Sincronização Segura de Relógio para Documentos Eletrônicos

Júlio da Silva Dias[2*], Ricardo Felipe Custódio[1] , Denise Bendo Demétrio[1]

[1]Laboratório de Segurança em Computação – Universidade Federal de Santa Catarina
Centro Tecnológico - Departamento de Informática e de Estatística
Caixa Postal 476 – 88040-900 Florianópolis, SC

[2]Departamento de Ciência da Computação – Universidade do Estado de Santa Catarina
Campus Universitário Prof. Avelino Marcante S/N – 89223-100 Joinville, SC

jdias@inf.ufsc.br, custodio@inf.ufsc.br, denise@inf.ufsc.br

Abstract. *Trusted time sources are required to insert time stamps in electronic documents. A time stamped electronic document can be equiparated to tradicional paper document and has legal weight. Clock synchronization protocols of the sort provided by NTP do not satisfy all requirements to assure that a time source is trusted. This paper propose the use of external Certificate Authority (CA) issuing digital certificates to all computer systems that wants to synchronize its clock using NTPv4 protocol. It is also proposed the use of external auditors and a Time Stamp Authority (TSA) based on relative techniques to make this kind of service trustworthy. All modules inserted will not affect the normal operation of NTPv4 protocol.*

Resumo. *Uma fonte segura de tempo é necessária à efetiva equiparação legal dos documentos eletrônicos aos documentos tradicionais em papel. Os protocolos existentes de sincronização de relógio dos sistemas computacionais não atendem aos requisitos necessários para se considerar que uma fonte de tempo é confiável. Este trabalho propõe o uso de autoridades de certificação externas para a emissão de certificados digitais a todas as entidades envolvidas no processo de sincronização do tempo no protocolo NTPv4. Além disso, propõe o uso de auditores externos e protocolizadoras digitais baseadas em métodos relativos de datação para agregar a segurança e rastreabilidade necessárias. Todas as alterações propostas não afetam o funcionamento normal do protocolo NTPv4.*

1 Introdução

Documentos eletrônicos são utilizados em sistemas de informação, comunicação de dados e comércio eletrônico para garantir os requisitos de autenticidade, integridade e tempestividade das informações. A autenticidade e a integridade são construídas através de métodos criptográficos tais como assinatura digital e funções resumo [Stinson, 1995, Menezes, 1997]. A tempestividade é estabelecida por uma entidade

*Apoiado pela Universidade do Estado de Santa Catarina e CAPES.

confiável que produz o chamado carimbo de tempo (timestamp). Esta entidade é denominada de Protocolizadora Digital de Documentos Eletrônicos - PDDE (Time Stamping Authority) [Pasqual, 2002]. O uso de terceiras partes confiáveis, tal como uma PDDE, tem sido recomendado por vários autores e instituições para agregar confiança aos documentos eletrônicos [Müller, 2000]. Associada à tempestividade há preocupação quanto a vida útil do documento eletrônico em relação a validade tecnológica dos mecanismos criptográficos utilizados para garantir os requisitos de segurança acima listados. Outro ponto importante é a determinação do instante no tempo em que eventos relacionados aos documentos ocorreram. A âncora temporal nos documentos eletrônicos permite ainda comprovar a sua existência em determinado instante do tempo no passado e que desde então não foi alterado. Tudo isto tem estimulado a comunidade científica nacional e internacional a estudar formas para garantir a validade a longo prazo dos documentos eletrônicos [Deng, 2000, Notoya, 2002] e em particular a sincronização dos relógios dos sistemas de informação. As PDDEs fornecem parte da infra-estrutura legal para que documentos eletrônicos possam ser utilizados em larga escala. Um documento protocolizado e assinado de forma digital apresenta a âncora de confiança necessária para que este seja considerado legalmente válido [Bortoli, 2002]. A sincronização segura dos relógios é talvez o maior problema ainda a resolver.

De acordo com Lombardi [Lombardi, 2000], os sistemas computacionais utilizados atualmente apresentam duas formas de manutenção da informação temporal que nomearemos por: relógio operacional e relógio do sistema. O relógio operacional é responsável pela manutenção da informação temporal enquanto o equipamento está operando normalmente. O relógio do sistema é utilizado nos períodos em que o equipamento está desligado. No momento em que o equipamento é inicializado o sistema operacional se encarrega de ajustar o relógio operacional através da leitura do tempo atual fornecido pelo relógio do sistema. Na maioria dos sistemas computacionais compatíveis com IBM-PC o relógio do sistema tem uma resolução de 1 segundo enquanto que o operacional consegue uma resolução de 55 milisegundos. Outro ponto importante é a estabilidade do relógio ao longo do tempo. Os relógios, em geral, não apresentam boas características em relação a estabilidade, sendo possível perder ou ganhar tempo de acordo com variação de temperatura ou operações de reinicialização do sistema que provocam atrasos no relógio operacional. A âncora temporal de um documento eletrônico não pode estar sujeita a essas variações ou qualquer outro tipo de variação do relógio.

Para resolver estes e outros problemas relativos a manutenção da informação temporal dos sistemas computacionais distribuídos, procura-se sincronizar os relógios destes sistemas com fontes de tempo confiáveis. A informação temporal seria disseminada a partir destas fontes para todas as entidades que desejam manter seu relógio sincronizado.

No Brasil, através de uma iniciativa do governo federal, o Governo Eletrônico, estabeleceu-se um plano de metas [Brasil, 2000] para o uso de tecnologia da informação no âmbito da administração federal. O uso de documentos eletrônicos e assinaturas digitais se insere neste contexto. Para tanto o governo brasileiro através da medida provisória 2.200 de agosto de 2001 [Brasil, 2001] criou a ICP-Brasil, responsável pela infra-estrutura de chaves públicas brasileira[1]. A questão do tempo foi tratada no decreto 4.264 de 10 de junho de 2002 [Federal, 2002], onde reafirmou-se a competência do Observatório Naci-

[1] www.icpbrasil.gov.br

onal na geração e disseminação da hora legal brasileira. O Comitê Gestor da ICP-Brasil através da resolução 16 de junho de 2002 [ICP-Brasil, 2002] estabeleceu que os sinais primários para sincronização de freqüência e de tempo utilizados pela ICP-Brasil serão distribuídos pelo Observatório Nacional. Uma iniciativa a ser destacada é a da Rede Nacional de Pesquisas - RNP que tem realizado um esforço na disseminação da hora utilizando o protocolo NTP [Mills, 2002c]. O foco da RNP está, porém, nos relógios dos roteadores e nos registros de eventos dos sistemas computacionais que devem apresentar hora confiável para efeitos de auditoria [RNP, 2000].

O principal objetivo deste trabalho é propor um sistema de auditoria para um serviço de tempo seguro e confiável que permitirá a necessária rastreabilidade da disseminação do tempo. A rastreabilidade permite confirmar a origem do tempo utilizado nos documentos eletrônicos. Além disso é proposto uma alteração no NTPv4 relacionado ao modelo de segurança do protocolo, o que facilita a distribuição e validação dos certificados digitais utilizados nos processos de autenticação.

A seção 2 apresenta uma revisão sobre documentos eletrônicos e métodos de protocolização. A seção 3 realiza um levantamento dos principais protocolos utilizados na sincronização do relógio dos sistemas computacionais. A seção 4 detalha o protocolo NTPv4 que é utilizado como base na proposição do sistema para sincronização segura de relógios. Na seção 5 é apresentada a proposta do sistema de auditoria para a sincronização de relógios contemplando as características desejadas. Finalmente a seção 6 apresenta as considerações finais sobre o trabalho desenvolvido.

2 Documentos Eletrônicos e Métodos de datação

O documento eletrônico é uma seqüência de bits que com o auxílio de suporte computacional pode ter seu conteúdo revelado. O suporte computacional é fornecido por software capaz de traduzir as informações de um formato específico para informações legíveis com auxílio de hardware apropriado. Normalmente utiliza-se um computador com terminal de vídeo para realizar a visualização de um documento eletrônico.

A tempestividade nos documentos eletrônicos pode ser obtida através do uso da protocolização digital de documentos eletrônicos. Esta seção apresenta os principais métodos utilizados na protocolização de documentos eletrônicos.

2.1 Técnicas de Datação

Existem dois tipos de técnicas de datação: aquelas que trabalham com uma terceira entidade confiável (Autoridade de Datação - AD); e aquelas que são baseadas no conceito de confiança distribuída [Benaloh and de Mare, 1994, Benaloh and de Mare, 1992]. 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 vários elementos de um grupo de modo a convencer o verificador que não se poderia corromper todos os elementos simultaneamente [Massias et al., 1999, Just, 1998].

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

Privacidade: Ninguém além do cliente pode ter acesso ao conteúdo do documento;
Canal de comunicação e armazenamento: Deve ser prático datar o documento independentemente de seu tamanho;
Erro na comunicação: Deve-se garantir a integridade dos dados e a operação ininterrupta do serviço de datação;
Confiança: Deve-se garantir que um documento será datado com a data e hora correta;
Anonimato: Deve-se garantir o anonimato do cliente.

As técnicas baseadas em AD são mais indicadas do que as técnicas baseadas em confiança distribuída para o atendimento destes requisitos.

Para atender-se aos requisitos de privacidade, canal de comunicação, armazenamento e erro de comunicação 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 [Stallings, 1998]. Assim, ao invés de se transmitir o documento, o cliente transmite o resumo que é muito menor que o documento e não revela seu conteúdo.

Outro aperfeiçoamento realizado é a adição da assinatura digital ao esquema. Quando o resumo do documento chega para ser datado, a AD produz um recibo assinado contendo a data e hora e o resumo. O recibo é enviado ao cliente que verifica a validade da assinatura digital e do resumo, confirmando a protocolização do seu documento. Com isso garante-se também o requisito de erro na comunicação.

O anonimato pode ser obtido através de redes de misturadores [Chaum, 1995], roteamento de cebolas [Goldschlag et al., 1999], *web mixes* [Berthold et al., 2001] ou *crowds* [Reiter and Rubin, 1998]. O anonimato oculta a identidade dos clientes perante a AD. É um complemento desejável mas existem situações onde não há a sua necessidade, tais como num procedimento de tarifação.

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 necessidade de confiança à uma terceira entidade, neste caso o auditor. O ideal seria que a AD não pudesse ser maliciosa. Isso já é possível utilizando-se alguns dos métodos descritos a seguir. Estes métodos levam em consideração a questão temporal, ou seja, como o documento recebe a data e hora. Ela pode ser **absoluta**, **relativa** ou **ambas**. A autenticação temporal absoluta contém informações de data e hora igual a usada no mundo real. Já a relativa contém informações que somente verificam se um documento foi datado antes ou depois de um outro documento [Roos, 1999, Just, 1998].

Qualquer um dos esquemas de datação descritos acima podem ser usados para se datar documentos, mas o absoluto pressupõe que a AD seja uma entidade confiável. Já no relativo, não é necessária a existência de entidade confiável, pois existem mecanismos que garantem que o documento sempre será datado com data e hora correta [Haber and Stornetta, 1991].

No esquema relativo, a AD encadeia todos os resumos dos documentos em uma cadeia utilizando uma função resumo *H*. Neste caso o recibo s_n de datação para o n-ésimo

documento H_n é dado por [Lipmaa, 1999]:

$$s_n = Sig_{AD}(n, t_n, ID_n, H_n, L_n) \quad (1)$$

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

$$L_n = (t_{n-1}, ID_{n-1}, H_{n-1}, H(L_{n-1})) \quad (2)$$

onde t_{n-1} e ID_{n-1} são a data e hora e o identificador do documento anteriormente protocolizado, H_{n-1} é o resumo do documento anterior e $H(L_{n-1})$ é o resumo do link anterior. L_1 é um valor arbitrário de conhecimento público. A figura 1 ilustra como seria este encadeamento com n elementos.

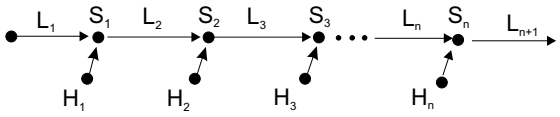

Figura 1: Esquema de encadeamento linear.

Com isto, associa-se a datação atual com a anterior afim de se obter uma seqüência de recibos ordenados por ordem de chegada.

O Método da Árvore Sincronizada proposto por Pasqual [Pasqual et al., 2002] utiliza o método de datação relativa e absoluta simultaneamente, apresentando esquemas adicionais que garantem melhor desempenho quando comparado com métodos tradicionais, além de possibilitar a auditoria interna e externa .

3 Protocolos de Sincronização de Relógios

A obtenção de informação temporal com resolução e precisão adequada poderia ser realizada utilizando-se relógios atômicos. Estes relógios têm excelente precisão e são denominados padrões primários de tempo [Lombardi, 2000]. Todavia apresentam elevado custo material e de manutenção, não sendo viável equipar todos os sistemas computacionais com os mesmos. Uma possível solução é a disseminação da informação temporal dos padrões primários através de redes de comunicação de dados e outros meios de comunicação para que todos os equipamentos possam se manter sincronizados.

Os protocolos apresentados a seguir buscam resolver o problema da disseminação da informação temporal de forma confiável. As várias formas de sincronização de relógios existentes diferem basicamente pela resolução atingida e pelo meio de comunicação utilizado para disseminar a informação de tempo. A necessidade de sincronização de relógios fez com que ao longo do tempo fossem desenvolvidas tecnologias que permitem que esta tarefa seja realizada com sucesso de forma mais independente possível dos meios de comunicação e localização das partes. Atualmente, a disseminação de informação de tempo pode ser realizada através de sinais de rádio, acesso telefônico ou através de redes de comunicação de dados como a Internet [Lombardi, 2000].

Nesta seção apresentam-se os protocolos ACTS, IRIG, GPS e NTP que são comumente utilizados no processo de sincronização de relógios. É importante salientar

que além destes há uma grande quantidade de outros protocolos e mecanismos para sincronização de relógios [Allan and et All, 1998].

O protocolo de sincronização ACTS (Automated Computer Time Service) estabelece uma forma de sincronização entre um relógio qualquer e um relógio padrão através de linha discada convencional com a utilização de modem analógico [Nist, 2000]. O computador a ser sincronizado conecta-se ao servidor ACTS e recebe a informação de tempo codificada em código ASCII. Esta informação é utilizada para ajuste do relógio do computador ao relógio padrão.

A sincronização através de sinais de rádio é outra forma utilizada. Há uma grande quantidade de padrões que utilizam esta forma de disseminação de informação de tempo entre os quais tem-se IRIG e GPS. O IRIG (Inter-Range Instrumentation Group) é uma família de padrões definido no documento IRIG 205-87 [IRIG, 1987]. O IRIG foi desenvolvido como infra-estrutura para transferência de dados entre instalações de teste de mísseis do governo americano. Este codifica a informação de tempo utilizando modulação por amplitude ou largura de pulso. O protocolo IRIG-B é o mais utilizado desta família.

Outro protocolo bastante comum é o Sistema de Posicionamento Global (GPS) [Allan and et All, 1998]. O GPS, pertencente ao Departamento de Defesa Norte Americano, conta com 24 satélites em seis planos orbitais inclinados em 55º em relação ao plano equatorial. Através do uso do GPS pode-se obter informação para sincronização de relógios com resolução de até 100ns.

Os protocolos baseados em rádio necessitam de um equipamento receptor de rádio freqüência e antenas. Estes equipamentos apresentam elevado custo e são de difícil manutenção. O protocolo ACTS necessita somente de um modem, todavia toda vez que é necessário realizar um sincronismo deve-se estabelecer uma conexão discada na forma de uma ligação de longa distância que não é economicamente aceitável em muitas aplicações.

Redes de comunicação de dados baseadas no protocolo TCP/IP, como a Internet, são encontradas em todas as partes do mundo tornando-se um meio de comunicação natural para disseminação da informação temporal. Neste sentido foram desenvolvidos vários protocolos para o sincronismo entre relógios, dentre os quais pode-se citar: Time Protocol [Postel and Harrenstien, 1983], Daytime Protocol [Postel, 1983], Network Time Protocol - NTP [Mills, 1992, Mills, 2002c] e Simple Network Time Protocol - SNTP [Mills, 1996]. O protocolo mais utilizado atualmente é o NTP. Na seção 4 o protocolo NTP tem sua funcionalidade detalhada.

A principal motivação para continuar a usar os protocolos ACTS, IRIG e GPS está na confiabilidade da fonte de tempo. Nestes o cliente tem uma maior confiança no provedor, apesar dos custos associados. Acredita-se que o NTP substituirá estes na medida em que seja agregado confiança ao mesmo.

4 Protocolo NTP

O protocolo NTP é usado para sincronizar o relógio de um computador cliente ou servidor a outro servidor ou fonte de referência de tempo, utilizando como meio de comunicação redes baseadas no protocolo TCP/IP tal como a Internet [Deeths, 2001a, Deeths, 2001b,

Deeths, 2001c]. O protocolo provê uma precisão de milisegundos em redes locais (LANs) e algumas dezenas de milisegundos em redes de longa distância (WANs) relativo ao Tempo Universal Coordenado UTC[2].

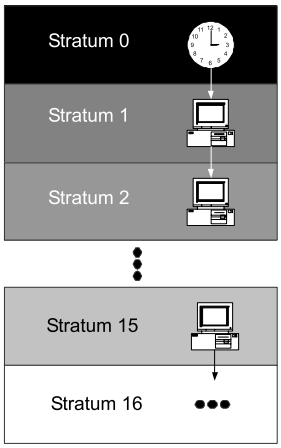

Figura 2: Strata do NTP.

De acordo com Mills [Mills, 1999] o protocolo NTP teve sua primeira versão desenvolvida na Universidade de Maryland em 1985 por Louis Mamakos e Michel Petry. A primeira especificação formal foi apresentada na RFC-958. Atualmente a iniciativa de desenvolvimento do protocolo é coordenada por David L. Mills da Universidade de Delaware. O NTP utiliza o conceito de stratum, isto é, uma camada na rede de sincronização. Quanto mais próximo estiver o cliente da fonte de tempo confiável, mais baixo será o seu stratum. Uma fonte de tempo confiável, como por exemplo um relógio atômico, está no stratum 0. O computador conectado diretamente a ela é um stratum 1 e assim por diante. O stratum mínimo para um computador é 1 e o máximo é 15, sendo que no stratum 16 são enquadrados todos as entidades que não possuem um relógio sincronizado com uma fonte de tempo confiável. A figura 2 ilustra o esquema de stratum.

Tipicamente, configurações NTP utilizam vários servidores redundantes e diversos caminhos de rede para alcançar uma maior robustez. O protocolo NTP estabelece que as entidades envolvidas podem associar-se utilizando três modos básicos:

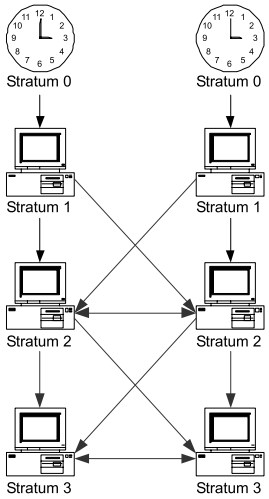

Figura 3: Representação Típica.

Cliente/Servidor a entidade cliente sempre requisita informação para sincronismo de relógio de servidor que apresenta stratum mais baixo possível.

Ponto a Ponto as entidades podem atuar como clientes ou servidores de acordo com seu posicionamento com relação aos relógios confiáveis;

Multicast/Broadcast fornece a descoberta automática de servidores NTP através de mensagens multicast ou broadcast.

O NTP pressupõe que há pelo menos uma fonte de tempo confiável e que o tempo que esta fonte oferece é transmitido a toda ”rede NTP” de forma segura e precisa. Os clientes NTP são conectados a vários servidores com stratum mais baixo possível e com o menor caminho de rede entre eles. A figura 3 ilustra uma representação da arquitetura típica do NTP.

[2]UTC (Coordinated Universal Time) é a medida oficial de tempo no mundo e é independente de zonas de tempo. O fluxo do tempo UTC é como o do TAI (Temps Atomique International), ou seja, é o tempo computado com métodos estatísticos para minimização de erros do tempo entre aproximadamente 200 relógios atômicos de cesium em cerca de 60 laboratórios metrológicos do mundo - exceto pela inserção dos leap seconds. Leap seconds são segundos que são adicionados ou subtraídos para corrigir a desaceleração da rotação da Terra.

O protocolo NTP apresenta uma série de mecanismos para garantia de serviço seguro. O mais importante destes mecanismos é a redundância de servidores e a inserção de ”timestamp” nas mensagens que torna o NTP resistente a falhas e ataques de repetição de mensagens.

A partir da versão 2 do NTP há uma preocupação quanto a autenticação das entidades envolvidas. Na versão 2, em particular, foi definido um mecanismo rudimentar de autenticação baseado em lista de acesso. Esta lista, mantida pelo servidor, contém os endereços IPs dos clientes autorizados. Um esquema de autenticação mais elaborado baseado em criptografia simétrica também foi incluído na versão 2 e está presente em todas as versões posteriores (3 e 4). Neste esquema, o servidor gera uma lista de chaves simétricas que são distribuídas a todos os clientes que farão uso do serviço, o que permite que as entidades envolvidas possam autenticar-se mutuamente. Assim qualquer comunicação entre as entidades pode ter sua autenticidade e integridade verificadas. Para a troca de mensagens, o protocolo determina que deve-se calcular o ”hash” do pacote, cifrá-lo com a chave secreta, distribuída pelo fornecedor, e concatená-lo à mensagem. Desta forma as mensagens trocadas pelos clientes e servidores tem garantia de integridade e autenticidade fornecida através do uso de chave que somente é conhecida pelas partes envolvidas.

Entretanto, este esquema tem como maior problema a distribuição das chaves. Para resolução deste problema foi proposta na versão 4 a adoção do protocolo Autokey que será descrito a seguir.

O protocolo Autokey [Mills, 2002b] utiliza certificados digitais para identificação dos servidores. Certificados digitais são documentos eletrônicos assinados por uma Autoridade Certificadora (AC), que contém o nome do proprietário, a entidade emissora, a chave pública do proprietário e o período de validade do certificado. No NTPv4 são utilizados certificados auto-assinados. Um certificado digital auto-assinado é um certificado assinado com a própria chave privada do proprietário do certificado.

O protocolo NTP com Autokey apresentam os seguintes passos:

- O servidor S gera um certificado digital auto-assinado;
- O cliente C copia o certificado de S ou o solicita através de uma mensagem apropriada. No caso de uma solicitação C deve possuir o endereço IP de S. C recebendo o certificado verifica se o nome corresponde ao IP que ele tem em sua base é o mesmo que o obtido através de protocolo para resolução de nomes (DNS);
- C após obter as credenciais do servidor envia uma requisição de um Cookie, que é uma informação a ser utilizada enquanto as entidades estiverem associadas.
- S calcula o Cookie baseado em informações públicas (endereços IPs do cliente e servidor, identificação da chave a ser utilizada) e números randômicos e o envia assinado ao cliente;
- C verifica a assinatura digital e gera a lista de chaves a ser utilizada na comunicação;
- Uma vez que as partes apresentam chaves simétricas comuns entra-se num estado onde há somente troca de informações para sincronismo de relógio de C.

O modelo de confiabilidade oferecido atualmente pelo NTP consiste em usar vários servidores como fonte de sincronismo de relógio. A falha ou comprometimento

de uns poucos servidores será dificultada pois para que algum elemento corrompa o sistema, este deverá corromper vários servidores simultaneamente, o que provavelmente não acontecerá. Os servidores maliciosos ou com mau funcionamento são descartados sem prejuízo ao sincronismo. O descarte dos servidores que apresentem dados incorretos é realizado pelo cliente utilizando-se métodos estatístico [Mills, 1997].

O NTP, em todas as suas versões, não prevê esquemas de auditoria. Esta lacuna fez com que algumas entidades propusessem sistemas alternativos de auditoria dos serviços de distribuição de tempo. O sistema de auditoria da empresa Wetstone [INC, 2001], denominado Sovereign Time, realiza verificações periódicas emitindo certificado de garantia para as partes envolvidas. Este mecanismo busca:

- Garantir que todos os elementos envolvidos estão sincronizados com uma fonte confiável;
- Garantir que as informações de tempo não foram manipuladas de forma maliciosa;
- Gerar evidências que garantam a rastreabilidade dos eventos ocorridos;
- Garantir o não repúdio por parte dos elementos envolvidos;
- Manutenção de registros confiáveis dos eventos ocorridos.

Contudo, este sistema de auditoria tem várias vulnerabilidades, destacando-se:

- Um servidor ao ser auditado, conhece a identidade do auditor e pode agir de forma maliciosa perante este;
- O registro dos eventos é feito por datação absoluta o que não garante a rastreabilidade dos eventos como foi exposto na seção 2. As partes agindo de maneira maliciosa podem inserir eventos posteriormente;
- Os clientes ficam em posição de desvantagem uma vez que não tem como comprovar a sua honestidade diante de servidores ou auditores desonestos.

5 Proposta de Protocolo de Acesso e Auditoria

O projeto do NTP foi desenvolvido para obtenção de precisão e resolução na disseminação do tempo [Mills, 2002a]. Contudo, existem muitas situações onde é necessário a rastreabilidade do tempo fornecido, como é o caso do sistema de pagamentos brasileiro - SPB[3]. As versões 2, 3 e 4 do NTP tem evoluído com relação a segurança, mas nenhuma delas se preocupa com a autenticação do requisitante do tempo (o cliente), autenticando apenas o servidor de tempo. A autenticação do requisitante é interessante para possibilitar o rastreamento dos seus clientes, verificando se este está operando corretamente e também possibilitando a tarifação do serviço ofertado.

Propõe-se, para possibilitar este novo serviço de segurança, o uso de autoridades certificadoras externas - AC[4] que permitem a autenticação dos requisitantes de tempo através de certificados digitais. Busca-se com isso obter uma maior confiabilidade entre os clientes e servidores de tempo ou entre os pares.

Além da AC externa, propõe-se a inclusão de novos módulos de autenticação e auditoria obtendo-se uma estrutura complementar, que permite um maior controle do sistema sem prejuízo à informação temporal a ser disseminada.

[3] http://www.bcb.gov.br

[4] Autoridade certificadora externa é uma autoridade que emite certificados digitais, sendo autorizada por um órgão competente

O protocolo NTPv4 garante a disseminação da informação de tempo, mas não apresenta garantias completas contra elementos maliciosos. De acordo com Mills [Mills, 2002b] a inclusão de funções criptográficas adicionais levariam a perca de precisão da operação de sincronização uma vez que o tempo gasto nestas operações não pode ser determinado e corrigido. As informações para auditoria do serviço devem somente ser obtidas dos registros de eventos armazenados pelos servidores envolvidos. Devido a isso, os módulos adicionais aqui propostos são todos externos ao NTP, evitando qualquer perturbação no seu funcionamento normal.

A solução proposta apresenta uma estrutura semelhante a uma hierarquia NTP conforme ilustra a figura 4, com a inclusão das seguintes entidades:

Auditor: Entidade responsável pelo controle das atividades das entidades envolvidas no processo de sincronização de relógios;

PDDE: Entidade que realiza a protocolização digital de documentos. Neste caso os documentos protocolizados são informações temporais requisitadas pelo auditor às demais entidades bem como registros de eventos das partes envolvidas;

AC/LCR: A Autoridade Certificadora e a Lista de Certificados Revogados que garantem a identidade das entidades envolvidas.

A arquitetura proposta busca alcançar um sistema no qual todos os elementos envolvidos sejam identificados e tenham sua informação temporal avaliada por auditor externo. Propõe-se a utilização do protocolo NTPv4 [Mills, 2002a] como provedor do serviço de sincronismo entre os relógios. Apesar de estar em processo de desenvolvimento, testes preliminares realizados em nosso laboratório tem mostrado a sua estabilidade e robustez.

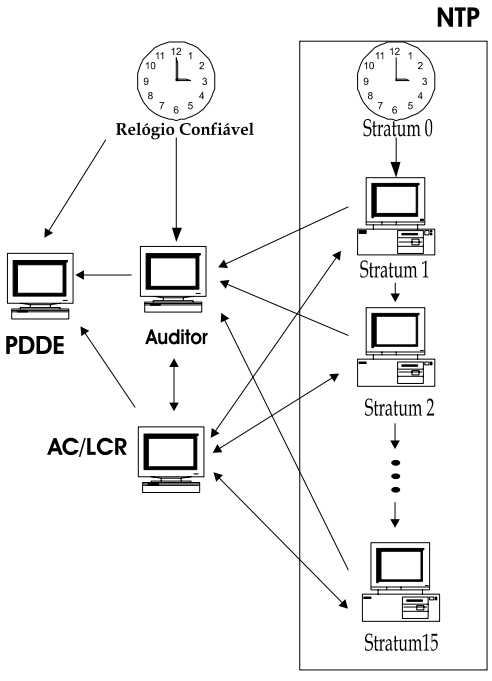

Figura 4: Arquitetura do Esquema de Auditoria.

O auditor na presente proposta atua de forma anônima, não sendo reconhecido como tal pelas demais entidades. De fato, o Auditor personifica qualquer entidade cliente ou servidora de tempo normal do NTP. Desta forma dificulta-se a atuação de entidades maliciosas dentro do sistema. O auditor requisita periodicamente informação temporal a todos as entidades participantes. Esta informação é armazenada e sua análise fornece evidências para identificar os possíveis elementos maliciosos na estrutura. O Auditor, através do conhecimento da estrutura do sistema de sincronismo de relógio, pode fornecer a informação de rastreabilidade necessária num processo de disputa.

Partindo-se do princípio que o próprio auditor pode apresentar comportamento malicioso foi adicionada uma PDDE. Os dados coletados são todos protocolizados que utiliza método relativo/absoluto. A utilização do Método da Árvore Sincronizada [Pasqual et al., 2002] garante a impossibilidade de fraude por parte do auditor. Este não tem como alterar os dados coletados sem ser descoberto.

O Auditor e a PDDE tem seus relógios sincronizados diretamente de um padrão primário de tempo ou de um conjunto de servidores de informação temporal confiáveis.

Um elemento essencial para a presente proposta é a utilização de uma Autoridade Certificadora - AC externa. Esta AC apresenta dupla funcionalidade:

- Garantia da identidade das partes envolvidas no processo de sincronização de relógios;
- Fornecedora de certificados digitais habilitando as entidades a participarem do sistema.

A AC fornece certificados digitais para todos os elementos participantes da estrutura. Somente elementos que apresentem um certificado digital válido são considerados confiáveis e tem acesso ao serviço de sincronismo seguro de relógio. A autenticação mútua realizada no momento do estabelecimento de uma associação entre clientes e servidores permite ou não que o serviço de sincronização seja executado. A utilização de certificados emitidos por AC externa confiável reforça o controle sobre as entidades do sistema.

O auditor tendo verificado que uma entidade apresenta comportamento anormal pode, uma vez comprovado a tentativa de fraude por parte desta entidade, requisitar junto à AC a revogação do certificado digital da entidade maliciosa, sendo desta forma excluída do sistema seguro.

Uma entidade pode, opcionalmente, requisitar os serviços de uma PDDE para garantir seus registros de eventos. Isso permite a comprovação de que a entidade não agiu de forma maliciosa, caso seja necessário. Um comportamento anormal desta entidade pode ser devido a comportamento anormal de outras entidades. Os registros mantendo todas as requisições que a entidade enviou aos outros participantes bem como suas respostas pode comprovar que a mesma não se comportou de forma maliciosa.

Propõe-se que este mecanismo seja instalado como um módulo do protocolo NTPv4. Desta forma o funcionamento já estabelecido do NTP não será alterado, sendo somente adicionadas as novas funcionalidades. É importante destacar que entidades clientes e servidores NTP, mesmo que não sejam identificadas pelo Auditor, podem participar do sincronismo de relógio, de forma natural conforme estabelece o NTPv4. Contudo, estas entidades não forneceriam um serviço de tempo seguro e certificado.

O esquema proposto apresenta como características principais:

- O uso de auditores anônimos, dificultando a localização dos auditores por parte de servidores maliciosos;
- O uso de autoridades de datação que utilizem o Método da Árvore Sincronizada, não permitindo que o auditor possa fraudar os resultados da análise inserindo dados em instante posterior ao da coleta;
- O uso de certificados digitais emitidos por Infra-estrutura de chaves públicas

oficial, aumentando a confiabilidade das atividades das entidades envolvidas no serviço;
- O uso da Lista de Certificados Revogados - LCR na garantia da qualidade dos serviços oferecidos pelas entidades do sistema.

6 Considerações Finais

O sistema de auditoria proposto possibilita o rastreamento e a agregação de confiança ao sincronismo dos relógios dos sistemas computacionais utilizados na manipulação de documentos eletrônicos. O levantamento dos protocolos e mecanismos existentes para a disseminação da informação temporal mostrou a fragilidade destes em relação à auditoria dos serviços ofertados e à necessidade de melhoria da autenticação das partes envolvidas.

O sistema de auditoria garante a disseminação de tempo de forma segura e confiável, com a obtenção de evidências que confirmem a origem do tempo utilizado nas transações eletrônicas, obtendo-se assim a necessária rastreablilidade do sistema.

O uso de Autoridades Certificadoras externas ao protocolo NTPv4 facilita a administração e distribuição das chaves de sessão além de possibilitar o controle dos servidores por parte de um auditor.

O sistema foi concebido de forma a minimizar as alterações no NTPv4. A inserção das novas funcionalidades não altera os princípios básicos de funcionamento do protocolo NTP, não havendo impacto significativo na transição para a nova estrutura.

A oferta de um serviço de tempo seguro possibilita uma maior confiança na âncora temporal dos documentos eletrônicos. O uso das evidências fornecidas pelo serviço proposto podem ser fundamentais na resolução de disputas no momento em que o uso de documentos eletrônicos e assinaturas digitais se disseminar nos sistemas de informação em geral.

Referências Bibliográficas

Allan, D. W. and et All (1998). The science of timekeeping. Technical Report 1289, Hewlett Packard.

Benaloh, J. and de Mare, M. (1992). Efficient broadcast time-stamping. *Clarkson University, Department of Math and Computer Science*.

Benaloh, J. and de Mare, M. (Berlin, 1994). One-way accumulators: A decentralized alternative to digital signatures. *Advances in Cryptology - Proceedeings of Eurocrypt 93, LNCS 756*, pages 274–285.

Berthold, O., Federrath, H., and Köpsell, S. (2001). Web mixes: a system for anonymous and unobservable internet access. In *Designing Privacy Enhancing Technologies*, pages 115–129. International Workshop on Design Issues in Anonymity and Unobservability.

Bortoli, D. L. (2002). O documento eletrônico no ofício de registro civil de pessoas naturais. Master's thesis, Curso de Pós-Graduação em Ciêncioa da Computação da Universidade Federal de Santa Catarina.

Brasil (2000). Proposta de política de governo eletrônico para o poder executivo federal. Proposta do Grupo Técnico de Novas Formas Eletrônicas de Interação.

Brasil (2001). Medida provisória 2.200-2. Media Provisória que instituíu a ICP-Brasil.

Chaum, D. C. (1995). Untraceable electronic mail, return address, and digital pseudonyms. *Communications of ACM*, 24(2):84–88.

Deeths, D. (2001a). Using NTP to control and synchronize system clocks. Technical report, Sun Microsystems.

Deeths, D. (2001b). Using NTP to control and synchronize system clocks - part II: Basic NTP administration and architecture. Technical report, Sun Microsystems.

Deeths, D. (2001c). Using NTP to control and synchronize system clocks - part III: NTP monitoring and troubleshooting. Technical report, Sun Microsystems.

Deng, J. Z. R. (2000). On the validity of digital signatures. *Computer Communications Review*, 30(2):29–34.

Federal, G. (2002). Decreto lei 4.264.

Goldschlag, D., Reed, M., and Syverson, P. (1999). Onion routing for anonymous and private internet connections. *Communications of ACM*, pages 39–41.

Haber, S. and Stornetta, S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, 3:99–112.

ICP-Brasil, C. G. D. (2002). RESOLUÇÃO no 16. Resolução que determina o Observatório Nacional como fornecedor da hora legal brasileira para a ICP-Brasil.

INC, W. T. (2001). Application of sovereign time to business and legal markets. Withe paper, Wetstone Technologies INC.

IRIG (1987). Irig standard 205-87. Range Commanders Council of the US Army White Sands Missile Range.

Just, M. K. (1998). *On the Temporal Authentication of Digital Data*. Ph.d., School of Computer Science - Carleton University.

Lipmaa, H. (1999). *SECURE AND EFFICIENT TIME-STAMPING SYSTEMS*. Ph.d, University of Tartu - Estonia.

Lombardi, M. (2000). Computer time synchronization. Technical report, National Institute of Starndards and Technology.

Massias, H., Avila, X. S., and Quisquater, J.-J. (1999). Timestamps: Main issues on their use and implementation. *IEEE 8th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*.

Menezes, P. V. O. S. V. A. (1997). *HandBook of Applied Criptography*. CRC Press, Boca Raton, FL - USA, 1 edition.

Mills, D. L. (1992). RFC 1305: Network time protocol (version 3) specification, implementation.

Mills, D. L. (1996). RFC 2030: Simple network time protocol (sntp) version 4 for ipv4, ipv6 and osi.

Mills, D. L. (1997). Authentication scheme for distributed, ubiquitous, real - time protocols. *Advanced Telecommunications/Information Distribution (ATIRP) Conference*.

Mills, D. L. (1999). Cryptography authentication for real-time network protocols. *AMS DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 45:135–144.

Mills, D. L. (2002a). *NTP Documentation*. http://www.eecis.udel.edu/ ntp/documentation.html.

Mills, D. L. (2002b). NTP implementation manual. Publicado eletrônicamente no sítio. Visitado em outubro de 2002.

Mills, D. L. (2002c). RFC 2026: Public key cryptrography for the network time protocol.

Müller, R. (2000). ISO/IEC 18014-1: Information technology - security techniques - time stamping services - part 1: Framework. Norma Estabelecendo Time Stamping Services.

Nist (2000). *Federal Emergency Management Information Systems*. NIST, Estados Unidos.

Notoya, A. E. (2002). Iarsde- infra-estrutura de armazenamento e recuperação segura de documentos eletrônicos. Master's thesis, Curso de Pós-Graduação em Ciêncioa da Computação da Universidade Federal de Santa Catarina.

Pasqual, E. S. (2002). Idde - uma infra-estrutura para a datação de documentos eletrônicos. Master's thesis, Curso de Pós-Graduação em Ciêncioa da Computação da Universidade Federal de Santa Catarina.

Pasqual, E. S., Dias, J. D. S., and Custódio, R. F. (2002). A new method for digital time-stamping of electronic document. In FIRST, editor, *Proceedings of the FIRST 14th Annual Computer Security*, 212 West Washington, Suite 1804 Chicago, IL 60606. Phoebe J. Boelter Conference and Publication Services, Ltd.

Postel, J. (1983). RFC 867: Daytime protocol.

Postel, J. and Harrenstien, K. (1983). RFC 868: Time protocol.

Reiter, M. K. and Rubin, A. D. (1998). Crowds: anonymity for Web transactions. *ACM Transactions on Information and System Security*, 1(1):66–92.

RNP (2000). Implementando o serviço ntp na sua rede local. Technical report, Rede Nacional de Pesquisas, Rio de Janeiro.

Roos, M. (1999). Integrating time-stamping and notarization. Masterthesis, University of Tartu - Estonia.

Stallings, W. (1998). *Cryptography and Network Security*. Prentice Hall, 2 edition.

Stinson, D. R. (1995). *Cryptography – Theory and Practice*. CRC Press, Boca Raton.