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

Juliano Romani

Integração de Serviços de Relógio para Infra-estrutura de Chaves Públicas

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

Florianópolis, Agosto de 2009

Integração de Serviços de Relógio para Infra-estrutura de Chaves Públicas

Juliano Romani

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

Frank Siqueira

Coordenador do Curso

Banca Examinadora

Prof. Ricardo Felipe Custódio, Dr.

Orientador

Prof. Frank Siqueira, Dr.

Profa. Carla Merkle Westphall, Dra.

Prof. Joni Fraga, Dr.

"Esse é o trabalho do analista: libertar o estágiário desse inferno."
Júlio Zeremeta

A minha família e minha namorada por tornar isso possível.

Agradecimentos

Primeiramente quero agradecer ao meu orientador, o professor Ricardo Felipe Custódio por acreditar em mim, e me convidar para esse grande trabalho com ele.

Aos professores Frank Siqueira, Carla Merkle Westphall, Joni Fraga, Dalton Francisco de Andrade e Paulo José Ogliari pelas contribuições e auxílios.

Aos meus pais, que sempre me apoiaram na minha vida e depositaram grande confiança em mim.

A minha namorada, Rubia Gomes Flores, pelo seu apoio e incentivo, que sem ela, esse trabalho não terminaria.

Aos meus amigos do LabSEC, que sempre ajudaram nos problemas e nas soluções. E nas festas feitas com eles.

Sumário

Lista de Figuras

Lista de Tabelas

Resumo

O carimbo de tempo é usado como prova, para referenciar que uma informação existia no passado. Para saber que hora é agora, usa-se o sincronismo de tempo. Para enviar uma informação para o futuro, utiliza-se o certificado digital temporal. O Módulo de Relógio Seguro provê serviços de tempo, como Autoridade de Carimbo de Tempo, Sincronismo de Relógio e Autoridade Certificadora Temporal, mantendo seu relógio sincronizado com uma Fonte de Tempo Confiável, através de um gestão segura do relógio.

Abstract

Capítulo 1

Introdução

Para o uso adequado dos serviços de criptografia pelas aplicações é necessário o estabelecimento de uma Infra-estrutura de Chaves Públicas. A Infra-estrutura de Chaves Públicas abstrai os detalhes tecnológicos da criptografia das aplicações e dos usuários. A Figura 1.1 demonstra isso.

Figura 1.1: Uso de serviços de criptografia pelas aplicações

Um dos elementos básicos de uma ICP é o uso do tempo pelos seus componentes. Para isso existem vários relógios distribuídos nos servidores que hospedam estes componentes.

Nos sistemas computacionais o tempo é utilizado para se determinar a precedência entre eventos ou quando um evento ocorre, permitir a comunicação cooperada entre processos ou estabelecer quando uma tarefa deve ser executada. Por isso, todos os computadores têm um relógio que permite registrar o tempo com determinada precisão e exatidão.

Uma análise mais cuidadosa do uso do tempo nos sistemas computacionais mostra que os serviços de tempo podem ser classificados em três grupos: passado;

presente; futuro. No passado, o registro de tempo pode ser usado como evidência de que uma informação digital existia naquele instante de tempo. O serviço que permite realizar esta tarefa é conhecido como carimbo de tempo. No presente, o tempo é usado nas cooperações entre diversos computadores, cada um com seu próprio relógio, os quais precisam estar sincronizados, para que uma determinada tarefa seja executada com sucesso. No futuro, a informação temporal é usada, por exemplo, para controlar o instante de tempo em que será liberada uma informação secreta ou quando uma tarefa deve ser executada.

O carimbo de tempo é emitido e assinado por um servidor de carimbo de tempo (SCT), que deve ter seu relógio sincronizado a uma fonte de tempo confiável. O carimbo serve como evidência de que uma informação digital já existia quando ele foi emitido. Um dos principais usos do carimbo de tempo é no processo de assinatura digital de documentos eletrônicos. A informação de quando foi realizada a assinatura digital de um documento eletrônico deve ser incorporada ao documento tal que seja possível garantir sua autenticidade.

No presente, o tempo é necessário para que tarefas sejam executadas de forma sincronizadas ou em um determinado instante de tempo estabelecido. As tarefas podem ser distribuídas em vários sistemas, formando um sistema distribuído. A cooperação entre as tarefas nos sistemas distribuídos utiliza protocolos de comunicação e criptografia. Para permitir essa cooperação é necessário que o relógio também seja distribuído. Manter esses relógios distribuídos sincronizados com uma fonte de tempo confiável é um trabalho difícil. Para isso, foram desenvolvidos os protocolos de sincronização de tempo, que disseminam a hora de uma fonte de tempo confiável. Um dos mais conhecidos e usados hoje, é o *network time protocol* (NTP). O NTP foi concebido para operar em redes de dados de troca de pacotes e com latência variada. Com essas características ele funciona muito bem em sistemas distribuídos, que usam a internet como o meio de comunicação.

O controle de quando uma informação secreta deve ser liberada pode ser feita com a criptografia temporal, ou seja, a informação é mantida em sigilo por um período de tempo pré-determinado. A criptografia temporal utiliza uma terceira entidade confiável, que ficará responsável por armazenar e liberar na data e hora estipuladas a informação em sigilo. Essa terceira entidade deve ter seu relógio sincronizado com uma fonte confiável de tempo, para que a informação não seja liberada antes ou após a hora estipulada.

Os serviços de tempo numa infra-estrutura de chaves públicas são providos em diversos sistemas. Para a emissão de um carimbo de tempo, para distribuir a hora certa em sistema que compõem a infra-estrutura e para garantir a liberação de uma informação na hora correta é necessário um relógio confiável e seguro.Essa dissertação propõe a integração desses serviços de tempo que compõem a infra-estrutura, em um único módulo de segurança criptográfico, o módulo de relógio seguro.

1.1 Objetivos

1.1.1 Objetivo Geral

Desenhar uma solução para a integração dos serviços de relógio no contexto de uma Infra-estrutura de Chaves Públicas (ICP).

1.1.2 Objetivos Específicos

- Analisar os usos e aplicações de relógio no componentes que formam uma ICP;
- Levantar como os relógios dos componentes de uma ICP são sincronizados entre si e com uma fonte confiável de tempo (FCT);
- Listar os serviços de relógios providos por uma ICP;
- Analisar a qualidade dos relógios usados em HSMs;
- Propor a integração de todos os serviços de relógios em um único sistema provedor;
- Propor uma gestão segura do relógio;
- Definir requisitos de exatidão, precisão e estabilidade dos relógios no contexto de uma ICP;
- Definir os documentos para uso do sistema integrador de relógios em uma ICP;
- Discutir o impacto da inclusão deste sistema sobre uma ICP.

1.2 Justificativa

Os requisitos de precisão e exatidão dos relógios em uma ICP são distintos para diferentes aplicações e componentes. Algumas aplicações gerais e componentes que usam relógio são:

- Transações distribuídas de banco de dados;
- Leilões;
- Controle de tráfego aéreo;
- Programação da televisão e rádio;
- Detecção de intrusão em sistemas computacionais;
- Sincronização de tele-conferência;
- Carimbos de tempo em documentos eletrônicos;
- Controle de quando uma informação pode ser lida.

Cada uma dessas aplicações são executadas em computadores distribuídos, até mesmo instâncias da mesma aplicação será executada em computadores distribuídos. Isso gera inconsistência nos tempos resultando inconsistência nos dados. Uma forma de minimizar a inconsistência, é a integração dos serviços de tempo.

1.3 Motivação

Como visto, em sistemas distribuídos, os relógios operam de forma independente um do outro, sem relação entre eles, causando inconsistência nos dados. Isso motivou a integração dos serviços de tempo em um único sistema, para que seja garantido o sincronismo do tempo nos relógios utilizados pelas aplicações.

O Laboratório de Segurança em Computação (LabSEC) desenvolve alguns projetos na área de ICP, entre eles existe o projeto do Módulo de Segurança Criptográfico (HSM, do inglês) em parceria com a Rede Nacional de Pesquisa (RNP), que provê a gestão segura de chaves privadas.

O uso de um HSM para a integração dos serviços de tempo em um único sistema, garante mecanismos para que os serviços sejam executados de forma segura e confiável. E as aplicações também utilizarão esses serviços de forma segura e confiável.

1.4 Metodologia

Para alcançar os objetivos desse trabalho, foram estudados artigos, publicações e trabalhos sobre os temas de relógio, carimbo de tempo, sincronização de relógio, certificado temporal, módulo de segurança criptográfico, políticas de uso e declaração de práticas de uso.

Foi feita uma visita ao Observatório Nacional do Rio de Janeiro (ON), onde se conheceu as instalações do serviço de tempo. Foram vistos e explicados os relógios atômicos e o modo de sincronismo dos relógios atômicos do ON com os do Bureau Internacional des Poids et Mesures (BIPM).

Foi levantando onde é utilizado relógio em serviços providos por uma ICP, e analisados esses relógios, comparando-os com uma FCT.

Foi escolhido o HSM da RNP para realizar a integração dos serviços de tempo. Esse HSM possui um sistema onde é possível customizar a imagem que é executada por ele. Com isso foi possível executar o diagnóstico do relógio, bem como a integração dos serviços de tempo.

Foi estudado como escrever a documentação de Política de Uso e Declaração de Práticas de Uso. Esses documentos são utilizados para normalizar o uso de um serviço dentro da ICP.

1.5 Trabalhos Correlacionados

Em 1991 [4] foram os primeiros a relatar que uma evidência no tempo é a hora correta em que um documento eletrônico existiu em um determinado instante do tempo. Essa evidência é chamada de carimbo de tempo. Em 1993 [5] mostraram como usar o carimbo de tempo, para verificar a autenticidade de uma assinatura digital.

Em sistemas distribuídos a sincronização de relógio é complexa. Em 1987, David Mills [6] relatou um protocolo de sincronização para sistemas distribuídos.

Em 1988 David Mills lançou a primeira versão do Network Time Protocol [7]. Em 2008 está prevista o lançamento da versão 4 do Network Time Protocol (NTP). O NTP é o protocolo mais utilizado na internet para a sincronização de relógio.

Em 1993 Timothy May [8] foi o primeiro autor a usar criptografia na liberação de documentos no futuro, usando o termo criptografia temporal (*timed-release cryptography*) para discutir esse problema. May propôs uma solução que usa uma terceira entidade confiável para guardar e liberar o documento na data específica. E também propôs que a chave usada para decifrar o documento seja guardada por uma terceira entidade confiável. Em 1996 [9] propõem duas técnicas para implementar a temporalidade em documento digitais: através de quebra-cabeças computacionais (*Time-lock puzzle*) e através de uma terceira entidade confiável. Em 2007 [10] propõem uma infra-estrutura de liberação de chaves temporais.

1.6 Conteúdo da Dissertação

No Capítulo 2 apresenta o tempo no contexto de uma ICP. Nele são apresentados os relógios e os serviços de tempo que são providos por uma ICP.

No Capítulo 3 os componentes que formam uma ICP são definidos mostrando onde é utilizado o relógio e como ele é utilizado.

A seguir, no Capítulo 4 é apresentada a solução de integração dos serviços de tempo em um único módulo, o Módulo de Relógio Seguro.

No Capítulo 5 apresenta um modelo de documento usado para normalizar o uso do Módulo de Relógio Seguro numa ICP.

No Capítulo 6 é discutido o impacto do Módulo de Relógio Seguro numa ICP e com o que existe na literatura.

E por fim, no Capítulo 7 conclui-se o trabalho, apresentando suas contribuições e trabalhos futuros.

Capítulo 2

O Tempo na Certificação Digital

2.1 Introdução

Este capítulo discute os relógios e suas características, e os serviços que tem como requisitos necessário à segurança da informação e a garantia da temporalidade em documentos eletrônicos.

O tempo é usado para saber quando um evento ocorreu, e compará-lo a outro evento, para se ter uma idéia da seqüencia de eventos. A Seção 2.2 define o que é tempo e explica algumas escalas de tempo. A Seção2.3 explica o relógio. A Seção 2.4 apresenta a unidade básica do tempo. A Seção2.5 define o termo rastreabilidade. A Seção 2.6 define termos usados quando se fala de relógio.

A Seção 2.7 apresenta o carimbo de tempo, mostrando os tipos de datação usados e modelos de carimbadoras usadas no Brasil. O modelo de carimbo de tempo aprovado no Brasil é também apresentado, e explicando o processo de auditoria.

A Seção 2.8 apresenta protocolos de sincronização de tempo, e explica com mais detalhes o protocolo *Network Time Protocol* (NTP), que está sendo adotado pela ICP-Brasil na sincronização dos relógios dos Servidores de Carimbo de Tempo.

A Seção 2.9 mostra como controlar a liberação futura de informação, utilizando método criptográficos.

2.2 Tempo

O tempo é um componente de um sistema de medidas usado para medir o intervalo de duração entre um evento e outro. Existem várias escalas para medir e representar o tempo. As escalas do tempo que são usadas neste trabalho são:

TAI (*Temps Atomique International*) É calculado pelo *Bureau International des Poids et Mesures* (BIPM) a partir da leitura de mais de 200 relógios atômicos localizados em institutos e observatórios de metrologia ao redor do mundo. Estima-se que o erro do TAI em relação a um relógio imaginário perfeito é de 100ns em um intervalo de 1 ano.

UTC (*Universal Time Coordinated*) É a base para o tempo legal em todo o mundo. O UTC acompanha o TAI, mas é disciplinado pelo período solar. Para ajustar o UTC ao período solar é acrescido ou diminuído um segundo, aproximadamente a cada 18 meses. Isso é chamado de *leap second*. O objetivo é, assegura-se que o sol esteja sobre o meridiano de Greenwich ao meio-dia, com um erro máximo de 0,9s.

GPS Time Os satélites GPS adotaram uma escala sincronizada com o UTC em 1980, mas desde então não sofreram as correções dos *leap seconds*. O GPS está 14s adiantado em relação ao UTC. Desconsiderando-se a questão dos *leap seconds*, o GPS não diverge do UTC mais do que $1u$s.

Fuso horário É uma escala de tempo baseada numa diferença em relação ao UTC, de forma a adequá-lo ao tempo solar local. Também conhecido como hora local. Por exemplo, o Brasil, desde o dia 24 de maio de 2008 possui apenas 3 fusos horários.

2.3 Medição de tempo

Para medir o tempo normalmente se utiliza um relógio. O relógio é um dispositivo composto de duas partes, um oscilador e um contador, conforme ilustra Figura 2.1. O contador é usado para contar o número de oscilações do oscilador. Com isso é possível medir o tempo entre dois eventos, contando quantas oscilações ocorreram no intervalo.

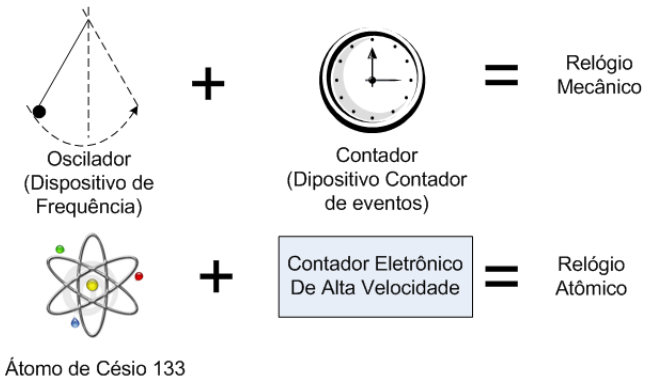


Figura 2.1: Partes de um relógio [1]

Os primeiros relógios mecânicos construídos pelo homem usavam um pêndulo como oscilador. Os relógios modernos, tais como aqueles usados em computadores, usam como oscilador um cristal de quartzo, que na maioria das vezes opera na freqüência de 32.768 kHz [1]. Um contador, que conta as oscilações, é representada pelas engrenagens e pelos ponteiros, num relógio a pêndulo.

Os relógios atômicos utilizam um elemento atômico como oscilador, como o césio 133, e geram freqüências com incertezas menores do que qualquer dispositivo físico ou oscilador a quartzo. Um relógio atômico usa como sua referência um sinal eletromagnético associado a uma transação quântica entre dois níveis de energia de um átomo, o fóton [1].

2.4 Unidade de medida de tempo

A unidade padrão de contagem de tempo é o segundo. De acordo com o Sistema Internacional de Unidades [11], a definição oficial do segundo corresponde a diferença de energia especifica a uma transição quântica do átomo de césio 133, cuja freqüência sem perturbação, foi definida como sendo de 9.192.631.770 Hz. Quando o número definido de ciclos acontece para o sinal eletromagnético associado ao fóton absorvido ou desprendido em sua transição quântica, teremos oficialmente 1 segundo.

2.5 Rastreabilidade

Para se ter confiança na hora de um relógio, é necessário rastrear a hora até a sua fonte de tempo.

O termo rastreabilidade vem da metrologia e proporciona uma forma de relacionar os resultados de uma medição ou valores de um padrão a padrões superiores. Esses padrões superiores correspondem a padrões nacionais ou a padrões internacionais, apresentando incertezas de medição bem conhecidas [12]. A rastreabilidade torna-se uma característica inerente a cada medição.

Segundo o Vocabulário Internacional de Termo Básicos e Gerais na Metrologia [13], a rastreabilidade é definida como a "propriedade do resultado de uma medição ou do valor de um padrão estar relacionado a referências estabelecidas, geralmente a padrões nacionais ou internacionais, através de uma cadeia contínua de comparações, todas tendo incertezas estabelecidas". Normalmente, nos diversos países, essa "cadeia contínua de comparações" origina-se no Instituto Nacional de Metrologia.

No Brasil, o Instituto Nacional de Metrologia é o Inmetro. O documento DOC-CGCRE-003 do Inmetro [14], estabelece a interpretação para os elementos necessários à rastreabilidade. Ele define que não é suficiente que o laboratório calibre seus equipamentos e disponha dos certificados de calibração correspondentes. É necessário informações sobre a competência dos laboratórios que realizam as calibrações que formam a cadeia de rastreabilidade.

De acordo com o Inmetro, são considerados competentes os laboratórios:

- laboratórios integrantes do INMETRO, do Serviço da Hora do Observatório Nacional (SH/ON) ou do Instituto de Radioproteção e Dosimetria (IRD);
- institutos nacionais de metrologia de outros países que sejam signatários de acordos de reconhecimento mútuo do Comitê Internacional de Pesos e Medidas (CIPM) e que participem das comparações chave organizadas pelo BIPM ou por organizações regionais de metrologia;
- institutos de calibração acreditados pelo INMETRO para a calibração específica;
- institutos de calibração acreditados pelo INMETRO para a calibração;
- laboratórios de calibração, que sejam acreditados para a calibração específica, por organismos de acreditação signatários dos acordos de reconhecimento mútuo do Cooperação de Acreditação de Laboratório Internacional (ILAC, do inglês, International Laboratory Accreditation Cooperation) e/ou da Cooperação Européia de

Acreditação (EA, do inglês, European Co-operation for Accreditation) e/ou da Co-operação de Acreditação Interamericana (IAAC, do inglês, Interamerican Accreditation Cooperation).

Como visto acima, o Serviço de Hora do Observatório Nacional (SH/ON) é competente para realizar a calibração de equipamentos de relógio. Além disso, o Decreto no. 4.264 de 10 de junho de 2002 restabelece o Decreto no. 10.546 de 05 de novembro de 1913 que regulamenta a Lei no. 2.784 de 18 de junho de 1913, estabelece no Artigo 6o.

- É da competência do Observatório Nacional, unidade de pesquisa do Ministério da Ciência e Tecnologia, gerar a Hora Legal do Brasil, bem como disseminá-la pelos meios de comunicação, observado o disposto na legislação vigente e nos tratados, acordos e atos internacionais de que o Brasil seja parte.

Isso garante que os relógios usados em equipamentos sejam homologados por um órgão credenciado ao Inmetro, e que a hora utilizada seja rastreável até a hora UTC.

2.6 Definições importantes sobre relógio

A seguir são apresentadas algumas definições usadas para referenciar efeitos e causas que atuam sobre o tempo em um relógio .

Exatidão (*Accuracy*) É quanto o valor indicado por um sistema de medição está próximo ao valor verdadeiro do tempo.

Um relógio de computador funcionando de forma isolada, sua exatidão tende a piorar com o passar do tempo. O relógio pode atrasar ou adiantar conforme o tempo passa.

Precisão (*Precision*) É o menor incremento de tempo que pode ser lido pelo computador.

Resolução (*Resolution*) É o menor incremento do contador do relógio.

Num relógio de computador é determinada pela freqüência das interrupções de hardware que fazem funcionar o contador. Os valores variam entre 100Hz e 1KHz, o que resulta em resoluções de 10ms a 1ms.

Granularidade (Granularity) É a interpolação de outras fontes de freqüências maiores com a obtida do relógio, para conseguir uma resolução maior.

Dispersão (*Dispersion*) É o desvio ou erro estimado nas leituras do relógio.

Pode ser causado por flutuações de curta duração na freqüência do oscilador, por erros na medida ocasionados por excesso de utilização do processador, latência causada pelas interrupções, latência na rede, etc.

Variação (*Jitter*) É o desvio ou erro nas leituras do relógio.

Deslocamento (*Offset*) É a diferença de tempo entre dois relógios.

Envelhecimento (*Aging*) É a instabilidade na freqüência do oscilador causada por fatores internos.

Isto é, quanto a freqüência do relógio varia com o tempo quando os fatores externos como radiação, pressão, temperatura e umidade são mantidos constantes.

Escorregamento (*Drift*) É a instabilidade na freqüência do oscilador causada por fatores externos.

Isto é, quanto a freqüência do relógio varia com o tempo quando os fatores externos como radiação, pressão, temperatura ou umidade, e pelo envelhecimento, variam.

Estabilidade (*Stability*) É a estimativa estatística da instabilidade na freqüência do oscilador num determinado período de tempo.

Monotonicidade (*Monotonicity*) A leitura sucessiva do relógio deve apresentar sempre um tempo no futuro do que a leitura anterior.

Sincronização (Synchronization) É o processo de ajustar a fase de dois osciladores de forma que a diferença entre eles seja nula.

Sintonização (*Syntonization*) É o processo de ajustar a freqüência de dois osciladores para que sejam a mesma.

2.7 Carimbo do Tempo

Em muitos casos é necessário associar uma informação a uma data, afirmando que a informação existia em um determinado instante de tempo [4]. Essa âncora temporal é conhecida como Carimbo de Tempo(CT), e pode ser emitido por uma terceira entidade confiável denominada de Autoridade de Carimbo de Tempo(ACT) através de Servidores de Carimbo de Tempo(SCT). O uso de terceira entidade confiável, tal como uma ACT, tem sido recomendada por vários autores e instituições para agregar confiança aos documentos eletrônicos [15].

Os SCT's adotam modelos de datação para garantir a hora correta nos CT's emitidos. Conforme Just [16] e Roos [17], existe 3 modelos: **absoluta**, **relativa** e **híbrida**. A datação absoluta consiste em informar a data e hora igual a usada no mundo real. A datação relativa apenas informa se uma informação foi datada antes ou depois de outra informação. A datação híbrida é constituída de uma base com estrutura relativa com a data e hora absoluta.

De acordo com a RFC3161 [18], para a emissão de um carimbo de tempo, deve haver uma troca de mensagens entre o subscritor e a ACT. Na primeira mensagem o subscritor faz uma requisição de um carimbo de tempo enviando uma requisição a uma ACT. A secunda mensagem, a ACT responde enviando uma resposta, que é ou contém um carimbo de tempo, para o subscritor. Uma vez recebida a resposta, o subscritor deve verificar a mensagem de erro retornada na resposta e se nenhum erro foi encontrado ele deve verificar os vários campos contidos no carimbo de tempo, e a validade da assinatura digital do carimbo de tempo. Em particular, ele deve verificar se o que foi carimbado, corresponde com o que foi pedido para carimbar. O subscritor deve verificar se carimbo de tempo contém o certificado correto da ACT, e o algoritmo de resumo contido no Object Identifier (OID). Então ele deve verificar o tempo incluso na resposta com uma fonte local confiável de tempo, se disponível, ou o valor do nonce, um grande número aleatório, incluído na resposta, é igual ao nonce enviado na requisição. Se qualquer uma das verificações acima falhar, o carimbo de tempo deve ser rejeitado.

2.7.1 Tipos de carimbadoras

No Brasil, existem duas soluções de carimbo de tempo que são homologadas. Mas existem outras que são mencionadas a seguir.

2.7.1.1 Bry

A Bry possui a carimbadora Bry SCT integra software e hardware, e gera carimbo de tempo em conformidade com o tempo de seu relógio e a ordem de recebimento das requisições, além da manutenção dos registros dos carimbos de tempo emitidos, de forma a permitir a rastreabilidade dos mesmos [2]. A Bry SCT utiliza a BRy SSR, que é um sistema de auditoria e sincronismo responsável por distribuir a informação temporal aos equipamentos, para se manter sincronizado com uma fonte confiável de tempo.

A Figura 2.2 mostra a estrutura de carimbo de tempo provida pela Bry Tecnologia.

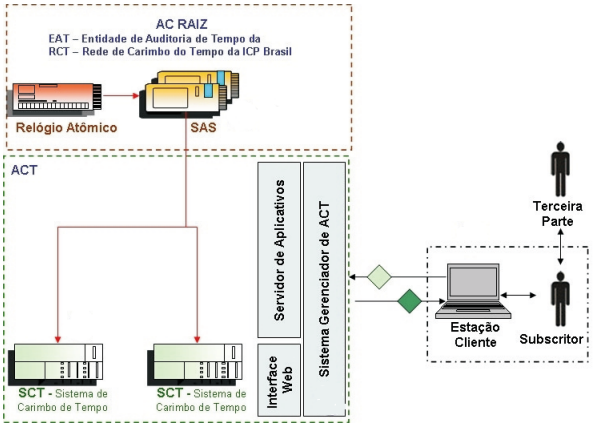


Figura 2.2: Estrutura do Carimbo de Tempo da Bry [2]

2.7.1.2 nCipher

A nCipher possui a carimbadora DSE200. É construída com base no módulo de segurança(HSM) nCipher nShield com execução do código de assinatura dentro do SEE - Secure Execution Engine, que executa as funções do código dentro do HSM. Pode assinar e aplicar o Carimbo de Tempo em nome de indivíduos, departamentos ou organizações. Vem implementado, além do Servidor de Carimbo de Tempo, uma Autoridade de Carimbo de Tempo. É capaz de gerar registros eletrônicos certificados dig-

italmente através de um registro auditável da autenticidade do documento, amarrando com segurança a identidade do remetente do documento e o tempo da criação do original eletrônico.

2.7.2 Outras

Cybernetica TrueSign - o sistema utiliza o método de datação híbrida, e consiste de um servidor de aplicação, um módulo de segurança criptográfico e um dispositivo GPS.

DigiStamp e-TimeStamp - serviço provido pela empresa para protocolação digital de documentos. Utilizam um software de protocolação e um módulo de segurança criptográfico provido pela IBM, o IBM 4758 Coprocessor.

Surety AbsoluteProof - provê serviços de que é possível verificar quando uma informação digital foi criada e se foi alterada e de certificar o conteúdo de um documento e a data em que foi criado. Possui método de datação híbrido.

Symmetricom Descontinuou as operações de carimbo de tempo em 2003.

2.7.3 Carimbo do Tempo na ICP-Brasil

Em 24 de agosto de 2001, foi aprovada a Medida Provisória No. 2200-2, que regulamenta o uso de chaves públicas do Brasil intitulada Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Somente no final de 2007 foi aprovado pelo Comitê Gestor(CG) da ICP-Brasil o modelo a ser adotado para a emissão de carimbos de tempo. O modelo foi amplamente discutido pela Comissão Técnica (Cotec) da ICP-Brasil, com o apoio do Observatório Nacional do Rio de Janeiro (ON) e de universidades brasileiras [19–22]. Foram criados quatro documentos que regem o uso do carimbo, com base em quatro resoluções.

- Resolução No. 57
  - Art. 1o. Aprovar a versão 1.0 da VISÃO GERAL DO SISTEMA DE CARIMBOS DO TEMPO NA ICP-BRASIL.
  - Art. 2o. Esta Resolução entra em vigor na data de sua publicação.
- Resolução No. 58

  - Art. 1º Aprovar a versão 1.0 dos REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL.
  - Art. 2º Esta Resolução entra em vigor na data de sua publicação.

- Resolução No. 59

  - Art. 1º Aprovar a versão 1.0 dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO DA ICP-BRASIL.
  - Art. 2º Esta Resolução entra em vigor na data de sua publicação.

- Resolução No. 60

  - Art. 1º Aprovar a versão 1.0 dos PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL.
  - Art. 2º Esta Resolução entra em vigor na data de sua publicação.

Esses documentos foram criados porque as normas da ICP-Brasil existentes até hoje, definem regras para criação e utilização de certificados digitais para permitir, entre outras aplicações, a assinatura digital de documentos eletrônicos, mas não definiam regras que pudesse ser determinada que uma informação digital existia num determinado instante de tempo passado ou se uma assinatura digital foi aplicada antes da revogação ou expiração do certificado digital correspondente. No âmbito da ICP-Brasil, a utilização de carimbos do tempo é facultativa, já que os documentos assinados digitalmente com chave privada correspondente a certificados ICP-Brasil, são válidos com ou sem o carimbo do tempo.

O modelo geral de funcionamento está representado na Figura 2.3.

Na sua estrutura, existem as seguintes entidades integrantes que fazem parte.

Comitê Gestor da ICP-Brasil Entidade responsável pela implantação da ICP-Brasil. Estabelece políticas, critérios e normas de funcionamento que devem ser seguidas pelas entidades integrantes da ICP-Brasil. Audita e fiscaliza a AC-Raiz.

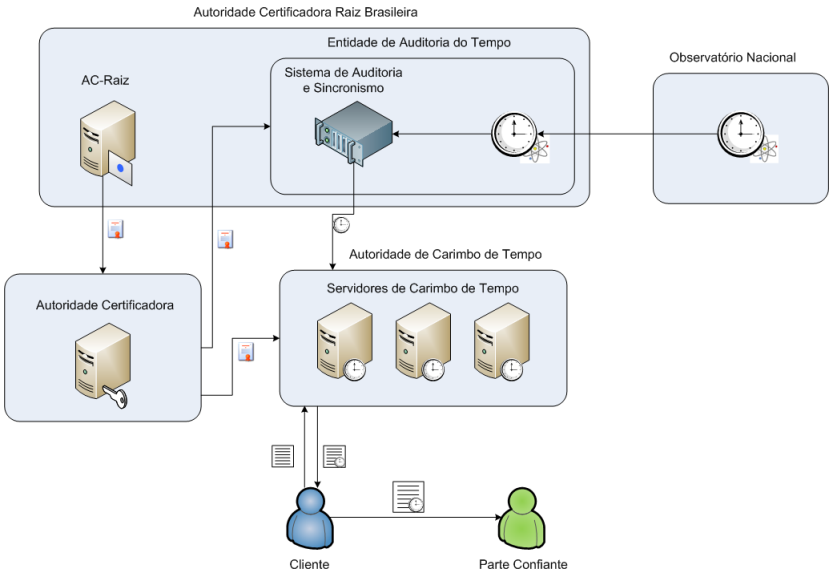


Figura 2.3: Estrutura da Rede de Carimbo de Tempo da ICP-Brasil

AC-Raiz da ICP-Brasil (AC-Raiz) Credencia, audita e fiscaliza entidades da ICP-Brasil. Assina seu próprio certificado e os certificados das AC imediatamente subordinadas. Atua também como EAT na Rede de Carimbo do Tempo ICP-Brasil.

Entidade de Auditoria do Tempo (EAT) É a AC-Raiz da ICP-Brasil, que utiliza Sistemas de Auditoria e Sincronismo (SAS), ligados a um relógio atômico e a partir deles realiza as atividades de auditoria e sincronismo dos Servidores de Carimbo do tempo (SCT), instalados nas ACT.

Autoridade Certificadora (AC) Emite, renova ou revoga certificados digitais de outras AC ou de titulares finais. Emite e publica LCR. Na estrutura de carimbo do tempo da ICP-Brasil, emite os certificados digitais usados nos equipamentos das ACT e da EAT e emite ainda os demais certificados utilizados nos processos relacionados aos carimbos do tempo.

Observatório Nacional (ON) Unidade de pesquisa do Ministério da Ciência e Tecnologia (MCT), integrante do Sistema Nacional de Metrologia (SINMETRO). O ON é o responsável legal pela geração, conservação e disseminação da Hora Legal do Brasil.

Prestador de Serviços de Suporte (PSS) Entidade contratada pela ACT para realizar todas ou parte das atividades previstas na sua Declaração de Práticas de Carimbo do tempo. A ACT, mesmo utilizando-se de um PSS para executar suas atividades,

é responsável pelos serviços por ele executados. Os PSS classificam-se em três categorias, conforme o tipo de atividade prestada:

- fornecedor de infra-estrutura física e lógica;
- fornecedor de recursos humanos especializados; ou
- fornecedor de infra-estrutura física, lógica e de recursos humanos especializados.

Autoridade de Carimbo do tempo (ACT) Entidade na qual os usuários de serviços de carimbo do tempo (isto é, os subscritores e as terceiras partes) confiam para emitir carimbos do tempo. A ACT tem a responsabilidade geral pelo fornecimento do carimbo do tempo. Além disso, a ACT deve:

- operar um ou mais Servidores de Carimbo do tempo (SCT), conectados à Rede de Carimbo do Tempo da ICP-Brasil, que geram carimbos em nome da ACT;
- manter disponível um serviço de páginas web onde é publicado, entre outras informações, sua Declaração de Práticas de Carimbo do Tempo (DPCT) e suas Políticas de Carimbo do tempo (PCT);
- operar diversos SCT, sendo que cada um deles deve utilizar um ou mais pares de chaves criptográficas específicas para essa finalidade;
- trabalhar com SCT específicos, com características diferenciadas.
- operar um ou mais Sistemas de Auditoria e Sincronismo do tempo (SAS). Entretanto, estes devem estar subordinados aos SAS da AC-Raiz;
- empregar PSS para fornecer partes dos serviços de carimbo do tempo. A ACT, no entanto, é a responsável e assegura que os requisitos identificados em sua PCT e DPCT sejam cumpridos. A chave ou as chaves privadas usadas para gerar o carimbo do tempo são identificadas como pertencendo à ACT responsável. Por exemplo, uma ACT pode subcontratar todos os componentes dos serviços, inclusive os serviços que geram o carimbo do tempo.

Subscritor ou Cliente Pessoa física ou jurídica que solicita os serviços de uma Autoridade de Carimbo do tempo implícita ou explicitamente concordando com os termos mediante os quais o serviço é oferecido.

Terceira Parte (Relying Part) Aquele que confia no teor, validade e aplicabilidade do carimbo do tempo produzido pela ACT.

A disseminação da hora UTC para as entidades que compõem a estrutura de carimbo do tempo da ICP-Brasil é realizada pela AC-Raiz, que utiliza mecanismos para garantir o sincronismo dos relógios dos equipamentos e a rastreabilidade do tempo informado até a fonte confiável do tempo. Os recursos usados para manter o sincronismo dos relógios dos equipamentos que compõem a Rede de Carimbo do tempo da ICP-Brasil são as seguintes:

- o Relógio Atômico, ou Fonte Confiável do Tempo (FCT), fornece a hora UTC para o relógio atômico da AC-Raiz;

- o relógio atômico da AC-Raiz fornece a hora UTC para o equipamento chamado de Sistema de Auditoria e Sincronismo (SAS) da AC-Raiz;

- o SAS da AC-Raiz, por sua vez, dissemina a hora para os equipamentos instalados na ACT e autoriza seu funcionamento por período de tempo pré-estipulado, emitindo-lhe um alvará com período de validade pré-estipulado com base no QoS do sistema e os principais atributos são: ano, mês. Dia, hora, minuto, segundo, compensação e retardo.

A garantia de que todos os equipamentos estejam sincronizados à hora UTC está baseada no fato de que os equipamentos que compõem a Rede de Carimbo do Tempo da ICP-Brasil somente receberão os respectivos alvarás se estiverem adequadamente sincronizados.

Há duas formas de solicitar um carimbo do tempo na ICP-Brasil: solicitação presencial e solicitação remota. A solicitação presencial ocorre quando um subscritor dirige-se a uma ACT e entrega uma mídia contendo o arquivo ou o documento que deseja carimbar ao responsável pelo atendimento. Esse utiliza uma estação de trabalho, formata o pedido e o envia ao SCT. Recebe de volta o carimbo emitido, que é repassado ao subscritor. A solicitação remota é feita a partir de um equipamento utilizando uma rede de comunicação de dados privada ou a Internet. O subscritor acessa a ACT, que dispõe de servidores atuando como interface de acesso ao SCT.

Tanto o subscritor que solicitou o carimbo do tempo, como a terceira parte, que irá receber o documento com esse carimbo, devem executar determinadas ações, antes de acreditar ou não na validade do carimbo. Como regras gerais devem ser verificadas: a identidade da ACT e do respectivo SCT; a validade dos certificados digitais; e o respeito à política sob a qual o carimbo foi emitido.

Somente são aceitos na ICP-Brasil carimbos do tempo emitidos por SCT com alvarás de sincronismo fornecidos por Sistemas de Auditoria e Sincronismo. Os equipamentos somente receberão os respectivos alvarás se estiverem adequadamente sincronizados, garantindo que todos estejam sincronizados à hora UTC. São utilizados chaves privadas vinculadas a certificados digitais ICP-Brasil, para assinatura dos alvarás, carimbos de tempo e autenticação, na garantia de autoria desses documentos.

O processo de auditoria é a avaliação periódica pela AC Raiz que verifica se o relógio do SCT está sincronizado com uma Fonte de Tempo Confiável (FCT), ou se se encontra dentro de um erro máximo pré-definido. E somente serão considerados sincronizados, os que forem monitorados pela AC Raiz. O resultado da auditoria e sincronização é a emissão de um alvará que permite o funcionamento do SCT por mais um período de tempo.

A AC Raiz possuí um equipamento denominado Sistemas de Auditoria e Sincronismo (SAS), que realiza auditoria e sincronismo. A comunicação entre o SAS e o SCT é feita através de um protocolo que permite identificação mútua utilizando certificados digitais e um protocolo de sincronismo de relógio. No SCT existe uma interface de auditoria, usado pela AC Raiz, para verificar os registros produzidos.

A AC Raiz manterá um relógio atômico sincronizado com o relógio atômico do Observatório Nacional. Esse relógio ficara ligado ao SAS da AC Raiz. Haverá um mínimo de dois SAS, instalados em locais diferentes, que proverá os serviços de auditoria e sincronismo, para cada SCT. Após a colocação do SCT em operação, a AC Raiz deve auditar periodicamente o relógio do SCT, em período tal que o erro máximo acumulado não ultrapasse o valor especificado na Política de Carimbo de Tempo correspondente. Emitir alvarás que habilita o funcionamento do SCT, ou na impossibilidade da emissão do alvará informar o motivo. Analisar e emitir relatórios dos registros de auditoria e sincronismo do relógio do SCT, utilizando os dados registrados no SAS.

2.8 Sincronização de Relógio

A medição do tempo em computadores é realizada por um cristal de quartzo. O quartzo a longo prazo, gera incertezas maiores se comparado a um relógio atômico. Isso se deve ao fato de que o a unidade de medida do tempo, o segundo, foi baseado utilizando-se um relógio atômico, como foi dito na Seção 2.4. O problema é que não se utiliza relógio atômico em computadores, o custo e a manutenção de um relógio atômico é muito alto, tornando inviável o uso em computadores, por isso utiliza-se o quartzo.

Para isso, é importante que o relógio do dispositivo seja sincronizado com uma fonte confiável de tempo. Relógio atômicos, são caracterizadas como fonte confiável do tempo, e são responsáveis por disseminar a hora.

Existe alguns protocolos responsáveis por realizar a sincronização do relógio, como o *Network Time Protocol* (NTP) [23] e *Digital Time Synchronization Service* (DTSS). Outros protocolos são discutidos na RFC1305. O NTP engloba o que há de melhor nos outros protocolos, tornando-o robusto. O DTSS foi desenvolvido para se trabalhar numa *local area network*, enquanto o NTP foi desenvolvido para um ambiente de Internet. A flexibilidade da relação cliente e servidor, faz com que o NTP seja capaz de funcionar em qualquer ambiente. O NTP não somente corrige o tempo, ele mantém um vestígio das variações do tempo e automaticamente ajusta as variações no cliente, isso permite que o relógio se mantenha correto, mesmo quando a rede de dados não esta funcionando.

2.8.1 Network Time Protocol

O NTP é baseado no princípio que todas as máquinas tenham o mais próximo possível a hora correta. Com esse principio, pode se entender a arquitetura do NTP. O NTP utiliza um modelo hierárquico, onde um pequeno número de servidores fornecem a hora para um grande número de clientes. Esse modelo se baseia no conceito de *stratum*, isto é, uma camada de rede de sincronização. Como pode ser visto na Figura 2.4, o *stratum* 0 normalmente são relógios de referência, como relógio atômicos, esses prevêem a hora no formato UTC. O *stratum* 1 são computadores que estão conectados diretamente a esses relógios de referência. O *stratum* 2 são computadores que se

conectam ao *stratum* 1 e assim por diante, até no máximo *stratum* 15.

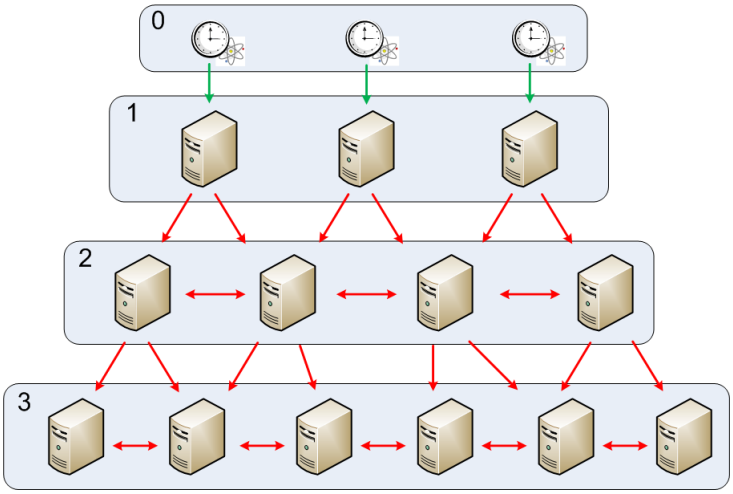


Figura 2.4: *Strata* do NTP

Os cliente podem utilizar vários servidores para sincronizar o seu relógio, para automaticamente determinar a melhor fonte de tempo e prevenir as más fontes de tempo. A relação entre os clientes e servidores NTP podem ser configurados para operar de diversas formas, tornando-o mais robusto. As entidades envolvidas podem operar da seguinte forma:

- Servidor - Um servidor de NTP provê a hora para o cliente
- Cliente - Um cliente de NTP pega a hora de um ou mais servidores
- Ponto - É um grupo de servidores NTP que são fortemente acoplados. Em um grupo de dois pontos, o mais exato, atua como servidor e o outro como cliente. O resultado é que o grupo estará sincronizado, e o cliente não precisa especificar mais de um servidor.
- Servidor *Broadcast/Multicast* - Enviam periodicamente atualizações da hora para um endereço *broadcast/multicast*.
- Client *Broadcast/Multicast* - Os clientes esperam por atualizações da hora em um endereço *broadcast/multicast*

Como visto, o protocolo NTP é usado na sincronização de relógios a partir de fontes confiáveis do tempo. Isso pode parece simples, como consultar o tempo no servidor e ajustar o relógio local. Existe uma implementação simplificada do NTP, o

Simple Network Time Protocol(SNTP) [24], que faz isso, e somente isso. Mas de uma forma completa, o NTP é muito mais complexo. Vários componentes colaboram para isso.

- obter informações de tempo de vários servidores como deslocamento, dispersão e variação.
- identificar quais fornecem tempo correto e quais estão mentindo.
- escolher qual a melhor referência, entre os servidores corretos.
- disciplinar o relógio local e ajustando de forma contínua e gradual, para que tenha a melhor exatidão possível.
- assegurar a monotonicidade do tempo.
- identificar, usando métodos criptográficos, servidores de tempo conhecidos e confiáveis.
- formar uma topologia simples, confiável, robusta e escalável para sincronização de tempo.

No início do desenvolvimento do NTP, teve uma preocupação quanto a autenticação das entidades envolvidas. Na versão 2 adotou-se a idéia de lista de controle de acesso(ACL). Essa ACL é mantida pelo servidor, e contém os endereços IPs dos clientes autorizados a se conectar. Outra idéia adotada, foi a autenticação simétrica. O servidor gera uma lista de chaves simétricas, cada chave é distribuída a um cliente autorizado a conectar-se. A troca de mensagens utilizando a chave simétrica pode ser resumida em: o remetente gera o *fingerprint* dos dados públicos usando a chave simétrica e envia junto aos dados a serem transferidos. O destinatário gera um *fingerprint* como o remetente fez, e verifica se bate o *fingerprint*, com isso garante que o remetente possui a chave. Isso garante a autenticidade e integridade das mensagens trocadas entre o servidor e cliente. Mas o maior problema, é a distribuição da chave simétrica.

Na versão 4 do NTP [25], adotou-se outra forma de autenticação, a assimétrica. O remetente gera o *fingerprint* dos dados públicos e cifra com a chave privada. A mensagem mais o *fingerprint* cifrado é enviado. O destinatário decifra o *fingerprint* e compara com o *fingerprint* gerado localmente com os dados recebidos. Se eles são iguais,

acredita-se que o remetente possui a chave privada. Este esquema é o protocolo Autokey. Este protocolo utiliza certificados digitais para identificação dos servidores.

O protocolo NTP apresenta mecanismos que garantem um serviço seguro, sendo a redundância de servidores e a inserção de *timestamp* nas mensagens as mais importantes, assegurando que o NTP seja resistente a falhas e a ataques de repetição.

2.9 Criptografia Temporal

O conceito de criptografia temporal consiste no esquema de enviar uma informação para o futuro [8]. A informação que se deseja proteger, é cifrada e a respectiva chave de decifrar é mantida em sigilo durante o período que a informação precisa ser mantida oculta. Existem dois métodos propostos para garantir o sigilo [9]:

Quebra-cabeça computacional consiste na realização de uma seqüencia de operações matemáticas, não escalonáveis e não distribuídas, que, aproximadamente, leva o mesmo tempo que a informação necessita ficar sigilosa.

Entidade confiável entidade que se compromete manter sigilosa a informação até sua data de liberação.

Esse dois métodos tem seus problemas, no quebra-cabeça computacional, é necessário um computador dedicado para realizar as operações, já que se trocar o computador no meio da operação por um mais rápido, o tempo de resolver diminuirá, e com isso a chave seria liberada antes do tempo. E mesmo com um computador dedicado, há a possibilidade de falhas no hardware. No método da entidade confiável, é necessário que ela garanta o sigilo do documento, armazenando-o de forma segura, e que não esteja sujeita a falhas no ataque. Além do que, armazenamento do documento, gera um alto custo. Outra forma de resolver isso, é o uso de criptografia simétrica ou assimétrica. Nesse caso, só se manteria em sigilo a chave para liberar o documento.

Em agosto de 2001, foi aprovada a Medida Provisória no. 2200-2, que institui a Infra-estrutura de Chaves Publicas Brasileira (ICP-Brasil). A Resolução 11, que define os requisitos mínimos de política de certificados na ICP-Brasil criou dois conjuntos de certificados: um para assinatura - denominados A1, A2, A3 e A4 - e outro de sigilo - S1, S2, S3 e S4. As outras resolução tratam em sua maioria de aspectos relacionados

a criação de autoridades certificadoras, autoridades de registro, prestadores de serviço de suporte e auditores.

2.9.1 Autoridade Certificadora Temporal

Uma Autoridade Certificadora Temporal (AC-Temporal) é uma entidade que tem como função prover temporalidade aos documentos eletrônicos. Essa entidade atua como uma terceira entidade confiável (TEC). Ela emite certificados temporais, no padrão X.509, o qual contém uma chave, que é usada para cifrar a informação desejada. A informação cifrada permanece assim, até que uma outra chave, é liberada pela AC-Temporal. Com posse dessa chave, a informação cifrada pode ser decifrada.

Recentemente Chan [26] propôs que a TEC seja completamente passiva sem interação entre ela e quem utiliza o certificado temporal, o que usa para cifrar e o que usa para decifrar. Assim assumindo a privacidade da informação e o anonimato de quem utiliza o certificado temporal. E Custódio [10] propôs uma TEC que utiliza criptografia assimétrica para geração do par de chaves temporal. A seguir é explicado o funcionamento de uma AC-Temporal proposto por Custódio.

O funcionamento da AC-Temporal utiliza criptografia assimétrica para geração de seu par de chaves. Uma é a chave de sigilo e a outra é a chave de liberação. A chave de sigilo está publicada no certificado temporal usado para cifrar uma informação. A AC-Temporal é responsável por manter sob sigilo a chave de liberação, até que a data de liberação do certificado temporal seja atingida. Na data especifica, a AC-Temporal publica a chave de liberação. Esta chave será usada para decifrar a informação antes cifrada com a chave de sigilo. A Figura 2.5 exemplifica o funcionamento básico de uma AC-Temporal:

A AC-Temporal, gera o par de chaves, chave de sigilo e liberação. A chave de sigilo é usada para cifrar uma informação. A informação sigilosa, é enviada ao destinatário, e na data especificada pelo remetente, a AC-Temporal libera a chave de liberação, e o destinatário poderá usar essa chave para decifrar a informação. Existe um projeto de uma AC-Temporal que está sendo desenvolvida no LabSEC/UFSC [27]. Nesse projeto existirão dois tipos de certificados temporais:

Certificado temporal de propósito geral São certificados emitidos pela própria AC-Temporal, para uso genérico. Esses certificados possuem a data de liberação corre-

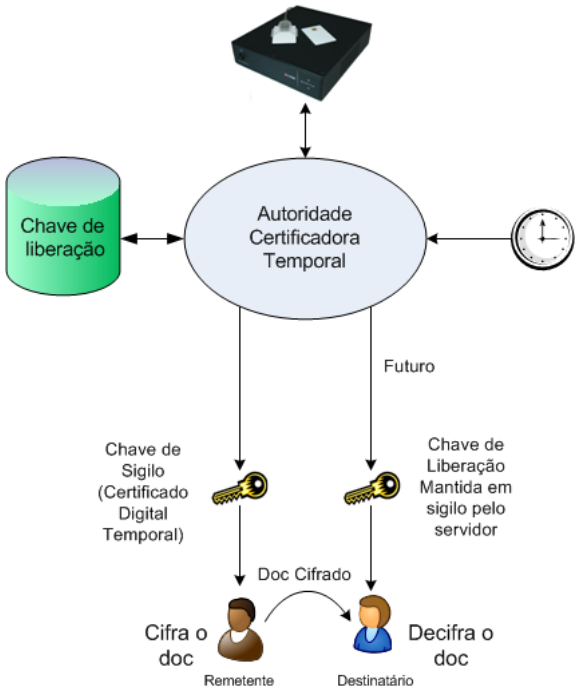


Figura 2.5: Funcionamento básico de um AC-Temporal

spondente a cada dia do ano, sendo o prazo máximo de um ano.

Certificado temporal com políticas especiais São emitidos pelos usuários da AC-Temporal, com uma política diferente da de propósito geral. Por exemplo, uma data especifica, 18:00h do dia 15 de maio de 2008.

Como numa Autoridade Certificadora(AC), os certificados temporais seguem o padrão X.509. O certificado de uma AC-Temporal deve ser assinado por uma AC, e o certificado temporal é assinado pela AC-Temporal, estabelecendo uma relação de confiança.

2.10 Conclusão

O tempo é essencial em todas as atividades realizadas por um computador, seja para manter o sincronismo dos processos, como ter a data e hora no registro dos eventos para uma posterior auditoria. Após ver os conceitos básicos de tempo, saber medi-lo e conhecer sua unidade básica de medição, é importante se familiarizar com o conceito de rastreabilidade. Pois além de se manter um relógio sincronizado, é importante manter uma rastreabilidade com uma FCT.

Para os serviços de carimbo de tempo, de hora e de criptografia temporal é essencial que a hora utilizada nesses serviços seja segura e confiável. Para se obter uma hora confiável, é necessário que o relógio que é utilizado ao se gerar a informação temporal, esteja sincronizado com uma FCT. E para se ter um relógio seguro, o uso de um hardware criptográfico faz-se necessário. Pois o mesmo possui mecanismos para garantir a segurança do relógio.

A utilização de um hardware criptográfico na gestão do relógio, protege o relógio do meio exterior e garante o correto funcionamento para ser utilizado pelos serviços de tempo.

O ideal é o uso de um único módulo que realiza a gestão do relógio, e provê os serviços de tempo que necessitam utilizar esse relógio seguro, como o serviço de carimbo de tempo, serviço de hora e serviço de criptografia temporal.

Capítulo 3

Componentes da uma ICP e seus relógios

3.1 Introdução

Em uma ICP são utilizados vários relógios. Cada elemento componente de uma ICP tem a sua disposição pelo menos um relógio. Com o objetivo de avaliar o uso dos relógios foi realizado um levantamento dos componentes prováveis de uma ICP, para saber onde exatamente e em que circunstâncias os relógios são utilizados. Para isso, foram estudadas as principais entidades certificadoras e seus serviços tais com a americana Verisign [28] e a brasileira ICP-Brasil [29]. O levantamento também foi baseado na experiência que o Laboratório de Segurança em Computação (LabSEC) da Universidade Federal de Santa Catarina (UFSC) possui na área de infra-estrutura de chaves públicas. Os principais componentes que fazem parte de uma ICP são: Autoridades Certificadoras, Autoridades de Registro, Autoridade de Carimbo de Tempo, Sistema de Auditoria e Sincronismo (SAS) e Sistema de Validação de Certificado.

Neste capítulo a Seção 3.2 apresenta os componentes que fazem parte de uma ICP e mostra onde existe relógio e como esse utilizado é sincronizado. A Seção 3.3 é uma análise do funcionamento dos relógios de uma ICP. A Seção 3.4 apresenta a conclusão.

3.2 Relógios na ICP

Uma ICP é formada por diversos componentes que são especializados em prover determinados tipos de serviços. Apesar de oferecerem serviços diferenciados, todos os componentes apresentam uma arquitetura semelhante em termos de hardware e software.

Os componentes são normalmente formados por um servidor, onde a aplicação servidora é executada, e por um hardware criptográfico (HSM) que provê serviços criptográficos e salva-guarda dos dados sensíveis dos serviços, tais como as suas chaves criptográficas. Alguns componentes oferecem serviços *online* e outros - ditos *offline* - operam desconectados de uma rede de comunicação de dados. A escolha entre operar online e offline depende do tipo de serviço ofertado. A forma como esses componentes são organizados e provêm serviços é descrita em documentos tais com a Política de Certificação (PC) e a Declaração de Práticas de Certificação (DPC) **??**. A PC dita o que deve ser provido e quais cuidados devem ser tomados para que o componente opere adequadamente. A DPC descreve como deve ser implementado os requisitos impostos pela PC.

Tanto o servidor quanto o HSM possuem relógios internos que disponibilizam o tempo para as aplicações. Servidores em geral, como a maioria dos computadores, possuem dois tipos de relógio: um relógio de hardware e outro de software. O relógio de hardware funciona independentemente da aplicação ou sistema operacional pois trata-se de um dispositivo autônomo, sendo alimentado por uma bateria quando o equipamento está desligado. O relógio de software, que é a hora do sistema, é mantido pelo *kernel* do sistema operacional. Esse relógio somente existe quando a máquina está ligada e possui uma melhor resolução quando comparada com a do relógio do hardware.

Normalmente, a iniciação do relógio do sistema é feita durante o processo de carga do sistema operacional e mantido atualizado enquanto o sistema permanece em execução. Durante a iniciação, o *kernel* do sistema operacional instância o relógio em software, e o configura com a hora lida do relógio de hardware. Após isso, o sistema, caso tenha acesso a Internet, pode manter sincronizado o relógio do sistema a um fonte confiável de tempo usando um serviço NTP (veja Seção 2.8.1, pg. 21). No processo de desligamento do sistema, o relógio do hardware é atualizado com a hora obtida do relógio do sistema. Esse procedimento permite manter o relógio de hardware sempre sin-

cronizado a uma FCT. É possível também, que o relógio do hardware não seja atualizado no desligamento do sistema. Isso é interessante quando não se tem o relógio do sistema sincronizado com uma FCT.

O problema do relógio do sistema não se manter sincronizado com uma FCT, pode acarretar num atraso significativo do relógio. O relógio é mantido por uma interrupção de tempo provido pela CPU do hardware. Como a CPU é utilizada por todos os processos do sistema, é formada uma fila de uso da CPU com os processos. Nessa fila, entra também o relógio do sistema. Muitas vezes, os processos utilizam 100% da CPU. Nesse caso, o relógio precisa ficar esperando até sua vez para utilizar a CPU. Isso resulta no atraso do relógio em relação a uma FCT.

Os HSMs são utilizados para aceleração e gestão do ciclo de vida de chaves criptográficas. Geralmente esses serviços utilizam a informação temporal advinda do servidor. É no servidor que a estrutura de dados contendo a informação temporal é montada. Ao HSM cabe exclusivamente a realização de processamento criptográfico tal com a geração de assinatura digital. Em algumas aplicações muito específicas onde há necessidade de um controle mais rigoroso sobre o relógio, são usados HSMs com relógios internos. O uso de um relógio interno ao HSM pode ser necessário para garantir que mesmo que o sistema seja malicioso, intencional ou não, não possa emitir documentos ou mensagens com data diversa daquela do HSM. Os relógios internos ao HSM, no entanto, precisam ser identificados e sua rastreabilidade e auditabilidade reconhecida pelas partes. Esses HSMs normalmente tem um custo maior e precisam de procedimentos especiais para garantir seu sincronismo com uma fonte confiável de tempo. A título de exemplo, o HSM nShield da nCipher [30] possui um relógio interno que pode ser usado através de sua funcionalidade de execução segura de código. Essa funcionalidade é usada, por exemplo, para montar uma carimbo de tempo dentro do HSM.

A identificação de um relógio ainda é um problema pouco explorado na literatura. Normalmente não se discute a fonte de tempo usada para apostar uma informação temporal a uma mensagem. Não é possível, por exemplo, comprovar a origem do tempo utilizado. Não existe ainda uma protocolo que permita fazer isso de forma simples e eficiente. É provável que a melhor forma de fazê-lo seja a partir do uso de protocolos de sincronismo de tempo auxiliados por sistemas de auditoria, como aquele descrito na Seção 2.7.3.

O controle do relógio interno do HSM deve ser realizado por usuários autorizados. Isso é necessário para se garantir o rastreamento das atualizações. Sem o rastreamento, não seria possível garantir a confiabilidade do relógio. Para evitar a atualização indevida do relógio interno de um HSM, alguns modelos não permitem uma mudança brusca nos parâmetros dos relógios. Qualquer alteração de maior magnitude é considerado, pelo HSM, um tipo de invasão e precisa ser adequadamente tratado. Se for realmente necessário tal modificação, é imperativo que fique registrado tais modificações e que a partir de uma análise dos registros, pelos auditores, seja possível explicar as modificações efetuadas.

A Figura 3.1 apresenta os principais componentes de uma ICP e seus relógios. A AC Off-line é composta por um servidor e um HSM e não possui conexão com

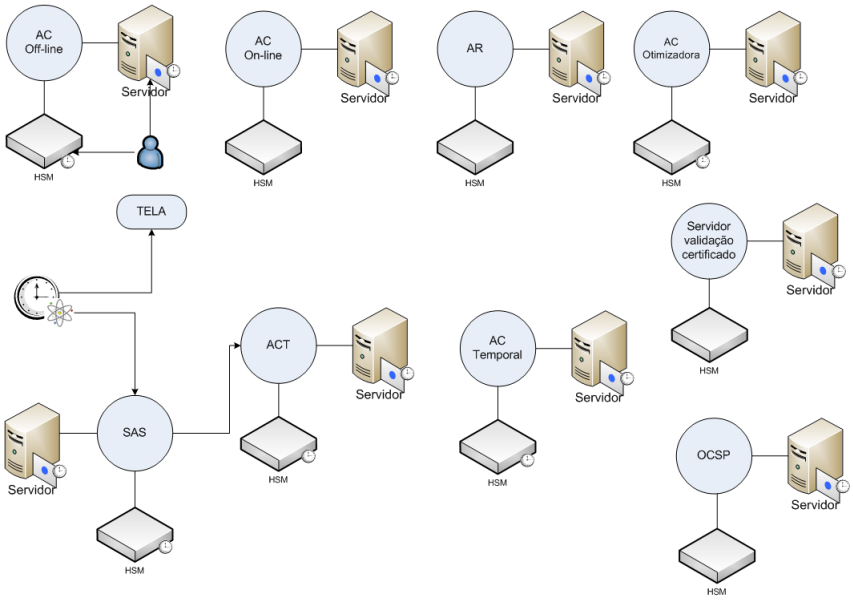


Figura 3.1: Principais componentes de uma ICP e seus relógios

nenhuma rede de comunicação de dados. Normalmente, uma AC Off-line é uma AC-Raiz ou uma camada de ACs intermediárias, que ditam as políticas de uma de todo o ramos de uma árvore de certificação. No servidor é executado a aplicação de gestão do ciclo de vida do certificado da AC Raiz e dos certificados e informação de status de certificados por ela emitidos. Os procedimentos e cerimoniais relacionados a AC Raiz impõem que a data de hora do sistema e do HSM devem ser atualizados antes que qualquer procedimento ou cerimônia seja executado. Como o componente é *offline*, a atualização do relógio é feita manualmente, pelo operador da AC Raiz, utilizando, por exemplo, um relógio de parede, que fica ligado a uma FCT. A FCT pode ser um relógio atômico, que provê a hora visual

para o operador da AC Off-line acertar a data e hora do servidor e do HSM.

A ACT é responsável pela emissão de carimbos de tempo, conforme foi visto na Seção 2.7. Uma ACT possui um ou mais servidores de carimbo de tempo. Cada servidor utiliza um HSM para proteção da chave de assinatura dos carimbos. Tanto o relógio de hardware do servidor quanto o relógio do HSM necessitam estar sincronizados a uma fonte confiável de tempo para poderem emitir carimbos. Provavelmente, esses relógio são os mais críticos de todos os utilizados por uma ICP. Vale lembrar que os carimbos de tempo são usados como evidência de que uma mensagem ou documento eletrônico já existia antes de uma determinada data e hora no passado. Uma forma de se manter esses relógio devidamente sincronizado a uma TCP, é através do uso de Sistemas de Auditoria e Sincronismo, conforme descrito na Seção 2.7.3. O SAS, por sua vez, possui um servidor e um HSM, que fica sincronizado com um relógio atômico. O SAS é o responsável por prover a hora correta para a ACT.

A AC On-line e a AR, possuem um servidor e um HSM cada, e precisam manter seu relógio atualizado para as operações. Essa sincronização pode ser realizada de forma manual ou automática. De forma manual o operador precisa entrar com a data e hora. De forma automática, pode ser utilizado o NTP para sincronizar a data e hora.

A AC-Temporal e AC Otimizadora possuem também um servidor e um HSM cada, e esses necessitam estar com seus relógios sincronizados com uma FCT, pois suas funções dependem da hora correta pra o correto funcionamento.

O Servidor de Validação de Certificado e o OCSP, utilizam servidor e HSM para funcionar, e utilizam o relógio do servidor no registro do eventos, para auditoria, e o HSM para assinar os dados que são disponibilizados.

3.3 Análise do modelo

A política e a prática de operação de um componente de uma ICP são descritos em dois documentos: o de Políticas de Certificação (PC) e o de Declaração de Práticas de Certificação (DPC). Neles são descritos todas as tarefas que um componente deve fazer e como esses devem ser implementados. Entretanto, apesar de ser necessário, não se observa nas PCs e DPCs das principais ACs governamentais e comerciais uma preocupação maior com os relógios que são usados pelas tarefas e principalmente como esses

são sincronizados. Esses documentos não definem claramente como deve ser realizado a sincronização, mas estabelecem que os relógios devem ser sincronizados e com uma determinada precisão “X”. Apesar de alguns serviços usarem sincronização automática e outros um acerto manual dos relógios, eles estão dessincronizados entre eles mesmos, e os que usam um acerto manual a sincronização não é confiável.

O ideal é que todos os HSMs pertencentes a ICP possuíssem um relógio e fossem capaz de realizar uma sincronização segura da hora com fontes de tempo confiáveis. Do mesmo modo, os servidores pertencentes a ICP também deveriam ser capazes de realizar a sincronização segura. E para assegurar que isso realmente aconteça é necessário que os documentos de PC e DPC definam um procedimento de sincronização segura. Isso garante que todos os relógios da ICP estejam sincronizados entre si e com uma FCT.

Mas ainda desse modo existe vários problemas de ordem prática para realizar o sincronismo desses relógios. Por exemplo, se o HSM possuir somente conexão com o servidor como esse pode realizar o sincronismo automático do relógio? Poderia ser implementado um programa que é executado no servidor, que pegaria a hora do sistema e enviaria para o HSM através de mecanismos fornecidos pelo fabricante do HSM. Mas mesmo assim, sempre haverá um erro por causa dos atrasos que ocorrem nesse esquema. Outro ponto que pode ser abordado, é o HSM possuir um serviço de sincronismo de hora, como o NTP. Mas os únicos que implementam algo semelhante, são os utilizados para carimbo de tempo, e o modelo utilizado é proprietário e não se tem acesso ao fonte. E é necessário ter mais um equipamento, além do HSM, que é utilizado no sincronismo. Esse equipamento utilizado, chamado de Sistema de Auditoria e Sincronismo (SAS), fica ligado a um FCT, como um relógio atômico, e provê o sincronismo aos HSMs em tempos pré-determinados.

Outro problema que ocorre, é no caso de uma AC Off-line, que não possui conexão com o mundo exterior, como sincronizar de maneira segura o relógio do servidor e do HSM? Como visto, hoje é utilizado um relógio atômico que está conectado diretamente a um “display"que mostra a hora para o operador da AC Off-line. O operador acerta a hora do servidor e do HSM de modo visual, ele olha a hora no “display"e entra com o valor visto. Desse modo, o servidor e o HSM estarão dessincronizados entre si, e essa AC estará dessincronizada com a FCT. Um modo de resolver esse problema, é

conectar diretamente a FCT no HSM e no servidor.

Acontece, na prática, que alguns HSMs e servidores são mantidos desligados por um longo período de tempo, como é o caso de uma AC-Raiz e ACs intermediárias *offline*. O servidor e o HSM que possui relógio, tem uma bateria cada um, que mantém a hora no relógio no caso em que o equipamento estiver desligado. Se a energia da bateria acabar enquanto o equipamento estiver desligado, o relógio para de funcionar. No momento em que o equipamento é religado, e ocorrer a próxima sincronização, é necessário que o usuário seja informado de que a hora do relógio do servidor ou do HSM, estão com erros superiores ao estabelecido, e seja registrado nos eventos que ocorreu uma sincronização onde a hora estava com um erro maior do que o estabelecido. Se isso não ocorrer, haverá um problema durante a utilização das aplicações que dependem do relógio e até mesmo de auditoria, pois ocorre uma dessincronização do tempo entre o HSM e o servidor e entre os componentes. Essa dessincronização gera também uma inconsistência no registro de eventos utilizados no processo de auditoria.

3.4 Conclusão

Esse capítulo apresentou os componentes que fazem parte de uma ICP, e os relógios que compõem os componentes. É mostrada a sincronização do relógio para cada tipo de componente. Após isso, foi feita uma análise crítica, falando da situação atual do sincronismo do relógio e como poderia ser feito para resolver o problema encontrado.

Capítulo 4

Módulo de Relógio Seguro

4.1 Introdução

A criptografia pode ser usada em aplicações que visam o controle de eventos no passado, no presente e no futuro conforme ilustra a Figura 4.1. São três as principais aplicações criptográficas em uma infra-estrutura de chaves públicas que utilizam relógios relacionadas a esses eventos. Por exemplo, para provar que uma informação digital existia no passado, utiliza-se o carimbo de tempo. No presente, utilizam-se certificado digital em processos de autenticação e serviços de tempo para o sincronismo de relógio. E para o futuro utiliza-se certificados temporais que permitem controlar quando uma informação digital pode ser visualizada pelo destinatário. Todas essas aplicações utilizam relógios como fonte confiável de tempo, para controlar os eventos no tempo.

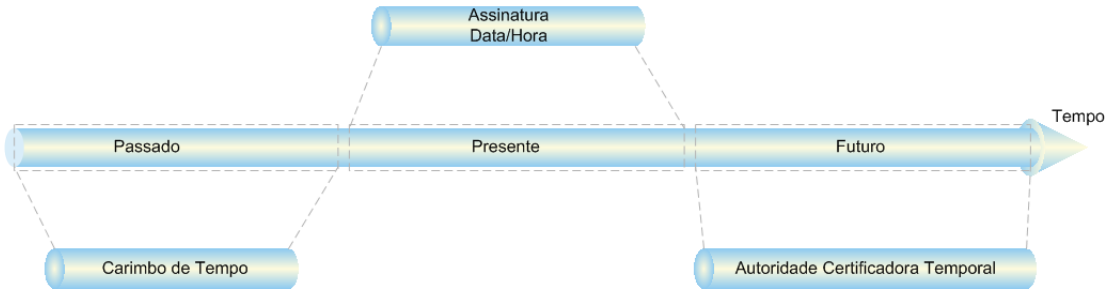


Figura 4.1: Linha do Tempo e Aplicações Criptográficas

Esses relógios precisam ser gerenciados de forma segura e confiável. Não deveria ser possível, por exemplo, que usuários, mesmo que sejam administradores do sistema, alterem os relógios sem a devida autorização. É necessário portanto, o estabelecimento de protocolos que permitam o rígido controle do ciclo de vida dos relógios.

A prática tem mostrado que só é possível esse tipo de controle com o auxílio de hardware criptográfico. Esse hardware deve ser projetado levando em consideração os serviços relacionados ao tempo exemplificados na Figura 4.1.

Assim este capítulo apresenta o projeto de um hardware criptográfico especializado em serviços relacionados com o tempo voltados a aplicações criptográficas. Deu-se o nome de Módulo de Relógio Seguro (MRS) a esse novo tipo de equipamento.

A Seção 4.2 explica o uso de um hardware criptográfico na construção do MRS. A Seção 4.3 apresenta dois HSM de mercado com relógio e o método de acesso ao relógio. A Seção 4.4 define os experimentos a serem realizados com os relógios para se conhecer a qualidade de cada um. A Seção 4.6 mostra os tipos de sincronismo de relógio que o MRS pode adotar. A Seção 4.7 apresenta os serviços que serão providos pelo MRS. A Seção 4.8 apresenta um modelo de gestão do MRS. A Seção 4.9 explica como que foi desenvolvido o protótipo do MRS.

4.2 Apresentação do Módulo de Relógio Seguro

O MRS foi desenvolvido pensando numa solução que concentre os serviços de carimbo de tempo, serviço de sincronismo de relógio e certificado digital temporal, em um único equipamento e que fosse possível sua gestão de forma segura e confiável.

Para se ter uma gestão de relógio segura e confiável, é necessário um hardware que seja confiável e seguro. Um hardware criptográfico, como o *Hardware Security Module*(HSM), é um hardware confiável e seguro pois ele foi avaliado e certificado como aderente as normas FIPS 140-2 [31] e *Common criteria* (CC) [32–34].

A FIPS 140-2 é publicada e mantida pelo *National Institute of Standards and Technology* (NIST) que especifica os requisitos de segurança dos módulos de hardware criptográficos. Ela classifica os HSM em quatro níveis crescentes e cumulativos de segurança:

Nível 1 É o menor nível de segurança. Não prevê mecanismos físicos de segurança. O software deve utilizar os algoritmos aprovados pelo NIST. Podem ser utilizados em qualquer computador.

Nível 2 Este nível aumenta os requisitos do nível anterior. É imposta a restrição de acesso

físico, como revestimento com detecção de violação ou lacres que permitam verificar a violação do sistema. A autenticação deve ser baseada em papéis. O sistema operacional utilizado pelo software criptográfico deve ser avaliado como nível 2 ou superior do CC.

Nível 3 Neste nível as restrições são maiores que as do nível 2, não sendo permitido o acesso aos dados críticos de segurança por parte da entidade que venha ter acesso ao hardware. Os mecanismos de segurança tentam evitar e responder as tentativas de invasão, como invólucros resistentes a invasão e com detecção de invasão, e em caso de quebra da segurança os dados críticos de segurança devem ser apagados por circuitos zeradores de dados. A autenticação é baseada na identidade. Todos os dados que entram ou saem do módulo devem estar na forma cifrada. O sistema operacional utilizado pelo software criptográfico deve ser avaliado como nível 3 ou superior do CC.

Nível 4 Este nível apresenta uma proteção física abrangente, como sensores de temperatura, pressão e tensão de alimentação. Qualquer mudança no ambiente externo, pode ser um indício de um ataque físico ao módulo, e os dados devem ser apagados pelo circuito zerador de dados. O sistema operacional utilizado pelo software criptográfico deve ser avaliado como nível 4 ou superior do CC.

A *Common Criteria* é um framework que define os requisitos de segurança para produtos voltados para a segurança da informação. Ela é composta por Perfis de Proteção, Alvos de Segurança e componentes que proverão funcionalidades de segurança ou darão garantias de compatibilidade com os níveis de avaliação de garantias. A CC possui 7 níveis de avaliação de garantias. Esse níveis foram criados para servirem de critérios para a avaliação de perfis de proteção e dos objetos de segurança. Uma visão geral das garantias obtidas em cada nível de avaliação de garantia pode ser visualizada na Tabela 4.1:

O uso de um hardware criptográfico para o desenvolvimento do MRS, garante que o MRS seja resistente a ataques e que as informações sensíveis estarão seguras.

Tabela 4.1: Requisitos dos níveis de avaliação de garantia [3]

Nível:	Garantia Obtida:
EAL1	Funcionalmente testado
EAL2	Estruturamente testado
EAL3	Metodicamente testado e verificado
EAL4	Metodicamente projetado, testado e verificado
EAL5	Semi-formalmente projetado e testado
EAL6	Semi-formalmente verificado, projetado e testado
EAL7	Formalmente verificado, projetado e testado

4.3 Relógio em HSM

Após a escolha do tipo de hardware criptográfico a ser usado, foi feita uma análise em dois HSMs que se obteve acesso. O ASI HSM da RNP e o PSO PL50 da Eracom-Safenet. No PSO PL50 o relógio do HSM fica dentro do HSM. Uma aplicação para usar os serviços do HSM, utiliza uma interface de acesso, o “Provedor de Acesso ao HSM PCI"conforme ilustra a Figura 4.2.

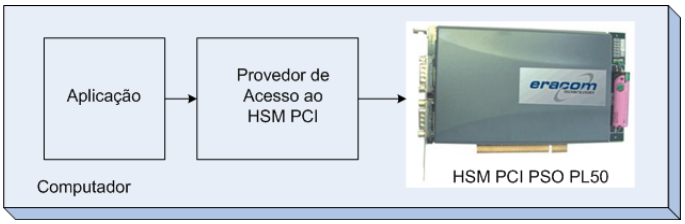


Figura 4.2: Interface de comunicação entre a aplicação e o HSM PSO PL50

O ASI HSM é um HSM que foi desenvolvido num Grupo de Trabalho da Rede Nacional de Pesquisa (RNP) em conjunto com o Laboratório de Segurança em Computação (LabSEC) da Universidade Federal de Santa Catarina (UFSC) para uso educacional. O relógio do HSM fica dentro do HSM, numa área chamada Unidade de Segurança. Uma aplicação para utilizar os serviços do ASI HSM usa uma *engine* do OpenSSL conforme ilustra a Figura 4.3.

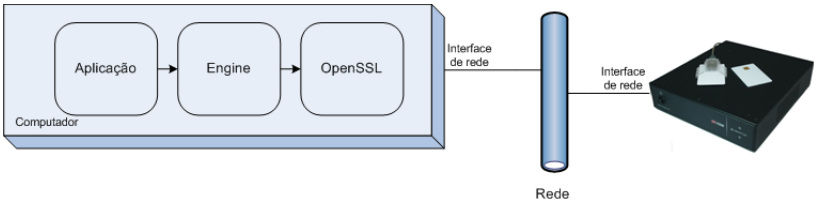


Figura 4.3: Interface de comunicação entre a aplicação e o HSM ASI

Esse dois HSMs possuem um relógio interno cada um. Foram definidos

experimentos para analisar a qualidade dos relógios desses dois HSMs. A Seção 4.4 apresenta esses experimentos e a análise que foi feita em cima dos dados coletados. E a Seção 4.5 mostra um resumo da análise feita em cima dos dados dos experimentos.

4.4 Definição e Análise dos Experimentos

A análise consistiu em calibrar o relógio do HSM com uma Fonte de Tempo Confiável (FCT). Foram utilizados como FCT o sincronismo via NTP utilizando 3 servidores stratum 2. As análises efetuadas foram feitas em cima de 2 experimentos conforme a Tabela 4.2. Cada experimento foi dividido em dois, um com o HSM não realizando operações criptográficas e outro com o HSM realizando operações criptográficas.

Tabela 4.2: Experimentos

Experimento	Sem carga criptográfica	Com carga criptográfica
1	Sincronização NTP Intervalo 1seg	Sincronização NTP Intervalo 1seg
2	Sincronização NTP Intervalo 1min	Sincronização NTP Intervalo 1min

O objetivo do experimento é levantar as possíveis dependências da estabilidade do relógio. Se os fatores como temperatura e tensões de alimentação alteram a estabilidade do relógio em condições normais de uso no dia a dia. Foram também analisados no HSM se a realização de operações criptográficas influência na estabilidade do relógio. A primeira parte do experimento o HSM não realiza operações criptográficas, na segunda parte o HSM está realizando operações criptográficas, como gerar assinaturas digitais.

As subseções a seguir são apresentadas as análises feitas em cima do resultado de cada experimento.

4.5 Resumo dos Resultado das Análises

Como pode ser visto nas análises, o deslocamento entre o relógio do HSM e da FCT, tem um aumento uniforme. Realizando uma regressão linear, é possível predizer o deslocamento entre os relógios em qualquer instante de tempo. Ainda de acordo com a regressão linear, é possível se conhecer a inclinação da reta a partir do

parâmetro β. A inclinação da reta foi usada para se conhecer a instabilidade dos relógios. A Tabela 4.3 mostra um resumo da análise sobre os experimentos da Seção 4.4.

Tabela 4.3: Resumo das análises dos experimentos

Experimento	PSO PL50	ASI HSM
Sem carga 1seg	β = 6,48 $\times 10^{-5}$	β = 8,139 $\times 10^{-6}$
Sem carga 1min	β = 0,004	β = 3,98 $\times 10^{-4}$
Com carga 1seg	β = 5,57 $\times 10^{-5}$	β = 1,585 $\times 10^{-6}$
Com carga 1min	β = 0,003	β = 8,738 $\times 10^{-5}$

Como pode ser notado na Tabela 4.3, o HSM ASI HSM tem uma instabilidade menor no seu relógio em relação ao relógio do HSM PSO PL50.

Os resultados apresentados na Tabela 4.3 são exclusivos dos HSM's testados, não podendo ser dito como resultados verdadeiros para qualquer HSM.

4.6 Sincronismo do Relógio do Módulo de Relógio Seguro

Nesta seção é proposto um modelo de sincronismo do relógio do Módulo de Relógio Seguro (MRS). A Figura 4.4 apresenta as principais FCT para o MRS. A primeira é o uso de um relógio atômico ligado diretamente no MRS. A segunda é o uso do GPS ligado diretamente no MRS, e provendo a hora UTC. E o terceiro modo é o uso do NTP para a sincronização do relógio.

O relógio atômico seria a opção ideal, porém tem um alto custo tornando o uso do MRS proibitivo. O GPS seria a próxima opção. Entretanto há várias dúvidas com relação ao seu uso uma vez que o GPS é comandado pelo governo americano. Então a melhor opção é o uso do NTP. O maio desafio do NTP é como afirmar à terceira parte que o relógio do HSM está sincronizado com o NTP. Como o MRS pode saber que está se sincronizando com servidor NTP confiável. Para isso pode ser utilizado esquemas de autenticação baseada no uso de certificados digitais.

O procedimento para a sincronização segura é:

1. O MRS autentica os servidores NTP em intervalos que são definidos;

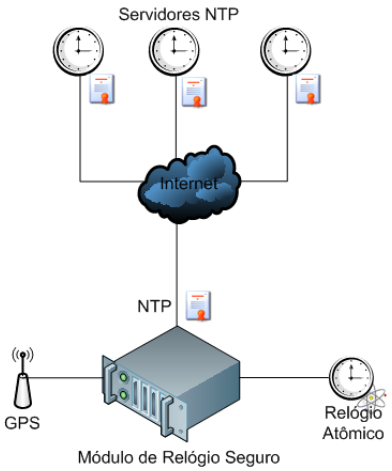


Figura 4.4: Possíveis FCT para o MRS

2. o MRS realiza a sincronização.

A autenticação é feita através de criptografia assimétrica, utilizando certificados digitais pertencentes a uma ICP a qual os servidores NTP e o MRS fazem parte. A sincronização é realizada através do NTP, com no mínimo três servidores, para um melhor funcionamento dos algoritmos do NTP na escolha de uma melhor FCT.

No MRS são definidas variáveis para o sincronismo, como exatidão do relógio, atraso de rede para ajustes do relógio, número de tentativas em casos de erro e intervalos de sincronismo.

4.7 Aplicações do MRS

Como o MRS é um módulo que provê os serviços de tempo para uma ICP, três dos principais serviços utilizados no módulo são descritos abaixo. O Serviço de Carimbo de Tempo e a Autoridade Certificadora Temporal foram desenvolvidas no LabSEC como parte de projetos e trabalhos de conclusão de curso. Para o Serviço Sincronismo de Relógio foi utilizado a aplicação NTP.

4.7.1 Serviço de Carimbo de Tempo

Para a marca de carimbo de tempo, foi desenvolvida a aplicação de Serviço de Carimbo de Tempo (SCT) [35].

O SCT é responsável por criar e assinar um carimbo de tempo em nome da Autoridade de Carimbo de Tempo. Foi desenvolvido conforme a RFC3161 [18], utiliza a biblioteca libcryptosec [36] que implementa funções criptográficas, incluindo suporte a *smartcards*, segredo compartilhado e outras. O mecanismo de transporte de mensagens entre o SCT e o cliente pode ser feita por dois tipos: *Socket Based Protocol* e *HyperText Transfer Protocol*.

4.7.2 Sincronismo de Relógio

Para o Serviço de Hora, foi utilizado o software do NTP Project (R&D) [23] , que já contém suporte ao Draft da versão 4 do NTP.

O serviço de hora é configurado para disseminar a hora UTC para os clientes. Ele pode operar em dois níveis de *Stratum*. Se estiver ligado a um relógio atômico ou a um GPS, e esse fornecer a hora correta, o servidor funcionará como *Stratum* 1. Se tiver utilizando o NTP, para se sincronizar a uma servidor *Stratum* 1, funcionará como *Stratum* 2.

A comunicação do NTP entre cliente e servidor pode ser configurada de duas maneiras. A primeira o servidor disponibiliza a hora, e o cliente precisa se conectar no servidor para pegar a hora. A segunda o servidor envia periodicamente atualizações de hora para um endereço *broadcast/multicast*, que o cliente faz parte.

A conexão NTP é uma conexão segura, onde cliente e servidor possuem certificados digitais emitidos por uma Autoridade Certificadora de confiança, utilizado na identificação de cada um.

4.7.3 Autoridade Certificadora Temporal

Para o envio de informação para o futuro, foi desenvolvida uma Autoridade Certificadora Temporal (AC-Temporal). A AC-Temporal desenvolvida foi baseada no conceito da criptografia temporal, e faz o uso de criptografia assimétrica para cifrar e decifrar. Na criptografia assimétrica, são usados dois algoritmos diferentes, o que um cifra somente o outro decifra, e com chaves diferentes para os algoritmos. A AC-Temporal atua como uma terceira entidade confiável (TEC), gerenciando as chaves usadas para decifrar. Ela foi dividia em duas partes, um servidor e um cliente. O servidor é executado no MRS e gerencia as chaves. O cliente é uma interface com o usuário que utiliza o sistema. Foi

desenvolvida em linguagem PHP [37], utilizando um módulo em php da libcryptosec, a php5-libcryptosec [38], para funções criptográficas.

A Figura 4.5 ilustra como funciona. Primeiro, um usuário requisita um Certificado Digital Temporal(CDT) para a AC-Temporal. A AC-Temporal envia o CDT para o servidor, que gera um par de chaves assimétricas, uma *chave de sigilo* e uma *chave de liberação*. A *chave de sigilo* é liberada, na forma de um CDT, pela AC-Temporal num serviço de diretório. O usuário, que requisitou o CDT, pega o CDT, cifra seu documento, e envia o documento cifrado para o destinatário. A *chave de liberação* é protegida pelo servidor, assegurando que a chave somente será liberada na data estipulada. No futuro, na data estipulada, o servidor libera a *chave de liberação*, na formato PKCS12. O destinatário acessa a AC-Temporal, e baixa a *chave de liberação* adequada no serviço de diretório, e decifra o documento cifrado recebido no passado.

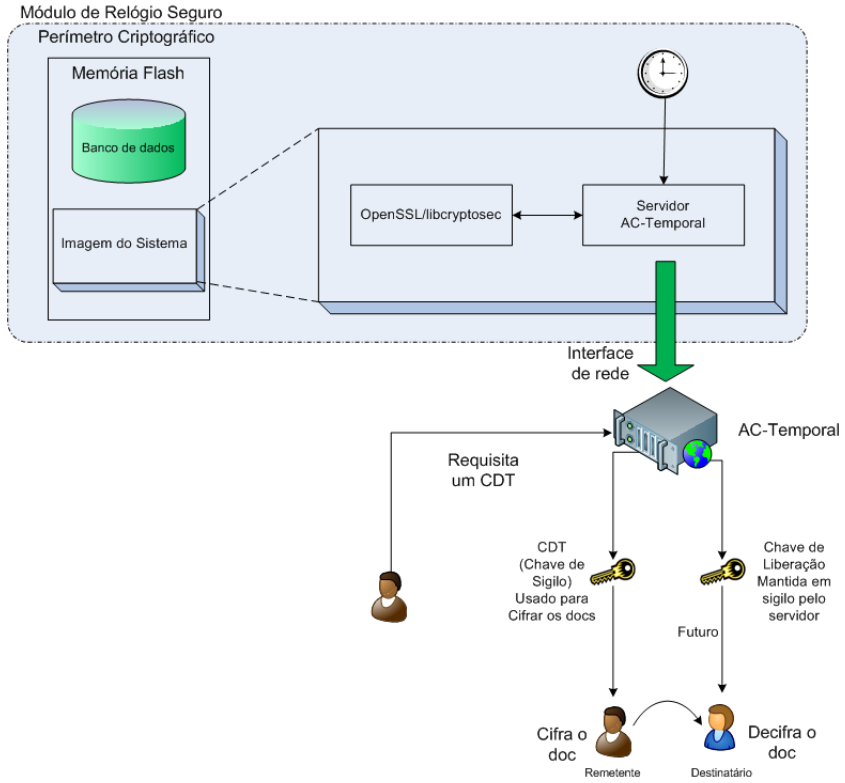


Figura 4.5: Esquema de funcionamento da Autoridade Certificadora Temporal

4.8 Modelo de Gestão

A gestão do relógio do MRS, compreende desde a sua inicialização, o seu sincronismo e o seu uso. Na análise da gerencia do relógio deve ser levado em

consideração:

- Inicialização do relógio - Garantir que haja um relógio, com uma boa qualidade.
- Sincronismo do relógio - Garantir a exatidão do relógio.
- Uso do relógio - O uso do relógio sera garantindo somente aos serviços que fazem parte do MRS.
- Auditoria do relógio - Garantir a criação de um histórico completo e rastreável de todos os ajustes do relógio.

Os processos responsáveis pelo gerenciamento do relógio devem ser adequadamente projetados e forma segura e ser executados em ambiente seguro. Para tal, no presente modelo colocamos a gerência do relógio como um mecanismo protegido por outros mecanismos de autenticação e autorização.

Ao estipularmos o gerenciamento do relógio com base nos requisitos acima citados, foi definido 3 conjuntos de atores para a iteração do sistema. O gerenciamento do relógio é realizado pelo seguinte conjunto de atores:

- Um conjunto de Administradores, os quais são responsáveis pelas operações administrativas, como inicialização do relógio, configuração do sincronismo do relógio, inicialização dos serviços de tempo, cadastramento dos operadores e auditores;
- Um ou mais conjuntos de Operadores, os quais são responsáveis pela criação das chaves privadas, configuração dos serviços de tempo, operação dos serviços de tempo;
- Um conjunto de Auditores, os quais são responsáveis pela auditoria dos eventos ocorridos no MRS.

4.9 Protótipo

A Figura 4.6 mostra uma foto do protótipo desenvolvido.

Para o desenvolvimento do protótipo do MRS, foi utilizado um computador e um HSM. O computador foi utilizado para instalar as interfaces de configuração dos serviços providos pelo MRS, e também o cliente da Autoridade Certificadora Temporal, como visto na Seção 4.7.3.

Figura 4.6: Protótipo do Módulo de Relógio Seguro

O HSM foi utilizado como hardware criptográfico do MRS. Foi escolhido o ASI HSM como hardware criptográfico. Como visto na Seção 4.5, o relógio do ASI HSM possui uma instablidade menor do que do PSO PL5. Além disso, como esse HSM foi desenvolvido no LabSEC, o acesso a imagem do sistema é completa. Nesse caso é possível customizá-la para atender todas as necessidades do MRS.

A imagem do sistema do MRS, possui o sistema operacional FreeBSD na sua versão 6.2 [39], que teve seu *kernel* totalmente customizado para atender as necessidades de *hardware* do ASI HSM. Somente os executáveis necessários para realizar as tarefas de inicialização e configuração do sistema operacional ficaram na imagem. Além disso, foi adicionado os serviço de carimbo de tempo, de sincronismo de relógio e certificado temporal.

A Figura 4.7 mostra a estrutura interna do MRS.

Nessa figura, dois relógios aparecem, um na imagem do sistema, que é o relógio do sistema, utilizado pelo kernel, para manter o sincronismo dos processos. E o relógio da unidade de segurança, que é o relógio provido pelo HSM, é utilizado pelos servidores ao montarem a informação temporal. O SCT ao gerar um carimbo de tempo, necessita do hora para anexar ao carimbo. O servidor de hora ao prover a hora, pega a hora do relógio. A AC-Temporal precisa da hora para saber quando deve liberar a chave de liberação. Os servidores de Carimbo de Tempo e AC-Temporal utilizam a libcryptosec

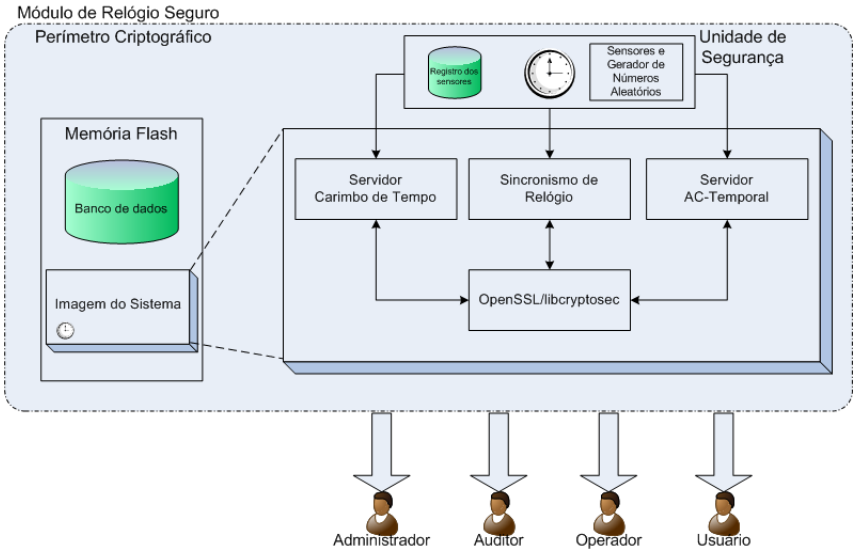


Figura 4.7: Estrutura interna do Módulo de Relógio Seguro

para as funções criptográficas, e o servidor de hora utiliza o OpenSSL para as funções criptográficas.

O MRS é acessado pelo administrador do sistema por uma interface web. Nessa interface, o administrador inicializa o relógio do MRS, configura como será o sincronismo desse relógio com a FCT, inicializa os serviços de tempo e cadastra os usuários operadores e auditores. Os operadores acessam o MRS por uma interface web também. Os operadores são capazes de criar as chaves privadas utilizada pelos serviços de tempo, e a configuração e operação dos serviços de tempo. Os auditores tem acesso pela interface web para realizar as operações de auditoria do MRS.

Capítulo 5

Infra-estrutura para Âncora Temporal

5.1 Introdução

Este capítulo apresenta uma proposta de políticas e práticas para o uso do Módulo de Relógio Seguro (MRS) numa ICP. As políticas e as práticas devem fazer parte do conjunto de normativos da ICP com o objetivo de regulamentar o uso do Módulo de Relógio Seguro. Um MRS, tem como sua principal meta, gerir de forma segura seu relógio, assegurando e emitindo evidências de que esteja sincronizado com uma fonte confiável do tempo. Toda as operações do MRS devem ser registradas e passíveis de auditoria.

Como proposto no Capítulo 4, o MRS oferece os seguintes serviços relacionados com o tempo: Autoridade Certificadora Temporal, Autoridade de Carimbo de Tempo e Servidor de Sincronismo de Relógio. Assim, as políticas e práticas levam em considerações esses três serviços.

A políticas e práticas propostas neste capítulo foram baseadas na RFC 3647 [40], na RFC 3628 [41]. A Seção 5.2 apresenta uma visão geral da infra-estrutura. As políticas e práticas propostas levam em consideração os componentes dessa infra-estrutura.

A Seção 5.3 apresenta a lista de requisitos (políticas) que o MRS deve atender e a Seção 5.4 como esses requisitos poderiam ser implementados, ou seja, um conjunto de boas práticas de gestão do MRS.

5.2 Visão Geral da Infra-estrutura

O MRS é um equipamento especializado em relógio que, propõe-se, seja o concentrador de todos os serviços de relógios dos componentes de uma ICP. A Figura 5.1 ilustra como o MRS deve ser incluído numa ICP.

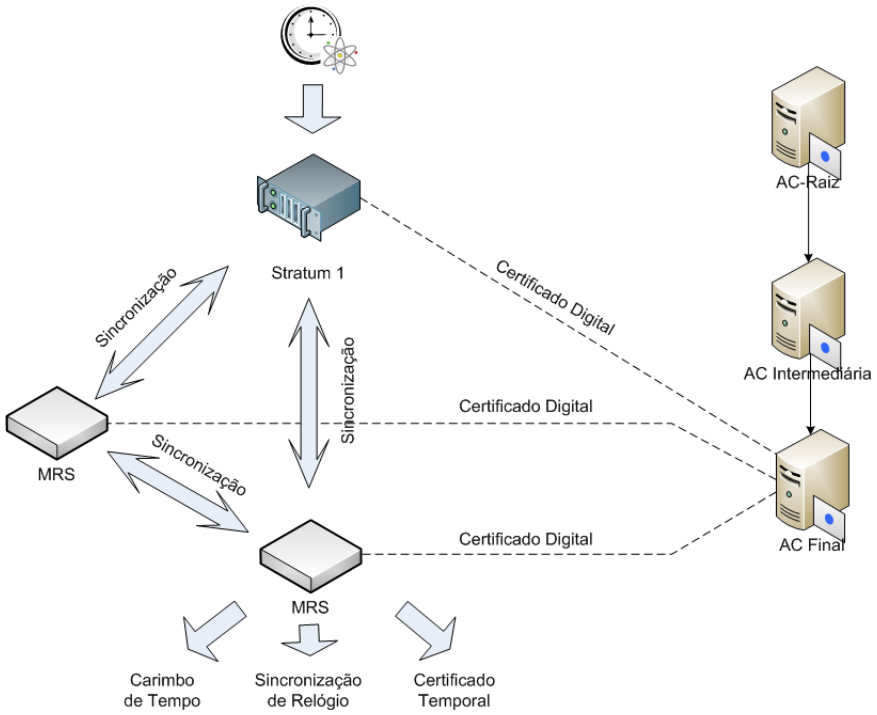


Figura 5.1: Modelo do MRS numa ICP

Uma ICP pode usar mais de um MRS, para que os serviços de relógio estejam sempre disponíveis e na qualidade necessária. A colocação em uso de MRSs numa ICP requer a definição e o entendimento de seu papel por todos os participantes da ICP, desde a AC Raiz até a parte confiante que se beneficiará dos seus serviços. A subseção 5.2.1 apresentadas cada uma dessas entidades, seu papel na ICP e se for o caso, sua responsabilidade sobre o MRS. A subseção 5.2.2 descreve como é realizado o processo de sincronização do relógio do MRS com servidores *stratum* 1 e entre outros MRS.

5.2.1 Entidades participantes

As entidades integrantes e seu papel na estrutura com o MRS são:

Comitê Gestor da ICP É responsável pela implantação da ICP como um todo. Estabelece políticas, critérios e normas de funcionamento que devem ser seguidas pelas

entidades integrantes, o que inclui os serviços do MRS, da ICP e audita e fiscaliza as AC raízes.

Autoridades Certificadoras Emitem, renovam ou revogam certificados digitais de outras AC ou de titulares finais e emitem e publicam listas de certificados revogados (LCR). Na estrutura do módulo de relógio seguro, emite adicionalmente os certificados digitais usados pelo MRS e por todos os serviços relacionados ao tempo.

Servidores *stratum* 1 Utiliza a autenticação mútua e provê o sincronismo do relógio, estão ligados a relógios atômicos.

Autoridade de Carimbo de Tempo Emite carimbos de tempo. É parte integrante do MRS.

Sincronismo de Relógio Provê o sincronismo do tempo. É parte integrante do MRS.

Autoridade Certificadora Temporal Emite certificados temporais. É parte integrante do MRS.

Subscritor ou Cliente Participante que solicita os serviços de tempo disponíveis no MRS, implícita ou explicitamente concordando com os termos mediante os quais o serviço é oferecido.

Terceira Parte Aquele que confia no teor, validade e aplicabilidade dos serviços de tempo disponíveis no MRS.

5.2.2 Processo de Sincronização do Tempo

As entidades que compõem a estrutura da ICP irão realizar a sincronização de seus relógios com o MRS, que utiliza mecanismos para garantir o sincronismo do relógio do equipamento com uma fonte confiável do tempo. Os procedimentos usados para manter sincronismo do MRS são os seguintes:

Procedimentos da FCT A FCT estará localizado nas instalações da AC Raiz, e terá um relógio atômico que está ligado a um servidor *stratum* 1. Esse possuirá certificados digitais para a autenticação mútua, que estarão disponíveis ao MRS.

Procedimentos do MRS O MRS disponibilizará seus certificados digitais à FCT, para a autenticação mútua. Após a autenticação, o sincronismo do relógio ocorrerá periodicamente, em período tal que o deslocamento acumulado não ultrapasse o valor especificado na política de relógio seguro correspondente ao MRS. O sincronismo deve ser realizado com no mínimo três FCT, como especificado na Seção 4.6.

Para posterior processo de auditoria, s operações de autenticação mútua e sincronismo gerarão arquivos nas FCT e MRS, contendo dados resultantes destas operações.

Os arquivos de registro da FCT devem conter no mínimo as seguintes informações quanto a autenticação:

- data e hora de realização da autenticação;
- endereço de rede da FCT;
- endereço de rede do MRS;
- identificação do certificado digital do MRS;
- mensagem de aviso ou de erro.

Os arquivos de registro do MRS devem conter as seguintes informações quanto a autenticação:

- data e hora de realização da autenticação;
- endereço de rede da FCT;
- endereço de rede do MRS;
- identificação do certificado digital da FCT;
- mensagem de aviso ou de erro.

Os arquivos de registro do SAS e do MRS devem conter no mínimo as seguintes informações quanto a sincronização:

- data e hora de realização do sincronismo;

- erro do relógio do MRS;
- retardo;
- endereço de rede da FCT;
- endereço de rede do SCT.

5.3 Políticas para Relógio Seguro

O conjunto de políticas de uso de um MRS deve ser formalizado em um documento chamado de Políticas para Relógio Seguro (PRS). Essa seção apresenta os requisitos gerais proposto para esse documento. As subseções a seguir seguem o formato sugerido na RFC-3647 [40]. Cada subseção é um capítulo do documento de políticas.

5.3.1 Introdução

Deve apresentar uma breve visão geral do documento, o nome do documento e sua identificação no formato Object Identifier (OID). É descrito a comunidade do MRS, a parte integrante da ICP e a parte que utiliza os serviços providos pelo MRS. É identificado a entidade responsável pelo MRS.

5.3.2 Responsabilidade de Publicação e Responsabilidade

Deve apresentar os repositórios, a hora ou freqüência de publicação das informações e definido o controle de acesso.

5.3.3 Identificação e Autenticação

Deve apresentar a identificação e o modo de autenticação das terceiras partes que usarão os serviços providos pelo MRS.

5.3.4 Requisitos Operacionais para o Módulo de Relógio Seguro

Deve apresentar a exatidão e o deslocamento máximo do relógio em relação a FCT. E também como se deve proceder o processo de sincronismo do relógio do MRS.

5.3.5 Componentes, Gerenciamento e Controles Operacionais

Deve apresentar os controles físicos de acesso, como a localização e a construção. O controle processual, como o número de pessoas por tarefa. O controle de pessoal, como a qualificação e experiência de quem vai trabalhar, e treinamento de pessoal. Procedimentos de geração de registros para auditoria, como tipos de eventos, freqüência de análise dos registros, procedimentos de backup. Arquivamento dos registros, como tipos de registros, período de arquivamento, procedimentos de obtenção e verificação dos registros arquivados. O processo de recuperação de desastre e no caso de comprometimento da chave privada.

5.3.6 Controles Técnicos de Segurança

Deve apresentar os requisitos de segurança da rede de dados.

5.3.7 Perfis de Certificados, LCR e OCSP

Deve apresentar os perfis dos certificados dos serviços providos pelo MRS, o perfil da lista de certificados revogados e de OSCP.

5.3.8 Fiscalização e Auditoria de Conformidade

Deve apresentar a freqüência das auditorias, e identificação e qualificação de pessoal que realizará as auditorias.

5.4 Declaração de Práticas para Relógio Seguro

A declaração de práticas de uso de um MRS deve ser formalizado em um documento chamado de Declaração de Práticas para Relógio Seguro (DPRS). Essa seção apresenta define requisitos gerais proposto para esse documento. As subseções a seguir seguem o formato sugerido na RFC-3647 [40]. Cada subseção é um capítulo do documento de declaração de práticas.

5.4.1 Introdução

Deve apresentar uma breve visão geral do documento, o nome do documento e sua identificação no formato Object Identifier (OID). É descrito a comunidade do MRS, a parte integrante da ICP e a parte que utiliza os serviços providos pelo MRS. É identificado a entidade responsável pelo MRS.

5.4.2 Responsabilidade de Publicação e Repositórios

Devem ser publicadas pela entidade responsável pelo DPRS do MRS, as informações, o modo pelo qual serão disponibilizadas e a sua disponibilidade. As seguintes informações, no mínimo, deverão ser publicadas:

- sua DPRS;
- as PRS que implementa;
- as condições gerais mediante as quais são prestados os serviços;
- a exatidão do relógio do MRS em relação ao UTC;

De modo a assegurar a disponibilização sempre atualizada de seus conteúdos, deve ser informada a freqüência de publicação das informações.

5.4.3 Identificação e Autenticação

Deve apresentar a identificação e o modo de autenticação das terceiras partes que usarão os serviços providos pelo MRS.

5.4.4 Requisitos Operacionais para o Módulo de Relógio Seguro

Como processo de sincronismo de tempo do relógio do MRS, o MRS deve se conectar, no mínimo, a três servidores confiáveis, realizar a autenticação mútua com certificado digital, escolher o melhor servidor para a sincronização, sincronizar o relógio do MRS com o do FCT.

5.4.5 Componentes, Gerenciamento e Controles Operacionais

A subseção 5.4.5.1 descreve os controles de segurança física, procedimental e de pessoal. A Subseção 5.4.5.2 descreve o processo de auditoria.

5.4.5.1 Controles de Segurança Física, Procedimental e de Pessoal

Toda entidade responsável pelo MRS integrante da ICP deverá implantar um sistema de controle de acesso físico que garanta a segurança de suas instalações, conforme o documento de políticas de segurança da ICP e os requisitos que seguem.

A DPC da entidade responsável pelo MRS deve definir pelo menos 3 (três) níveis de acesso físico aos diversos ambientes da entidade responsável pelo MRS e mais 1 (um) quarto nível relativo à proteção do MRS.

O primeiro nível - ou nível 1 - deverá situar-se após a primeira barreira de acesso às instalações da entidade responsável pelo MRS. O ambiente de nível 1 das entidade da ICP desempenha a função de interface com o cliente que deseja utilizar o serviço providos pelo MRS e necessita comparecer pessoalmente.

O segundo nível - ou nível 2 - será interno ao primeiro e deverá requerer a identificação individual das pessoas que nele entram. Esse será o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da entidade responsável pelo MRS. A passagem do primeiro para o segundo nível deverá exigir identificação por meio eletrônico e o uso de crachá.

O ambiente de nível 2 deverá ser separado do nível 1 por paredes divisórias de escritório, alvenaria ou pré-moldadas de gesso acartonado. Não deverá haver janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso. O acesso a este nível deverá ser permitido apenas a pessoas que trabalhem diretamente com os serviços providos pelo MRS ou ao pessoal responsável pela manutenção de sistemas e equipamentos dos serviços providos pelo MRS, como administradores de rede e técnicos de suporte de informática. Demais funcionários ou do possível ambiente que esta compartilhe não deverão acessar este nível. Preferentemente, no-breaks, geradores e outros componentes da infra-estrutura física deverão estar abrigados neste nível, para evitar acessos ao ambiente de nível 3 por parte de prestadores de serviços de manutenção.

Excetuados os casos previstos em lei, o porte de armas não será admitido nas instalações da entidade responsável pelo MRS, a partir do nível 2. A partir

desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, terão sua entrada controlada e somente poderão ser utilizados mediante autorização formal e sob supervisão.

O terceiro nível - ou nível 3 - deverá situar-se dentro do segundo e será o primeiro nível a abrigar material e atividades sensíveis da operação da entidade responsável pelo MRS. Qualquer atividade relativa os serviços providos pelo MRS deverão ser realizados nesse nível. Somente pessoas autorizadas poderão permanecer nesse nível.Deverão ser controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle deverão ser requeridos para a entrada nesse nível: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica ou digitação de senha. As paredes que delimitam o ambiente de nível 3 deverão ser de alvenaria ou material de resistência equivalente ou superior. Não deverá haver janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso. Caso o ambiente de nível 3 possua forro ou piso falsos, devem ser adotados recursos para impedir o acesso ao ambiente por meio desses, tais como grades de ferro estendendo-se das paredes até as lajes de concreto superior e inferior. Deve haver uma porta única de acesso ao ambiente de nível 3, que abra somente depois que o funcionário tenha se autenticado eletronicamente no sistema de controle de acesso. A porta deve ser dotada de dobradiças que permitam a abertura para o lado externo, de forma a facilitar a saída e dificultar a entrada no ambiente, bem como de mecanismo para fechamento automático, para evitar que permaneça aberta mais tempo do que o necessário.

Poderão existir vários ambientes de nível 3 para abrigar e segregar, quando for o caso:

- equipamentos de produção e cofre de armazenamento; e
- equipamentos de rede e infra-estrutura (firewall, roteadores, switches e servidores).

Caso a entidade responsável pelo MRS se situe dentro de um datacenter, com requisitos de segurança julgados adequados pela AC-Raiz, poderá ser dispensada a existência do ambiente de nível 3.

O quarto nível, ou nível 4, interior ao ambiente de nível 3, deverá compreender pelo menos 2 cofres ou gabinetes reforçados trancados, que abrigarão, separadamente:

- os MRS;
- outros materiais criptográficos, tais como cartões, chaves, dados de ativação e suas cópias.

Para garantir a segurança do material armazenado, os cofres ou os gabinetes deverão obedecer às seguintes especificações mínimas:

- ser feitos em aço ou material de resistência equivalente; e
- possuir tranca com chave.

O cofre ou gabinete que abrigará os MRS deverá ser trancado de forma que sua abertura seja possível somente com a presença de dois funcionários de confiança.

A segurança de todos os ambientes deverá ser feita em regime de vigilância 24 x 7 (vinte e quatro horas por dia, sete dias por semana). A segurança poderá ser realizada por:

- guarda armado, uniformizado, devidamente treinado e apto para a tarefa de vigilância; ou
- Circuito interno de TV, sensores de intrusão instalados em todas as portas e janelas e sensores de movimento, monitorados local ou remotamente por empresa de segurança especializada.

O ambiente de nível 3 deverá ser dotado, adicionalmente, de Circuito Interno de TV ligado a um sistema local de gravação 24x7. O posicionamento e a capacidade dessas câmeras não deverão permitir a captura de senhas digitadas nos sistemas. As mídias resultantes dessa gravação deverão ser armazenadas por, no mínimo, 1 (um) ano, em ambiente de nível 2.

O ambiente deverá possuir mecanismos que permitam, em caso de falta de energia:

- iluminação de emergência em todos os ambientes, acionada automaticamente;
- continuidade de funcionamento dos sistemas de alarme e do circuito interno de TV.

O sistema de controle de acesso deverá estar baseado em um ambiente de nível 3.

A infra-estrutura do ambiente de nível 3 deverá ser dimensionada com sistemas e dispositivos que garantam o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia devem ser mantidas de forma a atender os requisitos de disponibilidade dos sistemas e seus respectivos serviços. Um sistema de aterramento deverá ser implantado. Todos os cabos elétricos deverão estar protegidos por tubulações ou dutos apropriados. Deverão ser utilizados tubulações, dutos, calhas, quadros e caixas de passagem, distribuição e terminação projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. Deverão ser utilizados dutos separados para os cabos de energia, de telefonia e de dados. Todos os cabos deverão ser catalogados, identificados e periodicamente vistoriados, no mínimo a cada 6 (seis) meses, na busca de evidências de violação ou de outras anormalidades. Deverão ser mantidos atualizados os registros sobre a topologia da rede de cabos. Qualquer modificação nessa rede deverá ser documentada e autorizada previamente. Não deverão ser admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.

O sistema de climatização deverá atender aos requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente. A temperatura dos ambientes atendidos pelo sistema de climatização deverá ser permanentemente monitorada. A capacidade de redundância de toda a estrutura de energia e ar condicionado do ambiente de nível 3 deverá ser garantida por meio de nobreaks e geradores de porte compatível.

O ambiente de nível 3 deve estar instalado em local protegido contra a exposição à água, infiltrações e inundações.

Nas instalações não será permitido fumar ou portar objetos que produzam fogo ou faísca, a partir do nível 2. Deverão existir no interior do ambiente nível 3 extintores de incêndio das classes B e C, para apagar incêndios em combustíveis e equipamentos elétricos, dispostos no ambiente de forma a facilitar o seu acesso e manuseio. Em caso da existência de sistema de sprinklers no prédio, o ambiente de nível 3 não deverá possuir saídas de água, para evitar danos aos equipamentos. O ambiente de nível 3 deve possuir sistema de prevenção contra incêndios, que acione alarmes preventivos uma vez detectada fumaça no ambiente. Nos demais ambientes deverão existir extintores de in-

cêndio para todas as classes de fogo, dispostos em locais que facilitem o seu acesso e manuseio

Mecanismos específicos deverão ser implantados para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos deverão permitir o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos deve acionar imediatamente os alarmes de abertura de portas.

O MRS responsável deverá atender à norma brasileira NBR 11.515/NB 1334 (“Critérios de Segurança Física Relativos ao Armazenamento de Dados”). Todos os documentos em papel que contenham informações classificadas como sensíveis deverão ser triturados antes de ir para o lixo. Todos os dispositivos eletrônicos não mais utilizáveis e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis, deverão ser fisicamente destruídos.

Uma sala de armazenamento externa à instalação técnica principal do MRS deve ser usada para o armazenamento e retenção de cópia de segurança de dados. Essa sala deverá estar disponível a pessoal autorizado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e deverá atender aos requisitos mínimos estabelecidos para um ambiente de nível 2.

Na DPRS devem ser descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na entidade responsável pelo MRS, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, deve também ser estabelecido o número de pessoas requerido para sua execução.

A entidade responsável pela DPRS do MRS deverá garantir a separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize indevidamente o MRS sem ser detectado. As ações de cada empregado deverão estar limitadas de acordo com seu perfil. A entidade responsável pelo MRS deverá estabelecer um mínimo de 3 (três) perfis distintos para sua operação, a saber:

- Administrador do sistema - autorizado a instalar, configurar e manter os sistemas confiáveis para gerenciamento dos serviços providos pelo MRS, bem como administrar a implementação das práticas de segurança;
- Operador de sistema - responsável pela operação diária dos sistemas confiáveis.

Autorizado a realizar backup e recuperação do sistema.

- Auditor de Sistema - autorizado a ver arquivos e auditar os logs dos sistemas confiáveis.

Todos os empregados deverão receber treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso serão determinados, em documento formal, com base nas necessidades de cada perfil. Quando um empregado se desligar do serviço, suas permissões de acesso deverão ser revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa , deverão ser revistas suas permissões de acesso. Deverá existir uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver no ato de seu desligamento.

Todas as tarefas executadas no cofre ou gabinete onde se localizam o MRS deverão requerer a presença de, no mínimo, 2 (dois) empregados com perfis qualificados. As demais tarefas do MRS poderão ser executadas por um único empregado.

A DPRS deve garantir que todo empregado responsável terá sua identidade e perfil verificados antes de:

- ser incluído em uma lista de acesso físico às instalações;
- ser incluído em uma lista para acesso lógico aos sistemas confiáveis.

Os certificados, contas e senhas utilizadas para identificação e autenticação dos empregados deverão:

- ser diretamente atribuídos a um único empregado;
- não ser compartilhados; e
- ser restritos às ações associadas ao perfil para o qual foram criados.

A entidade responsável pelo MRS deverá implementar um padrão de utilização de "senhas fortes", definido na sua PS, juntamente com procedimentos de validação dessas senhas.

Na DPRS devem ser descritos requisitos e procedimentos, implementados pela entidade responsável pelo MRS em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem

profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. A DPRS deve garantir que todos os empregados da entidade responsável pelo MRS, encarregados de tarefas operacionais terão registrado em contrato ou termo de responsabilidade:

- os termos e as condições do perfil que ocuparão;
- o compromisso de observar as normas, políticas e regras aplicáveis da ICP; e
- o compromisso de não divulgar informações sigilosas a que tenham acesso.

Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da entidade responsável pelo MRS envolvido em atividades diretamente relacionadas com os processos dos serviços providos pelo MRS deverá ser submetido a:

- verificação de antecedentes criminais;
- verificação de situação de crédito;
- verificação de histórico de empregos anteriores; e
- comprovação de escolaridade e de residência.

A entidade responsável pelo MRS poderá definir requisitos adicionais para a verificação de antecedentes.

Todo o pessoal da entidade responsável pelo MRS envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverão receber treinamento documentado, suficiente para o domínio dos seguintes temas: PERGUNTAR

- princípios e tecnologias dos serviços providos pelo MRS;
- ICP;
- princípios e tecnologias de certificação digital e de assinaturas eletrônicas;
- princípios e mecanismos de segurança de redes e segurança;
- procedimentos de recuperação de desastres e de continuidade do negócio;

- familiaridade com procedimentos de segurança, para pessoas com responsabilidade de Oficial de Segurança;
- familiaridade com procedimentos de auditorias em sistemas de informática, para pessoas com responsabilidade de Auditores de Sistema;
- outros assuntos relativos a atividades sob sua responsabilidade.

Todo o pessoal da entidade responsável pelo MRS envolvido em atividades diretamente relacionadas com os processos dos serviços providos pelo MRS deverá ser mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas do MRS.

A DPRS pode definir uma política a ser adotada pela entidade responsável pelo MRS para o rodízio de pessoal entre os diversos cargos e perfis por elas estabelecidos.

A DPRS deve prever que na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da entidade responsável pelo MRS, deverá, de imediato, suspender o acesso dessa pessoa ao MRS, instaurar processo administrativo para apurar os fatos e, se for o caso, adotar as medidas legais cabíveis. O processo administrativo referido deverá conter, no mínimo, os seguintes items:

- relato da ocorrência com *modus operandis*;
- identificação dos envolvidos;
- eventuais prejuízos causados;
- punições aplicadas, se for o caso; e
- conclusões.

Concluído o processo administrativo, a entidade responsável pelo MRS deverá encaminhar suas conclusões à AC-Raiz. As punições passíveis de aplicação, em decorrência de processo administrativo, são:

- advertência;
- suspensão por prazo determinado; ou

- impedimento definitivo de exercer funções no âmbito da ICP.

A DPRS deve garantir que a entidade responsável pelo MRS tornará disponível para todo o seu pessoal, pelo menos:

- sua DPRS;
- as PRS que implementa;
- documentação operacional relativa à suas atividades; e
- contratos, normas e políticas relevantes para suas atividades.

Toda a documentação fornecida ao pessoal deverá estar classificada segundo a política de classificação de informação definida pela entidade responsável pelo MRS e deverá ser mantida atualizada.

5.4.5.2 Procedimentos de Auditoria

A entidade responsável pela DPRS do MRS deverá registrar em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema. Entre outros, os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria:

- iniciação e desligamento do MRS;
- tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores do MRS;
- mudanças na configuração do MRS ou nas suas chaves;
- tentativas de acesso (login) e de saída do sistema (logoff);
- tentativas não-autorizadas de acesso aos arquivos de sistema;
- geração de chaves próprias do MRS e demais eventos relacionados com o ciclo de vida destes certificados;
- operações falhas de escrita ou leitura, quando aplicável; e

- todos os eventos relacionados à sincronização dos relógios do MRS com a FCT; isso inclui no mínimo:
  - a própria sincronização;
  - desvio de tempo ou retardo de propagação acima de um valor especificado;
  - falta de sinal de sincronização;
  - tentativas de autenticação mal-sucedidas;
  - detecção da perda de sincronização.

A entidade responsável pela DPRS do MRS deverá também registrar, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema, tais como:

- registros de acessos físicos;
- manutenção e mudanças na configuração de seus sistemas;
- mudanças de pessoal e de perfis qualificados;
- relatórios de discrepância e comprometimento; e
- registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

A DPRS deve especificar todas as informações que deverão ser registradas pela entidade responsável do MRS. Deve prever que todos os registros de auditoria deverão conter a identidade do agente que o causou, bem como a data e horário do evento. Registros de auditoria eletrônicos deverão conter o horário UTC. Registros manuais em papel poderão conter a hora local desde que especificado o local, senão deve conter a hora UTC. Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços do MRS deverá ser armazenada, eletrônica ou manualmente, em local único.

A DPRS deve estabelecer a periodicidade, não superior a uma semana, com que os registros de auditoria da entidade responsável pelo MRS serão analisados pelo seu pessoal operacional. Todos os eventos significativos deverão ser explicados em relatório de auditoria de registros. Tal análise deverá envolver uma inspeção breve de

todos os registros, com a verificação de que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise deverão ser documentadas.

A DPRS deve estabelecer que a entidade responsável pelo MRS mantenha localmente os seus registros de auditoria por pelo menos 2 (dois) meses.

A DPRS deve descrever os mecanismos obrigatórios incluídos no sistema de registro de eventos da entidade responsável pelo MRS para proteger os seus registros de auditoria contra leitura não autorizada, modificação e remoção. Também devem ser descritos os mecanismos obrigatórios de proteção de informações manuais de auditoria contra a leitura não autorizada, modificação e remoção.

Na DPRS devem ser descritos os procedimentos adotados pela entidade responsável do MRS para gerar cópias de segurança (backup) de seus registros de auditoria e a sua periodicidade, que não deve ser superior a uma semana.

Na DPRS devem ser descritos e localizados os recursos utilizados pela entidade responsável do MRS para a coleta de dados de auditoria.

A DPRS deve assegurar que os eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da entidade responsável do MRS, serão analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes deverão ser implementadas pela entidade responsável pelo MRS e registradas para fins de auditoria.

Na DPRS deve estabelecer os períodos de retenção para cada registro arquivado, inclusive arquivos de auditoria, deverão ser retidos por, no mínimo, 6 (seis) anos. A DPRS deve estabelecer que todos os registros arquivados devem ser classificados e armazenados com requisitos de segurança compatíveis com essa classificação.

A DPRS deve estabelecer que uma segunda cópia de todo o material arquivado deverá ser armazenada em local externo às instalações principais da entidade responsável do MRS, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal. As cópias de segurança deverão seguir os períodos de retenção definidos para os registros dos quais são cópias. A entidade responsável pela DPRS do MRS deverá verificar a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

Na DPRS deve estabelecer os formatos e padrões de data e hora contidos em cada tipo de registro.

Na DPRS devem ser descritos e localizados os recursos de coleta de dados de arquivo utilizados pela entidade responsável do MRS.

Na DPRS devem ser detalhadamente descritos os procedimentos definidos pela entidade responsável do MRS para a obtenção ou a verificação de suas informações de arquivo.

Na DPRS deve descrever os procedimentos técnicos e operacionais que serão usados pelo MRS responsável para garantir que um novo par de chaves será gerado e instalado em algum serviço provido pelo MRS quando o ciclo de vida do par de chaves que estiver em utilização chegar ao fim. A geração de um novo par de chaves e instalação do respectivo certificado no MRS deve ser realizada somente por funcionários com perfis qualificados, através de duplo controle, em ambiente físico seguro.

O MRS deve assegurar, no caso de comprometimento de sua operação por qualquer um dos motivos relacionados abaixo, que as informações relevantes sejam disponibilizadas aos subscritores e às terceiras partes. O MRS deve disponibilizar a todos os subscritores e terceiras partes uma descrição do comprometimento ocorrido. No caso de comprometimento de uma operação de algum serviço disponibilizado pelo MRS (por exemplo, comprometimento da chave privada), suspeita de comprometimento ou perda de calibração, o MRS não deverá deixar funcionar os serviços até que sejam tomadas medidas para recuperação do comprometimento. Em caso de comprometimento grave da operação do MRS, sempre que possível, ela deve disponibilizar a todos os subscritores e terceiras partes informações que possam ser utilizadas, a não ser que isso viole a privacidade dos subscritores ou comprometa a segurança dos serviços do MRS.

Na DPRS devem ser descritos os procedimentos de recuperação utilizados pela entidade responsável do MRS quando recursos computacionais, software ou dados estiverem corrompidos ou houver suspeita de corrupção.

Na DPRS devem ser descritos os procedimentos de recuperação utilizados na circunstância de revogação do certificado de algum serviço provido do MRS responsável.

Na DPRS devem ser descritos os procedimentos de recuperação utilizados na circunstância de comprometimento da chave privada de algum serviço provido pelo MRS.

Na DPRS deve descrever os procedimentos de recuperação previstos pelo MRS para utilização nas hipóteses de perda de calibração e de sincronismo do MRS.

Na DPRS devem ser descritos os procedimentos de recuperação utilizados pela entidade responsável do MRS após a ocorrência de um desastre natural ou de outra natureza, antes do restabelecimento de um ambiente seguro.

A entidade responsável pelo MRS deve assegurar que possíveis rompimentos com os subscritores e terceiras partes, em conseqüência da cessação dos serviços providos pelo MRS sejam minimizados e, em particular, assegurar a manutenção continuada da informação necessária. Antes de o MRS cessar seus serviços os seguintes procedimentos serão executados, no mínimo:

- a entidade responsável pelo MRS disponibilizará a todos os subscritores e partes receptoras informações a respeito de sua extinção;
- a entidade responsável pelo MRS transferirá a outra entidade, após aprovação da AC-Raiz, as obrigações relativas à manutenção de arquivos de registro e de auditoria necessários para demonstrar a operação correta do MRS, por um período razoável;
- a entidade responsável pelo MRS manterá ou transferirá a outro entidade, após aprovação da AC-Raiz, suas obrigações relativas a disponibilizar sua chave pública ou seus certificados a terceiras partes, por um período razoável;
- as chaves privadas dos serviços providos pelo MRS serão destruídas de forma que não possam ser recuperadas;
- a entidade responsável pelo MRS solicitará a revogação dos certificados de seus serviços;
- a entidade responsável pelo MRS notificará todas as entidades afetadas.

A entidade responsável pelo MRS providenciará os meios para cobrir os custos de cumprimento destes requisitos mínimos no caso de falência ou se por outros motivos se ver incapaz de arcar com os seus custos.

5.4.6 Controles Técnicos de Segurança

Na DPRS devem ser descritos os controles relativos à segurança da rede da entidade responsável pelo MRS, incluindo firewalls e recursos similares. Todos os

servidores e elementos de infra-estrutura e proteção de rede, tais como roteadores, hubs, switches, firewalls e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda o MRS, deverão estar localizados e operar em ambiente de, no mínimo, nível 3. As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (patches), disponibilizadas pelos respectivos fabricantes deverão ser implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação. O acesso lógico aos elementos de infra-estrutura e proteção de rede deverá ser restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas deverão implementar filtros de pacotes de dados, que permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

Mecanismos de firewall deverão ser implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Os firewalls deverão ser dispostos e configurados de forma a promover o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo - a conhecida "zona desmilitarizada"(DMZ) - em relação aos equipamentos com acesso exclusivamente interno. O software de firewall, entre outras características, deverá implementar registros de auditoria. O Oficial de Segurança deve verificar periodicamente as regras dos firewalls, para assegurar-se que apenas o acesso aos serviços realmente necessários é permitido e que está bloqueado o acesso a portas desnecessárias ou não utilizadas.

O sistema de detecção de intrusão deverá ter capacidade de ser configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar traps SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta ao firewall ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do firewall. O sistema de detecção de intrusão deverá ter capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento. O sistema de detecção de intrusão deverá prover o registro dos eventos em logs, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

As tentativas de acesso não autorizado - em roteadores, firewalls ou IDS - deverão ser registradas em arquivos para posterior análise, que poderá ser automatizada.

A freqüência de exame dos arquivos de registro deverá ser, no mínimo, semanal e todas as ações tomadas em decorrência desse exame deverão ser documentadas.

As estações de trabalho e servidores devem estar dotadas de antivirus, antispyware e de outras ferramentas de proteção contra ameaças provindas da rede a que estão ligadas.

5.4.7 Perfis de Certificados, LCR e OCSP

Deve apresentar os perfis dos certificados dos serviços providos pelo MRS, o perfil da lista de certificados revogados e de OSCP.

5.4.8 Fiscalização e Auditoria de Conformidade

As fiscalizações e auditorias realizadas nos MRS da ICP têm por objetivo verificar se seus processos, procedimentos e atividades estão em conformidade com suas respectivas DPRS, PRS e demais normas e procedimentos estabelecidos pela ICP. As fiscalizações dos MRS da ICP são realizadas pela AC-Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio.

A entidade responsável pelo MRS deve informar que recebeu auditoria prévia da AC-Raiz para fins de credenciamento na ICP e que é auditada anualmente, para fins de manutenção do credenciamento.

5.5 Conclusão

A integração do MRS numa ICP, deve ser regida por uma política de uso e por uma declaração de práticas de uso que são descritas em documentos. Este capítulo definiu esses documentos.

Capítulo 6

Discussão

6.1 Introdução

Este trabalho propôs o uso de um hardware criptográfico para a gestão de relógio e que provesse serviços que utilizam o tempo como base para funcionamento. Foi proposto também, um conjunto de documentos, para normalizar o uso do Módulo de Relógio Seguro numa ICP.

Nesse capítulo é visto o impacto do MRS sobre o que existe na literatura, como a gestão segura do relógio, os serviços de carimbo de tempo, de hora e de liberação de chave no futuro. E também o impacto que a nova infra-estrutura proposta terá sobre a ICP.

6.2 Pontos

Como visto no Capítulo 3, os componentes de uma ICP são formados por dois elementos, um servidor e um HSM. Normalmente, a aplicação monta no servidor a estrutura de dados contendo a informação temporal a ser utilizada. Isso ocorre porque o HSM, na sua maioria, não possui um relógio. E quando possui, apresenta um custo elevado e um procedimento especial para garantir o sincronismo do tempo.

O relógio do servidor, não possui um esquema de proteção ao seu relógio. Ficando vulnerável a ataques que podem manipular a hora do relógio, deixando de ser uma fonte confiável de tempo. Toda informação temporal utilizada nos serviços providos por uma ICP, deve ser provida por uma fonte de tempo confiável e segura.

A utilização de um relógio atômico como FCT tem um custo elevado numa ICP, pois cada componente da ICP deveria ter seu próprio relógio, tornando sua adoção inviável. O Módulo de Relógio Seguro atua como uma fonte de tempo confiável e segura. Pois possui mecanismos que garantem a confiabilidade e a segurança de seu relógio. Mecanismos como a gestão segura vista na Seção 4.8 e o uso de um hardware criptográfico como visto na Seção 4.9.

O MRS, no sincronismo de seu relógio, utiliza o protocolo NTP para sincronizar com servidores stratum 1, com certificados digitais para autenticação, como fontes de tempo. Além de utilizar o protocolo NTP, a Seção 4.6 mostra que pode ser utilizado também relógio atômico e sinal GPS. As soluções encontradas no mercado que possuem sincronismo seguro de relógio, são destinadas a serviços de carimbo de tempo e sua sincronização é limitada a um sistema de auditoria e sincronismo (SAS) provido pelo fabricante do serviço de carimbo de tempo.

O MRS provê serviços temporais, que agregado a sincronização segura do relógio, assegura que o serviço utilize sempre a hora correta.

A temporalidade dos documentos eletrônicos é garantida pelo carimbo de tempo. O serviço de carimbo de tempo, segue o padrão da RFC3161 [18] e é executado dentro do perímetro criptográfico do MRS. Não é possível comparar a estrutura do serviço com os existentes no mercado, pois são como “caixas-pretas", não se tem acesso ao interior. Mas o funcionamento do serviço é praticamente o mesmo, já que todos são baseados na RFC3161. Além disso, para o serviço de carimbo de tempo, não será necessário a utilização de um SAS, como é necessário para os produtos de carimbo de tempo que existem no mercado. Pois o próprio MRS irá fornecer o tempo correto para a emissão de carimbos de tempo.

O serviço de sincronismo de tempo faz uso do relógio do MRS para prover a hora a outras aplicações e computadores. O uso desse servidor faz-se de modo seguro, já que o servidor roda dentro do perímetro criptográfico e aceita conexões seguras com certificados pertencentes a ICP ao qual faz parte. Desse modo, o MRS pode ser considerado uma fonte confiável de tempo. Os servidores de hora disponíveis hoje que funcionam como stratum 1, e são considerados fonte confiável de tempo, são computadores ligados diretamente a relógios atômicos. Esses computadores normalmente não são de uso público, são de uso restrito. O acesso é feito somente por computadores de

stratum 2, que são considerados servidores públicos. Como esses computadores não são protegidos por um *hardware criptográfico* e não possuem uma gestão segura do relógio, se tornam vulneráveis a ataques físicos e lógicos.

O serviço de liberação de chave no futuro, conhecido também como criptografia temporal é baseado na utilização de criptografia assimétrica, que é proposto por Custódio [10]. Com a utilização de criptografia assimétrica, é possível identificar a chave que será usada para a cifragem da informação se ela realmente pertence a entidade responsável pelo MRS. Desse modo, é garantido que a informação se manterá em sigilo pelo período estipulado.

Normalmente uma ICP não provê uma fonte de tempo confiável para todos os componentes que formam a ICP. Um serviço de carimbo de tempo, geralmente, é o único componente que utiliza uma fonte de tempo confiável. O problema, é que essa fonte de tempo do carimbo de tempo, é exclusiva para o carimbo de tempo. Não sendo possível utiliza-la para nenhum outro componente. Isso porque, os serviços de carimbo de tempo existentes no mercado são fechados e proprietários. Isso encarece o produto e o torna muito específico.

A utilização do MRS vem a suprir as necessidades de uma ICP em relação ao tempo. Os componentes poderão utilizar o MRS como uma FCT, e utilizando autenticação com certificados digitais pertencentes a ICP, terão uma confiança maior nessa fonte. O MRS tem um custo baixissímo, se comparado a um relógio atômico.

A utilização de relógio atômico em cada componente da ICP, que irá prover a hora correta, tem um custo elevado, já que seria necessário vários relógios atômicos para atender as necessidades de uma ICP. Com a utilização do MRS, cada MRS pode atender vários componentes reduzindo os custos em uma ICP.

6.3 Conclusão

Esse capítulo abordou a introdução do MRS numa ICP, comparando-o com o que existe no mercado. Também mostrou que sua utilização numa ICP reduzirá os custos com fontes confiáveis de tempo como relógios atômicos.

Capítulo 7

Considerações Finais

Os relógios utilizados nos equipamentos dos componentes que formam uma ICP não possuem um regulamentação clara no que diz respeito a sua forma de sincronização do tempo, nem sua exatidão em relação ao horário UTC.

Foi realizado um estudo para se conhecer onde existe relógio nos componentes que formam uma ICP, e como eles são utilizados. A sincronização desses relógios, entre si e com uma fonte confiável de tempo, é precária. Percebeu-se que o relógio é parte fundamental de uma ICP, mas não é confiável.

O relógio, como parte de uma ICP, propicia a ICP atender a temporalidade em documentos digitais com serviços de relógio.

Este trabalho tem como maior contribuição uma solução para a integração, em um *hardware criptográfico*, dos serviços de relógio no contexto de uma ICP. O nome dessa solução é Módulo de Relógio Seguro e provê serviços de relógio como a Autoridade de Carimbo de Tempo, Sincronização de Relógio e Autoridade Certificadora Temporal. Além disso o MRS realiza uma gestão segura do relógio, o que o torna uma fonte confiável de tempo.

A utilização de um *hardware criptográfico* fechado e muito específico, além de não prover todas as funcionalidades que se deseja para uma ICP, se torna caro pelo custos envolvidos desde a sua compra até eventuais suportes que se façam necessários. O uso de uma plataforma criptográfica aberta, além de ter um custo reduzido, pode ser implementado para suprir as necessidades de uma ICP.

O presente trabalho apresentou diversas contribuições, atingindo seus objetivos geral e específicos, os quais são listados abaixo:

- foi analisado os usos e aplicações dos relógios que compõem um ICP. Como cada componente utiliza o relógio e onde utiliza;
- foi levantado como os relógios são sincronizados entre si e com uma fonte confiável de tempo;
- foram listados os serviços de relógio que são providos por uma ICP;
- foram analisados a qualidade dos relógios utilizados em HSMs;
- foi proposto a integração dos serviços de relógio em um único módulo de hardware criptográfico;
- foi proposto uma gestão segura do relógio com a finalidade de garantir que o relógio seja considerado confiável;
- foram definidos os requisitos de exatidão, precisão e estabilidade dos relógios no contexto de uma ICP;
- foram definidos os documentos, os de políticas de uso, de declaração de práticas, e de auditoria, para uso do Módulo de Relógio Seguro numa ICP;
- foi discutido o impacto da inclusão deste sistema sobre uma ICP.

Normalmente uma ICP não conta com uma fonte confiável de tempo para uso nos componentes que formam uma ICP. A utilização do MRS como âncora confiável na ICP, propicia uma confiança no tempo, nos serviços providos pelos componentes que formam uma ICP.

Além de ser utilizado em ICP, o MRS pode ser utilizado, em empresas e universidades, como âncora confiável de tempo para seus sistemas, provendo a hora e a temporalidade em documentos digitais internos.

7.1 Trabalhos Futuros

O hardware criptográfico utilizado no protótipo, o ASI HSM, possui um relógio com uma resolução de 10 ms. Essa resolução pode ser aumentada, realizando uma interpolação com os sensores disponíveis no hsm e conseguir uma resolução na casa de μs ou até mesmo na casa de ηs.

O MRS poderia integrar um relógio com uma instabilidade menor com o passar do tempo. Para isso, poderia ser utilizado um relógio atômico integrado no MRS.

As interfaces de configuração dos serviços de tempo providos pelo MRS, não estão integradas. Poderia se ter uma integração dessas interfaces, tornando a administração do MRS seja mais fácil.

O serviço de carimbo de tempo, possui uma especificação de seu protocolo, definido na RFC-3161 [18]. O serviço de sincronismo de tempo, possui seu protocolo de funcionamento especificado nos rascunhos da definição do *network time protocol* versão 4 [23]. Entretanto, o serviço de certificados temporais não possui um protocolo para a emissão de certificados temporais. Como trabalho futuro, poderia ser especificado e formalizado um protocolo para emissão dos certificados temporais.

Outro protocolo que pode ser especificado também, é do processo de auditoria para o MRS como um todo.

E finalizando, o desenvolvimento do MRS na forma de um *appliance*.

Referências

[1] ALLAN, D. W.; ASHBY, N.; HODGE, C. C. *The Science of Timekeeping - Application Note 1289*. [S.l.], 1997.

[2] BRY Tecnologia. Junho 2008. Www.bry.com.br. Disponível em: <www.bry.com.br>.

[3] MARTINA, J. E. *Projeto de um Provedor de Serviços Criptográficos Embarcado para Infraestrutura de Chaves Públicas e suas Aplicações*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2005.

[4] HABER, S.; STORNETTA, W. S. How to time-stamp a digital document. In: *CRYPTO '90: Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology*. London, UK: Springer-Verlag, 1991. p. 437–455. ISBN 3-540-54508-5.

[5] BAYER, D.; HABER, S.; STORNETTA, W. S. *Improving the efficiency and reliability of digital timestamping*. 1993. Proceedings Sequences II: Methods in Communication, Security, and Computer Science,.

[6] MILLS, D. L. *A distributed-protocol authentication scheme*. April 1987. Network Working Group Report RFC-1004.

[7] MILLS, D. L. *Network Time Protocol (Version 1) specification and implementation.* July 1988. Network Working Group Report RFC-1059.

[8] MAY, T. C. *Timed-release crypto*. fev. 1993. http://www.hks.net/cpunks/cpunks-0/1460.html.

[9] RIVEST, R. L.; SHAMIR, A.; WAGNER, D. A. *Time-lock Puzzles and Timed-release Crypto*. [S.l.], fev. 1996. 21 p. Disponível em: <ftp://ftp-pubs.lcs.mit.edu/pub/lcs-pubs/tr.outbox/MIT-LCS-TR-684.ps.gz>.

[10] CUSTODIO, R. F. et al. Temporal key release infrastructure. In: PUBLICATION, N. T. (Ed.). *6th Annual PKI R&D Workshop*. [S.l.: s.n.], 2007.

[11] CGPM. *The Internacional System of Units*. [S.l.]: BIPM, 2006.

[12] STANDARDS, N. I. O.; NIST, T. *Frequency Measurement and Analysis System: Operator Manual*. NIST. Disponível em: <http://tf.nist.gov/timefreq/service/fms.htm>.

[13] INTERNATIONAL Vocabulary of Basic and General Terms in Metrology. second. [S.l.]: International Organization for Standardization ISO, 1993.

[14] INMETRO, I. N. de Metrologia Normalização e Q. I. *Orientações sobre Calibração e Rastreabilidade das Medições em Laboratórios de Calibrações e de Ensaio - DOQ-CGCRE-003*. Novembro 2003.

[15] MÜLLER, R. *ISO/IEC 18014-1: Information Technology - Security Techniques - Time Stamping Services - Part 1: Framework*. Norma Estabelecendo Time Stamping Services.

[16] JUST, M. K. *On the Temporal Authentication of Digital Data*. Tese (Doutorado) — School of Computer Science - Carleton University, Dezembro 1998.

[17] ROOS, M. *Integrating Time-Stamping and Notarization*. Dissertação (Mestrado) — University of Tartu - Estonia, 1999.

[18] ADAMS, C. et al. *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*. IETF, ago. 2001. RFC 3161 (Proposed Standard). (Request for Comments, 3161). Disponível em: <http://www.ietf.org/rfc/rfc3161.txt>.

[19] INFORMAÇÃO, I. de Tecnologia da. *VISÃO GERAL DO SISTEMA DE CARIMBOS DO TEMPO NA ICP-BRASIL.* Dezembro 2007. Www.iti.gov.br.

[20] INFORMAÇÃO, I. de Tecnologia da. *REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL.* Dezembro 2007. Www.iti.gov.br.

[21] INFORMAÇÃO, I. de Tecnologia da. *REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO DA ICP-BRASIL*. Dezembro 2007. Www.iti.gov.br.

[22] INFORMAÇÃO, I. de Tecnologia da. *PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL*. Dezembro 2007. Www.iti.gov.br.

[23] MILLS, D. L. *Network Time Protocol project*. 2007. Http://www.ntp.org. Disponível em: <http www.ntp.orgdownloads.html>.

[24] MILLS D., D. P.; MONTGOMERY, J. *Simple network time protocol (SNTP) version 4 for IPv4, IPv6 and OSI*. [S.l.], 2005.

[25] MILLS, D. *Network Time Protocol Version 4 Reference and Implementation Guide*. [S.l.], 2006.

[26] CHAN, A. C.-F.; BLAKE, I. F. Scalable, server-passive, user-anonymous timed release cryptography. In: *ICDCS*. IEEE Computer Society, 2005. p. 504–513. ISBN 0-7695-2331-5. Disponível em: <http://doi.ieeecomputersociety.org/10.1109/ICDCS.2005.72>.

[27] WWW.LABSEC.UFSC.BR. *Laboratório de Segurança em Computação*. Universidade Feredal de Santa Catarina.

[28] WWW.VERISIGN.COM. *VeriSign Inc.*

[29] INFORMAÇÃO, I. de Tecnologia da. *Infra-estrutura de Chaves Públicas Brasileira*.

[30] NCIPHER nShield. Http://www.ncipher.com/en/Products/Hardware%20Security%20Modules/nShield.aspx.

[31] STANDARDS, N. I. of; TECHNOLOGY. *FIPS 140-2 Security Requirements for Cryptographic Modules*. Http://csrc.nist.gov/groups/STM/cmvp/standards.html.

[32] STANDARDIZATION, I. O. for. *Evaluation criteria for IT security - Part 1: Introduction and general model*. ISO/IEC 15408-3:1999 Information tecnology - Security techniques.

[33] STANDARDIZATION, I. O. for. *Evaluation criteria for IT security - Part 2: Security functional requirements*. ISO/IEC 15408-3:1999 Information tecnology - Security techniques.

[34] STANDARDIZATION, I. O. for. *Evaluation criteria for IT security - Part 3: Security assurance requirements*. ISO/IEC 15408-3:1999 Information tecnology - Security techniques.

[35] LABSEC. *Serviço de Carimbo de Tempo*. Https://projetos.labsec.ufsc.br/carimbo-tempo.

[36] LIBCRYPTOSEC. Https://projetos.labsec.ufsc.br/libcryptosec.

[37] WWW.PHP.NET. *PHP.net*.

[38] LIBCRYPTOSEC https://projetos.labsec.ufsc.br/php5. *Módulo em PHP da libcryptosec*.

[39] FREEBSD. *6.2 Stable*. Http://www.freebsd.org.

[40] CHOKHANI, S. et al. *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. IETF, nov. 2003. RFC 3647 (Informational). (Request for Comments, 3647). Disponível em: <http://www.ietf.org/rfc/rfc3647.txt>.

[41] PINKAS, D.; POPE, N.; ROSS, J. *Policy Requirements for Time-Stamping Authorities (TSAs)*. IETF, nov. 2003. RFC 3628 (Informational). (Request for Comments, 3628). Disponível em: <http://www.ietf.org/rfc/rfc3628.txt>.

Apêndice

Apêndice A

Análise do relógio dos HSMS

A.1 Análise do experimento 1 no PSO PL50 sem realizar operações criptográficas

Para o HSM PSO PL50 foi utilizado o relógio do sistema operacional como FCT, pois esse foi mantido sincronizado via NTP com 3 servidores NTP stratum 2. Para cada medida da calibração entre os relógios do HSM e da FCT, foram coletados a hora do HSM, a hora da FCT, as tensões de alimentação do computador, a temperatura da CPU do computador e a temperatura da placa-mãe do computador. O intervalo entre as medições foi de 1 segundo. Esse HSM não possui sensores de tensões de alimentação e temperatura, por isso foram coletados da placa-mãe onde o HSM está ligado.

A Tabela A.1 apresenta uma parte das medidas realizadas onde o HSM não está realizando operações criptográficas.

Tabela A.1: Dados das medidas realizadas e o PSO PL50 não realizando operações criptográficas

Tempo	Relógio (m:s,ms)		Tensão					Temperatura	
	HSM	FCT	+3v	+5V	-5v	+12v	-12v	CPU	MB
0	9:20,216	9:19,676	3,28	5,06	-5,54	12,08	-12,13	37	26
1	9:21,231	9:20,690	3,28	5,06	-5,54	12,08	-12,13	37	26
2	9:22,242	9:21,701	3,28	5,06	-5,54	12,05	-12,13	37	26
3	9:23,251	9:22,711	3,28	5,06	-5,54	12,05	-12,13	37	26
...									
227095	49:58,679	50:12,888	3,28	5,02	-5.61	12,16	-12,13	36	25.5

Foram gerados gráficos para possibilitar a análise. A Figura A.1 mostra que com o passar do tempo, o deslocamento entre o relógio do HSM e o relógio da FCT aumenta. Esse aumento representa, numa análise de regressão linear, um coeficiente β de 6,48 $\times$ 10^{-5}.

Esse coeficiente indica a inclinação na reta.

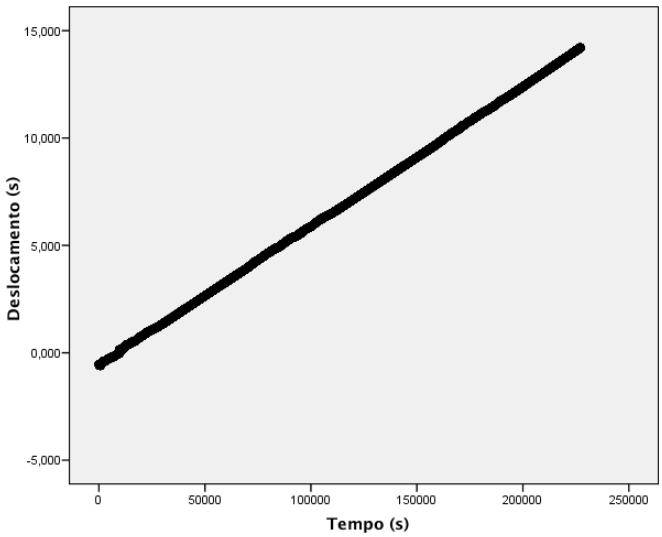


Figura A.1: Deslocamento entre o relógio do HSM e da FCT

Da Tabela A.1 separou-se as medidas de tensão de alimentação +3v em grupos com o mesmo valor de tensão. A Figura A.2 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +3V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

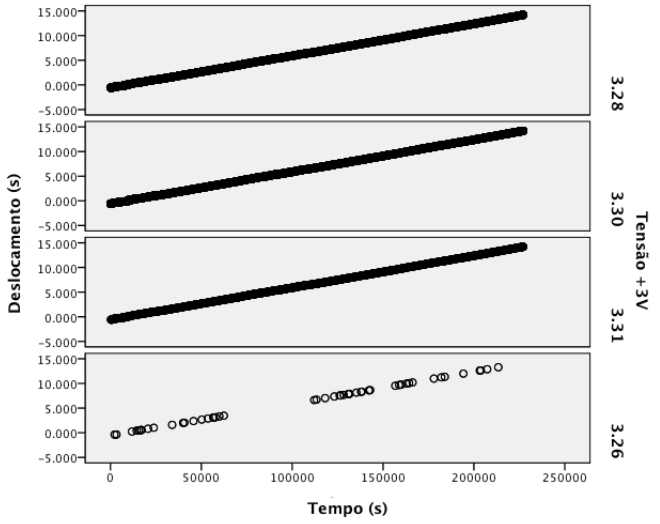
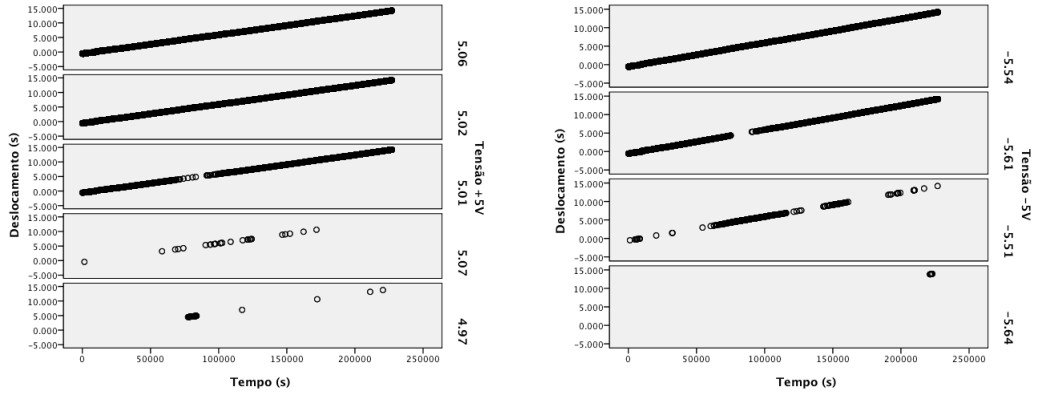


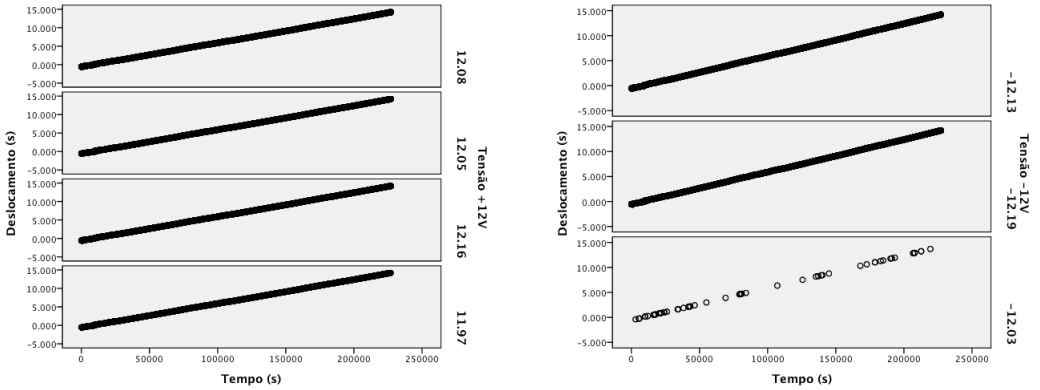
Figura A.2: Deslocamento entre o relógio do HSM e da FCT na tensão de +3V

Da Tabela A.1 separou-se as medidas de tensão de alimentação +5V e -5v em grupos com o mesmo valor de tensão. A Figura A.3(a) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +5V. A Figura A.3(b) mostra o



(a) Tensão +5V (b) Tensão -5V

Figura A.3: Deslocamento entre o relógio do HSM e da FCT nas tensões de +5V e -5V



(a) Tensão +12V (b) Tensão -12V

Figura A.4: Deslocamento entre o relógio do HSM e da FCT nas tensões de +12V e -12V

deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em -5V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Da Tabela A.1 separou-se as medidas de tensão de alimentação +12V e -12v em grupos com o mesmo valor de tensão. A Figura A.4(a) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +12V. A Figura A.4(b) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em -12V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Da Tabela A.1 separou-se as medidas de temperatura da CPU do computador em grupos com o mesmo valor de temperatura. A Figura A.5 mostra o deslocamento entre o

relógio do HSM e o relógio da FCT para as oscilações de temperatura da CPU do computador. Como pode ser visto, essas oscilações na temperatura não afetam a estabilidade do relógio. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

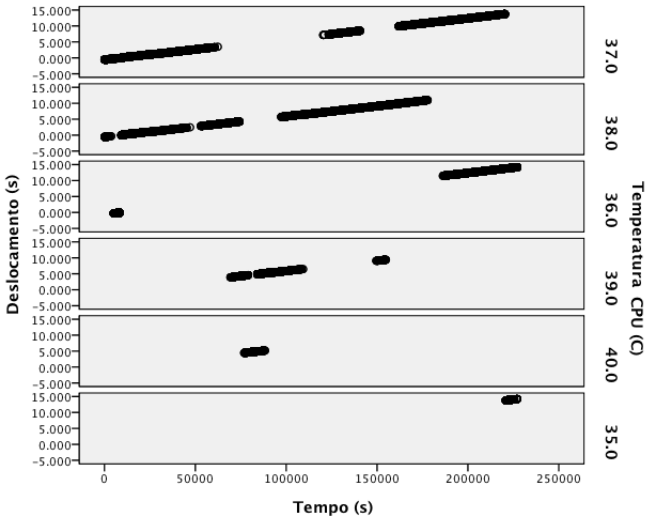


Figura A.5: Deslocamento entre o relógio do HSM e da FCT na temperatura da CPU

Da Tabela A.1 separou-se as medidas de temperatura da placa-mãe do computador em grupos com o mesmo valor de temperatura. A Figura A.6 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de temperatura da placa-mãe do computador. Como pode ser visto, essas oscilações na temperatura não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

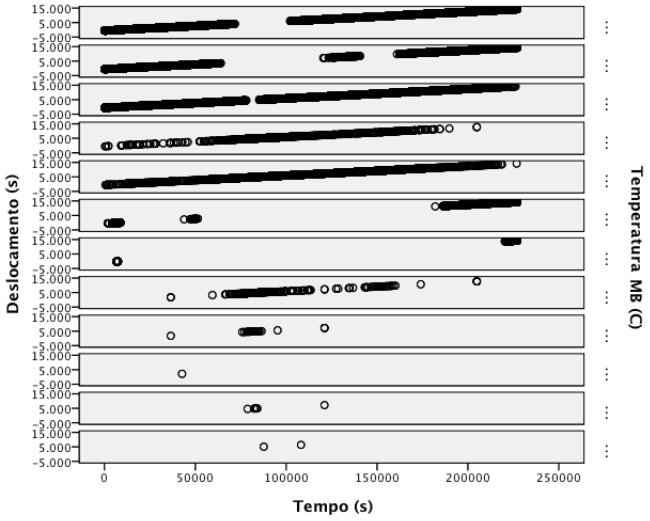


Figura A.6: Deslocamento entre o relógio do HSM e da FCT na temperatura da placa mãe

Em nenhum dos casos acima o relógio do HSM sofreu qualquer influência

quando se variou as tensões de alimentação e temperaturas. Isso quer dizer que o relógio não sofre atrasos nem adiantamentos com pequenas variações de temperatura e tensão que ocorrem no dia a dia.

A.2 Análise do experimento 1 no PSO PL50 realizando operações criptográficas

A Tabela A.2 apresenta uma parte das medidas realizadas onde o HSM PSO PL50 está realizando operações criptográficas.

Tabela A.2: Dados das medidas realizadas e o PSO PL50 realizando operações criptográficas

Tempo	Relógio (s,ms)		Tensão					Temperatura	
	HSM	FCT	+3v	+5V	-5v	+12v	-12v	CPU	MB
0	50,002	49,754	3,28	5,02	-5,61	12,08	-12,13	37	32
1	51,032	50,784	3,28	5,02	-5,61	12,08	-12,13	37	32
2	52,062	51,814	3,30	5,06	-5,61	12,08	-12,13	37	32,5
3	53,106	52,858	3,30	5,06	-5,61	12,08	-12,13	37	32,5
...									
72627	23,463	27,283	3,30	5,06	-5.51	12,05	-12,13	43	45

Foram gerados gráficos para possibilitar a análise. A Figura A.7 mostra que com o passar do tempo, o deslocamento entre o relógio do HSM e o relógio da FCT aumenta. Esse aumento representa, numa análise de regressão linear, um coeficiente β de 5,57 $\times$ 10^{-5}. Esse coeficiente indica a inclinação na reta.

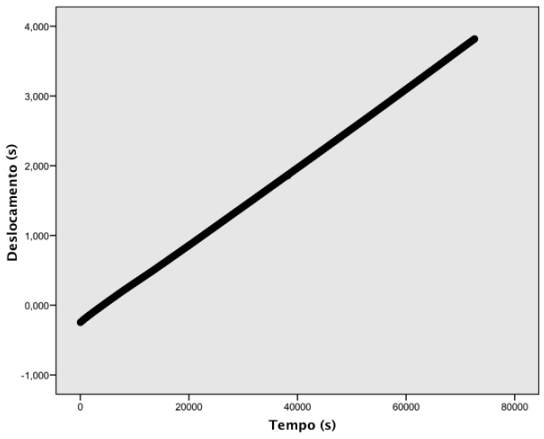


Figura A.7: Deslocamento entre o relógio do HSM e da FCT

Da Tabela A.2 separou-se as medidas de tensão de alimentação +3v em grupos com o mesmo valor de tensão. A Figura A.8 mostra o deslocamento entre o relógio do HSM e

o relógio da FCT para as oscilações de tensão em +3V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

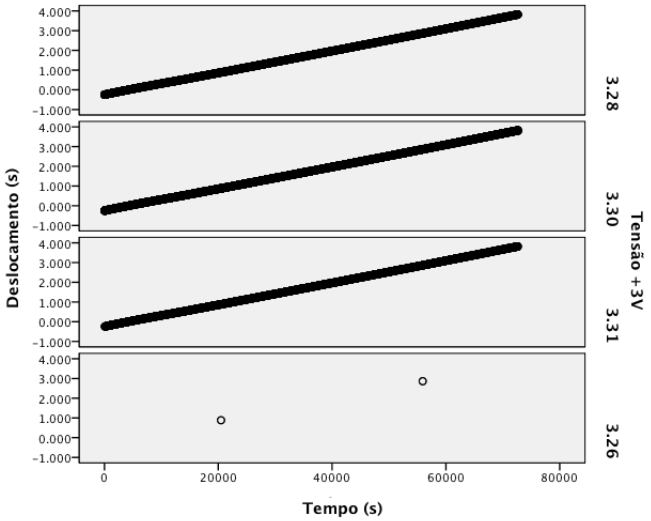
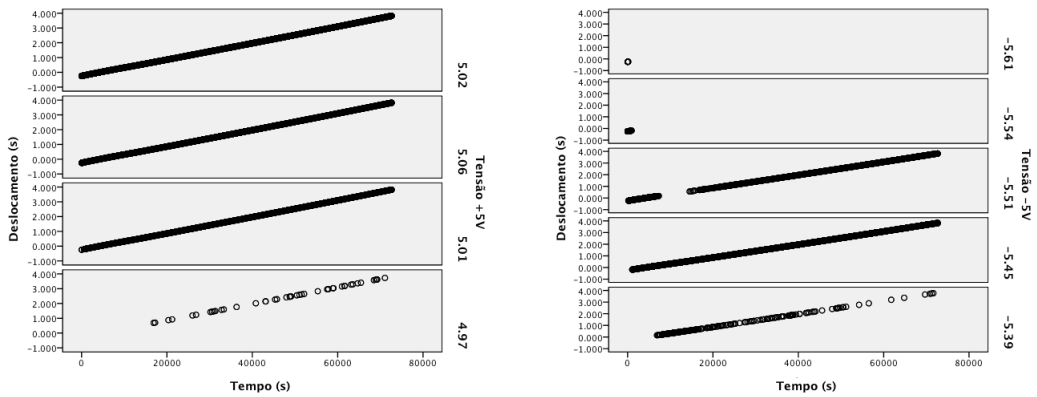


Figura A.8: Deslocamento entre o relógio do HSM e da FCT na tensão de +3V

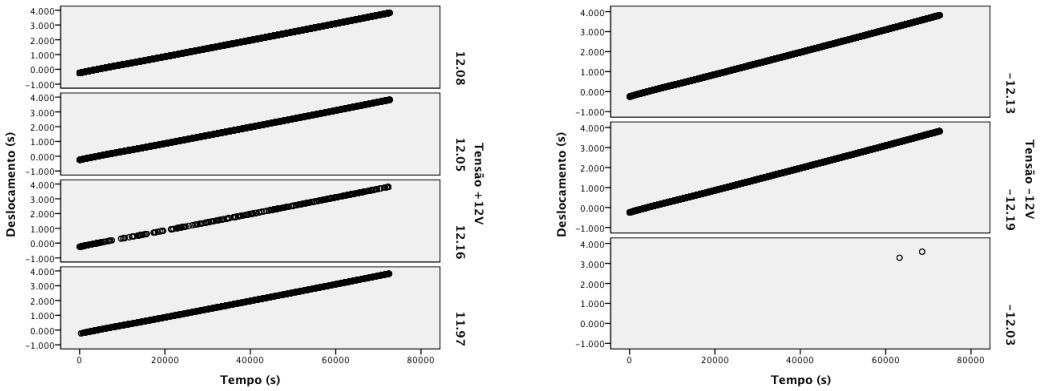
Da Tabela A.2 separou-se as medidas de tensão de alimentação +5V e -5v em grupos com o mesmo valor de tensão. A Figura A.9(a) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +5V. A Figura A.9(b) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em -5V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Da Tabela A.2 separou-se as medidas de tensão de alimentação +12V e -12v



(a) Tensão +5V (b) Tensão -5V

Figura A.9: Deslocamento entre o relógio do HSM e da FCT nas tensões de +5V e -5V



(a) Tensão +12V (b) Tensão -12V

Figura A.10: Deslocamento entre o relógio do HSM e da FCT nas tensões de +12V e -12V

em grupos com o mesmo valor de tensão. A Figura A.10(a) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +12V. A Figura A.10(b) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em -12V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Da Tabela A.2 separou-se as medidas de temperatura da CPU do computador em grupos com o mesmo valor de temperatura. A Figura A.11 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de temperatura da CPU do computador. Como pode ser visto, essas oscilações na temperatura não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Da Tabela A.2 separou-se as medidas de temperatura da placa-mãe do computador em grupos com o mesmo valor de temperatura. A Figura A.12 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de temperatura da placa-mãe do computador. Como pode ser visto, essas oscilações na temperatura não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Em nenhum dos casos acima o relógio do HSM sofreu qualquer influência quando se variou as tensões de alimentação e temperaturas. Isso quer dizer que o relógio não sofre atrasos nem adiantamentos com pequenas variações de temperatura e tensão que ocorrem no dia a dia. E mesmo o HSM PSO PL50 realizando operações criptográficas, o relógio do HSM não sofreu influência dessas operações.

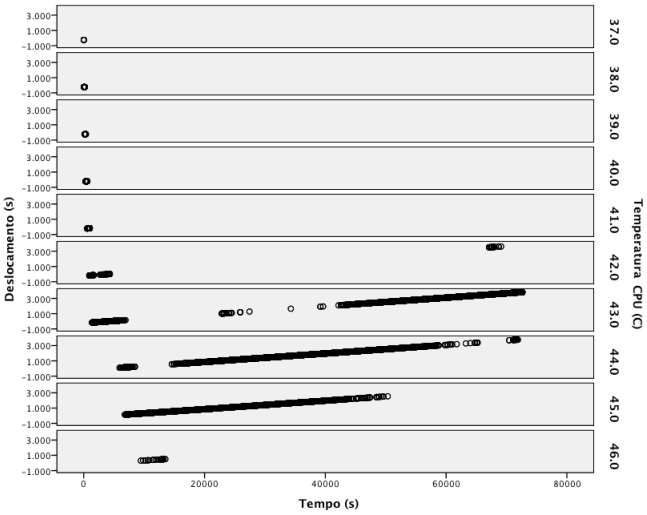


Figura A.11: Deslocamento entre o relógio do HSM e da FCT na temperatura da CPU

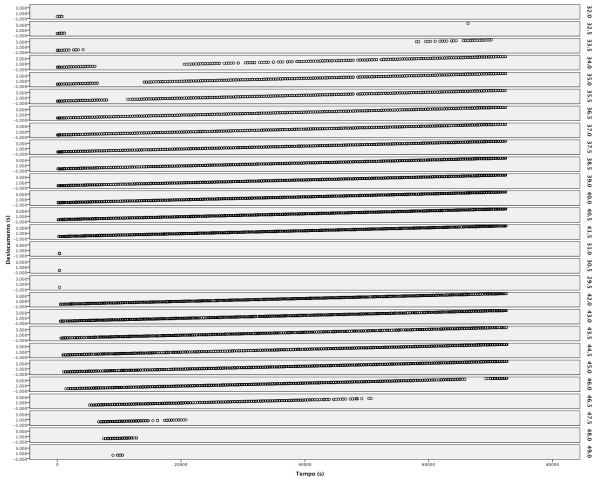


Figura A.12: Deslocamento entre o relógio do HSM e da FCT na temperatura da placa mãe

A.3 Análise do experimento 1 no ASI HSM sem realizar operações criptográficas

Foi feito o experimento 1 com o HSM ASI HSM. Como o ASI HSM foi desenvolvido pelo LabSEC, uma breve descrição do HSM é necessário para entender como foi realizado o experimento. A Figura A.13 representa como é a estrutura interna do HSM e o modo de acesso. A unidade gestora possui uma memória flash que contém o software de gestão de chaves, o OpenHSMd, e que tem acesso a unidade de segurança, que possui os sensores para detecção de intrusão, um gerador de números aleatórios para as operações criptográficas e um relógio. A comunicação com o HSM é feita através da interface de rede, e possui clientes para a configuração

do HSM, e uma engine OpenSSL para acesso ao HSM.

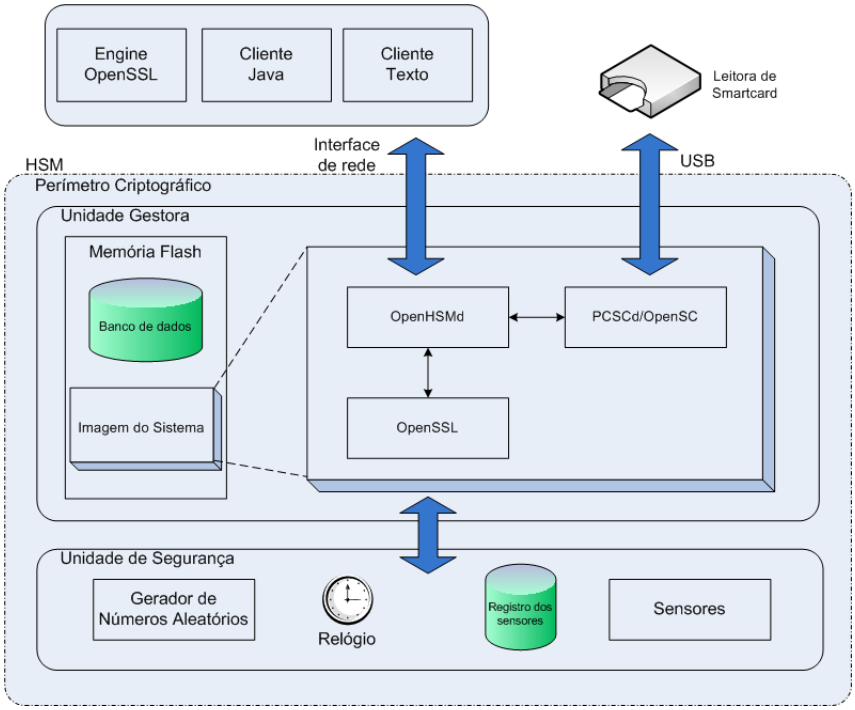


Figura A.13: Estrutura interna do ASI-HSM

Esse HSM teve a imagem do sistema criada no LabSEC. Essa imagem possui um sistema operacional de código aberto, e ali é executado o aplicativo de gestão de chaves do HSM. Foi criada uma outra imagem do sistema baseada nessa, e adicionado novos aplicativos, como o NTP e o de coleta de dados. Nesse caso, o relógio do sistema operacional do HSM foi mantido sincronizado via NTP com 3 servidores NTP stratum 2 e usado como FCT.

Para cada medida da calibração entre os relógios do HSM e da FCT, foram coletados a hora do HSM, a hora da FCT, as tensões de alimentação do HSM, a temperatura do HSM. O intervalo entre as medições é de 1 segundo.

A Tabela A.3 apresenta uma parte das medidas realizadas onde o ASI HSM não realizava operações criptográficas.

Tabela A.3: Dados das medidas realizadas e o ASI HSM não realizando operações criptográficas

Tempo	Relógio (s,ms)		Tensão		Temp.
	HSM	FCT	+5V	+12V	HSM
0	56,040	56,047	4,927	12,009	44
1	57,090	57,097	4,927	12,009	44
2	58,140	58,147	4,927	12,009	44
3	59,190	59,198	4,927	12,009	44
...					
63912	50,480	49,969	4,927	11,980	44

Foram gerados gráficos para possibilitar a análise. A Figura A.14 mostra que com o passar do tempo, o deslocamento entre o relógio do HSM e o relógio da FCT aumenta. Esse aumento representa, numa análise de regressão linear, um coeficiente β de 8,139 $\times$ 10^{-6}. Esse coeficiente indica a inclinação na reta.

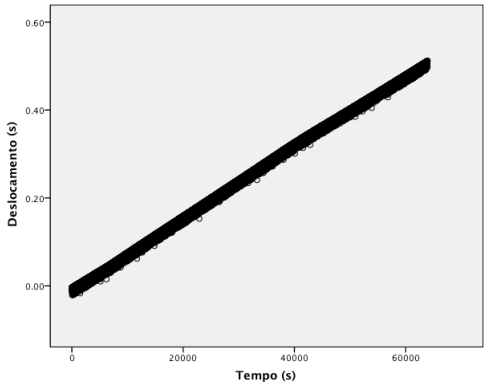


Figura A.14: Deslocamento entre o relógio do HSM e da FCT

A Figura A.15 mostra com mais detalhes o que ocorre entre os segundos 1.000 e 1.100. Isso ocorre por causa dos erros de arredondamentos ocorridos no relógio do ASI-HSM, que tem uma resolução de apenas 10 ms.

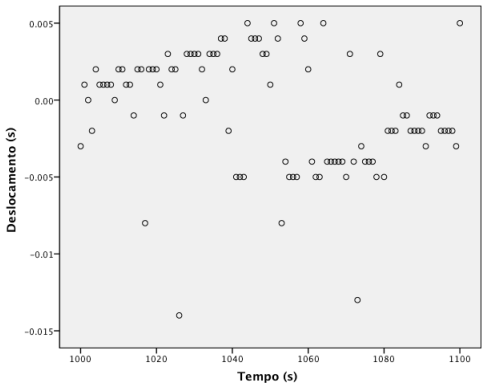
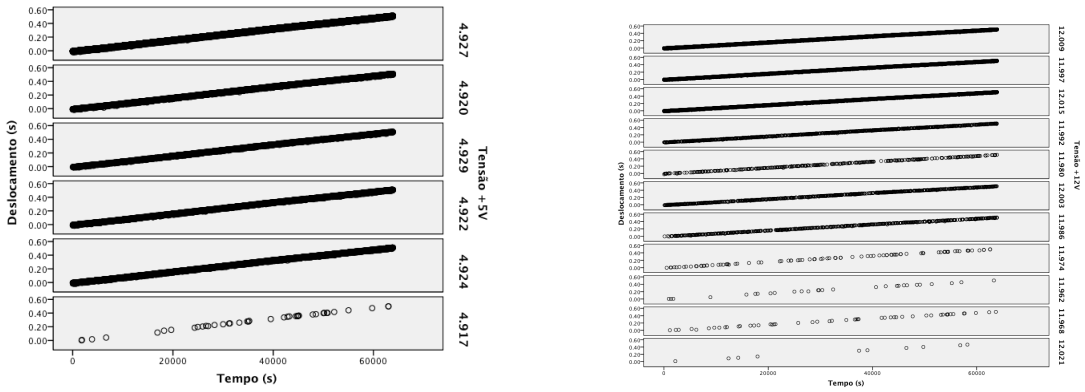


Figura A.15: Diferença entre o relógio do ASI-HSM e da FCT entre os segundo 1.000 e 1.100

Da Tabela A.3 separou-se as medidas de tensão de alimentação +5v e +12v em grupos com o mesmo valor de tensão. A Figura A.16(a) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +5V. A Figura A.16(b) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +12V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.



(a) Tensão +5V (b) Tensão +12V

Figura A.16: Deslocamento entre o relógio do HSM e da FCT nas tensões de +5V e +12V

Da Tabela A.3 separou-se as medidas de temperatura do HSM em grupos com o mesmo valor de temperatura. A Figura A.17 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de temperatura do HSM. Como pode ser visto, essas oscilações na temperatura não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

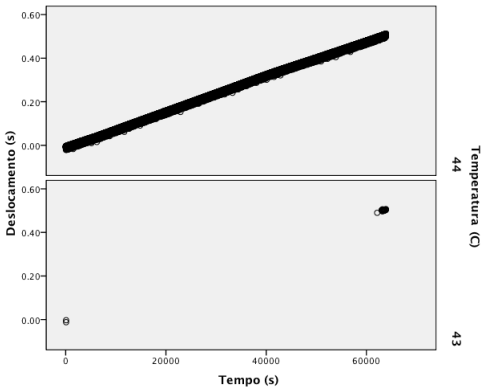


Figura A.17: Deslocamento entre o relógio do HSM e da FCT na temperatura do HSM

Em nenhum dos casos acima o relógio do HSM sofreu qualquer influência quando se variou as tensões de alimentação e temperaturas. Isso quer dizer que o relógio não sofre atrasos nem adiantamentos com pequenas variações de temperatura e tensão que ocorrem no dia a dia.

A.4 Análise do experimento 1 no ASI HSM realizando operações criptográficas

Para cada medida da calibração entre os relógios do HSM e da FCT, foram coletados a hora do HSM, a hora da FCT, as tensões de alimentação do HSM, a temperatura do HSM. O intervalo entre as medições foi de 1 segundo.

A Tabela A.4 apresenta uma parte das medidas realizadas onde o ASI HSM realizava operações criptográficas.

Tabela A.4: Dados das medidas realizadas e o ASI HSM realizando operações criptográficas

Tempo	Relógio (s,ms)		Tensão		Temp.
	HSM	FCT	+5V	+12V	HSM
0	23,740	23,631	4,927	11,992	47
1	24,790	24,682	4,927	11,997	47
2	25,850	25,743	4,927	11,997	47
3	26,910	26,800	4,927	11,992	47
...					
57999	9,580	9,366	4,920	11,980	47

Foram gerados gráficos para possibilitar a análise. A Figura A.18 mostra que com o passar do tempo, o deslocamento entre o relógio do HSM e o relógio da FCT aumenta. Pode-se notar que as leituras ficaram mais espaças, isso por causa do alto uso do processamento das operações de assinaturas realizadas no HSM. O aumento no deslocamento entre os relógios representa, numa análise de regressão linear, um coeficiente β de 1,585 $\times$ 10^{-6}. Esse coeficiente indica a inclinação na reta.

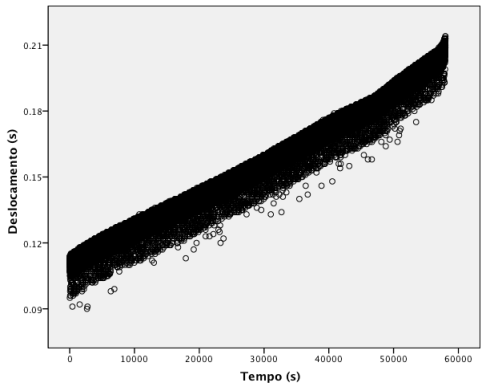


Figura A.18: Deslocamento entre o relógio do HSM e da FCT

A Figura A.19 mostra com mais detalhes o que ocorre entre os segundos 1.000 e 1.100. Isso ocorre por causa dos erros de arredondamentos ocorridos no relógio do ASI-HSM,

que tem uma resolução de apenas 10 ms e também pelo alto processamento das operações de assinaturas realizadas no HSM.

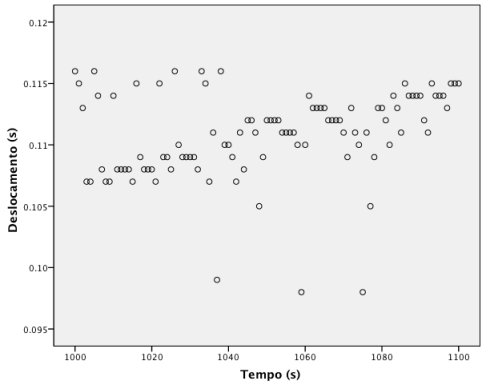
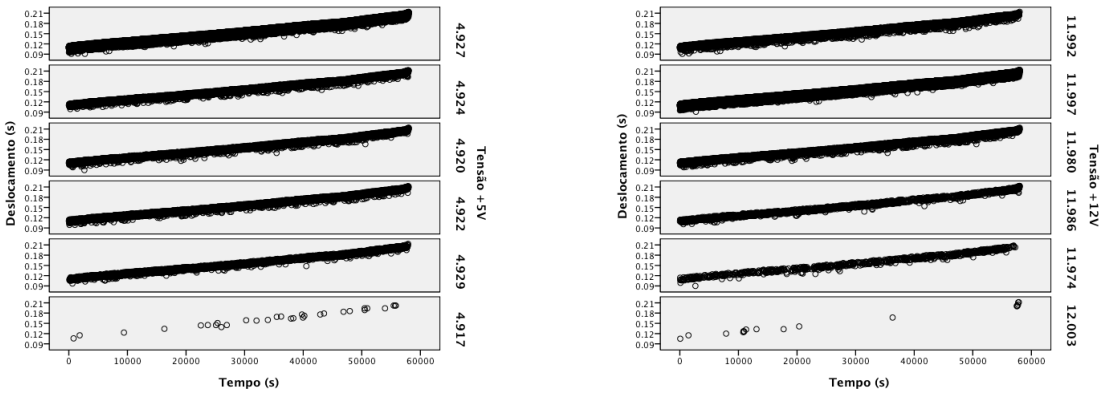


Figura A.19: Deslocamento entre o relógio do ASI-HSM e da FCT entre os segundo 1.000 e 1.100

Da Tabela A.4 separou-se as medidas de tensão de alimentação +5V e +12V em grupos com o mesmo valor de tensão. A Figura A.20(a) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +5V. A Figura A.20(b) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +12V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Da Tabela A.4 separou-se as medidas de temperatura do HSM em grupos com o mesmo valor de temperatura. A Figura A.21 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de temperatura do HSM. Como pode ser visto, essas oscilações na temperatura não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta



(a) Tensão +5V

(b) Tensão +12V

Figura A.20: Deslocamento entre o relógio do HSM e da FCT nas tensões de +5V e +12V

mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

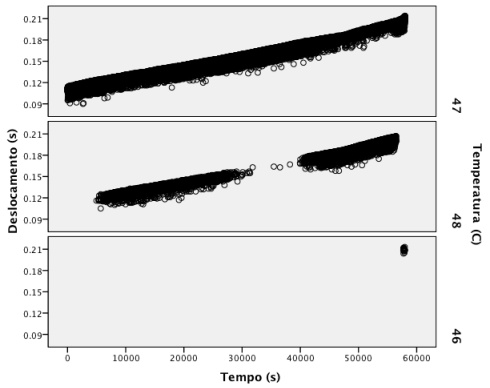


Figura A.21: Deslocamento entre o relógio do HSM e da FCT na temperatura do HSM

Em nenhum dos casos acima o relógio do HSM sofreu qualquer influência quando se variou as tensões de alimentação e temperaturas. Apenas uma dispersão alta por causa do alto processamento nas operações de assinatura realizadas no HSM. Isso quer dizer que o relógio não sofre um escorregamento maior com pequenas variações de temperatura e tensão que ocorrem no dia a dia.

A.5 Análise do experimento 2 no PSO PL50 sem realizar operações criptográficas

Para cada medida da calibração entre os relógios do HSM e da FCT, foram coletados a hora do HSM, a hora da FCT, as tensões de alimentação do computador, a temperatura da CPU do computador e a temperatura da placa-mãe do computador. Esse HSM não possui sensores de tensões de alimentação e temperatura, por isso foram coletados da placa-mãe onde o HSM está ligado. O intervalo entre as medições foi de 1 minuto.

A Tabela A.5 apresenta uma parte das medidas realizadas.

Foram gerados gráficos para possibilitar a análise. A Figura A.28 mostra que com o passar do tempo, o deslocamento entre o relógio do HSM e o relógio da FCT aumenta. Esse aumento representa, numa análise de regressão linear, um coeficiente β de 0,004. Esse coeficiente indica a inclinação na reta.

Da Tabela A.5 separou-se as medidas de tensão de alimentação +3v em grupos com o mesmo valor de tensão. A Figura A.23 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +3V. Como pode ser visto, essas oscilações na

Tabela A.5: Dados das medidas realizadas e o PSO PL50 não realizando operações criptográficas

Tempo	Relógio (m:s,ms)		Tensão					Temperatura	
	HSM	FCT	+3v	+5V	-5v	+12v	-12v	CPU	MB
0	46:41,067	46:40,719	3,30	5,02	-5,61	12,08	-12,19	37	24
1	47:41,073	47:40,728	3,30	5,02	-5,54	12,08	-12,13	37	24,5
2	48:41,074	48:40,733	3,30	5,06	-5,54	12,16	-12,13	38	24
3	49:41,075	49:40,738	3,30	5,06	-5,54	12,08	-12,13	37	23
...									
1526	13:23,135	13:28,523	3,30	5,02	-5.54	12,16	-12,13	36	22.5

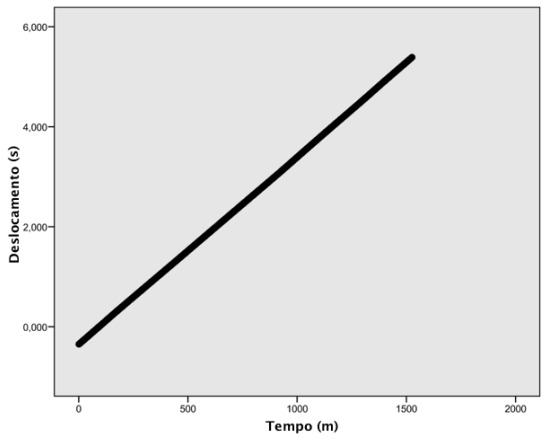


Figura A.22: Deslocamento entre o relógio do HSM e da FCT

tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Da Tabela A.5 separou-se as medidas de tensão de alimentação +5V e -5v em grupos com o mesmo valor de tensão. A Figura A.24(a) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +5V. A Figura A.24(b) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em -5V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Da Tabela A.5 separou-se as medidas de tensão de alimentação +12V e -12v em grupos com o mesmo valor de tensão. A Figura A.25(a) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +12V. A Figura A.25(b) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em -12V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

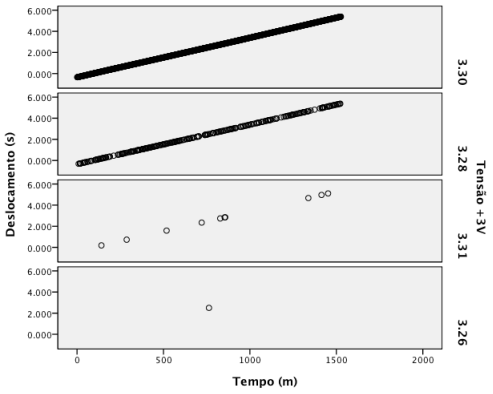
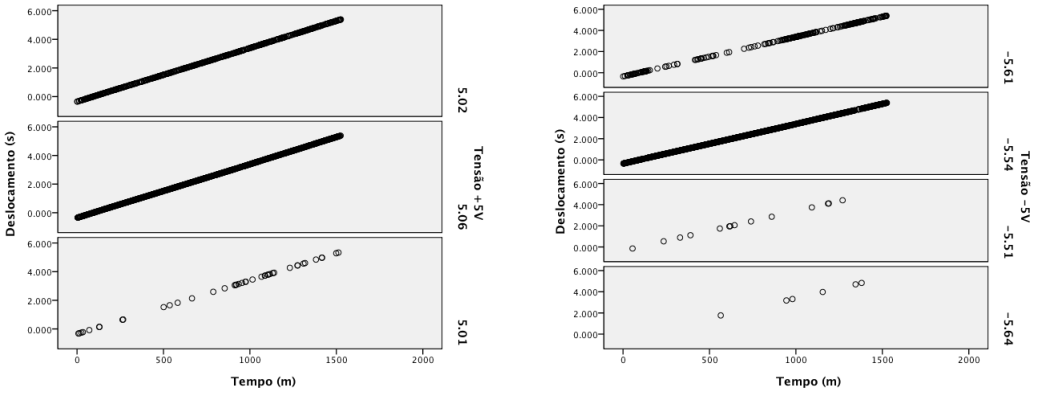


Figura A.23: Deslocamento entre o relógio do HSM e da FCT na tensão de +3V



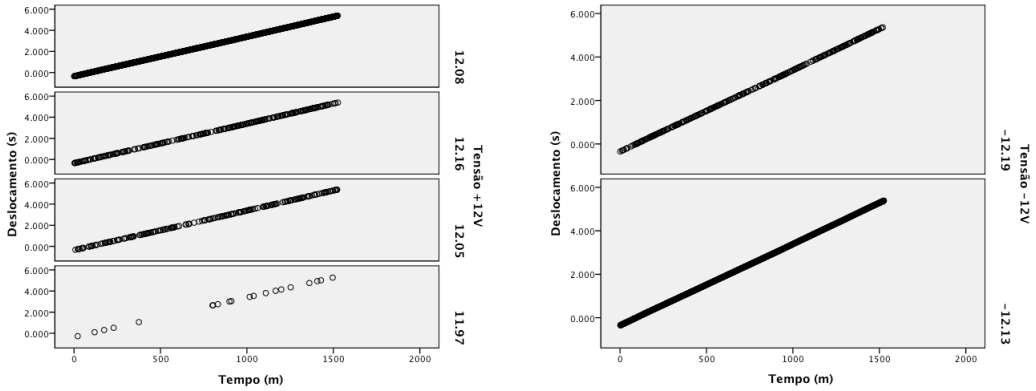
(a) Tensão +5V (b) Tensão -5V

Figura A.24: Deslocamento entre o relógio do HSM e da FCT nas tensões de +5V e -5V

Da Tabela A.5 separou-se as medidas de temperatura da CPU do computador em grupos com o mesmo valor de temperatura. A Figura A.26 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de temperatura da CPU do computador. Como pode ser visto, essas oscilações na temperatura não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Da Tabela A.5 separou-se as medidas de temperatura da placa-mãe do computador em grupos com o mesmo valor de temperatura. A Figura A.27 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de temperatura da placa-mãe do computador. Como pode ser visto, essas oscilações na temperatura não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Em nenhum dos casos acima o relógio do HSM sofreu qualquer influência quando se variou as tensões de alimentação e temperaturas. Isso quer dizer que o relógio não sofre



(a) Tensão +12V (b) Tensão -12V

Figura A.25: Deslocamento entre o relógio do HSM e da FCT nas tensões de +12V e -12V

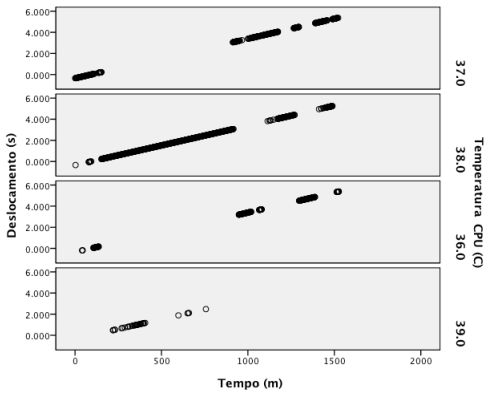


Figura A.26: Deslocamento entre o relógio do HSM e da FCT na temperatura da CPU

atrasos nem adiantamentos com pequenas variações de temperatura e tensão que ocorrem no dia a dia.

A.6 Análise do experimento 2 no PSO PL50 realizando operações criptográficas

Para cada medida da calibração entre os relógios do HSM e da FCT, foram coletados a hora do HSM, a hora da FCT, as tensões de alimentação do computador, a temperatura da CPU do computador e a temperatura da placa-mãe do computador. Esse HSM não possui sensores de tensões de alimentação e temperatura, por isso foram coletados da placa-mãe onde o HSM está ligado. O intervalo de medição foi de 1 minuto.

A Tabela A.6 apresenta uma parte das medidas realizadas.

Foram gerados gráficos para possibilitar a análise. A Figura A.28 mostra que

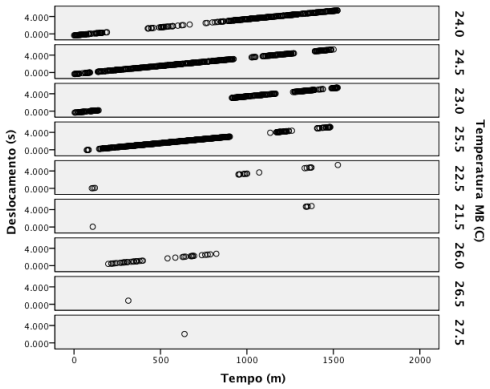


Figura A.27: Deslocamento entre o relógio do HSM e da FCT na temperatura da placa mãe

Tabela A.6: Dados das medidas realizadas e o PSO PL50 realizando operações criptográficas

Tempo	Relógio (m:s,ms)		Tensão		Temperatura	
	HSM	FCT	+5V	+12v	CPU	MB
0	46:41,054	46:40,547	5,14	12,04	55	29
1	47:41,084	47:40,580	5,14	12,04	55	29
2	48:41,112	48:40,612	5,14	12,04	55	29
3	49:41,140	49:40,643	5,14	12,04	55	29
...						
1526	13:23,135	13:28,523	5,02	12,16	36	22.5

com o passar do tempo, o deslocamento entre o relógio do HSM e o relógio da FCT aumenta. Esse aumento representa, numa análise de regressão linear, um coeficiente β de 0,003. Esse coeficiente indica a inclinação na reta.

Da Tabela A.6 separou-se as medidas de tensão de alimentação +5V em grupos com o mesmo valor de tensão. A Figura A.29 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +5V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Da Tabela A.6 separou-se as medidas de tensão de alimentação +12V em grupos com o mesmo valor de tensão. A Figura **??** mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +12V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Da Tabela A.6 separou-se as medidas de temperatura da CPU do computador em grupos com o mesmo valor de temperatura. A Figura A.31 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de temperatura da CPU do computador. Como pode ser visto, essas oscilações na temperatura não afetam a estabilidade do relógio, isto é,

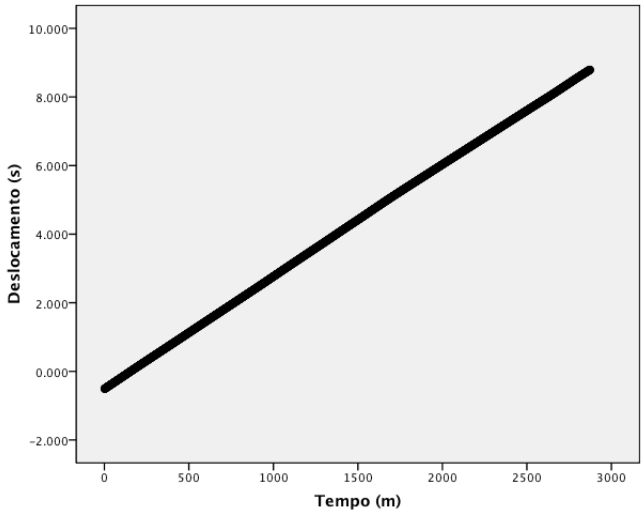


Figura A.28: Deslocamento entre o relógio do HSM e da FCT

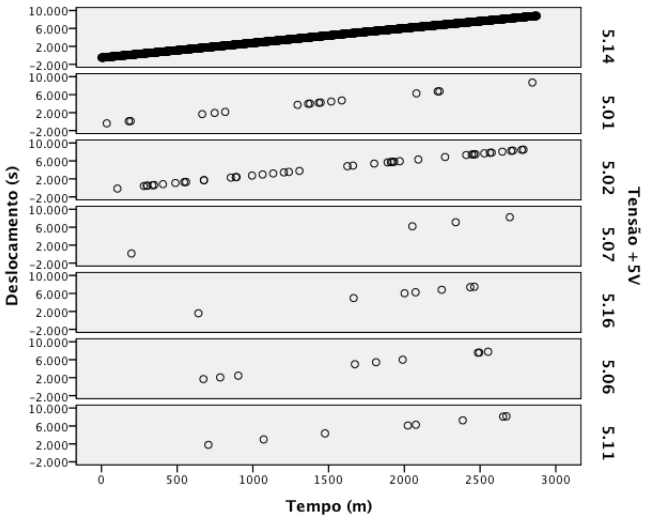


Figura A.29: Deslocamento entre o relógio do HSM e da FCT

o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Da Tabela A.6 separou-se as medidas de temperatura da placa-mãe do computador em grupos com o mesmo valor de temperatura. A Figura A.32 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de temperatura da placa-mãe do computador. Como pode ser visto, essas oscilações na temperatura não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Em nenhum dos casos acima o relógio do HSM sofreu qualquer influência quando se variou as tensões de alimentação e temperaturas. Isso quer dizer que o relógio não sofre

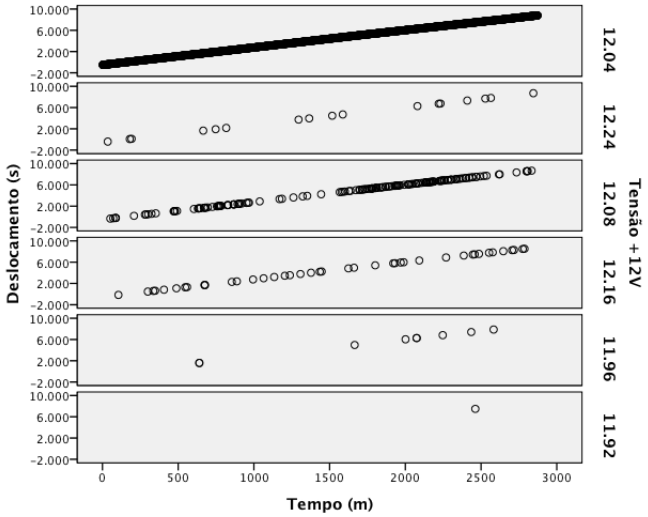


Figura A.30: Deslocamento entre o relógio do HSM e da FCT

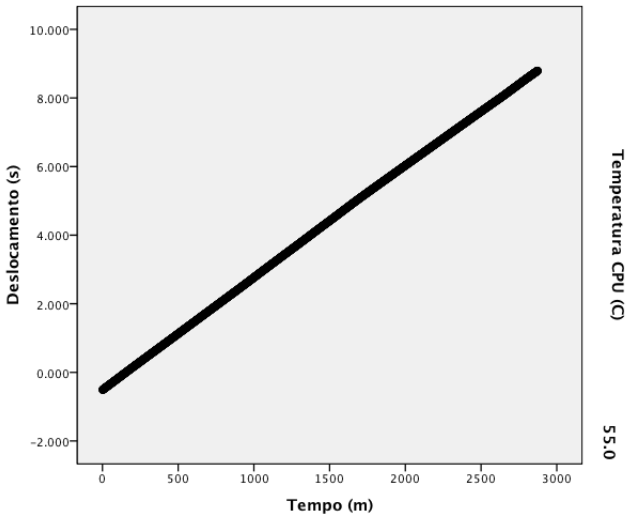


Figura A.31: Deslocamento entre o relógio do HSM e da FCT na temperatura da CPU

atrasos nem adiantamentos com pequenas variações de temperatura e tensão que ocorrem no dia a dia.

A.7 Análise do experimento 2 no ASI HSM sem realizar operações criptográficas

Para cada medida da calibração entre os relógios do HSM e da FCT, foram coletados a hora do HSM, a hora da FCT, as tensões de alimentação do HSM, a temperatura do HSM. O intervalo de medição foi de 1 minuto.

A Tabela A.7 apresenta uma parte das medidas realizadas onde o ASI HSM

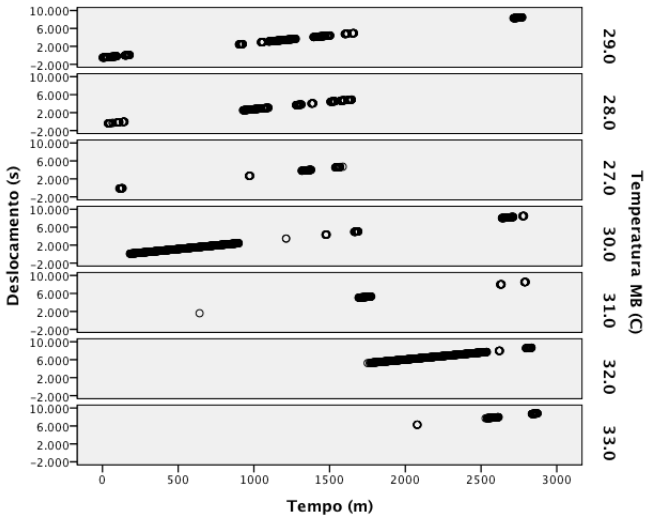


Figura A.32: Deslocamento entre o relógio do HSM e da FCT na temperatura da placa mãe

realizava operações criptográficas.

Tabela A.7: Dados das medidas realizadas e o ASI HSM sem realizar operações criptográficas

Tempo	Relógio (m:s,ms)		Tensão		Temp.
	HSM	FCT	+5V	+12V	HSM
0	54:33,010	54:31,261	4,927	12,021	43
1	55:33,070	55:31,315	4,927	12,027	43
2	56:33,120	56:31,368	4,927	12,021	43
3	57:33,180	57:31,422	4,927	12,021	43
...					
693	27:9,330	27:7,300	4,920	11,997	40

Foram gerados gráficos para possibilitar a análise. A Figura A.33 mostra que com o passar do tempo, o deslocamento entre o relógio do HSM e o relógio da FCT aumenta. O aumento no deslocamento entre os relógios representa, numa análise de regressão linear, um coeficiente β de 3,98 $\times$ 10^{-4}. Esse coeficiente indica a inclinação na reta. Mas pode-se notar que as leituras ficaram mais espaças, isso por causa do alto uso do processamento das operações de assinaturas realizadas no HSM.

Da Tabela A.7 separou-se as medidas de tensão de alimentação +5V e +12V em grupos com o mesmo valor de tensão. A Figura A.34(a) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +5V. A Figura A.34(b) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +12V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

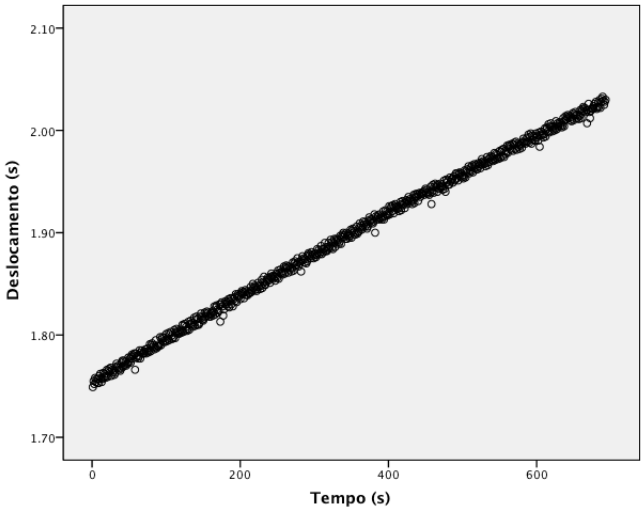
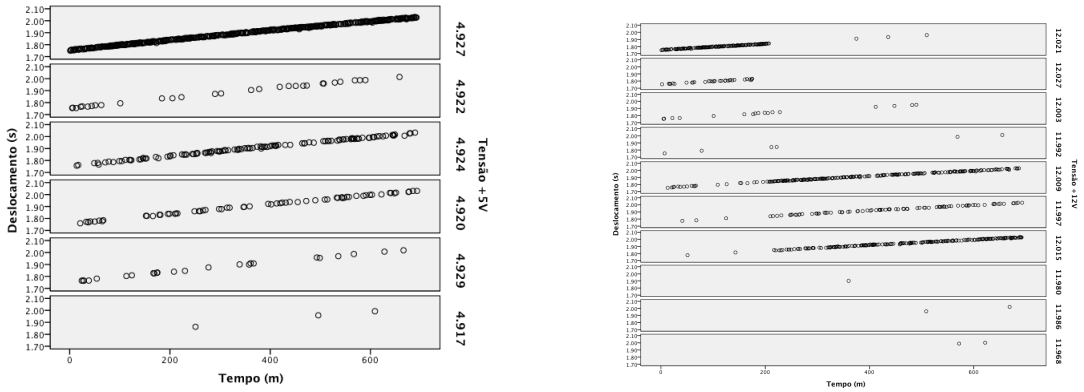


Figura A.33: Deslocamento entre o relógio do HSM e da FCT



(a) Tensão +5V (b) Tensão +12V

Figura A.34: Deslocamento entre o relógio do HSM e da FCT nas tensões de +5V e +12V

Da Tabela A.7 separou-se as medidas de temperatura do HSM em grupos com o mesmo valor de temperatura. A Figura A.35 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de temperatura do HSM. Como pode ser visto, essas oscilações na temperatura não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Em nenhum dos casos acima o relógio do HSM sofreu qualquer influência quando se variou as tensões de alimentação e temperaturas. Apenas uma dispersão alta por causa do alto processamento nas operações de assinatura realizadas no HSM. Isso quer dizer que o relógio não sofre um escorregamento maior com pequenas variações de temperatura e tensão que ocorrem no dia a dia.

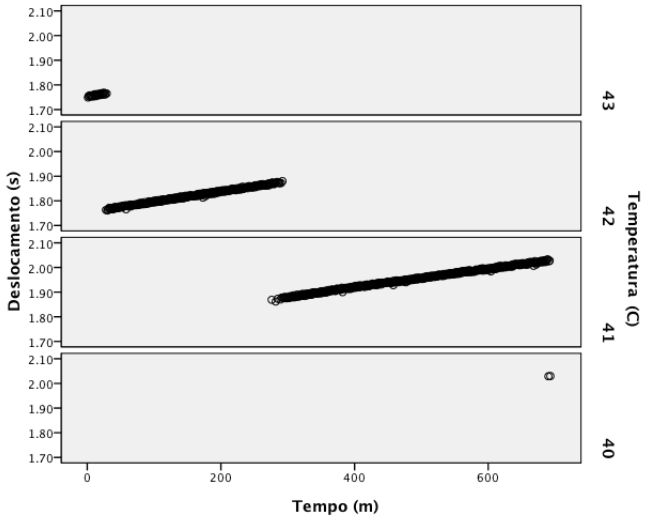


Figura A.35: Deslocamento entre o relógio do HSM e da FCT na temperatura do HSM

A.8 Análise do experimento 2 no ASI HSM realizando operações criptográficas

Para cada medida da calibração entre os relógios do HSM e da FCT, foram coletados a hora do HSM, a hora da FCT, as tensões de alimentação do HSM, a temperatura do HSM. O intervalo entre as medidas é de 60 segundos.

A Tabela A.8 apresenta uma parte das medidas realizadas onde o ASI HSM realizava operações criptográficas.

Tabela A.8: Dados das medidas realizadas e o ASI HSM realizando operações criptográficas

Tempo	Relógio (m:s,ms)		Tensão		Temp.
	HSM	FCT	+5V	+12V	HSM
0	47:13,720	47:13,331	4,927	11,997	47
1	48:13,770	48:13,379	4,927	11,997	47
2	49:13,820	49:13,432	4,927	11,997	47
3	50:13,870	50:13,480	4,927	11,997	47
...					
517	23:40,980	23:40,545	4,927	11,997	48

Foram gerados gráficos para possibilitar a análise. A Figura A.36 mostra que com o passar do tempo, o deslocamento entre o relógio do HSM e o relógio da FCT aumenta. O aumento no deslocamento entre os relógios representa, numa análise de regressão linear, um coeficiente β de 8,738 $\times$ 10^{-5}. Esse coeficiente indica a inclinação na reta. Mas pode-se notar que as leituras ficaram mais espaças, isso por causa do alto uso do processamento das operações de assinaturas realizadas no HSM.

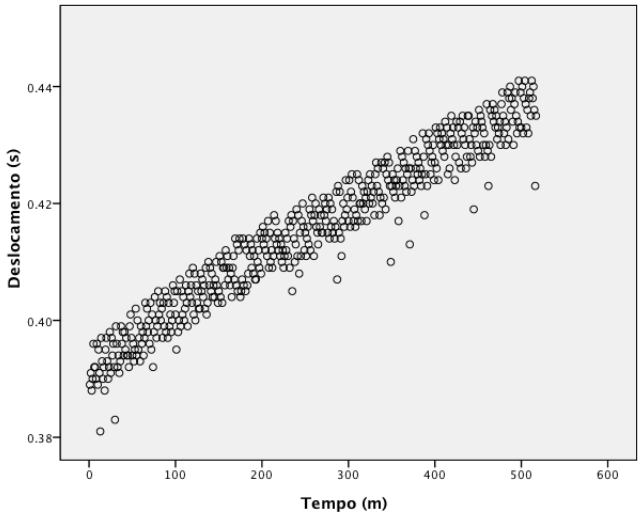
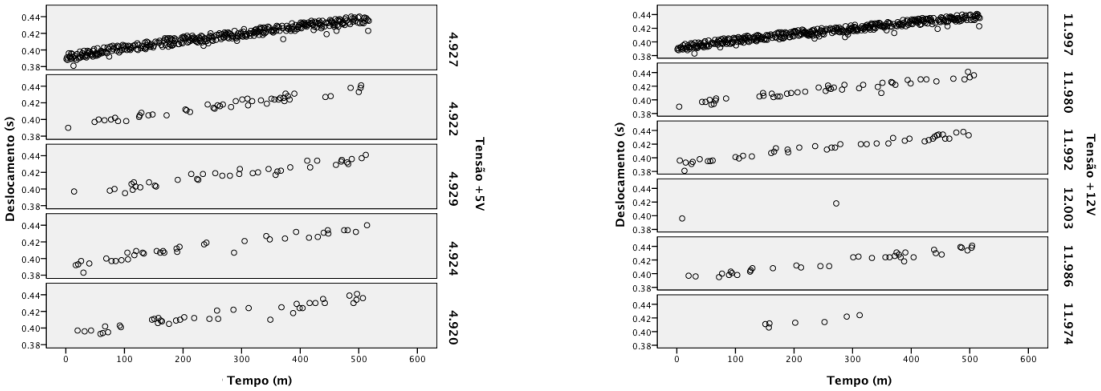


Figura A.36: Deslocamento entre o relógio do HSM e da FCT



(a) Tensão +5V (b) Tensão +12V

Figura A.37: Deslocamento entre o relógio do HSM e da FCT nas tensões de +5V e +12V

Da Tabela A.8 separou-se as medidas de tensão de alimentação +5V e +12V em grupos com o mesmo valor de tensão. A Figura A.37(a) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +5V. A Figura A.37(b) mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de tensão em +12V. Como pode ser visto, essas oscilações na tensão não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no dia a dia.

Da Tabela A.8 separou-se as medidas de temperatura do HSM em grupos com o mesmo valor de temperatura. A Figura A.38 mostra o deslocamento entre o relógio do HSM e o relógio da FCT para as oscilações de temperatura do HSM. Como pode ser visto, essas oscilações na temperatura não afetam a estabilidade do relógio, isto é, o relógio não se atrasa nem se adianta mais por causa dessas oscilações. Essas oscilações são para padrões normais de uso do HSM no

dia a dia.

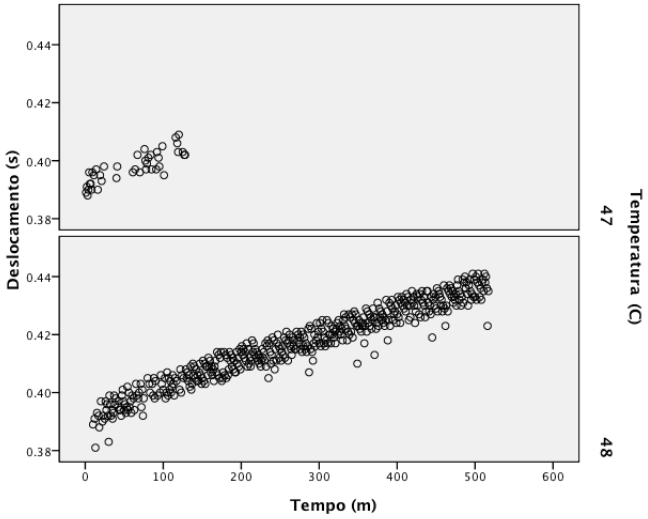


Figura A.38: Deslocamento entre o relógio do HSM e da FCT na temperatura do HSM

Em nenhum dos casos acima o relógio do HSM sofreu qualquer influência quando se variou as tensões de alimentação e temperaturas. Apenas uma dispersão alta por causa do alto processamento nas operações de assinatura realizadas no HSM. Isso quer dizer que o relógio não sofre um escorregamento maior com pequenas variações de temperatura e tensão que ocorrem no dia a dia.