ANEXO II À PORTARIA MCT Nº 293, DE 11.05.2007

1 DEFINIÇÕES

Autoridade de Carimbo do Tempo (ACT) – A autoridade 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. É responsável pela operação de uma ou mais SCT, conectados à ReTemp/HLB, que geram carimbos e assinam em nome da ACT.

Autoridade Certificadora (AC) – Entidade que emite, renova ou revoga certificados digitais de outras AC ou de titulares finais. Publica LCR. Na estrutura de carimbo do tempo da ICP-Brasil, emite os certificados digitais usados nos Servidores de Carimbo do Tempo (SCT) e nas EAT e emite ainda os demais certificados utilizados nos processos relacionados aos carimbos do tempo.

Autoridade Certificadora Raiz da ICP-Brasil (AC Raiz) – Entidade que credencia, audita e fiscaliza as demais entidades da ICP-Brasil. Assina seu próprio certificado e os certificados das AC imediatamente abaixo dela.

Autoridade Internacional do Tempo (AIT) – BIPM, órgão internacional responsável pela geração, manutenção e disseminação do UTC.

Calibração Temporal do Relógio - Processo pelo qual dois ou mais relógios passam a indicar o mesmo tempo.

Carimbo do Tempo (CT) – Documento eletrônico emitido pela ACT, que serve como evidência de que uma informação digital existia numa determinada data e hora no passado.

Certificado de Atributo - Estrutura de dados contendo um conjunto de atributos (características e informações) sobre a entidade final, que é assinada digitalmente com a chave privada da entidade que o emitiu. Deve possuir um período de validade, durante o qual os atributos incluídos no certificado são considerados válidos.

Certificado de Atributos do Tempo (CAT) – Certificado de atributos emitido e assinado digitalmente pelos equipamentos SAS (primário e secundário) autorizando ou não o funcionamento do equipamento na hierarquia imediatamente inferior. São emitidos com a periodicidade necessária de forma a manter os níveis de segurança e exatidão temporal definidas pela EAT.

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.

Compensação (Offset) - Calibração necessária no relógio interno ao HSM da Unidade Carimbadora do Tempo (UCT) para atingir a precisão temporária exigida pela Autoridade Nacional do Tempo (EAT) na emissão dos Carimbos do Tempo (CT).

Disseminação - a disseminação é o processo de provimento de rastreabilidade a um grande número de usuários, via uma cadeia metrológica (Diretrizes Estratégicas para a Metrologia Brasileira, Comitê Brasileiro de Metrologia).

Entidade de Auditoria de Tempo (EAT) - Entidade que realiza as atividades de autenticação e sincronismo de Servidores de Carimbo de Tempo – SCT, instalados nas ACT.

Na estrutura de carimbo de tempo da ICP-Brasil, a EAT é o próprio Observatório Nacional – ON, que possui Sistemas de Autenticação e Sincronismo – SAS, ligados diretamente ao relógio atômico ou indiretamente, por meio de outros SAS.

Estabilidade - Capacidade de um oscilador em manter a mesma freqüência em um determinado intervalo de tempo.

Fonte Confiável de Tempo (FCT): É a denominação dada ao Relógio Atômico localizado no Observatório Nacional.

Observatório Nacional (ON) – Vinculado ao Ministério da Ciência e Tecnologia, integrante do Sistema Nacional de Metrologia – Sinmetro, o ON é o responsável legal pela geração, conservação e disseminação da Hora Legal Brasileira, com rastreabilidade metrológica ao BIPM. Mantém e opera o Relógio Atômico, que é a Fonte Confiável de Tempo - FCT, a partir da qual se determina a Hora Legal Brasileira.

Na estrutura de carimbo de tempo da ICP-Brasil, além de gerar a Hora Legal Brasileira, atua como Entidade de Auditoria de Tempo.

Rastreabilidade - Relacionamento do resultado de uma medição com um valor de referência previamente estabelecido, geralmente um padrão nacional ou internacional.

Resolução (Resolution) - Menor diferença entre indicações de um dispositivo mostrador que pode ser significativamente percebida. A resolução de um relógio é o menor incremento de tempo que o mesmo pode indicar.

Serviço de Autenticação e Sincronismo (SAS) - Atividade periodicamente realizada, através da utilização de procedimentos de autenticação e sincronismo dos relógios internos aos HSMs utilizados pelos equipamentos pertencentes a infra-estrutura geradora do Carimbo do Tempo de forma a manter os níveis de segurança e exatidão temporal definidas pela Entidade de Auditoria do Tempo (EAT).

Servidores de Autenticação e Sincronismo Primário (SASp) - Equipamento que realiza as atividades de Autenticação e Sincronismo dos Servidores de Autenticação e Sincronismo Secundários (SASs). A responsabilidade referente aos serviços prestados por um SASp dentro da ICP-Brasil será sempre do Observatório Nacional .

Servidores de Autenticação e Sincronismo Secundário (SASs) - Equipamento que, uma vez autenticado e sincronizado pela SASp, realiza as atividades de Autenticação e Sincronismo das Unidades Carimbadoras do Tempo (UCT). A responsabilidade referente aos serviços prestados por um SASs dentro da ICP-Brasil será sempre do Observatório Nacional.

Tempo Universal Coordenado (UTC) - Escala de tempo adotada como padrão de Tempo Oficial Internacional, utilizada pelo sistema de Metrologia Internacional, Convenção do Metro, determinada e disseminada pela Autoridade Internacional do Tempo (AIT).

Servidor de Carimbo do Tempo (SCT) - Dispositivo único constituído por *hardware* e *software* que gera os carimbos do tempo, sob o gerenciamento da ACT. Deve possuir um HSM contendo um relógio a partir do qual são emitidos os carimbos do tempo. Nesse HSM devem ser também realizadas as funções criptográficas de geração de chaves e assinaturas digitais.

Usuários – Empresas públicas ou privadas que tenham contratado os serviços da ReTemp/HLB.

2 INTRODUÇÃO

A data/hora tem sido um dos elementos mais críticos nas relações comerciais entre países e entre pessoas por centenas de anos. Ela estabelece a necessária evidência de quando uma transação foi efetuada. Os documentos em papel tem certas características que permitem a verificação de sua autenticidade, após a sua emissão. Com o avanço da Tecnologia da Informática, estamos caminhando para a substituição do papel por "bits" e "bytes".

3 DOCUMENTO ELETRÔNICO

Definido por diversos autores como sendo uma seqüência de bits representando uma informação que será em algum momento processada por computadores, neste novo formato, a informação passou a ser vulnerável a ataques eletrônicos. Buscando resolver este problema foram criados os sistemas de criptografia e de infra-estruturas de chaves públicas - ICP, adotados internacionalmente e no Brasil pela ICP Brasil. Este sistema de Chaves Públicas, consegue garantir o conteúdo e a autoria dos documentos eletrônicos, mas não consegue garantir o instante de tempo em que tais documentos são assinados, gerados ou copiados, visto que se utilizam da data/hora gerada em computadores locais, sem nenhum controle sobre a origem da data/hora que é colocada no documento.

4 INFRAESTRUTURA DE TEMPO CERTIFICADO

Visando a garantir aos seus usuários a transposição da data/hora desde os padrões primários até os documentos eletrônicos, de forma segura, autêntica e auditável o ON implantou por intermédio da Rede de Carimbo do Tempo Certificado à Hora Legal Brasileira - ReTemp/HLB, uma infra-estrutura de Tempo Certificado que permite atingir este objetivo, de acordo com as normas internacionais [1,2] criadas pelo *Internet Engineering Task Force- IETF*, e pelo *Internet Engineering Steering Group – IESG.*

Esta estrutura consiste de padrões atômicos primários e secundários, servidores de carimbo do tempo auditados e sincronizados a estes padrões e um sistema de gerenciamento que forneça as evidências de que os resultados obtidos estejam rastreados à Hora legal Brasileira que por sua vez está rastreada ao sistema metrológico internacional sob a coordenação do *Bureau International de Poids et Mesures* – BIPM[4].

5 RASTREABILIDADE AO BIPM e DISSEMINAÇÃO

Criado em Paris em 1875 durante a Convenção do metro, o BIPM possui como atribuição principal "assegurar a nível mundial a uniformidade das medições e suas rastreabilidades ao sistema internacional de unidades".

Conforme definição do Vocabulário Internacional de Termos Fundamentais e Gerais de Metrologia – VIM, INMETRO/CNI/SENAI 2000, a **rastreabilidade** de uma medição é 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."

Esta organização não governamental calcula a partir de uma rede de laboratórios mundial (cerca de 50) a hora UTC que vem a ser o resultado de uma média ponderado de cerca de 200 padrões primários instalados nestes laboratórios.

Os resultados destes cálculos são divulgados pela página WEB do BIPM, www.bipm.fr aonde são relacionadas as diferenças entre as horas de cada um destes padrões e a hora UTC. O documento que contém esta informação chama-se circular T, publicada mensalmente pelo BIPM.
De acordo com o documento "Diretrizes Estratégicas para a Metrologia Brasileira 2003-2007, publicado pelo Comitê Brasileiro de Metrologia, "**disseminação** é o processo de provimento de rastreabilidade a um grande número de usuários, via uma cadeia metrológica", portanto cumpre ao ON realizar as funções de disseminação e rastreabilidade relacionadas com as grandezas tempo e freqüência, obedecendo a hierarquia do sistema metrológico internacional, Figura-2.

6 DESCRIÇÃO TÉCNICA

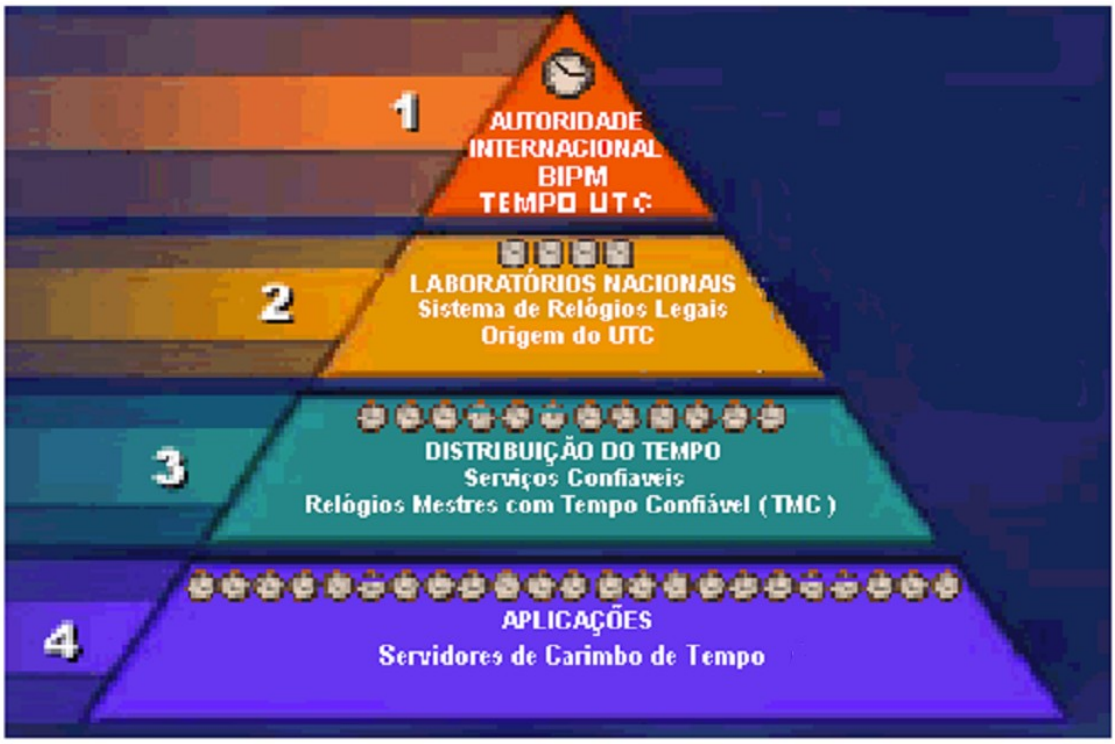

Figura -1 Rastreabilidade da ReTemp/HLB

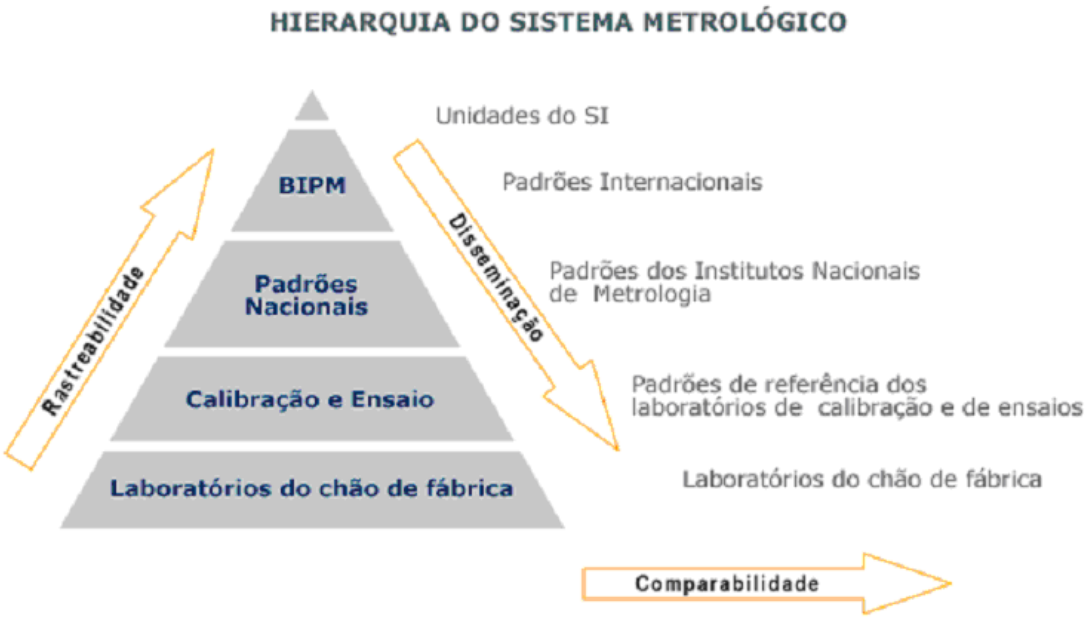

Figura -2 Modelo de hierarquia metrológica do BIPM

Introdução

A ReTemp/HLB atinge os seus objetivos por intermédio de servidores especiais, servidores de carimbo do tempo - SCT que recebem autorização para funcionar por intermédio de

certificados de atributos[3] emitidos por outros equipamentos em nível superior na hierarquia do sistema de autenticação/sincronismo que tem seu início em relógios atômicos rastreáveis ao BIPM.

Hierarquia adotada pela ReTemp/HLB

Na Figura -1 pode-se ver a representação da cadeia de rastreabilidade adotada na ReTemp/HLB que segue a hierarquia metrológica adotada pelo BIPM para as demais unidades de medidas do sistema internacional de medidas, Figura - 2. Conforme o fabricante do equipamento que esteja sendo utilizado poderemos ter ou não a presença do nível 3. No topo da cadeia temos o BIPM que centraliza a realização do cálculo da hora internacional - UTC. No nível 2 estão situados os equipamentos autenticadores/sincronizadores primários – SASp , primários e no nível 3 os equipamentos SAS secundários - SASs. Finalmente, no nível 4 os servidores de carimbo do tempo - SCT.

SAS primário - SASp

Os SASp devem possuir relógios atômicos secundários de acordo com modelo adotado pelo NIST, e HSM, para armazenamento seguro da data/hora e dos certificados digitais próprios, bem como armazenamento da chave pública dos certificados digitais dos SASs sob sua responsabilidade, para garantir a integridade do sistema.

Eles são sincronizados diretamente pelos padrões atômicos primários através do código IRIG B[9] , e têm como função autenticar/sincronizar os SASs, através de protocolos seguros num intervalo de tempo máximo de 5 segundos, por intermédio da emissão de certificados de atributos do tempo – CAT emitidos a cada 24 horas. Caso o fabricante não possua o nível 3 os SASp irão autenticar/sincronizar os SCT ao invés dos SASs.

SAS Secundário - SASs

Os SAS secundários, possuem relógios atômicos secundários e HSM, para armazenamento seguro da data/hora e dos certificados digitais próprios bem como da parte pública dos certificados digitais dos SCT sob sua responsabilidade.

Eles são autenticados/sincronizados pelos SASp através de protocolos seguros num intervalo de tempo máximo de 5 segundos.

Estes SAS secundários têm como função autenticar/sincronizar os SCT, através de protocolos seguros num intervalo de tempo máximo de 5 segundos por intermédio da emissão de CAT's emitidos a cada 6 horas.

No caso do fabricante que não possui o nível 3 este item 6.2.2 não se aplica.

Servidor de carimbo do tempo - SCT

Estes equipamentos são servidores especiais com HSM FIPS 140–2 level 3, dentro do qual está armazenado o certificado digital da ICP-BRASIL e o relógio autenticado/sincronizado pelo SASs (ou SASp, dependendo do fabricante) a partir do qual são emitidos os carimbos do tempo. Em relação às RFC's do IETF, eles correspondem ao "Time Stamping Unit –TSU".

Autenticação/Sincronização

Esta é uma das mais importantes operações no sistema adotado pelo ON, pois é por intermédio desta operação que a cadeia de rastreabilidade consegue chegar desde os relógios atômicos até os SCT.

Também resulta deste processo a emissão e o envio de CAT's por parte dos SAS's de forma que os equipamentos nos níveis inferiores possam funcionar adequadamente.

Entre o relógio atômico e o SASp

Neste nível não é realizado o processo de autenticação/sincronização, pois a comunicação entre o relógio atômico e o SASp é realizado em duas etapas e ocorre no interior de um "rack" instalado em ambiente com nível de segurança 4, ICP-BRASIL.

Na primeira etapa o Relógio atômico sincroniza um gerador de código IRIG B, cinco milhões de vezes por segundo, e a conexão entre os dois ocorre por intermédio de cabo coaxial de 2 metros de comprimento.

Na segunda etapa o gerador de código IRIG B, sincroniza o SASp uma vez por segundo e a conexão entre os dois se dá por intermédio de cabo coaxial de 2 metros de comprimento.

Os três equipamentos, o Relógio Atômico, o gerador de código IRIG B e o SASp ficam instalados juntos no interior de um mesmo "rack".

Entre o SASp e o SASs.

Somente ocorre com o sistema do fabricante que possui o nível 3, sendo utilizados o protocolo TLS[5] para autenticação mútua e o protocolo NTP[7] com autenticação por chave de seção simétrica. As duas operações devem ser realizadas num tempo máximo de 5 segundos, sendo que se a autenticação mútua não se realizar o sincronismo não se concretiza e o SASs não recebe o CAT que permite o seu funcionamento normal.

Entre o SASs e o SCT.

Também somente com o sistema do fabricante que possui o nível 3 são utilizados o protocolo TLS[5] para autenticação mútua e o protocolo NTP[7] com autenticação por chave de seção simétrica. As duas operações devem ser realizadas num tempo máximo de 5 segundos, sendo que se a autenticação mútua não se realizar o sincronismo não se concretiza e o SCT não recebe o certificado de atributos que permite o seu funcionamento normal.

Entre o SAS primário e o SCT.

Utilizado somente com o sistema do fabricante que não possui o nível 3, são utilizados o protocolo SSL v3.0 para autenticação mútua e o protocolo NTP[7] com autenticação por chave de seção simétrica. As duas operações devem ser realizadas num tempo máximo de 5 segundos, sendo que se a autenticação mútua não se realizar o sincronismo não se concretiza e o SCT não recebe o CAT que permite o seu funcionamento normal.

Meios de comunicação

Entre o Relógio Atômico e o gerador de IRIG B

Esta conexão se realiza por intermédio de um cabo coaxial com máximo de 2 metros de comprimento. Tanto o padrão atômico quanto o gerador de IRIG B ficam instalados fisicamente no mesmo "rack".

Entre o gerador de IRIG B e o SASp

Também realizada por intermédio de um cabo coaxial com máximo de 2 metros de comprimento. Tanto o gerador de IRIG B quanto o SASp ficam instalados fisicamente no mesmo "rack".

Entre o SASp e o SASs.

Esta conexão se realiza por intermédio da Internet, a cada 24 horas, de forma a se garantir que o êrro acumulado máximo, neste período, não ultrapasse o valor de 100 milisegundos no SASs. Tanto o SASp quanto o SASs são protegidos por firewalls internos ou externos.

Entre o SASs e os SCT.

Esta conexão se realiza por intermédio da Internet, a cada 6 horas de forma a se garantir que o êrro acumulado máximo, nestes períodos, não ultrapasse o valor de 100 milisegundos nas UCT . Tanto o SASs quanto as UCT são protegidos por firewalls internos ou externos.

Entre o SASp e os SCT.

Este tipo de conexão é realizada para o caso do fabricante que não implementa o nível 3. Ela se realiza por intermédio da Internet, a cada 20 minutos de forma a se garantir que o êrro acumulado máximo, nestes períodos não ultrapasse o valor de 100 milisegundos nos SCT . Tanto o SASp quanto os SCT são protegidos por firewalls internos ou externos.

"Logs" de autenticação/sincronização

As operações de autenticação e sincronização realizadas periodicamente são registradas em "logs" internos nos equipamentos, e estes "logs" são acessados e armazenados diariamente pelo ON. A partir destes "logs" são preenchidas planilhas eletrônicas e os cálculos em seguida efetuados permitem o acompanhamento diário dos SCT.

Certificados de autenticação/sincronização

No início de cada mês, os cálculos referentes ao mês anterior são publicados em um certificado em papel, assinado e enviado ao responsável do usuário por este setor. Caso seja necessário a emissão de algum certificado antes da emissão do certificado mensal, bastará que o usuário o solicite.

1 OBRIGAÇÕES DOS USUÁRIOS

Adquirir equipamentos

Os usuários devem adquirir os equipamentos SCT. Tais equipamentos devem ter sido homologados previamente pelo ON.

Assinar contrato

Para participar da ReTemp/HLB os usuários devem assinar contrato de prestação de serviços de acordo com modelo enviado pelo ON.

Enviar ao ON equipamento para calibração.

Ao receber os equipamentos do fabricante o usuário deverá enviá-los ao ON para que sejam calibrados. Em decorrência desta operação, o ON emitirá um certificado em papel e devolverá o equipamento devidamente lacrado e identificado ao usuário, para instalação em ambiente sob sua responsabilidade.

Instalar e testar equipamento e local de instalação.

O usuário ao receber de volta a unidade carimbadora do tempo deverá instalá-la em local adequado (com alimentação AC ininterrupta, temperatura ambiente de $25 \pm 5^{\circ}$ C, umidade relativa de 50 ± 30 %).

Após a instalação física do SCT, o usuário deve entrar em contato com o ON que enviará instruções de configuração adicionais de *firewall*, iniciando em seguida um período de testes de cerca de 5 dias, ao final do qual se poderá constatar a adequação das condições locais do usuário, no que se refere à qualidade da conexão com a Internet e confirmando o período de realização das operações de autenticação e sincronização de forma a se limitar o erro máximo acumulado ao valor de 0,1 segundos.

Operar o SCT e guardar os arquivos de carimbadas.

O usuário deve armazenar em pelo menos dois locais físicos separados os "tsr – *time stampig response*" que são arquivos[1] de cerca de 3 *kBytes* gerados pelo SCT em resposta a cada requisição de carimbada recebida.

Atender aos seus clientes quando estes solicitarem laudos.

No caso de solicitação de laudos técnicos por parte de seus clientes, o usuário deverá encaminhar ao ON um arquivo do tipo *zip* contendo cada um dos arquivos e seus respectivos *hashs* calculados por intermédio do algoritmo SHA-1. Este arquivo *zip*, juntamente com seu *hash* SHA-1 deverá ser enviado ao ON por correspondência assinado digitalmente pelo representante legal do usuário perante o ON.

2 OBRIGAÇÕES DO OBSERVATÓRIO NACIONAL

Publicar na página WEB da DSHO as especificações dos equipamentos homologados pelo ON para participar da ReTemp/HLB.

Fornecer ao usuário o modelo de contrato a ser assinado entre as partes.

Realizar a calibração inicial dos equipamentos, emitir certificado de calibração e aplicar o lacre.

Realizar os teste de instalação inicial dos equipamentos no ambiente do usuário.

Adquirir diariamente os "logs" dos equipamentos instalado nos usuários.

Manter em operação continua os equipamentos SASp e SASs, habilitando desta forma o funcionamento dos SCT de seus usuários.

Emitir e enviar mensalmente ao usuário o certificado em papel, referente ao último mês de medidas.

Emitir os laudos técnicos solicitados pelo usuário e efetuar auditorias em seus equipamentos e sistemas no que tange à ReTemp.

7 REFERÊNCIAS

1 – *RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), D. Pinkas Integris, R. Zuccherat Entrust August 2001.*

2 - *RFC 3628 - Policy Requirements for Time-Stamping Authorities (TSAs), Denis Pinkas Bull, Nick Pope, John Ross, November 2003.*

3 – *RFC 3281, An Internet Attribute Certificate Profile for Authorization INTERNET ENGINEERING TASK FORCE, 2002.*

4 – *http://www.bipm.fr/en/bipm/*

5 – *RFC 4346 - The TLS Protocol Version 1.0*

6 – *RFC 2631 - Diffie-Hellman Key Agreement Method*

7 – *RFC 1305 - Network Time Protocol (Version 3)*

8 – *RFC 4346 - Transport Layer Security (TLS) Extensions*

9 - IRIG Standard 200-89, published by the Range Commanders Council of the U.S. Army White Sands Missile Range.