

Nova solução de Carimbo de Tempo para ACTs



EXPLORE A CERTIFICAÇÃO DE TEMPO COM GESTÃO FACILITADA E EM CONFORMIDADE COM A ICP-BRASIL

A Certificação Digital tem proporcionado maior segurança para diversas aplicações, validando identidades, como usuários, dispositivos e sistemas, na realização de transações, permissão de acessos e assinaturas digitais. As soluções de Carimbo de Tempo complementam as certificações com os aspectos de validade jurídica ao atestar a data e a hora exata em que um documento eletrônico foi criado e recebeu a assinatura digital. O “selo” é emitido por uma Autoridade de Carimbo de Tempo (ACT) aprovada e homologada pela ICP-Brasil, que garante a veracidade das informações e assegura que o documento não foi adulterado em seu conteúdo original.

São várias chaves privadas e certificados envolvidos no processo de Carimbo de Tempo: os que estão dentro do HSM para emitir o CT, os da conexão TLS com os usuários, da conexão TLS com o SAS (Sistema de Auditoria e Sincronismo) e da conexão TLS do PTP (protocolo de comunicação de auditoria e sincronismo). Para facilitar a gestão de todos eles, o sistema da Kryptus oferece uma interface web, além de APIs programáticas para desenvolvimentos customizados.

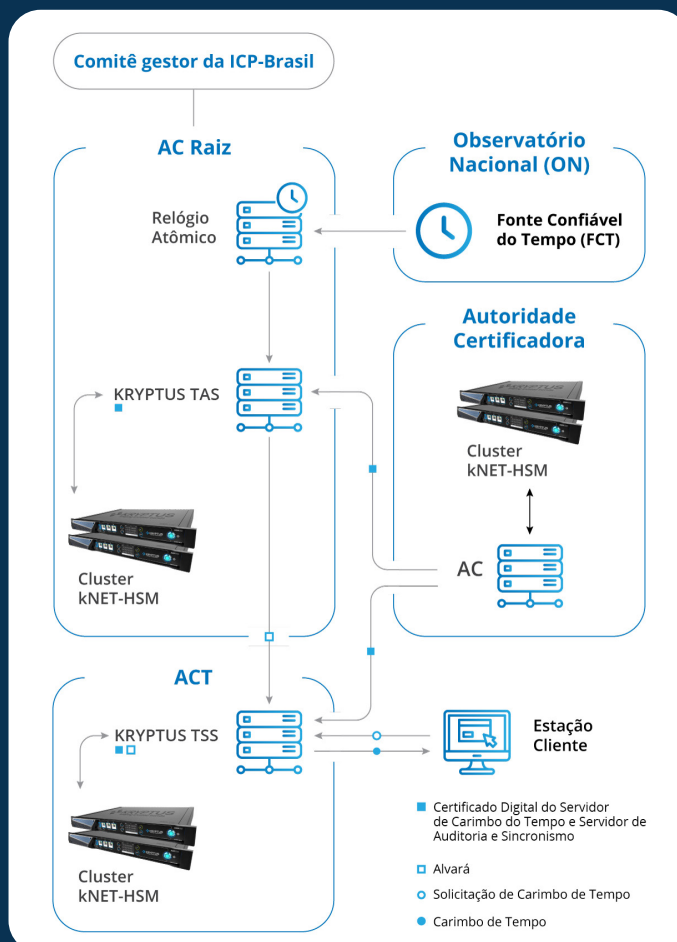
A Solução de Carimbo de Tempo da Kryptus está em conformidade com as normas do ITI e se integra nativamente com o novo Sistema de Auditoria e Sincronismo da ICP-Brasil, fornecido pela Kryptus como Kryptus TAS.

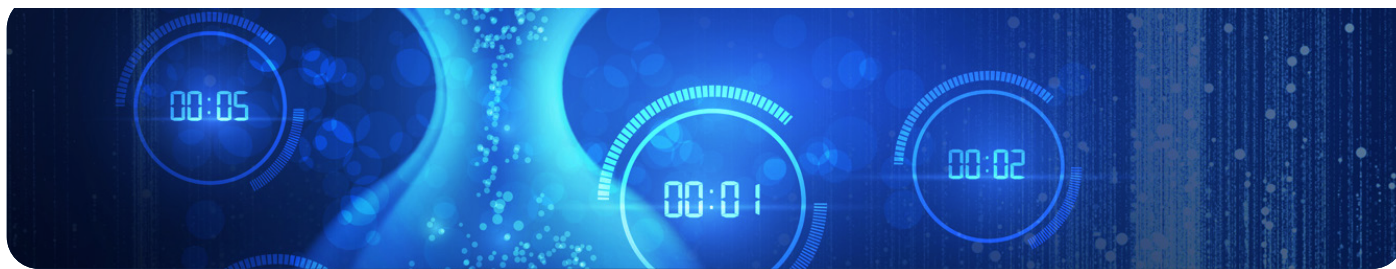
Para as ACTs, a Kryptus traz o Kryptus TSS: Solução de Carimbo de Tempo, composta por Servidor de Carimbo de Tempo (SCT), Módulo de Segurança Criptográfico (kNET HSM), Software embarcado com todas as funcionalidades de gestão e emissão dos carimbos de tempo, além de interfaces de comunicação. O kNET HSM é responsável pela proteção de chaves criptográficas do Kryptus TSS, realizando o registro de todos os dados de sincronismo e registro das assinaturas de carimbo de tempo.

Kryptus TSS

- Servidor de Carimbo de Tempo (SCT)
- kNET HSM para armazenamento seguro e assinatura (Timestamp e Alvará), compartilhável entre vários SCTs
- Sistemas de gestão externos
- Portal Web de administração
- Alertas por e-mail
- Envio automático de logs Syslog
- Logs disponíveis para download
- Alta performance e disponibilidade
- Em conformidade com as normas ICP-Brasil

Homologação de Carimbo do Tempo no âmbito da ICP-Brasil





ESPECIFICAÇÕES TÉCNICAS

CONFORMIDADE

Conformidade integral com as normas para Sistema de Carimbo de Tempo em suas últimas versões:

- DOC-ICP-11 – v2.0
- DOC-ICP-11.01 – v1.0
- DOC-ICP-12 – v2.0
- DOC-ICP-12.01 – v2.0
- DOC-ICP-13 – v2.0
- DOC-ICP-14 – v2.0
- Manual de Condutas Técnicas MCT 10 Volume I – v2.0 (Atende aos Requisitos)

PERFORMANCE E CAPACIDADE

- Performance de até 9000 (nove mil) assinaturas RSA 2048 por segundo.

CONECTIVIDADE

- HSM e Servidor (opcional): Interface de rede padrão Ethernet

INTERFACE DE USUÁRIO

- HSM: Display Frontal

RECURSOS

- Emissão de carimbos de tempo na mesma ordem em que são recebidas;
- Formato de Tempo: UTC;
- Garante a irretroatividade na emissão de carimbos de tempo.
- Alertas por e-mail
- Logs diversos disponíveis para download;
- Portal de Administração – Página Web
 - Implementado com SSL/TLS;
 - Cadastro de 3 (três) níveis de usuários – auditor, administrador e operador;
 - Configuração de acesso de cada funcionalidade a um ou mais níveis de usuários. (Apenas usuários administradores);
 - Autenticação do usuário por login/senha e certificado digital;
 - Permite a auditoria e sincronismo apenas de sistemas de auditoria e sincronismo cadastrado, identificados por seus certificados digitais;
 - Permite o download do alvará vigente;
 - Permite a solicitação manual de sincronismo e auditoria ao sistema auditor cadastrado, com emissão de um novo alvará em caso de sucesso;
 - Permite a visualização, edição, e exclusão de dados dos sistemas auditores cadastrados;

- Pesquisa dos alvarás recebidos por endereço IP do auditor, data, hash e número do alvará;
- Permite a definição dos seguintes níveis de log:
- Repositório confiável para armazenamento dos certificados digitais das autoridades certificadoras pertencentes às cadeias de certificação dos certificados digitais de usuários e equipamentos cadastrados;
- Permite listar e realizar o download de todos os certificados digitais confiáveis cadastrados;
- Atualização automática das listas de certificados digitais revogados dos certificados digitais cadastrados e armazenamento na base de dados;
- Cadastramento de certificado digital para conexão segura no portal de administração web, através de túnel seguro HTTPS;
- Permite o cadastramento de certificado digital para assinatura dos carimbos de tempo emitidos;
- Permite listar e realizar download de todos os certificados digitais para assinatura dos carimbos de tempo emitidos;
- Alertas aos usuários em caso do certificado sendo cadastrado não possua o propósito de uso estendido referente a assinatura de carimbos de tempo (id-kp-timeStamping), na extensão Extended Key Usage, conforme DOC-ICP-05;
- Mecanismo de gerenciamento de ciclo de vida de chaves privadas;
- Permite a geração de par de chaves criptográficas;
- Permite a geração de requisição de certificado digital;
- Permite a exclusão de requisição de certificado digital;
- Permite a renovação de certificado digital;
- Permite a instalação de certificado digital;
- Permite gerenciamento de interface de rede;
- Permite configuração de servidores DNS e proxy;
- Permite gerenciamento de rotas estáticas de rede;
- Permite configuração de servidor de e-mail para envio de mensagens;
- Atualização de firmware – assinado pela Kryptus
- Permite o envio automático de registros de eventos através do protocolo Syslog – RFC 5424;
- SNMP v3 (RFC 1157).

OUTROS RECURSOS

- Manuais e documentos técnicos redigidos em português e inglês.

ESPECIFICAÇÕES FÍSICAS

- 19" Rack mount 1U (somente HSM) ou 2U (1U + 1U, com servidor)
- Consumo de energia: 1020W (HSM: 300W, servidor: 720W)
- Temperatura de operação: 0°C até 40°C
- Temperatura de armazenamento: -40°C até 65°C
- Fonte de alimentação Bivolt



HQ

+55 (19) 3112-5000

faleconosco@kryptus.com
www.kryptus.com

Rua Maria Teresa Dias da Silva 270
Campinas – SP, Brazil

EMEA

+41 79 932 19 23

kryptus.emea@kryptus.com
emea.kryptus.com

Rue Gallinée 7, 1400, Yverdon
Switzerland



6018V9



Grande Réseau pour le Matériel de Défense et de Sécurité