MIRION TECHNOLOGIES

Operator Data Authenticator (ODA)

Features

- Provides electronic data authentication capability to facility operator's declaration data
- Compact and easily hand-transportable
- Sealed tamper indicating enclosure which may be sealed with E-type or fiber optic seals
- Accepts an unlimited number of fields included in each record
- Time and date stamp ensures host made the declaration at the stated time
- Non-resettable counter appended to each record that is signed and can only be changed by authorized personnel

Description

The Operator Data Authenticator (ODA) was designed by CANBERRA to provide a method of electronic authentication to a facility operator's declaration data in support of safeguards activities. By applying an unchangeable time stamp and unique signature to the declaration data, the ODA provides assurance to the facility inspector that the host made the declaration at the stated time. A non-resettable counter is appended to each record that is signed and once the declaration is made, the host cannot change it except through specified procedures.

The ODA consists of a CANBERRA Delta 2000/E with a PC-104 digital I/O card, mounted within an Agency-approved double-sealable tamper indicating enclosure. The ODA enclosure may be sealed with a metal E-type seal or with a fiber optic seal. Access to the internal ODA components and its firmware is possible only when the sealed tamper indicating enclosure is opened by an Inspector or other authorized personnel. A tamper switch mounted inside the ODA enclosure detects and records all tamper events. The ODA has a single main cable and a fixed data cable for connection to the serial port of a PC or laptop using an RS-232 compliant DB-9 connector. The cable connection is resistant to accidental disconnection. The ODA is protected against corrosion resulting from condensation, as well as against accidental damage of the seal wire or fiber on the recording console. The compact design of the ODA makes it easy for an Inspector to transport it by hand from one facility to another. A universal power supply enables its use in most countries.

The ODA utilizes two forms of memory: NVRAM and Flash memory. The NVRAM is read/write memory used to store the keys and tamper events for the ODA. Most of the NVRAM memory is not accessible and the portions that are accessible are available only from the console, such as the baud rate for the serial connection to the PC and setting the ODA time. Any other functions at the console are for display only. The Flash memory contains the operating system and application for the ODA. This memory is written at the factory, and a jumper is removed so that the Flash cannot be changed.

The ODA accepts host declaration data files in comma separated values (.CSV) in ASCII format from the host PC RS-232 port. It then appends a time/date stamp and a digital signature and returns the authenticated file, via the RS-232 port, to a specified drive on the host PC. The signature is generated using the operator's data, the counter, and the time/date stamp. The ODA performs authentication using RSA-compliant algorithms and public key encryption. The ODA application software, GemCheck, allows the Inspector an easy method to verify the authenticity of each record in the declaration file and to remove the authentication for further inspection verification use. The authentication removal process produces a log file of any records that fail authentication.

ISO 9001 SYSTEM CERTIFIED

C29212 – 10/06