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

Laurentino Augusto Dantas

ECN: Protocolo Criptográfico para Emissão de Certidões de Nascimento na Internet

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

Prof. Dr. Ricardo Felipe Custódio
Orientador

Florianópolis, Dezembro de 2001

ECN: Protocolo Criptográfico para Emissão de Certidões de Nascimento na Internet

Laurentino Augusto Dantas

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

Prof. Fernando Ostuni Gauthier, Dr.
Coordenador do Curso

Banca Examinadora

Prof. Dr. Ricardo Felipe Custódio
Orientador

Prof. Carlos Alberto Maziero. Dr.

Prof. Aires José Rover, Dr.

Prof. Sérgio Peters, Dr.

Ofereço esta dissertação a todos os professores, alunos e funcionários do CPGCC.

Agradecimentos

Aos meus pais, Idarci e Laurentino, pela educação e formação moral, que formam a base de todas as minhas conquistas.

Ao meu orientador Ricardo Felipe Custódio, por toda atenção a mim dispensada, pelas broncas nos momentos certos e por nunca ter me indicado o caminho mais curto, mas sempre o correto.

Ao Departamento de Pós-graduação em Ciência da Computação da Universidade Federal de Santa Catarina, pela qualidade do curso ministrado. Com uma lembrança especial às meninas da secretaria Verinha e Val.

Ao professor Júlio Szeremeta, por toda colaboração e sugestões ao trabalho, mas principalmente pela atenção dispensada a minha pessoa. Deixando registro da minha admiração pelo carinho com que ele exerce a sua tarefa de educador.

Aos companheiros de LabSEC, por toda a colaboração, críticas e sugestões ao trabalho.

Aos Professores Aires José Rover e Luiz Adolfo Olsen da Veiga do Centro de Ciências Jurídicas (CCJ), da Universidade Federal de Santa Catarina, por todo apoio e colaboração.

Aos colegas de mestrado, grandes companheiros durante o período de estudo, que me apoiaram e ajudaram em todos o momentos. Com agradecimentos especiais aos amigos Renato Bica Noal e Rodrigo Balzan.

Ao professor Fernando Ostuni Gauthier, coordenador do CPGCC, por todo o esforço demonstrado na tentativa de melhoria do curso, e pelas oportunidades de aprendizagem dadas a minha pessoa.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas

AC	Autoridade de Certificação
AD	Autoridade de Datação
AR	Autoridade de Registro
CD	Certificado Digital
CV	Cartório Virtual
D	Processo inverso de E, decifrar
DN	Declaração de Nascido Vivo
E	Cifrar, processo de criar o texto cifrado a partir do texto aberto
ENC	Emissão de Certidão de Nascimento
ICP	Infra Estrutura de Chaves Públicas
K	Chave
KR_i	Chave Privada de i
KU_i	Chave Pública de i
LCR	Lista de certificados revogados
LDAP	Diretório público
RP	Rede de Petri
RPC	Rede de Petri Colorida
RPCT	Rede de Petri Criptográfica
RPT	Rede de Petri com Temporização
X	Texto Aberto - texto de forma que pode ser entendido
Y	Texto Cifrado - texto de forma que não é possível entender

Resumo

A presente dissertação apresenta o protocolo Emissão de Certidão de Nascimento -ECN, um protocolo criptográfico para a Emissão de Certidão de Nascimento através da Internet. O objetivo é a incorporação de novas tecnologias ao processo atual de registro de nascimentos, tornando-o mais eficiente, menos dispendioso, mais seguro e direto, haja vista que poupará intermediários entre a comunicação do nascimento, pela maternidade, e sua oficialização, pelo cartório.

O Protocolo aqui proposto foi alcançado a partir de estudos sobre o atual sistema de Registro de Nascimento, desde a Maternidade até o agente de Registro Civil, além da revisão bibliográfica acerca da Criptografia e levantamento dos aspectos jurídicos que regem os documentos eletrônicos e a assinatura eletrônica no Brasil.

A formalização do protocolo deu-se através do uso de Redes de Petri, as quais possibilitaram uma análise detalhada e individual de todas as etapas do processo, além de gerar um modelo gráfico de fácil entendimento, o que pode ser averiguado no protótipo onde o ECN foi implementado, comprovando sua eficiência e simplicidade.

Não cabe aqui uma análise social, porém é sabido que em muitos desses ”lugares distantes”, são incontáveis os brasileiros que não alcançam sua cidadania e, conseqüentemente seus direitos constitucionais, pela falta de acesso ao Registro Civil. São brasileiros que nascem e morrem desconhecidos. E essa situação precisa ser modificada. Esperamos estar contribuindo para tanto.

Palavras Chaves: Segurança em redes de computadores, criptografia, protocolos criptográficos, metodologia de definição de protocolos criptográficos.

Abstract

This dissertation presents the Birth Certificate Emission (BCE) protocol, a cryptographic protocol for the emission of birth certificates through Internet. The purpose is the consolidation of new technologies to the current birth record process, making it more efficient, less costly, safer and more direct, once no broker intermediates are necessary between the communication of birth by the maternity and its officialisation by the record office.

The protocol here proposed was attained from studies about current Birth Certificates Registries system, from maternity to the civil record agent, besides bibliographic review concerning Cryptography and juridical aspects survey that rule the electronic documents and signatures in Brazil.

The protocol's formalization occurred through the use of Petri's Nets, which facilitate a detailed and individual analysis of every step of the process. Besides, it generates a graphic model easily understandable that can be verified on the prototype where BCE was implemented, confirming its efficiency and simplicity.

It does not compete here making a social analysis, therefore it is known that in many of theses "distant places"a large number of Brazilians do not obtain its citizenship and, consequently, its constitutional rights due to the lack of access to the Civil Records. They are those Brazilians who were born and die anonymous. It is necessary to modify this situation. We hope we have been some contribution to this.

Key Words: Network Security, cryptography, cryptography protocols, methodology of definition of cryptography protocols.

Capítulo 1

Introdução

As relações humanas têm passado por transformações de modo cada vez mais rápido, em virtude da influência que novas tecnologias exercem no cotidiano das pessoas. O computador e a Internet são participantes da atual revolução tecnológica, e a sua popularização tem trazido uma série de benefícios para as pessoas em geral.

Dentre as muitas vantagens proporcionadas pela Internet, uma é a agilidade na emissão e recepção de informação, de tal forma que as pessoas não precisam se locomover para realizar tarefas as mais variadas, tais como transações bancárias, estudar, comprar produtos, etc.

A conexão à Internet, que anteriormente era possível por um único aparelho, o computador, está disponível em um número sem precedente de outros aparelhos, como celulares e eletrodomésticos. É inevitável, portanto, um cenário no qual a Internet se torne uma ferramenta cada vez mais presente na vida das pessoas.

A Internet é um meio de comunicação relativamente barato, e existe um grande esforço, tanto por parte do Governo Federal quanto da iniciativa privada, de prover acesso à Internet a todos os cidadãos brasileiros, de todas as classe sociais.

Desta maneira, devemos enxergar a Internet como uma ferramenta que tem grande utilidade social. A democratização do acesso a Internet fará com que mais brasileiros aproveitem seus serviços, estendendo os benefícios do conhecimento disponível em sua estrutura, o que pode significar melhorias para a qualidade de vida da população

em geral.

O LabSEC - Laboratório de Segurança em Computação do Curso de Pós-graduação em Computação da Universidade Federal de Santa Catarina, vem desenvolvendo uma série de trabalhos os quais, através do uso de criptografia, permitem adicionar mecanismos de segurança aos serviços da Internet.

O Cartório Virtual (CV) é um dos projetos atualmente desenvolvidos pelo LabSEC. O CV tem como principal objetivo estudar e desenvolver tecnologias que garantam a segurança de documentos eletrônicos.

Entre os projetos do CV destaca-se o sub-projeto de Emissão de Registros Públicos, cuja preocupação básica é a especificação, a análise e a implementação de protocolos criptográficos para a emissão de Registros Públicos através da Internet.

1.1 Objetivos

Este trabalho tem por objetivo apresentar um protocolo criptográfico para emissão de certidões de nascimento através da Internet, denominado Protocolo Emissão de Certidão de Nascimento (ECN).

1.1.1 Objetivo Geral

Criar um protocolo criptográfico para a emissão de certidões de nascimento através da Internet, usando técnicas de criptografia e Infra-estrutura de Chaves Públicas, abrindo espaço para discussões jurídicas e criação de legislação que regulamente o processo.

1.1.2 Objetivos Específicos

1. Fazer um levantamento do funcionamento dos ofícios de registro civil de pessoas naturais, através da visita a um cartório e entrevista com o tabelião responsável;

2. verificar o modo como é feito o registro público, para se obter conhecimento das rotinas, de como é dada a fé pública e de como são arquivados os documentos;

3. fazer uma revisão bibliográfica sobre criptografia;

4. estudar alguns protocolos criptográficos básicos e entender o seu funcionamento;

5. propor um protocolo criptográfico adequado para emissão de certidão de nascimento através da Internet;

6. formalizar o protocolo ECN através de Redes de Petri;

7. implementar um protótipo que faça uso do protocolo ECN, a fim de validá-lo.

1.2 Motivação

A seguir são listadas as principais motivações para o desenvolvimento deste trabalho:

1. melhoria da qualidade dos serviços de cartórios de registros públicos, com a implantação da emissão de certidões de nascimento através da Internet;

2. facilidade de acesso aos dados das certidões de nascimento;

3. regulamentação da validade jurídica do documento eletrônico no Brasil através da MP $2.200-2$, de 24 de Agosto de 2001;

4. o grande número de brasileiros que não possuem certidão de nascimento;

5. planejamento das ações sociais e econômicas do governo e da iniciativa privada, através da obtenção de estatísticas confiáveis;

6. mostrar que novas tecnologias de assinatura digital podem ser usadas de forma eficiente e confiável.

1.3 Conteúdo

Este documento está assim estruturado:

Capítulo 2 - Descreve o registro de nascimentos. São apresentadas as leis que o regulamenta, os seus procedimentos, a análise das suas deficiências e os aspectos que motivam a sua informatização.

Capítulo 3 - Contém uma revisão bibliográfica sobre criptografia. É relatado como surgiu e como foi o seu desenvolvimento. Conceitua-se os dois tipos de criptografia (assimétrica e simétrica), os tipos de ataques que os sistemas podem sofrer e os protocolos criptográficos. Faz uma comparação entre a criptografia simétrica e assimétrica.

Capítulo 4 - Apresenta a Infra Estrutura de Chaves Públicas (ICP), cujo principal componente, a Autoridade Certificadora (AC), é responsável pela emissão dos certificados digitais. A ICP será a base para a implantação das propostas que serão discutidas dentro do capítulo 7.

Capítulo 5 - Apresenta as Redes de Petri, ferramenta que será utilizada para a formalização do protocolo ECN.

Capítulo 6 - Descreve o documento eletrônico e o compara com o documento tradicional no papel. Fala sobre Assinatura Digital e Assinatura Convencional. Este capítulo traz uma série de referências a artigos que tratam destes assuntos no âmbito jurídico.

Capítulo 7 - Apresenta três propostas para a informatização do processo de registro de nascimentos. São citados os benefícios de cada uma delas, bem como as dificuldades para implantação.

Capítulo 8 - Formaliza o protocolo ECN através de Redes de Petri e apresenta uma análise dos requisitos de segurança deste protocolo.

Capítulo 9 - Apresenta os resultados obtidos e propostas de novos trabalhos a serem desenvolvidos.

Capítulo 2

Registro de Nascimentos

2.1 Introdução

Neste capítulo é descrito como efetua-se atualmente o registro de nascimentos no Brasil. A seção 2.2 traz um histórico do registro e as leis que o regem. A seção 2.3 apresenta a Declaração de Nascido Vivo (DN). A seção 2.4 descreve o modelo atual e a seção 2.5 apresenta uma representação do processo. Finalmente na seção 2.6 são citadas as principais deficiências do sistema atual de registro de nascimento e a seção 2.7 os aspectos que motivam a sua informatização.

2.2 Aspectos Legais da Certidão de Nascimento

No Brasil, a partir da Lei 4.827, de $07/03/1924$, os registros públicos foram unificados. Posteriormente, esta disciplina foi alterada por outras legislações e regulamentações, e em 1973 foi publicada a Lei 6.015, de $31/12/1973$ [BRA a] [FED 00]. Com relação ao nascimento esta lei estabelece o seguinte:

> *"Art. 50. Todo o nascimento que ocorrer no território nacional deverá ser dado a registro no lugar em que tiver ocorrido o parto, dentro do prazo de quinze dias, ampliando-se até três meses para os lugares distantes mais de trinta quilômetros da sede do cartório."*

No Estado de Santa Catarina[dSC], um provimento de abril de 1999, que ”Aprova o Código de Normas da Corregedoria-Geral da Justiça, destinado ao foro extrajudicial”, determina, entre outros requisitos, a obrigatoriedade da utilização da Declaração de Nascido Vivo - DN, por todos os Ofícios de Registro Civil de Pessoas Naturais:

> *”Art.89 - .....*
>
> *§ 1º - É obrigatória a partir de 1º de janeiro de 1994, a utilização da Declaração de Nascido Vivo - DN, por todos os Ofícios de Registro Civil de Pessoas Naturais, para o registro do assento de nascimento, devendo constar no assento, o número da respectiva DN.”*

O procedimento do Cartório, portanto, é exigir que o responsável pelo registro apresente a Declaração de Nascido Vivo (DN), a qual será emitida pelo hospital ou maternidade. Ressalte-se aqui que esta é uma regra de todo o Território Nacional.

2.3 Declaração de Nascido Vivo

A DN foi instituída pela lei 8.069 [BRA b], que dispõe sobre o estatuto da criança e do adolescente.

A DN é um documento padronizado, pré-numerado, apresentado em três vias e impressas pelo Ministério da Saúde, através da Fundação Nacional de Saúde - FNS, repassadas às Regionais para serem enviadas aos respectivos municípios, e através destes, aos Estabelecimentos de Saúde e Cartórios.

A DN deve ser preenchida, em todo o território nacional, para todos os nascidos vivos:

- nas unidade de internação ou emergência dos estabelecimentos de saúde;
- fora dos estabelecimentos de saúde, mas que neles venham a receber assistência imediata;
- em domicílio ou em outros locais.

Tabela 2.1: Declaração de Nascido Vivo em Partos Hospitalares.

Via	Destino
Primeira Via (Cor Branca)	Regional de Saúde. Deve ser coletada juntamente com a via rosa, por busca ativa, pelos órgãos responsáveis.
Segunda Via (Cor Amarela)	Cartório. Deve ficar com o responsável, que a apresentará ao Cartório de Registro Civil para efetuar o registro de nascimento propriamente dito.
Terceira Via (Cor Rosa)	Secretaria Municipal de Saúde. Deve ser arquivada na Secretaria Municipal de Saúde do município de residência da mãe.

A DN pode ser preenchida por um médico, por um membro da equipe de enfermagem da sala de parto ou do berçário, ou por outra pessoa previamente treinada para tal fim.

As três vias da DN, dependendo do tipo de parto, hospitalar ou domiciliar, terão destinos diferentes conforme explicitado abaixo.

2.3.1 Partos Hospitalares

Nos Partos Hospitalares, isto é, os que ocorrem em Estabelecimentos de Saúde, é o próprio Estabelecimento de Saúde o responsável pelo preenchimento da DN. Cada uma de suas vias devem ser encaminhadas conforme mostra a tabela 2.1.

2.3.2 Partos Domiciliares

Nos Partos Domiciliares, os que comumente são realizados por parteiras leigas por ocorrerem em residências, o preenchimento da DN é fundamental e deve ser feito nos Estabelecimentos de Saúde ou em Cartórios de Registro Civil.

Tabela 2.2: Declaração de Nascido Vivo em Partos Domiciliares.

Via	Destino
Primeira Via (Cor Branca)	Regional de Saúde. Deve ser coletada juntamente com a via rosa, por busca ativa, pelos órgãos responsáveis.
Segunda Via (Cor Amarela)	Cartório. Deve ficar com o responsável, que a apresentará ao Cartório de Registro Civil para efetuar o registro de nascimento propriamente dito.
Terceira Via (Cor Rosa)	Secretaria Municipal de Saúde. Deve ser recolhida em busca ativa, pela Secretaria Municipal de Saúde e arquivada observando-se a residência da mãe.

Quando a DN for preenchida pelo cartório, este deve avisar imediatamente a Vigilância Epidemiológica Municipal, para que esta dê início à investigação. Cabe também à Vigilância cuidar do preenchimento dos campos ainda em branco.

A Secretaria de Saúde de cada estado tem autonomia para criar normas para garantir o preenchimento da DN, independente do lugar onde ocorra o nascimento. Neste tipo de parto, a DN deve ser tratada conforme mostra a tabela 2.2.

2.4 Processo de Registro de Nascimentos

Ao nascimento de uma criança, um Agente Autorizado emite uma DN, que é entregue para a pessoa responsável pelo registro. A própria lei 6.015 [BRA a] define o responsável pelo registro de nascimento.

”Art. 52. São obrigados a fazer declaração de nascimento:

1. *O pai;*

2. *em falta ou impedimento do pai, a mãe, sendo neste caso o prazo para declaração prorrogado por quarenta e cinco (45) dias;*
3. *no impedimento de ambos, o parente mais próximo;*
4. *em falta ou impedimento do parente referido no número anterior, os administradores de hospitais ou os médicos e parteiras, que tiverem assistido o parto;*
5. *pessoa idônea da casa em que ocorrer, sendo fora da residência da mãe;*
6. *finalmente, as pessoas (VETADO) encarregadas da guarda do menor. (Redação dada pela Lei nº* 6.216 *de* $30/06/1975$*).”*

Cabe ao responsável pelo registro levar a DN ao cartório para ser efetuado o registro de nascimento. No Cartório o tabelião a partir dos dados da Declaração de Nascido Vivo e de informações complementares passadas pela pessoa que efetua o registro, faz as devidas anotações no livro de registro de nascimentos e emite a Certidão de Nascimento.

Os dados necessários para o registro de nascimento também são definidos pela Lei 6.015 [BRA a]:

”Art 54:

1. *O dia, mês, ano e lugar do nascimento e a hora certa, sendo possível determiná-la, ou aproximada;*
2. *o sexo do registrando; (Redação dada pela Lei nº* 6.216 *de* $30/06/1975$*);*
3. *o fato de ser gêmeo, quando assim tiver acontecido;*
4. *o nome e o prenome, que forem postos à criança;*
5. *a declaração de que nasceu morta, ou morreu no ato ou logo depois do parto;*
6. *a ordem de filiação de outros irmãos do mesmo prenome que existirem ou tiverem existido;*

7. *os nomes e prenomes, a naturalidade, a profissão dos pais, o lugar e cartório onde se casaram, a idade da genitora, do registrando em anos completos, na ocasião do parto, e o domicílio ou a residência do casal; (Redação dada pela Lei nº* 6.140 *de* $28/11/1974$*).*
8. *os nomes e prenomes dos avós paternos e maternos;*
9. *os nomes e prenomes, a profissão e a residência das duas testemunhas do assento.*"

2.5 Processo de Registro de Nascimento

A figura 2.1 ilustra os passos do registro de nascimento para um melhor entendimento do processo. Como ilustrado nesta figura, o Agente Autorizado, após ao nascimento de uma criança viva, emite uma DN e a entrega ao responsável pelo registro. Este, por sua vez, encaminha a DN ao Cartório de Registros Civil. O Cartorário, após identificar e coletar informações do responsável, repassa os dados contidos na DN e os coletados no livro de registros e emite uma ou mais Certidões de Nascimento.

2.6 Deficiências do Processo

Pode-se dizer que uma das principais, senão a primeira, garantia da cidadania, após o nascimento é a pessoa receber o registro de nascimento. A partir deste, uma série de outros direitos são proporcionados. Tanto é importante este "primeiro" direito que a legislação o garante a todos os filhos de cidadãos brasileiros. Entretanto, este direito ainda não é tão acessível a população de baixa renda como deveria ser.

Uma evidência de como o sistema de registro de nascimentos atualmente em prática é ineficiente, é o grande número de pessoas brasileiras que não possuem certidão de nascimento, situação lembrada pelo Senador Carlos Patrocínio no seu discurso na 39.a Sessão Não Deliberativa, em $19/04/2000$.

"O SR. CARLOS PATROCÍNIO PFL-TO. Pronuncia o seguinte discurso.

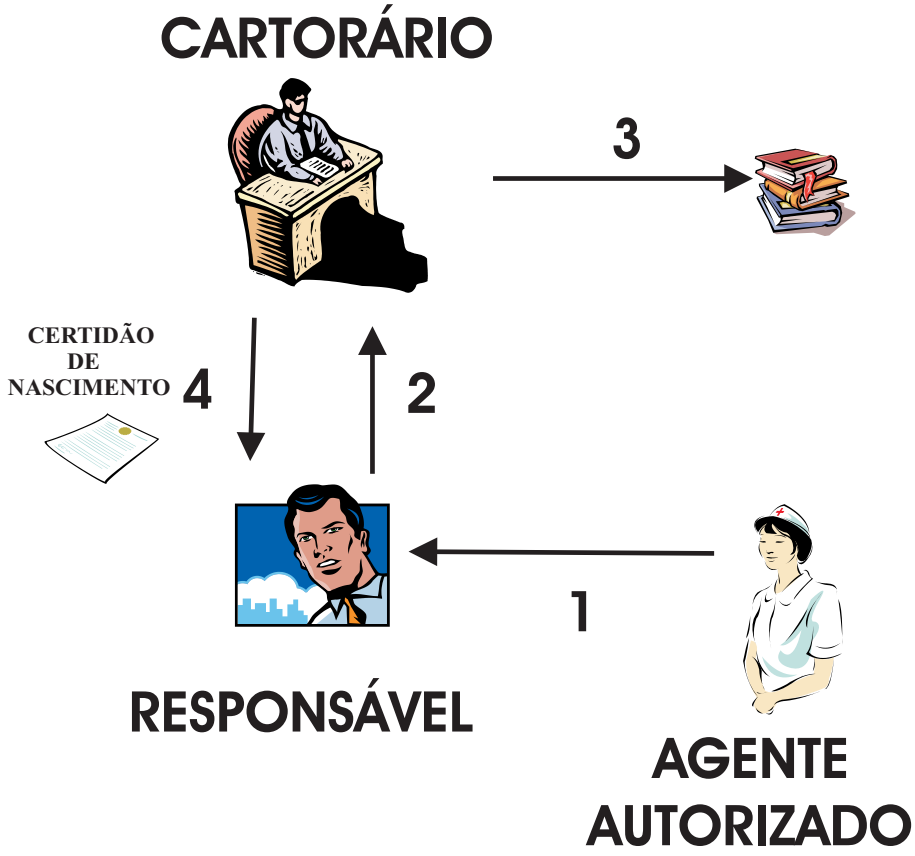

Figura 2.1: Representação do Processo de Registro de Nascimentos. 1. O Agente Autorizado emite uma Declaração de Nascido Vivo (DN) e a entrega ao responsável pelo registro. 2. O Responsável encaminha a DN ao Cartorário. 3. O Cartorário repassa os dados da DN no livro de registros e emite uma Certidão de Nascimento. 4. O Responsável pelo registro recebe a Certidão de Nascimento.

Sem revisão do orador. Sra. Presidente, Sras. e Srs. Senadores, muito se falou hoje sobre cidadania, e é justamente sobre esse tema que eu também gostaria de falar.

Na marcha do Brasil rumo a um processo civilizatório definitivo, nada mais pertinente do que trazer à pauta de nossas discussões o tema da garantia do Estado na emissão de certidão de nascimento a todos os brasileiros. As mais recentes estatísticas indicam, aterradoramente, que o País abriga 10 *milhões de brasileiros sem qualquer registro civil. No ingresso de um novo milênio, não se pode conceber que ainda existam compatriotas inteiramente desprovidos de um documento oficial de identificação.*”

É possível atribuir uma parcela da culpa deste problema, que conforme o senador é um atentado à cidadania de milhões de brasileiros, ao modo arcaico como ainda hoje é realizado o registro de nascimento.

O sistema de registro de nascimento atual faz uso de tecnologias ultrapassadas, e pode-se facilmente detectar variadas deficiências, que contribuem ou são decorrentes da ineficiência do sistema:

- para poder efetuar o registro, o responsável tem que se deslocar até o cartório, o que demanda tempo e custos com transporte;
- as estatísticas referentes ao crescimento demográfico são elaboradas em tempo já defasado, pois os cartórios mandam os mapas com as informações para o IBGE apenas a cada 3 meses, conforme está estipulado na Lei 6.015 [BRA a].
- Não há garantias que o registro seja definitivamente realizado, uma vez que cabe ao responsável pelo registro encaminhar a DN ao cartório.

2.7 Motivações para a Informatização do Processo

A lei brasileira que regulamenta o registros públicos data apenas de $31/12/1973$ [BRA a]. Esta lei permitiu a utilização de dispositivos mecânicos para a escrituração dos livros:

> *"Art. 3o."A escrituração será feita em livros encadernados, que obedecerão aos modelos anexos a esta Lei, sujeitos à correição da autoridade judiciária competente.*
>
> *§ 2o. Para facilidade do serviço, podem os livros ser escriturados mecanicamente, em folhas soltas, obedecidos os modelos aprovados pela autoridade judiciária competente."*

Esta medida visava facilitar o trabalho do escrivão, e mostrava que existia a aceitação para modernização do processo. Apesar da Lei 6.015 de 1973 ser relati-

vamente nova no ano da sua publicação, o uso de computadores ainda não era muito difundido.

No começo dos anos 70 os computadores eram máquinas enormes e caras, que demandavam mão de obra altamente especializada, não apresentavam grande poder de processamento, tinham capacidade de armazenamento baixa e eram desconhecidas da grande maioria das pessoas.

A situação atual com relação aos computadores é diferente. O preço dos computadores e custo de armazenamento digital diminuíram fazendo com que a maioria das empresas e instituições optam pelo armazenamento digital de dados.

Nos anos 80, os micro-computadores começaram a se tornar populares e acessíveis às pessoas em geral, e nos anos 90 a Internet permitiu que os computadores do mundo todo se conectassem. Nos dias de hoje o computador está presente em muitas residências, e a maioria destes computadores estão conectados a Internet. Através dela as pessoas têm à disposição uma série de serviços que possibilitam-nos realizar tarefas sem a necessidade de deslocamento.

O cenário atual é totalmente favorável à disponibilização dos mais diversos tipos de serviços na Internet, principalmente os serviços públicos, que desta maneira se tornariam mais acessíveis às pessoas de modo em geral.

O modelo atual de registro de nascimento é caro e ineficiente, pois não traz benefícios a nenhuma das partes. Os responsáveis legais têm gastos com perda de tempo e transporte, os cartorários necessitam manter estruturas onerosas e o governo demora para receber informações que nem sempre são precisas. Tal situação deve-se, em parte, ao uso de tecnologias muito antigas e que já poderiam ter sido substituídas por outras mais eficientes. Para que população, cartórios e governo usufruam destas novas tecnologias no processo de registro de nascimento, é necessário que novos modelos sejam criados de tal modo que o registro seja menos oneroso e mais dinâmico.

O uso de computadores traria benefícios incontestáveis:

- permitiria que o registro fosse efetuado sem a necessidade de envio de informações em papel e deslocamento de pessoas;

- com a criação de bancos de dados digitais, as informações poderiam ser disponibilizadas mais rapidamente, permitindo que os dados sobre a população fossem obtidos diariamente, de maneira mais precisa e confiável.

- mais importante é que com o registro sendo iniciado no Agente Autorizado, e enviados diretamente para o Cartorário, existiria a certeza que toda a criança nascida em território brasileiro seria registrada.

2.8 Conclusão

Este capítulo descreveu como é feito registro de nascimento e mostrou suas deficiências, os problemas decorrentes deste modelo, e as principais deficiências decorrentes da utilização de tecnologias ultrapassadas.

A informatização pode melhorar muito o processo e trazer benefícios a todas as partes envolvidas.

Capítulo 3

Fundamentos de Criptografia

3.1 Introdução

Neste capítulo são descritos os conceitos básicos de criptografia. O entendimento destes conceitos é importante para a compreensão de como serão adicionados mecanismos de segurança ao processo de emissão de registro de nascimento.

> *O termo segurança é utilizado com o significado de minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos. Vulnerabilidade é qualquer fraqueza que pode ser explorada para se violar um sistema ou as informações que ele contém.[ISO 89]*

> *A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados, e a utilização não autorizada do computador ou de seus dispositivos periféricos. A necessidade de proteção deve ser definida em termos das possíveis ameaças e riscos e dos objetivos de uma organização, formalizados nos termos de uma política de segurança.[SOA 95]*

A segurança para área da informática consiste na certeza de que as informações não serão visualizadas e nem modificadas por pessoas não autorizadas. Atualmente a principal forma de garantir esta propriedade é através do uso de criptografia.

A criptografia através do processo de cifragem, transforma a informação de texto aberto [1] para texto cifrado[2]. Uma vez que o texto cifrado é ilegível, faz-se necessário o processo de decifragem, que transforma o texto cifrado em texto aberto. No entanto para se executar o processo de decifragem, é necessário ter o conhecimento prévio de uma chave. Desta maneira a criptografia garante que apenas quem conheça a chave terá acesso à informação.

Apenas a criptografia, contudo, não consegue resolver problemas complexos de troca de mensagens, fazendo-se necessária uma série de regras, que é definida por um protocolo criptográfico.

Este capítulo está dividido da seguinte forma: na seção 3.2 são citados os principais termos da criptografia, nas seções 3.3, 3.4, 3.5 e 3.6 são transcritos os tipos de criptografia, suas características e é realizada uma comparação entre elas; finalmente na seção 3.7 são descritas quais as características de um protocolo criptográfico.

3.2 Termos utilizados

Criptografia (kriptós = escondido, oculto; grápho = grafia) é a arte ou ciência de escrever em cifra ou em códigos. Pode ser definida como a arte e ciência de garantir a segurança de mensagens [SCH 96], de forma a permitir que somente o destinatário a decifre e a compreenda .

Criptoanálise (kriptós = escondido, oculto; análysis = decomposição) é a arte ou ciência de determinar a chave ou decifrar mensagens cifradas sem conhecer a chave. Uma tentativa de criptoanálise é chamada *ataque*.

Criptologia (kriptós = escondido, oculto; logo = estudo, ciência) é a ciência que reúne a criptografia e a criptoanálise.

[1] Texto Aberto - Texto na forma em que pode ser lido ou entendido

[2] Texto Cifrado - Texto não legível que passou pelo processo de cifragem.

3.3 Criptografia

A criptografia é tão antiga quanto a própria escrita. Já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos também utilizavam códigos secretos para comunicar planos de batalha. O mais interessante é que a tecnologia de criptografia não mudou muito até meados deste século.

Foi somente depois da Segunda Guerra Mundial, com a invenção do computador, que a ciência realmente floresceu, incorporando complexos algoritmos matemáticos. Por exemplo durante a guerra, os ingleses ficaram conhecidos por seus esforços para decriptar códigos dos alemães. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna [GER 93] .

A criptografia computacional, como a conhecemos hoje, é baseada em algoritmos criptográficos, e protege os sistemas quanto à ameaça de perda de confiabilidade, integridade ou não-repudiação. Ou seja, é utilizada para garantir:

sigilo - somente os usuários autorizados têm acesso à informação;

integridade - garantia oferecida ao usuário de que a informação correta, original, não foi alterada, nem intencionalmente, nem acidentalmente;

autenticação do usuário - é o processo que permite ao sistema verificar se a pessoa com quem está se comunicando é de fato a pessoa que alega ser;

autenticação de remetente - é o processo que permite a um usuário certificar-se que a mensagem recebida foi de fato enviada pelo remetente, podendo-se inclusive provar perante um juiz, que o remetente enviou aquela mensagem;

autenticação do destinatário - consiste em se ter uma prova de que a mensagem enviada foi como tal recebida pelo destinatário;

autenticação de datação - consiste em provar que a mensagem foi produzida numa determinada data;

Para a utilização do processo de cifragem e decifragem, são necessários algoritmos criptográficos (comumente denominados cifradores) e chaves de criptografia. O cifrador é um algoritmo que, com base em substituições e permutações, transforma o texto aberto em texto cifrado. Se a segurança de um algoritmo de criptografia baseia-se no desconhecimento do algoritmo, ele é dito restrito. Todavia, estes cifradores não são largamente utilizados [SCH 96].

Nos cifradores modernos, segue-se o princípio de Kerckhoff, em que a segurança de um algoritmo de criptografia baseia-se no desconhecimento das chaves envolvidas, e não no desconhecimento do algoritmo em si [STI 95]. A chave é um parâmetro do cifrador, independente do texto aberto, que faz com que a saída do cifrador seja dependente do texto aberto e da chave. O conjunto de possíveis chaves de um cifrador é denominado *espaço de chaves*.

De acordo com [STI 95], um criptossistema é uma quíntupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, tal que:

- $\mathcal{P}$ é um conjunto finito de possíveis textos abertos;
- $\mathcal{C}$ é um conjunto finito de possíveis textos cifrados;
- $\mathcal{K}$ é o espaço de chaves;
- para cada $K \in \mathcal{K}$, há uma regra de cifragem $e_K \in \mathcal{E}$ e uma regra de decifragem correspondente $d_K \in \mathcal{D}$. Cada $e_K : \mathcal{P} \rightarrow \mathcal{C}$ e $d_K : \mathcal{C} \rightarrow \mathcal{P}$ são funções tais que $d_K(e_K(x)) = x$ para cada texto aberto $x \in \mathcal{P}$.

A diferença de como um criptossistema trata a relação entre os conjuntos $\mathcal{E}$ e $\mathcal{D}$ pode dividi-los em duas categorias de algoritmos de criptografia: os simétricos e os assimétricos.

3.4 Criptografia Simétrica

Em um sistema de criptografia simétrica, a mesma chave que é utilizada para cifrar o texto aberto, é utilizada para decifrar o texto cifrado correspondente. Para

que a entidade emissora e a entidade receptora consigam estabelecer uma comunicação segura, através de um sistema de criptografia simétrica, é necessário que as duas tenham entrado previamente em acordo para definir qual a chave que deve ser utilizada, ou então a chave precisa ser transmitida por um canal seguro, o que pode ser difícil de se conseguir.

A figura 3.1 ilustra o processo de criptografia simétrica.

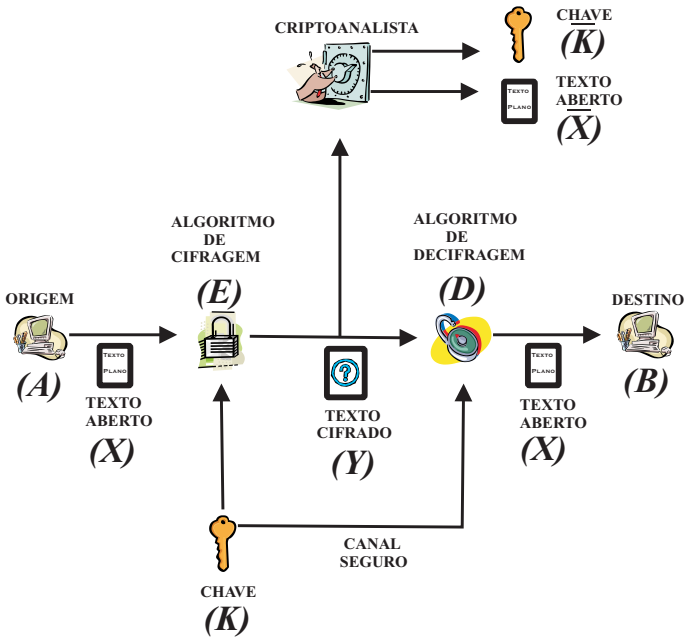

Figura 3.1: Processo de Criptografia Simétrica. Com a mensagem X e a chave K, o algoritmo de cifragem E formou o texto cifrado Y; o Receptor em posse do algoritmo de decifragem D e da chave K, usada para decifrar, consegue obter novamente a mensagem X; um oponente observando Y, porém sem acesso a K ou X, pode tentar descobrir X, caso esteja interessado numa mensagem específica, ou K caso esteja interessado em poder ler mensagens futuras (ou ambas).

Com a mensagem X e a chave K o algoritmo de cifragem E formou o texto cifrado Y. Este processo pode ser representado como:

$$Y = E_K(X)$$

O Receptor de posse do algoritmo de Decifragem D e da chave K usada para decifrar, consegue obter novamente a mensagem X.

$$X = D_K(Y)$$

Um oponente observando Y, porém não tendo acesso a K ou X, pode tentar descobrir X, caso esteja interessado nesta mensagem específica, ou K, caso esteja

interessado em poder ler mensagens futuras (ou ambas). Assume-se que o oponente tenha conhecimento dos algoritmos de cifragem (E) e do algoritmo de decifragem (D).

3.5 Criptografia Assimétrica

O desenvolvimento da criptografia de chave pública é a maior e possivelmente a única verdadeira revolução na história da criptografia [STA 99].

Os algoritmos de chave pública são baseados em funções matemáticas ao invés de substituições e permutações, mas a principal característica é que a criptografia de chave pública é assimétrica, envolvendo o uso de duas chaves diferentes para cifrar e decifrar. O uso de duas chaves traz profundas conseqüências para a confidencialidade, distribuição de chaves e autenticação.

Algoritmos de chave pública usam uma chave para cifrar, chamada de chave privada (KR) e uma diferente, porém relacionada, para decifrar, chamada de chave pública (KU). A chave para decifrar deve ser amplamente divulgada .

Para garantir segurança, deve ser computacionalmente impraticável determinar a chave privada tendo conhecimento da chave pública e do algoritmo de cifragem. Alguns algoritmos, como o RSA [STA 99], permitem que qualquer uma da chaves seja usada para cifrar, com a outra sendo usada para decifrar.

Os passos básicos para execução do processo são:

- cada participante gera um par de chaves;
- as chaves públicas são divulgadas;
- se A quer mandar uma mensagem autenticada para B, este envia a mensagem cifrada com a sua chave privada. Caso queira mandar uma mensagem confidencial para B, irá cifrá-la com a chave pública de B;
- B recebe a mensagem e decifra a mensagem com a sua chave privada em caso de mensagem confidencial, ou com a chave pública de A em caso de mensagem autenticada;

3.5.1 Confidencialidade

Dada uma mensagem X e uma chave de cifragem KU_b como entrada, A monta o texto cifrado $Y = [Y1, Y2...Yn]$ da seguinte forma:

$$Y = E_{KU_b}(X)$$

B de posse da sua chave privada, consegue inverter a transformação:

$$X = D_{KR_b}(Y)$$

A figura 3.2 ilustra este processo.

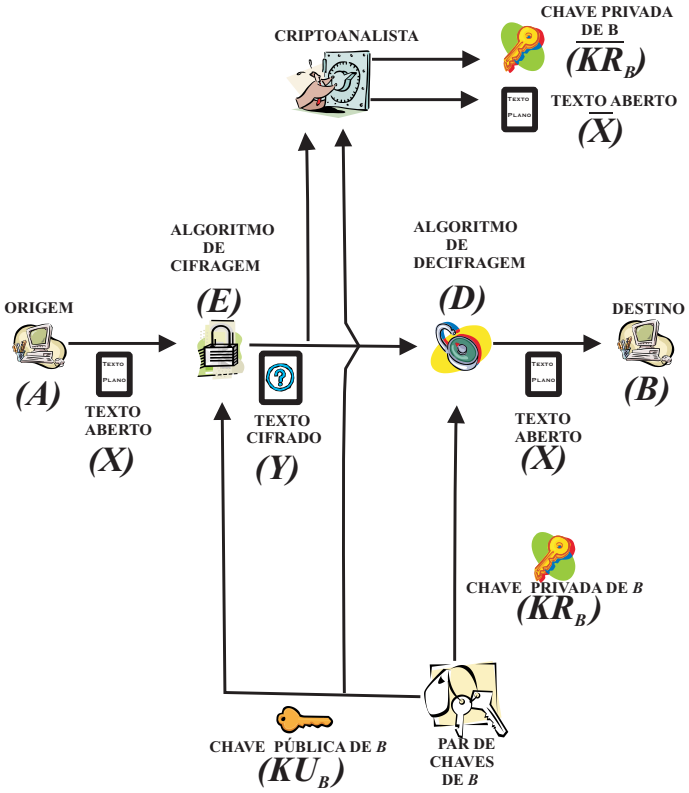

Figura 3.2: Figura que representa o processo de Criptografia Assimétrica para providenciar confidencialidade. A mensagem é cifrada por A usando a KU_b, produzindo o texto cifrado Y; B para ter acesso ao texto aberto X, deve decifrar Y usando KR_b. Um oponente observando Y e tendo acesso a KU_b, E e D, porém não tendo acesso para KR_b ou X, pode tentar descobrir X caso esteja interessado nesta mensagem específica, KR_b caso esteja interessado em poder ler mensagens futuras (ou ambas).

Um oponente observando Y e tendo acesso a KU_b, porém não tendo acesso para KR_b ou X, pode tentar descobrir X caso esteja interessado nesta mensagem específica, KR_b caso esteja interessado em poder ler mensagens futuras (ou ambas).

Assume-se que o oponente tenha conhecimento dos algoritmos de Cifragem (E) e do algoritmo de Decifragem (D).

3.5.2 Autenticação

A origem A cifra da seguinte forma a mensagem com a sua chave privada e a envia para B.

$$Y = E_{KR_a}(X)$$

O Destino B só poderá decifrar a mensagem com a chave pública de A, tendo desta forma a certeza da origem da mensagem, ou seja:

$$X = D_{KU_a}(Y)$$

A figura 3.3 ilustra este processo:

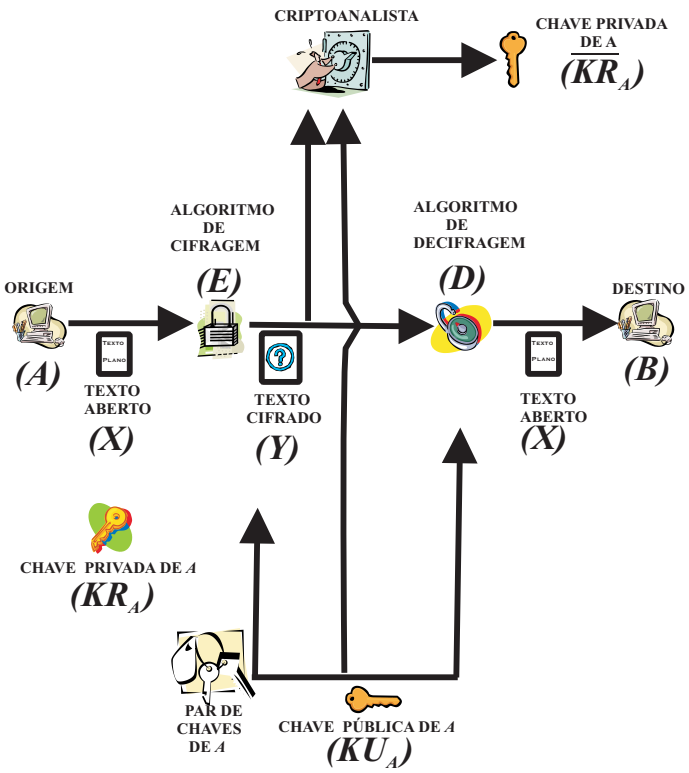

Figura 3.3: Processo de Criptografia Assimétrica para providenciar autenticidade. A origem A cifra a mensagem com a sua chave privada. O Destino B só poderá decifrar a mensagem com a chave pública de A, identificando desta forma a origem da mensagem.

3.5.3 Autenticação e Confidencialidade

Para poder enviar a mensagem, garantindo-se tanto a autenticidade quanto sua confidencialidade, uma origem deve cifrar a mensagem com a sua chave privada e com a chave pública do destino:

$$Y = E_{KU_b}[E_{KR_a}(X)]$$

O Destino deve primeiro decifrar com a sua chave privada e depois com a chave pública da origem:

$$X = D_{KU_a}[D_{KR_b}(Y)]$$

A figura 3.4 ilustra o processo de transmissão de uma mensagem, tanto com autenticação quanto com confidencialidade:

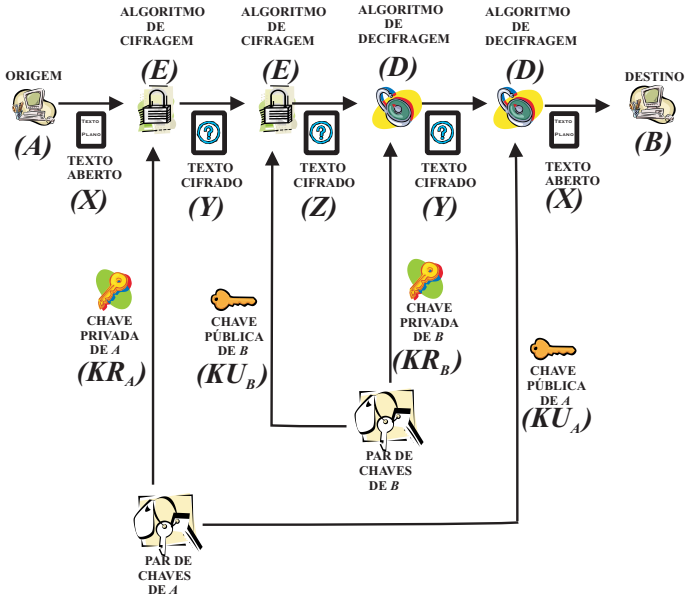

Figura 3.4: Processo de Criptografia Assimétrica para providenciar tanto autenticidade quanto privacidade. Uma origem deve cifrar a mensagem com a sua chave privada e com a chave pública do destino. O Destino deve primeiro decifrar com a sua chave privada e depois com a chave pública da origem.

3.5.4 Aplicação dos Sistemas de Chave Pública

Em termos gerais, o uso de criptossistemas de chave pública pode ser classificado em três categorias [STA 99]:

a - Cifragem/Decifragem o emissor cifra a mensagem com a chave pública do receptor.

b - Troca de Chaves dois lados cooperam para compartilharem uma chave de seção. Várias e diferentes aproximações são possíveis, envolvendo a chave privada de uma ou ambas as partes.

c - Assinaturas Digitais: o emissor assina a mensagem com a sua chave privada.

A assinatura digital é um algoritmo criptográfico com as seguintes características [SCH 96]:

- **Autenticidade**: a assinatura garante que o remetente tenha de fato assinado a mensagem;
- **Não-Falsificação**: a assinatura garante que o remetente, e ninguém mais, assinou a mensagem;
- **Unicidade**: a assinatura é parte de uma mensagem, portanto não pode ser reutilizada em uma mensagem diferente;
- **Integridade**: depois de ter sido assinada, uma mensagem não pode ser alterada;
- **Não-Repúdio**: a assinatura impede que o remetente alegue não ter assinado a mensagem.

3.6 Criptografia de Chave Pública versus Criptografia Simétrica

A questão de qual dos dois tipos de algoritmo é melhor vem sendo debatida desde o surgimento do algoritmo de chave pública. Alguns debates assumem que eles podem ser comparados em condições semelhantes, porém isso não é possível.

"Os algoritmos de chave simétrica são mais rápidos e usam chaves menores. Desta maneira, são mais eficientes" [STI 95].

Convém ressaltar, como discutido nas seções 3.4 e 3.5, *"os dois tipos de criptografia são diferentes tipos de ferramentas, resolvem diferentes tipos de problemas. Os algoritmos simétricos são melhores para cifrar dados, porém os algoritmos de chave pública são melhores para gerenciamento de chave e são os mais utilizados em protocolos"* [STI 95].

3.7 Protocolos Criptográficos

Todo e qualquer criptossistema, quando utilizado isoladamente (somente cifragem e decifragem) tem uma utilidade muito restrita. Para ser realmente útil, a criptografia deve prover meios para a troca de mensagens com segurança.

Um protocolo é uma série de passos, envolvendo um ou mais participantes, objetivando executar uma tarefa [SCH 96]. Entende-se por protocolos criptográficos, aqueles que se utilizam de criptografia em um ou mais de seus passos, normalmente com o objetivo de criar alguma aplicação mais complexa do que simplesmente cifrar e decifrar textos.

Os diversos participantes de um protocolo podem trocar informações entre si, confiando ou não uns nos outros, e através desta troca de informações realizar tarefas como votação secreta, assinatura de contrato em grupo e outras mais. Para que uma série de passos possa realmente ser chamada de protocolo, é necessário que as seguintes premissas sejam obedecidas:

1. todos os participantes de um protocolo devem conhecê-lo e saber todos os passos de antemão, antes da execução do mesmo;

2. todos os participantes de um protocolo devem concordar em segui-lo;

3. o protocolo não deve apresentar ambigüidade. Cada passo deve ser bem definido e não deve haver possibilidade de alguma instrução ser mal entendida;

4. o protocolo deve ser completo, deve haver uma ação específica para cada situação possível.

A utilização de um protocolo adequado e eficiente é de extrema importância para garantir a segurança das mensagens trocadas durante as transações.

Existe a possibilidade de se implantar uma transação segura em qualquer uma das camadas do modelo de referência OSI [TAN 96]. Na Internet, pode-se citar como exemplo o IPSec [SMI 97], o qual garante uma comunicação segura na camada de rede, e o SSL/TLS [SMI 97], que possibilita uma comunicação segura na camada de transporte provendo os serviços de integridade, confidencialidade e autenticação na comunicação.

Apesar dos protocolos que garantem segurança nas camadas inferiores no modelo de referência OSI, sistemas que necessitam de segurança na camada de aplicação requerem outros itens de segurança, os quais não são supridos pelos serviços oferecidos nas camadas inferiores.

3.8 Conclusão

O presente capítulo apresentou uma série de conceitos sobre criptografia. Sua principal finalidade foi apresentar as técnicas que serão utilizadas para especificar o ECN.

Foram descritas a criptografia simétrica e assimétrica, suas características, traçando-se uma breve comparação entre elas. Introduziu-se o conceito de protocolos criptográficos e sua importância no desenvolvimento de aplicações seguras.

Capítulo 4

Infra-estrutura de Chaves Públicas (ICP)

4.1 Introdução

"A ICP descreve um sistema que utiliza Chaves Públicas e Certificados Digitais para garantir a segurança do sistema e confirmar a identidade de seus usuários"[CER].

A ICP baseia-se em um sistema de confiança, no qual duas entidades (que podem ser pessoas ou computadores) confiam mutuamente em uma Autoridade Certificadora (AC). Neste capítulo, discute-se o funcionamento da AC.

Devido as suas características, a ICP será utilizada no ECN para possibilitar a identificação das Entidades que participarão do processo de registro de nascimentos.

O capítulo tem a seguinte estrutura: na seção 4.2 são descritas as autoridades certificadoras; a seção 4.3 apresenta o que são os certificados digitais; e finalmente a seção 4.5 descreve a revogação de certificados.

4.2 Autoridades Certificadoras

Autoridades Certificadoras são as entidades que emitem e assinam os certificados digitais. Também é responsabilidade da AC a revogação de certificados e a publicação de uma lista pública onde constem os certificados revogados.

Uma AC pode certificar outras ACs de modo que as mesmas sejam ramificações da AC original. Tais ramificações são chamadas de ACs filiadas e seguem as mesmas políticas impostas pelas ACs hierarquicamente superior.

Para permitir que Autoridades de Certificação diferentes cooperem entre si, é possível que autoridades emitam certificados para outras autoridades, conhecido como *certificação cruzada* .

4.3 Certificados Digitais

"Os Certificados Digitais fornecem um meio eletrônico de verificar a identidade de uma pessoa. Eles fornecem uma solução de segurança mais completa, assegurando a identidade de todas as partes envolvidas numa transação " [STA 99].

Os certificados digitais são definidos conforme as normas do padrão X.509 da ITU-T (International Telecommunication Union).

Um certificado associa uma Chave Pública e um único nome para um usuário [FEG 99], de forma que:

- a AC irá satisfazer a necessidade de identidade de um usuário criando um certificado para ele.
- a AC não poderá emitir dois certificados com o mesmo nome para pessoas diferentes.

A figura 4.1 mostra a estrutura de Certificado Digital, sendo que seus principais elementos são:

Versão - elemento que diferencia as sucessivas versões de formato de certificado, podendo ter o valor 0,1 ou 2, representando as versões 1, 2 ou 3 da recomendação

X.509;

Número Serial - valor inteiro único atribuído pela AC a um certificado;

Identificação do Algoritmo de Assinatura - algoritmo usado para assinar o certificado e os parâmetros associados;

Nome do Emissor - nome X.500 [FEG 99] da AC que criou e assinou o certificado;

Período de Validade - consiste de duas datas que determinam o período durante o qual o certificado é válido;

Nome do Sujeito - nome do usuário a quem o certificado se refere;

Informação sobre a Chave Pública do sujeito - a chave pública do sujeito, junto com a identificação do algoritmo com o qual esta chave pode ser usada;

Identificação Única do Emissor - elemento usado para identificar se a AC emissora é única (no padrão X.509 o nome pode ser reutilizado por várias ACs);

Identificação Única do Sujeito - elemento usado para identificar se o sujeito é único (no padrão X.500 o nome pode ser reutilizado por diferentes entidades);

Extensões - conjunto de uma ou mais informações de extensão. As extensões foram implementadas na versão 3;

Assinatura - elemento que protege todos os outros campos do Certificado. Contém o código *hash* dos outros campos, cifrado com a chave privada da AC, e a identificação do algoritmo de assinatura.

4.4 Obtendo o Certificado de um Usuário

Os certificados emitidos por uma AC possuem as seguintes características:

- qualquer usuário com acesso à chave pública da AC pode recuperar a chave pública do usuário que foi certificado;

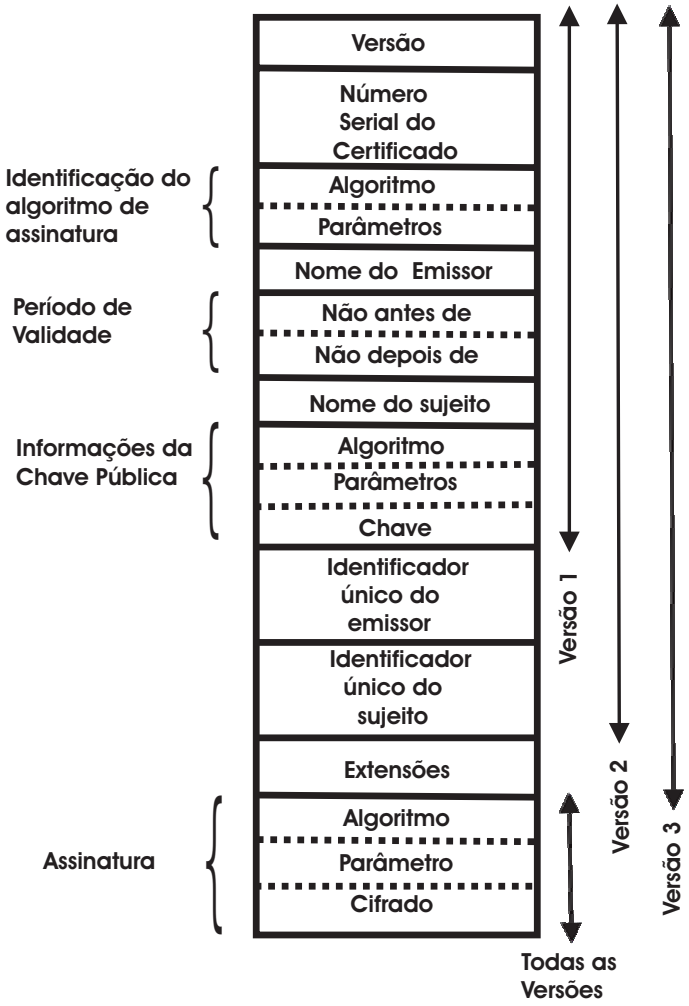

Figura 4.1: Estrutura dos certificados digitais

- ninguém, a não ser a AC, pode modificar o certificado sem que a alteração seja detectada.

Por serem inesquecíveis, os certificados podem ser colocados em um diretório sem a necessidade do serviço de diretório criar esforços especiais para protegê-los.

Se todos os usuários possuem certificados de uma mesma AC, então existe uma negociação comum desta AC, para que possa transmitir seu certificado diretamente para outro usuário.

Agora no caso de um usuário A que obteve o seu certificado de uma AC $X1$ e um outro usuário B, que por sua vez tenha obtido o seu certificado da AC $X2$, o certificado de B, emitido pela AC $X2$ é desconhecido para A. A pode ler o certificado de B porém não pode verificar a assinatura.

Se as duas CAs tiverem negociado as suas próprias chaves públicas, o seguinte procedimento propiciará condições para que A obtenha o certificado de B:

1. A obtém no diretório o certificado de $X2$ assinado por $X1$, por conhecer a chave pública de $X1$. A pode obter a chave pública de $X2$ deste certificado e verifica-lo por meio da assinatura de $X1$ no certificado;

2. A obtém o certificado de B no diretório público assinado por $X2$, obtendo assim a chave pública de $X2$, podendo verificar sua assinatura.

4.5 Revogação de Certificados

Cada certificado possui um período de validade, porém pode ser necessária a revogação de um certificado antes do prazo de sua expiração por uma das seguintes razões:

1. o dono do certificado perdeu as prerrogativas que o habilitava a possuir o certificado e não tem mais o direito de usá-lo;

2. a chave privada foi comprometida;

3. o dono do certificado não quer mais usá-lo;

4. a chave privada da AC que emitiu o certificado foi comprometida;

Quando um certificado é revogado, os usuários devem ser comunicados de que o certificado não é mais válido. Esta notificação é feita através de uma lista dos certificados revogados. Esta lista é chamada de LCR.

A LCR é uma lista pública que assegura que certificados revogados não serão mais utilizados. As LCRs são emitidas e assinadas digitalmente pela Autoridade de Certificação que emitiu os certificados incluídos na lista de revogação.

A função da AC inclui criar LCRs periodicamente e a distribuí-las às aplicações clientes através de meios apropriados. LCRs podem ser disponibilizadas às entidades de ICP por vários mecanismos, dos quais os mais comuns são: LCRs publicadas no diretório LDAP e LCRs em sites HTTP.

4.6 Conclusão

Neste capítulo, foram descritos os principais elementos que formam a infra-estrutura de Chaves Públicas.

A ICP baseia-se em um sistema de confiança, no qual duas entidades (que podem ser pessoas ou computadores) confiam mutuamente em uma AC (Autoridade de Certificação) para verificar e confirmar a identidade de ambas as partes.

Todo certificado tem um prazo de validade, contudo pode ser revogado antes do prazo previsto se alguma anormalidade ocorrer. A AC é responsável por divulgar todos os certificados revogados.

Os certificados revogados são publicados numa LCR, lista emitida pelas autoridades certificadoras, com a finalidade de garantir que os certificados que não são válidos não sejam utilizados. As ACs conseguem identificar o proprietário de um certificado e garantir que este certificado não seja utilizado quando o seu proprietário não tiver mais o direito de fazê-lo.

Capítulo 5

Redes de Petri

5.1 Introdução

As Redes de Petri (RP) foram desenvolvidas por Carl Adam Petri, em sua tese de doutorado intitulada *Kommunikation mit Automaten* (1962) [PET 81], na faculdade de Matemática e Física da Universidade de Dortmund, Alemanha.

Redes de Petri são um formalismo do tipo diagrama de transição de estado para a modelagem e validação de sistema. *"As RPs se adaptam bem a um grande número de aplicações em que noções de eventos e de evoluções simultâneas são importantes"* [CAR 97].

Trata-se de uma ferramenta gráfica e algébrica de modelagem (descrição e especificação) que pode ser aplicada em diversos tipos de sistemas, apresentando um bom nível de abstração em comparação com outros formalismos[CAR 97].

Além disso, as Redes de Petri (RP) possibilitam a verificação da corretude do sistema especificado. Usando-se RP, pode-se modelar sistemas discretos em geral, representando facilmente os paralelismos, concorrências, sincronismos, conflitos não determinísticos, etc.

Devido às suas características, as Redes de Petri serão utilizadas neste projeto para a definição do modelo formal do protocolo ECN.

Este capítulo está estruturado da seguinte forma: na seção 5.2 são apre-

sentados os conceitos básicos de RPs como suas notações algébrica e gráficas; na seção 5.3 serão abordadas algumas extensões e abreviações da conceituação original.

5.2 Conceitos Básicos

O conceito fundamental das RPs é que todo sistema dinâmico e discreto pode ser modelado através de três conjuntos de primitivas [CAR 97], a saber:

Estados : situação em que se encontra o sistema em determinados instantes;

Eventos : ocorrências internas ou externas ao sistema que ao serem percebidas pelo mesmo causam mudanças de estado;

Condições : atributos associados aos eventos e que habilitam a sua ocorrência;

A representação gráfica de uma RP é efetuada por um multigrafo, bipartido e dirigido. Os dois tipos de nós deste multigrafo são:

Nós Lugares : representados por círculos e que serão os depósitos das primitivas condições;

Nós Transições : representados por barras e que modelam as primitivas eventos;

Uma condição verdadeira é representada por uma ficha no respectivo lugar.

A rede é efetivada unindo-se lugares a transições e transições a lugares (bipartido). A figura 5.1 representa uma RP com três lugares (p_1, p_2, p_3) e duas transições (t_1, t_2).

A primitiva estado do sistema é representada pela distribuição das fichas nos respectivos lugares. A RP da figura 5.1 está representando: 2 condições em p_1, nenhuma em p_2 e uma única em p_3.

Algebricamente, uma RP é representada por uma quádrupla [CAR 97]

$R = (P, T, Pre, Pos)$

onde:

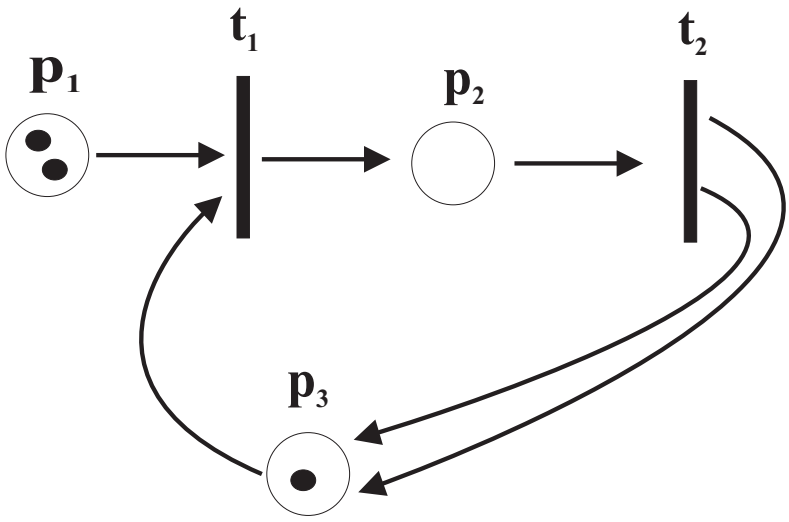

Figura 5.1: Representação de uma RP com 3 lugares(p_1, p_2, p_3) e duas transições (t_1, t_2), que está com 2 condições em p_1, nenhuma condição em p_2 e uma única condição em p_3

$P = p_1, p_2, p_3, ..., p_n =$ Conjunto de Lugares, $n > 0$;

$T = t_1, t_2, t_3, ..., t_m =$ Conjunto de Transições, $m > 0$;

$Pre : P \times T \longrightarrow N$ é a aplicação de arcos de entrada das transições (lugares precedente).

$Pos : T \times P \longrightarrow N$ é a aplicação de arcos de saída das transições (lugares posteriores).

$P \cap T = \emptyset$

N: é o conjunto de números naturais.

Um evento (transição) só pode ocorrer se existirem fichas em todos os seus lugares de entrada, em quantidade igual ou superior à das respectivas arestas. A ocorrência do evento retira fichas dos lugares de entrada e as coloca nos lugares de saída, em quantidade igual à das respectivas arestas, e causa uma mudança de estado.

Na RP da figura 5.1 o único evento que pode ocorrer é t_1 e sua ocorrência conduz à rede representada na figura 5.2

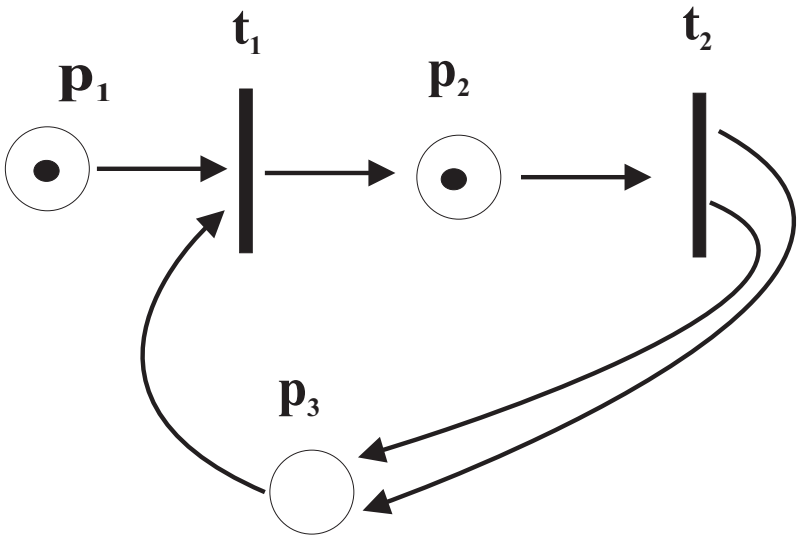

Figura 5.2: Representação da uma RP da figura 5.1 após o disparo da transição t_1, agora a rede que está com 1 condição em p_1, uma condição em p_2 e nenhuma condição em p_3. Não é possível o disparo de nenhuma transição

5.3 Variantes do Modelo Original de Redes de Petri

Conforme definidas no item anterior, as RP possuem expressividade para representar apenas as relações de causa e efeito entre os eventos e os estados do sistema. Almejando ampliar o poder de modelagem, mesmo que em detrimento do poder de decisão, têm sido desenvolvidas extensões do modelo original que já chegam às dezenas. Aqui serão apresentadas sucintamente três destas extensões, com destaque para uma desenvolvida especificamente para a modelagem e análise de sistemas criptográficos, abordados nesta dissertação.

5.3.1 Redes de Petri envolvendo o Tempo

Como as RP são um diagrama de transição de estado, naturalmente muitos dos sistemas modelados envolvem o fator tempo. Dentre as várias propostas que incluem a variável tempo, destaca-se a extensão denominada de Rede de Petri com Temporização - RPT desenvolvidas por Merlin (1974) [CAR 97]. Uma RPT é uma RP na qual associa-se um intervalo de tempo $[\theta_{min}, \theta_{max}]$ para cada t_i. Neste caso t_i deve

esperar o tempo θ_{min} para poder disparar após habilitada, e não poderá disparar após o tempo θ_{max}, mesmo estando habilitada.

Por exemplo na RPT da figura 5.3 a transição t_2 só pode disparar 2 unidades tempo após a chegada da ficha em p_2, e não pode disparar transcorridos 5 unidades de tempo após a chegada da ficha.

Note-se que uma RP é uma RPT com a restrição de que $[\theta_{min}; \theta_{max}] = [0; \propto]$.

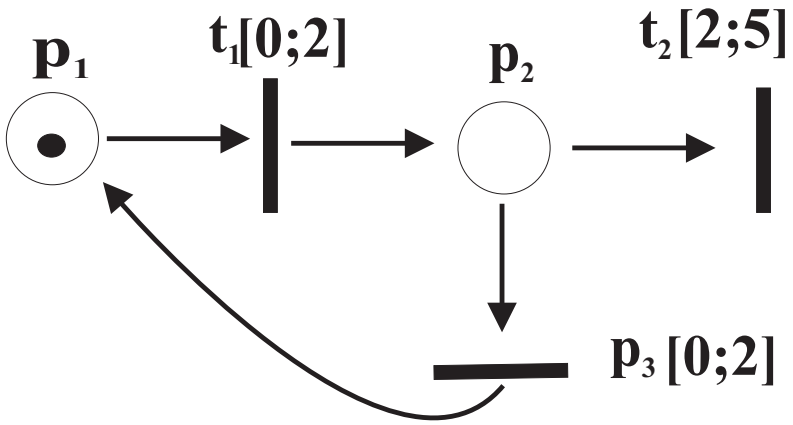

Figura 5.3: Representação de uma RP com Temporização conforme Merlin, t_1 só pode disparar até 2 unidades de tempo após a chegada da ficha em p_1,t_2 só pode disparar até 2 unidades de tempo após a chegada da ficha em p_2, e t_3 só pode disparar após 2 unidades e antes de 5 unidades de tempo após a chegada da ficha em p_2

Outras extensões envolvendo o tempo são RP t-temporizadas apresentada por Ramchandani em sua tese de Doutorado em 1973 no MIT [PAL 95], às quais associa-se em cada t_i um tempo $\theta(t)$ de disparo. Por exemplo na rede da figura 5.4 o disparo de t_1 dura 5 unidades de tempo.

Seguindo as extensões que envolvem tempo, pode-se citar as RP p-temporizadas de Sifakis (1977) [PAL 95], nas quais associa-se um tempo de indisponibilidade da ficha no lugar p. Por exemplo na rede da figura 5.5, quando chegar em p_2 a ficha só estará disponível a t_2 disparar três unidades de tempo após.

Observe-se que as extensões de Ranchandani e de Sifakis podem facilmente ser transformadas em equivalentes no modelo de Merlin.

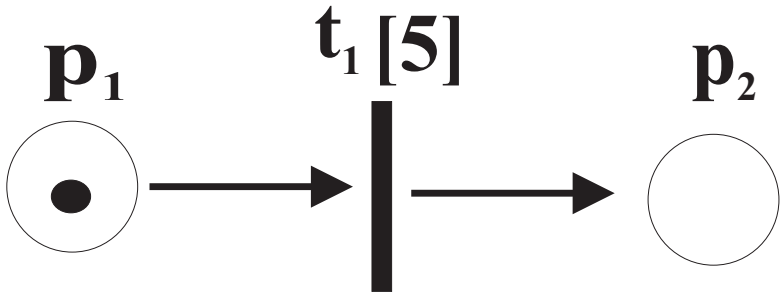

Figura 5.4: Representação de uma RP com Temporização conforme Ranchandani. O disparo de t_1 dura 5 unidades de tempo

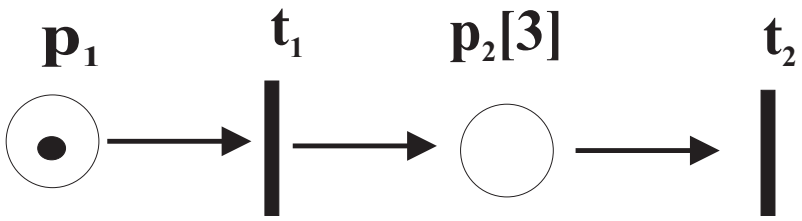

Figura 5.5: Representação de uma RP com Temporização conforme Sifakis, quando a ficha chegar em p_2, ela só estará disponível para t_2 disparar três unidades de tempo após.

5.3.2 Redes de Petri Coloridas

A especificação de sistemas complexos com RP produz modelos extensos devido à ocorrência de partes idênticas ou quase, e a necessidade de lugares específicos para a identificação das condições (fichas). Além disso, outro inconveniente é que pequenas alterações no sistema podem implicar no redesenho de todo o modelo.

As Redes de Petri Coloridas - RPC, desenvolvidas por Jensen (1991)[PAL 95], simplificam o modelo gráficos das RP e evitam o inconveniente do redesenho para alterações. Elas fazem parte de uma família de extensões denominada Redes de Alto Nível.

Numa RPC, um mesmo lugar é o depósito de fichas de vários tipos (cores) distintas. O fluxo destas fichas é controlado por dois conjuntos de atributos: um associado as transições e que definem restrições para a sua ocorrência e outro associado aos arcos e que indicam as quantidades e tipos das fichas que serão removidas das entradas e colocadas nas saídas quando da ocorrência da transição. Por exemplo na rede da figura 5.6 tem-se 3 tipos de fichas em p_1 e o disparo de t_1 será controlado pelos atributos $< k >$,

$< x >$ e $< y >$.

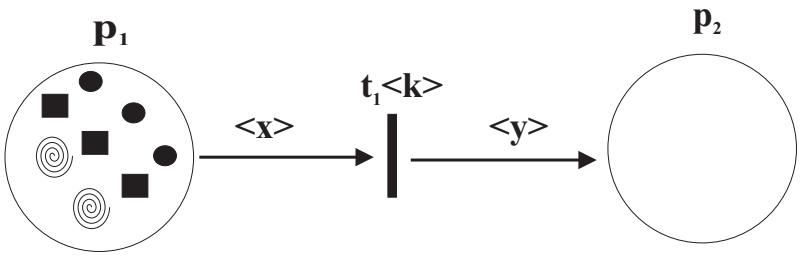

Figura 5.6: Representação da uma RP Colorida, onde tem-se 3 tipos de fichas em p_1, o fluxo destas fichas é controlado por dois conjuntos de atributos, um associado as transições e que definem restrições para a sua ocorrência e outro associado e outro associado aos arcos que indicam a quantidade e tipos das fichas que serão removidas. Neste caso o disparo de t_1 será controlado pelos atributos $< k >$, $< x >$ e $< y >$, .

5.3.3 Redes de Petri Criptográficas

Especificamente propostas para a área de segurança em computação, esta extensão desenvolvida por Lee (1997) [LEE 97] consiste em se complementar o modelo de RP convencional com conjuntos de classes de lugares e de classes de transições.

Desta forma uma Rede de Petri Criptográfica - RPCT é uma quíntupla $RPCT = (P, T, I, O, M_0)$, onde:

P é um conjunto de três classes de lugares formado pelas seguintes classes: dos lugares convencionais das RP; dos lugares denominados de ”criptolugares”os quais serão depósitos de textos cifrados; e a classe de lugares inicializadores e finalizadores, os quais não possuem transições de entrada e de saída respectivamente;

T é um conjunto de classes de transições que abrange a classe dos convencionais das RP: a classe das cifradoras/decifradoras; as modulares que representam a compactação de blocos do modelo e o bloco das transições temporizadas;

$I \exists P \times T$ é um conjunto de funções de entrada (i.e. conjunto de arcos de entradas para as transições), que incluem arcos-inibidores e arcos-chaves.

$O \exists T \times P$ é um conjunto de funções de saída, ou seja um conjunto de arcos de saída para as transições;

$M \exists P \rightarrow NI$ é um conjunto de marcas, onde NI é um conjunto de inteiros não negativos.

5.4 Conclusão

Este capítulo teve por objetivo fazer uma breve descrição de alguns modelos de redes de petri. Foram apresentadas suas características e salientadas todas as suas qualidades para a descrição de modelos onde o sincronismo e controle de processos paralelos são importantes.

Receberam atenção também as extensões, que são novas características que podem ser adicionadas às redes quando se quer permitir fazer representações que não são definidas na Rede de Petri original.

Capítulo 6

Considerações Jurídicas Sobre Documentos Eletrônicos

6.1 Introdução

Este capítulo fará uma breve abordagem sobre os conceitos de documentos tradicionais e eletrônicos, citando as características de cada um e os requisitos para que obtenham validade jurídica. Trará também definições de assinatura convencional e assinatura digital, mostrando que a primeira é considerada uma forma de medida biométrica, enquanto que na assinatura digital o signatário usa um algoritmo para resumir a mensagem e em seguida utiliza a chave privada (que somente ele conhece), para cifrar o resumo, estabelecendo assim a assinatura digital.

Ressalte-se que estas abordagens estão sendo feitas tendo em vista que o processo de Emissão de Certidão de Nascimento através da Internet está baseado em procedimentos que se utilizam de assinatura digital e de documentos eletrônicos.

O presente capítulo está estruturado da seguinte forma: na seção 6.2 fala-se do documento tradicional e do documento eletrônico e a seção 6.3 descreve as diferenças entre a assinatura tradicional e a assinatura eletrônica.

6.2 Documentos Tradicionais e Documentos Eletrônicos

A expressão ”documento”sempre veio atrelada à idéia de um escrito oficial que identifica uma pessoa. *”No meio jurídico, representa um escrito que faz fé daquilo que atesta, de forma que se apresentado em juízo, prova o que o litigante alega”*[dFM].

> *”Documentos em geral, para serem legalmente válidos, precisam depender de confiança e credibilidade, que dependem de três características: a integridade, a genuinidade e a segurança. Para que seja autêntico, o documento não pode sofrer alterações, seja por erros humanos (involuntários ou intencionais), falhas técnicas, fatores externos ou fraudes, e precisa ser seguro. Um documento é seguro quando é difícil de alterá-lo. Essas características visam manter o documento autêntico, íntegro e confidencial.”[dFM]*

Com efeito, observa-se que a idéia de documento sempre esteve ligada à imagem de algo escrito, com a perfeita identificação da pessoa, ou no caso de um contrato, dos contratantes.

Com o advento da Internet e a sua rápida expansão pelo mundo, o conceito de documento teve que passar por uma adequação, de forma a se tornar viável a sua aplicação no meio virtual, tendendo a atualização deste conceito alcançar os mesmos objetivos já consolidados no meio tradicional. Dentro dessa nova conjuntura, surgiu então a conceituação do documento eletrônico, que mantém as principais características do documento tradicional, excetuando-se o meio no qual é celebrado e a questão pertinente à identificação da pessoa signatária.

> *”Documento eletrônico é, em termos singelos, aquele gerado por meio eletrônico, e que por esse mesmo meio pode ser arquivado, recuperado ou transmitido. Ele vem substituir o papel nas contratações realizadas por via eletrônica.”[COS b]*

A principal diferença entre o documento eletrônico e o tradicional, se dá no meio em que são celebrados, haja vista que, os documentos tradicionais representam-se por escritos em papéis, enquanto o documento eletrônico se representa por bits.

Verificado que um documento foi firmado em meio eletrônico, cumpre comprovar sua validade a fim de que se possa apurar sua segurança jurídica.

> *"Nesta apuração, para que um documento eletrônico tenha validade jurídica e possa servir, por si só, de meio probatório em juízo, faz-se mister a ocorrência de dois requisitos: impossibilidade de alteração do seu conteúdo e perfeita identificação das partes."[COS b]*

Duas abordagens que tratam do documento digital levando em consideração o aspecto jurídico, podem ser vistas em [COS a] e [JUN].

6.3 Assinaturas Digitais e Assinaturas Convencionais

A assinatura convencional é facilmente verificada no documento convencional, pois o autor, ao assinar o documento de forma a autenticálo, o faz em algo tangível, o papel, sendo este a entidade física de ligação entre a informação impressa e a assinatura. A assinatura manuscrita é considerada uma forma de medida biométrica indireta, pois imprime no papel uma escrita que tem dependência das biocaracterísticas de uma pessoa.

Uma definição para a assinatura convencional pode ser *"ato físico por meio do qual alguém coloca em um suporte físico a sua marca ou sinal. A marca é personalíssima e tem eficácia e validade jurídica, podendo ser levada ao tabelião para que este faça o seu reconhecimento por semelhança, já que pode ser conservada em arquivos e periciada por meios grafológicos"* [BRA c].

Em documentos eletrônicos não existe um meio físico que estabeleça a ligação entre o documento e a pessoa que assina a informação. A assinatura digital é uma aplicação da técnica de criptografia assimétrica, que envolve o uso de um par de

chaves: chave privada, a qual serve para assinar e a chave pública, utilizada para verificar a assinatura do documento.

> *"Ela consiste em duas etapas: inicialmente o signatário utiliza um algoritmo para realizar a operação de resumo dos dados do documento, chamada função resumo. Em seguida a chave privada é empregada na cifragem desse resumo. Como somente o signatário conhece a chave privada, conseqüentemente somente ele pode realizar esta operação. Isto garante a assinatura digital"[STI 95].*

> *"O algoritmo da função resumo deve satisfazer algumas características de implementação: direção única onde dado o resumo da mensagem, seja computacionalmente impossível encontrar a mensagem de origem; forte resistência à colisão, de forma a ser impraticável encontrar duas mensagens diferentes com o mesmo resumo e finalmente fraca resistência a colisão, que deve garantir que seja impossível encontrar um par de mensagens tal que o resumo seja igual. Dessa forma a geração do resumo, garante a integridade do documento"[STA 99].*

Devido ao resumo ser totalmente dependente dos dados do documento, cada assinatura é diferente para cada arquivo, diferentemente da assinatura real, que são apostas da mesma forma em documentos papéis.

O destinatário ao receber o documento, obtém a chave pública do signatário para verificar a autenticidade da assinatura, decifrando o resumo com esta.

Em seguida aplica a mesma função resumo no documento recebido e compara os dois resumos. Se o resultado obtido for igual, o documento é autêntico e confiável.

A assinatura digital garante a integridade do documento, pois se ocorrer qualquer alteração, por menor que seja, a assinatura não será verificada; essa é uma vantagem apresentada sobre a assinatura escrita, uma vez que depois de assinado no papel, podese alterar o documento sem que isso afete a assinatura.

Porém, a assinatura escrita autêntica garante a presença física do dono, enquanto a assinatura digital apenas indica que a chave privada foi utilizada, não tendo meios de garantir que o tenha sido efetuado pelo proprietário da chave.

Abordagens muito interessantes sobre validade jurídica de assinaturas digitais, podem ser vistas em [dCF], duas visões divergentes entre si [FER] e [BRA c], e outros artigos que também tratam deste assunto [dR], [dFM].

6.4 Conclusão

Neste capítulo foram apresentadas definições de documentos tradicionais e documentos eletrônicos, mostrando as características de cada um.

O documento tradicional está atrelado à idéia do escrito ligado ao papel. Já o documento eletrônico é representado por bits. De maneira geral, para ser considerado legalmente válido, o documento depende de requisitos como autenticidade e integridade.

No documento tradicional a assinatura que é uma marca personalíssima de quem assina, usa o papel como meio de ligação entre a informação e quem a gerou, ou a quem é imputada a autoria.

Por outro lado, no documento eletrônico a assinatura é uma aplicação da técnica de criptografia assimétrica, a qual envolve o uso de um par de chaves: privada que serve para assinar, e pública que serve para verificar a assinatura do documento.

Capítulo 7

Protocolo ECN

No capítulo 2 foi descrito o processo de registro de nascimento. Levando-se em consideração que o objetivo principal deste trabalho é propor um protocolo seguro para emissão de certidão de nascimento através da internet, neste capítulo serão apresentados os modelos propostos para a informatização do processo.

Para que este protocolo evite uma mudança muito grande de forma abrupta, propõe-se que o mesmo seja implementado em três fases, sendo que para cada fase é proposto um modelo. Os modelos são apresentados nas seções 7.5, 7.6 e 7.7.

A apresentação destes modelos é importante para o entendimento dos passos do protocolo e para compreensão do que irá mudar no processo de registro de nascimentos em cada uma das propostas.

O protocolo ECN, num primeiro momento, será um protocolo dividido em duas etapas bem distintas: etapa 1) o registro por parte de um Agente Autorizado (descrito na subseção 7.4.2); etapa 2) a liberação dos registros por parte do Cartorário (descrito na subseção 7.4.3). Num segundo momento, a segunda etapa é eliminada.

Neste capítulo apresentam-se: os modelos propostos para a emissão da certidão de nascimento através da Internet e os benefícios pretendidos com cada um deles. Apresentam-se também todos os passos do protocolo ECN e caracterizam-se as entidades envolvidas.

O capítulo está estruturado da seguinte forma: na seção 7.1 é feita uma

análise do modelo atual, para levantamento dos requisitos necessários para a informatização; na seção 7.2 são apresentados os requisitos do projeto de um sistema baseado no ECN, isto é, situações que precisam ser satisfeitas, para que o processo possa ser implementado; na seção 7.3 é dada a descrição do que é a central de registros, que será o principal elemento para o funcionamento do protocolo; na seção 7.4 são demonstrados os passos do protocolo ECN; na subseção 7.4.2 é apresentado o protocolo de registro do agente autorizado; na subseção 7.4.3 é apresentado o protocolo de liberação do cartorário; nas seções 7.5, 7.6 e 7.7 são apresentadas as propostas para informatização da emissão de certidão de nascimento.

7.1 Análise do Processo de Registro de Nascimentos

Analisando o processo de registro de nascimentos, é fácil observar que o destino final das informações que constam em uma DN, emitida pelo Agente Autorizado, é o Cartorário. A única função a ser exercida pelo Responsável pelo Registro é a de transportar o documento do Agente Autorizado até para o Cartorário, Num processo informatizado, esse transporte físico tende a ser desnecessário.

As informações que chegam ao Cartorário são transcritas para o livro de Registro Civil, que é um banco de dados textual onde são arquivadas as informações sobre as pessoas.

É dever do Cartorário somente aceitar as DNs procedentes de pessoas autorizadas. Desta maneira o sistema tem que prover ao Cartorário um mecanismo que lhe permita definir as pessoas habilitadas a enviar informações para serem gravadas.

Há também a necessidade de que um processo informatizado de registro de nascimento:

1. permita que o cartorário defina as pessoas que podem ou não efetuar registros;
2. permita que um agente autorizado efetue os registros;
3. permita que o cartorário recupere os registros efetuados pelos agentes autorizados.

7.2 Requisitos do Projeto

A seguir serão apresentados os requisitos que devem ser atendidos para que estas propostas possam ser implantadas com sucesso:

1. Permissão para que uma outra autoridade competente, que não apenas o Cartorário, possa efetuar registros;
2. Aceitação de que documentos digitais armazenados tenham mesmo valor jurídico de documentos tradicionais;
3. Validação legal de informações enviadas por meio digital;
4. Garantia de identificação das partes envolvidas;
5. Garantia de segurança na comunicação entre as partes, de privacidade, de integridade e do não-repúdio das informações.

Os requisitos 1, 2 e 3 são de ordem legal, necessitando de alterações na legislação para que as propostas possam ser implementadas.

As propostas apresentadas na seqüência pretendem atender os requisitos 4 e 5.

7.3 Central de registros

A Central de Registro - CR será uma aplicação disponível na Internet, tendo a função de executar as principais tarefas do sistema de registro de nascimentos.

A CR ficará sob responsabilidade do cartorário, que irá gerenciar o sistema e controlar o acesso, permitindo que apenas pessoas autorizadas consigam efetuar os registros de nascimentos.

Esta aplicação será o cérebro do sistema, o sincronismo e o bom funcionamento de todo o processo dependerão do bom funcionamento da CR.

Será responsabilidade da CR:

1. receber os registros dos Agentes Autorizados, verificar a validade das informações e garantir data e hora dos registros.
2. efetuar a liberação com autorização do Cartorário, verificar a validade das informações e garantir data e hora das liberações.
3. armazenar todas a informações, registros e liberações, de maneira segura e confiável, garantindo sempre a integridade das informações armazenadas.
4. garantir o acesso ao sistema apenas para pessoas autorizadas.

7.4 Descrição dos Passos para efetuar os registros

O processo para o registro de nascimento via Internet é dividido em duas partes:

1. a solicitação do registro por parte do Agente Autorizado;
2. a fé pública por parte do Cartorário.

Para o perfeito funcionamento do sistema serão definidos os protocolos para registro por parte do Agente Autorizado e a aceitação por parte do Cartorário. Estes protocolos serão utilizados nos modelos apresentados nas seções 7.5, 7.6 e 7.7.

Passaremos a expor tais protocolos a seguir:

7.4.1 Notação para definição dos passos para o registro de documentos

Foi utilizada a seguinte notação para a especificação do ECN:

7.4.2 Protocolo para Registro de Documento por Parte do Agente Autorizado

Num primeiro momento, será efetuado o registro da documentação pelo Agente Autorizado. Este registro, que contém os dados de uma criança recém-nascida, é

Tabela 7.1: Notação utilizada para especificação do ECN.

Símbolo	**Siginificado**
$\rightarrow$	Direção da Mensagem
$\triangleright$	Produz
$\|\|$	Concatenação
X	Texto Aberto
Y	Texto Cifrado
A	Assina
E	Cifra
D	Decifra
K	Chave
i	Membros A or B
KU_i	Chave Pública de i
KR_i	Chave Privada de i
M	Mensagem

enviado para a Central de Registros. O protocolo básico para efetuar tal registro compreende os seguintes passos:

1. um Agente Autorizado A que possui um certificado digital que o habilita a fazer o registro de nascimento, acessa através da Internet a Central de Registros B. Assim que é efetuado este contato, o certificado digital é apresentado.

2. a Central de Registros verifica na LCR se o certificado é válido;

3. caso tenha ocorrido algum erro ou o certificado apresentado não seja válido, a Central de Registros retorna uma mensagem de erro para a aplicação do Agente Autorizado e encerra o processo. Uma mensagem para ser dada seqüência no processo retorna ao Agente Autorizado caso o certificado seja válido e nenhum erro tenha ocorrido;

4. o Agente Autorizado envia os dados da DN e a cópia digitalizada e assinada dos documentos dos pais ou seja:

   $M = A_{KR_A}(DN + DG)$

   $A \rightarrow B : E_{KU_B}(E_{KR_A}(M))$, onde DG é cópia digitalizada dos documentos dos pais;

5. a Central de Registros assina e grava no Banco de Dados os documentos recebidos;

6. a Central de Registros assina e retorna cópia do documento recebido, assinado digitalmente, comprovando que foi feita a declaração pelo agente autorizado. A Mensagem será o documento enviado pelo agente autorizado, assinado também pela Central de Registros.

   $M = A_{KR_B}(DE)$

   $B \rightarrow A : E_{KU_A}(E_{KR_B}(M))$, onde DE = documentos enviados pelo Agente Autorizado.

7.4.3 Protocolo para aceitação de um documento por parte do Cartorário

Um outro processo necessário para a informatização dos registros de nascimento via Internet é a assinatura dos registros pelo cartorário. Após os dados terem sido registrados pelo agente autorizado, há a necessidade de que os mesmos sejam validados pelo cartorário. Devido à necessidade da definição de um protocolo que demonstre os passos necessários para a liberação, por parte do cartorário A, dos documentos existentes na Central de Registros B, os passos para efetuar este processo são os seguintes:

1. o Cartorário acessa a Central de Registros, apresentando o seu Certificado Digital;

2. a Central de Registros entra em contato com a AC que emitiu o certificado para verificar se houve alteração na LCR;

3. caso tenha ocorrido alterações na LCR, a AC envia cópia da nova LCR para a Central de Registros. Caso ocorra algum erro ou o certificado não seja mais válido, o sistema retorna uma mensagem de erro ao cartorário;

4. o Sistema irá recuperar todos os documentos R que sejam referentes ao cartorário que está acessando o sistema, e irá marcar que os enviou para o cartorário guardando os dados do certificado digital para quem ele enviou a informação;

5. o sistema envia para o cartorário todos o seus registros pendentes;

   $M = A_{KR_B}(Doc[1]) + A_{KR_B}(Doc[2]) + ... + A_{KR_B}(Doc[n])$

   $B \rightarrow A : E_{KU_A}(E_{KR_B}(M))$

6. o Cartorário assina digitalmente todos os documentos recebidos da Central de Registros, montando uma mensagem onde serão listados todos os documentos liberados;

   $M = A_{KR_A}(Doc[1]) + A_{KR_A}(Doc[2]) + ... + A_{KR_A}(Doc[n])$

   $A \rightarrow B : E_{KU_B}(E_{KR_A}(M))$

7. a central de registros recebe os documentos assinados pelo cartorário, os quais são conferidos e novamente armazenados;

8. a central de registros retorna ao cartorário todos os documentos registrados, montando uma mensagem na qual constará a confirmação de todos os documentos liberados.

   $M = A_{KR_B}(Doc[1]) + A_{KR_B}(Doc[2]) + ... + A_{KR_B}(Doc[n])$

   $B \rightarrow A : E_{KU_A}(E_{KR_B}(M))$

7.5 Proposta seguindo o modelo atual

A presente proposta tem por objetivo otimizar o processo atual de registro de nascimentos. Exemplifica o processo automatizado sem causar um impacto muito grande, demonstrando que a informatização é possível e pode trazer muitos benefícios, porém necessita de alterações na forma de execução de algumas tarefas.

Tendo em vista os benefícios possíveis oriundos da implementação da informatização do processo de registro de nascimentos, é desejável que todo o processo seja efetivamente colocado em prática o mais breve possível. Para isto, propomos uma implementação que aproveite a estrutura do atual modelo tanto quanto possível.

A figura 7.1 demonstra como será o processo.

Os passos de 1 até 7 seguem os do protocolo do Agente Autorizado. Após isto, a primeira etapa, que é a gravação por parte do Agente Autorizado, está encerrada, sendo que a continuidade do processo dependerá agora do cartorário. Os passos de 8 a 14 seguem o modelo do protocolo apresentado para o registro por parte do Cartorário. Após terminado o registro eletrônico os passos seguintes serão:

16) o Cartorário registra no livro de registro civil, descrito no capítulo 2, os dados da certidão de nascimento;

17) a certidão é enviada para o agente responsável, para que possa ser entregue aos pais da criança.

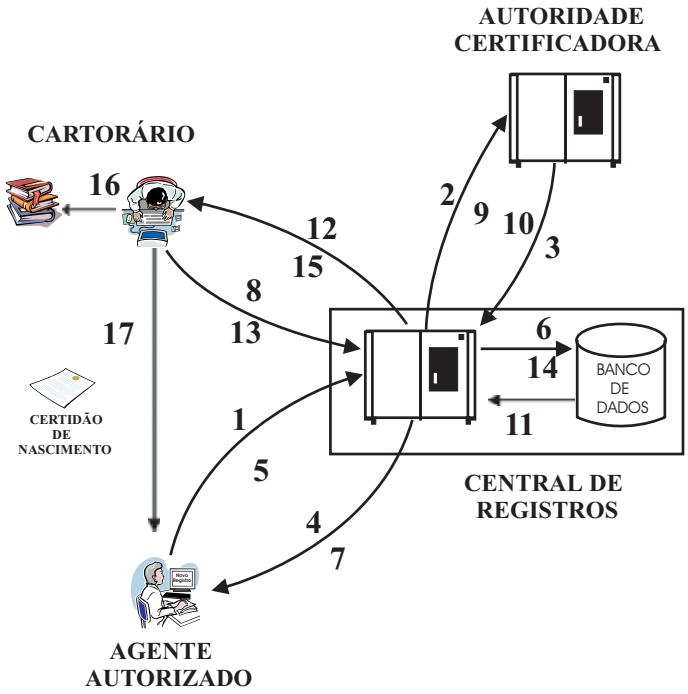

Figura 7.1: Modelo de registro de nascimentos melhorada. Os passos de 1 até 7 seguem os do protocolo do Agente Autorizado. Após isto, a primeira etapa, que é a gravação por parte do Agente Autorizado, está encerrada, sendo que a continuidade do processo dependerá agora do cartorário. Os passos de 8 a 14 seguem o modelo do protocolo apresentado para o registro por parte do Cartorário. Após isto o registro eletrônico está encerrado, e o próximos passos são: 16) o Cartorário registra no livro os dados da certidão de nascimento; 17) a certidão é enviada para o Agente Autorizado, para que possa ser entregue aos pais da criança.

7.5.1 Características

1. O modelo é capaz de agilizar o processo sem mexer na estrutura existente, por se basear no modelo atual. Não se tornam necessárias mudanças profundas;

2. exemplifica o processo automatizado sem causar muito impacto: por ser quase idêntico ao modelo atual, irá trazer benefícios, sem porém causar estranheza nas pessoas que farão uso dele;

3. pode ser colocado em prática rapidamente, devido às duas características acima;

4. atende aos itens 4 e 5 dos requisitos de projeto;

5. necessita de alterações na legislação para atender os itens 1,2 e 3 dos requisitos de

projeto;

7.5.2 Vantagens em relação ao sistema atual

Dentre os vários benefícios aos envolvidos no processo de registro de nascimento, dois parecem-nos primordiais:

1. elimina a necessidade do deslocamento do responsável até o cartório;

2. certeza de que o registro de nascimento será efetuado, caso a DN seja enviada.

7.6 Proposta com um banco de dados em substituição ao Livro de Registro

Faz parte da implementação do sistema informatizado de registro de nascimentos a substituição do livro físico de registro por um banco de dados conforme mostra a figura 7.2. Nesta figura os passos de 1 até 7 seguem o protocolo do Agente Autorizado.

Após o registro por parte do agente Autorizado, a primeira parte do processo está encerrada, sendo que a continuidade do processo dependerá então do cartorário. Os passos de 8 a 14 seguem o modelo do protocolo apresentado para o registro por parte do cartorário. Em seguida (passo 15) o Cartorário imprime as certidões e as envia ao Agente Autorizado (passo 16), para que as confira e entregue aos pais da criança.

7.6.1 Características

As principais características deste modelo são:

1. a substituição do Livro de Registro por um Banco de Dados Digital que é mais seguro, prático e confiável;

2. atende aos ítens 4 e 5 dos requisitos de projeto;

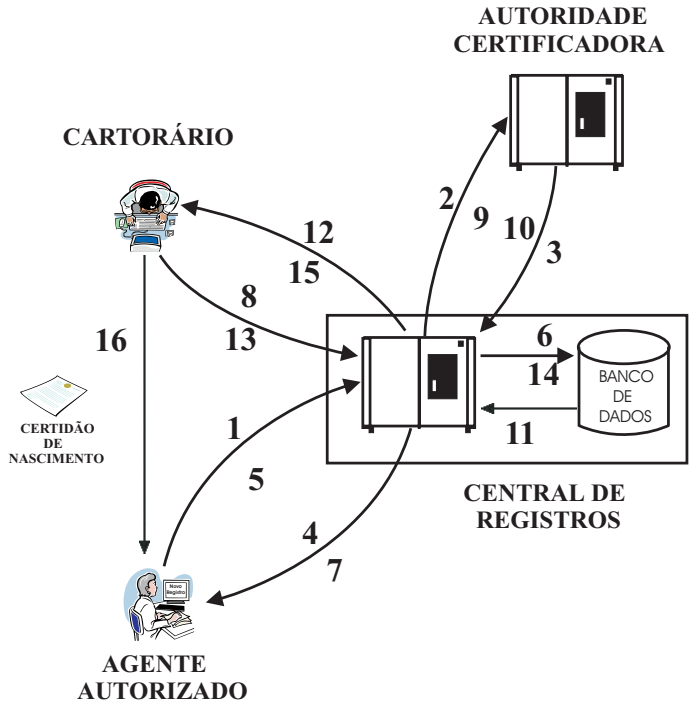

Figura 7.2: Proposta de registro de nascimentos com o uso de um banco de dados em substituição ao livro de registros. Os passos de 1 até 7 seguem o protocolo do Agente Autorizado, Após estes passos, a primeira parte do processo, a da gravação por parte do Agente Autorizado, está encerrada, sendo que a continuidade do processo dependerá então do cartorário. Os passos de 8 a 14 seguem o modelo do protocolo apresentado para o registro por parte do cartorário. Em seguida (passo 15) o Cartorário imprime as certidões, e as envia ao Agente Autorizado (passo 16).

3. necessidade de alterações na legislação para atender os itens 1, 2 e 3 dos requisitos de projeto.

7.6.2 Vantagens em Relação ao Modelo Atual

Há diversos benefícios quando da efetivação da armazenagem de informações no meio digital:

1. eliminação de arquivos com documentos impressos, que ocupam muito espaço físico e dificultam a localização de informações específicas;

2. maior facilidade na obtenção de informações;

3. possibilidade de implantação de funções para a identificação pessoal, com o armazenamento de características biométricas [BOL 00];

4. com a implementação de funções para a identificação pessoal, possibilidade de controle dos registros de tal forma que não ocorra duplicidade de registro de um mesmo nascimento.

7.7 Proposta com um banco de dados e emissão da certidão *on-line*

Apesar da proposta com o banco de dados agilizar muito o processo de registro de nascimento em relação ao modelo atual, ainda não atinge todos os objetivos almejados, pois a legalização da certidão de nascimento ainda fica na dependência da assinatura do cartorário. O sistema que realmente nos interessa é um no qual quando do nascimento, a criança seja registrada automaticamente, e que os pais possam receber imediatamente a certidão de nascimento.

Esta terceira proposta tem por objetivo automatizar de forma definitiva o processo de registro de nascimento. Assim o cartorário só executa o papel de guardião do sistema e das informações. O registro por parte do Agente Autorizado se torna definitivo. No momento em que se efetua o registro, o Agente Autorizado já recebe um documento válido como uma certidão de nascimento.

A figura 7.3 representa como ficaria o processo. Pode-se notar na figura que a única pessoa envolvida no registro é o Agente Autorizado.

Os passos de 1 a 7 seguem o protocolo de registro por parte do Agente Autorizado. A grande diferença, com relação ao modelo anterior, é que o retorno do sistema para o Agente Autorizado já é uma certidão de nascimento válida.

Neste caso, não existe a necessidade dos registros serem assinados digitalmente pelo cartorário. O próprio sistema será encarregado de efetuar esta assinatura. A função do Cartorário é manter o funcionamento do sistema, controlando quem pode registrar ou não o nascimento.

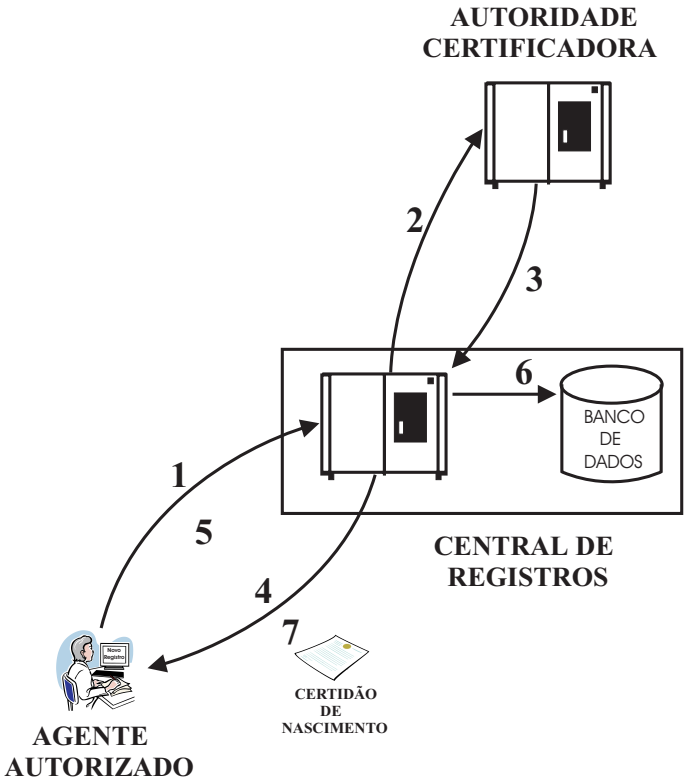

Figura 7.3: Proposta de registro de nascimento com emissão da Certidão de Nascimento on-line. Os passos de 1 a 7 seguem o protocolo de registro por parte do Agente Autorizado. Neste caso, não existe a necessidade dos registros serem assinados digitalmente pelo cartorário. O próprio sistema será encarregado de efetuar esta assinatura. A função do Cartorário é a de manter o funcionamento do sistema, controlando quem pode registrar ou não o nascimento.

7.7.1 Características

Algumas características do processo apresentado, já em sua forma definitiva são:

1. a certidão é emitida no ato do nascimento da criança, sem necessidade que outra pessoa além do Agente Autorizado precise passar informações ao sistema;

2. atende aos itens 4 e 5 dos requisitos de projeto;

3. necessita de alterações na legislação para atender os itens 1, 2 e 3 dos requisitos de projeto.

7.7.2 Vantagens em relação ao sistema atual

Além de agrupar as vantagens das propostas anteriores, esta proposta apresenta as seguintes vantagens:

1. permite que a certidão de nascimento seja emitida no ato do nascimento da criança;
2. não é necessário nenhum tipo de deslocamento por parte do responsável para se efetuar o registro.

7.8 Conclusão

Este capítulo teve por objetivo apresentar as três propostas que serão utilizadas para a informatização do processo de registro de nascimentos. Preocupa-se em apresentar as propostas de forma que a informatização seja suave e gradativa com o uso de modelos subseqüentes que agregam novas características ao modelo anterior, permitindo o adequado aculturamento das entidades envolvidas.

Estes processos gradativos visam definir parâmetros para que se possam criar leis que permitam legalizar o registro através da Internet sem, contudo, criar mudanças drásticas que trariam transtornos ao modelo atual.

Capítulo 8

Formalização do Protocolo ECN

8.1 Introdução

Neste capítulo, são apresentadas as Redes de Petri, que representam o protocolo dos modelos propostos no capítulo 7. Estas representações têm por objetivo facilitar o estudo dos passos do protocolo, para análise detalhada na busca de possíveis falhas.

Para as representação do protocolo ECN, foram usadas apenas Redes de Petri ordinárias, as quais se mostram suficientes para demonstrar os passos do protocolo de maneira satisfatória.

A representação em Redes de Petri mostrou-se extremamente eficaz e permitiu que cada etapa do protocolo fosse estudada individualmente. Deste modo foi possível uma análise do protocolo.

Devido ao fato do Protocolo ECN possuir 3 modelos com duas variações, serão apresentadas duas redes, uma que satisfaz o protocolo usado nos modelos propostos nas seções 7.5 e 7.6, e uma segunda rede que representa a proposta da seção 7.7.

Apesar do estudo do protocolo ECN através de Redes de Petri ter sido de extrema importância na análise dos passos do protocolo, este não consegue comprovar os requisitos de segurança do protocolo. Para complementar a análise foi inserida uma seção onde se discute apenas os requisitos de segurança do protocolo, e quão seguro este

é.

Este capítulo está estruturado desta forma: na seção 8.2 é apresentada a Rede de Petri que representa os dois primeiros modelos propostos no capítulo 7; na seção 8.3 é apresentada a Rede de Petri que representa o terceiro modelo proposto no capítulo 7; finalmente na seção 8.5 são analisados os requisitos de segurança do protocolo, e qual o seu comportamento perante aos principais tipos de ataque.

8.2 Rede usada para representar as duas primeiras propostas

A rede apresentada na figura 8.1 representa o modelo do protocolo que atende as necessidades das duas primeiras propostas para emissão de registro de nascimentos através da Internet. A grande diferença entre as propostas está na atuação da Central de Registros: na primeira proposta, a Central de Registros assume um papel de arquivo temporário das certidões de nascimentos que são enviadas da maternidade para o Cartório; já na segunda, a Central de Registros tem a função de banco de registros, devendo manter as certidões armazenadas em um Banco de Dados, que passa a ser permanente.

A rede da figura 8.1 foi dividida em 5 partes básicas:

Agente Autorizado : As transições demonstradas nesta parte da rede indicam as operações que ocorrem na máquina do Agente Autorizado, quando este vai enviar uma nova certidão para ser registrada;

Central de Registros : As transições demonstradas nesta parte da rede indicam as operações que ocorrem na Central de Registros. As transições TCR01 e TCR02 ocorrem quando está sendo efetuado o registro por parte do Agente Autorizado. As transições TCR03, TCR04 e TCR05 ocorrem quando está sendo efetuada a liberação por parte do Cartorário;

Cartorário : As transições demonstradas nesta parte da rede indicam as operações que ocorrem na máquina do Cartorário, quando este vai efetuar a liberação dos registros;

Comunicação entre Agente Autorizado e Central de Registros: Indica a comunicação entre o Cartorário e a Central de Registros, quando o primeiro vai efetuar a liberação dos registros. Estas transições foram colocadas para que se pudesse estudar os problemas que podem ocorrer na transmissão das informações.

Uma observação a ser feita, é que para o disparo das transições na Central de Registros, no Agente Autorizado e no Cartorário é necessário o conhecimento da chave privada da origem e a chave pública do destino. Estas chaves foram representadas como lugares, porém estes lugares foram omitidos no desenho da rede, mas foram listados na descrição.

Os lugares da rede são definidos por:

No Agente Autorizado:

PR01 - Máquina do Agente Autorizado liberada para o registro. Indica que a máquina do Agente Autorizado está apta a efetuar um novo registro de nascimento. A inexistência de ficha indica que está sendo efetuado um registro de nascimento e não é possível começar um outro.

PR02 - Chave Privada do Agente Autorizado

PR03 - Chave Pública da Central de Registros

PR04 - Certidão a ser registrada. Indica que existe uma nova certidão a ser registrada.

PR00 - Contador de erros na tentativa de registro pelo Agente Autorizado. Para garantir que não existem problemas de comunicação entre o Agente Autorizado e a Central de Registros foi criado um contador de erros. Caso tenha ocorrido problemas um número pré-determinado de vezes no registro de uma mesma certidão o sistema entrará em um estado de espera e emite uma mensagem de alerta.

PR05 - Documento que está sendo registrado pelo Agente Autorizado que já passou da primeira fase e aguarda resposta. Após a primeira fase do processo de registro será armazenada no Agente Autorizado uma cópia do documento que foi enviado para registro, para conferência no retorno dos dados.

PR06 - Chave Privada do Agente Autorizado. [1]

PR07 - Chave Pública da Central de Registros.

PR08 - Documentos registrados pelo Agente Autorizado. Após o envio da Certidão por parte do Agente Autorizado, a Central de Registro manda uma resposta confirmando os dados do documento. Com a confirmação o Agente Autorizado coloca num depósito as certidões registradas.

No Cartorário:

PC01 - Máquina do cartório liberada para registro. Indica que o sistema do Cartorário está apto a efetuar um novo registro de nascimento.

PC02 - Chave Privada do cartorário.

PC03 - Chave Pública da Central de Registros.

PC04 - Chave privada do Cartorário.

PC05 - Pedido dos documentos para liberação por parte do Cartorário. O primeiro processo para liberação por parte do cartorário é o processo de pedido das certidões a serem liberadas quando é feita esta requisição. É gerado um documento informando que a requisição foi feita.

PC06 - Chave Pública da Central de Registros.

PC07 - Chave Privada do Cartorário.

[1] No desenho da rede, para ficar mais claro, as chaves foram suprimidas, porém assume-se que a Central de Registros conheça a chave pública do Agente Autorizado e vice-versa e a Central de Registros conhece a chave pública do Cartorário e vice-versa

PC08 - Chave Pública da Central de Registros.

PC09 - Documentos recebidos da Central de Registros para serem liberados. Após o pedido por parte do Cartorário, a Central de Registros envia todos os documentos que o Cartorário possui para serem liberados. O Cartorário receberá todos o documentos que tem que liberar.

TC02 - Elemento que irá verificar e liberar os documentos e enviará a resposta da liberação para a central de registros; os documentos que são assinados (liberados ou não) ficam arquivados no Cartório para confirmação.

PC10 - Documentos Liberados.

Na Central de Registros:

PCR01 - Central de Registros liberada para receber registros do Agente Autorizado. Indica que a central de registros está liberada para efetuar novos registros de nascimento por parte do Agente Autorizado.

PCR02 - Chave Privada da Central de Registros

PCR03 - Chave Pública do Agente Autorizado.

PCR00 - Central de Registros pode receber novos registros por parte do Agente Autorizado. Este é um objeto contador, que serve para a central de registros verificar se não possui um número excessivo de certidões a serem liberadas.

PCR05 - Chave Privada de Central de Registros.

PCR06 - Documentos que foram enviados pelo Agente Autorizado e esperam confirmação. Após o envio dos documentos por parte do Agente Autorizado a Central de registros gera uma resposta para verificar se os dados recebidos estão corretos.

PCR07 - Chave Pública do Agente Autorizado.

PCR08 - Documentos que foram enviados pelo Agente Autorizado e esperam liberação por parte do Cartorário. Após verificação dos dados por parte do Agente Autorizado os documentos ficam armazenados temporariamente, esperando liberação por parte do cartorário.

PCR09 - Chave privada da Central de Registros.

PCR10 - Chave Pública do Cartorário.

PCR11 - Chave Privada do Cartorário.

PCR12 - Documentos que estão sendo liberados pelo cartorário e esperam liberação. Para efetuar a liberação dos documentos, a Central de Registros após o pedido do Cartorário, envia todos os documentos ao Cartorário e guarda uma cópia dos documentos enviados para um confirmação posterior.

PCR13 - Chave pública do Cartorário.

PCR14 - Chave privada da Central de Registros.

PCR15 - Documentos que estão sendo liberados pelo cartorário e aguardam confirmação. Após os documentos recebidos pelo cartorário terem sido confirmados a central gera uma nova cópia que ficará aguardando os documentos assinados pelo Cartorário.

PCR16 - Chave pública do Cartorário.

PCR17 - Depósito de documentos que foram armazenados e liberados. Depois de confirmados e assinados os documentos liberados ficam armazenados na central de Registros. Neste armazenamento é que se constata a diferença entre a proposta 1 e a proposta 2. Na proposta 1 os documentos ficam armazenados apenas para efeito de controle por parte da Central de Registros. Na proposta 2, os documentos ficarão armazenados de forma definitiva, ficando inclusive disponíveis para consultas externas quando for necessário.

Na comunicação entre o Agente Autorizado e a Central de Registros:

PA01 - Documento enviado do Agente Autorizado para a Central de Registros.

PA02 - Confirmação dos documentos enviados pelo Agente Autorizado e que foram Recebidos pela Central de Registros.

PA03 - Documentos que foram enviados pelo Agente Autorizado e recebidos pela Central de Registros e foram confirmado pelo Agente Autorizado.

Na comunicação entra a Central de Registros e o Cartorário:

PB01 - Pedido de envio dos documentos a serem liberados pelo Cartorário à Central de Registros.

PB02 - Documentos a serem liberados pelo Cartorário enviados pela Central de Registros.

PB03 Confirmação por parte do Cartorário dos documentos recebidos da Central de Registros.

PB04 - Documentos confirmados pela Central de Registros.

PB05 - Documentos assinados pelo Cartorário e enviados para a Central de Registros.

As transições da rede são definidas por:

No Agente Autorizado:

TR01 - Processo de início do registro por parte do Agente Autorizado. É o processo que começa o registro de nascimento, é executado regularmente num determinado período de tempo, mesmo que não existam certidões a serem registradas, para não permitir que um atacante que tenha conseguido descobrir a chave privada do Agente Autorizado consiga registrar certidões falsas. A restrição para este processo é não mandar uma segunda certidão enquanto uma outra certidão esteja sendo registrada.

O sistema do Agente Autorizado deverá conhecer a chave pública da Central de Registros. O documento a ser enviado deve ser assinado com a chave privada do Agente Autorizado e cifrado com a chave pública da Central de Registros, para garantir que o seu conteúdo não seja conhecido, e nem a autoria do documento.

TR02 - Processo de confirmação do Registro por parte do Agente Autorizado. Este é o processo que irá checar se um documento que está sendo registrado na Central de Registros é idêntico ao documento enviado pelo Agente Autorizado para ser registrado. Ele irá guardar os documentos confirmados num depósito interno do Agente Autorizado que armazenará os documentos registrados.

Na comunicação entre o Agente Autorizado e a Central de Registros:

TA01, TA02, TA03 - Erro na transmissão de documentos entre a Central de Registros e o Agente Autorizado. Estes processos são os que checam os erros na transmissão entre a Central de Registros e o Agente Autorizado. Caso ocorra algum problema, entram em ação encerrando o processo e reinicializando a Central de Registros e o Agente Autorizado para que possam efetuar um novo registro.

Na Central de Registros

TCR01 - Recebimento dos documentos a serem registrados, enviados pelo Agente Autorizado, e confirmação dos registros recebidos. Este processo é o processo de entrada do documento na Central de Registros e é ele que vai checar todos os dados do documento e verificar se o emissor do documento tem autorização para fazê-lo. Ele conhece a chave pública do emissor (no caso, o Agente Autorizado pelo registro) e a chave privada da Central de Registros. Caso o documento esteja dentro dos padrões e a pessoa que o enviou tenha autorização para fazê-lo, o processo irá criar um documento que espera a confirmação e irá definir a máquina como ocupada e mandar uma mensagem ao emissor com os dados do documento enviado.

TCR02 - Recebimento da confirmação dos documentos enviados pelo Agente Autorizado. Este processo tem um documento de espera que foi o documento recebido no processo $TCR01$. É a confirmação do documento por parte do emissor (Agente

Autorizado). Ele irá colocar o documento no banco temporário que irá armazenar os documentos até que o Cartorário os libere.

TCR03 - Recebimento do pedido do Cartorário e envio dos documentos para serem liberados. Este processo irá mandar os documentos para o cartorário fazer a liberação. Só é disparado mediante pedido do cartorário, ele manda os documentos enviados pelo Agente Autorizado para o Cartorário para que o mesmo efetue a liberação, e diz qual os documentos enviados.

TCR04 - Recebimento dos documentos liberados pelo Cartorário e envio do pedido de confirmação. Conhecendo os documentos que foram enviados para liberação por parte do cartorário, este processo faz a verificação dos documentos que o Cartorário está enviando. Caso os documentos estejam corretos, manda uma resposta ao Cartorário e cria um outro armazenamento temporário que irá aguardar a confirmação por parte do Cartorário.

TCR05 - Recebimento e Armazenamento dos documentos liberados pelo Cartorário. Último processo para registro da certidão de nascimento. Este processo recebe os dados de resposta do Cartorário e encerra todo o processo, liberando as máquinas para que possam efetuar novos registros. Neste ponto é criado um depósito, que terá versões diferentes para os dois modelos. No modelo em que ainda existe o livro físico de registros, este depósito será apenas para fim de controle, no modelo em que o livro físico foi abolido, o depósito criado será um banco de dados que armazenará as certidões de nascimento.

Na comunicação entre a Central de Registros e o Cartorário:

TB01,TB02,TB03,TB04,TB05 - Erro na transmissão entra a Central de Registros e o Cartorário. Processos que ocorrem caso exista algum tipo de problema na transmissão dos dados da Central de Registros para o Cartorário. Quando um desse processos entram em ação tanto o Cartorário quanto a Central de Registros são liberados para começar de novo os processos.

No Cartorário:

TC01 - Começo da Liberação das Certidões por parte do Cartorário. Este é o processo que inicia a liberação das certidões de nascimento por parte do Cartorário, quando o Cartorário quiser efetuar a liberação os documentos, deve enviar uma requisição para a Central de Registros pedindo que todas as certidões lhe sejam enviadas.

TC02 - Recebimento das Certidões a serem liberadas por parte do Cartorário. Após o pedido o sistema ficará aguardando que a Central de Registros envie os documentos do Cartorário. A Central irá recuperar todos os documentos e os enviará junto com o pedido de liberação enviado pelo Cartorário. Este processo recebe os documentos enviados pela Central de Registros os assina e os envia de volta para que sejam confirmados e reconhecidos pela Central de Registros e cria uma cópia para conferência por parte da Central de Registros.

TC03 - Confirmação da liberação das certidões de nascimento por parte do Cartorário. Este processo irá verificar se todos os documentos estão corretos e irá encerrar o processo de liberação por parte do Cartorário, emitindo a relação de todas as certidões que foram verdadeiramente registradas.

8.3 Rede que representa a terceira proposta

Como a diferença básica entre a redes das três propostas é que na terceira proposta não existe a figura do cartorário, a RP se torna, portanto, simplificada conforme o modelo da figura 8.2, que foi dividida em 3 partes básicas:

Agente Autorizado : as transições demonstradas nesta parte da rede indicam as operações que ocorrem na máquina do Agente Autorizado, quando este vai enviar uma nova certidão para ser registrada;

Central de Registros : as transições demonstradas nesta parte da rede indicam as operações que ocorrem na Central de Registros;

Comunicação entre Agente Autorizado e Central de Registros : indica a comunicação entre o Agente Autorizado e a Central de Registros, quando é efetuado um novo re-

gistro. Estas transições foram colocadas para que se pudesse estudar os problemas que podem ocorrer na transmissão das informações.

Uma observação a ser feita, é que para o disparo das transições na Central de Registros e no Agente Autorizado é necessário o conhecimento da chave privada da origem e a chave pública do destino. Estas chaves foram representadas como lugares, estes lugares que foram omitidos no desenho da rede para facilitar a visualização. Contudo são listados na descrição.

Os lugares da rede são definidos por:

No Agente Autorizado:

PR01 - Máquina do Agente Autorizado liberada para o registro. Indica que a máquina do Agente Autorizado está apta a efetuar um novo registro de nascimento. A inexistência de ficha indica que está sendo efetuado um registro de nascimento e que no momento não é possível começar outro.

PR02 - Chave Privada do Agente Autorizado.

PR03 - Chave Pública da Central de Registros.

PR04 - Certidão a ser registrada. Indica que existe uma nova certidão a ser registrada.

PR00 - Contador de erros na tentativa de registro pelo Agente Autorizado. Para Garantir que não existem problemas de comunicação entre o Agente Autorizado e a Central de Registro, é criado um contador de erros. A ocorrência de problemas em um número pré-determinado de vezes no registro de uma mesma certidão, ocasiona uma paralisação momentânea do sistema.

PR05 - Documento que está sendo registrado pelo Agente Autorizado que já passou da primeira fase e aguarda resposta. Após o primeira fase do processo de registro será armazenada no Agente Autorizado uma cópia do documento que foi enviado para registro, para conferência quando do retorno dos dados.

PR06 - Chave Privada do Agente Autorizado.

PR07 - Chave Pública da Central de Registros.

PR08 - Documentos registrados pelo Agente Autorizado. Após o envio da certidão por parte do Agente Autorizado, a Central de Registro manda uma resposta confirmando os dados do documento. De posse da confirmação, o Agente Autorizado coloca as certidões registradas num depósito.

Na Central de Registros:

PCR01 - Central de Registros liberada para receber registros do Agente Autorizado. Indica que a central de registros está liberada para efetuar novos registros de nascimento por parte do Agente Autorizado.

PCR02 - Chave Privada da Central de Registros

PCR03 - Chave Pública do Agente Autorizado.

PCR00 - Central de Registros pode receber novos registros por parte do Agente Autorizado. Este é um objeto contador, que serve para a central de registros verificar se não possui um número excessivo de certidões a serem liberadas.

PCR05 - Chave Privada de Central de Registros.

PCR06 - Documentos que foram enviados pelo Agente Autorizado e esperam confirmação. Após o envio dos documentos por parte do Agente Autorizado, a Central de Registros gera uma resposta para verificar se os dados recebidos estão corretos.

PCR07 - Chave Pública do Agente Autorizado.

PCR08 - Certidões de Nascimento armazenadas.

Na comunicação entre o Agente Autorizado e a Central de Registros:

PA01 - Documento enviado do Agente Autorizado para a Central de Registros.

PA02 - Confirmação dos documentos enviados pelo Agente Autorizado e que foram Recebidos pela Central de Registros.

PA03 - Documentos que foram enviados pelo Agente Autorizado e recebidos pela Central de Registros e foram confirmado pelo Agente Autorizado.

As transições da rede são definidas por:

No Agente Autorizado:

TR01 - Processo de início do registro por parte do Agente Autorizado. Este é o processo que começa o registro de nascimento. Será executado regularmente num determinado período de tempo, mesmo que não existam nascimentos, para impedir que um atacante que tenha conseguido descobrir a chave privada do Agente Autorizado consiga registrar certidões falsas. A restrição para este processo é não mandar uma segunda certidão, enquanto um outro nascimento esteja sendo registrado. O sistema do Agente Autorizado deverá conhecer a chave pública da Central de Registros. O documento a ser enviado deve ser assinado com a chave privada do Agente Autorizado e cifrado com a chave pública da Central de Registros, para garantir que o seu conteúdo não seja conhecido, e nem a autoria do documento.

TR02 - Processo de confirmação do Registro por parte do Agente Autorizado. Este é o processo que irá checar se um documento que está sendo registrado na Central de Registros é idêntico ao documento enviado pelo Agente Autorizado para ser registrado. Ele irá guardar os documentos confirmados num depósito interno no Agente Autorizado.

Na comunicação entre o Agente Autorizado e a Central de Registros:

TA01, TA02, TA03 - Erro na transmissão de documentos entre a Central de Registros e o Agente Autorizado. Estes processos são os que checam os erros na transmissão entre a Central de Registros e o Agente Autorizado. Caso ocorra algum problema, encerram o processo e reinicializam a Central de Registros e o Agente Autorizado para que possam efetuar um novo registro.

Na Central de Registros

TCR01 - Recebimento dos documentos a serem registrados enviados pelo Agente Autorizado. e confirmação dos registros recebidos. É o processo de entrada do documento na Central de Registros, é ele que vai checar todos os dados do documento, e verificar se o emissor do documento tem autorização para fazê-lo. Ele conhece a chave pública do emissor (no caso, o Agente Autorizado pelo registro) e a chave privada da Central de Registros. Caso o documento esteja dentro dos padrões e a pessoa que o enviou tenha autorização para fazê-lo, o processo irá criar um documento que espera a confirmação, e irá definir a máquina como ocupada e mandar uma mensagem ao emissor com os dados do documento enviado.

TCR02 - Recebimento da confirmação dos documentos enviados pelo Agente Autorizado. Este processo tem um documento de espera que foi o documento recebido no processo TCR01. É a confirmação do documento por parte do emissor (Agente Autorizado); ele irá colocar o documento no banco de dados e emitir a certidão de nascimento.

8.4 Verificação do Protocolo

A verificação do protocolo consiste na análise dos requisitos de segurança em relação ao protocolo ECN, bem como a verificação do comportamento do protocolo diante de ataques maliciosos.

Assume-se como verdadeiras as seguintes hipóteses:

Hipótese 1 (Autoridade Certificadora) - Assume-se que a Autoridade Certificadora é um participante honesto.

Hipótese 2 (Protocolo SSL/TSL) - A comunicação em nível da camada de Transporte, através do protocolo SSL/TSL[SMI 97] , oferece comunicação confiável entre processos e provê os serviços de autenticação, confidencialidade e integridade.

Hipótese 3 (Central de Registros) - Assume-se que a Central de Registros seja um participante honesto. A sua implementação deve garantir mecanismos de auditoria para ser considerada honesta.

8.4.1 Confidencialidade

As mensagens trocadas são cifradas com a chave pública do destino - A troca de mensagens entre as entidades participante (Agente Autorizado, Central de Registros e Cartorário), são cifradas com a chave pública do destino [2].

Garantia de confidencialidade na comunicação - O protocolo SSL garante a confidencialidade nos canais de comunicação.

8.4.2 Autenticação

Apenas participantes autorizados podem ter acesso ao sistema - Através do protocolo SSL, com o uso de certificados digitais, é possível autenticar corretamente os participantes legítimos do sistema.

Autenticação do registro de nascimento - Todo registro é assinado pelo agente autorizado, portanto, são autenticados.

Autenticação da liberação do registro de nascimento - Todo Registro liberado pelo Cartorário é assinado, portanto, são autenticados.

8.4.3 Não-repúdio

O Agente Autorizado não pode negar que efetuou um registro - Como a Central de Registros é honesta (hipótese 3), e todo registro é assinado pelo agente autorizado, então o Agente Autorizado não pode negar que efetuou o registro.

[2] Durante todo o trabalho é citado o uso da chave pública do destino, para um melhor entendimento do processo, no entanto durante a implementação poderá ser utilizada uma chave de seção simétrica, negociada a cada troca de mensagem

O Cartorário não pode negar que liberou um registro - Como a Central de registros é honesta (hipótese 3), e todo registro liberado pelo cartorário é assinado então o Cartorário não pode negar que liberou o registro.

8.4.4 Unicidade

Emissão de apenas um certificado por participante - A Central de Registros, conforme hipótese 3, responsabiliza-se por identificar de forma única qualquer participante.

8.5 Segurança do Modelo contra os principais tipos de ataques

Um agente malicioso pode:

1. interceptar, alterar, modificar ou produzir informações (no caso de um agente externo);

2. produzir ou alterar informações (no caso de um participante válido).

A possibilidade de interceptar, alterar, modificar ou produzir informações por agente externo não é possível, pois o tráfego das informações entre os participantes ocorre sobre o protocolo SSL/TSL. De acordo com a hipótese 2, o SSL/TSL garante que uma comunicação seja confidencial, íntegra e autêntica.

Para que um agente externo tente se passar por um participante válido, este deve possuir um certificado digital cadastrado na Central de Registros. Para isso o Cartorário deve ser desonesto (hipótese estudada mais a frente).

Agente Autorizado

1. **Tentar se cadastrar mais uma vez na Central de Registros** - O Cartorário que é o Agente Autorizado pelo cadastro dos Agentes Autorizados, deverá garantir que cada Agente Autorizado tenha apenas uma identificação na Central de Registros.

2. **Tentar incluir registros de nascimentos falsos** - Além de exercer a função de verificar a veracidade dos registros efetuados, o Cartorário deverá também checar as informações do registros e não efetuar a liberação quando não estiverem corretos.

3. **Digitar dados incorretos nos registros** -Como é função do Cartorário verificar a veracidade dos registros efetuados, deverá checar as informações dos registros, e não efetuar a liberação quando não estiverem corretos.

Cartorário

Como o Cartorário é o responsável pela Central de Registros, e o detentor da fé pública, o protocolo não possui nenhum tipo de defesa contra um cartorário malicioso.

Desta maneira, os órgãos públicos responsáveis deverão acompanhar com atenção o trabalho dos cartorários.

8.6 Conclusão

Este capítulo teve por finalidade formalizar através de RP os protocolos das propostas apresentada no capítulo 7 e listar as condições de segurança do protocolo contra as principais formas de ataques.

Foram apresentadas as redes e a descrição de seus módulos, mostrando como o protocolo irá se portar durante o registro de um título, desde o envio por parte do Agente Autorizado até a liberação por parte do Cartorário.

Foram discutidos os requisitos de segurança, e os tipos de proteção contra agentes maliciosos.

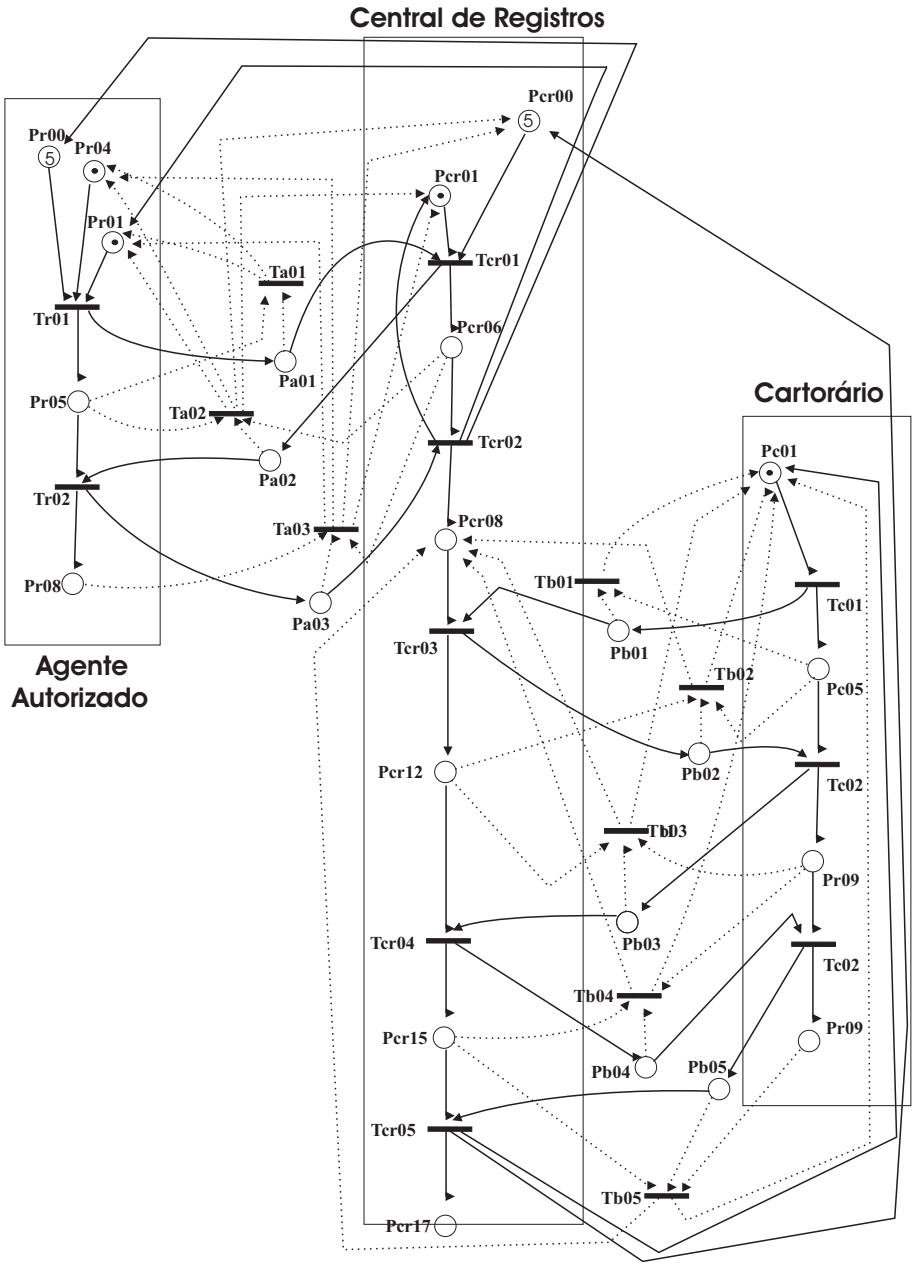

Figura 8.1: RP para o protocolo onde existe a interação do Agente Autorizado e do Cartorário.

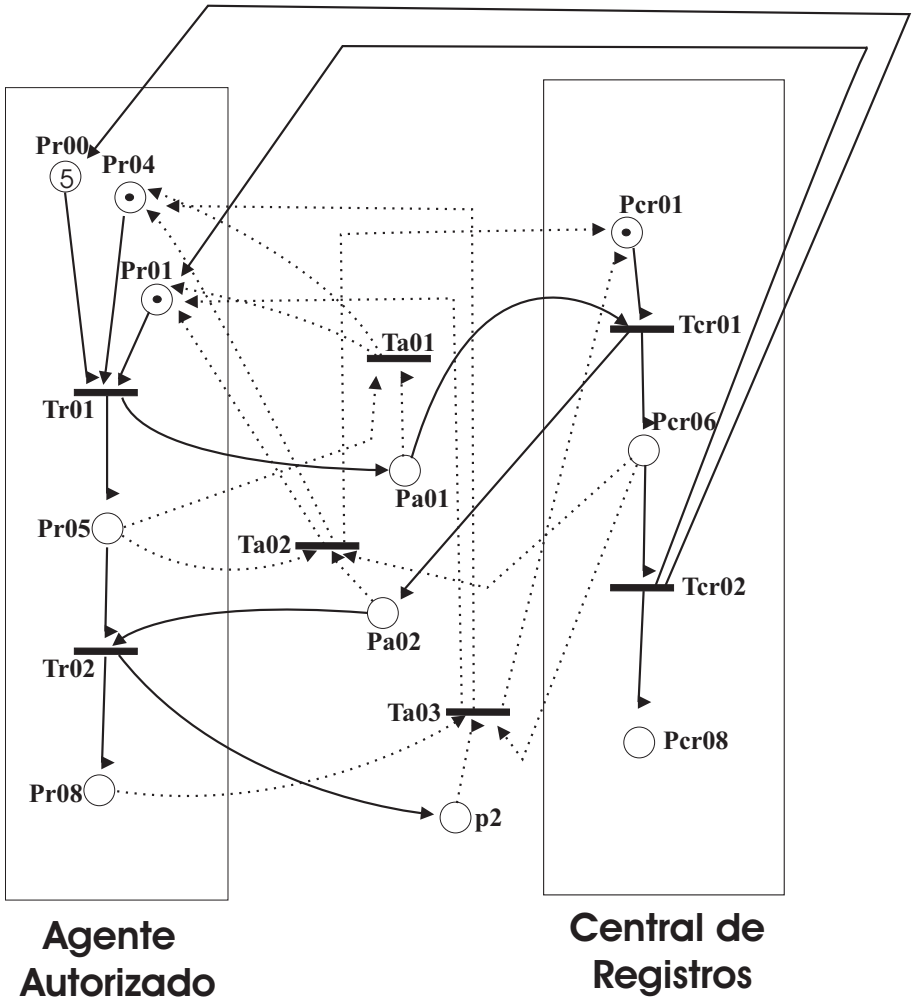

Figura 8.2: RP para o protocolo com emissão de certidão de nascimentos on-line

Capítulo 9

Considerações Finais

O presente apresentou um protocolo criptográfico para efetuar a emissão de Certidões de Nascimento através da Internet de maneira segura e rápida.

O grande problema, e talvez único, esbarra em aspectos não técnicos, que inclusive já foram observados por autores que visualizam a informática como ferramenta para melhoria dos serviços: *"É claro que precisamos adaptar as nossas leis para que o homem não seja escravo, mas senhor e beneficiário da tecnologia. Será necessário um remodelamento econômico e jurídico-institucional, sem o qual o progresso tecnológico poderá ser um previlégio de poucos"* [FIL 98].

Todos os benefícios que podem ser alcançados com a informatização do processo e da criação de um banco de dados de âmbito nacional são inegáveis e incontestáveis, benefícios estes que podem ser estendidos a todos, principalmente à população em geral, que terá um serviço mais eficiente e mais rápido. Os cartorários, por sua vez, terão condição de prestar seus serviços com gastos reduzidos e de maneira mais eficaz. Os órgãos públicos, finalmente, possuirão informações legítimas com atualizações instantâneas.

O presente projeto foi apresentado na Fenasoft nos anos de 2000 e 2001, e demonstrou ser um trabalho de grande aceitação pela opinião pública, levando em consideração o entusiasmo das pessoas que visitaram o *stand* da Universidade Federal de Santa Catarina (onde um protótipo estava exposto). A Emissão de Certidão de

Nascimento através da Internet teve grande atenção da imprensa, tendo sido citado em reportagens de diversos jornais e revistas de diferente áreas.

A definição de um protocolo seguro para emissão de certidão de nascimentos através da Internet, pode ser o primeiro passo de um grande processo de modernização dos serviços dos cartórios, desde que os estudos não sejam encerrados e novos trabalhos sejam iniciados.

9.1 Trabalhos Efetuados

- Através de pesquisa *in loco* foi feito um levantamento do processo de registro público, principalmente com relação a que se refere à emissão de certidão de nascimento;
- Levantamento e estudo das leis que regem o registro de nascimentos;
- Criação de duas versões do protocolo ECN, protocolo criptográfico proposto para a emissão de certidão de nascimento através da internet, tendo sido todos os passos detalhados e explicados;
- Foram criados modelos formais das duas variações do protocolo, em Redes de Petri, e as redes resultantes foram avaliadas com as ferramenta HPsim [ANS] e ARP [MAZ];
- Implementação de um sistema protótipo que utiliza o protocolo ECN.

9.2 Sugestões para Trabalhos Futuros

Umas das principais intenções deste trabalho é servir de base para novos trabalhos que irão fazer com que, no futuro, a emissão das certidões de nascimento através da WEB seja uma realidade. Dentre as pesquisas que se pode visualizar, no momento, como complemento desta, estão as seguintes:

- Elaboração do banco de dados do segundo e terceiro modelos;

- Estudos de técnicas de Biometria [BOL 00] para reconhecimento das pessoas registradas;
- Criação de Extensões para Redes de Petri para estudo detalhado de Protocolos Criptográficos;
- Criação de uma ferramenta para análise de Protocolos Criptográficos usando Redes de Petri;
- Implantação de um protótipo em que seja utilizado um banco de dados digital em substituição ao Livro;
- Implantação de um protótipo em que seja efetuada a emissão de certidão de nascimento *on-line*;
- Estudo das características dos protótipos para a elaboração de novas leis;
- Estudo detalhado da Central de Registros.
- Implantação de um protótipo para estudo dos modelos propostos com relação à escalabilidade, acesso concorrente e tolerância a falhas.

Referências Bibliográficas

[ANS] ANSCHUETZ, H. **HPsim**. Disponível em <http://home.t-online.de/home/henryk.a/download45644/hpsim.zip>. Acesso em: 10/11/2001.

[BOL 00] BOLLE, R. M.; JAIN, A. Biometrics: The future of identification. **IEEE**, [S.l.], v.0018-9162, p.46, 2000.

[BRA a] BRASIL. Lei n. 6.015, de 31 DE DEZEMBRO DE 1973. Dispõe sobre os registros públicos, e dá outras providências.

[BRA b] BRASIL. Lei n. 8.069, de 13 DE JULHO DE 1990. Dispõe sobre os registros públicos, e dá outras providências.

[BRA c] BRASIL, A. B. **Assinatura Digital Não É Assinatura Formal**. Disponível em <http://www.cbeji.com.br>. Acesso em: 20/10/2001.

[CAR 97] CARDOSO, J.; VALETTE, R. **Redes de Petri**. Editora UFSC, 1997.

[CER] CERTISIGN. **Certisign**. Disponível em <http://www.certisign.com.br/>. Acesso em: 20/09/2000.

[COS a] COSTA, A. A. **Validade Jurídica de Documentos Eletrônicos. Considerações Sobre O Projeto de Lei Apresentado Pelo Governo Federal.** Disponível em <http://www.cbeji.com.br>. Acesso em: 20/10/2001.

[COS b] COSTA, M. D. **O Apagão Do Comércio Eletrônico No Brasil**. Disponível em <http://www.cbeji.com.br>. Acesso em: 20/10/2001.

[dCF] DE CASTRO FERREIRA, A. A. M. B. **E-Cartórios**. Disponível em <http://www.cbeji.com.br>. Acesso em: 20/10/2001.

[dFM] DE FARIA MARTINS, H. **Assinatura Eeltrônica - O Primeiro Passo Para O Desenvolvimento Do Comércio Eletrônico?** Disponível em <http://www.cbeji.com.br>. Acesso em: 20/10/2001.

[dR] DE REZENDE, P. A. D. **Palavras Mágicas Sobre Entidades Certificadoras, Assinaturas Eletrônicas e Projetos de Lei.** Disponível em <http://www.cbeji.com.br>. Acesso em: 20/10/2001.

[dSC] DE SANTA CATARINA, T. **Página Do Tribunal de Santa Catarina**. Disponível em <http://www.tj.sc.gov.br>. Acesso em: 20/09/2000.

[FED 00] FEDERAL, G. **Web Site Oficial Do Governo Brasileiro**. Disponível em <http://www.brasil.gov.br>. Acesso em: Agosto. Retirada as Leis.

[FEG 99] FEGHII, J.; FEGHHI, J.; WILLIAMS, P. **Digital Certificates – Applied Internet Security**. Addison Wesley Longman, Inc., 1999.

[FER] FERREIRA, P. R. G. **A Assinatura Digital É Assinatura Formal**.

[FIL 98] FILHO, J. C. **O e M Integrado À Informática**. Rio de Janeiro: Editora LTC, 1998.

[GER 93] GERSTING, J. L. **Fundamentos Matemáticos Para a Ciência Da Computação**. LTC, 1993.

[ISO 89] **"Information Processing Sustems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture"**, 1989.

[JUN] JUNIOR, I. A. **Documentos Eletrônicos, Autoridade Certificadoras e Legislação Aplicável**. Disponível em <http://www.cbeji.com.br>. Acesso em: 20/10/2001.

[LEE 97] LEE, G.-S.; LEE, J.-S. Petri net basead models for specification and analysis of criptographic protocols. 1997.

[MAZ] MAZIERO, C. A. **Redes de Petri**. Disponível em <http://www.ppgia.pucpr.br/ maziero/petri/>. Acesso em: 20/09/2000.

[PAL 95] PALOMINO, R. C. **Uma Abordagem Para a Modelagem, Análise e Controle de Sistemas de Produção Utilizando Redes de Petri**. Universidade Federal de Santa Catarina, 1995. Dissertação de Mestrado.

[PET 81] PETERSON, J. L. **Petri Net Theory and the Modelling of System**. Prentice-Hall Editions, 1981.

[SCH 96] SCHNEIER, B. **Applied Cryptography**. 2. ed. New York, NY: John Wiley & Sons, Inc., 1996. 675 p.

[SMI 97] SMITH, R. E. **Internet Criptography**. Addison Wesley Longman, 1997.

[SOA 95] SOARES, L. F. G.; LEMOS, G.; COLCHER, S. **Redes de Computadores das LANs, MANs e WANs às Redes ATM**. Sexta. ed. Editora Campus, 1995.

[STA 99] STALLINGS, W. **Cryptography and Network Security**. 2. ed. Upper Saddle River, NJ: Prentice-Hall, 1999. 569 p.

[STI 95] STINSON, D. R. **Cryptography – Theory and Practice**. Boca Raton: CRC Press, 1995. 434 p.

[TAN 96] TANENBAUM, A. S. **Computer Networks**. Upper Saddle River, NJ: Prentice-Hall PTR, 1996.

Apêndice A

Representação da evolução das redes de Petri da Formalização

A.1 Introdução

Para ilustrar como a RP foi importante na avaliação do protocolo ECN, este anexo vai mostrar passo a passo a evolução da rede e uma descrição do que pode ocorrer em cada momento.

A.2 Evolução da Rede do Agente Autorizado

A figura A.1 representa o momento em que o Agente Autorizado possui uma certidão para ser enviada, a única transição passível de disparar é a de inicio do registro por parte do agente autorizado.

A figura A.2 representa o momento em o Agente Autorizado enviou a certidão para a Central de Registros e duas situações podem ocorrer: a Cental de Registros receber a mensagem e emitir uma resposta; ocorrer um erro na transmissão.

A figura A.3 representa o momento em que a Central de Registro enviou a resposta ao Agente Autorizado e duas situações podem ocorrer: o Agente Autorizado receber a mensagem e emitir uma resposta; ocorrer um erro na transmissão.

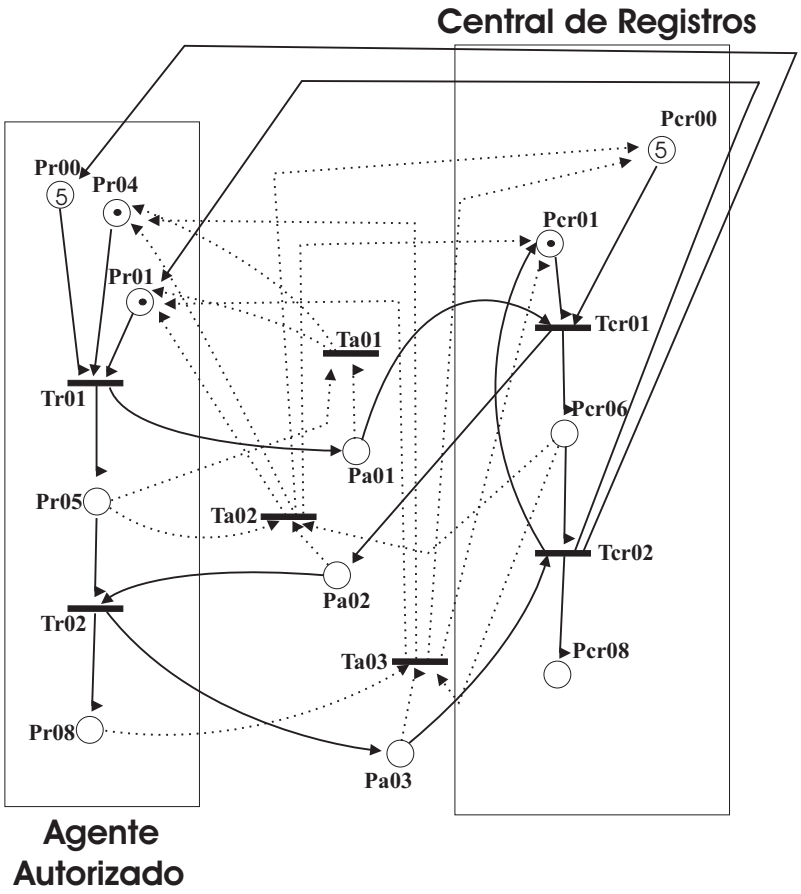

Figura A.1: Passo 1

A figura A.4 representa o momento em que o Agente Autorizado recebeu a confirmação da Central de Registros e armazenou o registro efetuado e duas situações podem ocorrer: a Central de Registros receber a mensagem e finalizar o processo com sucesso; ocorrer um erro na transmissão.

A figura A.5 representa o momento em a Central de Registro recebeu a confirmação do Agente Autorizado e armazenou os dados do registro efetuado, encerrando o processo com sucesso .

A figura A.6 representa o momento em que ocorreu um erro na transmissão. Todos o lugares são reinicializados menos o contador de erros no Agente Autorizado.

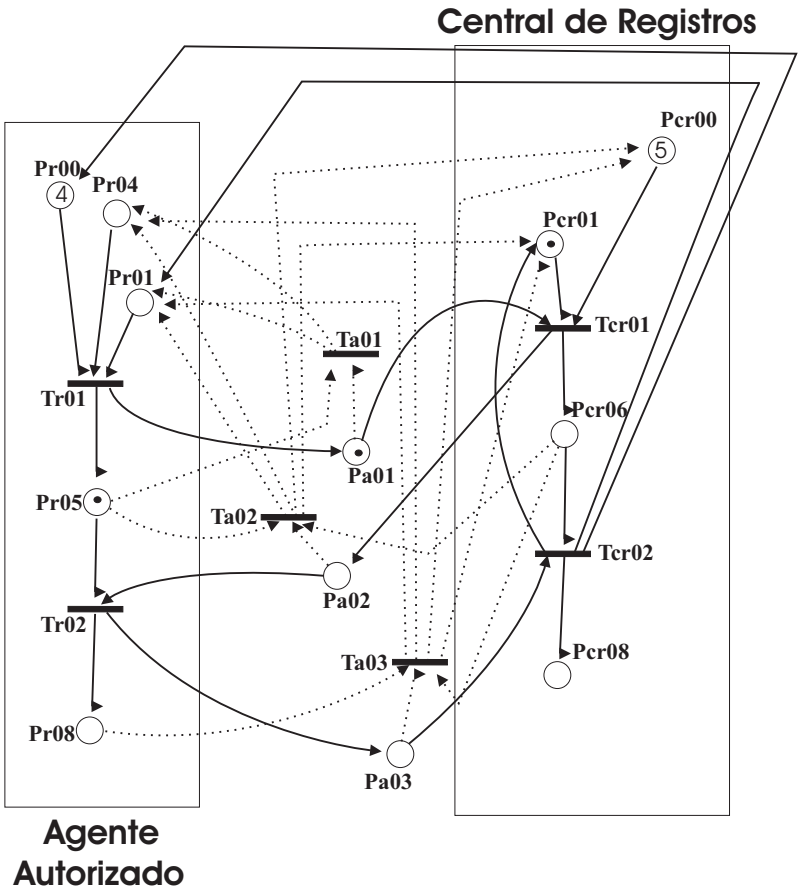

Figura A.2: Passo 2.

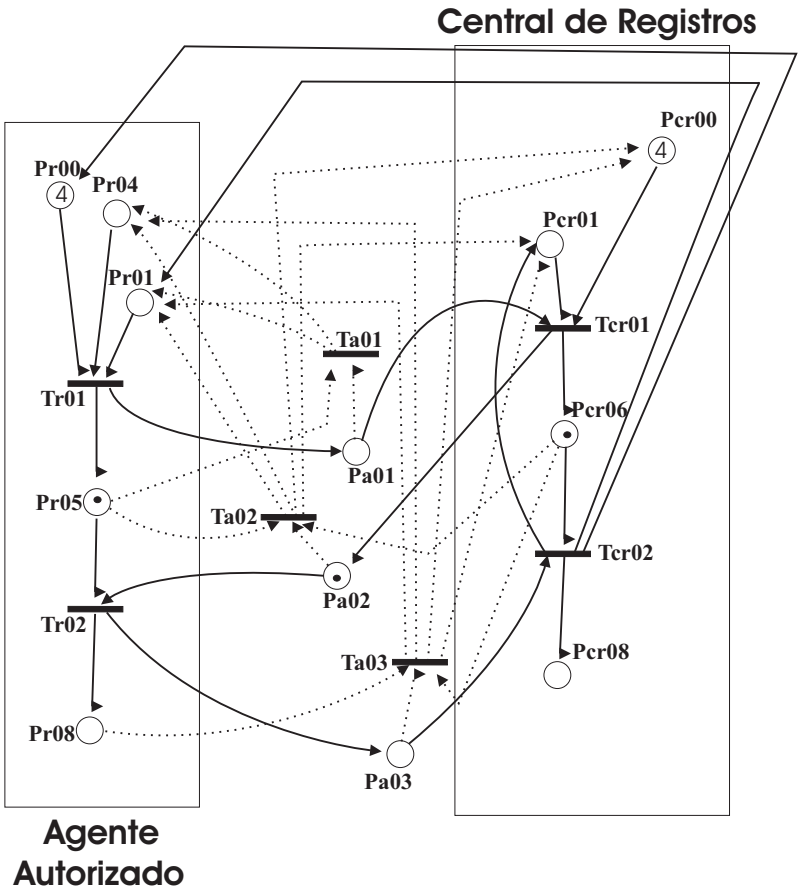

Figura A.3: Passo 3.

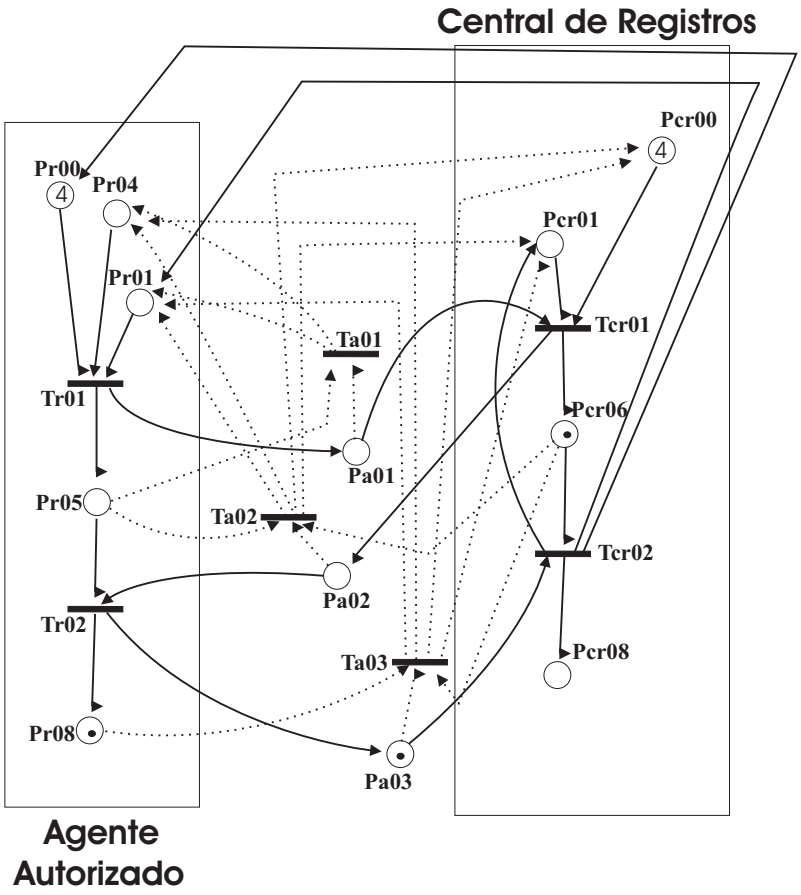

Figura A.4: Passo 4

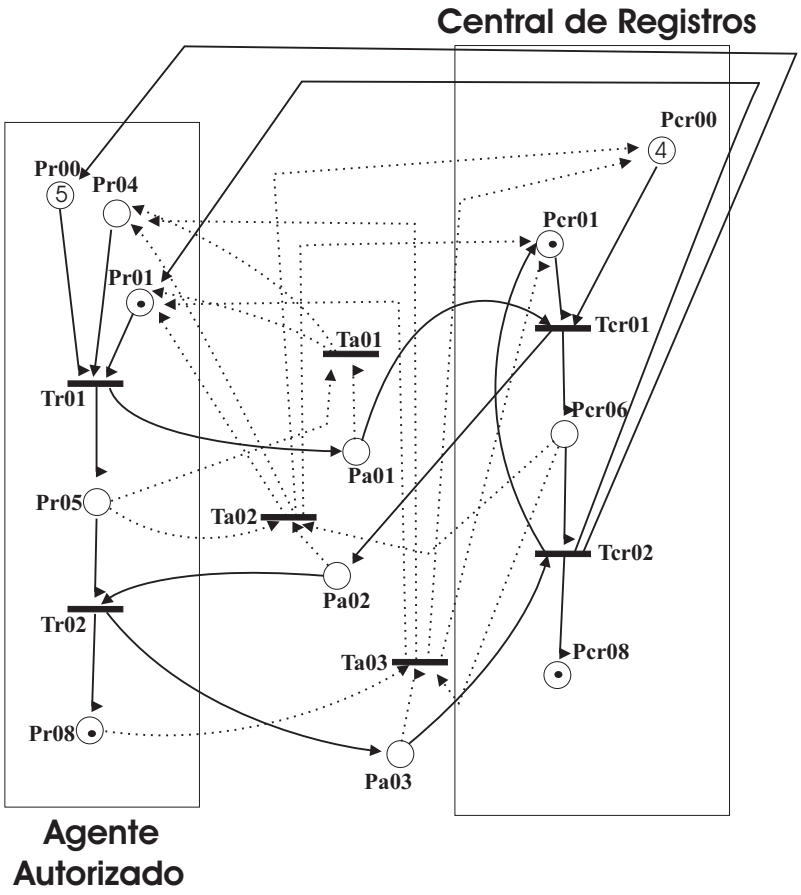

Figura A.5: Passo 5

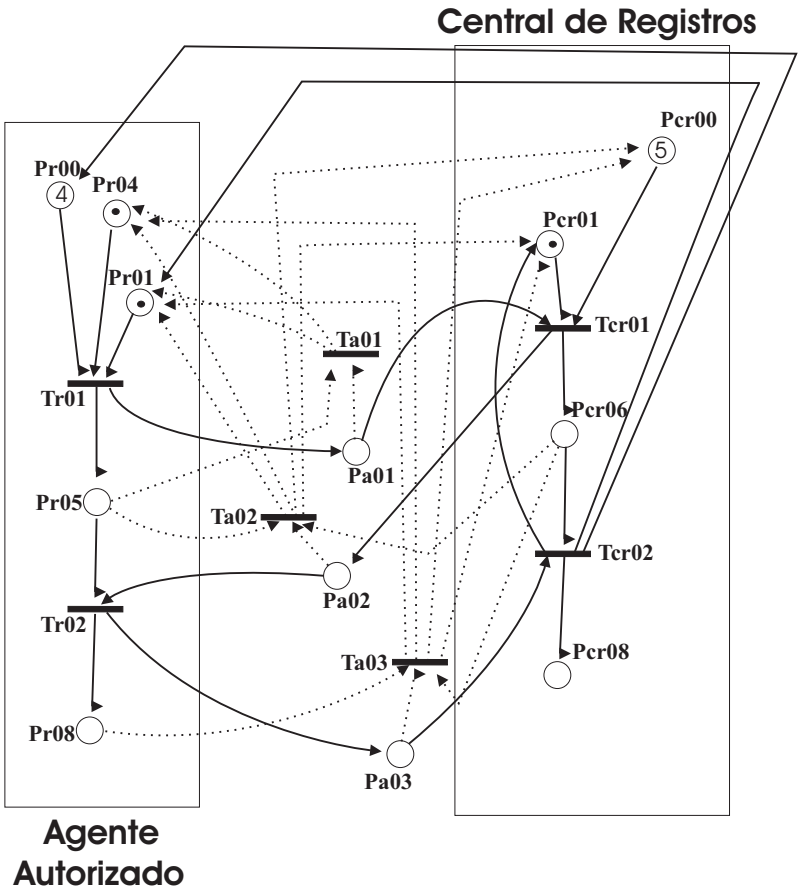

Figura A.6: Erro na Transmissão.

Apêndice B

Protótipo

Para a demonstração do protocolo ECN foi implementado um protótipo que, após a realização de testes, pretende-se implantar na Maternidade da UFSC e no Cartório da Trindade na cidade de Florianópolis-SC. Nesta seção serão descritos os módulos do protótipo.

B.1 Descrição do módulo Agente Autorizado

A função do Agente Autorizado é digitar todos os dados da DN, porém como pretende-se que todos os dados sejam enviados diretamente do Agente Autorizado para o Cartorário, faz-se necessário implementar campos adicionais além dos campos da DN. Uma solicitação por parte do Cartório da Trindade foi que, além dos dados, fossem enviadas cópias dos documentos dos pais da criança.

No programa, os campos foram divididos em 3 janelas: dados da DN; dados do Cartório; e documentos dos pais, conforme lista fig B.1.

Após a digitação de todos os campos, e o Agente Autorizado solicitar o envio dos dados, serão efetuados os processos ilustrados na figura B.2 e executados os seguinte passos.

1. a função de concatenação juntará todos os dados numa única *string* de dados.

2. A função de cifragem irá cifrar a *string* gerada pela função de concatenação com

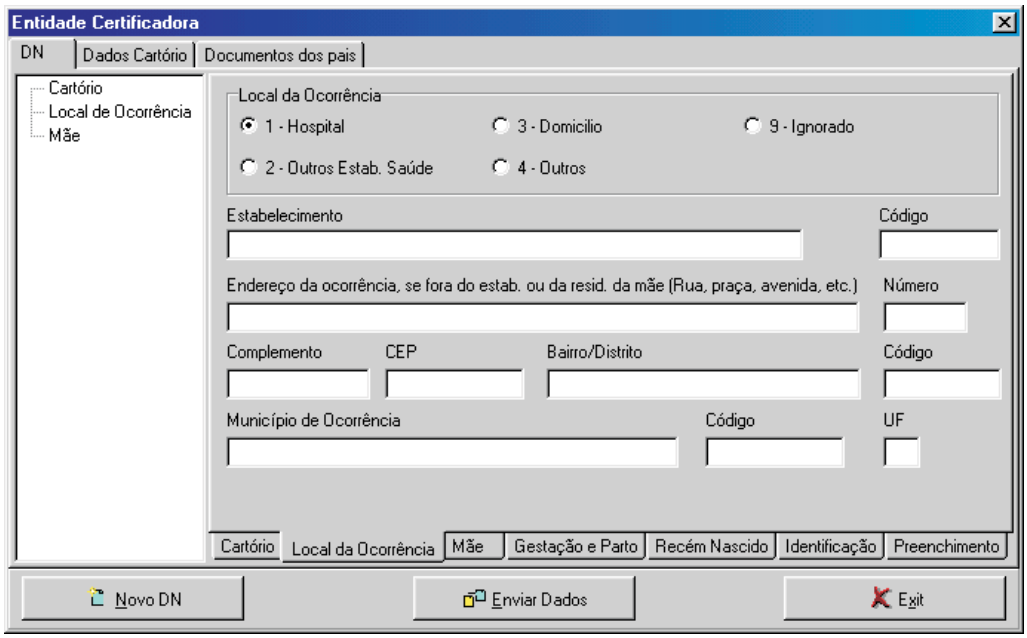

Figura B.1: figura que mostra a Interface do Programa de emissão de Certidão de Nascimento do Agente Autorizado.

a chave pública da central de registros e assinar com a chave privada do Agente Autorizado. O resumo da mensagem será armazenado para ser utilizada pela função de comunicação;

3. a função de comunicação irá: enviar os dados para a Central de Registros; receber a confirmação e conferir com o resumo da mensagem enviada e caso esteja correto armazenar o documento enviado no banco local do Agente Autorizado.

B.2 Descrição do funcionamento do programa utilizado pela Central de Registros

O programa da Central de Registros deverá prover comunicação com o Agente Autorizado e a comunicação com o Cartorário. Os dois tipos de comunicação diferem muito entre si e por isso serão explicadas separadamente.

Comunicação entre a Central de Registros e o Agente Autorizado

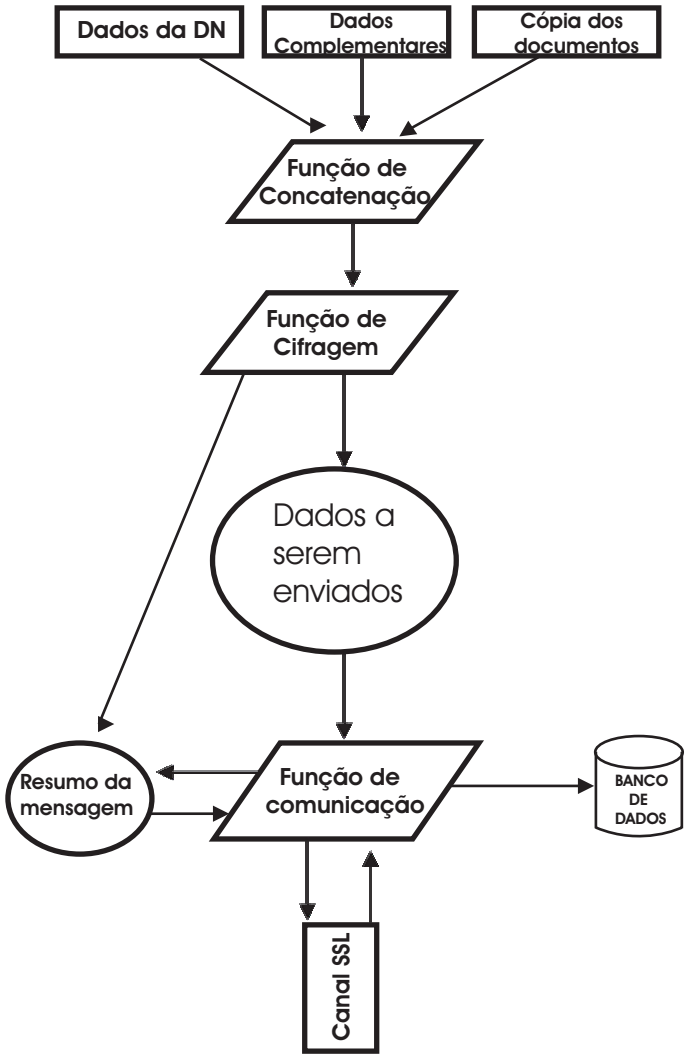

Figura B.2: Processo do envio dos dados do Agente Autorizado para a Central de Registros

O recebimento dos dados enviados pelo Agente Autorizado por parte da Central de Registros está representado na figura B.3 e segue os seguintes passos:

1. a função de comunicação recebe a mensagem enviada pelo Agente Autorizado e a repassa para a função de decifragem;

2. a função de decifragem gera o resumo da mensagem e recupera os dados assinados;

3. a função de comunicação envia o resumo da mensagem recebida para o Agente Autorizado e espera confirmação;

4. após receber a confirmação a função de comunicação armazena os dados no banco de dados.

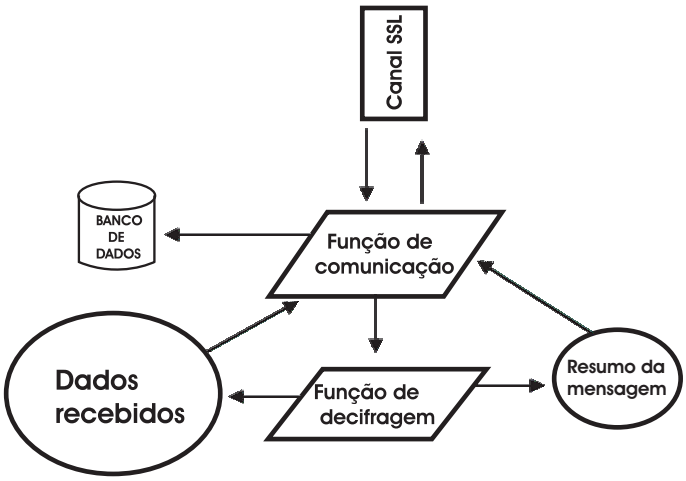

Figura B.3: Passos dos processo do recebimento dos dados do Agente Autorizado pela Central de Registros

Comunicação entre a Central de Registros e o Cartorário

A liberação por parte do Cartorário dos registros na Central de Registros está representada na figura B.2, e segue os seguintes passos:

1. a função de comunicação recebe do cartorário uma mensagem em que solicita os documentos a serem liberados;

2. a função de comunicação avisa a função de gravação, que retira do banco de dados todos os registros destinados àquele cartorário;

3. a função de concatenação junta todos os registros, montando uma mensagem que é cifrada pela função de cifragem;

4. a mensagem cifrada é enviada pela função de comunicação;

5. a função de comunicação recebe a mensagem com os registros liberados pelo Cartorário;

6. a função de cifragem decifra a mensagem e passa para a função de concatenação;

7. a função de concatenação ”quebra”a mensagem e cria os registros novamente;

8. a função de gravação confere os registros enviados com os registros recebidos e os armazena no banco, avisando a função de comunicação;

9. a função de comunicação envia a resposta para o Cartorário.

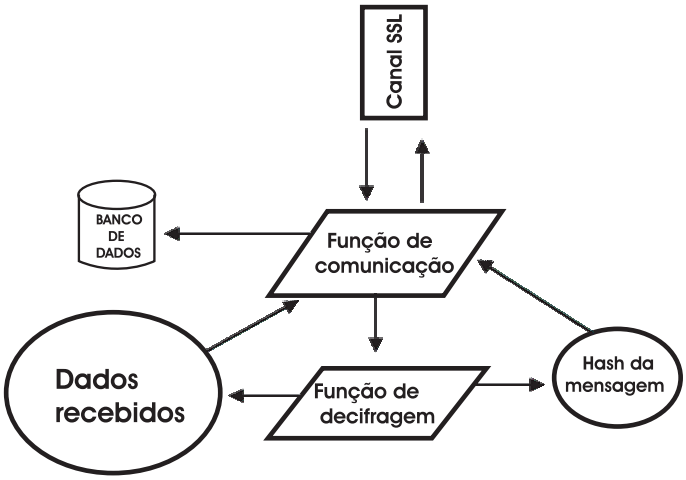

Figura B.4: Processo de liberação dos registros pelo Cartorário por parte da Central de Registros

B.3 Descrição do funcionamento do programa utilizado pelo Cartorário

A função do Cartorário é liberar os registros enviados pelo Agente Autorizado para a Central de Registros. Para isto fez-se necessário criar um programa que possui uma interface onde aparecem os registros a serem liberados e uma opção de liberação ou não liberação. Após escolher a opção se libera ou não o Cartorário deve enviar os dados para a Central de Registros.

Todo o processo começa com a solicitação dos Registros a serem liberados pelo Cartorário. O que acontece quando o cartorário solicita a liberação está ilustrado na figura B.3 e segue os seguintes passos:

1. o Cartorário solicita que a Central envie os documentos a serem liberados a função de apresentação manda uma mensagem para a função de comunicação;
2. a função de comunicação envia uma solicitação a Central de Registros;
3. a função de comunicação recebe os dados da central de registros e passa para a função de cifragem, que irá decifra a mensagem e passar para a função de concatenação;
4. a função de concatenação irá quebrar a mensagem em registros e passar para função de apresentação;
5. a função de apresentação mostra os registros para o Cartorário para que este possa efetuar a liberação;
6. após ter visualizado os registros e escolhidos quais serão liberados o Cartorário envia a liberação para a Central de Registros. A função de apresentação irá assinar os registros e passar os dados para a função de concatenação, que irá novamente concatenar os registros e passar para a função de cifragem.
7. a função de cifragem irá montar a mensagem a ser enviada pela seção de comunicação;
8. a função de comunicação irá receber a confirmação da Central de Registros e irá comunicar a seção de apresentação se ocorreu tudo bem;
9. a função de apresentação irá gravar no banco os registros liberados.

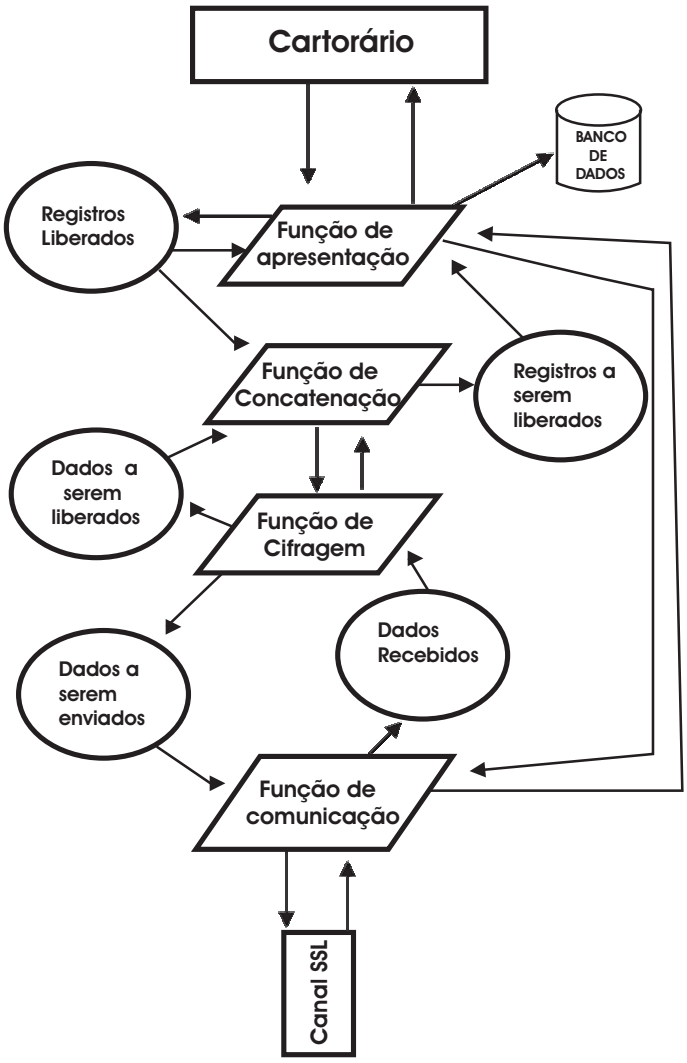

Figura B.5: Passos dos processo de liberação dos registros que estão na Central de Registros por parte do Cartorário