PROTOCOLO DE AUTENTICACIÓN PARA LA VERIFICACIÓN DEL SERVICIO DE SINCRONÍA DEL CENAM POR MEDIO DE CRIPTOGRAFÍA HASH.

Ricardo Martínez López[1], Eduardo de Carlos López[2], y Luis Adrián Lizama Pérez[1]
Universidad Politécnica de Pachuca[1]
Carretera Pachuca -Ciudad Sahagún Km. 20, Ex-Hacienda de Santa Bárbara, 43830 Zempoala, Hgo.[1]
Teléfono771-526-5801, ricardomartinezlopez@micorreo.upp.edu.mx

Centro Nacional de Metrología.[2]
Km 4.5 carretera a los Cues, 76246 Municipio del Marques, Qro.[2]

Palabras clave: (criptografía; hash; NTP; sincronía)

Resumen:

La sincronización de sistemas de cómputo con la hora oficial Mexicana es vital para las transacciones digitales que necesitan sustentar la duración de sus operaciones o la hora en la que fueron ejecutadas. Ejemplo de estas transacciones son las subastas electrónicas, la transmisión de comerciales en televisión y en otras actividades cotidianas como el tiempo transcurrido en estacionamientos. Por lo tanto se debe asegurar la integridad de las estampas de tiempo así como autenticar el origen de las mismas. Existen diversas formas de sincronizar sistemas con la hora oficial mexicana, uno de los medios más usados es el protocolo de tiempo de red (NTP por sus siglas en inglés) el cual nos permite obtener los valores del retardo de red y el ajuste o diferencia entre el tiempo del servidor y del cliente. En el presente trabajo se presenta un protocolo de autenticación para la verificación del servicio de sincronía del CENAM por medio de criptografía hash. El protocolo permite la autenticación de las dos partes involucradas en la comunicación gracias a una fase de sesión. Además la información transferida en cada transacción es autenticada por medio de un protocolo básico de firma electrónica. A través de las pruebas realizadas se determinan los parámetros adecuados para obtener los niveles de sincronía más precisos en el orden de milisegundos.