYAN, P.; SCHNEIDER, S. *The Modelling and Analysis of Security Protocols*. [S.l.]: Addison Wesley, 2001.

SCHNEIER, B. *Applied Cryptography*. 2nd. ed. [S.l.]: John Wiley & Sons,, 1996.

SONG, W. J.; AHN, B. H.; KIM, W. H. Healthcare information systems using digital signature and synchronized smart cards via the internet. In: *Information Technology: Coding and Computing, 2002. Proceedings. International Conference on*. [S.l.: s.n.], 2002. p. 177–182.

STALLINGS, W. *Cryptography and Network Security Principles and Pratice*. 5. ed. [S.l.: s.n.], 2010.