INSTRUÇÃO NORMATIVA ITI N° 17, DE 07 DE OUTUBRO DE 2021

Aprova a versão 1.0 do documento Protocolos de Auditoria e Sincronismo do Tempo da Rede de Carimbo do Tempo da ICP-Brasil – DOC-ICP-11.02.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso VI do art. 9° do anexo I do Decreto n° 8.985, de 8 de fevereiro de 2017, pelo art. 1° da Resolução n° 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004, e pelo art. 2° da Resolução n° 163 do Comitê Gestor da ICP-Brasil, de 17 de abril de 2020, de 17 de abril de 2020,

RESOLVE:

Art. 1° Aprovar a versão 1.0 do documento DOC-ICP-11.02 – Protocolos de Auditoria e Sincronismo do Tempo da Rede de Carimbo do Tempo da ICP-Brasil.

Art. 2° Os interessados deverão obter do Instituto Nacional de Tecnologia da Informação a autorização para promover suas implementações nos protocolos de auditoria e sincronismo de tempo.

Art. 3° Esta Instrução Normativa entra em vigor em 1° de novembro de 2021.

CARLOS ROBERTO FORTNER

Assinado de forma digital por CARLOS ROBERTO FORTNER
Dados: 2021.10.07 15:47:27 -03'00'

CARLOS ROBERTO FORTNER

Infraestrutura de Chaves Públicas Brasileira

ANEXO

PROTOCOLOS DE AUDITORIA E SINCRONISMO DO TEMPO DA REDE DE CARIMBO DO TEMPO DA ICP-BRASIL

DOC-ICP-11.02

Versão 1.0

07 de outubro de 2021

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Ato que aprovou a alteração	Item alterado	Descrição da alteração
IN ITI nº 17, de 07.10.2021 Versão 1.0		Aprova a versão 1.0 do documento Protocolos de Auditoria e Sincronismo do Tempo da Rede de Carimbo do Tempo da ICP-Brasil.

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
DER	*Distinguished Encoding Rules*
EAT	Entidade de Auditoria do Tempo
FCT	Fonte Confiável do Tempo
HTTPS	*Hypertext Transfer Protocol Secure*
JSON	*JavaScript Object Notation*
MCT	Manual de Condutas Técnicas
PTP	*Precision Time Protocol*
RCT	Rede de Carimbo do Tempo
RFC	*Request For Comments*
SAS	Sistema de Auditoria e Sincronismo
SCT	Servidor de Carimbo do Tempo
TCR	*Time Calibration Report*
TCT	*Time Chaining Tree*
TLS	*Transport Layer Security*
VPN	*Virtual Private Network*

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

1.1 Este documento descreve os protocolos de auditoria e sincronismo do tempo da Rede de Carimbo do Tempo – RCT da ICP-Brasil e serve como referência para as implementações dos Servidores de Carimbo do Tempo – SCT e Sistemas de Auditoria e Sincronismo – SAS que desejam operar na RCT da ICP-Brasil.

1.2 Este documento é um complemento aos documentos que especificam o padrão para carimbos do tempo na ICP-Brasil, incluindo, mas não limitado aos seguintes documentos:

a) VISÃO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA ICP-BRASIL [1];

b) REDE DE CARIMBO DO TEMPO NA ICP-BRASIL – RECURSOS TÉCNICOS [2];

c) REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL [3];

d) REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO DA ICP-BRASIL [4];

e) PROCEDIMENTOS PARA AUDITORIA DO TEMPO DA ICP-BRASIL [5];

f) MANUAL DE CONDUTAS TÉCNICAS 10 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE CARIMBO DO TEMPO NO ÂMBITO DA ICP-BRASIL [6], e

g) MANUAL DE CONDUTAS TÉCNICAS 10 – VOLUME II: PROCEDIMENTOS DE ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE DE CARIMBO DO TEMPO NO ÂMBITO DA ICP-BRASIL [7].

1.3 Visão Geral do Sistema

1.3.1 A Rede de Carimbo do Tempo da ICP-Brasil é formada por Autoridades de Carimbo do Tempo – ACTs que utilizam relógios de tempo real, do inglês *real time clock* – RTC, confiáveis - sincronizados e auditados pela Entidade de Auditoria do Tempo – EAT, para emitir carimbos do tempo para os usuários da ICP-Brasil.

1.3.2 As funções de emissão de carimbos do tempo, sincronia do tempo e auditoria do tempo das ACTs são realizadas por Servidores de Carimbo do Tempo – SCT, enquanto as funções de sincronia e auditoria do tempo providas pela ACT são realizadas por Sistemas de Auditoria e Sincronismo – SAS.

1.3.3 Servidores de Carimbo do Tempo são computadores especializados capazes de:

a) manter seus relógios internos sincronizados com o relógio do SAS;

b) manter registro da qualidade do sincronismo dos seus relógios internos com o relógio do SAS;

c) submeter os registros de qualidade de sincronismo do tempo ao processo de auditoria realizado pelo SAS;

d) solicitar a emissão de alvarás de funcionamento ao SAS; e

e) emitir carimbos do tempo, entre outras funcionalidades.

1.3.4 Sistemas de Auditoria e Sincronismo são computadores especializados capazes de:

a) manter seus relógios internos sincronizados com a Fonte Confiável de Tempo – FCT;

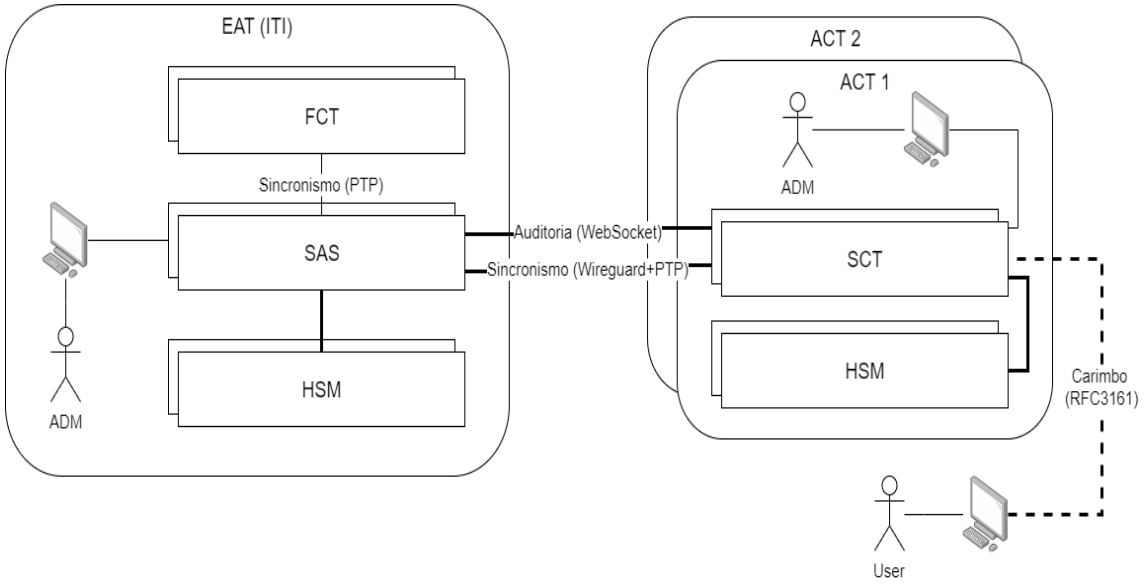
b) utilizar seus relógios internos para prover uma fonte de sincronismo do tempo para relógios dos SCTs;

c) auditar a qualidade do sincronismo dos relógios dos SCTs; e

d) emitir alvarás de funcionamento para SCTs, entre outras funcionalidades.

1.3.5 A Figura 1 ilustra os componentes que formam a RCT e seus relacionamentos, com destaque para os protocolos de auditoria e sincronismo executados entre SAS e SCT, que são o escopo deste documento e detalhados nos itens 2 e 3.

Figura 1: Componentes da RCT e suas Relações



1.4 Isenção de Responsabilidade

1.4.1 Termos e Condições Gerais de Utilização do Protocolo de Auditoria e Sincronismo

A utilização do protocolo de auditoria e sincronismo, referido também neste documento como "protocolo" ou "protocolos", implica a aceitação plena e completa das condições gerais de utilização descritas abaixo. Estes termos de uso ou avisos legais podem ser modificados ou complementados a

qualquer momento, pelo que os utilizadores dos protocolos são convidados a consultá-los regularmente.

1.4.2 Descrição dos Protocolos

A AC Raiz da ICP-Brasil atua como Entidade de Auditoria do Tempo – EAT, operando Sistemas de Auditoria e Sincronismo – SAS, que inspecionam permanentemente os equipamentos das Autoridades de Carimbo do Tempo e os Servidores de Carimbo do Tempo – SCT. Esta atribuição é exclusiva da AC Raiz, sendo que estes equipamentos – SAS e SCT – compõem a Rede de Carimbo do Tempo – RCT da ICP-Brasil.

1.4.3 Créditos

1.4.3.1 O ITI adquiriu os direitos de utilização no âmbito da ICP-Brasil dos protocolos computacionais de Carimbo do Tempo, sejam modelos de dados e/ou base de dados oriundos dos protocolos.

1.4.3.2 É proibido modificar (ainda que para fins de correção de erro), adaptar ou traduzir os protocolos ou criar trabalhos originários dos mesmos, a descompilação reversa (inclusive compilação reversa para assegurar a interoperabilidade), engenharia reversa ou testes de segurança e outra derivação dos protocolos.

1.4.3.3 Qualquer utilização não autorizada dos protocolos ou de qualquer elemento neles contidos será considerada uma infração e processada de acordo com as disposições da Lei nº 9.279, de 14 de maio de 1996 (Lei de Propriedade Industrial).

2 PROTOCOLO DE SINCRONISMO DO TEMPO

2.1 Disposições Gerais

2.1.1 A RCT da ICP-Brasil utiliza o protocolo de sincronismo do tempo *Precision Time Protocol* – PTP, versão 2, especificado pelo padrão IEEE-1588 2008 [8], para prover o mecanismo de sincronia do tempo entre SAS e SCT. Neste documento é utilizado o termo Rede PTP para se referir à rede de computadores na qual o PTP é executado.

2.1.2 Para assegurar a autenticidade das mensagens trocadas pela Rede PTP, o SAS utiliza uma rede virtual privada, do inglês *Virtual Private Network* – VPN, que provê um canal de comunicação cifrado e autenticado para os pacotes que transitam por essa rede. A implementação de VPN utilizada pelo SAS é a do Wireguard [13], compatível com sua implementação de referência para Linux na versão 1.0.

2.1.3 Nos itens a seguir é descrito como cada um desses protocolos é utilizado no contexto da RCT da ICP-Brasil.

2.2 Rede Virtual Privada

2.2.1 O SAS e SCT devem se conectar à VPN utilizando uma implementação do *Wireguard* [13] que seja compatível com sua implementação de referência para Linux na versão 1.0.

2.2.2 O SAS deve ter a VPN Wireguard configurada para operar como servidor, escutando IP e porta configurada pelo administrador do SAS.

2.2.3 O SAS deve prover ao SCT, por meio de mensagens para Registro na Rede PTP (ver mensagem ptp_network_response no item 3) ou por meios externos ao protocolo (out-of-bounds):

a) a chave pública do servidor VPN do SAS;

b) o endereço IP do servidor VPN do SAS (e.g.: 30.0.0.1);

c) a porta do servidor VPN do SAS (e.g.: 51820);

d) o endereço IP e máscara de rede da VPN reservada para o SCT (e.g.: 20.0.0.2/24);

e) o endereço IP e máscara de rede da rede PTP reservada para o SCT (e.g.: 10.0.0.2/24);

f) o endereço IP e máscara de rede da VPN reservada para o SAS (e.g.: 20.0.0.1/24);

g) o endereço IP e máscara de rede da rede PTP reservada para o SAS (e.g.: 10.0.0.1/24).

2.2.4 O SCT deve prover ao SAS, por meio de mensagens para Registro na Rede PTP (ver mensagem ptp_network_request no item 3) ou por meios externos ao protocolo (out-of-bounds):

a) a chave pública do cliente VPN do SCT.

2.2.5 O SCT deve ter a VPN Wireguard configurada para operar como cliente, conectado no IP e porta do servidor VPN do SAS.

2.2.6 Após a troca de informações com o SCT, o SAS deve adicionar o SCT como peer da rede VPN, conforme exemplificado pela configuração de peer do Wireguard, abaixo (os IPs, máscaras de rede e portas são exemplos ilustrativos):

[Peer]

PublicKey = <chave-pública-do-sct>

AllowedIPs = 20.0.0.2/24, 10.0.0.2/24

2.2.7 Após a troca de informações com o SAS, o SCT deve adicionar o SAS como peer da rede VPN, conforme exemplificado pela configuração de peer do Wireguard, abaixo (os IPs, máscaras de rede e portas são exemplos ilustrativos):

[Peer]

PublicKey = <chave-pública-do-sas>

Endpoint = 30.0.0.1:51820

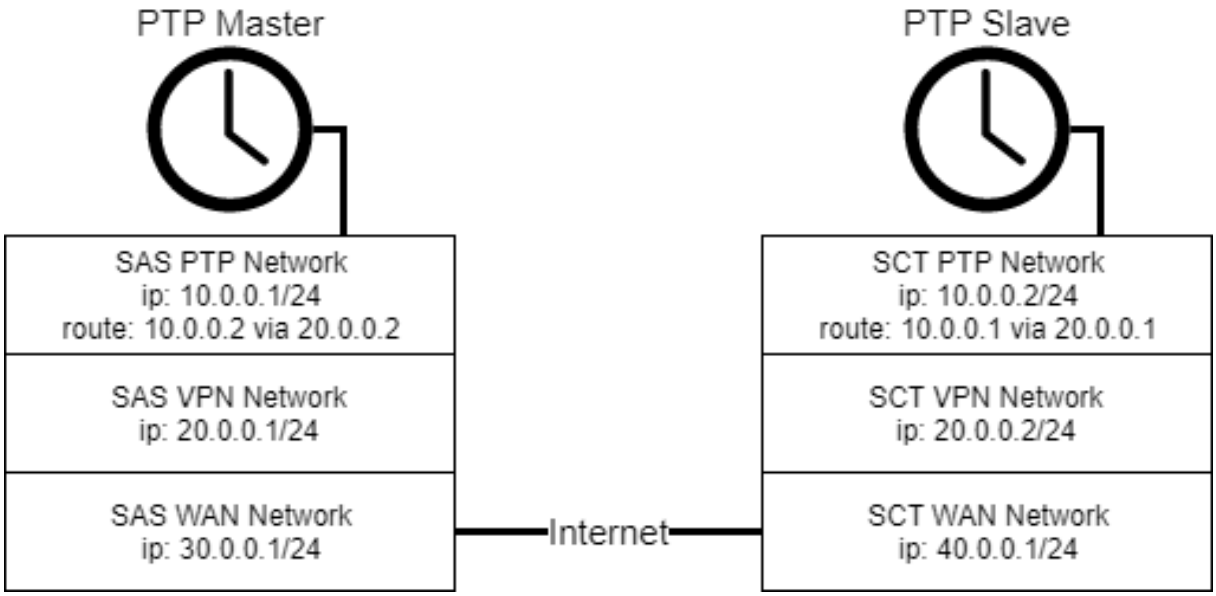
AllowedIPs = 20.0.0.1/24, 10.0.0.1/24

2.2.8 O SCT deve gerar o par de chaves da VPN, pública e privada, conforme definido pelo padrão do Wireguard.

2.2.9 Todas as demais configurações do Wireguard do SAS e SCT devem ser a padrão do protocolo.

2.2.10 Todo tráfego da Rede PTP deve ser roteado por meio da VPN, conforme exemplificado na Figura 2 (os IPs, máscaras de rede e portas são exemplos ilustrativos).

Figura 2: Organização das Redes e Rotas



2.3 Precision Time Protocol

2.3.1 O SAS e SCT devem utilizar uma implementação em *hardware* do PTP que atenda o padrão IEEE-1588 2008 [8].

2.3.2 O SAS deve prover ao SCT, por meio de mensagens para Registro na Rede PTP (ver ptp_network_response no item 3) ou por meios externos ao protocolo (out-of-bounds):

a) O endereço IP do SAS na rede PTP.

2.3.3 O SAS deve utilizar as seguintes configurações para o servidor de sincronismo do tempo:

a) Modo: master

b) Fonte do carimbo do tempo: hardware

c) Protocolo de Transporte: UDP IPv4

d) Tipo de Comunicação: unicast

e) Mecanismo de *delay*: end-to-end

2.3.4 O SCT deve utilizar as seguintes configurações para o cliente de sincronismo do tempo:

a) Modo: *slave*

b) Fonte do carimbo do tempo: hardware

c) Protocolo de Transporte: UDP IPv4

d) Tipo de Comunicação: unicast

e) Mecanismo de *delay*: end-to-end

f) Endereço do *master clock*: endereço IP do SAS na rede PTP.

2.3.5 Durante a execução do protocolo PTP, o SCT deve armazenar em *log* o *delay* e offset calculados para o ajuste do relógio do SCT. A frequência de geração desses *logs* deve ser suficiente para atender os parâmetros de auditoria especificados pelo administrador do SAS para o SCT (ver item 3.7).

3 PROTOCOLO DE AUDITORIA DE TEMPO

3.1 Disposições Gerais

3.1.1 De forma a garantir o correto funcionamento e a confiabilidade dos relógios utilizados por SCTs para a emissão de carimbos do tempo no âmbito da Rede de Carimbos do Tempo da ICP-Brasil, é necessário um procedimento que ateste a qualidade dos relógios dos SCTs de forma periódica. Tal procedimento é chamado de Auditoria do Tempo e é realizado pelo Sistema de Auditoria e Sincronismo – SAS.

3.1.2 A auditoria consiste na troca de uma série de mensagens entre o SAS e o SCT, a fim de realizar uma análise estatística de desempenho do relógio do SCT a partir dos registros de sincronismo realizados por meio do protocolo PTP. O procedimento também realiza a validação dos carimbos do tempo emitidos pelo SCT desde a última auditoria.

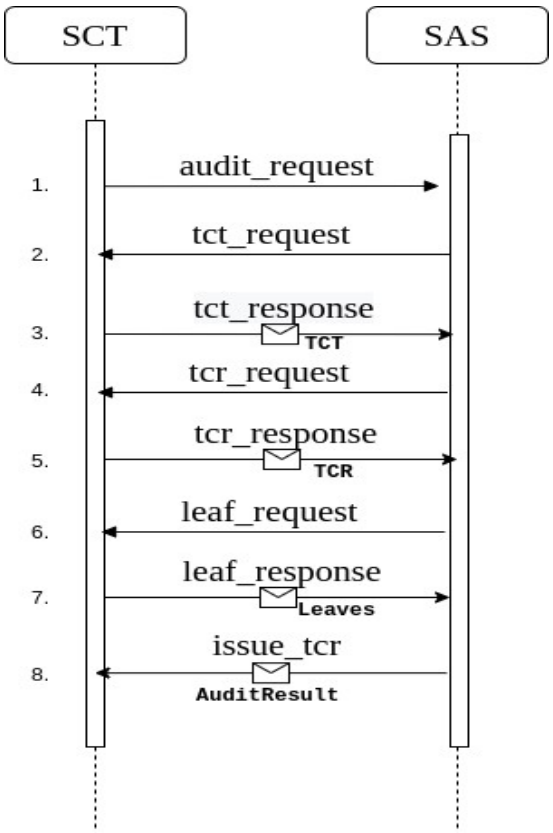
3.1.3 Uma auditoria deve ser iniciada a pedido do SCT e finaliza com a emissão de um alvará (*Time Calibration Report* - TCR) pelo SAS. O alvará emitido ao final da auditoria pode conter um período de validade maior que zero, permitindo a operação normal do SCT, ou um período de validade igual a zero, para o caso em que o SCT não esteja de acordo com os parâmetros de qualidade da auditoria configurados no SAS conforme item 3.7.

3.1.4 Durante o processo de auditoria, o SCT deve parar a emissão de carimbos do tempo e o registro de *logs* de sincronismo de forma a manter a consistência dos registros nas Árvores de Encadeamento do Tempo a serem analisados pelo SAS.

3.1.5 Entre o início e o fim da auditoria, são realizadas validações pelo SAS sobre os dados recebidos pelo SCT. Em caso de inconsistências nos dados, falhas internas ou perdas de conexão, o SAS abortará o processo de auditoria e o SCT deve resumir sua operação após um período sem resposta do SAS.

3.2 Visão Geral do Protocolo de Auditoria de Tempo

Figura 3: Troca de mensagens entre SAS e SCT durante processo de auditoria



3.2.1 O procedimento de auditoria é ilustrado pela Figura 3 e pode ser descrito da seguinte maneira:

a) o SCT inicia o processo de auditoria enviando uma mensagem de audit_request;

b) com o processo iniciado, o SAS realiza a requisição da Árvore de Encadeamento do Tempo para o SCT com uma mensagem de tct_request;

c) o SCT deve então finalizar a sua Árvore de Encadeamento do Tempo atual, parar a emissão de carimbos até o final do processo de auditoria e enviar a árvore ao SAS por meio de uma mensagem de código tct_response;

d) o SAS irá analisar a árvore recebida e requisitará, por meio de uma mensagem de tcr_request, o alvará vigente correspondente ao período dos registros na árvore;

e) o SCT então deve enviar seu último alvará vigente válido (i.e. com validade maior que zero) para o SAS por meio de uma mensagem de tcr_response;

   i. para o caso da primeira árvore de encadeamento onde não há um alvará anterior, o SCT deve enviar a mensagem de tcr_response sem nenhum conteúdo.

f) com o recebimento do alvará, o SAS irá requisitar os dados (folhas da Árvore de Merkle) utilizados para a construção da Árvore de Encadeamento do Tempo por meio de uma mensagem de leaf_request;

g) o SCT então envia todos os dados de sincronismo e carimbos emitidos correspondentes a Árvore de Encadeamento do Tempo por meio de uma mensagem de leaf_response;

h) o SAS então realiza a análise de todos os registros de sincronismo e carimbos do tempo, validando, dentre outras coisas:

   i. a reconstrução da Árvore de Merkle a partir das folhas;

   ii. qualidade do sincronismo de acordo com os parâmetros de auditoria descritos no item 3.7;

   iii. a compatibilidade do alvará presente nos carimbos do tempo emitidos com o fornecido no passo descrito na alínea "e";

3.2.2 Em caso de conformidade com todos os parâmetros de auditoria, o SAS irá emitir um alvará com validade maior que zero. Caso contrário, o SAS emitirá um alvará com período de validade zero, juntamente com a razão da rejeição da concessão do alvará. Em ambos os casos, o alvará também é acompanhado de um indicador do resultado da auditoria.

3.3 Protocolo de Comunicação

3.3.1 A comunicação com o serviço de auditoria do SAS deve ser realizada por meio do protocolo WebSocket, conforme definido pela RFC 6455 [11], sobre uma conexão TLS v1.3 (RFC 8446 [12]) ou posterior.

3.3.2 Todas as mensagens trocadas entre SAS e SCT pelo canal WebSocket devem ser codificadas em formato JSON.

3.3.3 O SAS deve escutar por requisições de conexão HTTPS (*Hypertext Transfer Protocol Secure*) na porta 443 no caminho "/auditor" (e.g.: https://domain.com/auditor).

3.3.4 O SCT deve estabelecer a conexão neste endereço e em seguida requisitar um upgrade da conexão para um WebSocket Seguro (WSS), conforme especificado pela RFC 6455 [11].

3.3.5 O estabelecimento da conexão entre os sistemas é feito com uma autenticação mútua por meio do protocolo TLS.

3.3.6 Para permitir a autenticação mútua por meio do protocolo TLS, o SAS deve prover ao SCT por um canal autenticado externo ao protocolo (out-of-bounds):

a) a lista de certificados raízes utilizados para a autenticação de seus servidores TLS; e

b) o endereço IP ou *hostname* do servidor de auditoria do SAS.

3.3.7 Para permitir a autenticação mútua por meio do protocolo TLS, O SCT deve prover ao SAS por um canal autenticado externo ao protocolo (out-of-bounds):

a) o certificado de autenticação TLS do SCT; e

b) o endereço IP que será utilizado para a conexão com o SAS.

3.4 Mensagens do Protocolo de Auditoria de Tempo

3.4.1 No protocolo de auditoria entre SAS e SCT serão trocadas mensagens em formato JSON com os seguintes campos:

Tabela 1: Formato das Mensagens do Protocolo de Auditoria

Tag	Tipo	Descrição
"operation"	string	A string identificadora da operação (vide Tabela 2)
"content"	TCT/TCR/Leaves/AuditResult	Estrutura de dados ou vazio
"error"	string	Erro associado à operação ou vazio

3.4.2 Os possíveis códigos para operação de auditoria estão definidos na Tabela 2.

Tabela 2: Códigos de Operação Utilizados no Processo de Auditoria

#	"operation"	"content"	Descrição
1	audit_request	Vazio	Operação para requisitar o início do processo de auditoria
2	tct_request	Vazio	Requisição de envio da Árvore de Encadeamento do Tempo
3	tct_response	TCT (item 3.5.2.1) em Base64	Envio da Árvore de Encadeamento do Tempo finalizada
4	tcr_request	Vazio	Requisição de envio do alvará

#	"operation"	"content"	Descrição
			vigente para verificação
5	tcr_response	TCR (item 3.5.2.2) vigente em Base64	Envio do alvará vigente
6	leaf_request	Vazio	Requisição de envio dos dados utilizados para construir a Árvore de Merkle
7	leaf_response	Leaves (item 3.5.2.3)	Envio dos dados (carimbos do tempo e eventos de sincronização) com seus respectivos índices na Árvore de Merkle
8	issue_tcr	AuditResult (item 3.5.2.4)	Emissão e envio do novo alvará, junto do resultado da auditoria e razão de rejeição, caso exista.
9	force_audit_request	Vazio	Pedido de execução de auditoria fora de período
10	force_audit_response	Vazio	Confirmação de recebimento do pedido da execução de auditoria fora de período
11	ptp_network_request	PTPClientRequest (Anexo item 1.4 Estrutura de dados PTPClientRequest)	Pedido de registro do SCT na VPN e na rede PTP.
12	ptp_network_response	PTPServerResponse (Anexo item 1.5 Estrutura de dados PTPServerResponse)	Confirmação do registro da chave pública Wireguard e envio dos dados

#	“operation”	“content”	Descrição
			necessários para o SCT se conectar na VPN e na Rede PTP.

3.4.3 Os códigos de 1 a 10 descritos pela Tabela 2 correspondem às operações de mensagens trocadas durante o procedimento de auditoria. Adicionalmente, também estão presentes na tabela os códigos 11 e 12, utilizados para o registro do SCT na rede PTP. A definição das estruturas externas ao protocolo de auditoria estão presentes no Anexo.

3.5 Estruturas de Dados no Protocolo de Auditoria

3.5.1 Conforme descrito no item anterior, existem 4 tipos de estruturas utilizadas no protocolo de auditoria:

a) TCT;

b) TCR;

c) Leaves;

d) AuditResult.

3.5.2 Neste item, serão apresentadas as definições de cada estrutura acima, assim como a codificação necessária para o envio delas durante a auditoria.

3.5.2.1 Estrutura de Dados TCT

3.5.2.1.1 Conforme descrito pelo DOC-ICP-11.01 [2], a auditoria realizada pelo SAS se dá por meio do uso das chamadas Árvores de Encadeamento de Tempo (*Time Chaining Trees* - TCT) onde estarão contidas informações relativas aos últimos carimbos emitidos e registros de sincronização realizados pelo SCT desde a última auditoria.

3.5.2.1.2 De forma a padronizar a formatação das TCTs para haver consistências nos resumos criptográficos, a TCT deve possuir a estrutura definida pela Tabela 3.

Tabela 3: Estrutura de dados TCT

Req	Campo	Tipo	Tamanho	Descrição
I	finishTs	int64	8 bytes	Unix timestamp com precisão de nanosegundos
Ii	sequenceNumber	uint32	4 bytes	Número sequencial da Árvore de Encadeamento do Tempo codificada em *Big Endian*
Iii	leafCount	uint32	4 bytes	Número de transações (folhas da Árvore de Merkle) codificado em *Big Endian*
Iv	bitSize	uint32	4 bytes	Tamanho da Árvore de Encadeamento do Tempo codificada em *Big Endian*
V	merkleRoot	byte[32]	32 bytes	Resumo criptográfico da Árvore de Merkle - (SHA-256)
Vi	prevHash	byte[32]	32 bytes	Resumo criptográfico do bloco anterior em *Big Endian* - (SHA-256)
Vii	currHash	byte[32]	32 bytes	Resumo criptográfico do bloco atual em *Big Endian* - (SHA-256)

3.5.2.1.2.1 Na Tabela 3, a coluna “Req” é referente aos requisitos definidos pelo DOC-ICP-11.01 [2], e há uma correspondência entre cada um dos requisitos e o tipo, tamanho e formatação dos campos da TCT. Para o envio da TCT como conteúdo durante o processo de auditoria na mensagem de tct_response, o valor binário (conforme a Tabela 3) da TCT deve ser codificado em Base64 para a inclusão no campo content.

3.5.2.1.3 Árvore de Merkle

3.5.2.1.3.1 Com o objetivo de realizar a conexão entre os registros de sincronismo e carimbos do tempo emitidos com a TCT, é necessário a construção de uma Árvore de Merkle a fim de resumir criptograficamente todos os registros do período analisado em um único valor.

3.5.2.1.3.2 A construção da Árvore de Merkle se dá da seguinte forma:

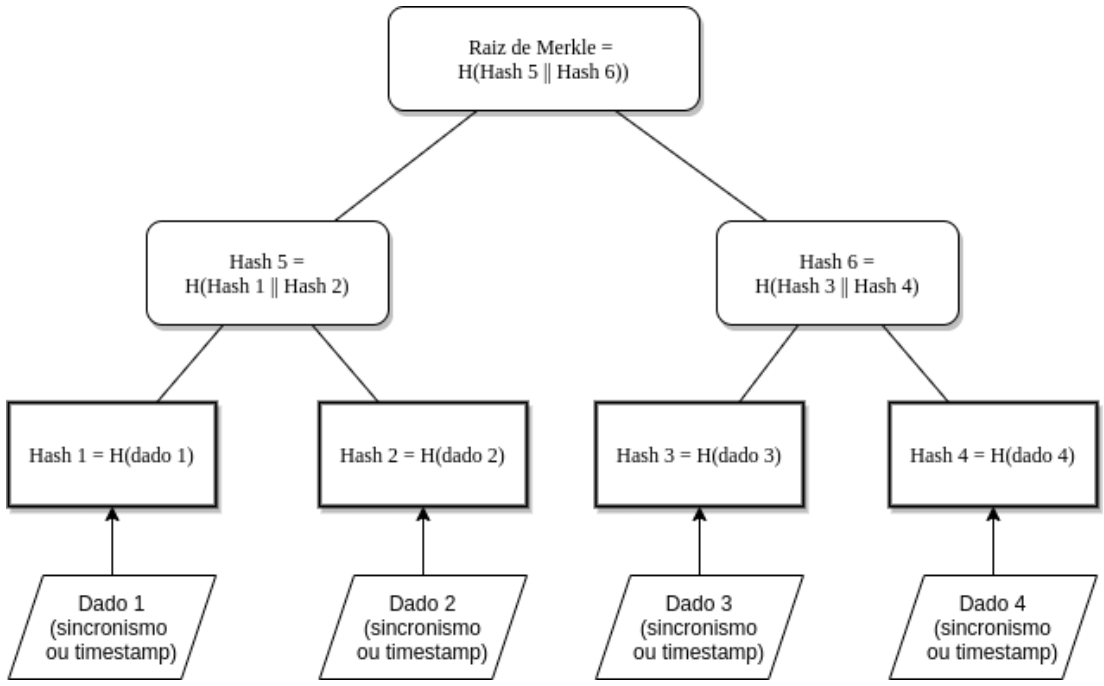
a) cada dado de entrada (carimbo do tempo ou evento de sincronização, conforme item 3.5.2.3) é resumido criptograficamente utilizando o algoritmo SHA-256;

b) cada nó pai da árvore é construído como o resumo criptográfico da concatenação de seus respectivos filhos, vide Figura 4.

   i. caso o número de folhas seja ímpar, é necessário duplicar a última folha para construir o seu nó pai.

c) o passo descrito na alínea "b" é repetido até que se chegue a um único resumo, denominado de raiz da Árvore de Merkle (ou Raiz de Merkle).

Figura 4:Exemplo de uma Árvore de Merkle



3.5.2.2 Estrutura de Dados TCR

3.5.2.2.1 O Alvará, ou *Time Calibration Report* - TCR, para a autorização de funcionamento dos SCTs deve seguir a especificação descrita pela RFC 5755 [10] juntamente com o Manual de Condutas Técnicas - MCT 10 [6].

3.5.2.2.2 Conforme a Recomendação V.1 presente no MCT 10 [6], para evitar problemas na interpretação do campo *holder* do alvará, o SAS utilizará exclusivamente a opção baseCertificateID, contendo o número de série e o nome do Emissor do certificado de autenticação do SCT.

3.5.2.2.3 A codificação do alvará emitido pelo SAS é feita em formato ASN.1 em formato DER (*Distinguished Encoding Rules*), e a definição dos atributos utilizados no alvará se dá da seguinte maneira:

Tabela 4: OIDs utilizados para os atributos do TCR

OID	Atributo	Descrição
1.3.6.1.4.1.44588.100.4.1.1	Delay	Delay médio durante o período analisado pela auditoria
1.3.6.1.4.1.44588.100.4.1.2	OffSet	Offset médio durante o período analisado pela auditoria
1.3.6.1.4.1.44588.100.4.1.3	Max Offset	Offset máximo permitido pela auditoria
1.3.6.1.4.1.44588.100.4.1.4	Status	Status resultante do processo de auditoria
1.3.6.1.4.1.44588.100.4.1.5	Max Delay	Delay máximo permitido pela auditoria
1.3.6.1.4.1.44588.100.4.1.6	Agendamento do *leap second*	Quando presente, contém a data de agendamento do segundo adicionado para compensar o atraso da rotação da Terra e manter a hora UTC em sincronismo com o tempo solar
1.3.6.1.4.1.44588.100.4.1.7	*Hash* atual da TCT	Resumo criptográfico da Árvore de Encadeamento do Tempo utilizada no processo de auditoria.

3.5.2.2.4 Adicionalmente, para a inclusão do alvará como uma extensão do timestamp, conforme o Requisito I.2 do MCT 10 [6], é necessário o uso do seguinte OID:

Tabela 5: OID para inclusão do TCR como uma extensão do Timestamp

OID	Extensão	Descrição
1.3.6.1.4.1.44588.100.4.2.1	Alvará	Alvará que deve ser incluso em todos os carimbos do tempo gerados no período de vigência do alvará.

3.5.2.3 Estrutura de dados Leaves

3.5.2.3.1 Para o envio dos dados utilizados na construção das Árvores de Encadeamento do Tempo, o SCT enviará uma mensagem com código leaf_response tendo a estrutura Leaves como conteúdo.

3.5.2.3.2 A estrutura Leaves consiste de um vetor com os registros coletados ao longo da vigência do último alvará. Nesta estrutura, o SCT registra dois tipos de conteúdo diferentes: eventos de sincronismo e os carimbos do tempo emitidos no período.

Tabela 6: Estrutura de Dados Leaves

Tipo	Tamanho	Descrição
Leaf[ ]	Variável	Vetor contendo os registros de sincronização e carimbos do tempo emitidos desde a última auditoria

Tabela 7:Estrutura de Dados Leaf

Campo	Tipo	Descrição
data	byte[ ]	Dados de sincronismo (Tabela 8) ou carimbo do tempo (RFC 3161 [9])
index	int32	Posição na Árvore de Merkle do registro
type	string	“timestamp” / ”synchronization”

3.5.2.3.3 Registro de Sincronismo

3.5.2.3.3.1 As informações referentes aos registros de sincronismo devem ser obtidas por meio dos eventos de sincronia do PTP. De forma a padronizar a estrutura dos registros para a auditoria, foi adotada uma estrutura de 24 bytes conforme a Tabela 8.

Tabela 8: Estrutura do Registro de Sincronismo

Tipo	Tamanho	Descrição
int64	8 bytes	Unix timestamp da data e hora de realização do sincronismo com precisão de nanosegundos
uint64	8 bytes	O atraso médio do SCT em *Big Endian*
int64	8 bytes	O desvio médio do SCT em *Big Endian*

3.5.2.3.4 Carimbos do Tempo

3.5.2.3.4.1 Para fins de auditoria, os registros de carimbos do tempo inseridos na Árvore de Encadeamento do Tempo a serem enviados na estrutura Leaves devem seguir as especificações da RFC 3161 [9] e MCT-10 [6], em formato DER e codificado em Base64.

Tabela 9: Estrutura do registro de carimbo do tempo

Tipo	Tamanho	Descrição
byte[]	Variável	Carimbo do tempo conforme RFC 3161 [9] e MCT-10 [6] em formato DER, codificado em Base64

3.5.2.4 Estrutura de dados AuditResult

3.5.2.4.1 Ao final do processo de auditoria, o SAS encaminha uma mensagem de código issue_tcr, junto à emissão de um novo alvará. O conteúdo dessa mensagem contém uma estrutura chamada de AuditResult, que possui:

a) indicação da validade do alvará (resultado da auditoria);

b) o novo alvará emitido;

c) a razão para a rejeição da emissão de um alvará válido, caso exista.

3.5.2.4.2 Na Tabela 10, temos representado a estrutura contida na mensagem de issue_tcr.

Tabela 10:Estrutura do AuditResult

Campo	Tipo	Descrição
isValid	boolean	Resultado da auditoria
tcr	byte[]	Estrutura TCR conforme especificado no item 3.5.2.2, codificado em Base64
reason	Reason (Item 3.5.2.4.3)	Razão da rejeição do alvará, caso ocorra

3.5.2.4.3 Estrutura de Dados Reason

3.5.2.4.3.1 De forma a padronizar e facilitar o tratamento de recusas na emissão de alvarás válidos por parte do SCT, o SAS incluirá dentro da estrutura AuditResult, uma outra estrutura contendo a razão para a recusa no formato definido pela Tabela 11.

Tabela 11: Estrutura Reason

Campo	Tipo	Descrição
reject_reason	string	Identificador da razão de rejeição para a emissão do alvará
expected_value	Dependente do reject_reason	Valor limite ou valor esperado para determinado parâmetro que levou à rejeição da emissão do alvará
received_value	Dependente do reject_reason	Valor calculado ou valor recebido para determinado parâmetro que levou à rejeição da emissão do alvará

Tabela 12: Razões para a Rejeição de Emissão do Alvará

Código de rejeição	Descrição	Valor Esperado	Valor recebido
tct_leaf_number_mismatch	Incompatibilidade entre o número de folhas (transações) descrito pelo campo leafCount da TCT e o número de folhas válidas recebidas.	**Tipo:** uint32 **Valor:** Número descrito no campo leafCount	**Tipo:** uint32 **Valor:** Número de folhas válidas recebidas
tct_bitsize_mismatch	Incompatibilidade entre o tamanho descrito pelo campo bitSize da TCT e o tamanho real calculado da TCT.	**Tipo:** uint32 **Valor:** Número descrito no campo bitSize	**Tipo:** uint32 **Valor:** Tamanho calculado da TCT recebida

Código de rejeição	Descrição	Valor Esperado	Valor recebido
tct_hash_mismatch	Incompatibilidade entre o *hash* presente no campo currHash da TCT e o *hash* calculado da TCT recebida.	**Tipo:** byte[32] **Valor:** Valor de hash descrito no campo currHash	**Tipo:** byte[32] **Valor:** Valor de hash calculado da TCT recebida
tct_merkle_root_mismatch	Incompatibilidade entre o *hash* da raiz de merkle presente no campo merkleRoot da TCT e a raiz de Merkle recalculada a partir das folhas recebidas.	**Tipo:** byte[32] **Valor:** Valor de hash descrito no campo merkleRoot	**Tipo:** byte[32] **Valor:** Valor de hash calculado das folhas (dados) recebidas
tct_prev_hash_mismatch	Incompatibilidade entre o *hash* da TCT anterior presente no campo prevHash da TCT recebida e o *hash* presente no alvará anterior ou alvará presente nos carimbos do tempo.	**Tipo:** byte[32] **Valor:** Valor de hash descrito no campo prevHash	**Tipo:** byte[32] **Valor:** Valor de hash presente no alvará anterior e nos alvarás presentes nos carimbos do tempo
sync_max_instant_offset	Número de offsets instantâneos maiores que o	**Tipo:** int64	**Tipo:** int64

Código de rejeição	Descrição	Valor Esperado	Valor recebido
	limite esperado acima da quantidade permitida.	**Valor:** Valor máximo permitido para offsets instantâneos	**Valor:** Último valor de offset instantâneo acima do valor permitido
sync_max_instant_delay	Número de delays instantâneos maiores que o limite esperado acima da quantidade permitida.	**Tipo:** uint64 **Valor:** Valor máximo permitido para delay instantâneos	**Tipo:** uint64 **Valor:** Último valor de delay instantâneo acima do valor permitido
sync_max_average_offset	Offset médio acima do limite permitido.	**Tipo:** int64 **Valor:** Valor máximo permitido para a média de offsets no período	**Tipo:** int64 **Valor:** Média de offsets no período
sync_max_average_delay	Delay médio acima do limite permitido.	**Tipo:** uint64 **Valor:** Valor máximo permitido	**Tipo:** uint64 **Valor:** Média de delays no período

Código de rejeição	Descrição	Valor Esperado	Valor recebido
		para a média de delays no período	
sync_max_offset_deviation	Desvio padrão do offset acima do limite permitido.	**Tipo:** int64 **Valor:** Valor máximo permitido para o desvio padrão de offsets no período	**Tipo:** int64 **Valor:** Desvio padrão dos offsets no período
sync_max_delay_deviation	Desvio padrão de delay acima do limite permitido.	**Tipo:** uint64 **Valor:** Valor máximo permitido para o desvio padrão de delays no período	**Tipo:** uint64 **Valor:** Desvio padrão dos delays no período

3.5.2.4.3.2 Na Tabela 12, estão descritos os códigos de erros e seus respectivos tipos, valores esperados e valores recebidos para cada tipo de erro. Para o caso dos valores baseados em registros de sincronismo, os valores estarão em nanosegundos e encodados em *Big Endian*.

3.6 Auditoria Fora de Período (Force Audit)

3.6.1 Para a realização de uma auditoria fora do período estabelecido, o SCT deve estar preparado para receber, por meio do websocket, um pedido de auditoria forçada enviado pelo SAS com o código de operação force_audit_request.

3.6.2 Em caso do recebimento de uma mensagem de force_audit_request, o SCT deve responder a requisição com uma mensagem de force_audit_response, indicando o recebimento do pedido. Logo em seguida, o SCT deve iniciar um novo procedimento de auditoria conforme o descrito no item 3.

3.7 Parâmetros da Auditoria

3.7.1 Neste item, estão listados os parâmetros utilizados para a validação de qualidade de sincronismo durante a auditoria. Na Tabela 13 estão descritos os parâmetros configuráveis para auditoria no SAS.

Tabela 13: Parâmetros da Auditoria

Parâmetro	Descrição	Unidade
Validity period	O período de validade do alvará	Segundos
Min number of synchronization logs	A quantidade mínima de registros de sincronismo necessária para a realização da auditoria do tempo	Inteiro
Max instant offset	O máximo valor de *offset* permitido para cada evento de sincronismo	Nanosegundos
Max offset faults	A quantidade máxima de *offsets* acima do limite permitido	Inteiro
Average max offset	O máximo valor permitido para a média de *offsets* no período analisado	Nanosegundos
Max Offset Deviation	O máximo desvio padrão permitido para o *offset*	Nanosegundos
Instant max delay	O máximo valor de atraso (*delay*) permitido para cada evento de sincronismo	Nanosegundos
Max delay faults	Quantidade máxima de atrasos (*delay*) acima do limite permitido	Inteiro
Average max delay	O máximo valor permitido para a média de atrasos (*delay*) no período analisado	Nanosegundos
Max Delay Deviation	O máximo desvio padrão permitido para o atraso (delay)	Nanosegundos

3.8 Tratamento de erros, perdas de conexão e falhas internas no protocolo de auditoria

3.8.1 Devido à estrutura de mensagens do protocolo de auditoria e sincronismo, o tratamento de erro dependerá da natureza do erro ocorrido.

a) Para situações de falhas internas ou perdas de conexão, onde um dos lados da conexão não consegue tratar o erro ou enviar uma resposta de retorno, o lado da conexão ainda disponível deve reconhecer a ausência de uma resposta em tempo viável (*timeout*), abortar o processo de auditoria e reiniciar o procedimento do passo 1 (item 3.2) quando restabelecida a conexão.

   i. Exemplo: Um SCT perde a conexão com o SAS e não possui registros de sincronismo o suficiente para realizar a auditoria;

1. caso o alvará atual ainda esteja válido, o SCT pode retomar a emissão de carimbos do tempo com o alvará vigente;
2. quando a conexão estiver sido restabelecida com o SAS, o SCT deve esperar ter registros o suficiente de sincronismo para a realização da auditoria e então iniciar um novo processo incluindo todos os carimbos anteriores e os novos emitidos.

b) Para mensagens do tipo “response” i.e., mensagens em resposta a uma requisição feita anteriormente por meio de uma mensagem do tipo “request”, é possível responder à mensagem com conteúdo (“content”) vazio, e com o valor de “error” preenchido.

3.8.2 Como a maioria das mensagens enviadas pelo servidor do SAS são do tipo “request”, o SCT deve possuir um *timeout*, caso ocorra erros internos ao SAS sem um retorno de erro. Em caso de *timeout* do lado do SCT e seu alvará vigente ainda estiver válido, o SCT poderá retomar suas emissões de carimbos e registros de sincronismo na árvore de Merkle e tentar iniciar o protocolo novamente em tempo mais oportuno.

4 DOCUMENTOS REFERENCIADOS

4.1 Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as resoluções que os aprovaram.

REF.	NOME DO DOCUMENTO	CÓDIGO
[1]	**VISÃO GERAL DO SISTEMA DE CARIMBOS DO TEMPO NA ICP-BRASIL** Aprovado pela Resolução nº 58, de 28 de novembro de 2008.	**DOC-ICP-11**
[3]	**REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL** Aprovado pela Resolução nº 59, de 28 de novembro de 2008.	**DOC-ICP-12**
[4]	**REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO DA ICP-BRASIL** Aprovado pela Resolução nº 60, de 28 de novembro de 2008.	**DOC-ICP-13**
[5]	**PROCEDIMETOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL** Aprovado pela Resolução nº 61, de 28 de novembro de 2008.	**DOC-ICP-14**

4.2 O documento abaixo é aprovado por Instrução Normativa da AC Raiz, podendo ser alterado, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desse documento e a instrução normativa que o aprovou.

REF.	NOME DO DOCUMENTO	CÓDIGO
[2]	**REDE DE CARIMBO DO TEMPO NA ICP-BRASIL – RECURSOS TÉCNICOS** Aprovado pela Instrução Normativa ITI nº 17, de 18 de novembro de 2020.	**DOC-ICP-11.01**

4.3 Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio http://www.iti.gov.br.

REF.	NOME DO DOCUMENTO	CÓDIGO
[6]	**REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE CARIMBO DO TEMPO NO ÂMBITO DA ICP-BRASIL**	**MCT-10-VOL I**
[7]	**PROCEDIMENTOS DE ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE DE CARIMBO DO TEMPO NO ÂMBITO DA ICP-BRASIL**	**MCT-10-VOL II**

5 REFERÊNCIAS BIBLIOGRÁFICAS

[8] IEEE-1588 2008 - IEEE *Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*.

[9] RFC 3161 - *Internet* X.509 *Public Key Infrastructure - Time-Stamp Protocol* – TSP

[10] RFC 5755 - *An Internet Attribute Certificate Profile for Authorization*

[11] RFC 6455 - *The WebSocket Protocol*

[12] RFC 8446 - *The Transport Layer Security* - TLS *Protocol Version* 1.3

[13] *Wireguard - WIREGUARD – FAST, MODERN, SECURE VPN TUNNEL* - wireguard.com

ANEXO - ESTRUTURAS ADICIONAIS DE DADOS

1 ESTRUTURAS DE MENSAGENS PARA A TROCA DE CHAVES DA VPN

1.1 De forma a simplificar o estabelecimento de conexões VPN durante a configuração do protocolo de sincronismo, é possível realizar a troca de chaves e outros parâmetros adicionais por meio da conexão WebSocket de auditoria entre SAS e SCT.

1.2 Para realizar a troca de informações com o intuito de estabelecer a rede VPN por meio da conexão WebSocket, é necessário realizar o procedimento inicial de conexão como descrito no item 3.3.

1.3 Com a conexão WebSocket estabelecida, o formato de mensagem a ser enviado pelo SCT deve seguir o mesmo formato de mensagem descrito pela Tabela 2 contido no item 3.3 As operações utilizadas nessas mensagens devem ser ptp_network_request e ptp_network_response.

1.4 Estrutura de dados PTPClientRequest

O SCT que desejar requisitar os parâmetros de VPN para conexão com o SAS, deve enviar uma mensagem, via WebSocket, com o código de operação ptp_network_request para o SAS, com o conteúdo da Tabela 14.

Tabela 14: Estrutura PTPClient Request

Campo	Tipo	Descrição
sct_vpn_public_key	string	Chave pública Wireguard do SCT

1.5 Estrutura de dados PTPServerResponse

Após o recebimento de um pedido de ptp_network_request, o SAS irá registrar a chave pública do SCT e retornará, em uma mensagem de ptp_network_response, o conteúdo presente na Tabela 15 contendo as informações necessárias para que o SCT realize a conexão na VPN e rede PTP.

Tabela 15: Estrutura PTPServerResponse

Campo	Tipo	Descrição
sas_vpn_public_key	string	Chave pública Wireguard do SAS
sas_vpn_server_host	string	Endereço IP do servidor de VPN do SAS
sas_vpn_server_port	int	Porta do servidor de VPN do SAS
sas_vpn_ip	string	Endereço IP interno a VPN do SAS

Campo	Tipo	Descrição
sas_ptp_network_ip	string	Endereço IP do SAS na rede PTP
sct_vpn_ip	string	Endereço IP reservado para o SCT solicitante na VPN
sct_ptp_network_ip	string	Endereço IP reservado para o SCT solicitante na rede PTP
vpn_netmask	string	Máscara de rede da VPN
ptp_network_netmask	string	Máscara da rede PTP