SnT 2019
CTBT: SCIENCE AND TECHNOLOGY CONFERENCE

CTBTO PREPARATORY COMMISSION

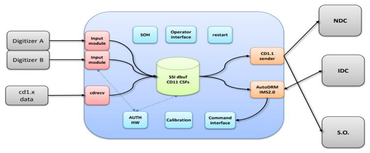
Improvements to the Standard Station Interface (SSI) software: State of Health and Authentication with ECDSA

Vera Miljanovic(vera.miljanovic@ctbto.org), Julien Marty (julien.marty@ctbto.org), James Mattila (james.mattila@ctbto.org), Nurcan Meral Ozel (nurcan.meral.ozel@ctbto.org)

T3.3-P8

Abstract

CTBTO Standard Station Interface (SSI) is a is a data acquisition software system specially designed and developed by the CTBTO for supporting waveform IMS stations in order to collect, sign, buffer, reformat and transmit data using IDC formats and protocols.



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.

SSI is currently installed in more than **100+ IMS sites**, in all waveform technologies, and also is in use in several National Data Centres.

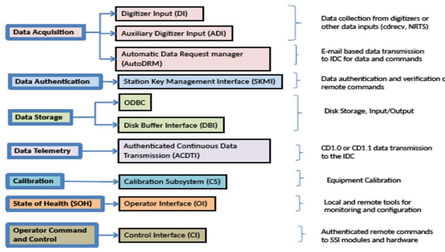
Designed to meet all IMS requirements;

- CD1.1, IMS2.0;
- Data Authentication;
- Commands Authentication;
- Secure Remote Connection;
- PTS owned, ensures support and maintenance.

SSI Today: Main Strengths

- Reliability; SSI is a field-tested system that requires (little or) no maintenance to work;
- Standardization, simplifies the support and maintenance of stations;
- Assurance of Compliance to Formats and Protocols, by using IDC's reference implementation (CDtools);
- Flexibility, SSI can be configured in many ways, and for different uses.
- For example: 3C stations, arrays, NDCs;
- Long Term Maintainability, by using SSI as the effective PTS developed solution.

SSI Modules and Functions



SSI Development Strategy 2018/2019

- **The SSI Documentation** - ongoing work on a complete set of documents that will adequately support users and developers, and that is maintained with any change to SSI .
- **Improvement of the State of Health (SOH) system** - The purpose of the SOH module is to collect SOH and status information related to the SSI; collect underlying hardware and software layers; and present this information to the user in a user-friendly format.
- **ECDSA support for Spyrus and SmartHSM cards** – EC curves and parameters supported by CDtools were used in order to implement the ECDSA support. Web Configurator is updated to include ECDSA option.
- **Release Process** – new user friendly release process that includes three options: rpm packages with script, Virtual Machine with pre-installed software, and pre-installed LiveCD
- **Station Key Management / Certificates** – ongoing work to modernize the handling of keys, certificates and certificate revocation lists. The current approach has known technical shortcomings and is a frequent source of deployment problems. The new approach aims introduce more flexibility and automation.
- **SSI Configuration Modernization** – SSI Web-Configurator is inflexible, and should be more user friendly. It will be replaced by a new configuration and management system with modern user experience design and appealing visuals. It will address both the needs of station operators, as well as CTBTO staff. It will eventually cover the full range of SSI's possibilities and may add novel features such as centralized archival of configurations.
- **SSI Next Generation Disk Buffer** – Remove dependency on MySQL which is the source of many problems in production, streamline the SSI architecture, decrease the amount of buffering, increase robustness
- **Calibration** – continue to develop and extend SSI's calibration module. Add support for more digitizers and instruments. Create automated regression tests for the calibration module

SSI SoH module goal requirements:

- Improve Station Operator monitoring capability (early detection of problems).
- Support problem analysis and restoration of service for both SO and PTS staff.
- Gather state of health data at the station including station elements.
- State of health data should contain meaningful information about the station and its equipment (e.g. digitizer voltage, radio, logger etc).
- Provide graphical and text visualizations to PTS staff and station operators.

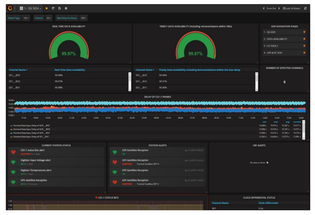
SSI SoH Modules Components

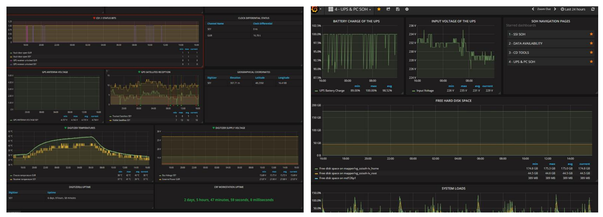
- libssi_soh library, which allows other SSI modules to collect SoH parameters and save the parameters in the InfluxDB
- ssi_soh binary executable programs, which directly collect SoH parameters and save the parameters in the InfluxDB
- SSIConfig tool Operator Interface Configuration PageSoH page in SSI Config tool showing the system's state of health
- CONTROL and STATUS pages of SSI Config tool showing the state of the running SSI programs
- Program ssi_mon showing oldest and latest data into the SSI disk buffer
- Grafana and InfluxDB software systems used to store and display SoH history for a predefined period

Data Availability (disk buffer)

Detailed information is available in <Grafana

	Data Availability	Timely Data Availability
all channels	100.00%	100.00%
2103__BHE	100.00%	100.00%
2103__BHN	100.00%	100.00%
2103__BHZ	100.00%	100.00%
2103__HHE	100.00%	100.00%
2103__HHN	100.00%	100.00%
2103__HHZ	100.00%	100.00%
GUR__BHE	100.00%	100.00%
GUR__BHN	100.00%	100.00%
GUR__BHZ	100.00%	100.00%
SEY__BHE	100.00%	100.00%
SEY__BHZ	100.00%	100.00%
SEY__BHZ	100.00%	100.00%



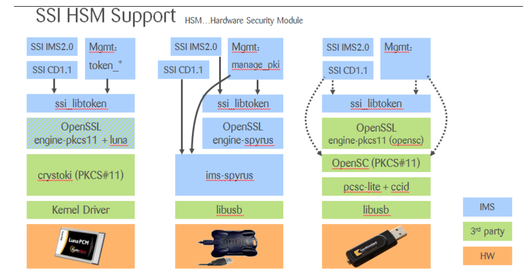


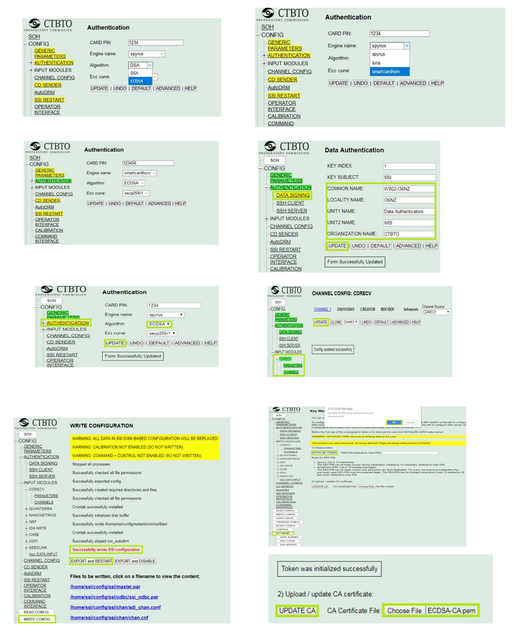
Authentication with ECDSA and SmartCard-HSM

The DSS(digital signature standard)was adopted by the PTS for IMS use in 1999.In its original form, DSS uses SHA-1 as hashing algorithm and DSA with key lengths up to 1024bits.In the meantime, vulnerabilities were discovered in SHA-1, to the effect that SHA-1 is no longer considered to provide adequate security. In addition, the key length of 1024 bits used in IMS does no longer provide an adequate safety margin. The PTS proposed to WGB a staged migration plan to ECDSA for IMS and IDC. This is well described in the presentation: WGB34 Info Sec Presentation.

This is the reason why SSI was updated to the newer ECDSA (Elliptic Curve Digital Signature Algorithm). This algorithm is supported by the tokens used at stations, but a software/firmware update was needed to enable its use. ECDSA algorithm was added to SSI, and successfully deployed and tested in several stations, including I09 Brazil, IS41 Paraguay, PS45 Ukraine in 2018.

In the past, the SPYRUS Links Series II HSM was the preferred HSM device. In August 2017,end-of-life for this LYNKS product family was announced and SPYRUS will no longer manufacture additional units after the current manufacturing run with inventory available by mid-September 2017. For this reason, the IMS/ED decided to support additional HSM cards. The SmartCard HSM is a cost-effective alternative (56 EUR) to the expensive LYNX product (more than 1000EUR). SSI support for SmartCard-HSM was added in 2018, and successfully deployed and tested in PS19, Freyung, Germany.





SSI Webconfigurator Requirements

A new configuration system for SSI should ideally combine the advantages of configuration files and Web-Configurator. Top-level requirements are:

R1. Support full range of SSI's features (including calibration, SoH, key management and auxiliary channels)
This is most easily implemented if there exists only a single representation of SSI configuration. This pre-vents a situation like the status quo where some configurations are only supported by files and not by Web-Configurator. Web-Configurator should evolve or be replaced by a tool that works on the same representation that is read by SSI.
R2. Work in a bandwidth-constrained environment (over GCI)
This entails that we should not design the system around a rich GUI that needs to be used remotely. There are several options:
- Rich GUI that runs locally and communicates with the back-end over some form of API (i.e. something similar to Calibration-GUI)
- Minimal, bare-bones GUI optimized for remote access (i.e. an optimized Web-Configurator)
- Rich text-UI optimized for remote access
- Any of the above plus a command-line based power-user interface for configuring SSI

R3. Co-exist with AutoDRM
Since AutoDRM can change the configuration, there should be a well-defined way for allowing that. One option is that the configuration system has an API or command-line language that allows to mutate the active configuration programmatically. The other option is that the configuration system can co-exist in an environment where the underlying representation changes dynamically.

R9. Handling of certificates and other file-based configuration items
Some things fall between the categories – their neither strictly configuration parameters, nor production data. Examples are certificates or calibration nominals. Handling of these configuration items should be supported by the configuration system. Specific mechanisms may be necessary for each of these.
R10. Central versioning and central archival of configurations
Versioning entails a structured way of handling certain meta-data, like dates and names. This meta-data is not part of the configuration proper but needs to be saved with it. Versioning also requires a way of com-paring different versions. Effective comparison requires a compact representation. There are good tools for comparing text representations. Comparison based on GUI data entry masks is typically not effective. Central archival is a special way of moving a configuration from the system under consideration to a central location.
R11. Backups
Backups should be made and saved at a central point fully automatically.
R12. Documentation and explanations
The system should allow users to comment on and explain their choices within the UI. Ideally, these comments are kept inline with the configuration for archival. The system should NOT mix system docu-mentation with configuration (like classical Unix config files). System documentation should be accessible from the UI, but not saved inline with the configuration.

SSI Status 2019

- SoH metrics is equipment/vendor neutral
- Grafana/Influx DB is used instead of Graphite
- Number of shown statistics was minimized to show only the most important values, and only the most important metrics is saved in Influx DB
- Authentication with ECDSA (Elliptic Curve Digital Signature Algorithm) has 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.
- User friendly build system, all modules and dependencies are packed into one tar ball and can be installed with one command

- Ongoing work on Webconfigurator, requirements are defined and prototype is finished.