



GSCT

**Gerenciador de Sistemas de
Carimbo do Tempo**

Sumário

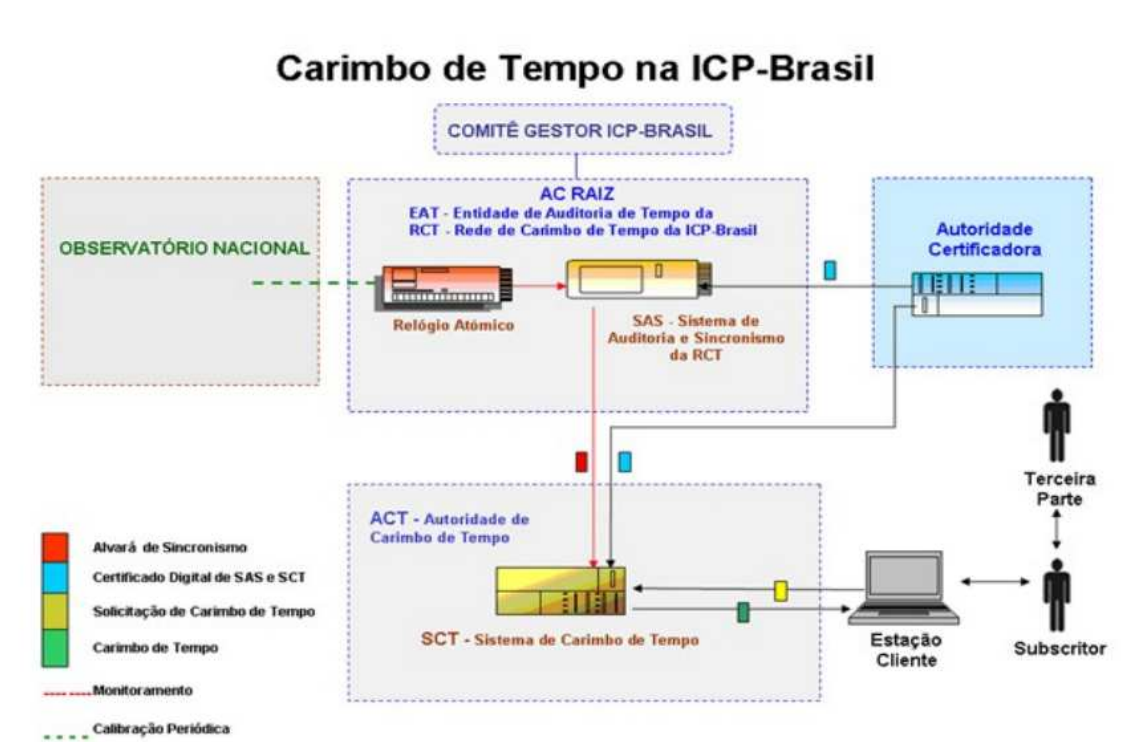
Visão Geral	4
Modelo Geral de Funcionamento do Carimbo do Tempo na ICP-Brasil	4
Sincronização do tempo	5
GSCT - Gerenciador de Sistemas de Carimbo do Tempo.....	6
Funcionalidades do GSCT	7
Customizações	7
SIGLAS	8

Visão Geral

Um carimbo do tempo aplicado a uma assinatura digital ou a um documento prova que ele já existia na data incluída no carimbo do tempo. Os carimbos de tempo são emitidos por terceiras partes confiáveis, as Autoridades de Carimbo do tempo – ACT, cujas operações devem ser devidamente documentadas e periodicamente auditadas pela própria AC-Raiz da ICP-Brasil. Os relógios dos SCTs devem ser auditados e sincronizados por Sistemas de Auditoria e Sincronismo (SASs).

A utilização de carimbos do tempo no âmbito da ICP-Brasil é facultativa. Documentos eletrônicos assinados digitalmente com chave privada correspondente a certificados ICP-Brasil são válidos com ou sem o carimbo do tempo.

Modelo Geral de Funcionamento do Carimbo do Tempo na ICP-Brasil



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.

AC-Raiz da ICP-Brasil (AC-Raiz) – Credencia, audita e fiscaliza entidades da ICPBrasil. Assina seu próprio certificado e os certificados das ACs 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 (SASs), ligados a um relógio atômico e a partir deles realiza as atividades de auditoria e sincronismo dos Servidores de Carimbo do tempo (SCTs), instalados nas ACTs.

Autoridade Certificadora (AC) - Emite, renova ou revoga certificados digitais de outras ACs ou de titulares finais. Emite e publica LCR. Na estrutura de carimbo do tempo da ICPBrasil, emite os certificados digitais usados nos equipamentos das ACTs 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 PSSs classificam-se em três categorias, conforme o tipo de atividade prestada.

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.

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.

Sincronização do tempo

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.

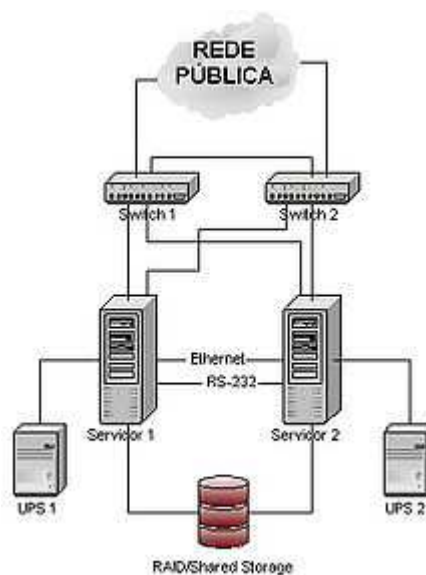
A garantia de que todos os equipamentos estejam sincronizados à hora UTC está baseada no fato de que os equipamentos que compõem a Rede de Carimbo do tempo da ICPBrasil somente receberão os respectivos alvarás se estiverem adequadamente sincronizados.

Os SASs e SCTs utilizam, para assinatura dos alvarás e carimbos do tempo e autenticação, chaves privadas vinculadas a certificados digitais ICP-Brasil, o que garante a autoria desses documentos.

GSCT - Gerenciador de Sistemas de Carimbo do Tempo

Um dos requisitos esperados de um serviço é a alta disponibilidade. Um sistema de alta disponibilidade é um sistema resistente a falhas de hardware, software e energia, cujo objetivo é manter os serviços disponibilizados o máximo de tempo possível. Cada vez mais é necessário garantir a disponibilidade de um serviço, mas sendo que muitos componentes dos sistemas de informação atuais contêm partes mecânicas, a fiabilidade destes é relativamente insuficiente se o serviço for crítico. Para garantir a ausência de interrupções de serviço é necessário, muitas vezes, dispor de hardware redundante que entre em funcionamento automaticamente quando da falha de um dos componentes em utilização.

Quanto mais redundância existir, menores serão os SPOF (*Single Point Of Failure*), e menor será a probabilidade de interrupções no serviço. Até há poucos anos tais sistemas eram muito dispendiosos, e tem-se vindo a intensificar uma procura em soluções alternativas. Surgem então os sistemas construídos com hardware acessível (*clusters*), altamente escaláveis e de custo mínimo. *Cluster* é um conceito que está diretamente relacionado aos sistemas de alta disponibilidade e que permite agregar vários computadores, ou servidores, como se fossem uma única máquina de grande porte.



Como se pode observar, não existe um único ponto nesta arquitetura que, ao falhar, implique a indisponibilidade de outro ponto qualquer (SPOF). O fato de ambos servidores se encontrarem em funcionamento e ligados à rede não implica, porém, que se encontrem a desempenhar as mesmas tarefas. Esse é uma decisão por parte do administrador e que tem o nome de balanceamento de carga.

Ao trazermos a alta disponibilidade para o ambiente do carimbo do tempo, teremos no mínimo 2 SCTs. É neste momento que surge a necessidade do GSCT, que vai gerenciar o SCT existentes.

Funcionalidades do GSCT

Cadastro de SCT – O GSCT tem uma funcionalidade para cadastro de SCT. Neste cadastro será conhecido o endereço físico do SCT, um usuário administrador, um usuário **superuser**.

Cadastro de clientes – o GSCT tem uma funcionalidade para cadastro de clientes com suas aplicações ou servidores, onde é possível implementar um controle sobre o serviço de carimbo personalizado dependendo do tipo de contrato.

Validação dos Certificados da ACT – O GSCT possui um serviço de validação dos certificados envolvidos. No caso do certificado da ACT está perto de expirar ou expirar ou for revogado, haverá avisos para o administrador da infraestrutura tomar providências. Está validação também impedirá que carimbos sejam emitidos por ACT com certificados expirados.

Balanceamento de Carga e Fail over – O GSCT vai distribuir as requisições entre os SCTs cadastrados. No caso de falha, o GSCT reenviará a mesma requisição para outro SCTs. Somente se todos os SCTs falharem, um TSR com Fault será gerado.

Registro de Eventos – O GSCT registra todos os eventos no âmbito da estrutura de carimbo de tempo.

Relatórios – o GSCT emite relatórios com base nas informações coletadas ao longo do tempo, sobre:

- Balanceamento de carga
- ACT e seus certificados
- Clientes, aplicações, contratos e carimbos por período
- Registro de eventos
- Demais relatórios customizados

Customizações

O GSCT é um serviço desenvolvido pela Tservices e pode ser customizados para atender necessidades específicas do cliente.

SIGLAS

AC - Autoridade Certificadora

AC-RAIZ - Autoridade Certificadora Raiz da ICP-Brasil

ACT - Autoridade de Carimbo do Tempo

BIPM - Bureau International des Poids et Mesures

CT - Carimbo do tempo

DPCT - Declaração de Práticas de Carimbo do tempo

EAT - Entidade de Auditoria do Tempo

FCT - Fonte Confiável do Tempo

HLB - Hora Legal do Brasil

ICP-Brasil - Infra-Estrutura de Chaves Públicas Brasileira

IETF - Internet Engineering Task Force

ISO – International Organization for Standardization

ITI - Instituto Nacional de Tecnologia da Informação

NTP - Network Time Protocol

OID - Object Identifier

ON - Observatório Nacional

PC - Políticas de Certificado

PCT - Política de Carimbo do tempo

PS - Política de Segurança

PSS - Prestadores de Serviço de Suporte

RFC – Request For Comments

SAS – Sistema de Auditoria e Sincronismo

SCT - Servidor de Carimbo do tempo

SHA - Secure Hash Algorithm

SINMETRO - Sistema Nacional de Metrologia

TSP - Time Stamp Protocol

TSQ - Requisição de Carimbo do tempo (Timestamp-query – request)

TSR – Carimbo do tempo (Timestamp response)

UTC - Tempo Universal Coordenado