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

Everton Schonardie Pasqual

IDDE - Uma Infra-estrutura para a Datação de Documentos Eletrônicos

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

Prof. Ricardo Felipe Custódio, Dr.
Orientador
custodio@inf.ufsc.br

Florianópolis, Abril de 2001

IDDE - Infra-Estrutura para a Datação de Documentos Eletrônicos

Everton Schonardie Pasqual

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação , area 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
gauthier@inf.ufsc.br

Banca Examinadora

Prof. Ricardo Felipe Custódio, Dr.
Orientador
custodio@inf.ufsc.br

Prof. Dr. Ricardo Dahab
rdahab@ic.unicamp.br

Prof. Dr. Carlos Roberto De Rolt
rolt@datalan.com.br

Prof. Dr. Ségio Peters
peters@inf.ufsc.br

"Tudo posso naquele que me fortalece" Filipenses 4:13

Ofereço este trabalho a todos os pesquisadores em criptografia.

Agradecimentos

A Universidade Federal de Santa Catarina, em especial ao Departamento de Pós-graduação em Ciências da Computação.

Gostaria de agradecer ao meu orientador Ricardo Felipe Custódio, que sempre me encorajou durante todo o tempo. Sou muito grato a sua orientação e a sua amizade.

Aos colegas do mestrado, Roberto Samarone, Adriana Elissa Notoya e Rodrigo Bianco, pelo ambiente cooperativo e amigo que, sem dúvida, teve um relevante papel na transposição das várias e trabalhosas etapas do curso.

Aos meus pais Valmor e Olivia, pela educação e formação moral que tem alicerçado todas as minhas vitórias.

Resumo

O foco desta dissertação é a proposta de uma Infraestrutura de Datação de Documentos Eletrônicos. O trabalho está inserido na linha de pesquisa Segurança e Comércio Eletrônico do Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina.

O objetivo deste trabalho é propor um novo método de datação digital seguro e eficiente, capaz de minimizar o tempo de verificação de um recibo e de administrar uma enorme gama de requisições de datação ao mesmo tempo e propor uma Infra-estrutura de Datação de Documentos Eletrônicos - IDDE especificando suas entidades, relacionamentos, método de encadeamento e suas políticas de gerenciamento. Este trabalho pode ser resumido em quatro objetivos básicos: estudar os métodos de datação de documentos eletrônicos; estudar as técnicas de criptografia; definir o novo método de datação e propor uma Infra-estrutura de Datação de Documentos Eletrônicos.

Palavras-chave: Segurança em redes de computadores, criptografia, métodos de Datação, Time-stamping e Documentos Eletrônicos.

Abstract

The central subject of this Master Thesis is the proposal of a Digital Time-Stamping Electronic Documents Infrastructure. The work is inserted in the research of Security and Electronic Commerce of the Course of Master Degree in Computer Science of the Federal University of Santa Catarina.

The objective of this work is to consider a new method of time-stamping, capable of minimizing the time of verification of a receipt and to manage a lot of simultaneous time-stamping requisition and to consider a Digital Time-Stamping Electronic Documents Infrastructure, specifying its entities, relationships, method of chaining and its management politics. This work can be summarized in four basic objectives: the study of methods of time-stamping electronic document; the study of cryptographys techniques; definition of a new method for time-stamping and to consider a Digital Time-Stamping Electronic Documents Infrastructure.

Key Word: Network Security, cryptography, Time-Stamping methods, and Electronics Documents.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas

AC - Autoridade de Certificação

AD - Autoridade de Datação

AR - Autoridade de Registro

AES - Advanced Encryption Standard

ATR - Autenticação Temporal Relativa

BIPM - Bureau International des Poids et Mesures

CUT - Coordinated Universal Time

DES - Data Encryption Standard

DSS - Digital Signature Standard

GMT - Greenwich Mean Time

IAT - International Atomic Time

ICP - Infra-estrutura de Chave Pública

IDDE - Infra-estrutura de Datação de Documentos Eletrônicos

K - Chave de cifragem e decifragem simétrica

KR_B - Chave privada de Beto

KU_B - Chave pública de Beto

MD5 - Algoritmo que calcula o resumo de um arquivo digital qualquer

RSA - Padrão de cifragem assimétrica

SD - Serviço de Datação

SHA1 - Algoritmo que calcula o resumo de um arquivo digital qualquer

TSP - Time-Stamping Protocol

Capítulo 1

Introdução

Devido à crescente importância de relacionamentos internacionais e novas conexões comerciais, ficou evidente para as empresas de hoje, a necessidade de compartilhar e remeter documentos assinados ou não a uma longa distância. O sistema de correio tradicional é lento por natureza para atender toda a demanda gerada atualmente pelos sistemas de informação. Uma solução para o problema é utilizar a tecnologia de documentos eletrônicos para guardar as informações e utilizar o sistema de comunicação eletrônica para enviar tais documentos de um ponto à outro com uma maior agilidade. Claro que o receptor do documento eletrônico não pode supor que o documento recebido é autêntico, porque:

- podem ser facilmente modificados;
- podem ser facilmente forjados;
- não guardam individualidades;
- o conteúdo dos documentos eletrônicos não está fisicamente ligado com a assinatura, como é em um documento em papel.

Com estas desvantagens, documentos eletrônicos são raramente considerados em situações de disputas. Para resolver os problemas de modificação de mensagens foi criada a técnica de assinatura digital [SCH 95], a qual garante que a informação

contida no documento não possa ser modificada sem ser detectada. Para ambientes eletrônicos, a assinatura convencional pode ser eficientemente substituída por esta técnica. Em muitos países, leis e normas foram estabelecidas, de modo a legalizar a situação de documentos eletrônicos assinados digitalmente. No entanto, não se tem conhecimento se em algum destes países já foram utilizados dados digitais assinados como provas ou evidências para um julgamento em um tribunal.

A importância de que documentos eletrônicos tenham valor jurídico é muito grande. Isto se torna claro quando tais documentos precisam ser utilizados em situações de disputas. Mas o passo mais importante para o uso legal de documentos eletrônicos é a regulamentação da assinatura digital perante a justiça.

A técnica de assinatura digital provê para os documentos eletrônicos confidencialidade, integridade, autenticidade e não repúdio. Porém, existem algumas questões que devem ser consideradas.

1.1 Administração da chave privada

Um problema relacionado ao uso de assinaturas digitais é a administração das chaves de assinatura, chamadas de chaves privadas [STA 98]. Se outra pessoa, excluindo o dono da chave, tem acesso à chave privada, este poderá se passar pelo assinante original e assinar documentos em seu nome. Sem falar que um documento legitimamente assinado pode ser questionado, pois não se sabe, se foi realmente o assinante legal que o assinou.

1.2 Datação digital

Para que a assinatura digital tenha validade jurídica, além de associar o conteúdo de um documento a uma pessoa, deve ter também a data e hora de quando o documento foi assinado.

A datação digital tem como objetivo assegurar a existência de um documento eletrônico qualquer em uma determinada data e hora [MAS 99, LIP 99, SCH 95].

Mas o que é data e hora? Se esta pergunta fosse feita a Albert Einstein ele simplesmente responderia: "Tudo é Relativo", pois pela sua teoria nenhum tempo absoluto existe. Mas se fosse feita para uma pessoa comum ela responderia: "Data e hora é uma informação que estabelece referência temporal a um determinado evento".

Datação é um processo pelo qual é anexada data e hora em um documento. Esta data e hora deve condizer com a data e hora corrente, de modo a garantir que aquele documento existia em um determinado momento no tempo. Sem este procedimento, não seria possível dizer que um documento é ou não intempestivo, ou seja, fora do prazo legal, fora de tempo, inoportuno. A datação nada mais é do que uma prova legal que o documento existia em uma determinada data e hora.

Para se datar um documento precisa-se de uma referência de tempo confiável, a qual deve fornecer a data e hora exata para aquele momento. A referência mais recomendada para datar documentos é a data e hora instituída pelo *Coordinated Universal Time* (CUT). O CUT é o padrão de tempo universal definido em 1 janeiro de 1972. Ele também é referenciado como *Greenwich Mean Time* (GMT). O CUT é sincronizado de acordo com o *International Atomic Time* (IAT) que é mantido pelo *Bureau International des Poids et Mesures* (BIPM).

Como pode ser datado um documento? Um documento em papel pode ser datado através de um carimbo que contenha data e hora confiável. Já um documento eletrônico recebe data e hora através de um processo conhecido como datação digital de documentos eletrônicos. O serviço de datação digital recebe o documento a ser datado, efetua um cálculo único referente àquele documento, anexa data e hora no resultado do cálculo e o remete para o cliente. Estas informações resultantes são chamadas de recibo de datação. Um documento eletrônico para ser efetivamente assinado de forma digital, portanto para ter validade jurídica, deve conter a data e hora de sua criação (de quando foi assinado).

Note que diferentemente dos documentos em papel, os documentos eletrônicos não incluem um selo de tempo. Quando um documento é assinado, segundo o padrão de assinatura PKCS#7 [TEC 93], como pode ser visto na figura 1.1, somente informações referentes à assinatura são anexadas ao documento. Com isto, tem-se o que

se pode chamar de assinatura digital atemporal, pois não existe uma referência de tempo de quando este documento foi assinado. Com isto cria-se uma série de problemas:

- A assinatura foi efetivada dentro da data de validade do certificado digital[1]?
- O certificado digital não estava revogado quando o documento foi assinado?
- No momento da verificação da assinatura, como o verificador pode ter certeza de que o documento foi assinado dentro do prazo de validade do certificado digital?
- Como o verificador tem certeza de que o certificado não estava revogado no instante da assinatura?

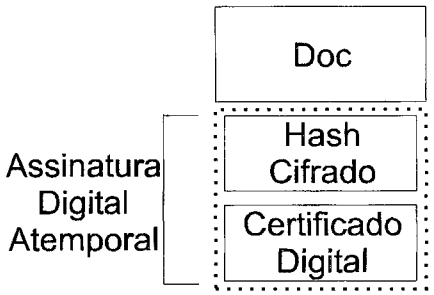

Figura 1.1: Assinatura Digital Atemporal. Quando um documento é assinado, segundo o padrão de assinatura PKCS#7 algumas informações devem ser anexadas ao documento: o resumo do documento (*hash*) cifrado com a chave privada do usuário e o certificado digital do usuário. Mas somente com estas informações não se pode determinar quando o documento foi assinado.

Segundo uma iniciativa da XML [ETS 01], propõe-se que sejam anexadas ao documento no ato da assinatura outras informações inclusive a data e hora da assinatura, figura 1.2, dando ao documento a propriedade de ser auto-verificável. Mas com isto surge um novo problema: como se pode garantir que a informação de data e hora contida na assinatura é realmente a data e hora em que o documento foi assinado? Com isto surge a necessidade de se ter uma entidade que disponibilize uma marcação de data e hora confiável.

[1]Certificado digital é um arquivo assinado de forma digital por uma entidade confiável com o objetivo de associar a chave pública à uma pessoa ou entidade.

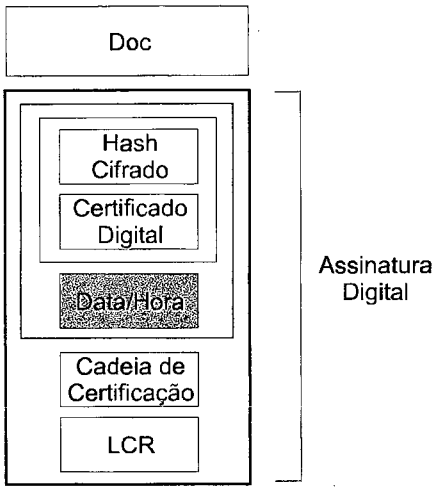

Figura 1.2: Assinatura Digital. Quando um documento é assinado algumas informações devem ser anexadas ao documento: o resumo do documento (*hash*) cifrado com a chave privada do usuário; o certificado digital do usuário. ; a cadeia de certificação; a lista de certificados revogados e a data e hora da assinatura. Com estas informações o documento tem a propriedade de ser auto-verificável.

Quem pode datar um documento? Um documento pode ser datado por uma entidade autorizada pelo governo de modo que todas as suas datações sejam reconhecidas como válidas e íntegras perante a justiça.

Para o mundo em papel tal entidade é o Cartório [2]. Para o mundo digital, o documento pode ser datado em qualquer entidade que disponibilize um serviço de datação. Hoje no Brasil não existe tal serviço.

A Constituição Federal, artigo 239§§ 1 a 3; lei número 3.015/73 dos registros públicos define as responsabilidades de entidades que disponibilizam serviços notariais:

> *"Art. 239. Os serviços notariais e de registro são exercidos em caráter privado, por delegação do poder público.*
>
> *§ 1. Lei regulará as atividades, disciplinará a responsabilidade civil e criminal dos notários, dos oficiais de registro e de seus prepostos, e definirá*

[2]Entidade incumbida de registro e guarda de documentos e de escrituras públicas. Serviços notariais e de registro são exercidos em caráter privado, por delegação do poder público.

a fiscalização de seus atos pelo Poder Judiciário.

§ 2. Lei federal estabelecerá normas gerais para fixação de emolumentos relativos aos atos praticados pelos serviços notariais e de registro.

§ 3. O ingresso na atividade notarial e de registro depende de concurso público de provas e títulos, não se permitindo que qualquer serventia fique vaga, sem abertura de concurso de provimento ou de remoção, por mais de seis meses."

Mas como se pode garantir a datação por um longo período de tempo? No conceito papel, o simples fato de se arquivar no cartório uma cópia de cada documento datado já pode ser considerado uma garantia de datação. No conceito eletrônico, a responsabilidade em garantir a datação por um longo período de tempo deverá ser de uma Autoridade de Datação, pois é ela que define quais serão os métodos criptográficos que serão utilizados para a implementação do serviço notarial.

O que é uma Autoridade de Datação? É uma entidade responsável em disponibilizar um serviço de datação confiável e que siga os padrões e normas instituídos pelo governo em que atua.

Muitos dos sistemas de datação se utilizam de uma entidade confiável chamada de Autoridade de Datação - AD (*Time-Stamping Authority*). O resultado da datação de um documento eletrônico é um arquivo digital, um recibo, assinado pela AD que contém informações da data e hora em que o documento foi submetido à AD. Este recibo atesta que um documento eletrônico foi submetido à AD em um certo momento do tempo. A datação digital é, na verdade, uma série de técnicas que permitem a uma pessoa averiguar se um documento eletrônico existia antes de uma determinada data.

Durante estes últimos anos, especialmente no contexto da regulamentação legal de assinaturas digitais, os aspectos organizacionais e legais da datação se tornaram um assunto de relevância internacional. Além de definir as responsabilidades do dono da assinatura, deveres e responsabilidades da Autoridade de Datação também devem ser definidos. Conseqüentemente, há um interesse crescente em sistemas de datação onde a necessidade de confiar na AD seja minimizada, para que os usuários desconfiem apenas

de seus próprios atos e não da confiabilidade do processo de datação.

Mas como documentos digitais não incluem um selo de tempo, a associação de um documento eletrônico com um certo momento de tempo é muito complexa, se não impossível. Até mesmo pela teoria de relatividade, nenhum tempo absoluto existe. O melhor que se pode alcançar com a datação é a autenticação temporal relativa - ATR (*Relative Temporal Authentication*), baseada na teoria da complexidade de funções unidirecionais. A ATR habilita ao usuário verificar entre dois documentos dados, qual dos dois foi datado primeiro.

Dez anos atrás a datação digital era uma área um tanto desconhecida para a sociedade científica e o único método de datação conhecido utilizava uma entidade que precisava ser completamente confiável. Mais pessoas se interessaram por este campo depois da publicação de Haber e Stornetta [HAB 91] onde foi mostrado que a confiança na AD pode ser claramente reduzida usando um método chamado encadeamento linear. Desde então foram publicados vários trabalhos que promoveram melhorias neste esquema, contudo, depois deste inicio fértil, as publicações se cessaram e a área se tornou desinteressante. Até que Buldas, Laud, Lipmaa e Villemson publicaram seu artigo [BUL 98b].

1.3 Trabalhos relacionados

As contribuições para este campo são bem diversificadas. O artigo publicado por Buldas, Laud, Lipmaa e Villemson [BUL 98b] foi o primeiro artigo científico que explicitamente tratou dos requisitos de segurança da Autoridade de Datação e com a idéia da autenticação temporal relativa, este artigo apresentou novos métodos de datação que permitem à pessoa descobrir e demonstrar as fraudes cometidas pela AD, ou seja, o método proposto de datação garantia a auditoria da AD. Ele também define um esquema de encadeamento baseado em rodadas e não mais seqüencial, como era o encadeamento linear. O grande ganho deste método foi a redução do tempo de verificação de um recibo na cadeia de datação. Neste artigo ainda foram analisados vários outros métodos previamente definidos por outros autores e discutidas suas vantagens e desvantagens. Viu-se

também que o esquema de encadeamento linear de Haber e Stornetta [HAB 91] pode ser usado para tornar auditável a AD, mas o sistema resultante não seria prático, devido ao tempo de verificação de recibos na cadeia ser elevado. Um novo método baseado em um esquema de encadeamento binário foi proposto, o qual garante a auditoria da AD e poderia ser utilizado na prática.

O artigo de Buldas e Laud [BUL 98a] formaliza o esquema de encadeamento binário, o qual é definido como sendo um grafo acíclico formado pelos recibos de datação. Por ser um grafo, o caminho de verificação pode ser formado de várias formas, possibilitando ao verificador escolher o menor caminho.

O artigo de Buldas, Lipmaa e Schoenmakers [BUL 00] mostrou que o requisito do grafo ser acíclico é desnecessário para garantir que a AD seja auditável. Consequentemente, uma nova geração de grafos foi proposta e validada no sentido de confiabilidade e o tempo de verificação seja minimizado.

1.4 Objetivos

O objetivo geral deste trabalho é propor um novo método de datação digital seguro e eficiente, capaz de minimizar o tempo de verificação de um recibo e de administrar uma enorme gama de requisições de datação ao mesmo tempo e propor um Infra-estrutura de Datação de Documentos Eletrônicos - IDDE especificando suas entidades, relacionamentos, método de encadeamento e suas políticas de gerenciamento. E tem como objetivos específicos:

- Estudar as técnicas de criptografia;
- Estudar os métodos e tecnologias de segurança existentes para o campo de datação eletrônica;
- Especificar um novo método de datação digital
- Propor e definir uma Infra-estrutura de Datação de Documentos Eletrônicos.

1.5 Motivação

Por que se precisa de um método de datação confiável e de uma infra-estrutura inteira para se datar documentos eletrônicos, se pode criar uma máquina lacrada e com auditorias constantes para se garantir a autenticidade das datações?

Se a Autoridade de Datação seguisse o princípio de funcionamento das máquinas de Cupom Fiscal [3], cujo a garantia de funcionamento não malicioso se dá segundo uma auditoria no hardware e software da máquina e segundo a confiança no lacre, se poderia sim confiar em tais datações, mas isto implica em custos e desconfiança.

Figura 1.3: Datadora de documentos em papel. Possui um relógio interno sincronizado periodicamente por uma entidade confiável e sua garantia de datação confiável se dá através da confiança do software da máquina e na confiança depositada no lacre da datadora, já que a mesma antes de ser lacrada para ser utilizada passa por uma auditoria de software e hardware.

O custo de se manter uma AD segundo ente princípio é muito alto, pois se precisa de um funcionário exclusivo e treinado para dar manutenção e utilizar os serviços desta AD, sem contar com os custos de segurança física para esta máquina, no sentido de proteger a mesma contra riscos de ambiente e de pessoas não autorizadas.

Precisa-se também de uma equipe que constantemente realize auditorias nesta máquina, afim de assegurar os documentos que foram datados até esta data. Isto é necessário, porque se houver um rompimento do lacre, não se tem provas e nem indícios de quando e quem fraudou a máquina, além de não se poder mais confiar nos documentos datados deste a última auditoria. É claro que a máquina guarda uma log de tudo o que

[3] Máquinas destinadas a emissão de notas fiscais para o recolhimento do ICMS das empresas

aconteceu e através dela pode-se apurar os fatos, mas sem ter um método de datação confiável não se tem provas para atestar a validade dos documentos datados naquela AD.

Como a máquina é selada e não se tem acesso ao software de datação como se pode garantir que as datações não são maliciosas e que não gerem desconfiança por parte de quem utiliza a AD ? A única garantia que se tem é que as pessoas que lacraram a máquina atestam a corretude do software. Este é o mesmo princípio das urnas eletrônicas.

Mas como fazer para que não seja necessário se confiar na AD e mesmo assim ter um serviço confiável? Isto é possível? Este trabalho vai de encontro a estas perguntas, apresentando meios e técnicas de se conceber uma AD que data documentos com data e hora corrente.

Tendo-se uma AD seguindo este princípio não se necessita de um auditoria constante, pois se houver um problema prova-se que a AD agiu de forma maliciosa e que os documentos datados nesta AD não foram alterados.

A AD disponibilizando um serviço confiável, pode ser utilizada como componente básico para o atendimento de requisitos de segurança de outros protocolos e aplicações, como no protocolo Farnel [DEV 00]. Para que o protocolo funcione a atenda os requisitos de segurança definido em [DEV 00] a Autoridade de Registro tem que ser confiável, mas se por outro lado a Autoridade de Registro datar todos os seus atos em uma AD, não se precisa mais confiar absolutamente na Autoridade de Registro. A AD talvez seja o principal componente necessário para garantia de confiança nos sistemas de comunicação.

1.6 Materiais e métodos

Desde 2000 trabalhos de pesquisa e desenvolvimento vem sendo realizados no Laboratório de Segurança - LabSEC da Universidade Federal de Santa Catarina tendo como atividades principais:

- 2000:

- inicio dos trabalhos na área de datação digital;
- primeira implementação real de uma Autoridade de Datação;
- realização de um Trabalho de Conclusão de Curso de Graduação em Ciência da Computação;

- 2001:
  - proposta e definição de um novo método de datação digital;
  - implementação de uma versão melhorada de uma autoridade de datação com a contribuição de dois alunos de graduação do curso de Ciência da Computação;
  - criação de uma parceria com uma empresa privada de base tecnológica;
  - proposta e definição de uma Infra-estrutura de datação de documentos eletrônicos.

- 2002:
  - conclusão de uma dissertação de mestrado na área com o título: IDDE - Infra-estrutura de Datação de Documentos Eletrônicos.

1.7 Conteúdo do documento

Esta é uma pesquisa teórica-prática. A parte teórica abrange os métodos e os procedimentos para a viabilização do projeto. A parte prática consiste na definição do método de datação e da Infra-estrutura IDDE.

Para tanto, será necessário conhecer alguns conceitos básicos de criptografia para poder adotar os métodos criptográficos mais apropriados, capítulo 2. Já no capítulo 3 serão apresentadas algumas das técnicas de datação mais relevantes contidas na literatura para ser ter uma visão geral do que se tem hoje em termos de datação digital. No capítulo 4 será apresentada e definida a proposta de um novo método de protocolação digital. Por fim, no capítulo 5 é discutida e definida uma proposta de uma Infra-estrutura de Datação de Documentos Eletrônicos para viabilizar o requisito de escalabilidade, ou

seja, com esta infra-estrutura é possível imaginar um cenário nacional de serviços de protocolização.

O anexo A traz uma lista das questões mais freqüentes sobre protocolização de documentos eletrônicos. E o anexo B mostra um exemplo numérico do método da Árvore Sincronizada proposto nesta dissertação. O objetivo deste exemplo numérico é prover um facilitador adicional para o entendimento do método proposto.

Capítulo 2

Fundamentos de Criptografia

2.1 Introdução

O sentido da palavra segurança em computação consiste na garantia de que as informações sigilosas não serão acessadas, copiadas ou modificadas por pessoas ou entidades não autorizadas. Uma forma de se conseguir isso é embaralhar a informação, tornando-a incompreensível, de tal forma que somente as pessoas ou entidades autorizadas saibam como desembaralha-la. Este processo é chamado de criptografia.

A palavra criptografia tem origem grega (kriptos = escondido, oculto e grifo = escrita) e consiste na arte de escrever em cifras ou em códigos, utilizando um conjunto de técnicas que torna uma mensagem incompreensível, chamado comumente de **texto cifrado**, através de um processo chamado de **cifragem**. O processo inverso, chamado de **decifragem**, consiste em decifrar a mensagem original, de tal forma que somente o destinatário consegue a informação [STA 98].

Para **cifrar** um texto, utiliza-se uma **chave** ou **senha** com um determinado número de bits. Quanto maior o número de bits da chave, maior é o **espaço de chaves** [1]. Seja b o número de bits da chave, então o espaço de chaves é 2^b. O **ataque de força bruta** consiste em verificar todas as possíveis chaves de forma a encontrar a chave que foi utilizada para cifrar uma determinada mensagem. Desta forma, quanto maior o

[1] Conjunto de possíveis chaves

número de bits da chave, maior será o esforço computacional para se descobrir a chave utilizada.

Devido a muitas discussões envolvendo os termos de criptografia, procurou-se convencioná-los, afim de que se consiga uma padronização de termos:

- **Texto aberto** - informação sigilosa que se deseja proteger;
- **Texto fechado ou cifrado** - informação sigilosa já embaralhada, depois de ter passado por um processo de cifragem;
- **Cifragem** - processo de embaralhamento da informação;
- **Decifragem** - processo de desembaralhamento da informação;
- **Cifrador** - algoritmo responsável em cifrar a informação (texto aberto) com um outro objeto (chave), com a intenção de se obter uma saída incompreensível (texto fechado);
- **Decifrador** - algoritmo que realiza o processo inverso do cifrador;
- **Chave** - informação, muitas vezes aleatória, que é cifrada junto com o texto aberto. Existe dois tipos de chaves: chaves simétricas, onde que a mesma chave é utilizada para cifrar e decifrar a mensagem, e chaves assimétricas, onde existe uma chave para cifrar e outra para decifrar.
- **Alice** - entidade emissora
- **Beto** - entidade receptora

A criptografia pode ser classificada em duas categorias , de acordo com o tipo de chave utilizada. A **criptografia simétrica** é um sistema criptográfico em que a cifragem e a decifragem utilizam a mesma chave, seção 2.2. A **criptografia assimétrica**, conhecida também como **criptografia de chave pública**, é um sistema criptográfico em que a cifragem e a decifragem utilizam chaves diferentes, uma delas pode ser chamada de **chave privada** e a outra de **chave pública**, seção 2.3.

Neste capítulo ainda serão apresentados conceitos de funções resumo, seção 2.4, assinatura digital, seção 2.5, certificados digitais, seção 2.6, e infra-estrutura de chaves públicas, seção 2.7.

2.2 Criptografia simétrica

A criptografia simétrica utiliza a mesma chave para cifrar e decifrar uma mensagem. Isso significa que a chave deve ser de conhecimento tanto do emissor como do receptor da mensagem. Normalmente na criptografia simétrica, o algoritmo para cifrar e decifrar é basicamente o mesmo, mudando apenas a forma como é utilizada a chave. Devido esta técnica de criptografia ser muito utilizada ao longo dos anos e por seus algoritmos serem normalmente muito simples, muitos aperfeiçoamentos e avanços foram realizados neste tipo de sistema criptográfico. [STI 95].

Um sistema criptográfico simétrico é composto por uma quintupla (*P, C, K, E, D*), onde seguintes condições devem ser atendidas:

1. P é um conjunto finito de possíveis textos abertos;
2. C é um conjunto finito de possíveis textos cifrados;
3. K é um conjunto finito de possíveis chaves;
4. Para cada $k \in K$, existe uma cifragem $e_k \in E$ a uma decifragem $d_k \in D$. Cada $e_k : P \rightarrow C$ e $d_k : C \rightarrow P$ são funções tais que $d_k(e_k(x)) = x$ para cada texto aberto $x \in P$.

A figura 2.1 monstra como funciona o sistema criptográfico simétrico, aplicada a um texto aberto qualquer, utilizando-se de uma chave K. A mensagem a ser enviada é cifrada por Alice com uma chave K que é de seu conhecimento. Para Beto conseguir decifrar esta mensagem, ele deve ter a mesma chave K utilizada por Alice.

O algoritmo simétrico mais conhecido hoje é o DES (*Data Encryption Standard*) [NIS 77], o qual foi por muitos anos o padrão de cifragem simétrica. Após a definição do DES outros algoritmos, seguindo os mesmos princípios de Caixas-S e

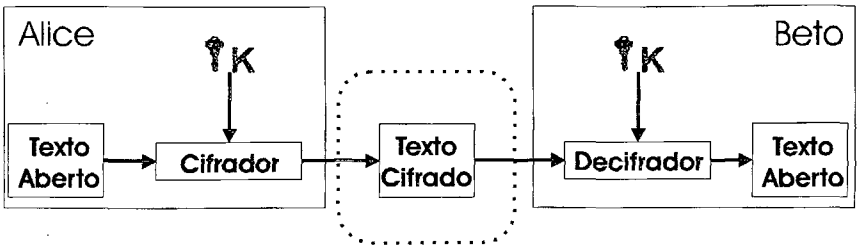

Figura 2.1: Criptografia Simétrica. Alice, utilizando um cifrador e uma chave K, cifra o texto aberto produzindo o texto cifrado. Beto utilizando o texto cifrado e a mesma chave K, decifra o texto cifrado obtendo o texto aberto original.

rodadas, foram surgindo, é o caso do Blowfish [SCH 93], IDEA [LAI 91], CAST128 [ADA 97] e o RC5 [RIV 94]. Devido a fragilidade do DES o governo americano lançou um concurso para a definição de um novo padrão de cifragem simétrica. O algoritmo que venceu o concurso foi o Rijndael e como ele o novo padrão de cifragem foi definido, chamado de AES (*Advanced Encryption Standard*) [NIS 01].

O principal problema relacionado à criptografia simétrica está no fato de que os atores devem ter acesso à mesma chave. Portanto, existe a necessidade da adoção de uma política de segurança para a troca e a guarda da chave. Esta política acarreta dois problemas quanto à segurança, decorrentes do gerenciamento de chaves. O primeiro, diz respeito à conservação do segredo de uma chave que é de conhecimento de várias pessoas. Bastaria uma delas agir de forma maliciosa para que todos sofressem as eventuais conseqüências. O segundo problema refere-se à própria distribuição da chave. Sempre que um novo ator fosse admitido no grupo, necessitaria receber essa chave. Uma forma de resolver estes problemas é utilizar a criptografia assimétrica.

2.3 Criptografia assimétrica

A técnica de criptografia assimétrica, também chamada de criptografia de chave pública, é aquela em que cada ator possui um par de chaves: uma chave pública e uma chave privada [2]. Se a chave privada é usada para cifrar, então deve-se usar a chave

[2]Na verdade pode existir mais de 2 chaves

pública para decifrar. Se a chave pública é usada para cifrar, deve-se usar a chave privada para decifrar. A chave privada deve ser mantida em segredo, enquanto que a chave pública deve ser tornada de alguma forma pública [STA 98]. A chave privada leva este nome pois somente o dono da chave a conhece e mais ninguém.

O conceito de criptografia de chave pública foi apresentado em 1976 por Whitfield Diffie e Martin Hellman [DIF 76]. Em 1977, Ron Rivest, Adi Shamir e Len Adleman desenvolveram um algoritmo assimétrico denominado RSA [RIV 78], que implementava os conceitos apresentados por Diffie e Hellman um ano antes. O RSA é a base, atualmente, da maioria das aplicações baseadas na criptografia assimétrica. As chaves pública e privada no RSA tem as seguintes propriedades:

- Diferentemente da criptografia simétrica, no qual a chave é única, existem agora duas chaves de criptografia;
- Cada chave pode, indiferentemente, ser utilizada para cifrar ou decifrar;
- Uma mensagem cifrada com uma das chaves somente pode ser decifrada com a outra chave;
- O conhecimento da chave pública não permite a descoberta da chave privada correspondente.

Seja $n = pq$, onde p e q são primos. Seja $P = C = Z_n$ e $K = \{(n, p, q, a, b) : n = pq, p, q \ primos, ab \equiv 1(mod\ \phi(n))\}$. Para $K = (n, p, q, a, b)$ e $(x, y \in Z_n)$, define-se:

$$y = e_k(x) = x^b \ mod\ n \tag{2.1}$$

$$d_k(y) = y^a \ mod\ n \tag{2.2}$$

Os valores n e b são públicos, e os valores p, q, a são secretos.

Com a criptografia assimétrica, pode-se prover a autenticação e confidencialidade. A autenticação é a garantia de identificação das pessoas ou organizações envolvidas na comunicação. A figura 2.2 ilustra este processo. Nesta figura, Alice cifra o texto aberto com sua chave privada. Beto decifra o texto cifrado com a chave pública de

Alice. Percebe-se que o texto cifrado pode ser unicamente decifrado com a chave pública de Alice, pois somente Alice tem a chave privada correspondente daquela chave pública. Assim sabe-se que foi Alice quem cifrou a mensagem. Cabe salientar que não há sigilo, pois qualquer pessoa pode decifrar o texto cifrado enviado por Alice, já que sua chave pública está disponível de alguma forma.

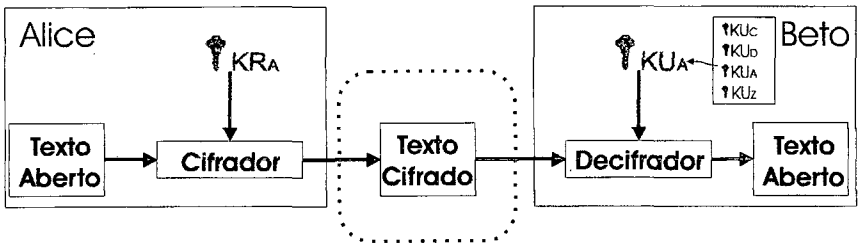

Figura 2.2: Criptografia assimétrica para garantir autenticação. Alice, utilizando um cifrador e sua chave privada KR_A, cifra o texto aberto produzindo o texto cifrado. Beto utilizando o texto cifrado e a chave pública KU_A de Alice contida em seu repositório de chaves, decifra o texto cifrado obtendo o texto aberto original.

Já a garantia da confidencialidade, na qual somente os participantes na comunicação possam ler e utilizar as informações, conforme ilustra na figura 2.3, pode ser garantida da seguinte forma:

- Alice cifra o texto aberto com a chave pública de Beto KU_B;
- O texto cifrado é enviado para Beto;
- Beto utiliza sua chave privada KR_B, para decifrar e voltar a ter o texto aberto. A mensagem é confidencial porque somente Beto tem a chave privada.

2.4 Função resumo

Um resumo é gerado por uma função H da forma:

$$h = H(M) \tag{2.3}$$

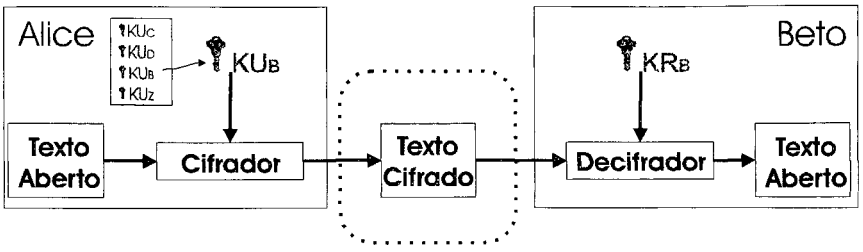

Figura 2.3: Criptografia assimétrica para garantir confidencialidade. Alice utiliza a chave pública de Beto KU_B, contida em seu repositório de chaves, para cifrar o texto. Beto por sua vez, decifra o texto cifrado com um decifrador utilizando sua a chave privada KR_B.

onde M é uma mensagem de tamanho variável e $H(M)$ é o valor do resumo da mensagem M com um tamanho fixo. O objetivo da função resumo é produzir um *"fingerprint"*do arquivo, da mensagem ou de um outro bloco de dados qualquer, ou seja, gerar uma identificação curta para um bloco de dados específico. Para que se possa confiar no resultado gerado por uma função resumo, a função H deve atender as seguintes propriedades [STA 98]:

1. A função H deve ser aplicada a um bloco de dados de qualquer tamanho;
2. A função H deve produzir uma saída de tamanho fixo, não importando o tamanho da entrada;
3. $H(x)$ é relativamente fácil de se calcular, tornando possível a implementação desta função tanto em software quanto em hardware;
4. Para qualquer resumo h, é computacionalmente impraticável achar um x que satisfaça $H(x) = h$. Esta propriedade é chamada unidirecionalidade;
5. Para qualquer bloco de dados x, é computacionalmente impraticável achar $y \neq x$ em que $H(y) = H(x)$. Esta propriedade é chamada de resistência fraca a colisão.
6. É computacionalmente impraticável achar um par (x, y) de modo que $H(x) = H(y)$. Esta propriedade é chamada de resistência forte a colisão.

As funções resumos mais utilizadas são a MD5, concebida por Ron Rivest [RIV 92], que recebe como entrada um bloco de dados de qualquer tamanho e

produz uma saída de tamanho de 128-bits, e o SHA1 (*Secure Hash Algorithm*) [NIS 93], que recebe como entrada um bloco de dados de tamanho máximo de 2^{64} e produz uma saída de tamanho de 160-bits. A principal diferença entre estes dois algoritmos é com certeza o tamanho da saída. Com isto, a dificuldade de se gerar uma mensagem qualquer que produza o mesmo resumo varia da ordem de 2^{128} do MD5 para a ordem de 2^{160} do SHA1.

A função resumo pode ser utilizada em conjunto com a criptografia assimétrica para se obter uma forma de assinatura digital [SCH 95]. Isso pode ser feito enviando-se para Beto a mensagem e o resumo da mensagem cifrado com a chave privada de Alice. Beto, decifra o resumo com a chave pública de Alice, calcula um novo resumo com base na mensagem recebida e compara os dois valores. Se forem iguais, a mensagem não foi alterada, garantindo-se dessa forma a sua integridade. A figura 2.4 ilustra este processo.

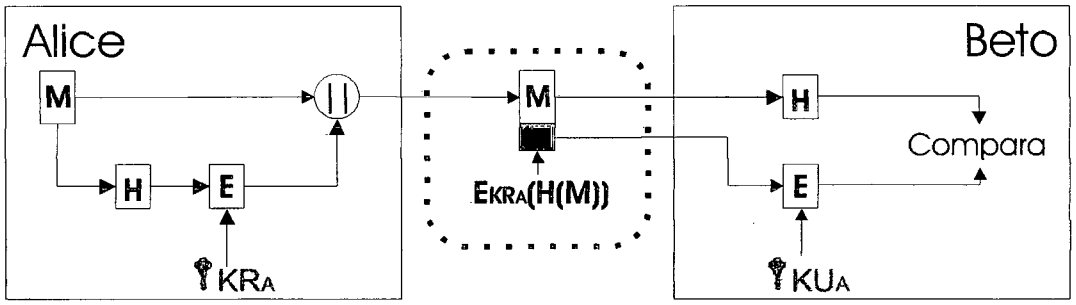

Figura 2.4: Assinatura digital com criptografia assimétrica. Alice calcula o resumo da mensagem M com um função H e cifra este resumo com sua chave privada, KR_A. O resultado é então concatenado com a mensagem original e enviado para Beto. Beto por sua vez decifra o pacote recebido com a chave pública de Alice, KU_A, calcula o resumo da mensagem M recebida e compara os dois resultados. Se os dois forem iguais Beto tem a certeza que a mensagem não foi alterada.

2.5 Assinatura digital

Quando se assina um documento no papel, o que se assina efetivamente é o próprio papel. O papel neste caso é uma entidade física que faz a ligação entre a

assinatura propriamente dita e a informação impressa no mesmo papel. A assinatura manuscrita é considerada uma forma de medida biométrica indireta, pois imprime no papel uma escrita que tem uma certa dependência das bio-características de uma pessoa. Assim, existe uma ligação entre a pessoa que assina e o documento no papel. O mesmo não ocorre em documentos eletrônicos. Nestes não há um meio físico que permite estabelecer a ligação entre a informação e a assinatura. A assinatura digital é um código binário que é determinado com base no documento e alguma outra informação que associa este a uma determinada pessoa. Essa associação é conhecida como autenticação e pode ser feita basicamente em três níveis:

1. algo que se sabe, uma senha por exemplo;
2. algo que se possui, um cartão magnético;
3. algo que se é, uma medida biométrica da pessoa.

Existem estudos e pesquisas que definiram mais dois níveis de autenticação, eles são:

- onde você se encontra e em que horário;
- quem estava com você no ato da assinatura, testemunha.

A associação considerada mais frágil é a primeira e a mais forte é a relação entre uma pessoa e a assinatura. Pode-se utilizar mais de uma dessas formas para aumentar o grau de associação. Os bancos, por exemplo, normalmente utilizam algo que se sabe (uma senha) com algo que se tem (um cartão magnético) para autenticar um cliente.

A assinatura digital usa técnicas de criptografia para permitir, de forma única e exclusiva a comprovação da autoria de um determinado conjunto de dados. A assinatura digital tem sido implementada basicamente de três formas:

- usando funções resumo por meio dos padrões MD5 e SHA1, como foi visto na seção anterior;

- utilizando o DSS (*Digital Signature Standard*) [NIS 94a];
- utilizando o conceito de chaves públicas.

Um esquema de assinatura é composto de uma quintupla (P, A, K, S, V), onde seguintes condições devem ser atendidas [STI 95]:

1. P é um conjunto finito de possíveis mensagens;
2. A é um conjunto finito de possíveis assinaturas;
3. K é um conjunto finito de possíveis chaves;
4. Para cada $k \in K$, existe um algoritmo de assinatura $sig_k \in S$ a um algoritmo de verificação correspondente $ver_k \in V$. Cada $sig_k : P \rightarrow A$ e $ver_k : PxA \rightarrow \{true, false\}$ são funções tais que a equação é satisfeita para toda mensagem $x \in P$ e para toda assinatura $y \in A$:

$$ver(x, y) = true, se\ y = sig(x) \tag{2.4}$$

$$ver(x, y) = false, se\ y \neq sig(x) \tag{2.5}$$

Um exemplo de um esquema de assinatura pode ser concebido utilizando-se o sistema criptográfico assimétrico RSA.

Seja $n = pq$, onde p e q são primos. Seja $P = C = Z_n$ e $K = \{(n, p, q, a, b) : n = pq, p, q\ primo, ab \equiv 1(mod\ \phi(n))\}$. Os valores n e b são públicos, e os valores p, q, a são secretos. Para $K = (n, p, q, a, b)$, defini-se:

$$sig_k(x) = x^a mod\ n \tag{2.6}$$

$$ver_k(x, y) = true \Leftrightarrow x \equiv y^b mod\ n \tag{2.7}$$

2.6 Certificado digital

O certificado digital é um arquivo assinado de forma digital por uma entidade confiável com o objetivo de associar a chave pública a uma pessoa ou entidade. O certificado digital serve então como um mecanismo para a divulgação da chave pública.

A Autoridade de Certificação - AC assina o certificado com sua chave privada. Quem desejar confirmar a autenticidade do certificado, basta pegar a chave pública da AC, e verificar a assinatura do certificado.

Existem várias propostas de codificação de certificados digitais o mais conhecido e aceito é a recomendação ITU-T X.509v3 [ADA 99a] [IT 00]. Na estrutura de dados de um certificado, estão no mínimo as seguintes informações: chave pública, nome do usuário, número de série do certificado, nome da AC que emitiu o certificado, assinatura digital da AC. A figura 2.5 ilustra, de forma simplificada, a estrutura de dados do certificado.

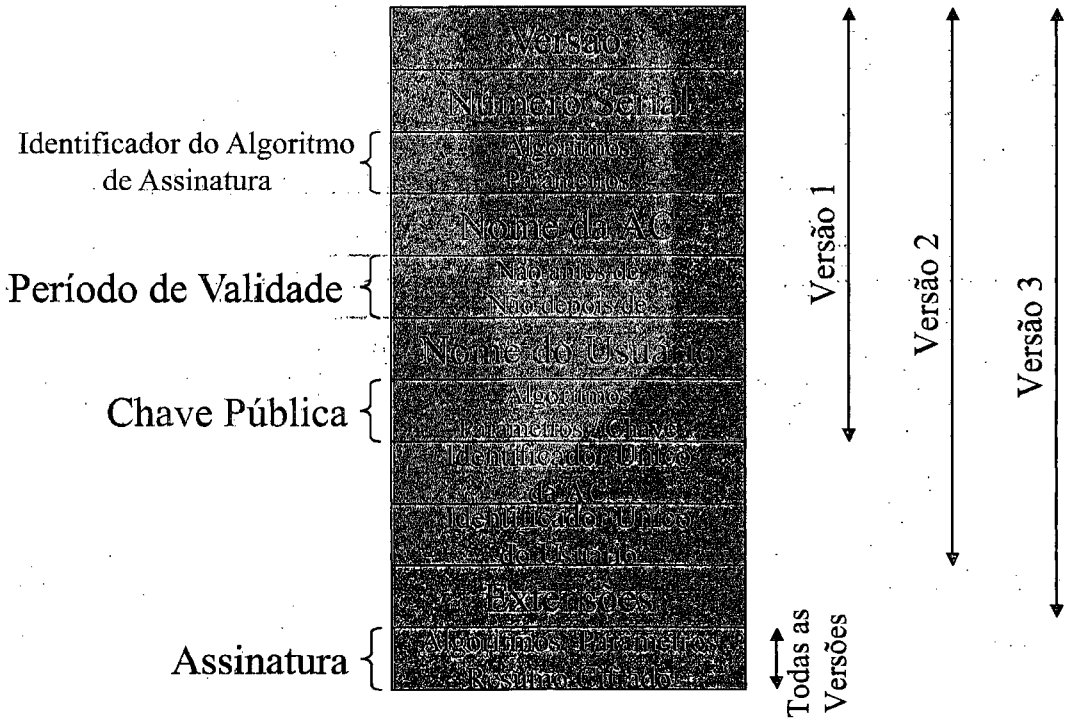

Figura 2.5: Estrutura de um certificado digital. Além dos dados como nome e período de validade, pode-se incluir extensões que adicionam peculiaridades aos certificados. Todas as informações do certificado estão assinadas pela AC.

2.7 Infra-estrutura de Chaves Públicas - ICP

A Infra-estrutura de Chaves Públicas é um conjunto de ferramentas e processos para a implementação e a operação de um sistema de emissão de certificados digitais baseado em criptografia de chave pública [FEG 99] [ADA 99b]. Engloba também os detalhes do sistema de credenciamento e as práticas e políticas que fundamentam a emissão de certificados e outros serviços relacionados.

De forma genérica, para a emissão de um certificado digital existe a necessidade de três módulos, conforme ilustra a figura 2.6. O primeiro é o módulo público, é onde ocorre a requisição de um certificado, bem como a geração do par de chaves, o segundo módulo é a Autoridade de Registro, que envia a requisição, assinada por ele, para a Autoridade de Certificação e a Autoridade de Certificação por sua vez emite um certificado digital, disponibiliza-o em um diretório público.

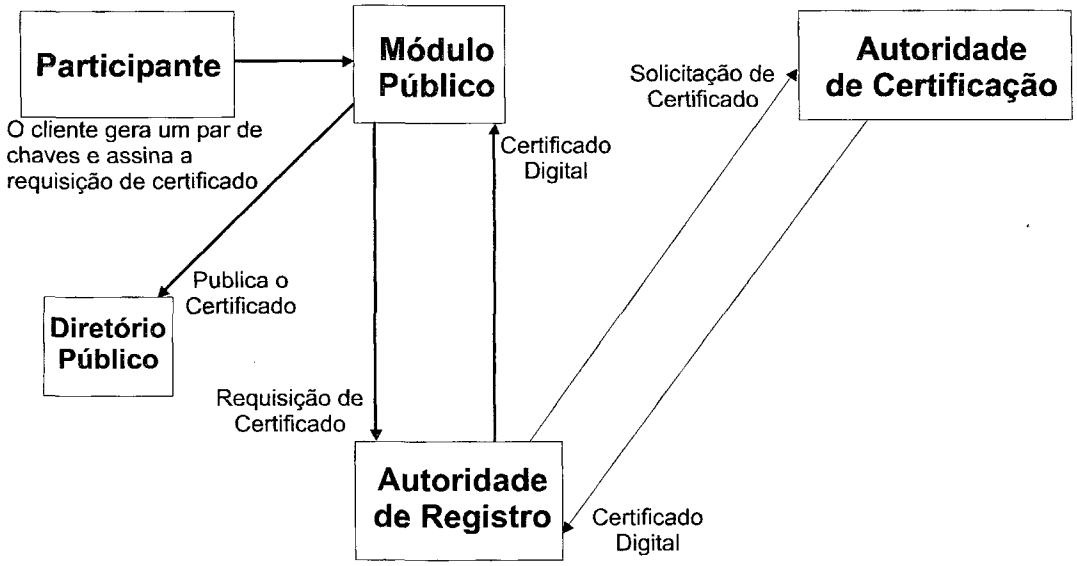

Figura 2.6: Infra-estrutura de chave pública para obtenção de certificado. O participante insere seus dados em um módulo público. Estes dados são autenticados pela Autoridade de Registro, que verifica e autentica a identidade do usuário. Com base nesta autenticação, a Autoridade de Certificação expede o certificado e o disponibiliza em um diretório público.

2.8 Conclusão

Para se propor um protocolo de datação seguro é necessário utilizar conceitos de criptografia assimétrica, funções resumo, assinatura digital, certificado digital e a infra-estrutura de chave pública, para a emissão e controle dos certificados digitais.

Mas, a utilização destes fundamentos não garante por si só segurança. Precisa-se de uma metodologia que defina a seqüência de passos a serem executados para a realização de uma datação digital.

Capítulo 3

Métodos de Datação Eletrônica

Neste capítulo são descritos os métodos de datação de documentos eletrônicos citados na literatura, um exemplo de um sistema de datação que pode ser usado em uma implementação real e algumas vulnerabilidades muito comuns em uma Autoridade de Datação - AD.

3.1 Introdução

Existem dois tipos de técnicas de datação: aquelas que trabalham com uma entidade confiável chamada de Autoridade de Datação - AD (*Time-Stamping Authority*) e aquelas que são baseadas no conceito de confiança distribuída [BEN 94] [BEN 92]. Técnicas baseadas em AD confiam na imparcialidade da entidade encarregada da datação. Já a técnica baseada na confiança distribuída consiste em datar e assinar o documento por várias entidades de um grupo de modo a convencer o verificador que não se poderia corromper as entidades simultaneamente [MAS 99] [JUS 98a].

Um bom método de datação deve atender os seguintes requisitos de segurança:

1. **Privacidade**: Ninguém além do cliente pode ter acesso ao conteúdo do documento;
2. **Praticidade**: Deve ser prático datar o documento independentemente de seu tamanho;

3. **Integridade**: Deve-se garantir a integridade dos dados e a operação ininterrupta do serviço de datação;

4. **Anonimato**: Deve-se garantir o anonimato do cliente.

5. **Confiança**: Deve-se garantir que um documento será datado com a data e hora correta;

As técnicas baseadas em AD são mais indicadas do que as técnicas baseadas em confiança distribuída para o atendimento destes requisitos, já que a ultima é mais propícia a erros na comunicação devido aos vários caminhos que o documento tem que tramitar para ser datado.

Uma maneira de datar um documento é enviá-lo para uma AD. A AD acrescenta data e hora no documento, armazena uma cópia que será utilizada em caso de disputa e devolve um recibo indicando que o documento foi datado. Este não é um bom procedimento já que não atende aos requisitos de privacidade uma vez que a AD fica conhecendo o documento e o de praticidade uma vez que todo o documento deve ser transmitido e armazenado [HAB 91]. Este será um problema caso o documento seja muito grande.

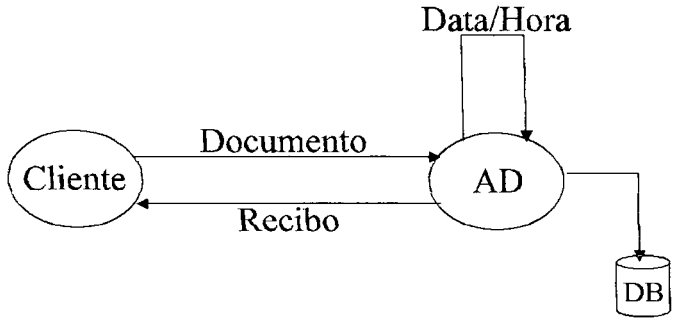

Figura 3.1: O cliente envia para a AD o seu documento para ser datado. A AD por sua vez anexa data e hora ao documento, armazena um cópia em seu banco de dados e remete um recibo para o cliente.

Para resolver este problema pode-se utilizar um resumo do documento, conhecido como *hash*. O *hash* representa de forma única um documento. Os mais conhecidos são o MD5 e o SHA-1 com tamanhos de 128 e 160 bits respectivamente[STA 98].

Assim, ao invés de se transmitir o documento, o cliente transmite o resumo, atendendo aos requisitos de privacidade e praticidade, pois o tamanho do resumo é muito menor que o do documento.

Outro aperfeiçoamento que pode ser realizado é adicionar assinatura digital ao esquema [HAB 95], ou seja, quando o resumo do documento chega para ser datado, a AD anexa data e hora ao resumo, assina e o envia ao cliente do serviço. O cliente por sua vez verifica a assinatura e tem certeza de que o resumo que ele enviou foi realmente o resumo que foi enviado para a AD. Com isso garante-se também o requisito de integridade.

Existem várias formas de resolver o requisito de anonimato. Este trabalho não trata deste requisito em particular. O anonimato não invalida o cumprimento dos outros requisitos de segurança. O anonimato pode ser visto como um complemento desejável, existindo muitas situações onde não há a sua necessidade.

O requisito de confiança pode ser atendido se a AD é considerada confiável. Isso pode ser obtido, na prática, tendo-se um equipamento lacrado e passível de auditoria. Contudo, o lacre e a auditoria implicam em custos e possibilidade de fraudes, provocando uma desconfiança por parte do cliente. Na realidade, o uso de auditoria só transfere a dependência de confiança a uma terceira entidade, neste caso o auditor. O ideal seria que a AD não pudesse ser maliciosa, mesmo que seu administrador o fosse.

Este capítulo esta dividido da seguinte forma: a seção 3.2 descreve como os documentos recebem autenticação temporal; a seção 3.3 descreve quais são os requisitos de um sistema de datação deve atender para garantir sua responsabilidade; a seção 3.4 demonstra como o esquema de encadeamento linear funciona; a seção 3.5 descreve o encadeamento em árvore; a seção 3.6 demonstra como um sistema real de datação pode ser definido; a seção 3.7 expõe como o encadeamento binário foi implementado; a seção 3.8 define um possível ataque que pode ser empregado para tentar invalidar recibos ou até mesmo validar recibos maliciosos na cadeia de verificação; já na seção 3.9 será visto como algumas empresas implementam suas soluções de datação digital.

3.2 Autenticação temporal relativa

Em um sistema de datação de documentos eletrônicos deve-se levar em consideração a questão temporal, ou seja, como o documento recebe a autenticação de data e hora. Ela pode ser **absoluta** ou **relativa**. A autenticação temporal absoluta contém informações de data e hora reais igual a que é usado, no mundo real. Já a autenticação temporal relativa contém informações que somente verifica se um documento foi datado antes ou depois de um outro documento [ROO 99] [JUS 98a].

Os dois esquemas temporais podem ser usados para se datar documentos, mas o esquema absoluto pressupõe que a AD seja confiável. Para o esquema relativo não é necessário confiar cegamente na AD, pois existem mecanismos que garantem que a AD não possa ser maliciosa, ou seja, o documento sempre será datado com data e hora correta.

Uma função de autenticação temporal relativa pode ser definida como: seja H uma função resumo. Um esquema de encadeamento L é um procedimento para encadear uma família H_n de itens de dados usando itens de encadeamento auxiliares L_n, satisfazendo a equação recursiva:

$$L_n = H(H_n, L_{n-1}, ..., L_{n-m}) \tag{3.1}$$

onde m é o tamanho da cadeia de encadeamento que também pode ser chamado de tamanho da cadeia de verificação.

No contexto de datação de documentos eletrônicos, o resumo do n-ésimo documento submetido a AD é H_n, onde $H_n = H(X_n)$. O item de encadeamento L_n é também referente ao resumo do n-ésimo documento. Note que a relação entre L_n e um $L_{n'}$ qualquer onde (n < n'), não prova que no momento da criação do documento X_n o documento $X_{n'}$ não existia. Tudo que se sabe é que L_n existia no momento da criação de $L_{n'}$ [LIP 99].

Usando a autenticação temporal relativa é possível determinar não apenas o momento da submissão do documento à AD mas também um período de tempo onde foi realizado a assinatura do mesmo. Antes de assinar o documento X, Alice gera o

resumo H do documento e o envia para a AD para ser datado. Ela então anexa o recibo *L(H)* de H no documento, assina e o envia para a AD, obtendo o recibo *L(X')* da assinatura $sig_A = (L(H), X)$. Do ponto de vista da AD estas duas submissões de datação são executadas da mesma forma, pois ela não faz distinção de documentos. Como existe uma dependência unidirecional entre *L(H),X* e *L(X')*, o verificador conclui que a assinatura foi criada dentro da janela de tempo definida pelos momentos de criação de *L(H)* e de *L(X')* respectivamente. Com isto, pode-se determinar aproximadamente, quando o documento foi assinado desde a criação de H. Este procedimento é ilustrado na figura 3.2

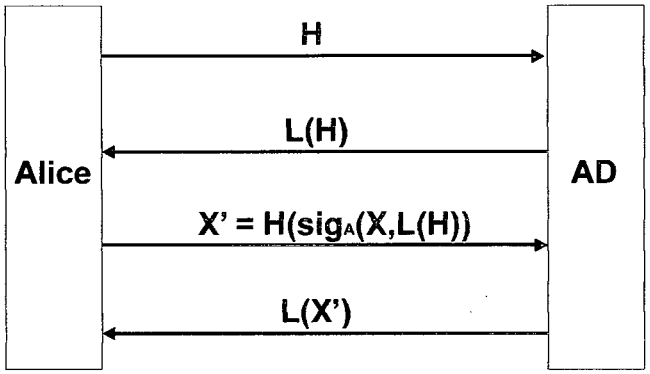

Figura 3.2: Dupla datação de um documento usando o esquema de autenticação relativa. Alice gera o resumo H do documento e o envia para a AD para ser datado. A AD retorna para Alice o recibo *L(H)* do resumo do documento. Alice então anexa o recibo *L(H)* ao documento X, assina e o envia para a AD. A AD produz *L(X')* da assinatura $sig_A = (L(H), X')$.

3.3 Sistemas de Datação

Um sistema de datação que é utilizado em situações reais consiste em uma tripla de protocolos (S,V,A). O protocolo de datação (*Stamping Protocol - S*) permite a cada usuário submeter um documento qualquer para ser datado. O protocolo de verificação (*Verification Protocol - V*) é usado por uma terceira entidade que tem posse de dois recibos para verificar a ordem temporal relativa entre eles. O protocolo de auditoria (*Audit Protocol - A*) é usado pela entidade responsável em prestar o serviço de datação

para verificar se a AD está fazendo o que ela tem que fazer, datar documentos com data e hora corrente [BUL 98b] [JUS 98b].

Uma Autoridade de Datação deve atender a alguns requisitos de segurança e de implementação:

- **Segurança**:
  - **Privacidade**: Ninguém além do cliente pode ter acesso ao conteúdo do documento;
  - **Anonimato**: Deve-se garantir o anonimato do cliente no ato da datação do documento.
  - **Imparcialidade**: A AD não deve considerar no ato da datação nenhuma informação referente ao cliente além do resumo do documento.
  - **Confiabilidade**: Deve-se garantir que um documento será datado com a data e hora correta;
- **Implementação**:
  - **Desempenho**: A AD deve utilizar métodos de datação que se utilizem do conceito de rodadas. A rodada visa agilizar e proporcionar uma maior velocidade de verificação.
  - **Escalabilidade**: O método que a AD utiliza para encadear as datações deve ser flexível o bastante para suportar a inclusão de novas AD's em sua comunidade, e estas novas AD's devem, de alguma forma, se relacionar com a AD.
  - **Verificabilidade**: A AD deve adotar um método que propicie um ambiente onde o verificador possa, de uma maneira fácil e eficiente, verificar algum recibo em particular dentro de uma enorme gama de encadeamentos.
  - **Flexibilidade**: O método de datação deve ser flexível na definição de quando e como as rodadas devem executar.

- **Auditoria**: Existem dois tipos de auditoria: externa e interna. A auditoria externa usa somente as informações contidas nos recibos e nas informações publicadas pela AD em um diretório público. A auditoria interna usa informações internas armazenadas na AD como as logs e o próprio encadeamento. Devido a isto a AD deve ser protegida com lacres e deve estar em um lugar seguro para que ninguém não autorizado tenha acesso a máquina.

As principais obrigações de uma Autoridade de Datação são :

- Não deve identificar o cliente que está requisitando o seu serviço de datação;
- Deve executar datações em rodadas, que são períodos de tempo bem definidos ou quantidades de solicitações máximas;
- Deve processar a requisição de datação assim que ela chega na AD;
- Deve assegurar as informações de cada rodada encadeando-as com o recibo da rodada anterior;
- Por definição, deve esperar até o fechamento da rodada para efetivar o encadeamento com a rodada anterior;
- Deve datar os documentos que são submetidos à rodada com a data e hora do fechamento da rodada e não com a data e hora da submissão da solicitação de datação;
- O valor de cada recibo de rodada deve ser armazenado em um banco de dados e deve estar disponível para o verificador poder verificar os recibos;
- Cada valor publicado pela Autoridade em um diretório público deve ser assinado pela mesma, da mesma forma todos os recibos dos usuários também devem ser assinados;
- A periodicidade de publicação no diretório público é definida segundo a política adotada.

O sistema deveria permitir também (1) determinar se um recibo foi alterado e (2) no caso de alteração determinar se a alteração foi feita pela AD. Para tentar aumentar a confiança do usuário para com o processo de datação, deveria ser permitido que os clientes periodicamente inspecionem os encadeamentos relativos produzidos pela AD e no caso de encontrarem algo que não condiz deveria existir mecanismos para averiguar onde o erro ocorreu. Adicionalmente, a AD deve publicar regularmente de uma maneira autentica e segura os recibos da cadeia de encadeamento em um local público para que os usuários possam acessá-los para possíveis verificações [PRE 98].

Mas o maior problema que deve ser tratado pelo sistema é o tempo de verificação de um recibo na cadeia de encadeamento. Seja n o número total de recibos encadeados no momento da execução do protocolo de verificação, temos [BUL 98b]:

- O número de cálculos de funções resumo durante a execução do protocolo de verificação deveria ter um teto igual ou próximo ao da busca binária, *O(log(n))*;
- Deveria existir para o tamanho das rodadas um teto conveniente, de modo que os clientes possam ter seu recibo de datação verificado o mais agilmente possível. Para tanto isto requer que o protocolo de datação também execute com um teto de *O(log(n))*.
- O recibo individual deve guardar o mínimo de informações possíveis de modo a proporcionar uma maior agilidade de busca.

Existem métodos propostos na literatura que procuram atender os requisitos de segurança e implementação definidos anteriormente. Tais métodos serão apresentados e analisados segundo os requisitos propostos.

3.4 Encadeamento linear

Para não ser necessário confiar cegamente na AD, ela poderia encadear todos os resumos dos documentos datados em uma cadeia utilizando uma função resumo H. Neste caso o recibo s de datação para o n-ésimo documento H_n seria [LIP 99]:

$$s = Sig_{AD}(n, t_n, ID_n, H_n, L_n) \tag{3.2}$$

onde Sig_{AD} é a assinatura da AD, t_n é a data e hora corrente, ID_n é o identificador do n-ésimo documento e L_n é a informação do link definido como:

$$L_n = (t_{n-1}, ID_{n-1}, H_{n-1}, H(L_{n-1})) \tag{3.3}$$

onde t_{n-1} e ID_{n-1} são a data e hora e o identificador do documento anterior, o H_{n-1} é o resumo do documento anterior e $H(L_{n-1})$ é o resumo do link anterior. A figura 3.3 dá um exemplo de como seria o encadeamento de 9 elementos.

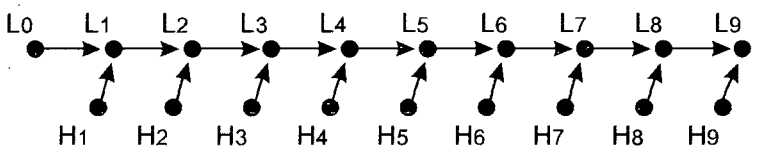

Figura 3.3: Encadeamento Linear. Ao começar o processo de encadeamento a AD gera um número randômico e assume que aquele número é o primeiro elemento da cadeia, L_0. Quando o primeiro resumo, H_1, chega para ser datado, a AD calcula o próximo elemento da cadeia L_1 segundo a equação 3.3, assina um recibo contendo as informações definidas pela equação 3.2 e o envia para o cliente.

Com isto, associa-se a datação atual com a anterior afim de se obter uma seqüência de recibos ordenados por ordem de chegada, resolvendo então problemas de disputa, já que se consegue identificar se um documento foi datado antes do outro.

Mas existem alguns problemas com esta implementação. Um deles é o tempo que é gasto na verificação do relacionamento entre dois recibos, que é diretamente proporcional ao número de recibos encadeados. Outro, é a questão de confiabilidade por parte da AD, por exemplo, se dois documentos chegarem nos tempos t1 e t2, a AD não deve gerar o recibo de datação para o documento que chegou em t2 antes de ter gerado para o documento que chegou em t1.

Tabela 3.1: Tabela do Encadeamento Linear

Requisito	**Análise**
Privacidade	Atende
Anonimato	Não atende
Imparcialidade	Atende
Confiabilidade	Atende
Desempenho	Não atende
Escalabilidade	Não atende
Verificabilidade	Não atende
Flexibilidade	Não atende
Auditoria (Externa/Interna)	Somente Auditoria Interna

3.5 Encadeamento em árvore

Com o objetivo de agilizar o processo de verificação e adicionar mais segurança ao método de encadeamento linear foi criado uma generalização, chamada de encadeamento em árvore. A idéia deste esquema de datação é dividir o encadeamento em unidades de tempo denominadas rodadas.

O tamanho de uma rodada pode ser definida como o quantidade máxima de solicitações ou o tempo máximo que a rodada pode ficar aberta para receber solicitações de datação. O objetivo de uma rodada não é exatamente para atender algum requisito de segurança, mas sim atender o requisito de implementação chamado desempenho, pois a criação de rodadas dentro do encadeamento propicia ao verificador um ambiente onde ele pode dar saltos entre as rodadas não precisando se preocupar com os encadeamentos dentro da rodada, agilizando assim a verificação de recibos.

No método de encadeamento em árvore a criação de cada rodada é definida da seguinte maneira: em cada rodada podem ser submetidos à AD vários pedidos de datação até um determinado tempo, e ao final, é gerado um recibo que representa todos os pedidos submetidos naquela rodada. Isto é representado através da criação de uma árvore, onde suas folhas são os pedidos submetidos na rodada e seus nós são calculados através de uma função F, a qual pode ser definida como sendo uma função resumo, um XOR ou uma operação que seja unidirecional [LIP 99].

Cada participante que queira datar pelo menos um documento na rodada

r, envia para a AD o resumo de seu do documento, definido aqui como y_{ri}. As folhas da árvore são formados por diferentes y_{ri}. Cada nó k da árvore é definido como $F_k = (F_{kL}, F_{kR})$, onde k_L e k_R são os nós esquerdo e direito, respectivamente, ao nó k.

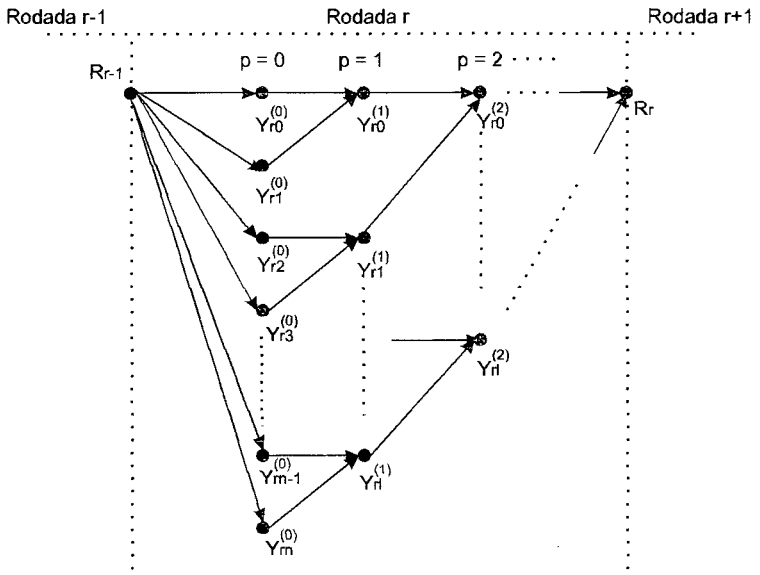

Figura 3.4: Encadeamento em árvore. A AD ao receber um resumo o encadeia com o recibo de rodada R_{r-1}, através da função F. Ao final da rodada r, cada y_{ri}^0 é encadeado de dois em dois através da função F de modo a gerar os y_{ri}^1, até que restem apenas dois, os quais vão gerar o recibo de rodada R_r para a rodada r.

A figura 3.4 ilustra o processo descrito acima, ou seja, o ponto de partida para a criação da árvore são os resumos que são submetidos à AD naquela rodada, conseqüentemente são calculados os valores de cada nó aplicando-se a função F nos nós folhas y_{ri} pegos dois a dois, e assim por diante, como é visto na ilustração, onde m é o número de solicitações submetidas a AD, p é o índice do nível da árvore que varia entre $0 <= p <= (m)div(2)$, y_{ri} são os valores dos respectivos nós decorrentes da operação da função F, ou seja:

$$y_{ri}^{(p)} = F(y_{r(2i)}^{(p-1)}, y_{r(2i+1)}^{(p-1)}), se/; p = 0, y_{ri}^{(0)} = y_{ri} \tag{3.4}$$

e l é o índice máximo de $y_{ri's}$ contidos em cada etapa e é definido como sendo:

$$l = [(n+1)div(2p)] - 1 \tag{3.5}$$

Esta técnica permite ainda que se possa criar variações no método de encadeamento da árvore [LIP 99], visto que o recibo anterior R_{r-1} pode ser associado a qualquer nó da árvore ou até ser associado diretamente com o recibo atual R_r, possibilitando que o verificador checar imediatamente a relação de dependência entre dois R_i sem examinar os recibos contidos na rodada r, como pode ser visto na figura 3.5 .

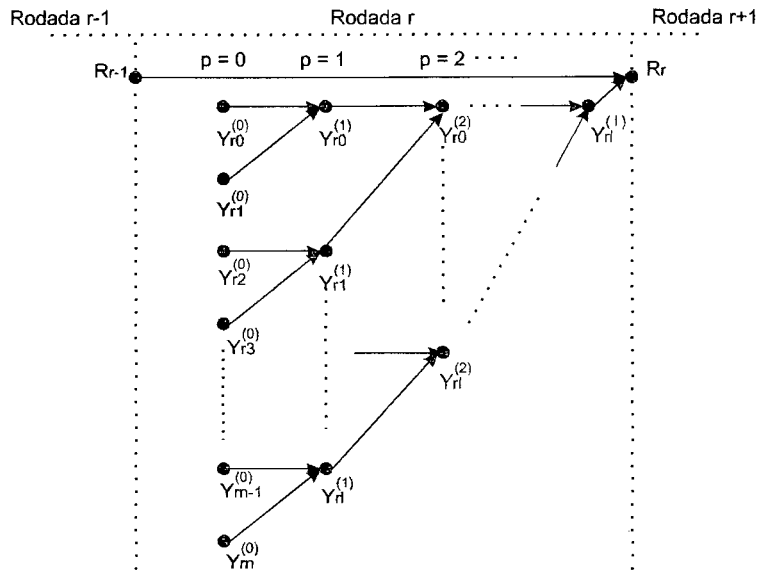

Figura 3.5: Um outro tipo de encadeamento em árvore. A diferença deste esquema de encadeamento é que o recibo de rodada R_{r-1} da rodada anterior não é encadeado imediatamente nos resumos submetidos, mas encadeado com o recibo de rodada R_r da rodada r.

Uma outra diferença entre as duas variações é o número de operações da função F na criação da árvore. Note que na primeira variação, figura 3.4, a função F é aplicada em cada solicitação de datação submetida à AD e na criação de cada nó da árvore, totalizando $n + (n - 1)$ operações, onde n é o número de solicitações de datação. Já na segunda variação o número é de n operações, pois cada solicitação não é mais encadeada com o recibo de rodada R_{r-1}.

Para a verificação de um resumo específico, por exemplo y_{r3}, o verificador calcula $R_r = F(F(F(y_{r0}, y_{r1}), F(y_{r3}, y_{r4})), R_{r-1})$; se for igual, o resumo y_{r3} realmente pertence a rodada r. Aqui o tempo gasto para a verificação é bem menor do que

no encadeamento linear, pois a procura de um recibo é feita somente em uma rodada e não na cadeia inteira como é no método linear.

Tabela 3.2: Tabela do Encadeamento em árvore

Requisito	**Análise**
Privacidade	Atende
Anonimato	Não atende
Imparcialidade	Atende
Confiabilidade	Atende
Desempenho	Atende
Escalabilidade	Não atende
Verificabilidade	Não atende
Flexibilidade	Não atende
Auditoria (Externa/Interna)	Somente Auditoria Interna

3.6 Um exemplo de um sistema de datação

Para a implementação de um sistema se datação pode ser usada qualquer técnica. Neste caso o esquema adotado foi o de encadeamento linear com algumas modificações, por exemplo, a criação de rodadas, de modo que ele atenda a todos os requisitos propostos na seção 3.3. Porem este sistema é impraticável, pois seu tempo de verificação é muito grande [BUL 98c] [BUL 98b] [BAY 91].

Seja M um número constante de recibos submetidos para a rodada e todos os ítens de dado $H(X_n)$ forem do mesmo tamanho, então no caso do encadeamento linear o recibo para a rodada r tem o identificador $\xi_r = M.r$, onde ξ_r é o recibo que representa todos as solicitações de datação submetidas a AD na rodada r.

3.6.1 O papel da Autoridade de Datação

A AD mantém as seguintes bases de dados:

1. a base *Dc* dos recibos da rodada corrente;

2. a base *Da* dos recibos da rodada anterior;

3. a base *Dr* das solicitações de datação na rodada r;

4. a base *Dt* de todos os recibos.

Estas base de dados devem estar disponíveis para que um cliente possa fazer requisições e verificações a estas bases a qualquer momento. A quarta base, que consiste nas informações de todos os recibos datados, é também mantida pela AD, mas ela não se encontra on-line.

3.6.2 Protocolo de datação

O protocolo de datação para a rodada *r* é:

1. o cliente envia o resumo $H(X_n)$ do documento X_n;

2. a AD calcula o $H_n = H(n, X_n)$ e o $L_n = (H_n, L_{n-1})$;

3. a AD assina o par (n, L_n) e envia $(n, L_n, sig_{AD}(n, L_n))$ para o cliente;

4. a AD envia a tupla $head(n) = (H_{n-1}, H_{n-2}, ..., H_{\xi_{r-1}+1})$;

5. o cliente verifica a assinatura da AD e checa se:

$$H(H_n, H(H_{n-1}, ..., H(H_{\xi_{r-1}+1}, L_{\xi_{r-1}})...)) = L_n \tag{3.6}$$

onde L_ξ pode ser achado no diretório público da AD, ou seja, na base *Dr*.

Após M pedidos a AD termina a rodada calculando $L_{\xi_r} = H(H'_{\xi_r}, L_{\xi_{r-1}})$, onde $H'_{\xi_r} = H(H_{\xi_r}, L_{\xi_r-1})$, e publica no diretório público o L_{ξ_r} e seu certificado digital contendo sua chave pública K_{AD}. O cliente a partir deste momento quando surgir uma situação de disputa ou de verificação entre dois recibos ele pode proceder mais alguns passos:

6. o cliente envia uma solicitação à AD para completar seu recibo com as informações adicionais de sua rodada;

7. seja $tail(n) = (H_{\xi_r-1}, H_{\xi_r-2}, ..., H_{n+2}, H_{n+1})$. A AD envia a resposta para o cliente $(tail(n), sig_{AD}(tail(n)))$;

8. o cliente verifica se:

$$L_{\xi_r} = H(H_{\xi_r-1}, H(H_{\xi_r-2}, ..., H(H_{n+2}, H(H_{n+1}, L_n))...)); \quad (3.7)$$

9. o recibo completo do cliente s_n é:

$$s_n = (tail(n), head(n), n, L_n, sig_{AD}(n, L_n)) \quad (3.8)$$

3.6.3 Protocolo de verificação

Seja *r(n)* a rodada onde s_n é válido. Assume-se que o verificador tem dois recibos de dois documentos (X_m, s_m) e (X_n, s_n), onde $m < n$.

1. o verificador checa a igualdade das equações *3.6* e *3.7* para os dois recibos;

2. se *r(m) = r(n)* então o dado assegurado por *tail(m)* e *head(n)* serão suficientes para a verificação:

$$L_n = H(H_n, H(H_{n-1}, ..., H(H_{m+1}, L_m)...)) \quad (3.9)$$

3. se *r(m) < r(n)*, o verificador envia um pedido para a AD;

4. a AD responde enviando a tupla assinada $sig_{AD}(v_{mn})$:

$$v_{mn} = (H'_{\xi_{r(n)}-1}, H'_{\xi_{r(n)}-2}, ..., H'_{\xi_{r(m)}}) \quad (3.10)$$

5. o verificador valida a assinatura, calcula $L_{\xi_{r(m)}}$ usando a equação *3.7*, calcula $L_{r(n)-1}$ usando a seguinte equação:

$$L_{r(n)-1} = H(H'_{\xi_{r(n)-1}}, H(H'_{\xi_{r(n)-2}}, ..., H(H_{\xi_{r(m)}}, L_{\xi_{r(m)}})...)) \quad (3.11)$$

E finalmente, compara o valor de L_n em s_n com o valor dado pela equação *3.6*. Se for igual, significa que realmente *r(m) < r(n)*.

3.6.4 Protocolo de auditoria

Por causa da possível importância legal dos recibos assegurados pela AD devem existir mecanismos para efetuar algum tipo de auditoria no sistema. Um modo fácil de se fazer isto é periodicamente verificar de forma aleatória alguns recibos da AD. Se eles estiverem encadeados inconsistentemente, então a AD agiu maliciosamente e não pode ser considerada confiável.

Existe dois tipos de auditoria: externa e interna. A auditoria externa usa somente as informações contidas nos recibos e nas informações publicadas pela AD em um diretório público. A auditoria interna usa informações internas armazenadas na AD como as logs e o próprio encadeamento. Devido a isto a AD deve ser protegida com lacres e deve estar em um lugar seguro para que ninguém não autorizado tenha acesso a máquina.

- **Auditoria Externa**
  - **Vantagens**:
    1. A AD não precisa guardar uma enorme gama de informações;
    2. Não se precisa confiar cegamente na AD;
    3. No momento da verificação não se precisa consultar a AD;
    4. A AD não precisa ser necessariamente lacrada e nem se precisa realizar verificações constantes na máquina para se garantir confiabilidade;
    5. Não se precisa gastar recursos financeiros e nem humanos para administrar a AD;
    6. Torna as atividades da AD totalmente transparente;
  - **Desvantagens**:
    1. O recibo contém muitas informações, aumentando assim seu tamanho físico;
- **Auditoria Interna**
  - **Vantagens**:

1. O recibo contém somente informações pertinentes ao seu encadeamento, diminuindo assim seu tamanho;

– **Desvantagens**:

1. A AD precisa ser lacrada e precisa estar em um lugar fechado e seguro;
2. Se precisa confiar cegamente na AD;
3. A AD precisa administrar uma enorme gama de informações, conseqüentemente e precisa-se de uma máquina um pouco mais robusta;
4. Aumento no custo de pessoal especializado para realizar auditorias constantes na AD;

Um método adicional de auditoria seria criar um algoritmo que faça uma varredura na árvore de encadeamento, de modo a realizar uma busca por possíveis ramos maliciosos, que por ventura foram criados por algum tipo de vulnerabilidade do sistema.

Pode-se também, verificar a integridade dos encadeamentos dos recibos na hora da efetivação destas informações no banco off-line mantido na AD. Com isto pode-se detectar possíveis ramos maliciosos que tenham ocorridos naquela rodada.

3.7 Encadeamento binário

O sistema acima descrito pode ser usado em situações reais, mas é impraticável, pois seu tempo de verificação é muito grande. Com o intuito de diminuir o tempo gasto na verificação foi desenvolvido um esquema binário de encadeamento, que pode ser definido como sendo um grafo direcionado não cíclico, onde todos os vértices tem pelo menos duas arestas. A construção de tais grafos se dá da seguinte forma [BUL 98b]:

- T1 consiste de um simples vértice o qual é denominado com o número 1. Este vértice é ao mesmo tempo a origem e o final do grafo;
- Seja T_k um grafo que já foi formado anteriormente. Seu final é denominado de $2^k - 1$. O grafo T_{k+1} consiste de duas cópias de T_k, onde o final da segunda cópia

é encadeada com a origem da primeira cópia, e um vértice adicional denominado de $2^{k+1} - 1$, que é encadeado com a origem da segunda cópia. conforme ilustra a figura 3.6.

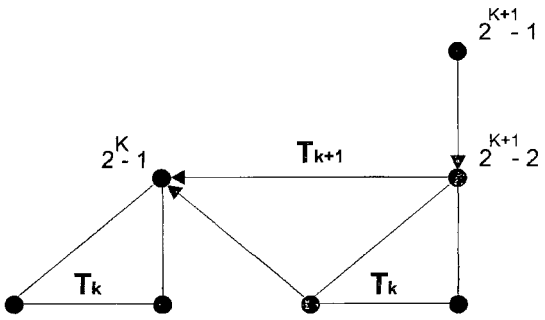

Figura 3.6: Encadeamento binário.

Após a construção deste esquema de encadeamento binário, são adicionados encadeamentos adicionais das origens de qualquer segmento inicial com um vértice especial chamado 0, como mostra a figura 3.7

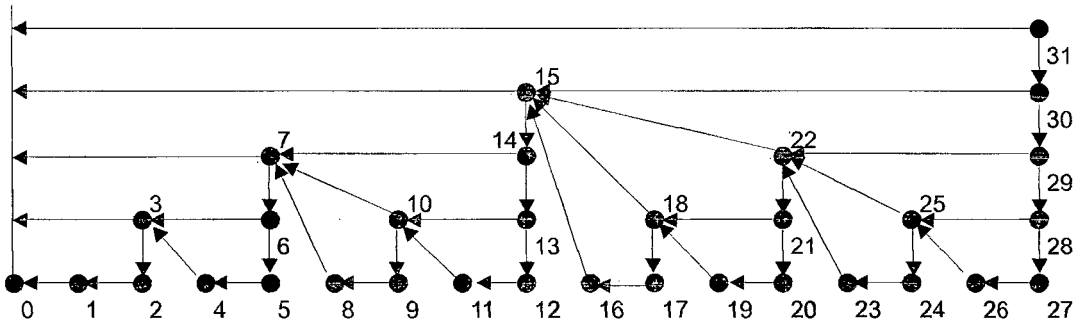

Figura 3.7: Estrutura de datação com o encadeamento binário.

3.8 Possíveis vulnerabilidades no esquema de encadeamento

Já que todos os recibos datados precisam da assinatura da AD, este tipo de ataque precisaria da colaboração da mesma para assinar falsos recibos que serão

Tabela 3.3: Tabela do Encadeamento Binário

Requisito	**Análise**
Privacidade	Atende
Anonimato	Não atende
Imparcialidade	Atende
Confiabilidade	Atende
Desempenho	Atende
Escalabilidade	Não atende
Verificabilidade	Atende
Flexibilidade	Não atende
Auditoria (Externa/Interna)	Somente Auditoria Interna

anexados de alguma forma na cadeia de encadeamento. Na figura 3.8 é apresentado o ataque à árvore de encadeamento, onde com a participação da AD pode-se inserir um recibo inválido na cadeia criando mais um ramo na árvore [JUS 98b].

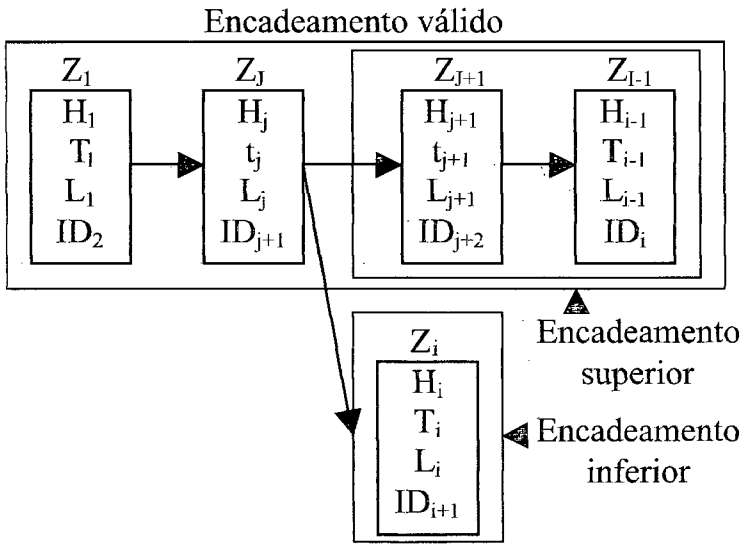

Figura 3.8: Demonstração da vulnerabilidade da árvore de encadeamento.

O ataque procede com o usuário u_i em conjunto com a AD para datar um documento y_i, o qual gera um recibo z_i. Na figura 3.8, o recibo z_i deveria aparecer imediatamente depois do recibo z_{i-1}, considerando o esquema liner de encadeamento. No entanto, z_i aparece imediatamente depois de z_j. Suponha que z_j, z_{j+1} e z_{i-1} tem os respectivos tempos t_j,t_{j+1} e t_{i-1}, onde $t_j < t_{j+1} < t_{i-1}$. Se o recibo z_i estivesse no lugar

correto, depois de z_{i-1}, teria-se $t_i > t_{i-1}$, mas colocando-o depois de z_j, pode-se associar qualquer tempo t_i para o documento y_i, de modo que $t_i > t_j$ [JUS 98b].

Subseqüentemente os novos documentos que chegarem à AD poderão ser encadeados nesta nova cadeia criada pelo recibo z_i.

Agora suponha que alguém queira verificar o recibo z_i. Se ele executar o protocolo de verificação ele não poderá descobrir a falha na cadeia de encadeamento e acabará concluindo que aquele recibo z_i é autentico. No entanto, se o verificador de alguma forma aplicar o protocolo de modo que ele comece pelo último recibo, ele vai descobrir que z_j nomeado como u_j foi previamente dado pelo ID_{j+1} e não por ID_i, mas ainda resta outras armas para o atacante:

- AD e u_i podem se juntar com u_j para que ele pegue ID_i em vez de ID_{j+1};
- Gerar $ID_{j+1} = ID_i$. Isto pode ser feito desde que u_i periodicamente date documentos. Subseqüentemente, u_i pode criar encadeamentos falsos em qualquer lugar onde seus recibos estejam localizados, mas tudo isto só é possível com a ajuda da AD.

3.9 Empresas que implementação soluções de Datação Digital

Com o intuito de suprir a necessidade crescente de datadoras digitais, algumas empresas se lançaram na frente e implementaram suas próprias soluções.

3.9.1 Surety

Surety é uma empresa que presta serviço de datação digital de documentos. Seu serviço disponibiliza um garantia de existência de qualquer tipo de dado digital em um dado momento. Uma vez protocolado, o recibo é facilmente verificado [SUR].

Para se datar os documentos o serviço se utiliza de duas técnicas criptográficas já citas: funções resumo e o esquema de encadeamento em árvores. O cenário do serviço de datação é definido da seguinte maneira:

- **Cliente**: o software cliente gera o hash do documento que vai ser protocolado e o envia assinado digitalmente pelo cliente;
- **Servidor de datação**: recebe os pedidos dos clientes, verifica, consultando o servidor de validação, se a assinatura é legítima e válida, guarda todas as requisições dos usuários até que o grupo tenha um certo tamanho definido, gera a árvore de resumos e calcula o resumo da rodada, submete o resumo calculado para o servidor de coordenação para o encadeamento e datação, o resultado gerado então retorna para o servidor e é gerado um recibo para o cliente;
- **Servidor de validação:** recebe a solicitação do servidor de datação e se comunica com o servidor de contas para verificar se a conta do usuário está ativa e verifica se a assinatura digital é válida e legítima;
- **Servidor de contas:** guarda as informações dos usuários;
- **Servidor de coordenação:** recebe o hash calculado do servidor de datação e o encadeia através de um xor com o hash anterior, então é gerado um novo valor, o qual é anexado data e hora e enviado para o servidor de datação;

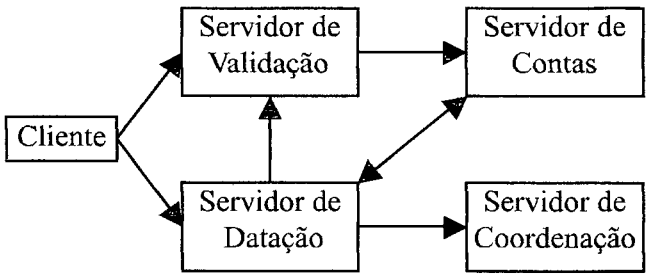

Figura 3.9: Arquitetura dos servidores da Surety.

3.9.2 TimeProof

A TimeProof desenvolve e confecciona sistemas de assinaturas temporais para [TIM]:

- Autoridades de certificação;
- Provedores de serviço de protocolação;
- Companhias que autenticam suas transações eletrônicas.

Na verdade esta empresa fabrica um hardware capaz de datar documentos eletrônicos. Esta caixa preta (Trust Box, como eles definem), garante que mesmo que a data seja manipulada, o processo continua com a mesma precisão. Ela funciona em parceria com o software que é instalado no servidor, e este tem as funções de conectar o hardware à rede e logar todos os eventos de datação.

A TimeProof disponibiliza três tipos de hardware para seus clientes:

- TSS 380: foi desenvolvido para serviços comerciais. Este sistema disponibiliza para os usuários um serviço de time-stamp seguro provendo segurança para suas transações na internet.
- TSS400: foi desenvolvido para autoridades de datação, que com ele podem fornecer a seus usuários um serviço de datação seguro. Desta forma pode-se afirmar a existência de um documento em um dado momento e garantir que ele não foi alterado.
- TSS80: habilita a empresas a prover para todos os documentos e todos os processos uma autenticação de serviço temporal.

3.9.3 DATUM

Fundada há 30 anos atrás a DATUM tem uma larga experiência em projeto, desenvolvimento e divulgação em produtos de precisão e freqüência de tempo.

Ela possui várias linhas de produtos, mas uma linha em particular visa atender o ramo de datação digital de documentos, chamada de *Trusted Time* [DAT].

Trusted Time é uma solução de e-business e vai de encontro a dois conceitos: a segurança do recibo gerado e a auditoria do processo. O aspecto segurança atende tanto a integridade e a autenticidade da fonte de tempo para o sincronismo das AD's e a proteção do tempo contido nas AD's. Já a auditoria, apoiada na fonte de tempo segura e nas técnicas criptográficas, tem levantar provas de que o recibo foi realmente datado com dada e hora correta. Vale ressaltar que o equipamento da DATUM somente realiza auditoria interna.

Trusted Time é baseado em uma hierarquia de relógios de rede especializados. Um Instituto Nacional de Medição é escolhido para ser o servidor de tempo seguro. Sua fonte de tempo é inquestionável e é a base de todo o sistema. Abaixo dele existem servidores intermediários, chamados de *Trusted Time Master Clocks*, que são responsáveis em repassar esta fonte segura de tempo para os demais servidores de datação. O *Trusted Time Master Clocks*, cujo o tempo é sincronizado através de um canal seguro com o Instituto Nacional, é responsável em disponibilizar uma fonte segura de tempo para milhares de organizações que tempo um servidor de datação. Este servidor de datação se sincroniza periodicamente de uma maneira segura com o *Trusted Time Master Clock* e é responsável em disponibilizar o serviço de datação para os clientes.

3.9.4 BRy - Tecnologia

A BRy é uma sociedade anônima de capital fechado, brasileira, que tem como missão desenvolver, produzir e comercializar produtos e serviços para garantir a segurança e promover a confiança no novo ambiente virtual de negócios. Sua visão é ser a maior empresa nacional de confiança na área de segurança computacional [TEC].

A BRy é uma empresa totalmente nacional, situada no Pólo Tecnológico de Florianópolis - TECNÓPOLIS e conta com a cooperação tecnológica da Universidade Federal de Santa Catarina através do LabSEC - Laboratório de Segurança em Computação do Departamento de Informática.

A BRy disponibiliza para seus usuários um serviço seguro de protocolação digital de documentos eletrônicos através do BRy PDDE. Este produto/serviço é composto por um conjunto de sistemas computacionais, equipamentos e serviços que permitem às corporações e prestadoras de serviços integrar, em seu ambiente informatizado, os serviços próprios de protocolação digital.

O BRy PDDE é fornecido em módulos que permitem a agregação de funcionalidades conforme as necessidades do cliente. Os módulos são:

- Módulo Básico
- Módulo com Auditoria
- Módulo de Gerenciamento de Usuários
- Módulo de Contabilidade Interface para Aplicações
- Módulo Filtro Firewall

Esta empresa é a primeira no Brasil a disponibilizar uma implementação real e confiável de uma Autoridade de Datação e prestar serviços e desenvolver soluções baseadas em identificação digital.

3.10 Conclusão

Com foi visto os três métodos acima podem ser usados para uma implementação de um sistema de datação, mas cada um deles tem suas peculiaridades:

- **Encadeamento Linear**: este método foi a primeira técnica que foi desenvolvida para tentar deixar de confiar cegamente na AD através de encadeamentos sucessivos de acordo com a ordem de chegada, mas este métodos não é prático devido a possibilidade da AD ser maliciosa ao ponto de trocar a ordem de datação dos documentos submetidos a ela e o tempo elevado de verificação da cadeia de encadeamento, o qual é diretamente proporcional ao tamanho da cadeia.

- **Encadeamento em Árvore**: Com a idéia de dividir as datações em rodadas, o tempo de verificação diminuiu, devido a criação de uma série de ligações entre os recidos de rodada que possibilitam a pessoa que está verificando dar saltos dentro da cadeia de encadeamento agilizando assim o processo. Esta técnica, impede que a AD troque a ordem dos recibos, pois se isto acontecer pode-se facilmente provar que o recibo não foi datado na ordem que devia com o recibo de rodada, o qual representa todos os documentos submetidos em uma rodada qualquer.

- **Encadeamento Binário**: Este método agilizou o processo de verificação, pois pode-se escolher por qual caminho se deseja verificar o recibo. Além disso é possível verificar a veracidade dos encadeamentos, pois pode-se testar todos os caminhos.

Capítulo 4

Método da Árvore Sincronizada para Datação de Documentos Eletrônicos

4.1 Introdução

Este capítulo apresenta um novo método de datação que foi batizado com o nome de Árvore Sincronizada. Com ele tentou-se diminuir o tempo de verificação de um recibo e garante que a AD não possa ser maliciosa, ou seja, o documento sempre será datado com data e hora correta.

4.2 Árvore Sincronizada

Este novo método traz além de uma forma diferente de encadeamento novos conceitos que precisam ser definidos:

- **Rodada**: Neste método a rodada é regida por unidades de tempo bem definidas como segundos e minutos. E as rodadas são flexíveis ao ponto de se criar sobre-rodadas com diferentes unidades de tempo, horas, meses e anos.

- **Recibo**: O recibo de datação do método da árvore sincronizada difere um pouco dos outros recibos dos outros métodos, pois além de retornar os encadeamentos de sua

rodada retorna também todas as informações das rodadas dos pontos de sincronismo anteriores até o ultimo ponto de confiança publicado.

- **Ponto de sincronismo**: Este ponto é definido como sendo o ponto que representa todas as rodadas presentes em um determinado intervalo. Por exemplo, se cada rodada tem um pulso de um segundo e que depois de 60 rodadas, ou seja, 1 minuto um ponto de sincronismo é criado e este ponto representa todas as rodadas presentes neste minuto, exatamente igual o que a rodada é para os encadeamentos. Os pontos de sincronismo são representados por S_i.

- **Ponto de confiança**: O método da árvore sincronizada define como sendo o ponto de confiança o ponto onde ocorreu a última publicação de um recibo que representa todos os encadeamentos desde o último ponto de confiança, ou seja, se a AD definir que a publicação de um ponto de confiança deverá ocorrer ao final de todos os dias, este recibo conterá informações que representam todos os encadeamentos do dia. Após feita a publicação todos os encadeamentos podem ser descartados da AD, pois o ponto de confiança juntamente com o recibo de datação da pessoa contém todas as informações necessárias para a verificação de tal recibo. Os pontos de confiança são representados por C_i

Tendo estas definições em mente e partindo do princípio que todos os resumos que chegam para ser datados são encadeados, e que ao final de um determinado tempo (pulso) é aplicada uma função F em todos estes resumos para gerar um único recíbo que os represente, pode-se montar o seguinte esquema:

1. O participante que queria datar seu documento, gera um resumo e o encaminha para a Autoridade de Datação;

2. Quando um resumo chega para ser datado, ele é encadeado com os outros pedidos, através de um função F, na cadeia de encadeamento;

3. Ao final de cada pulso, por exemplo 1 segundo, é aplicada novamente a função F com o último elemento do encadeamento e com o recibo de rodada R_{r-1} da rodada anterior, gerando assim o recibo atual daquela rodada, como mostra a figura 4.1.

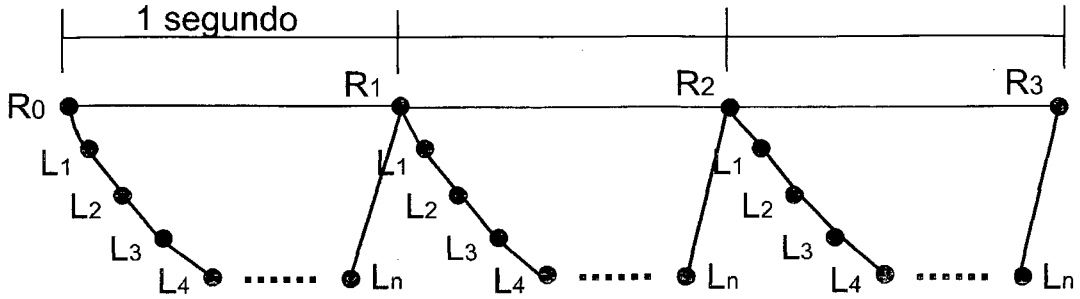

Figura 4.1: Esquema da Árvore Sincronizada. Ao receber um resumo para ser datado, a AD o encadeia através de uma função F com o recibo anterior L_{i-1}. Ao final do pulso a AD encadeia o último L_i gerado naquela rodada com o recibo de rodada R_{r-1} da rodada anterior, gerando o R_r atual.

Cada L_i é a representação de cada resumo encaminhado para a AD encadeado na cadeia de datação através de uma função F. R_0 é o recibo de rodada anterior ao pulso 1 e R_1 é o recibo de rodada atual e assim por diante.

Generalizando o processo, pode-se criar pontos de sincronismo, representando unidades de tempo conhecidas como horas, dias, meses e até anos, e estes pontos representam todas as rodadas contidas em um determinado intervalo de tempo, visando agilizar o processo de busca para se ter um menor tempo de verificação de documentos, já que o verificador pode executar saltos entre um ponto de sincronismo para o outro. Esta generalização pode ser vista na figura 4.2.

Note que tanto o ponto de confiança C_0 ,o ponto de sincronismo S_0 e a rodada R_0 coincidem e portando tem o mesmo valor para o encadeamento, assim como o ponto de sincronismo S_1 com a rodada R_{n+1}.

A verificação pode ser feita realizando uma busca na árvore formada, de acordo com a data e valor que o recibo foi gerado. Por exemplo, para um documento que foi datado em 22/03/2001 as 14:32 PM, a ordem de sua verificação será: ano, mês, dia, hora, minuto e então é verificado se o resumo do documento confere com algum que esteja encadeado naquele minuto. Lembrando que todos os métodos citados até agora, publicam em um diretório público todos os recibos gerados, que é o caso do encadeamento linear, ou os recibos de rodada.

Análise dos requisitos de segurança e de Implementação:

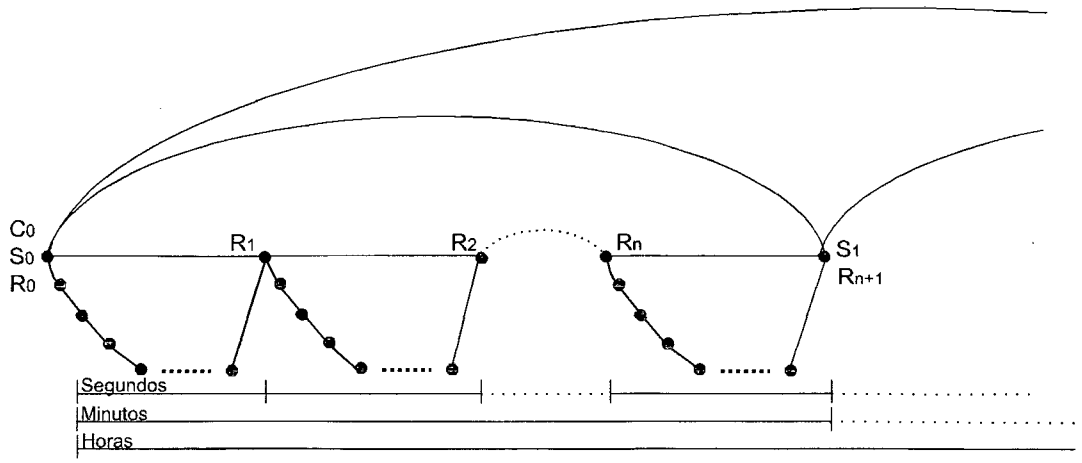

Figura 4.2: Generalização do método Árvore Sincronizada. Como o método trabalha com pontos sincronismo, pode-se definir políticas de encadeamentos maiores do que um simples pulso de 1 segundo, criando um ambiente onde o verificador possa buscar uma determinada informação com muito mais agilidade.

Tendo por base os pontos de confiança publicados e as informações contidas nos recibos dos usuários a auditoria externa pode ser realizada.

Para fins de definição do novo método, a seguir são apresentados os protocolos de datação e verificação. Lembrando que o protocolo de auditoria é flexível e pode ser definido segundo uma política de segurança particular de uma empresa.

4.2.1 Protocolo de datação

Seja T o pulso definido para o fim de uma rodada específica e todos os ítens de dados $F(X_n)$ sejam do mesmo tamanho e R_r é o recibo de rodada para a rodada r, então pode-se definir:

1. o cliente envia o resumo do documento $H(X_n)$;

2. a AD calcula o $F_n = F(X_n)$ e o $L_n = F(F_n, L_{n-1})$;

   Após o pulso T ser finalizado a AD termina a rodada calculando $R_r = F(F'_{R_r}, R_{r-1})$, onde $F'_{R_r} = F(F_{R_r}, L_{R_r-1})$.O cliente a partir deste momento pode receber seu recibo de datação que é gerado pela AD da seguinte forma:

Tabela 4.1: O método da Árvore Sincronizada atende ao requisito de escalabilidade, devido ao fato de que novas AD's podem ser adicionadas em uma comunidade e o pontos de sincronismo podem ser executados entre as AD's criando assim um relacionamento entre elas, veja capítulo 5. E atende também o requisito de Auditoria externa tendo por base os pontos de confiança publicados e as informações contidas nos recibos dos usuários.

Requisito	**Análise**
Privacidade	Atende
Anonimato	Não atende
Imparcialidade	Atende
Confiabilidade	Atende
Desempenho	Atende
Escalabilidade	Atende
Verificabilidade	Atende
Flexibilidade	Atende
Auditoria (Externa/Interna)	Auditoria Interna e Externa

3. a AD assina o par (n, L_n) e envia $(n, L_n, sig_{AD}(n, L_n))$ para o cliente;

4. a AD envia a tupla $head(n) = (F_{n-1}, F_{n-2}, ..., R_{r-1}, R_{r-2}, ..., S_i, S_{i-1}, ..., C_j)$, onde i e j são indices que correspondem ao encadeamento;

5. o cliente verifica a assinatura da AD e checa se:

$$F(F_n, F(F_{n-1}, ..., F(F_{R_{r-1}+1}, L_{R_{r-1}})...)) = L_n \tag{4.1}$$

6. seja $tail(n) = (F_{R_r-1}, F_{R_r-2}, ..., F_{n+2}, F_{n+1})$. A AD envia a resposta para o cliente $(tail(n), sig_{AD}(tail(n)))$;

7. o cliente verifica se:

$$L_{R_r} = F(F_{R_r-1}, F(F_{R_r-2}, ..., F(F_{n+2}, F(F_{n+1}, L_n))...)); \tag{4.2}$$

8. o recibo completo do cliente s_n é:

$$s_n = (tail(n), head(n), n, L_n, sig_{AD}(n, L_n)) \tag{4.3}$$

4.2.2 Protocolo de verificação

Seja *r(n)* a rodada onde s_n é valido. Assume-se que o verificador tem dois recibos de dois documentos (X_m, s_m) e (X_n, s_n), onde $m < n$.

1. o verificador checa a igualdade das equações *4.1* e *4.2* para os dois recibos;
2. se *r(m) = r(n)*, então o verificador analisa se a equação é verdadeira:

$$L_n = F(F_n, F(F_{n-1}, ..., F(F_{m+1}, L_m)...)) \tag{4.4}$$

3. se *r(m) < r(n)*, calcula $L_{R_{r(m)}}$ usando *4.2*, calcula $L_{r(n)-1}$ usando a formula:

$$L_{r(n)-1} = F(F'_{R_{r(n)-1}}, F(F'_{R_{r(n)-2}}, ..., F(F_{R_{r(m)}}, L_{R_{r(m)}})...)) \tag{4.5}$$

E finalmente, compara o valor de L_n em s_n com o valor dado pela equação *3.6*, se for igual significa que realmente *r(m) < r(n)*.

4.2.3 Definição ASN.1 do Método Árvore Sincronizada

Toda a comunicação entre o cliente e a Autoridade de Datação seguem o padrão de requisição e resposta definido na RFC 3161 onde é instituído um protocolo de comunicação chamado TSP - *Time-Stamping Protocol* [ADA 01].

Mas este padrão de protocolo não define como será o formato ASN.1 do recibo de datação, pois de acordo com o algoritmo de encadeamento e de acordo com as políticas de cada AD o recibo pode mudar de formato. Mas como este trabalho de dispõe a definir um novo método de datação, o formato ASN.1 do recibo s_n definido na seção 4.2.1 deste capítulo pode ser visto a seguir.

```
TimeStampToken ::= SEQUENCE { - - - - - - - - - - - -
        tstInfo         TSTInfo,
        tail            TSTTail         OPTIONAL,
        head            TSTHead,
        idStamp         INTEGER,
        resLink         MessageImprint
```

```
        signature       RSTSign
}

TSTInfo ::= SEQUENCE { - - - - - - - - - - - - - - - - - - -
        version         INTEGER  v1(1) ,
        policy          TSAPolicyId,
        messageImprint  MessageImprint,
        serialNumber    INTEGER,
        genTime         GeneralizedTime,
        accuracy        Accuracy                OPTIONAL,
        ordering        BOOLEAN                 DEFAULT FALSE,
        nonce           INTEGER                 OPTIONAL,
        tsa             [0] GeneralName         OPTIONAL,
        extensions      [1] IMPLICIT Extensions OPTIONAL
}

TSTTail ::= SEQUENCE { - - - - - - - - - - - - - - - - - - - - - - -
        messageImprints  SEQUENCE OF MessageImprint
}

TSTHead ::= SEQUENCE { - - - - - - - - - - - - - - - - - - - - - - -
        messageImprints  SEQUENCE OF MessageImprint
}

MessageImprint ::= SEQUENCE { - - - - - - - - - - - - - - -
        hashAlgorithm    AlgorithmIdentifier,
        hashedMessage    OCTET STRING
}

TSTSign ::= SEQUENCE { - - - - - - - - - - - - - - -
        sigAlgorithm       AlgorithmIdentifier,
        detachedSigneture OCTET STRING
}
```

4.3 Conclusão

Este método pode ser resumido nos seguintes pontos:

- **Encadeamento**: o encadeamento de um recibo é feito através de uma função F e a cada final de um pulso é formado um recibo de rodada. Note que o final de um pulso pode coincidir com um outro, por exemplo o final de um dia coincide com um de final de uma semana que por sua vez coincide com um final de um mês.
- **Verificação**: o processo é efetuado de acordo com a política utilizada pela AD, ou seja, quais são os pulsos que foram definidos para a execução do encadeamento.
- **Flexibilidade**: o método é flexível no sentido de se poder definir quais são os pulsos que serão executados.
- **Confiabilidade**: como o método se utiliza da autenticação temporal relativa, não existe meios de se datar um documento antes de um outro que já tenha sido datado pela AD.
- **Auditoria**: como o método está sujeito ao ataque da cadeia de encadeamento, pode-se desenvolver um procedimento que varra a árvore de encadeamento formada e verifique sua autenticidade, isto depende é claro da política de encadeamento adotada e das políticas de auditorias definidas.
- **Performance**: como o método se utiliza basicamente de funções unidirecionais, o processamento de cada recibo é insignificante, proporcionando à AD receber vários pedidos de datação ao mesmo tempo.

Capítulo 5

IDDE - Infra-estrutura de datação de documentos eletrônicos

5.1 Introdução

Inspirada na recomendação X509 que padroniza a Infra-estrutura de Chaves Públicas [ADA 99b] [HOU 01], pode-se definir uma Infra-estrutura com os mesmos moldes, mas com conceitos diferentes. Esta nova Infra-estrutura se destina a especificar os relacionamentos, as políticas e as responsabilidades que cada Autoridade de Datação contida na estrutura deve seguir, de modo a proporcionar um ambiente de datação transparente, integro e confiável.

É extremamente fácil para uma terceira entidade (Marcos) verificar se o documento de Alice foi datado antes do documento de Beto, se estas duas datações foram feitas na mesma AD. No entanto, Alice precisa se comunicar com centenas de pessoas, e algumas delas utilizam diferentes ADs para datar seus documentos. Com isto, em uma situação de disputa, Marcos precisaria processar datações de diferentes Autoridades? Como Marcos pode determinar se as ADs envolvidas no processo são confiáveis e seguem o mesma política de datação?

Esta nova Infra-estrutura IDDE visa atender ao requisito de escalabilidade que foi definido no capítulo 3, estabelecendo regras e conceitos que cada AD de-

ve seguir, propiciando um ambiente totalmente transparente para todos que utilizam o serviço de datação, ou seja, todas as AD's ligadas na Infra-estrutura passam a ser uma só para o usuário. Mas como as ADs podem criar tais ligações entre si?

As estruturas de Autoridades de Datação descrevem a organização das ADs e seus relacionamentos. Mas esta estrutura pode diferenciar de acordo com as respostas das seguintes perguntas:

- Em quantas ADs Marcos pode confiar?
- Que tipo de relacionamentos existem entre as ADs?
- Como se pode adicionar novas ADs na estrutura?
- Como se dá a construção de um caminho de verificação de recibos de datação? Uma vez construído o quão é complexo de se verificar?

Cada estrutura tem diferentes qualidades. Este capítulo começa examinando os detalhes de uma simples AD. Esta simples AD oferece uma boa solução para pequenas comunidades de usuário, como pequenas empresas, mas para satisfazer a necessidade de grandes empresas, como agências do governo, que precisam ter várias AD's para atender sua demanda, é requerida uma estrutura um pouco mais complexa. Estas estruturas são chamadas de: Modelo em Árvore e Modelo em Malha, as quais são compostas por múltiplas AD's e por diferentes tipos de relacionamentos, gerando assim diferentes atributos para cada estrutura.

Mas como Alice se comunica com diferentes empresas e cada empresa se utiliza de um tipo diferente de estrutura, este capítulo também descreve dois modelos híbridos: Datação cruzada e Datação em Ponte.

Cada estrutura descrita neste capítulo tem suas vantagens e desvantagens. Cada uma é adequada a um tipo de aplicação ou a um tipo de empresa. Este capítulo conclui propondo uma Infra-estrutura de Datação de Documentos Eletrônicos.

5.2 Modelo Simples

O mais básico de todas as estruturas é o Modelo Simples, que provê todas as datações para uma comunidade de usuários. Neste modelo, todos os usuários confiam na mesma AD. Os usuários somente aceitam datações efetuadas por esta AD. Como resultado, o protocolo de verificação e de auditoria de recibos restringem-se a AD.

A figura 5.1 ilustra como é o Modelo Simples de Datação. Embora simples de implementar, esta estrutura não suporta uma comunidade muito grande de usuários. Com isto, para uma empresa que contém vários setores e cada setor tem muitos documentos para serem datados por dia, este modelo de serviço de datação não suportaria tal demanda.

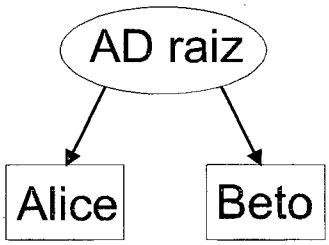

Figura 5.1: Modelo Simples. Dentro de uma comunidade existe somente uma AD que disponibiliza o serviço de datação, o caminho de verificação de um recibo é extremamente simples e a verificação de dois recibos por Marcos envolve somente a busca na árvore de encadeamento da AD.

5.3 Modelo em Árvore

Nesta estrutura, múltiplas ADs provem serviços de datação, e as ADs estão ligadas através de relacionamentos de sincronismo. Todos os usuários confiam em uma única AD raiz sempre. Com exceção da AD raiz, todas as ADs são ligadas a alguma AD de nível superior. Qualquer AD pode ter uma AD ligada a si e/ou datar documentos dos usuários.

Para adicionar uma nova AD na estrutura, uma das ADs existentes pode ser alocada como a AD de nível superior a aquela nova AD. A figura 5.2 ilustra o modelo

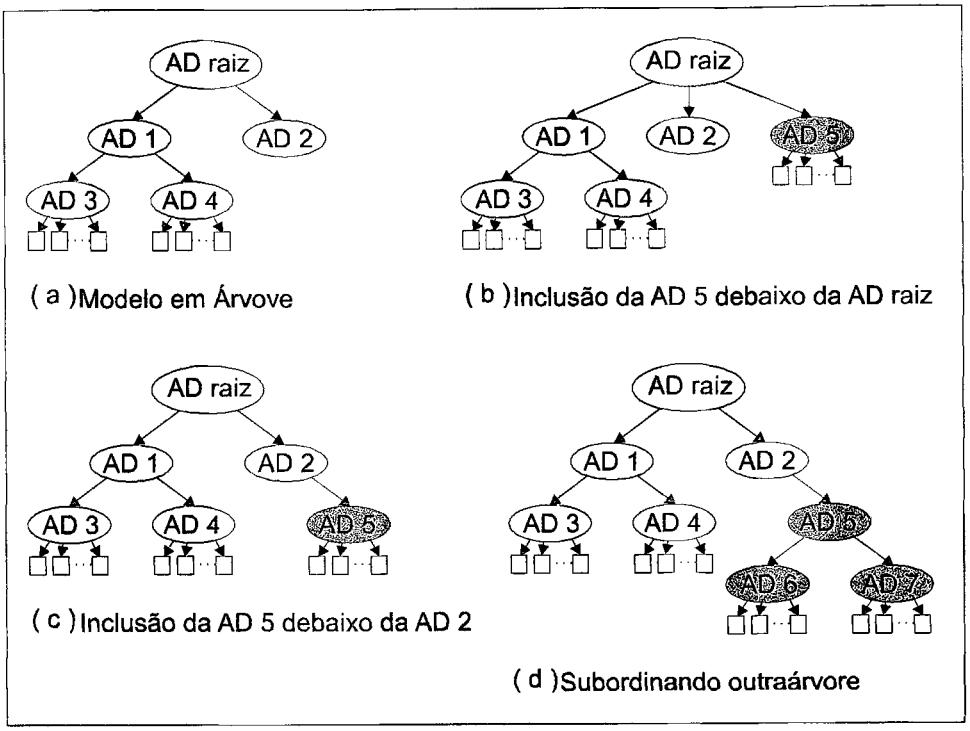

Figura 5.2: Modelo em Árvore. Este modelo é bastante flexível ao ponto de se poder adicionar novas AD em praticamente qualquer lugar. Na figura (b) e (c) é possível verificar que se pode adicionar uma nova AD exatamente embaixo da AD raiz ou em qualquer lugar da árvore. Na figura (d) é demonstrado que se pode adicionar também uma nova árvore na árvore existente.

em árvore e três maneiras diferentes de se adicionar uma nova AD no modelo.

Cada relacionamento de sincronismo é definido da seguinte forma: quando uma AD deseja se filiar a uma outra AD de nível superior, ela deve sincronizar sua cadeia de encadeamento a partir de um *átomo* fornecido pela AD superior. O *átomo* nada mais é do que o último ponto de confiança C_i publicado pela AD de nível superior em um local público. Com isto todas as datações desta AD terão uma referência com a AD de nível superior. Periodicamente, todos os dias a meia noite por exemplo, a AD gera seu próprio ponto de confiança e o publica em um local público. Para que as duas AD's mantenham um relacionamento sincronizado, a AD de nível inferior pode sincronizar novamente sua cadeia com a AD de nível superior datando seu ponto de confiança nesta AD. Conseqüentemente, o resultado desta datação é um recibo especial chamado de recibo de

ponto de confiança e contém informações referentes à cadeia de encadeamento da AD de nível superior. Este sincronismo não depende de nenhuma autorização ou qualquer avaliação por parte da AD de nível superior.

Os caminhos de verificação de recibos do modelo em árvore são facilmente definidos porque cada AD tem somente uma AD de nível superior. Existe somente um caminho de verificação entre o usuário e a AD em que ele confia, no caso AD raiz. Então quando Marcos quiser verificar os recibos de dois documentos datados em ADs diferentes ele só precisa montar o caminho de verificação dos dois recibos até que os seus caminhos se cruzem em alguma AD de nível superior; no pior caso esta AD seria a AD raiz. Sendo assim, Marcos não conseguirá determinar o tempo relativo exato que existe entre os dois recibos, mas poderá determinar uma janela de tempo em que aqueles recibos foram datados, ou seja, Marcos não consegue determinar qual dos dois documentos foi datado antes do outro, mas consegue concluir que estes dois documentos foram datados na mesma janela de tempo, por exemplo no mesmo dia.

Isto porque as ADs de nível inferior criam um relacionamento com as ADs de nível superior através de um sincronismo de suas cadeias. Como este sincronismo precisa ser restabelecido em tempos em tempos, por exemplo no final de cada dia, todos os documentos datados naquele dia pela as ADs inferiores são considerados pela AD de nível superior como documentos datados em um dia específico. Com isto, cada vez que Marcos sobe na árvore para reconstruir o caminho de verificação ele perde a precisão da datação, mas consegue concluir que os recibos são válidos e foram datados em uma determinada época, como ilustra a figura 5.3. Vale lembrar que todas as informações necessárias para a reconstrução do caminho de verificação estão no próprio recibo de datação.

5.4 Modelo em Malha

O modelo em malha é uma estrutura alternativa ao modelo em árvore e pode ser chamada também de modelo em rede. Nesta estrutura, múltiplas ADs provêm serviços de datação, e as ADs estão ligadas através de relacionamentos de ponto a ponto. Cada usuário confia em uma AD, no entanto, a AD que ele confia não é a mesma para

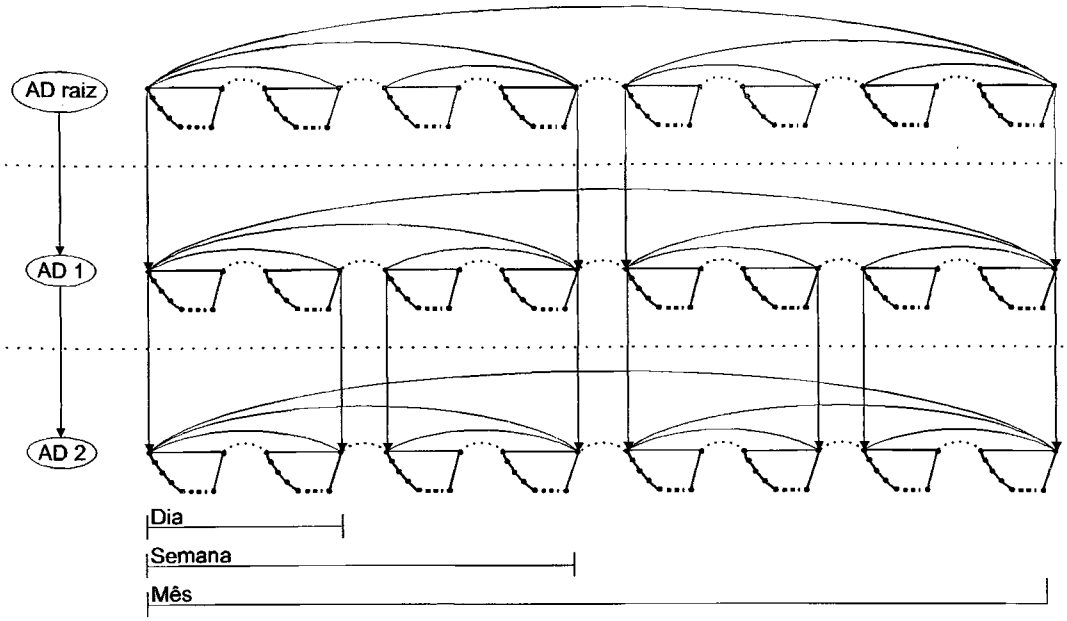

Figura 5.3: Relacionamentos entre Autoridades de Datação. Cada vez que um ponto de confiança é gerado por uma AD ele é publicado em um local público. Quando alguma outra AD queira de filiar a esta AD basta sincronizar sua cadeia com este ponto de confiança publicado e periodicamente datar seus próprios pontos de confiança na AD de nível superior.

todos os usuários.

Neste modelo, os usuários confiam na AD onde são datados os seus documentos. As ADs por sua vez criam um relacionamento entre si, da mesma forma que é criado no modelo em árvore, criando um ambiente ilustrado na figura 5.4.

Uma nova AD pode ser facilmente adicionada no modelo. Basta que ela inicialize sua cadeia de encadeamento com o *átomo* fornecido pela AD vizinha e a AD vizinha sincronizar sua cadeia com o *átomo* fornecido pela nova AD. No entanto, a construção do caminho de verificação de um recibo é particularmente complexa. No modelo em árvore a construção do caminho é determinístico, ou seja, só existe um caminho até a AD de confiança, já neste modelo a construção é não determinística, e não existe uma AD de confiança comum. Existem sim vários caminhos a serem seguidos, uns destes caminhos são caminhos válidos, mas outros chegam a lugar algum. O tamanho do caminho é maior do que no modelo em árvore, o qual depende do número de níveis da árvore.

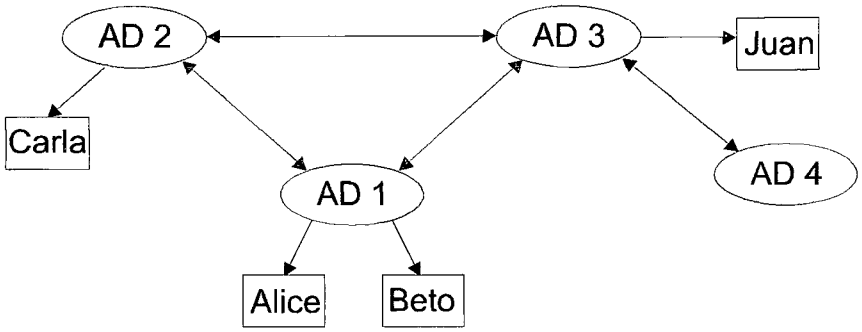

Figura 5.4: Modelo em Malha. Cada usuário confia na AD que ele efetua suas datações e cada AD cria um relacionamento de ponto a ponto da mesma forma feita no modelo em árvore com outras ADs. Neste modelo Marcos pode encontrar dificuldades em verificar dois documentos datados em ADs diferentes, pois como existem vários caminhos que podem ser percorridos, podem existir caminhos que não levam a lugar nenhum.

No pior caso neste modelo, o tamanho pode chegar ao número de ADs interligadas.

5.5 Datação Cruzada

Quando uma AD quer passar a reconhecer as datações efetuadas numa outra AD e manter um sincronismo com ela, se efetua o processo chamado de datação cruzada. Este processo é ilustrado na figura 5.5

Note que a estrutura da AD1 e da AD2 não influi no processo de datação cruzada. Com isto pode-se efetuar este processo em diferentes ambientes com diferentes modelos de estrutura, possibilitando assim, uma interação muito maior entre os usuários de diferentes empresas.

Com este processo instituído, torna possível uma verificação de dois recibos que foram datados em ADs diferentes de diferentes ambientes, pois até então não se poderia compará-los porque os dois não tinham nenhum tipo de relação.

Quando Marcos verificar estes dois recibos ele terá que construir o caminho de verificação até a entidade que esteja efetuando o processo de datação cruzada, geralmente é a AD em que ele confia. Se esta entidade estiver fazendo múltiplas datações cruzadas, Marcos terá que construir um caminho de verificação diferente para

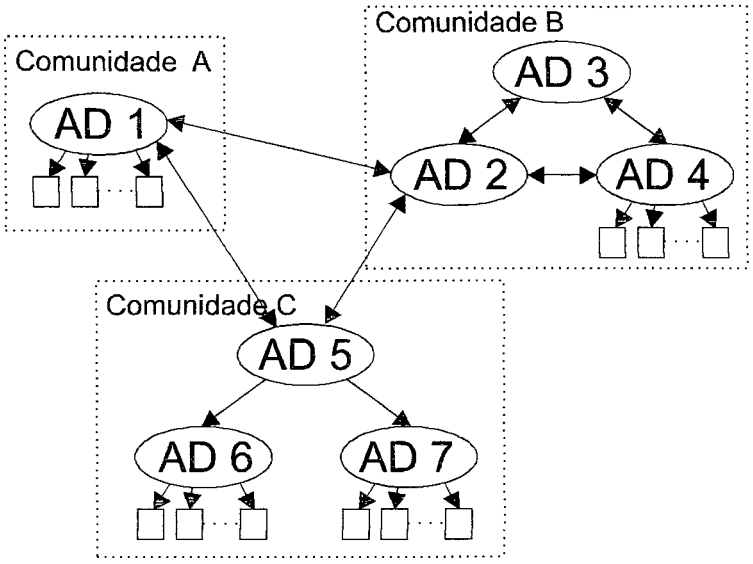

Figura 5.5: Datação Cruzada. Se a AD1 quiser passar a reconhecer as datações da AD2 por um período de tempo, ela precisa sincronizar sua cadeia de encadeamento com o *átomo* fornecido pela AD2. Quando este período estabelecido se expirar a AD1 só precisa parar de sincronizar sua cadeia com a AD2. Com isto a referência que era passada da AD2 para AD1 não mais existe e o processo de datação cruzada é finalizado.

cada cruzamento até que ele encontre a AD Raiz do outro recibo e concluir a verificação determinando qual é a janela de tempo entre os dois recibos.

5.6 Datação em Ponte

O processo descrito na seção acima 5.5 tem um problema. Se por um acaso uma empresa precisar reconhecer datações de outras 20 empresas e se estas 20 empresas precisarem reconhecer datações entre si, isto criaria uma malha bastante complexa o que aumentaria, e muito, o tempo de verificação entre os recibos e a complexidade de encadeamentos cruzados entre as empresas. Para resolver tal problema pode-se instituir uma entidade que funcionará como uma ponte. Veja figura 5.7

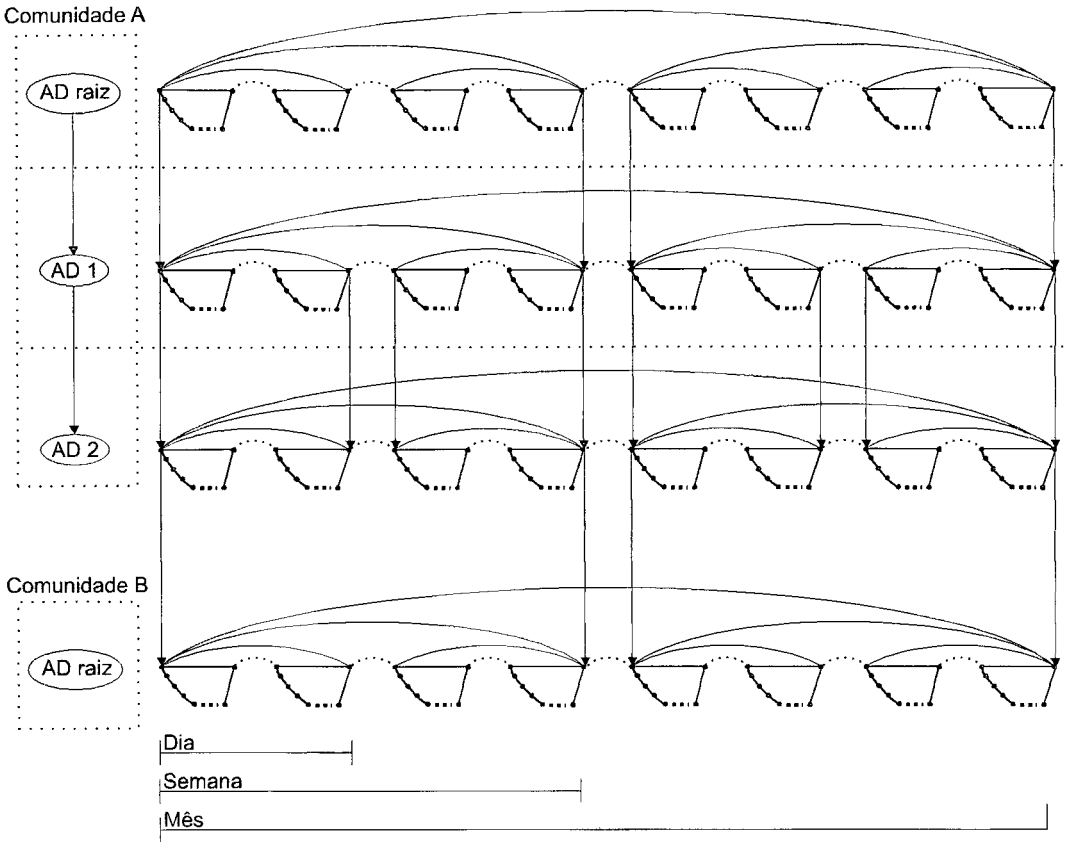

Figura 5.6: Relacionamentos de Datação cruzada. Se a AD raiz da Comunidade B quiser reconhecer as datações efetuadas em qualquer AD da Comunidade A, no caso a AD2, ela terá que sincronizar sua cadeia de encadeamento com o *átomo* fornecido pela AD2, de modo que a AD raiz tenha uma referência do encadeamento da AD2.

5.7 Uma proposta de uma IDDE

Hoje no Brasil nenhuma empresa adota qualquer tipo de padronização de datação de documentos eletrônicos e ainda não existe uma infra-estrutura ou até mesmo um modelo a ser seguido.

Esta proposta de IDDE se destina a especificar o modelo e o método de datação, os relacionamentos, as políticas e as responsabilidades de cada Autoridade de Datação contida na IDDE, de modo que para o usuário o serviço de datação seja transparente. Todas as ADs devem seguir tais recomendações para que suas datações sejam reconhecidas como válidas e integras.

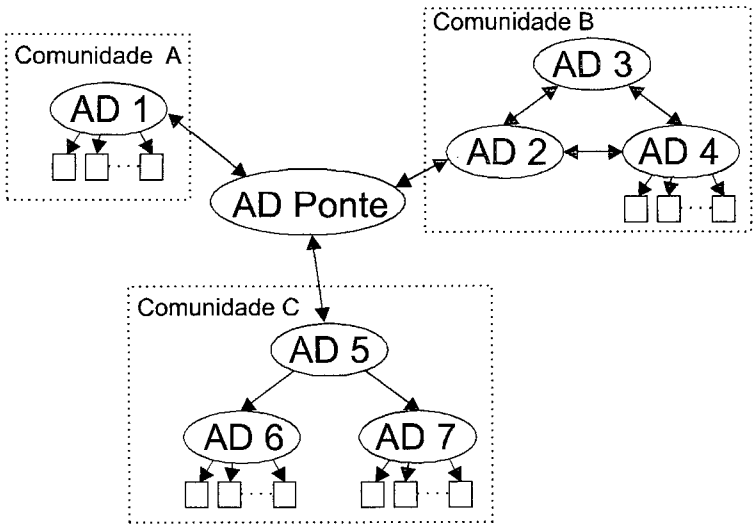

Figura 5.7: Datação em ponte. Quando a AD1 queira efetuar uma datação cruzada com a AD2 em vez de sincronizar a sua cadeia com o *átomo* fornecido pela AD2, as duas sincronizam suas cadeias com o *átomo* da AD Ponte.

5.7.1 Modelo de Datação

A IDDE se utilizará do modelo em árvore de datação devido a vários fatores:

- por sua facilidade de compreensão da estrutura;
- por ser um modelo escalável;
- pela fácil construção do caminho de verificação de recibos;
- por sua flexibilidade de inclusão de novas ADs;

A figura 5.8 ilustra como pode ser modelada a infra-estrutura pegando-se o exemplo do Brasil. Em um primeiro nível se encontraria a AD raiz responsável em disponibilizar para as demais ADs um ponto onde todos os usuários confiam. Em um segundo nível se encontram as ADs Estaduais que são responsáveis em disponibilizar o serviço de datação para uma região especifica. Em um terceiro nível estariam as ADs que prestariam serviços para os maiores municípios da região ou os municípios que tenham uma demanda muito grande de datações de documentos. Um quarto nível poderia ser

definido para as cidades que tenham uma alta gama de datações que uma simples AD não suportaria. Lembrando que em qualquer nível da estrutura pode-se incluir ADs de empresas públicas e privadas, dependendo da importância da datação.

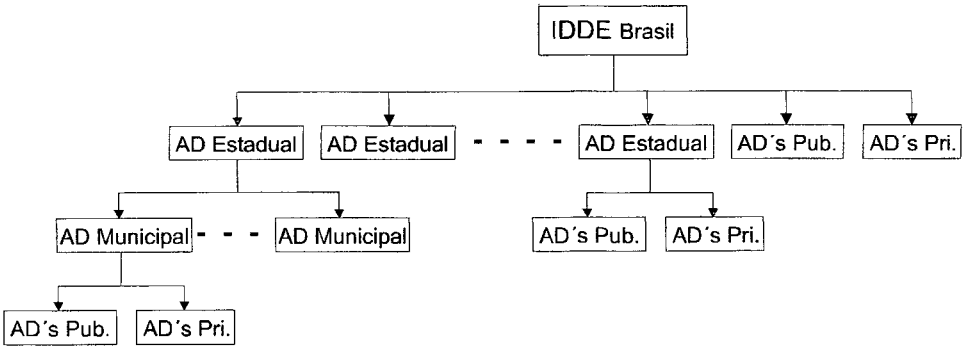

Figura 5.8: Modelo de Datação da IDDE. Esta figura ilustra como o modelo de datação pode ser definido, por exemplo, para o Brasil. No nível mais alto existe somente a AD raiz, responsável em disponibilizar um ponto único de confiança para todos os usuários. No segundo nível se encontram as ADs Estaduais, responsáveis em disponibilizar o serviço de datação para seus estados, e pode-se encontrar também ADs de empresa públicas e privadas. Em um terceiro nível seriam definidas as ADs municipais juntamente com ADd de empresa públicas e privadas. Dependendo da demanda de datações um ou mais níveis poderiam ser definidos na estrutura.

A criação ou não dos níveis no modelo, dependem da demanda de datações. Cada AD tem um número máximo de datações por segundo. Com isto a decisão de se criar um novo nível para dividir a demanda de requisições, vem da análise do número de datações por segundo que cada AD está efetuando.

5.7.2 Método de Datação

De modo a não utilizar nenhum método de datação patenteado ou ineficiente, será utilizado o novo método de datação, Árvore Sincronizada. Este método, como já foi visto no capítulo 4, atende aos requisitos de segurança e de implementação definidos no capítulo 3 e se mostrou bastante flexível em termos de definição e incorporação do método na IDDE.

A figura 5.9 demonstra como este método pode ser usado na IDDE e como são feitas as sincronizações de ADs inferiores com as ADs superiores.

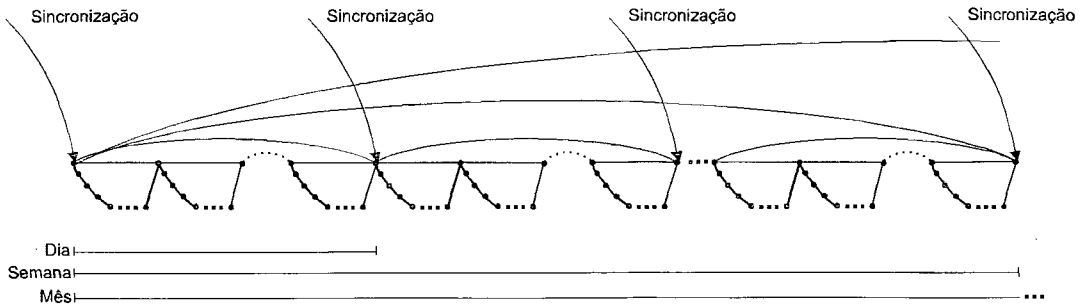

Figura 5.9: Método de Datação da IDDE. Ao inicializar a AD, ela deve se filiar a alguma outra AD no modelo requisitando o seu *átomo*, de modo que suas datações se referenciem com a AD raiz. Periodicamente, esta nova AD, deve datar seus ponto de confiança na AD superior de modo a restabelecer uma nova sincronização. Com isto, Marcos pode verificar diferentes recibos datados em diferentes ADs determinando suas respectivas janelas de tempo.

5.7.3 Políticas

Para esta Infra-estrutura podem ser instituídas uma série de políticas de gerenciamento:

- **Política de Inicialização**: Quando uma Autoridade de Datação é inicializada duas providências devem ser tomadas: (1) fornecer um certificado digital válido de uma Autoridade de Certificação para que a AD possa assinar os recibos de datação e (2) fornecer um *átomo* válido da AD que se deseja se filiar ligada à infra-estrutura.

- **Política de Encadeamento e Sincronização**: Ao fornecer um *átomo* válido para a AD na hora de sua inicialização, a AD passou a referenciar em suas datações com a AD que forneceu o *átomo*. Dependendo do nível desta AD, a periodicidade de sincronização pode variar. Segundo o exemplo descrito anteriormente pode se definir que para as ADs de empresas públicas e privadas sua sincronização é diária e o horário de sincronização é definido pela sua AD superior. Para as ADs Municipais sua sincronização com as ADs Estaduais é semanal, onde o dia e hora da sincronização é definida pelas ADs Estaduais. Para as ADs Estaduais sua sincronização com a AD raiz é mensal.

- **Política de Verificação**: quanto a verificação do recibo de datação, o cliente deve

verificar se o certificado digital da AD está válido e se caso este estiver revogado ou expirado o cliente deve verificar se o documentos foi datado antes da revogação ou expiração deste certificado.

Quanto a comparação de dois recibos de datação, para verificar qual dos dois foi datado antes do outro, Marcos pode construir um caminho de verificação determinístico no modelo em árvore proposto até que os dois caminhos se cruzem em uma AD nos níveis superiores acima. Com isto, Marcos pode comparar as janelas de tempo dos dois documentos e determinar suas validades.

- **Política de Atualização de Certificado**: Ao inicializar a AD foi fornecido um certificado digital válido por uma ano para ser usado pela AD nas assinaturas. Mas depois de um período de tempo este certificado se expira e as assinaturas não tem mais validade. Com isto, o operador da AD executa, por um método de autenticação segura, uma requisição de geração de um novo par de chaves. Assim o operador pode levar esta requisição a uma Autoridade de Certificação, a qual gerará um novo certificado digital para ser instalado na AD.

  Mas se o certificado digital da AD for revogado. É de responsabilidade do operador da AD verificar periodicamente na lista de certificados revogados na Autoridade de Certificação se o certificado digital da AD foi revogado ou não. Caso o seja, o operador deve executar o processo de atualização de certificado.

- **Política de Auditoria**: Mesmo considerando que o método de datação garante que um documento eletrônico seja datado com data e hora corrente, é necessário definir mecanismos de auditoria, com vista em demonstrar transparência no processo como um todo. O sistema deve prover ferramentas e fornecer dados para o auditor, de modo a provar a idoneidade da Autoridade de Datação.

5.7.4 Segurança física nas ADs

Além de considerar a segurança e a integridade do método de datação utilizado e dos relacionamentos entre entidades, deve ser levado em consideração também

a segurança física dos equipamentos onde estão os softwares das ADs

O *Federal Information Processing Standards Publication* (FIPS) define quatro níveis de segurança que pode ser dado a um equipamento específico [NIS 94b], eles são:

- **Nível 1**: provê o menor nível de segurança. Este nível especifica os requisitos de segurança básicos para um módulo de criptografia. Nenhum mecanismo de segurança físico é requerido, além da exigência que o equipamento seja de produção.

- **Nível 2**: este nível aprimora a segurança física do nível 1 adicionando lacres e selos de modo que se alguém tentar obter as informações guardadas no equipamento tais lacres sejam violados, e cadeados e fechaduras para as portas de acesso ao equipamento para o proteger de acessos não autorizados. Este nível provê ainda autenticação baseada em papéis, de modo que o operador é autorizado a desempenhar um determinado papel dentro do sistema.

- **Nível 3**: O nível 3 requer uma segurança física maior do que está geralmente disponível em muitos produtos comerciais existentes. Ao contrário do nível 2 de segurança que emprega lacres para proteger o equipamento de acesos indevidos e selos de segurança para detectar se o equipamento foi violado, o nível 3 protege o equipamento mesmo que tais selos e lacres sejam abertos. Por exemplo, se algum selo for violado ou algum lacre estiver aberto as informações contidas dentro do equipamento, tais como a chave privada, são destruídos automaticamente. O nível 3 se utiliza ainda da autenticação por identidade, que é mais seguro do que a autenticação baseada em papeis.

- **Nível 4**: fornece o nível mais elevado de segurança. A segurança física neste nível implementa uma espécie de envelope em torno do módulo criptográfico, visto que os métodos de detecção de um dos níveis anteriores podem ser contornados. Por o exemplo, se uma pessoa conseguir ultrapassar todos os lacres e selos, a tentativa deve ser detectada e todos as informações devem destruídas. Os métodos do nível 4

são particularmente úteis para a operação em um ambiente fisicamente desprotegido onde um intruso poderia possivelmente alterar um dispositivo.

O nível 4 também protege o equipamento contra de condições anormais de ambiente, ou seja, variáveis de temperatura e de tensão de rede elétrica podem ser considerados como fatores de invasão, se tais variáveis ultrapassarem valores pre-estabelecidos todas as informações devem ser destruídas.

Para esta aplicação de datação de documentos eletrônicos pode ser definido o nível 3 de segurança. O equipamento que esteja executando o software da AD deve ser mantido em uma sala trancada e isolada. Este equipamento deve estar dentro de um hack que disponibilize uma tranca e o gabinete deste equipamento deve ser lacrado, assim como todas as suas portas de comunicação e seus drives de dispositivos. Deve existir censores nas trancas e lacres, de modo que se estes forem violados as informações contidas no equipamento sejam destruídas. O acesso a esta máquina deve ser restrito e uma única porta de comunicação desta máquina com o mundo exterior deve ser definida.

5.8 Conclusão

Neste capítulo foi visto um proposta para uma Infra-estrutura de Datação de Documentos Eletrônicos, assim como sua estrutura, seu método de datação e a definição de sua políticas básicas.

Capítulo 6

Considerações Finais

A motivação para o desenvolvimento este trabalho foi a necessidade observada de se ter um autoridade onde se pudesse datar documentos de uma forma integra e segura. Para tanto a autoridade deveria ser transparente ao ponto de disponibilizar um serviço de datação confiável, e onde todas estas datações pudessem ser verificadas e validadas de uma forma eficiente e eficaz.

Com isto foi especificado um método de datação que garante que a AD não possa ser maliciosa, ou seja, o documento sempre será datado com data e hora correta. E com este novo método instituído pode-se então utilizá-lo como sendo o método padrão de datação do modelo IDDE proposto, de modo a não utilizar nenhuma técnica já patenteada ou ineficiente.

O primeiro objetivo especifico deste trabalho foi estudar as técnicas de criptografia. Este objetivo foi alcançado, o qual esta relatado no capítulo 2. Este objetivo é fundamental para o entendimento do funcionamento da criptografia e também porque estes fundamentos são utilizados na construção dos métodos de datação. As cifras simétricas e assimétricas garantem o sigilo em uma comunicação e que é inviável computacionalmente a quebra deste sigilo. A assinatura digital é feita através da cifra assimétrica e da função resumo. O certificado digital relaciona a chave privada a um usuário garantindo assim que a aplicação desta chave privada somente poderá ser feita por este usuário. É importante o entendimento da Infra-estrutura de Chave Pública porque ela

defini os procedimentos para expedição de certificados digitais.

O segundo objetivo específico foi estudar os métodos e tecnologias de segurança existentes para o campo de datação eletrônica. Este objetivo foi alcançado através do estudo e análise dos esquemas de encadeamento linear, árvore e binário, vistos no capítulo 3. Desta análise foi extraido os requisitos que um sistema de datação seguro e confiável deve atender. Também foram analisadas as falhas e possíveis vulnerabilidades que podem ser encontradas nos métodos de datação, como por exemplo, o ataque à cadeia de recibos.

O terceiro objetivo específico deste trabalho foi especificar um método que atenda aos requisitos de segurança e implementação e que não seja propício a eventuais ataques. Este objetivo foi alcançado no capítulo 4, onde se encontra toda a definição de encadeamento e de verificação de recibos.

Este novo método de datação pode ser comparado com os demais métodos em relação ao atendimento ou não dos requisitos de segurança e implementação propostos, como pode ser visto na tabela 6.1. Nota-se que o único método de datação que atente a todos os requisitos é a Árvore Sincronizada,lembrando que o requisito anonimato não invalida o cumprimento dos outros requisitos de segurança e é visto como um requisito de caráter desejável. Percebe-se ainda que Árvore Sincronizada atente também ao requisito de auditoria externa, qualidade tal que é muito importante para a instituição de uma AD, já que esta qualidade torna transparente toda e qualquer atividade que a AD realize.

Tabela 6.1: Tabela de comparação dos métodos de datação

Requisito \ Método	**Linear**	**Árvore**	**Binário**	**Árvore sincronizada**
Privacidade	X	X	X	X
Anonimato				
Imparcialidade	X	X	X	X
Confiabilidade	X	X	X	X
Desempenho		X	X	X
Escalabilidade				X
Verificabilidade			X	X
Flexibilidade				X
Auditoria	Interna	Interna	Interna	Interna e Externa

O quarto objetivo específico deste trabalho foi especificar uma Infra-estrutura de Datação de Documentos Eletrônicos que se destina a especificar o modelo e o método de datação, os relacionamentos, as políticas e as responsabilidades de cada Autoridade de Datação contida na IDDE. Todas as ADs devem seguir tais recomendações para que suas datações sejam reconhecidas como válidas e integras. Este objetivo foi alcançado no capítulo 5, onde se encontra toda a definição da infra-estrutura.

A Infra-estrutura IDDE foi concebida primeiramente para atender o requisito de implementação escalabilidade definido no capítulo 3, mas logo percebeu-se que ela trazia outra vantagens para com o processo de datação digital, pois ela proporciona um ambiente totalmente confiável e auditável para que os usuários possa ter a certeza que seus documentos sejam datados com data e hora correta.

A IDDE é uma Infra-estrutura que se destina a oferecer um ambiente de datação transparente para o usuário tanto para a datação de documentos eletrônicos como a verificação de recibos de datação. Para o usuário final não interessa em qual AD ele datou seu documento e como foi datado, só lhe interessa saber se o recibo que ele recebeu é confiável. Com a IDDE, além de ele conseguir tal recibo ele poderá também auditá-lo, já que o método de datação utilizado pela Infra-estrutura, a Árvore Sincronizada, suporta auditoria externa.

6.1 Contribuições

Dentro do escopo deste trabalho e dos resultados descritos anteriormente, pode-se identificar as seguintes contribuições:

- A primeira de caráter exclusivamente investigativo, envolvendo pesquisa bibliográfica, aprofundamento de conhecimento e elaboração de textos explicativos referente ao estudo dos fundamentos de criptografia e ao estudo dos métodos de datação existentes.

- Discussão de caráter inovador a respeito das responsabilidades e obrigações que uma Autoridade de Datação deve seguir, definindo assim seus requisitos de segurança

e implementação.

- Este trabalho proporcionou a base e os requisitos para o desenvolvimento real de uma AD por uma empresa privada, BRy Tecnologia, em Florianópolis.
- Formalização das fórmulas de construção e das ilustrações do método de encadeamento em árvore, possibilitando um melhor entendimento.
- Proposta e definição de um novo método de Datação de documentos eletrônicos chamado de Árvore Sincronizada e a proposta e definição de uma Infra-estrutura de Datação de Documentos Eletrônicos.

6.2 Trabalhos futuros

Os trabalhos desenvolvidos dentro do contexto desta monografia, em particular o novo método de encadeamento, oferecem subsídios ao desenvolvimento de outros projetos de pesquisa nesta universidade e em outras instituições com interesse na área. As sugestões são:

1. Especificação formal da Infra-estrutura IDDE;
2. Comparação de desempenho entre os métodos de encadeamento vistos com o novo método Árvore Sincronizada;
3. Sincronização segura do relógio da AD com uma fonte de tempo confiável, como o GPS;
4. Propor um modelo computacional de um Protocolo Geral;
5. Para a área de administração, definir políticas de gestão para a AD e para a IDDE;
6. Para a área de Direito, propor algumas alterações na legislação para que se venha reconhecer judicialmente na lei brasileira as datações efetuadas por AD's.

Referências Bibliográficas

[ADA 97] ADAMS, C. The cast-128 encryption algorithm. Network Working Group, May, 1997. Request for comments: 2144.

[ADA 99a] ADAMS, C. **Undertanding Public-Key Infraestructure: Concepts, Standards and Deployment Considerations**. Indianapolis, 1999.

[ADA 99b] ADAMS, C.; FARREL, S. Internet x.509 public key infrastructure certificate management protocols. Network Working Group, 1999. Request for comments: 2510.

[ADA 01] ADAMS, C. et al. Internet x.509 public key infrastructure time-stamp protocol (tsp). Network Working Group Category: Standards Track, August, 2001. Request for comments: 3161.

[BAY 91] BAYER, D.; HABER, S.; STORNETTA, W. S. Improving the efficiency and reliability of digital time-stamping. **Sequences91: Methods in Communication, Security, and Computer Science**, [S.l.], p.329–334, 1991.

[BEN 92] BENALOH, J.; DE MARE, M. Efficient broadcast time-stamping. **Clarkson University, Department of Math and Computer Science**, [S.l.], Abril, 1992.

[BEN 94] BENALOH, J.; DE MARE, M. One-way accumulators: A decentralized alternative to digital signatures. **Advances in Cryptology - Proceedeings of Eurocrypt 93, LNCS 756**, [S.l.], p.274–285, Berlin, 1994.

[BUL 98a] BULDAS, A.; LAUD, P. New linking schemes for digital time-stamping. **The 1st International Conference on Information Security and Cryptology**, [S.l.], p.3–14, December, 1998.

[BUL 98b] BULDAS, A. et al. Time-stamping with binary linking schemes. **Advances in Cryptology - CRYPTO '98, LCNCS 1462**, [S.l.], 1998.

[BUL 98c] BULDAS, A.; LIPMAA, H. Digital signatures, time-stamping and corresponding infrastructure. Kberneetika AS, 1998. Technical report.

[BUL 00] BULDAS, A.; LIPMAA, H.; SCHOENMAKERD, B. Optimally efficient accountable time-stamping. **Public Key Cryptography '2000, LNCS 1751**, [S.l.], 2000.

[DAT] DATUM. www.datum.com. Disponvel em 22/03/2002.

[DEV 00] DEVEGILE, A. J. **FARNEL: Uma proposta de protocolo criptogrfico para votao digital**. Curso de Ps-Graduao de Cincia da Computao da Universidade Federal de Santa Catarina, 2000. Masterthesis.

[DIF 76] DIFFIE, W.; HELLMAN, M. New direction in criptography. **IEEE Transactions on Information Theory**, [S.l.], November, 1976.

[ETS 01] ETSI. Xml advanced electronic signatures (xades). European Telecommunications Standards Institute, 2001. Etsi ts 101 903 - technical specification.

[FEG 99] FEGHII, J. **Digital Certificates - Applied Internet Security**. Addison Wesley Longman, 1999.

[HAB 91] HABER, S.; STORNETTA, S. How to time-stamp a digital document. **Journal of Cryptology**, [S.l.], v.3, p.99–112, 1991.

[HAB 95] HABER, S.; KALISKI, B.; STORNETTA, S. How do digital time-stamps support digital signatures? **CRYPTOBYTES**, [S.l.], p.14–15, 1995.

[HOU 01] HOUSLEY, R.; POLK, T. **Planning for PKI - Best Practices Guide for Deploying Puclic Key Infrastucture**. 1. ed. Wiley, 2001.

[IT 00] ITU-T. The directory - authentication framework. 2000. Recommendation x509.

[JUS 98a] JUST, M. K. **On the Temporal Authentication of Digital Data**. School of Computer Science - Carleton University, December, 1998. Ph.d.

[JUS 98b] JUST, M. K. Some timestamping protocol failures. **Proceedings of the Internet Society Symposium on Network and Distributed Security (NDSS'98)**, [S.l.], 1998.

[LAI 91] LAI, X.; MASSEY, J. A proposal for a new block encryption standart. **Proceedings of EUROCRYPT'91**, [S.l.], 1991.

[LIP 99] LIPMAA, H. **SECURE AND EFFICIENT TIME-STAMPING SYSTEMS**. University of Tartu - Estonia, July, 1999. Ph.d.

[MAS 99] MASSIAS, H.; AVILA, X. S.; QUISQUATER, J.-J. Timestamps: Main issues on their use and implementation. **IEEE 8th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises**, [S.l.], 1999.

[NIS 77] NIST. Data encryption standart. National Bureal of Standards, 1977. Federal information processing standards publication 46.

[NIS 93] NIST. Secure hash standard. National Institute of Standards and Technology - Department of Commerce, May, 1993. Federal information processing standards publication 180.

[NIS 94a] NIST. Digital signature standard. National Institute of Standards and Technology - Department of Commerce, May, 1994. Federal information processing standards publication 186.

[NIS 94b] NIST. Security requirements for cryptographic modules. National Institute of Standards and Technology, January, 1994. Federal information processing standards publication 140.

[NIS 01] NIST. Advanced encryption standard (aes). National Institute of Standards and Technology, 2001. Technical report.

[PRE 98] PRENEEL, B. et al. Design of a timestamping system. Universit Catholique de Louvain, 1998. Technical report.

[RIV 78] RIVEST, R.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public key cryptosystems. **Communications of the ACM**, [S.l.], February, 1978.

[RIV 92] RIVEST, R. The md5 message digest algorithm. Network Working Group, April, 1992. Request for comments: 1321.

[RIV 94] RIVEST, R. The rc5 encryption algorithm. **Proceedings of Second International Workshop on Fast Software Encryption**, [S.l.], December, 1994.

[ROO 99] ROOS, M. **Integrating Time-Stamping and Notarization**. University of Tartu - Estonia, 1999. Masterthesis.

[SCH 93] SCHNEIER, B. Description of a new variable-length key, 64-bit block cipher (blowfish). **Proceedings of Workshop on Fast Software Encryption**, [S.l.], December, 1993.

[SCH 95] SCHNEIER, B. **Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition**. 2. ed. John Wiley and Sons, 1995.

[STA 98] STALLINGS, W. **Cryptography and Network Security**. 2. ed. Prentice Hall, 1998.

[STI 95] STINSON, D. R. **Cryptography : Theory and Practice**. CRC Press, 1995.

[SUR] SURETY. www.surety.com. Disponvel em 22/03/2002.

[TEC] TECNOLOGIA, B. www.bry.com.br. Disponvel em 22/03/2002.

[TEC 93] TECHNICAL, R. L. Pckcs #7 - cryptographic message syntax standard. RSA Data Security, November, 1993. Technical specification.

[TIM] TIMEPROOF. www.timeproof.com. Disponvel em 22/03/2002.

Apêndice A

FAQ sobre Datação de documentos Eletrônicos

1. **O que é data/hora?**

   Se esta pergunta fosse feita a Albert Einstein ele simplesmente responderia: "Tudo é Relativo", pois pela sua teoria nenhum tempo absoluto existe. Mas se fosse feita para uma pessoa comum (da área de exatas) ela responderia: "Data e hora é uma informação que estabelece referência temporal a um determinado evento".

2. **O que é datação?**

   Datação é o processo pelo qual é anexado data e hora em um documento. Esta data e hora deve condizer com a data e hora corrente, de modo a garantir que aquele documento existe em um determinado momento do tempo.

3. **Por que é necessário datar um documento?**

   A necessidade de se data um documento se torna evidente quando se queira provar que aquele documento existia naquela data, caso contrário, não existe maneira de se determinar se este documentos é ou não intempestivo. A datação nada mais é do que uma prova que o documento existia em uma determinada data e hora.

4. **O que é um documento intempestivo?**

Fora do prazo legal ou convencional preestabelecido; fora de tempo; inoportuno.

5. **Como pode ser datado um documento?**

Um documento em papel pode ser datado através de um carimbo que contenha data e hora confiável. Já um documento eletrônico recebe data e hora através de um processo conhecido como datação de documentos eletrônicos. O serviço de datação recebe o documento a ser datado, efetua um calculo único referente a aquele documento, anexa data e hora no resultado do calculo e o remete para cliente. Estas informações resultantes são chamadas de recibo datação.

6. **Quem pode datar um documento?**

Um documento pode ser datado por uma entidade autorizada pelo governo de modo que todas as suas datações sejam reconhecidas como válidas e integras perante a justiça.

Para o mundo em papel tal entidade é o Cartório, a qual é uma repartição incumbida de registro e guarda de documentos e de escrituras públicas. Serviços notariais e de registro são exercidos em caráter privado, por delegação do poder público.

Para o mundo digital, no Brasil ainda não existe tal entidade.

7. **Onde um documento pode ser datado?**

No conceito papel, o documento tem que ser datado por um cartório registrado, pois só ele detém a autorização legal para datar documentos. No conceito eletrônico, o documento pode ser datado em qualquer entidade que disponibilize um serviço de datação confiável. Hoje no Brasil não existe tal serviço.

Constituição Federal, artigo 239§§ 1 a 3; lei número 3.015/73 - registros públicos

Art. 239. Os serviços notariais e de registro são exercidos em caráter privado, por delegação do poder público.

§ 1. Lei regulará as atividades, disciplinará a responsabilidade civil e criminal dos notários, dos oficiais de registro e de seus prepostos, e definirá a fiscalização de seus atos pelo Poder Judiciário.

§ 2. Lei federal estabelecerá normas gerais para fixação de emolumentos relativos aos atos praticados pelos serviços notariais e de registro.

§ 3. O ingresso na atividade notarial e de registro depende de concurso público de provas e títulos, não se permitindo que qualquer serventia fique vaga, sem abertura de concurso de provimento ou de remoção, por mais de seis meses.

8. **Qual é a referência temporal utilizada para datar?**

Para se datar um documento precisa-se de uma referência de tempo confiável, a qual deve fornecer a data e hora exata para aquele momento. A referência mais recomendada para datar documentos é a data e hora instituída pelo *Coordinated Universal Time* (CUT). O CUT é o padrão de tempo universal definido em 1 janeiro de 1972, ele também é referenciado como *Greenwich Mean Time* (GMT). O CUT é sincronizado de acordo com o *International Atomic Time* (IAT) que é mantido pelo *Bureau International des Poids et Mesures* (BIPM).

9. **Existe um padrão de referência temporal mundial?**

É o *Coordinated Universal Time* (CUT). O CUT é o padrão de tempo universal definido em 1 janeiro de 1972, ele também é referenciado como *Greenwich Mean Time* (GMT)

10. **Como garantir a datação por um longo período de tempo?**

No conceito papel, o simples fato de se arquivar no cartório uma cópia de cada documento datado já pode ser considerado uma garantia de datação.

No conceito eletrônico, a responsabilidade em garantir a datação pro um longo período de tempo é da Autoridade de Datação, que é a entidade que disponibiliza o serviço de datação.

11. **Um documento eletrônico precisa ser datado para ter utilidade jurídica? Por que?**

Sim, porque para se garantir a validade legal de documentos deve ser utilizado o serviço de datação pois sem ele não se poderia confiar em documentos que somente

foram assinados digitalmente, não existindo forma de se provar a existência do documento antes da alegação do extravio da chave privada ou o comprometimento do algoritmo de assinatura utilizado.

12. **O que é uma Autoridade de Datação?**

É uma entidade responsável em disponibilizar um serviço de datação confiável e que siga os padrões e normas instituídos pelo governo brasileiro.

Esta entidade implementa uma tripla de protocolos (S,V,A). O protocolo de datação (*Stamping Protocol - S*) permite a cada usuário submeter um documento qualquer para ser datado. O protocolo de verificação (*Verification Protocol - V*) é usado por uma terceira entidade que tem posse de dois recibos para verificar a ordem temporal relativa entre eles. E o protocolo de auditoria (*Audit Protocol - A*) é usado pela entidade responsável em prestar o serviço de datação para verificar se a AD está fazendo o que ela tem que fazer, datar documentos

13. **Quais são as obrigações de uma Autoridade de Datação?**

Ela são :

- Não deve identificar o cliente que está requisitando o seu serviço de datação;
- Deve executar datações em rodadas, que são períodos de tempo bem definidos ou quantidades de solicitações máximo;
- Deve processar a requisição de datação assim que ela chega na AD;
- Deve assegurar as informações de cada rodada encadeando-as com o recibo da rodada anterior;
- Por definição, deve esperar até o fechamento da rodada para efetivar o encadeamento com a rodada anterior;
- Deve datar os documentos que são submetidos à rodada com a data e hora que do fechamento da rodada e não com a data e hora da submissão da solicitação de datação;

- O valor de cada recibo de rodada deve ser armazenado em um banco de dados e deve estar disponível para o verificador poder verificar os recibos;
- Cada valor publicado pela Autoridade em um diretório público deve ser assinado pela mesma, da mesma forma todos os recibos dos usuários também devem ser assinados;
- A periodicidade de publicação no diretório público é definida segundo a política adotada.

Apêndice B

Exemplo numérico do método Árvore Sincronizada

Por motivos didáticos e explicativos este anexo tem como objetivo esclarecer o funcionamento do novo método de datação chamado Árvore Sincronizada.

O exemplo conta com dois programas (cliente e servidor) que se comunicam via socket. O servidor é um programa DAEMON que escuta a porta 30000, de modo que toda e qualquer conexão estabelecida com esta porta é tratada, mas somente as requisições no padrão definido na RFC 3161 são reconhecidos. O Servidor é responsável em datar o resumo enviado, gerar um recibo válido definido na seção 4.2.3 do capítulo 4, assinar este recibo e envia-lo para o cliente. Já o programa cliente deve gerar o resumo do documento a ser datado e envia-lo no padrão de requisição definido na RFC 3161 para o servidor. Ele é responsável também em receber uma resposta e verificar sua validade.

Cada passo do processo de datação da Árvore Sincronizada pode ser visto como maiores detalhes como se segue:

Programa Cliente - PDDE Client

1. O usuário escolhe um documento texto para ser datado como o seguinte conteúdo: "PDDE TESTE";
   Lembrando que o cliente poderia escolher qualquer tipo de arquivo para ser datado.
2. O PDDE Client gera o resumo deste documento:

"BCEE0C904D5560EE341270FC050575F21F97145F"

E gera o pacote de requisição no padrão da RFC 3161:

Lembrando que o campo nonce é um número randomico gerado aleatoriamente para cada nova requisição seja ela para o mesmo resumo como para resumos diferentes.

Campo	Valor
version	1
reqpolicy	"1.1.1.1.1.1.1.1.11"
messageImprint.algorithmIdentifier	"00.0.0.1.3.14.3.2.26"
messageImprint.hashedMessage	BCEE0C904D5560EE341270FC050575F21F97145F
certReq	true
nonce	25976134

3. E envia este pacote via socket para a porta 30000 do servidor onde esteja rodado o servido de datação;

4. Ao receber o pacote de resposta do servidor, o PDDE Client verifica se é uma mensagem válida e se está no padrão da RFC 3161;

5. Verifica também se é uma mensagem de erro ou se é uma resposta de datação. Se for uma mensagem de erro o programa mostra a respectiva mensagem de erro. Se for uma resposta de datação o PDDE Client verifica se a assinatura do pacote é válida, se o nonce que ele tem é o mesmo que veio no pacote e se o resumo que ele enviou foi realmente datado.

Programa Servidor - PDDE Server

1. Recebe do cliente a requisição e verifica se é uma requisição válida e se está no padrão da RFC 3161;

2. Se não for válida retorna para o cliente uma resposta de erro definida na RFC 3161.

3. Se for válida o servidor consulta de sua base de dados o valor a ser encadeado com o novo resumo submetido. Este valor pode ser:

(a) o último recibo de rodada gerado, se a caso o resumo submetido for o primeiro a chegar na rodada corrente ou;

(b) o último valor encadeado para esta rodada.

Sendo assim, o valor consultado:
"51FE174CC4DDC1C3500563A7E5ED675DD2B4EA1E"
pode ser o último recibo de rodada ou o último valor encadeado. Para fins explicativos o valor consultado representa o último recibo de rodada R_{r-1}.

4. O servidor concatena as duas informações, o resumo submetido e o recibo de rodada R_{r-1}, através de uma função F para gerar o encadeamento L_1 . Para o nosso exemplo a função F é definida como sendo uma função resumo que utiliza o algoritmo SHA1. Temos:
   H_1:= BCEE0C904D5560EE341270FC050575F21F97145F
   R_{r-1}:= 51FE174CC4DDC1C3500563A7E5ED675DD2B4EA1E
   L_1:= $F(H_1,R_{r-1})$
   L_1:= F87C63CC496C661636703A4692EFB7482EC3982C

5. Dentro desta rodada mais outros dois resumos forma submetidos para o servidor gerando as seguintes informações:
   H_2:= 4C22151408084FF55A9F945AF9BEF848BFB4A65D
   L_2:= $F(H_2,L_1)$
   L_2:= 0FEBA8EB57476B794A8DBF82F9CC265B12B39443

   H_3:= 2FFF58EA2A5DFA4331BD0760D24756B97662719E
   L_3:= $F(H_3,L_2)$
   L_3:= CA85C882EA76B1C45DD7E2A5E2A1F2E6B3D0A1BA

6. Ao final da rodada, um único recibo é gerado, o qual representa todos os resumos submetidos nesta rodada. O recibo R_r é gerado da seguinte maneira:

$R_r := F(L_1, L_2, L_3, R_{r-1})$

$R_r :=$ A735DEDBBCF0E7AAD223FEBD21AC2A93D0E03B57

7. Com isto é produzido o pacote de resposta para todos os clientes que submeteram seus documentos para serem datados naquela rodada:

Campo	Valor
status.status	0
status.failInfo	0
timeStampToken.tstInfo.genTime	20020422100000.000Z
timeStampToken.tstInfo.version	1
timeStampToken.tstInfo.policy	"1.1.1.1.1.1.1.1.11"
timeStampToken.tstInfo.serialNumber	001
timeStampToken.tstInfo.messageImprint.algorithmIdentifier	"00.0.0.1.3.14.3.2.26"
timeStampToken.tstInfo.messageImprint.hashedMessage	BCEE0C904D5560EE341270FC050575F21F97145F
timeStampToken.tstInfo.link.algorithmIdentifier	"00.0.0.1.3.14.3.2.26"
timeStampToken.tstInfo.link.hashedMessage	F87C63CC496C661636703A4692EFB7482EC3982C
timeStampToken.tstInfo.nonce	25976134
timeStampToken.tstInfo.tsa	"PDDELABSEC"
timeStampToken.signature.algorithmIdentifier	"1.1.1.1.1.1.1.1.11"
timeStampToken.signature.detachedSignature.signlen	Depende do certificado emitido para a AD
timeStampToken.signature.detachedSignature.signature	Depende do certificado emitido para a AD