



ID:

Type: **Poster**

## **to the Standard Station Interface (SSI) software: State of Health and Authentication with ECDSA**

CTBTO Standard Station Interface (SSI) is a set of executable programs and application programming interfaces for acquisition, authentication, archiving, and telemetry of seismic, infrasound, and hydroacoustic data acquired by the stations of the IMS nuclear monitoring network. The State of Health (SoH) module of the SSI is the interface which allows station operators to monitor and control parameters of the SSI operation. This module collects State-of-health information related to the SSI, underlying hardware and software layers and presents this information to the station operators in a user-friendly format. The objective of the module modification is to provide the station operator with a modern means to access SoH information of the running station. This includes meaningful measurements provided by the digitizers, by SSI, the CRF and by supporting equipment. Authentication with ECDSA (Elliptic Curve Digital Signature Algorithm) has also been integrated to the SSI. This algorithm is supported by the tokens used at stations, and a software/firmware update has been done to enable its use. SSI Configurator is updated to include the ECDSA option. SPYRUS Links Series II HSM and the SmartCard HSM are the supported HSM devices.

**Primary author:** MILJANOVIC TAMARIT, Vera (CTBTO)

**Presenter:** MILJANOVIC TAMARIT, Vera (CTBTO)

**Track Classification:** Theme 3. Verification Technologies and Technique Application