IAEA-SM-367/17/04

Trilateral Initiative: IAEA Authentication and National Certification of Verification Equipment for Facilities with Classified Forms of Fissile Material

Eckhard Haas
International Atomic Energy Agency, Vienna, Austria

Alexander Sukhanov
Russian Ministry of Atomic Energy, Moscow, Russia

John Murphy
US Department of Energy (Pacific Northwest National Laboratory), Washington D.C., USA

Abstract

Within the framework of the Trilateral Initiative, technical challenges have arisen due to the potential of the International Atomic Energy Agency (IAEA) monitoring fissile material with classified characteristics, as well as the IAEA using facility- or host country-supplied monitoring equipment. In monitoring material with classified characteristics, it is recognized that the host country needs to assure that classified information is not made available to the IAEA inspectors. Thus, any monitoring equipment used to monitor material with classified characteristics has to contain information security capabilities, such as information barriers. Conversely, in using host country-supplied monitoring equipment to monitor material, the IAEA has to have confidence that the information provided by the equipment is genuine and can be used to fulfill its obligation to derive conclusions based on independent verification measures. Thus the IAEA needs to go through the process of authenticating the monitoring equipment. In the same way the host country needs to go through the process to assure itself that the monitoring equipment integrated with an information barrier will not divulge any classified information about an inspected sensitive item. To a large extent both processes require identical measures, but partially also may conflict with one another. The fact that monitoring equipment needs to exhibit information security capabilities throughout its life cycle while, at the same time, be capable of being authenticated necessitates the need for creative technical approaches to be pursued.

1. INTRODUCTION

The United States, the Russian Federation, and the International Atomic Energy Agency (IAEA) undertook the Trilateral Initiative in September 1996 to investigate technical, legal and financial issues associated with IAEA verification of weapon-origin fissile material [1]. According to the Draft Model Verification Agreement it is the goal of IAEA verification to confirm that material subject to the Agreement conforms to the State's declarations and remains accounted for under the Agreement. A Joint Working Group was established to carry out the investigations. An important requirement for the verification of material with classified characteristics is the restriction of IAEA access to classified weapon design information. This requirement is derived directly from Article 1 of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) [2]. It obliges the State not to provide to any recipient any information that the State considers classified due to its relationship to nuclear weapons. Vice versa the IAEA would not wish to have access to any such information. Technical experts from the three parties involved made significant progress in the elaboration of the general technical requirements for "Attribute Verification Systems with Information Barriers for Plutonium with Classified Characteristics utilizing Neutron Multiplicity Counting and High-Resolution Gamma-ray Spectrometry (AVNG)" [3,4], and the general technical requirements for "Inventory Monitoring Systems (IMS) for Facilities Storing Fissile Material with and without Classified Characteristics" [5].

It is a common understanding within the Joint Trilateral Initiative Working Group, especially for information security reasons, that equipment used for verification of material with classified characteristics by the IAEA will most likely be produced and certified by the host State. This is particularly true for attribute measurement systems.

The requirement for information security and its certification by the host State, the fact that the equipment used for verification may not be owned by the IAEA, and that the host State may even refuse direct access to the equipment for authentication purposes when in use, results in a significant complexity of the authentication issue. Regardless of such possible restrictions, the IAEA for its part must implement credible verification resulting in the ability to draw independent conclusions. For this purpose the IAEA has to assure that genuine information is obtained while using equipment which is not under its control. Meeting both requirements is an essential task for the Trilateral Initiative.

2. FUNDAMENTAL ASPECTS OF INORMATION SECURITY AND ITS CERTIFICATION

Within the framework of the Trilateral Initiative, particular parameters of the fissile material are important to the IAEA in verifying the States declarations, for example, "the presence of plutonium", "the presence of weapons-grade plutonium", and "the mass of the plutonium" [6]. To ascertain such parameters involves the acquisition of radiation measurements that might be classified, such as radiation spectra. In some cases, such as mass, the parameter itself might be classified.

Non-destructive analysis techniques based on radiation measurements are a requisite to gaining information on the parameters to allow independent conclusions to be made by the IAEA. Such techniques under consideration are low- and high-resolution gamma-ray detection and neutron multiplicity counting.

From the point of view of the State's national security, the general issue is the protection of the classified information.

Information security in this context is the process of assuring that any classified information about an inspected sensitive item will be protected from unauthorized access.

Information security is accomplished through relevant organizational and technical measures.

As a technical measure the concept of *Information Barriers* was developed by the technical experts and adopted as most promising. In essence, this concept consists of using hardware and software to restrict the information provided to the IAEA by denying access to any classified data [4].

Certification in this context is the process by which the host State assures itself that an inspection system integrated with an information barrier will not divulge any classified information about an inspected sensitive item to the IAEA. Certification includes all processes required for the host to allow operation of the system within its facility [7].

Consequently certification is a significant part of information security. It can be split again into the examination of the type of the inspection system and into the examination of the equipment to be installed in a facility.

For equipment to be placed in a nuclear facility, certification of that equipment, from a safety perspective, is normally accomplished. In the same way, certification of equipment from the perspective of secure information needs to be done. During certification both hardware and software need to be examined. This requires investigation of the system model and all documentation, including the description of software codes. This process applies to all sensors/detectors, data processing, and data transmission. In addition, access to the source of the classified information needs to be protected against clandestine information gathering. In meeting these requirements there is doubtless advantage in having the State be responsible for the engineering of such a system.

Finally, before installation and use the system/equipment has to be examined for conformity with the certified sample/prototype of equipment or technical standards.

Once this process has been completed, an inspection system can be used in a nuclear facility for the stated purpose. Issues then arise regarding the interface of an inspecting agency with the equipment. From the perspective of the State, the preferred approach is for the facility operator to be the sole interface to the equipment, with the inspecting party having oversight only. The issue of access to equipment and the inspector interface with equipment must be defined in protocols (administrative controls) that are evaluated as the equipment is certified.

3. FUNDAMENTAL ASPECTS OF AUTHENTICATION

Even before the Trilateral Initiative investigation into the verification of classified materials the development and implementation of unattended verification systems in safeguards raised the question of authentication. Meanwhile "Authentication" is a familiar quotation in the safeguards community and significant progress has been made especially in the field of electronic seals and surveillance equipment.

However, when asking what authentication means in terms of a process, it is not so easy to reach a common understanding. On the occasion of an IAEA Consultants' Meeting in 1991 the consultants arrived at the following definition:

> *Authentication is the process of assuring that genuine information is obtained for safeguards purposes using equipment for which the IAEA lacks sufficient control or knowledge* [8].

In this sense authentication is an essential prerequisite for the IAEA to fulfill its obligation to derive conclusions based on independent verification measures when using equipment which the operator has supplied or to which the operator has access. To get genuine, falsification-proof data, in principle two basic strategies for the IAEA are possible:

- Protection of equipment against tampering and/or indication of any tampering with the equipment; and
- Authentication of data by using a recognition code/electronic signature and/or encryption.

In addition, the ability to sample the items under verification to inspect and assure the correctness of the item can contribute to the authentication process. In IAEA safeguards, most often a combination of the strategies is applied.

Authentication of a measurement system with a detector/sensor, with data processing and with data transmission means the certainty that the measurement results obtained by the inspector for verification purposes are generated in accordance with the specification and give a true representation of the object. From this one can deduce that the function of the detector and its characteristics, once initially tested and accepted, must remain unchanged. To make this provable for inspectors the detector and those components relevant for its function, therefore, must be physically protected, and direct access to "state of health data" including the signals from integrated "normalization sources" should be possible outside the information barrier.

More problematic is the authentication of the data processing part of the system, behind the information barrier. It may be already doubted that somebody who has no direct access to production data of its components can validate such a complex system without destroying it. Authentication, as a continuous requirement, becomes even more problematic when the system is once in use and any access, especially to components behind the information barrier becomes, for information security reasons, impossible. The consequence is that the data processing function can be tested only by observing its results. One possibility is the regular but predictable use of NDA standards with known results. First and foremost a commissioning and functional test program needs to be established in order to check whether the performance of the system meets the given specification. Such a commissioning and functional test program may include the use of test data packages. In the case of a radiometric measurement system the test program also includes the use of specially prepared calibration standards. For the preparation of such reference materials and standards the following essential requirements are to be kept:

- The standards used for authentication must be accepted by the IAEA based on independent destructive analysis conducted under IAEA supervision.
- The standards must be representative of the material being measured and cover the expected range of material content.
- The standards must remain under uninterrupted IAEA Containment & Surveillance (C/S) measures.

Once the data processing part of a system is authenticated, for later routine use the system or the relevant parts of the system must be protected again by C/S measures against tampering. [In addition inspectors may want to use their own tamper protected software copy.] Note: How software is handled/controlled and what software may be used will be part of the certification process.

Another open issue is the usual requirement by the IAEA that a vulnerability assessment of the authenticated system be carried out by a third party. The main reason for bringing in a third party is to increase the “credibility” of the authentication measures taken by the IAEA by using also independent resources and recognized expertise. In doing so, the information security issue will be once more of greatest importance. One solution could be that the vulnerability assessment might be done by an acceptable institution of the other State concerned. The real need for bringing in a “third party” at last has to be assessed under the aspect of additional gains in the context of transparency and confidence built by the States concerned.

Finally, authentication is not merely a single activity. It remains a permanent requirement and an on-going process throughout the life cycle of the equipment. Especially after maintenance activities with intrusion on C/S measures, re-authentication becomes essential.

4. AUTHENTICATION AND INFORMATION SECURITY IN THE REALITY OF THE STORAGE OF MATERIALS WITH CLASSIFIED CHARACTERISTICS

Information Security and Authentication are not restricted to just the instruments used for verification. They cover the whole process of verification; beginning with the object (signal source) to be verified followed by the appropriate sensor/detector, data transmission, and data processing and data recording/evaluation.

Object/Signal Source

Concerns of Information Security on the signal source are a high priority for the State. The radiation emitted from the source contains the information, which needs to be protected. Thus operational procedures need to be established to restrict the use of equipment to only that which has been basically certified and tested. On the other hand, when using radiometric measurements for verification, authentication of the object/signal source also assures that the object presented is the object declared regarding the identity and integrity and not always the same radiation source presented in different containers. In the case of material with classified characteristics it will not be possible to get an unequivocal “finger print” of the signal source, only the attributes for the acceptance of that source under the Agreement can be verified. The proof of an unchanged identity and integrity of the signal source can be furnished therefore only via the storage container. From this, having the verification goal in mind, one can deduce the need for a falsification-proof identification number of the storage container and the need to exclude or detect any undeclared change of its content once it is recorded and accepted as submitted to the Agreement. The latter, however, could be achieved by quite different measures: by “design verification” of the container and sealing, by continuous observation of an individual container after verification, or by the exclusion of any manipulation possibility with the content during storage via design information verification supported by extensive surveillance.

Sensor/Detector

Authentication of the sensor/detector not only means that the signals produced are coming from the sensor/detector as they should, but also that the functioning and characteristics of the detector remain unchanged. These requirements may be achieved by using a tamper resistant or tamper indicating enclosure for the detector/sensor. The functioning, characteristics and efficiency of the detector/sensor are checked by test signals and integrated “normalization sources”. In addition, self-testing and malfunction recording techniques may be implemented. On the other hand, information security as a process must assure the protection of the signals produced by the sensor/detector and, in connection with authentication, that there is no impact or influence on information security caused with the implementation of the above authentication features. The application of technologies to reduce or resist the transfer of electromagnetic signals may also be necessary.

Data Processing

The hardware and software determine the data processing part of a system. Consequently authentication of data processing starts with the examination of the complete system’s documentation as well as the validation/evaluation of the relevant hardware components and the operating and application software including the use of test data. This also applies to certification. The crucial issue for both authentication and certification is that the software processes the signals from the sensor/detector as specified and that there are no hidden features in the system to pass erroneous information [7]. The regular but “predictable” measurement/re-measurement of specially prepared calibration standards, as part of the authentication process, and the use of test data packages means testing the overall function of the system over its results. To exclude for such tests the possibility of hidden features one has to overcome the problem of the “predictability”. One solution might be to “embed” real data of a measurement “unpredictably” in a sequence of test data and to connect the identification of data sets with results after the information barrier. Prior to being implemented into operation for the first time, an authentication review of the information barrier software and hardware should be allowed; however, once operation has commenced, subsequent reviews will need to be negotiated. A crucial issue in this connection may be that the information barrier and its technique, once used for the measurement of material with classified characteristics, may become classified itself and therefore cannot be examined directly any more.

Data Transmission

In a verification system the detector and data processing components are often physically separated. The same may also apply to data processing, data recording, and data display. If this is the case, the data transmission needs to be authenticated amongst all components. To accept electronic data as authentic the following conditions must be fulfilled:

a) The data must remain unchanged and complete when passing from the transmitter to the receiver.
b) Data generation, transmission and receipt takes place within a specific time interval. In other words, data generated “in the past”, even when coming from a genuine detector/sensor are not valid.
c) The data have to be issued from the genuine transmitter.

To prove the authenticity of the data transmitted, one may either protect the transmission media against interference or detect and record any such interference, for example, by the application of shielding and C/S measures. Another possibility of data authentication is the use of electronic signatures and encryption, including the incorporation of date and time stamps on the data.

Information security is faced with the challenge of ensuring that features added to assure authentic data are transmitted do not allow the release of classified information. This can be a tedious effort especially if an information barrier is placed in a data transmission link. Signal emanations are also a concern, and employing shielding technologies may be necessary.

Testing the basic requirements and measures for authentication, taking into account information security restrictions in storage of materials with classified characteristics, will be extremely difficult. If one, however, takes into account the separate measures, not only isolated but also as part of a process within its boundary conditions, the verification goal of the IAEA and the meaning of each measure within that process, then some alternatives and possibilities that will meet the requirements of both information protection and authentication, may turn out.

Table 1 shows the different technical subjects within such an authentication process and possible measures that can be differently combined, depending on the facility design and verification approach, to achieve both information security and the authentication goals.

5. CONCLUSIONS

Authentication is not only an essential prerequisite for the IAEA to fulfill its obligation to derive conclusions based on independent verification measures, it is also essential for the implementation of a credible verification regime. The requirement for information security, its certification and other boundary conditions means a big but manageable challenge for the issue of the authentication of equipment to be installed and, because of that, for the design of a credible verification approach. As long as one regards authentication as a process of connected measures within the overall verification approach, depending on the facility design and other boundary conditions, solutions can be developed to satisfy both the requirement of the State for information security and the requirement of the IAEA for authentication. The first, most important, step to create awareness, is already done, but also the next step, to think in terms of concrete solutions, has already started.

Subject/ Component	Information Security Requirements	Possible Information Security Measures	Authentication Requirements	Possible Authentication Measures*
Object/Signal Source	Integrity No direct access	Secured enclosure Facility seals Surveillance Physical protection techniques	Integrity ID number	Certified container Design verification ID number Agency seals Surveillance Re-verification
Sensor/Detector	No clandestine function No signal emanations Integrity Unchanged settings No direct access	Certification Exam. of equipment Tempest enclosure Facility seals Physical protection techniques	Integrity Unchanged settings	Tamper Indicating Enclosure State of health information Malfunction records Re-measurement of standards
Data Processing	No clandestine function No signal emanations No display of classified Information Integrity Unchanged settings No direct access	Certification and examination of - data processing - hardware component Information barriers Tempest enclosures Physical protection techniques	Hardware as specified Performance as specified	Validation of - data processing - hardware components Evaluation of software Tamper indicating enclosure Duplicate secured software file Re-measurement of standards
Data Transmission	No signal emanations No tapping of transmission lines No direct access	Certification Exam. of equipment Shielded cables Physical protection techniques Encryption	Data has not been - altered - removed - or substituted Date and time are valid	Application of C/S Electronic signatures Encryption

* Under operational conditions any access to the measurement equipment by an Agency inspector for authentication purposes might be at least made more difficult or even be refused due to information security

Table 1. Basic Measurements for Implementing Information Security and Authentication

REFERENCES

[1] T.E. Shea, et al, *The Trilateral Initiative: IAEA Verification of Weapon-Origin and Other Fissile Material Released from Defense Programs,* 42nd Annual Meeting of the Institute of Nuclear Materials Management, July 15-19, 2001.

[2] *Treaty on the Non-Proliferation of Nuclear Weapons (NPT),* Adopted June 12, 1968; Entered into Force March 5, 1970 (IAEA INFCIRC/140).

[3] J.M. Puckett et al, *General Technical Requirements and Functional Specifications for an Attribute Measurement System for the Trilateral Initiative*, 42nd Annual Meeting of the Institute of Nuclear Materials Management, July 15-19, 2001.

[4] D. MacArthur et al, *The Effects of Information Barrier Requirements on the Trilateral Initiative Attribute Measurement System (AVNG)* 42nd Annual Meeting of the Institute of Nuclear Materials Management, July 15-19, 2001.

[5] I.I. Kuleshov et al, *General Technical Requirements for an Inventory Monitoring System for the Trilateral Initiative*, 42nd Annual Meeting of the Institute of Nuclear Materials Management, July 15-19, 2001.

[6] J.M Puckett et al, *General Technical Requirements and Functional Specifications for an Attribute Measurement System for the Trilateral Initiative*, 42nd Annual Meeting of the Institute of Nuclear Materials Management, July 15-19, 2001.

[7] KOUZES, R.T. et al., Authentication of Radiation Measurement Systems for Non-Proliferation, Pacific Northwest National Laboratory, PNNL-SA-34871, July 2001.

[8] International Atomic Energy Agency, Authentication of Operators' Systems used for Safeguards Purposes, Consultants Meeting, Vienna, March 1991, STR-272.

[9] HAAS, E., MANGAN, D.L., Information Security and Authentication – A Trilateral Initiative Challenge, 42nd INMM Annual Meeting, Indian Wells, 2001.