Contribution ID: **151** Type: **oral**

The IAEA's Universal Instrument Token

Thursday 23 October 2014 11:00 (20 minutes)

The IAEA currently seeks to improve the harmonization of security approaches across safeguards equipment. The protection of digital safeguards data is based on several principles: a) the signing of data in measurement devices using standard public/private-key-based signature generation, b) the storage of secret keys on certified, tamper-protected cryptographic devices, and c) well-established cryptographic algorithms and protocols based on global standards and internationally recognized cryptographic libraries. This paper discusses a cryptographic token, the Universal Instrument Token, which constitutes the core element of the architecture for signing safeguards data. This architecture supports the above principles and is compliant with the IAEA's information security policies and guidelines. An important side-condition is that the UIT must be implemented across a wide range of operating systems and hardware architectures, which mandates the use of open-source software for all software-related parts involved.
The UIT is permanently connected to the measuring device (usually via the USB port) and requires complex hardware drivers and middleware components. Identifying open-source based, mature and ready-for-use smart card drivers and tools that are compatible with a range of operating systems was a major challenge. Reliable and well-established cryptographic libraries reside at the core of every information-security application. Different types of review software, typically software products used at IAEA headquarters in Vienna but occasionally also in the facilities, need to contain some specific software modules in order to verify the digital signatures attached to the data. Finally, also required are enrolment tools which generate private keys and certify their corresponding public counterparts using the IAEA's internal Certification Authority.
In 2014, the roll-out of the UIT has raised the security of IAEA instrument data signing to a level which is currently considered to be impractical to defeat, provided that the correct procedures are followed.

Country or International Organization

IAEA

EPR Number (required for all IAEA-SG staff)

697

Author: NAUMANN, Ingo (IAEA)

Co-authors: SCHWIER, Andreas (CardContact, Germany); WISHARD, Bernard (iaea); BRUNHUBER, Christoph (IAEA); MORGAN, Keith (IAEA); FRANK, Thater (CardContact, Germany)

Presenter: SCHWIER, Andreas (CardContact, Germany)

Session Classification: Equipment Security and Considerations for Joint Use