Projeto novos protocolos para carimbo do tempo

Briefing

O Projeto de novos protocolos para carimbo do tempo do ITI busca entregar, de forma inédita e inovadora, à sociedade brasileira, e também a outros países, caso entendam assim, uma nova forma de atuação da Entidade de Auditoria do Tempo da ICP-Brasil. Faremos isso por meio de sua Fonte Confiável do Tempo - FCT, que realiza as funções de auditar, sincronizar e autorizar o funcionamento das Autoridades Certificadoras de Tempo – ACT, que fazem parte da ICP-Brasil, visando melhorias na interoperabilidade, rastreabilidade, performance e confiabilidade da rede. As principais alterações propostas são:

Protocolos de uso livre – Os protocolos utilizados pelo SAS para auditoria e sincronismo das ACTs passarão a ser disponibilizados para uso livre pela rede da EAT, de forma a garantir a interoperabilidade entre todos entes da rede, sem a dependência tecnológica de um fabricante ou solução específica.

Separação de Auditoria e Sincronismo – O sincronismo passa a ser feito de forma contínua entre a EAT e as ACTs, sem a dependência do processo de auditoria, através de protocolos padrões de mercado e com vasta documentação técnica disponível.

Arvore de Encadeamento do Tempo – Será proposto o encadeamento de dados de carimbos do tempo e de sincronismo, empregando recursos criptográficos baseados em Árvores de Merkle e encadeamento de blocos, garantindo assim a autenticidade, rastreabilidade e a segurança dos dados gerados na rede.

Segue abaixo em maiores detalhes:

1 SINCRONISMO

1.1PROCESSO

1.1.1 Processo no SCT

Operações de sincronismo ocorrerão permanentemente, em períodos variáveis definidos e iniciados pelo SAS.

1.2DADOS

1.2.1 Dados no SCT

Dados de estampa de tempo no SCT (timestamp), desvio médio (offset) e atraso médio (delay), de cada operação de sincronismo deverão ser armazenados em registros de eventos (log), sendo seus resumos criptográficos registrados na árvore de encadeamento do tempo em uso pelo SCT.

1.2.2 Dados de Sincronismo no SAS

O SAS recolherá a cada ciclo de auditoria a árvore de encadeamento do tempo do SCT e os registros de eventos correspondentes.

1.3Protocolo de Sincronismo

1.3.1 Sincronismo SCT - SAS

Usaremos o protocolo PTPv2 – IEEE 1588v2-2008 para realizar o sincronismo do relógio do SCT com o SAS. A fim de prover autenticação de dados no protocolo PTP deve-se associá-lo ao subprotocolo NTS-KE - “NTS Key Establishment”, parte do protocolo para segurança do tempo em redes para o protocolo NTP (Network Time Security for the Network Time Protocol), servindo para iniciar a troca de chaves criptográficas e outros dados de segurança, por meio do protocolo TLS, entre servidor (SAS) e o cliente (SCT).

1.3.2 Sincronismo SAS - FCT

Sincronismo entre a Fonte Confiável do Tempo e o SAS empregará o protocolo PTPv2.1 – IEEE 1588v2-2008, com uso de estampas de tempo produzidas pelo hardware das interfaces de rede (hardware com suporte timestamping).

2 AUDITORIA

2.1PROCESSO

i. SAS envia Alvará ao SCT
ii. SCT recebe Alvará e inicia, com este Alvará, nova Árvore de Encadeamento do Tempo
iii. SAS solicita dados de sincronismo e árvore de encadeamento do SCT
iv. SCT envia dados para SAS

2.1.1 PROCESSO no SCT

Para mitigar ataques de falsificação de carimbos do tempo, o SCT deve utilizar uma árvore de encadeamento do tempo.

Os nós da árvore de encadeamento do tempo deverão ser construídas da seguinte forma:

i. o SCT, ao receber um novo alvará, calcula seu resumo criptográfico e inicia uma nova árvore;
ii. toda operação de sincronismo deverá ter seus dados de estampa de tempo no SCT (timestamp), desvio médio (offset) e atraso médio (delay), resumidos criptograficamente e registrados na árvore;

iii. carimbos do tempo emitidos pelo SCT devem ser resumidos criptograficamente e inseridos na árvore;
iv. os dados usados para gerar os resumos criptográficos da árvore deverão ser armazenados em registros de eventos (logs).

- blocos (ou hashes) poderão ser enviados para framework blockchain;

2.1.2 PROCESSO no SAS

A auditoria no SAS será realizada pela avaliação estatística dos blocos de log de sincronismo recebidos, com o objetivo de checar a estabilidade, a precisão e a exatidão dos relógios dos SCTs. Caso o SAS detecte que o SCT está operando fora dos parâmetros de qualidade preestabelecidos, será emitido um alvará com validade igual a zero, revogando a operação do SCT até que, através do sincronismo permanente, atinja os níveis estabelecidos de qualidade.

2.2Protocolo para Auditoria

O envio de dados de auditoria será realizado com Protocolo Websocket (RFC 6455 e atualizações) sobre Protocolo Transport Layer Security (TLS) v 1.3 ou posterior (RFC 8446 e atualizações).