PNNL-13550

Pacific Northwest
National Laboratory
Operated by Battelle for the
U.S. Department of Energy

Authentication Procedures - The Procedures and Integration Working Group

R. T. Kouzes
L. Bratcher
T. Gosnell
D. Langner
J. Mihalczo
C. Pura
A. Riedy
P. Rexroth
M. Scott
J. Spingarn

July 2001

Prepared for the U.S. Department of Energy
under Contract DE-AC06-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-ACO6-76RL0183O

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm


This document was printed on recycled paper.
(8/00)

PNNL-13550

Authentication Procedures - The Procedures and Integration Working Group[1]

R. Kouzes
L. Bratcher[(a)]
T. Gosnell[(b)]
D. Langner[(c)]
D. MacArthur[(c)]
J. Mihalczo[(d)]
C. Pura[(e)]
A. Riedy[(d)]
P. Rexroth[(f)]
M. Scott[(g)]
J. Spingarn[(f)]

July 2001

Prepared for
the U.S. Department of Energy
under Contract DE-AC06-76RLO 1830

Pacific Northwest National Laboratory
Richland, Washington 99352

(a) Pantex Plant, Amarillo, Texas.
(b) Lawrence Livermore National Laboratory, Livermore, California.
(c) Los Alamos National Laboratory, Los Alamos, New Mexico
(d) Oak Ridge National Laboratory, Oak Ridge, Tennessee.
(e) Sandia National Laboratory/DTRA, Albuquerque, New Mexico
(f) Sandia National Laboratory, Albuquerque, New Mexico

Abstract

Authentication is the process of establishing trust in monitoring systems and measurements to verify compliance with, for example, agreements dealing with the storage of nuclear weapons material. Authentication helps assure the monitoring party that accurate and reliable information is provided by any measurement system and that any irregularities are detected. The authentication of a system utilizes a set of approaches, including: functional testing using trusted calibration sources, evaluation of documentation, evaluation of software, evaluation of hardware, random selection of hardware and software, tamper-indicating devices, and operational procedures.

Authentication of measurement systems should occur throughout their lifecycles, including system design, off-site authentication, on-site authentication, and authentication following repair. The most important of these is authentication during the initial design of systems. Hardware and software design criteria and procurement decisions can make future authentication relatively straightforward or conversely very difficult. Facility decisions can likewise ease the procedures for authentication since reliable and effective monitoring systems and tampering indicating devices can help provide the assurance needed in the integrity of such items as measurement systems, spare equipment, and reference sources.

This paper will summarize the results of discussions by U.S. technical experts on the role of procedures in authentication.

INTRODUCTION

A joint[1] Authentication Task Force (ATF) was established in September 2000 to elaborate upon the requirements for authentication of instrumentation that may be used as part of future verification or confidence building activities. The ATF, consisting of technical experts from the DOE National Laboratories, the Defense Threat Reduction Agency, and other governmental organizations, considered authentication in general as potentially applied to multiple regimes of non-proliferation. Four working groups of the ATF developed reports on aspects of authentication, specifically, Procedures and Integration, Hardware, Software, and Policy. This paper reports on the discussions of the Procedures and Integration Working Group of the ATF. An integrated report from the ATF has been developed. [ATF2001]

DEFINITIONS

Authentication is the process by which the Monitoring Party gains appropriate confidence that the information reported by a monitoring system accurately reflects the true state of the monitored item.

Vulnerability Assessment is the set of procedures typically used by the Host Party to identify potential threats to a system and to establish that a system protects classified information. Monitoring Party concerns of system vulnerability are an aspect of authentication.

It should be noted that the definitions of terms vary somewhat between various technical communities, which can lead to some confusion. In the US usage, authentication is the activity applied to equipment to assure correct results are obtained, while the International Atomic Energy Agency (IAEA) applies authentication to the verification of data validity, and applies vulnerability assessment to the equipment assurance [Andress1995, Hatcher1982, IAEA2001]. In the end, all parties generally share a common interest in the protection of the Host's classified information and in the Monitor's desire for correct results.

Because of the requirement to protect the classified information of the Host Party, the measurement systems developed for non-proliferation and arms-control utilize an information barrier to prevent the Monitoring Party from observing such classified information.[2] An *Information Barrier* consists of technology and procedures that prevent the release of Host-country classified information to a Monitoring Party during a joint inspection of a sensitive item, while promoting assurance of an accurate assessment of Host country declarations regarding the item. [Fuller2000] The information barrier blocks the Monitor from access to any classified information, but allows the Monitor complete knowledge of the data processing converting the classified information into an unclassified result confirming whether the material conforms to the Host's declaration by meeting pre-agreed criteria. Authentication carefully explores that data processing and involves a combination of functional testing, and detailed examination of systems and documentation.

Certification is the process by which a Host Party assures itself that an inspection system integrated with an information barrier will not divulge any classified information about an inspected sensitive item to a Monitoring Party. Certification includes all processes required for the Host to allow operation of the system within its facility.

Measurement systems can be classified as *attribute measurement* systems or as *templating* systems. An *attribute* is a specific physics related quantity, such as the ratio of two isotopes as determined from a gamma ray spectrum. The system that makes a measurement and analyzes the data to produce an attribute value must include physics knowledge of the observation. On the other hand, a templating system can be implemented to make a comparison of measurements, such as parts of gamma ray spectra, between an unknown item and a known item. The templating system may just state that the two items are similar without any physics based analysis of the data. Attribute measurement systems are specific examples of radiation measurement systems that are being developed in the United States and the Russian Federation for possible use in future verification or confidence building activities.

A demonstration, the Fissile Material Transparency Technology Demonstration at Los Alamos National Laboratory, was conducted by the US in August 2000, of an information barrier protected attribute measurement system to show the ability to make the type of measurements required for non-proliferation without compromising classified information [FMTTD2000].

There are two basic requirements for both attribute or template measurement system: protection of classified information during and after measurements, and credible performance of the system during the measurement. Under the "*Host supply*" scenario, where the Host Party would supply the system to be used by the Monitoring Party in a Host Party facility to provide paramount protection of any classified information, the crucial authentication issues are that the measurement system correctly measures the attributes, and that there be no hidden features in the system to pass erroneous information.

AUTHENTICATION BASICS

The automated measurement system must be designed from the start to facilitate the authentication process. Thus, the design task becomes much more difficult than merely designing a functional system. Designing for authentication is especially important in a resource-limited regime, where the potential gain from an expedient design decision must be balanced against the cost of the additional authentication effort it may produce. The authentication effort can be viewed as gaining a continuity of knowledge regarding all the data processing occurring within the automated measurement system that comprises the information barrier.

Authentication can be described by a set of high-level guidelines. The basic tenets of authentication are that systems: 1) are designed for correct operation; 2) are assembled as designed; 3) function as designed; and 4) do not contain hidden features that allow the passing of

material inconsistent with accepted declaration. Authentication of systems by a Monitoring Party involves a collection of tools and methods and is operationally realized through:

- the measurement of unclassified radiation reference sources,
- complete documentation for all hardware and software,
- surveillance plus tamper indicating devices placed on system components and enclosures,
- random selection of system hardware and software modules for inspection, and
- private testing of duplicate systems in monitoring party facilities.

Authentication can be facilitated by following a set of reasonable, basic guidelines when a system is being specified and designed:

- Documentation should be complete for all aspects of system hardware and software.
- Hardware components should be simple and without extraneous functionality.
- Hardware components should be laid out for easy physical examination.
- Physical enclosures and shielding should provide a two-way information barrier to prevent both disclosure of information and remote control signals.
- Identical and modular hardware components should be used across a system.
- Hardware and software components should be selected on the basis of availability and share-ability of complete documentation.
- Operating systems should be minimal or non-existent.
- Software should be transparent and well documented.
- Software should be simple, concise, and without extraneous functionality.
- Unused hardware should be rendered inoperable.

System components should be the most basic possible for the measurement task, containing only the required functionality. Since the cost and difficulty of Authentication rises with included functionality and the interaction between system components, extraneous functionality is extremely expensive.

LIFECYCLE OF A MEASUREMENT SYSTEM

Procedures for carrying out authentication are central to the successful implementation of the complex process of authenticating systems. The procedures must allow for the varying requirements of authentication throughout the lifecycle of a system, which can be divided into the following elements with respect to authentication.

- Design – It is essential that systems be designed with the requirements of authentication in mind. Authentication requirements will significantly impact hardware and software design criteria and may impact the overall cost. In some cases, non-optimized performance may have to be accepted to meet the programmatic authentication goals. For example, an older generation of processor might be preferred for simplicity over a newer, more powerful one with a wide array of unnecessary features. Hardware and software design criteria and procurement decisions can greatly influence the available options and costs for authentication.

Facility design and facility monitoring system design decisions can likewise impact the ability to authenticate systems.

- Fabrication – Authentication of a system requires that the procurement, fabrication, assembly, and testing proceed in a manner that has been agreed to by all parties. Authentication activities during fabrication may include monitoring the actual fabrication practices on-site, review of documentation for compliance, sub-assembly testing, random destructive or non-destructive testing of components, and an exhaustive review of all software (source code, compiled/executable, and embedded).

- Installation – Installation for systems requiring authentication must be documented by detailed installation and test procedures. Appropriate physical control or oversight must be maintained of the system during this phase, unless authentication occurs after installation. For example, it is recommended that all installation activities will likely be observed by the Monitoring Party to include equipment installation, software installation, calibration, and testing. Functional testing should be performed as part of the acceptance testing process for a system during the installation phase.

- Operations – Once the facility becomes operational, access may be limited for the Monitoring Party. Some systems may only be used intermittently; in this case, periodic re-authentication prior to each use may be required. Other systems may be in continuous use and re-authentication would by necessity be accomplished by means that do not hinder operations. Whether systems operate in inspector attended or unattended mode will also impact what authentication and continuity of knowledge measures are required. For any complex system some amount of maintenance, upgrade and repair is expected. Re-authentication may be required following such events. Mutually agreed procedures will be required to assure that equipment (e.g., systems, spares, and sources) left in a stored condition between Monitoring Party on-site visits, has remained in a protected state. If the equipment has not remained in a protected state, some level of re-authentication will be required.

APPROACHES TO AUTHENTICATION

Some authentication activities will be common across the lifecycle elements discussed above, while others will be unique to one aspect of the lifecycle. The outcome of authentication is a level of confidence that accurate and reliable information is provided to the Monitor, and that irregularities are detected. It is recommended that the Monitoring Party has the ability to authenticate the correct operation of a system under a variety of conditions spanning a range of operational and off-normal scenarios. Authentication utilizes a set of tools and approaches to provide evidence that a system performs its required tasks, including the following:

- Functional Testing Using Trusted Unclassified Calibration Sources – Radiation sources play an important role in verifying the correct functioning of a system. Artificial sources of data,

such as a recorded pulse train from a similar system or a mathematical model of the system, can be a valuable cross-reference means of validating physical sources and of functionally testing a system over a broader range of source values. An additional feature of an artificial data source is that it may, in principle, be used to transfer a calibration point between identical measurement systems.

- Evaluation of Data – The data provided by a system must be validated. Depending upon the complexity of the system this may be a simple task or this could be a very time consuming and difficult task. The validation of the data displayed, stored, or removed is possibly independent of software and hardware that has been authenticated. Data must be protected from tampering throughout its lifecycle.

- Evaluation of Documentation – Examination of hardware, software, operations and maintenance documentation, and a comparison of these documents with the as-built system can be an important tool in determining the validity of the authentication scheme. Examination of documentation can also help define sensitive design points for targeted authentication procedures.

- Evaluation of Software – Software exists at several levels in systems, from firmware to acquisition software to analysis software to operating systems. An examination of all software, including source code, is central to authentication. A necessary component of the software evaluation is the use of the same compilers and associated software tools used to produce the executable code. A means for determining changes in the agreed upon software should be incorporated in the design and inspection procedures. All software must be available as source code form, or be a mass commodity product, and be fully documented. Compiled and executable software either stored on magnetic/optical or other fixed media or in firmware must be shown to be identical to the source code. Commercial software with a significant market might be obtained through a blind buy as a means to assure that it is free of tampering.

- Evaluation of Hardware – A variety of hardware makes up a system (e.g. detectors, computers, power supplies, data acquisition boards, etc.). An examination of these components is critical to authentication.

- Random Selection of Hardware and Software – Random selection of hardware and software components or systems is a powerful authentication tool. Any party attempting to subvert any particular module must do so with the knowledge that the Monitor will be examining one of these modules during private inspection at a Monitor's facility. Random selection will be one of the tools used during on-site authentication efforts. Random selection can be applied at the component level or the system level. Random selection can be used in two possible modes. A large number of components or systems can be procured or built and the

Monitoring Party can select which components or systems are to be used during equipment assembly or operation. The Monitoring Party may also identify specific components or systems to be placed in secure storage or to be shipped off-site for further examination.

- Usage of Tamper Indicating Devices – Tags, seals, and other tamper indicating devices (TIDs) are important verifications of the physical integrity of systems. Tamper indicating devices provide some assurance of continuity-of-knowledge of a system and its components. Tamper indicating devices are of great importance for equipment that operates in unattended mode.

- Usage of Surveillance - To increase the level-of-confidence that systems have not been modified or altered by the Host Party, surveillance systems are routinely used to augment the protection that TIDs provide. Defeating an enclosure sealed with a TID and viewed by a video surveillance system, for example, requires the generation and simultaneous application of two separate tampering strategies.

- Usage of Procedures – Documented procedures should be provided for all aspects of authentication and for any other on-site activities that affect the reliability of a system to provide accurate information. Formal procedures, for example, clarify the respective roles of the Host and Monitor Parties during random selection.

EXAMPLES OF AUTHENTICATION DURING NORMAL OPERATIONS

During normal operation of a facility, information will potentially be provided to the Monitoring Party through a combination of Host declaration, unattended measurements, and on-site inspections. Declarations might include information on each item entering and leaving a facility along with declared attributes for each item. Unattended measurements might include video surveillance of equipment and material that could be reviewed during on-site visits to insure continuity of knowledge of measurement equipment. On-site inspections should have as an important goal the measurement of items with authenticated measurement equipment. The measurement equipment would undergo some level of authentication prior to use during such on-site visits. Such authentication procedures could include, but not be limited to, the following:

- Checking TIDs on systems, components, and reference sources.
- Establishing characteristics of reference sources through independent measurements.
- Examining facility-monitoring information to provide continuity of knowledge of measurement equipment and reference sources.
- Performing functional testing of the system with randomly selected reference sources.
- Performing random comparisons of physical components to documentation.
- Performing random comparisons of software components to documentation.
- Verifying that the installed software and firmware exactly match the golden copy.
- Performing random selection of system components for possible off-site authentication procedures.

Following a repair or upgrade of a system, it will be necessary to re-authenticate the system.

APPLICATION OF TOOLS FOR AUTHENTICATION

Table 1 provides examples of a few of the possible uses of authentication tools at various stages of a system lifecycle. These examples show how tools can be used at various points as a system lifecycle progresses. The cumulative effect is to help insure that confidence is established in the system and that the system is designed and implemented to be authenticatable and to provide reliable measurements. Each entry in the table will have associated mutually agreed procedures for implementation.

Figure 1 indicates conceptually how the cost or time required for authentication is related to the level of confidence in a system. Generally speaking, as the required level of confidence is increased, the cost and time needed to authenticate the system will grow nonlinearly. Policy decisions will determine the desired level of confidence in a system. This then implies the level of technological implementation that will meet the requirements. Examples of how different tools can be used to increase confidence are shown in Table 2.

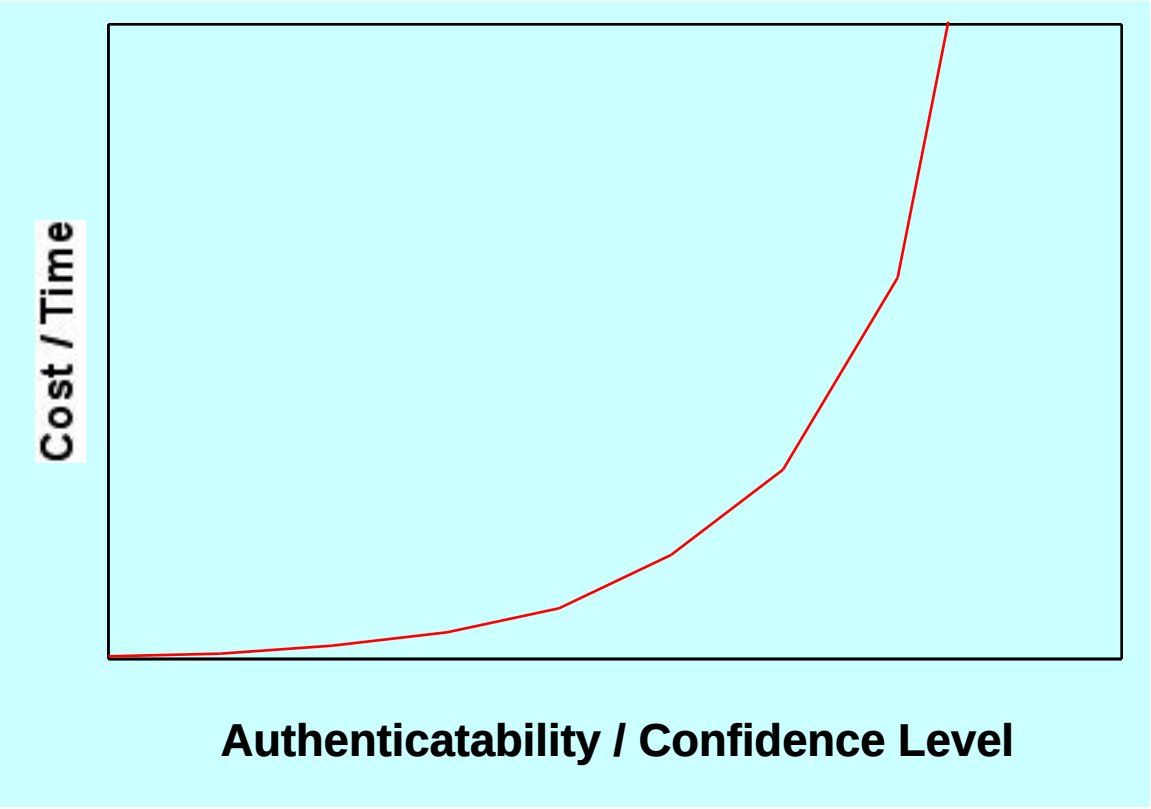

Figure 1. Authentication helps create a certain level of confidence in a system. Generally speaking, as the required level of confidence (or authenticatability) is increased, the cost and time to authenticate the system will grow nonlinearly. Note that the confidence level can approach, but not reach, 100% even for very large expenditures of time and money.

Tool→ **Lifecycle Element**	*Functional Testing*	*Evaluation of Data and Documentation for Hardware and Software*	*Random Selection*	*Usage of TIDs and Surveillance*	*Usage of Procedures*
Design		Specify and select authenticatable components.			Follow authentication guidance.
Fabrication	Component testing.	Generate complete documentation and revision history. Compare to independently procured components.	Quantity purchase of commercial off the shelf components.		Follow authentication guidance.
Installation	System testing with physical and electronic sources.	Assure complete documentation. Comparison of design to as built system. Comparison of software to documented source. Photographic baseline.	Random selection of system hardware or software components, or of entire systems for private examination.	Place TIDs on system components, enclosures, spares, sources, and rooms.	Follow defined procedures for entry and exit, functional testing, random selection, system operation, and placement of TIDs.
Operation	Random selection of system testing with physical and electronic sources.	Random comparison of system components with documentation including photographs.	Random selection of components such as PROMS; random selection of test sources.	Remove and inspect TIDs; evaluate facility monitoring video coverage of systems.	Follow defined procedures for entry and exit, functional testing, random selection, system operation, and placement of TIDs.

Table 1. Examples of some of the possible uses of authentication tools at various stages of a system lifecycle. Clear guidance in the above areas must be provided to achieve cost and schedule estimates.

Tool→ **Level of Confidence**	*Functional Testing*	*Evaluation of Data and Documentation for Hardware and Software*	*Random Selection*	*Usage of TIDs and Surveillance*	*Usage of Procedures*
Modest Confidence Level Examples	On-site functional testing with randomly selected sources.	Validate completeness of crucial documentation.	Random selection of system hardware or software components during on-site inspections.	Passive TIDs applied to measurement equipment and reference sources.	On-site procedures to verify continuity of knowledge for measurement systems and reference sources.
Medium Confidence Level Examples	On-site functional testing with a set of physical and electronic sources.	Validate completeness of crucial documentation, and make selected comparisons to as built hardware and software.	Random selection of system hardware or software components, or of entire systems initially, and during on-site inspections.	Passive TIDs applied to measurement equipment and reference sources; active TIDs on selected rooms and equipment.	On-site procedures to verify continuity of knowledge for measurement systems and reference sources.
Higher Confidence Level Examples	On-site functional testing with set of physical and electronic sources; Monitoring Party-site full functional testing program.	Validate completeness of documentation, and make complete comparisons to as built hardware and software.	Random selection of system hardware or software components, and of entire systems initially, and during on-site inspections.	Active TIDs applied to measurement equipment, reference sources and rooms; facility monitoring of all equipment and material, including video surveillance.	On-site procedures to verify continuity of knowledge for measurement systems and reference sources.

Table 2. Examples of level-of-confidence in a system versus possible uses of authentication tools to obtain that level of confidence. These are examples only, and are not meant to imply that a level of confidence is reached through the listed activities alone.

INTEGRATION ISSUES FOR AUTHENTICATION

Integration of systems from components or subsystems has historically been a significant time consuming exercise. When systems are integrated at a Host facility, problems may arise from the integrated system, which were not apparent or even present at the unit/module level. Examples would include backgrounds in radiation measurement systems introduced by proximity to other equipment, operational conflicts between material flow and measurement system operation, and issues of impacting continuity of knowledge of measurement systems and reference sources by inadequate placement of facility monitoring equipment.

There are two key issues regarding authentication during system integration. First, continuity of knowledge of the measuring equipment must be maintained. This will give the Monitoring Party some assurance that the equipment that was previously authenticated is the same equipment that will be used in the final system. Second, care must be taken to avoid any loss of confidence due to the interactions between the various elements of the system. Just because each element operates correctly in a "stand-alone" mode, does not mean that all of the elements will operate correctly when attached to each other.

Integration issues for authentication of systems used for transparency measurements are exacerbated because some or all of the measurements made will nearly always include classified information. Inclusion of an information barrier to protect this information complicates system integration. A detailed integration plan must be prepared with a detailed testing plan being a key element. The information barrier aspect of the equipment will hinder the debugging of the combined system.

Integrators must take care not to allow side effects stemming from hardware and/or software that establishes and monitors the operational mode of the system to inadvertently affect the operation of the instrument or its result. For example, the measurement system must not be able to determine if it is open or closed mode. The measurement system must receive definite and very limited operator or host controlled input. If this is not the case, then the Monitoring Party cannot have confidence that the system will return the same results in various operational modes.

PROCESS FOR GENERATION OF AUTHENTICATION PROCEDURES

Moving from abstract guidelines to usable procedures for authentication requires a process that incorporates policy considerations and regime specific constraints. The first step in this process is to assess: "what are the possible spoofing methods that could be used against the equipment being authenticated, what is the likelihood the Host will use a given method, and what is the cost to the Host if the spoofing is detected?" The results of this assessment are generally sensitive information.

Once this assessment is complete, then the Monitor needs to assess how much authentication activity is reasonable. There are several factors that must be considered in deciding what authentication activities to undertake. The assessment of how much authentication activity is

enough is also sensitive information. It is a deterrent if the Host does not know all methods used to authenticate equipment.

Once an authentication strategy has been developed, the next step in the process is to adapt the strategy to the facility or facilities where it will be carried out. The quality of the authentication effort rests on the degree of access to the equipment provided under the negotiated protocols. Facility specific details such as source and equipment storage, access restrictions, health and safety requirements, all must be understood before authentication procedures can be negotiated and finalized. Because authentication activities impact facility operations, finalizing authentication procedures is usually an iterative process between the Monitor, the Host and the facility operator.

SUMMARY

Authentication is a necessary aspect of the implementation of systems for the assurance of compliance with non-proliferation and arms-control agreements. A consistent basis for this authentication activity has been developed by the United States technical community.

Some high level conclusions and recommendations are:

- Procedures must allow for authentication throughout the lifecycle of a system.
- Authentication procedures must be defined and jointly accepted for each application, each system, and each applicable lifecycle element.
- The Monitoring Party should negotiate the ability to authenticate the correct operation of a system under a variety of conditions spanning the range of operational and off-normal conditions and scenarios.
- Policy guidance should establish the desired level of confidence required from the authentication process, which will then determine the authentication activities.
- Systems must be designed for the ability to be authenticated, and to minimize the amount of authentication required to achieve confidence in system operation.
- Simplicity of design and good engineering practices are desirable to reduce the cost and time required for authentication.
- System design must consider how on-site procedures and conditions might affect the robustness of the hardware design and operation.

ACKNOWLEDGEMENTS

This work was supported by the U.S. Defense Threat Reduction Agency and by the U.S. Department of Energy. Pacific Northwest National Laboratory is operated for the U.S. Department of Energy by Battelle under contract DE-AC06-76RLO 1830. The joint DOE-DoD Authentication Task Force working group on Procedures and Integration has discussed and evaluated the issues presented here.

REFERENCES

[Andress1995] J.C. Andress, *The Assurance of Genuineness*, 17th European Safeguards Research and Development Association (ESARDA) Annual Symposium on Safeguards and Nuclear Material Management, Aachen, Germany, May 9-11, 1995.

[ATF2001] Authentication Task Force Report, June 2001. Washington, DC

[FMTTD2000] Fissile Material Transparency Technology Demonstration at LANL, August 2000, www-safeguards.lanl.gov/FMTT/index_main.htm.

[Fuller2000] J. L. Fuller, *Information Barriers*, PNNL-SA-33328, Pacific Northwest National Laboratory, Richland, WA, June 2000.

[Geelhood2000] B. Geelhood, R. Kouzes, W. K. Pitts, *Design Guidelines for Authenticatable Systems*, PNNL-13386, Pacific Northwest National Laboratory, Richland, WA, November 2000, updated May 2001.

[Hatcher1982] C. R. Hatcher, S.T. Hsue, and P. A. Russo, *Authentication Of Nuclear Material Assays Made With In-Plant Instruments*, IAEA-SM-260/103, International Symposium on Recent Advances in Nuclear Material Safeguards, Vienna, Austria, November 8-12, 1982.

[IAEA2001] *Procedure for the Authorization of Equipment Systems and Instruments Software for Inspection Use*, Department of Safeguards, February 2001, IAEA, Vienna, Austria.

[IBWG1999] Joint DoD/DOE Information Barrier Working Group, *Functional Requirements and Design Basis for Information Barriers*, PNNL-13285, Pacific Northwest National Laboratory, Richland, WA, May 1999.

[1] The Procedures and Integration Working Group of the Joint DOE/DoD Authentication Task Force (ATF).

[1] U.S. Department of Defense (DoD), Defense Threat Reduction Agency – Department of Energy (DOE) National Nuclear Security Administration, Office of Defense Nuclear Nonproliferation

[2] The Joint DOE-DOD Information Barrier Working Group (May 1999) report [IBWG1999] states that the fundamental functional requirements for the information barrier portion of an integrated radiation signature-information barrier inspection system are twofold:

i. The host must be assured that his classified warhead design information is protected from disclosure to the monitoring party, and
ii. The monitoring party must be confident that the integrated inspection system measures, processes, and presents the radiation signature based measurement conclusion in an accurate and reproducible manner.