SANDIA REPORT

SAND2014-19460
Unlimited Release
Printed November 2014

Spent Fuel NDA Project: Data Authentication Considerations

George T. Baldwin

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-2087
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: http://www.ntis.gov/help/ordermethods.aspx#online

SAND2014-19460
Unlimited Release
Printed November 2014

Spent Fuel NDA Project: Data Authentication Considerations

George T. Baldwin
International Safeguards & Technical Systems
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1371

Abstract

The overall spent fuel nondestructive assay project seeks to develop improved measurement capability for the verification of spent nuclear fuel, especially before its disposal or movement to hard-to-access storage. Various systems are being considered, employing neutron and/or gamma radiation detection with either passive or active methods; their use scenarios are not yet well defined. In a practical deployment, the measurement system would likely need to operate in unattended mode. The output results may also need to be shared between multiple recipients with various interests. The data authentication task considers what issues are important in being able to trust the measurement results. By defining and analyzing a generic "baseline" system scenario, we have identified five key factors needing specific attention: application use-case details, equipment tamper indication, supporting (ancillary) instruments, systems implementation, and instrument state-of-health reporting.

ACKNOWLEDGMENTS

Support to Sandia National Laboratories provided by the NNSA Office of Nuclear Safeguards and Security, Next Generation Safeguards Initiative is gratefully acknowledged. Many others on the multi-laboratory Spent Fuel NDA Project Team contributed with helpful discussions and information about the various NDA systems, particularly Steve Tobin and Holly Trellue. I also wish to thank Dianna Blair and Heidi Smartt for reviewing the draft, Mike Coram and Maikael Thomas for contributions to the cryptography discussion, and Laura Hansen for the formatting of the report.

CONTENTS

FIGURES

TABLES

ACRONYMS

BU	Burnup
BWR	Boiling Water Reactor
CIPN	Californium-252 Interrogation with Prompt Neutron Detection
CoK	Continuity of Knowledge
CRISP	Central RADAR Inspection Software Package
CT	Cooling Time
DDA	Differential Die-Away
DDSI	DDA Self-Interrogation
DOE	(U.S.) Department of Energy
ESARDA	European Safeguards Research and Development Association
FDET	Fork Detector
IAEA	International Atomic Energy Agency
IE	Initial Enrichment
InfCirc	Information Circular (publication of the IAEA)
INMM	Institute of Nuclear Materials Management
LEU	Light Enriched Uranium
NDA	Nondestructive Assay
NGSI	Next Generation Safeguards Initiative
NNSA	National Nuclear Security Administration
ORIGEN	Oak Ridge Isotope Generator (series of computer codes for simulating radioactive material buildup and decay in spent fuel)
PA	Partnership Agreement
PNAR	Passive Neutron Albedo Reactivity
PWR	Pressurized Water Reactor
RADAR	Remote Acquisition of Data and Review
SF	Spent Fuel
SFA	Spent Fuel Assembly
SINRD	Self-Interrogation Neutron Resonance Dosimetry
SKB	Svensk Kärnbränslehantering AB (Swedish Nuclear Fuel and Waste Management Company)
TIE	Tamper Indicating Enclosure

1. INTRODUCTION

Data authentication is just one task supporting the Next Generation Safeguards Initiative (NGSI) Spent Fuel (SF) project. The purpose of the project is to strengthen the technical tools for safeguards inspections. The technical goals are to develop improved nondestructive assay (NDA) to:

- Verify initial enrichment (IE), burnup (BU), and cooling time (CT) in facility declarations,
- Detect the diversion or replacement of fuel pins, and
- Quantify the mass of plutonium (Pu) in SF.

The measurement approaches being developed are limited to commercial reactor fuel, where SF exists as intact fuel assemblies in water cooling ponds. While the project has been underway now for several years, this report marks the first consideration of data authentication for envisioned deployment scenarios.

Measuring SF plutonium content is of primary interest for international nuclear material safeguards. In particular, the International Atomic Energy Agency (IAEA) is interested in these improved technical tools for "partial defect verification" before SF transfers to long-term, hard-to-access storage or disposition. For example, we envision routine application at an encapsulation plant, prior to ultimate disposal of the SF in a geological repository.

The scope of the data authentication task is broader than simply data authentication, per se.[1] "Data surety" may better reflect the appropriate higher level concern. (Baldwin & Tolk, 2009) We pose the question:

> *Assuming that an instrument would be deployed for routine application to spent fuel safeguards measurements, what else may be necessary for a safeguards inspectorate to be able to trust the measurement results?*

"Trust" is the key word in this consideration. While cryptographic means to authenticate digital data may be a necessary element for trust, it is by no means sufficient. One also has to be assured that the equipment itself has not been altered, that the item being measured is indeed what is claimed, that the measurement geometry is correct, the instrument is configured as intended, and so forth.

There are yet other factors that will be critical to implementing a SF measurement system, such as reliability, ease of operation, maintainability, and so on, but those are beyond the scope of this report.

Because the NDA systems being considered are still in development, we must make assumptions about what the "production" version of these systems would look like, and how they would be

[1] See Appendix.

employed in practice. By considering the data authentication problem in broad perspective now, we can anticipate potential issues for deployment. There may still be time to make changes before costly decisions are made.

Several measurement systems are candidates for eventual deployment for SF NDA. Specifically, those we consider are summarized in Table 1. The systems differ in the technical approach used to elicit information from the spent fuel assembly (SFA). Individually, these NDA systems will not be described further in this report; instead, references are given for the requisite background information.

Table 1 Candidate SF NDA Instruments

CIPN	Californium-252 Interrogation with Prompt Neutron Detection
	Fission chambers embedded in polyethylene surround a SFA to detect neutrons. Two measurements are done, passive and active. CIPN detects the neutrons passively emitted from the SFA, as well as the increased signal when the SFA is interrogated with a nearby ^{252}Cf neutron source. (Hu, et al., 2012) (Hu, et al., 2012)
DDA	Differential Die-Away
	DDA begins with a neutron generator burst; the burst neutrons thermalize and induce fission in the SFA. Those induced fission neutrons are then detected with ^{3}He tubes embedded in polyethylene, each within a Cd shield. (Henzl, Swinhoe, Tobin, & Menlove, 2012)
DDSI	DDA Self-Interrogation
	DDSI "interrogates" the SFA with neutrons originating from any random spontaneous fission event in the SFA (thus self-interrogation; there is no external neutron source). The neutron detectors are arrays of ^{3}He tubes embedded in polyethylene on three sides of the SFA. There is a lead shield between the SFA and the detectors. (Menlove, Menlove, & Tobin, 2009) (Belian, Menlove, Swinhoe, & Tobin, 2012)
FDET	Fork Detector
	FDET has two polyethylene "arms" positioned on opposite sides of a SFA. Each arm includes an ion chamber and two fission chambers, one bare and the other enclosed in cadmium, thus measuring gammas, thermal neutrons and fast neutrons, respectively. The ion chamber runs in current mode; the fission chambers in pulse mode. (Vaccaro, et al., 2013)
PNAR	Passive Neutron Albedo Reactivity
	PNAR uses fission chambers to detect neutrons emanating from the SFA in both a multiplying configuration (i.e., surrounded by polyethylene) and a non-multiplying one (i.e., surrounded by an air chamber lined with cadmium). Multiplication (related to fissile content) can be derived from comparing signals from the two axially-separated sections. (Eigenbrodt, et al., 2014)
SINRD	Self-Interrogation Neutron Resonance Dosimetry
	SINRD measures the relative ^{239}Pu and ^{235}U content in the SFA, based upon the different neutron signals from fission chambers encased in various absorber materials (cadmium, gadolinium, hafnium, and boron) and thicknesses. (LaFleur, Menlove, Tobin, & Swinhoe, 2010)

An eventual NDA deployment might turn out to be some combination of the methods in Table 1 and others, as discussed elsewhere. (Tobin & Jansson, 2013) Moreover, certain other advanced SF NDA systems might also be considered, such as calorimetry, tomography, Cerenkov viewing, and others, yet they were not included in this study for data authentication. Nevertheless, to the extent that the systems share certain common features, the findings in this report may be useful to inform consideration of data authentication practices for the other instruments or combinations of instruments.

With the possible exception of the unattended FDET, all of the systems in Table 1 should be regarded currently as developmental prototypes. A "production" system for routine deployment would include system engineering to meet the additional operational requirements (including, but not limited to, those related to data authentication).

For the purposes of this data authentication task, we will consider the systems generically. The systems may be active, i.e., produce a signal from an item under test in response to an external neutron source, or passive, i.e., derive a measurement signal from the item without such a source. Active systems employ either a radioisotope neutron source, such as ^{252}Cf, or a neutron generator (only DDA). The distinction is important, because radioisotope sources are always emitting neutrons; a neutron generator on the other hand can be turned "on" or "off."

2. MEASUREMENT SYSTEM OBJECTIVES

2.1 What is measured

Ideally, a deployed SF NDA system would give count rates that can be used to meet the goals of the project (IE, BU, CT, pin diversion and Pu mass) through a technique called data mining, which mathematically fits signals to initial parameters. (Burr & Tobin, 2014)

Most published work describing the candidate SF NDA systems refers to "what is measured" as the final output from the entire device as a whole. From the data authentication perspective, however, we also need to be concerned not just with the results, but with the internal details of any exposed data within the instrument, since none of the systems presently comes neatly packaged within a single tamper-indicating box.

2.2 Where/when the measurement is employed

While in principle the SFA could be measured at any time after discharge from a nuclear reactor, here we assume that the primary application would be near the end of its life cycle, before transferring the SFA to long term storage or disposal in a geological repository. In particular, we envision an instrument installed at an encapsulation facility, used to make a final assay of the SFA in water before transfer out of wet storage.

In principle, the measurement could take place at the reactor SF cooling pond, before a SFA is shipped to interim storage or an encapsulation facility. Whatever the case, safeguards would require maintaining continuity of knowledge (CoK) of all SFAs after measurement, even during transport, to avoid any need for reverification. Final measurement at reactor sites would entail more SF NDA instruments and deployment locations, as well as greater demands on containment and surveillance measures to maintain CoK.

Given the large inventory of SF to be measured, any SF NDA system would need to operate without an inspector present (an "unattended" system). Optionally, the system may report results over a communications link to a recipient, thus termed a "remote [monitoring]" system. The IAEA implementation of remote monitoring is guided by Policy Paper 16. (IAEA, 1998) (Abedin-Zadeh, et al., 1998)

2.3 Who will be using the measurement results

The SF NDA systems are intended primarily for the purpose of a safeguards inspectorate. The inspectorate may be Euratom, IAEA, or both. If both, a system is considered to be under joint use, which is governed by the IAEA Policy Paper 20 (International Atomic Energy Agency, 2006) as well as the Euratom-IAEA Safeguards Agreement (International Atomic Energy Agency), as amended, (International Atomic Energy Agency, 2005) and the Partnership Agreement (PA). (Thorstensen & Chitumbo, 1995) (International Atomic Energy Agency, 2008)

Information from the systems might also be shared with a facility operator and/or state regulatory authority. The various possible combinations of interested parties have major implications for the data authentication problem.

2.4 How the measurement results are used

It is not entirely clear how the information from a SF NDA measurement would be used; for now, we make assumptions and leave some questions unanswered.

IAEA safeguards involve the voluntary declaration of nuclear material by the state, followed by independent verification of that declaration by the inspectorate. Most likely the SF NDA system would be used for the latter, independent verification by the inspectorate. In that case, the inspectorate will insist on receiving the operator declaration before it would agree to share those verification measurement results with the operator. In other words, the "independent verification" requirement precludes the operator from using the SF NDA measurement to inform that declaration (unless the two parties happened to be using separate and independent instruments).

After safeguards verification, then what? It seems inconceivable that the IAEA would permit the SFA to proceed to encapsulation if verification were unable to confirm the operator declaration. Does the safeguards verification therefore function as a go/no-go decision for the operator on whether to forward the SFA to encapsulation? If so, how promptly must the inspectorate inform the operator after the verification measurement?

Furthermore, the operator may want to use the measurement results to inform a decision about the further handling of a particular SFA in the encapsulation process. The decision may have nothing at all to do with safeguards considerations. For example, the operator likely needs to anticipate heat loads on the canisters containing SFAs. Based upon the SF NDA measurement, the operator might decide not to add a particular SFA to a disposal canister.

Especially when considering such multiple-party involvement in the measurement system, it is therefore important to realize that each party may have different measurement system objectives. Provided that the objectives are not mutually exclusive, they may still conflict, putting constraints on the sequence and timing of the data sharing and imposing additional requirements on data authentication. See Recommendation 1.

2.5 Caveat: The problem space is still not well defined

The disposal of SFAs in a geological repository is a relatively new and evolving development for the nuclear fuel cycle. The associated international safeguards approach itself is not yet fully defined and may change in the future. Moreover, different safeguards authorities (e.g., IAEA and Euratom) may establish different requirements. Here we do not only mean the requirements for an NDA partial defect measurement alone, but the requirements for all related issues—data security, joint use provisions, and so on. Here we rely on the best available information and past experience, but cannot guarantee that we anticipate all of the requirements that could arise.

3. CRITICAL MEASUREMENT FACTORS

The SF NDA measurement assumes that the user knows (and can trust) several critically important factors:

- What item (SFA) is being measured
- The integrity of that item
- The position of that item with respect to the NDA instrument
- The absence of anything extraordinary in the vicinity that could affect the measurement (e.g., capable of adding to or blocking the radiation signal)
- The integrity and configuration of the submerged instrument (potentially multiple factors, such as bias voltage on detectors, …)
- Integrity of the tether (see Figure 1)
- Integrity and configuration of the instrument electronics
- Timing (i.e., coincidence of all of the above factors with the data acquisition time)
- The reported output data stream

For active systems, additionally:

- What neutron source is being used
- Its packaging
- The position of that source with respect to the NDA instrument and item under test
- For a neutron generator: when it was pulsed, and the defining parameters for the pulse

Note that in the case of active systems, verification is a differential measurement. It involves both an active and a passive measurement (i.e., with and without the neutron source present, respectively). The stronger detected neutron signal for the active measurement is due to both the additional source neutrons and their multiplication through induced fission in the SFA. The passive measurement is usually made by removing the source to a distant, shielded location, or, in the case of a neutron generator, simply by keeping it turned off.

Even with passive systems, multiple measurements with differing configurations may be necessary (for example, the introduction of a neutron absorber, such as a cadmium liner, between the item under test and the detectors). Again, it is critical that any recipient of the measurement information can trust the associated environmental conditions and instrument configuration in all cases.

None of these factors is much of an issue when testing a development instrument attended by a knowledgeable expert. A production environment, however, where there is no expert present and a distant recipient is trying to make sense of a remote monitoring data stream, presents a much more complicated problem. One must be concerned both with accidental faults (e.g., the wrong item placed in the NDA instrument) and intentional acts at deception (e.g., insertion of neutron absorbers in the pool water).

The envisioned use scenario is still not entirely clear for the SF NDA system. At a minimum, and to simplify the consideration, we first assume that the measurement constitutes (only) an independent verification of SFAs by a single safeguards inspectorate, without any sharing of

information with other parties or any effect on the facility process flow. Any other elaboration of this “baseline” use scenario introduces further complications to the data authentication problem. In a later section we will consider one likely complication, the sharing of measurement with multiple parties.

4. BASELINE SYSTEM SCENARIO AND ASSUMPTIONS: GENERALIZED NDA SYSTEMS

Even given the uncertainties, there is much that can be done to investigate data authentication issues for the measurement. Our baseline scenario assumes a permanently installed system. We rule out any use of portable equipment, because the NDA system is expected to be in routine unattended use, eventually for tens of thousands of SFA measurements.

Figure 1 illustrates the generalized measurement scenario. Essentially the NDA systems rely on sensing radiation (gamma and/or neutron), which emanates from the item under test. In active systems (only), there is also a nearby neutron source, either steady-state or pulsed, which serves to "interrogate" the item under test. The NDA instrument, the source and the item under test all operate while submerged under water in a SF storage facility.

The figure might suggest that the neutron source is somehow detached and "loose," but that is not the case. The location of the neutron source, when it is required for the measurement, must be fixed with respect to the NDA instrument, to ensure a consistent illuminating neutron flux.

The detection element of the NDA instrument must be in close proximity to the item under test. Reproducible measurement geometry is important, as well as (for neutron coincidence counting in particular) radiation detection efficiency. The generalized instrument design therefore surrounds the fuel on three or four sides. As an unattended system, we assume that the NDA instrument is in a fixed location and that facility remote handling moves the SFA into the instrument for measurement and removes it when the measurement has finished. For a four-sided instrument, either the SFA would enter by being lowered into it from above, or the instrument includes a movable side (e.g., a door) to allow the SFA to enter from the side.

After the SFA is positioned within the NDA instrument, it may be held stationary for the duration of the measurement, repositioned at various axial locations, or even scanned while moving axially. The use case(s) have not yet been precisely defined. In any of these cases, however, the instrument configuration may also need to be changed deliberately, such as to introduce a source, and the measurement repeated with the new configuration.

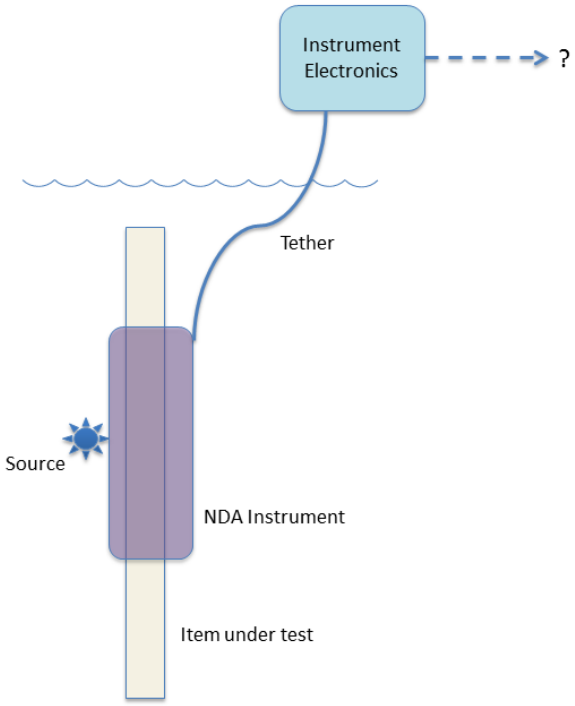

Figure 1 Baseline system scenario (not to scale)

Typically the NDA instrument is sensing only a finite axial section of a SFA. The measurement is likely fairly tolerant of variation in axial position, yet there needs to be some means to determine the axial position of the SFA in the NDA instrument. This is especially true for SFA with tailored axial enrichment profiles. Sweden has considered the possibility of measuring boiling water reactor (BWR) SFAs at three locations. (Tobin & Jansson, 2013, p. 9)

In contrast to the detection element of the NDA instrument, much of the associated electronics for the system ideally should not be exposed to a high radiation environment, and therefore would be separated by distance and shielding from both the item under test and the neutron source. As shown in Figure 1, a tether connects the NDA instrument to the control and data processing electronics that are outside of the pool, perhaps a few meters away. The tether would be a cable bundle carrying control signals, data, and electrical power. Although we illustrate it here suggesting a flexible connection, in practice this could be realized instead as a rigid connection such as a pole, conduit or pipe.

The signals being passed up the tether to the instrumentation electronics are typically either analog tail pulses or logic timing pulses. Current mode detectors (e.g., ion chambers) are an exception, where the time-varying signal amplitude conveys the detector information. For pulse mode detectors, it is the number and timing of the pulses (e.g., count rate) that encodes the information of interest to the electronics. There may be multiple signal cables bundled in the tether, ideally one for each physical detector in the instrument. These timing pulses are being tallied by pulse counting, shift register, or list mode electronics of some sort, in an electronics package somewhere nearby but outside of the pool. Also in the tether would be power for biasing

the detectors and operating the electronic components in the submerged instrument (e.g., preamplifier, amplifier, pulse height discriminator).

The instrument electronics piece of the system includes everything else for the measurement system that does not otherwise need to be in close proximity to the SFA under test. Some flexibility may exist in the precise division of the system between the in-pool and out-of-pool pieces.

Depending on the particular instrument, for any given SFA, there in general may be multiple measurements with different conditions. There can be a measurement with a neutron source present, and another without. Similarly, a measurement could include a cadmium liner between the SFA and the detector, or not. A given SFA may be measured at various axial positions. Count times of 100s are typical, but in general could vary.

5. DATA SURETY ISSUES FOR THE BASELINE SCENARIO

The most straightforward problem for data authentication is the single remote user. In particular, this could be independent verification by safeguards inspectorate. Two fundamental questions must be answered: 1) Can I, as the remote user, trust the validity of the measurement result I receive, and 2) can I also be confident that none of the measurement information has been revealed to anyone else?

The validity of the measurement result depends on several factors, which were listed in the previous section. Here we group those factors into three considerations: 1) the measurement equipment integrity, 2) the measurement environmental conditions, and 3) neutron source considerations.

5.1 Equipment Integrity

The remote user must be assured that no one is able to manipulate the instrument artificially at the facility. That "end point" of the measurement system must be intact and secure, such that any tampering with the equipment would be detected.

Typically, safeguards instruments that must operate unattended in the facility (such as surveillance cameras or electronic seals) are fully enclosed in tamper indicating enclosures (TIEs). The TIE does not prevent deliberate or accidental breaches of the equipment periphery, but does dependably indicate it. "Indicate" often requires occasional visual inspection (e.g., to notice a surface irregularity in a powder-coated case, which suggests attempted repair of a hole); in other cases, the equipment may be able to report the breach promptly and remotely (e.g., a microswitch that is activated when a cover is removed). Measurement results from the equipment can only be accepted as true on the condition that the tamper status is verified.

We illustrate an idealized periphery of this end point with the dashed line in Figure 2, where all of the various pieces of the measurement system are within a single tamper-indicating enclosure. Assuming that such a periphery could be secured, breached only by facility mains power and possibly a remote communication link carrying secured (cryptographically-signed) digital information, then the remote user is better able to trust that the output from the system is a faithful measurement.

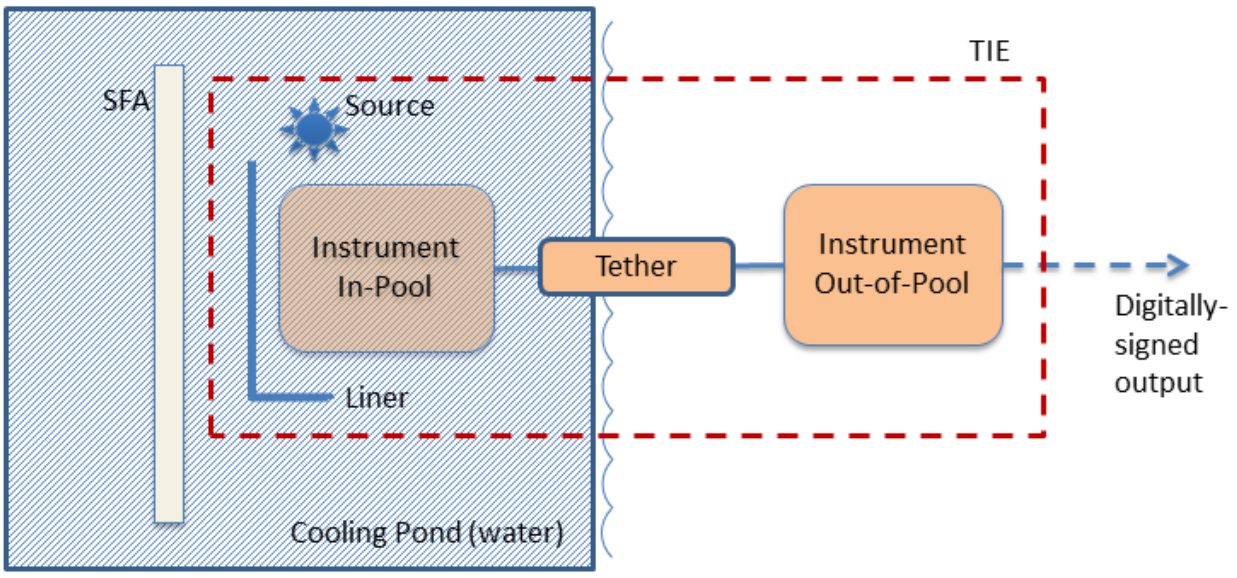

Figure 2 Rearranged baseline scenario for SFA measurements

Results emerge from the secured endpoint as digitally-signed data, but that digital signature can only be trusted if we are confident that the hardware and software cryptographic tools within the endpoint have not been compromised. Furthermore, the data stream itself must be trusted to originate from the measurement instrument. A valid digital signature applied to fraudulent data is not only meaningless, it would be deceptive.

Clearly the idealized dash line does not translate easily to a physically-realizable TIE. For example, a radioisotope neutron source, or a cadmium liner, may need to be separate from and outside of the TIE. If so, it must be kept in mind that these will then become external factors in the measurement.

But consider the other extreme: Imagine that we only include the out-of-pool instrument in the TIE, as in Figure 3. Unless some means are used to assure the integrity of the instrument pieces outside of the TIE, there can be no guarantee of what we're measuring. Signals entering the out-of-pool instrument could be from any source. Although we may still be able to protect the cryptographic keys used to sign the digital output information stream, just what data would we be "signing"? Digitally-signed garbage is still garbage. There is no a priori reason to consider that the other parts of the instrument are immune to tamper. How could we know whether or not the out-of-pool instrument was merely looking at the signal from a remote-controlled tail pulse generator, rather than the signal from fission chamber detectors?

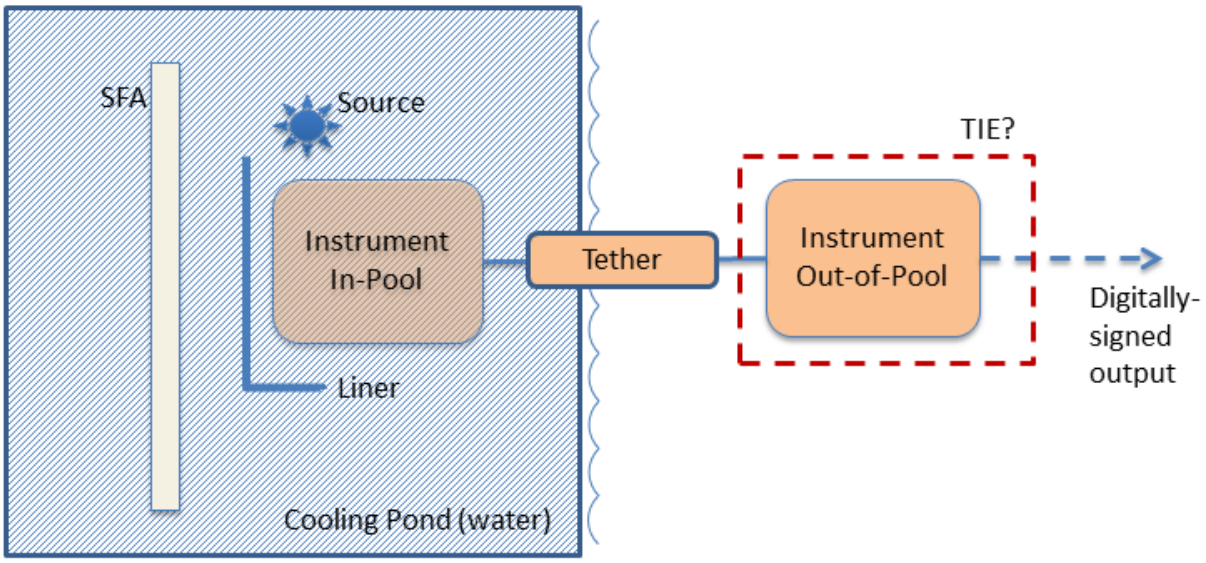

Figure 3 Limited application of equipment tamper indication

Presently, none of the SF NDA instruments currently incorporates tamper indication that would permit unattended operation. Moreover, tamper indication is likely difficult, for several reasons:

1) These are not small and compact instruments: the in-pool detector, the tether, and the out-of-pool instrumentation expose a large surface area.
2) Even if all surfaces of an instrument were tamper-indicating, visual verification would be impractical. Much of the instrument is under water and inaccessible, especially if it is installed semi-permanently.
3) Tamper indication that does not involve visual inspection could interfere with instrument operation, or be compromised by radiation (e.g., from both SFA and neutron source, if applicable). Here the concern is with the surfaces of the NDA instrument that are closest to the SFA under test—polyethylene; possibly with cadmium lining.

Assuming that we could at least enclose both the in-pool and out-of-pool parts of an instrument in separate TIEs, one might ask whether and how the instrumentation lines in the tether might be secured. Even the data lines themselves are not amenable to cryptographic methods, since they are generally timing pulses and/or analog (current / voltage) signals. One would have to redesign the instrument so that the tether passed only signed digital data. A secret key system could be employed just to secure such intra-instrument communication between the TIEs. However, that would demand a significant increase in the complexity of the submerged electronics that are subject to radiation exposure.

Even if equipment integrity is assured, a remote user still could not be certain just what is being measured. There is nothing within our measurement system that can assure us exactly what SFA we're measuring, whether or not it's in the right position, whether or not there is anything else close enough to influence the measurement, etc. We will defer these questions to be addressed at a higher-level systems implementation; for now, we focus on just the measurement equipment—just the pieces within the dashed line.

5.2 Environmental Conditions

By "environmental conditions," here we refer to anything apart from our SF NDA instrument itself that could affect the measurement—all externalities. The position of the SFA under test might be one such externality. Boron concentration in the water might be another, as would the presence of another SFA nearby or even a second neutron source.

Because unattended operation would depend on more information than is produced by the SF NDA instrument itself, there needs to be some definition of the larger system implementation that has a means to assess the environmental conditions affecting the measurement. Figure 4 depicts such a hypothetical arrangement:

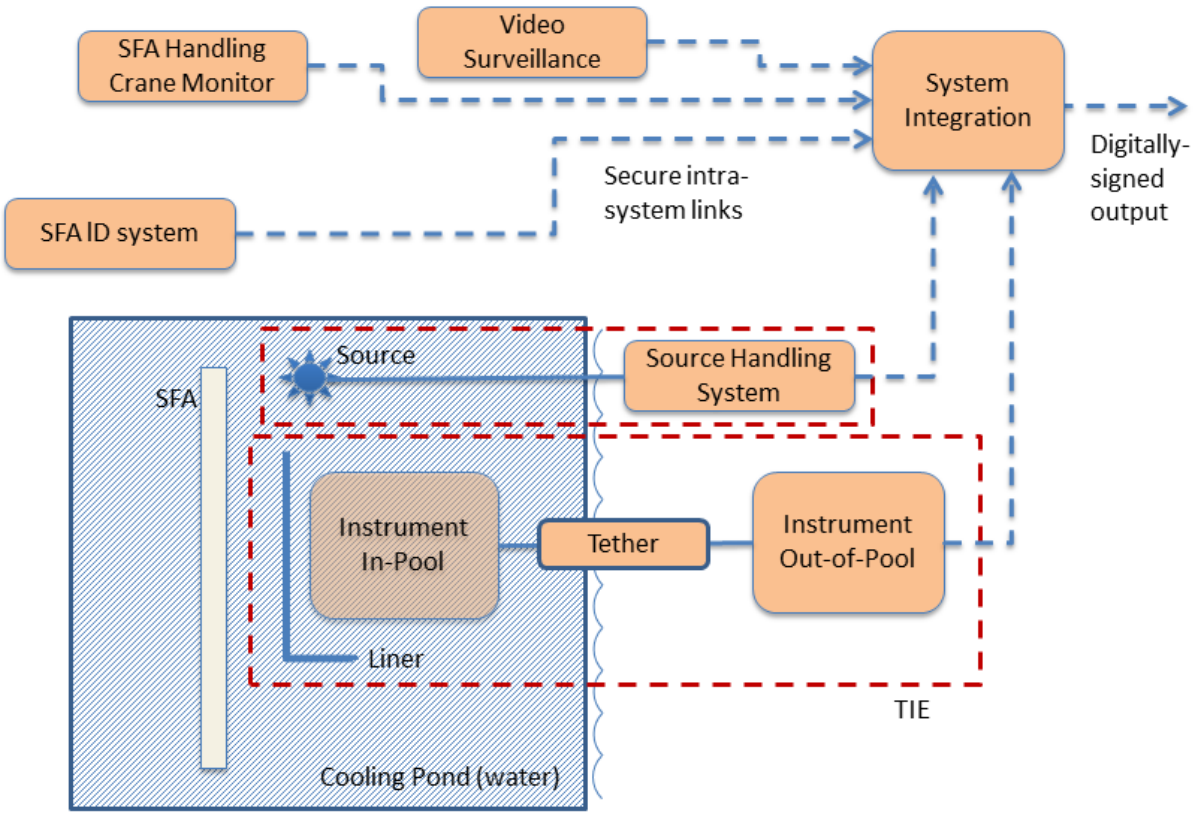

Figure 4 Notional system configuration for unattended or remote NDA measurements

Note that the TIE for equipment integrity actually is required for each separate component of the system, although shown here just for the SF NDA instrument and the neutron source (the neutron source TIE separate from the SF NDA instrument TIE). Communication between such secured nodes (the dashed lines) in all cases presumes digitally-signed and validated information flows. A separate system integration node would be where measurements could be coordinated—by digesting the separate inputs. It is where the system truly "knows" what measurement is being

done on what object. The SF NDA instrument itself is only tasked with the single purpose of obtaining a specific set of instrument count rates.

The system integration is able to do more than just coordinate the measurements; it can also serve to monitor the system state of health. In attended operation, a SF NDA instrument only needs to acquire measurement data after the SFA and source are in place; typically the instrument is idle (i.e., not tallying counts) at other times. For unattended/remote operation, however, the system would best be monitoring the SF NDA instrument output continuously, as noted later in Recommendation 5. The count rates could be tallied for prescribed fixed-duration time windows. An actual "measurement" might then require summing one or more of contiguous time windows to acquire desired measurement statistics. If the system also pays attention to the non-measurement time windows, the data can provide some further assurance of system integrity. The non-measurement data could be retained within the local system for some arbitrary retention period and eventually discarded.

If the detected signal in the interim between measurements is low, it would be advisable to induce an artificial signal deliberately. Supplementing the normal background with a reference source (neutron, gamma, or both) under the automated control of the measurement system would be a means to inject improved statistics and variability into this system state of health monitoring between measurements.

5.3 Neutron Source Considerations

For active measurements, the absolute intensity of the neutron source, the source position with respect to both the instrument and the SFA, and the absence of another nearby source and/or neutron absorbers are all critical experimental considerations. Otherwise the count rate signal with a source present (and thus the inferred multiplication) could be anything one would like. While ensuring that all other experimental conditions are kept constant, procedurally there should be four separate measurements for each assembly:

1. SFA only, no source,
2. SFA with source,
3. source only but no SFA, and
4. no SFA or source.

6. DATA AUTHENTICATION ISSUES FOR JOINT USE

The foregoing discussion assumed a single remote user of the SF NDA instrument. The instrument is a sophisticated, costly investment, so there is likely interest in leveraging its use for the benefit of multiple parties. In general, we can imagine interest from not only the IAEA, but also a regional safeguards inspectorate (e.g., Euratom), a national authority / regulator, and the facility operator.

These separate parties also likely have differing interests on what the SF NDA measurement results would be used for, and how they would be used. They may also have different trust requirements for the measurement data, which in turn may depend on what other parties are involved.

It is hard to imagine that the SF NDA measurement results would be obtained purely for informational purposes, and simply archived for unspecified future reference. Particularly for the SFA encapsulation plant, where the SFA is next destined for packaging in a canister to be emplaced in a geological repository (in IAEA parlance, “difficult to access storage”), the measurement may lead to a decision, i.e., a decision either to proceed with encapsulation or not to proceed. When multiple parties share the measurement information, how does that sharing affect the overall decision? Can any one of the parties prevent a SFA from going forward to encapsulation? Do some parties have a stake in the decision, and others not?

The IAEA will certainly wish to use the instrument measurement for “partial defect verification” of the operator declaration. The operator would not be able to know the instrument measurement results until after making a declaration to the IAEA. For that reason, the operator may use other information (e.g., known characteristics of the SFA together with its operational history in the reactor) as input to the declaration that the state provides to the IAEA. As soon as the IAEA has received that declaration, it could share the measurement data with the operator.

When considering joint and/or shared use scenarios, it is important to clarify not only the sharing of the instrument output, but also the control and configuration of the instrument; the “input,” so to speak. A workable arrangement for multiple parties is most straightforward if only one entity is capable of controlling the instrument. If more than one entity can control the instrument, then it becomes necessary to consider not only data authentication, but also control authentication.

7. DISCUSSION

Ultimately the user of the measurement data from the SF NDA instrument has the responsibility for defining the requirements that pertain to being able to trust the instrument's measurement results. The foregoing sections of the report make an assessment from a purely technical point of view, which may or may not be consistent with what becomes official policy. Different recipients of the measurement data may decide to establish different trust requirements. To the extent that the trust requirements are less stringent than what we suggest in this report, the recipient is accepting residual risk. There is also the possibility that the recipient might insist on even more stringent requirements, due to an awareness of threats that we may not have covered. What is critically important, however, is that any definition of trust requirements be made with a clear understanding of what risks are addressed by the requirements and what risks are not, rather than without such an understanding.

An instrument intended to be used for IAEA safeguards verification would necessarily be subject to a vulnerability assessment (VA) before being approved for routine use in the field. If intended for joint use, the IAEA further requires an additional VA to assess the particular issues associated with sharing the instrument. The VA is a critical procedural assurance to the IAEA that an instrument can be deployed in an untrusted environment and can still provide measurement information able to support an independent safeguards conclusion.

8. RECOMMENDATIONS

Recommendation 1

Develop use cases for these measurements. Who will share the results, when, and how? Who will control the instrument? What are the data retention requirements?

Recommendation 2

There is a critical need to develop readily-verifiable tamper indicating enclosures for submerged NDA instruments to be used in unattended mode: both for the tether and for the detector assembly. Otherwise these instruments will be useful only as attended systems or as operator-only systems.

Recommendation 3

Develop the individual ancillary instruments needed to support a systems implementation. Those instruments would:

1. Identify the SFA item under test
2. Confirm presence of the SFA within active region of the detector
3. Determine the axial position of the SFA in the SF NDA instrument
4. If applicable, determine the detector door position (open/closed)
5. If applicable, ensure that the same radioisotope neutron source, and only one source, is present and positioned correctly
6. If applicable, provide the parameters for, or confirm the output of, the neutron generator
7. Ensure the time synchronization of system components
8. Provide a means to “hand off” a just-assayed SFA to associated containment and surveillance equipment, used to maintain CoK of the SFA

Recommendation 4

Develop the system implementation for automated, unattended measurements, which coordinates the necessary ancillary equipment (per Recommendation 3) and the SF NDA instrument.

Recommendation 5

The SF NDA instrument should be operated continuously (never “off”). Although the main purpose of the instrument is to assay SFAs, it is also capable of some self-monitoring to detect and deter tampering. Some provision to monitor the instrument output to assess and report its state of health is advisable.

9. CONCLUSION

From a “data authentication” perspective, we have reviewed the candidate advanced technologies for nondestructive radiation measurements of SFAs, which are now in the late stages of research and development. In this context, “data authentication” refers to any aspect of the equipment design, installation or operation that affects a recipient’s ability to trust the associated measurement results. Ultimately that concern would be a critical factor in instrument acceptance.

Thus far, all instruments except the FDET have been used exclusively in attended-mode operation. Provided that the user of an instrument maintains custody of it (and the data from it) at all times (e.g., under seal while not being used), there should never be any additional data authentication concern.

However, any envisioned application for unattended operation of the instruments implies a significant leap in technical sophistication compared to an attended instrument. To date, no such development work has been undertaken for these instruments. None of these instruments could be dependably used “as-is” for unattended operation in a safeguards deployment; additional development work would be required.

10. REFERENCES

Abedin-Zadeh, R., Whichello, J., Martelle, G., Hurt, R., Saied, M., Olsen, R., et al. (1998). The IAEA Remote Monitoring Project. *Institute of Nuclear Materials Management 39th Annual Meeting* (pp. 1-6). Naples, FL USA: INMM.

Baldwin, G., & Tolk, K. (2009). Information Surety for Safeguards and Nonproliferation. *31st ESARDA Annual Meeting, Symposium on Safeguards and Nuclear Material Management* (pp. 1-6). Vilnius, Lithuania: ESARDA.

Belian, A., Menlove, H. O., Swinhoe, M. T., & Tobin, S. J. (2012). New Design of the Differential Die-away Self-interrogation Instrument for Spent Fuel Assay. *Journal of Nuclear Materials Management*, 58-60.

Eigenbrodt, J., Tobin, S. J., Charlton, W. S., Bolind, A. M., Menlove, H. O., Seya, M., et al. (2014). Passive Neutron Albedo Reactivity Measurements of Fugen Fuel. *Institute of Nuclear Materials Management 55th Annual Meeting* (pp. 1-10). Atlanta GA: INMM.

Henzl, V., Swinhoe, M. T., Tobin, S. J., & Menlove, H. O. (2012). Measurement of the Multiplication of a Spent Fuel Assembly with the Differential Die-away Method Within the Scope of the Next Generation Safeguards Initiative Spent Fuel Project. *Journal of Nuclear Materials Management*, 61-69.

Hu, J., Henzlova, D., Tobin, S. J., Kim, H.-D., Park, S.-H., Menlove, H. O., et al. (2012). Customized Design and Simulated Performance of the 252Cf Interrogation with Prompt Neutron Detector for Spent Fuel Measurement at the Post Irradiation Examination Facility in the Republic of Korea. *Institute of Nuclear Materials Management 53rd Annual Meeting* (pp. 1-9). Orlando FL: INMM.

Hu, J., Tobin, S. J., Menlove, H. O., Henzlova, D., Gerhart, J., Swinhoe, M. T., et al. (2012). Developing the Californium Interrogation Prompt Neutron Technique to Measure Fissile Content and to Detect Diversion in Spent Nuclear Fuel Assemblies. *Journal of Nuclear Materials Management*, 49-57.

IAEA. (1998). *Safeguards Policy Series No. 16, Remote Monitoring for Safeguarding Nuclear Facilities.* Vienna, Austria: IAEA.

International Atomic Energy Agency. (2005, 01 12). *INFCIRC/193/Add.8.* Retrieved 08 05, 2014, from IAEA Publications: Information Circulars: http://www.iaea.org/Publications/Documents/Infcircs/2005/infcirc193a8.pdf

International Atomic Energy Agency. (2006). *SMR 2.20 Policy Paper 20: Joint Use of Safeguards Equipment between the IAEA and an External Party; Entry Into Force: 2006-04-26.*

International Atomic Energy Agency. (n.d.). *InfCirc 193.*

LaFleur, A. M., Menlove, H. O., Tobin, S. J., & Swinhoe, M. T. (2010). *Development of Self-Interrogation Neutron Resonance Densitometry to Measure the Fissile Content in PWR 17×17 Spent LEU Fuel.* Los Alamos NM: Los Alamos National Laboratory.

Menlove, H. O., Menlove, S. H., & Tobin, S. J. (2009). Fissile and fertile nuclear material measurements using a new differential die-away self-interrogation technique. *Nuclear Instruments and Methods in Physics Research A*, 588–593.

Tobin, S. J., & Jansson, P. (2013). *Nondestructive assay options for spent fuel encapsulation.* SKB.

Vaccaro, S., Hu, J., Svedkauskaite, J., Smejkal, A., Schwalbach, P., De Baere, P., et al. (2013). New approach to Fork measurements data analysis by RADAR-CRISP and ORIGEN integration. *3rd International Conference on Advancements in Nuclear Instrumentation Measurement Methods and their Applications (ANIMMA)* (p. 8). Marseilles, France: IEEE.

APPENDIX: DATA AUTHENTICATION

"Data authentication" is used in international nuclear safeguards principally to support unattended and remote monitoring instrumentation. It consists of two critical steps: signing the data at its origin, and validating the data signature by the recipient. If employed correctly, data authentication enables the recipient of the data to be able to trust (1) where the data originated (authenticity), and (2) that it has not changed since it was signed (integrity). A change could either be accidental (e.g., corrupted due to transmission errors) or intentional (e.g, malicious attempt to deceive). It is not always possible to tell the difference. Data authentication is most commonly accomplished by applying cryptographic techniques to digital data.

Note that data authentication is not the same as encryption. Encryption is a means to hide the data from eavesdroppers, which is a means to ensure confidentiality. Encryption also employs cryptographic techniques, but it serves an entirely different purpose.

Data signing

A data stream is signed near the source of the data using a secret key. The basic process is illustrated in Figure 5.

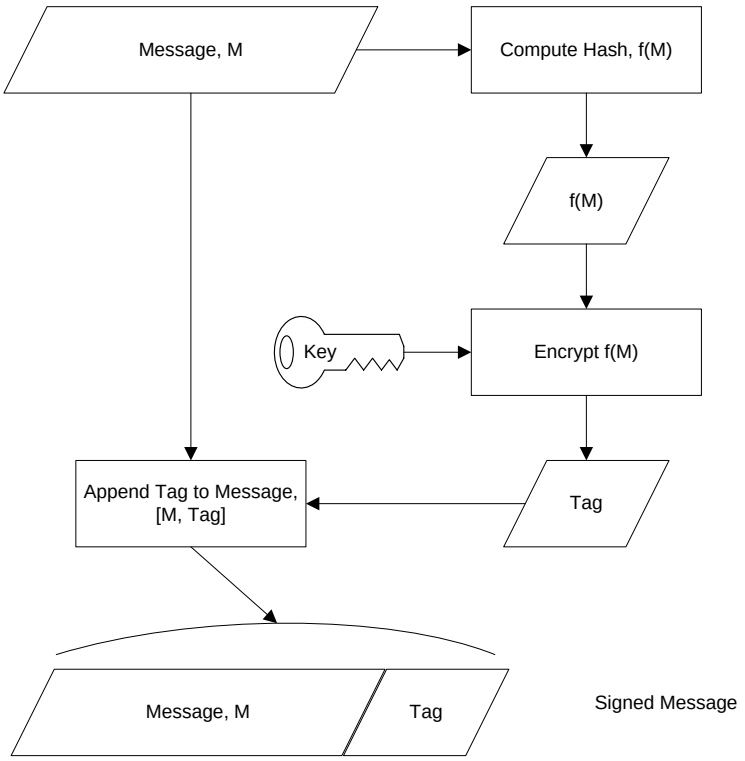

Figure 5 Signing a data message

The key is necessary to ensure that no other entity could impersonate the source of the data. If others were to know or obtain the signing key, then we would no longer be able to trust the signed data. Someone else could have signed fraudulent data.

Note that the message itself appears in the clear; data are not hidden by the signing process.

It is important that the data message always include a time varying parameter, so that no two transmissions could ever be the same. Otherwise, messages would be vulnerable to a replay attack, where a third party simply records signed (and thus trusted) messages, then plays them again at a later time (e.g., substituting them for actual messages).

Data validation

As shown in Figure 6, the signed message can be validated on the receiving end, again with a key.

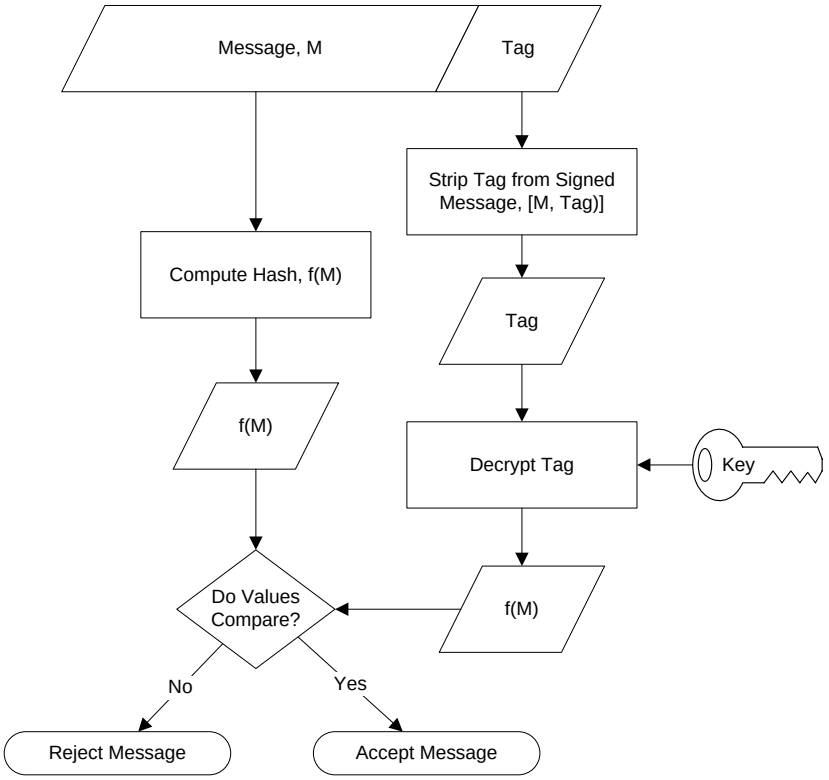

Figure 6 Validating a signed data message

Secret Key vs Public Key Systems

In secret key systems, the key used to validate a signed message is identical to the key used to sign the message. That key must be kept secret, otherwise the recipient could not trust who may have signed the message. Secret key cryptography is efficient and does not require significant computational power, but is only appropriate when only one recipient party requires authenticated data.

In public key systems, the key used to validate the signed message is different from the key used to sign the message. (The computational algorithms for signing and validation are different as well.) In that way it is possible to have multiple recipients, all able to validate the same signed data. None of the recipients is able to sign data, however, so all can trust the one source. The

signing and validation keys together constitute a key pair. Ideally the key pair can be generated internally within the sending instrument.

DISTRIBUTION

5 National Nuclear Security Administration
Attn: A. Dougan, K. Durbin, C. Orton, K. Veal, E. Wonder

9 Los Alamos National Laboratory
Attn: A. Belian, J. Eigenbrodt, A. Favalli, D. Henzlova, A. Kaplan, A. LaFleur, S. Tobin, H. Trellue, D. Vo

2 Lawrence Livermore National Laboratory
Attn: Y. Ham, V. Mozin

5 Oak Ridge National Laboratory
Attn: I. Gauld, B. Grogan, J. Hu, G. Ilas, A. Worrall

1 Svensk Kärnbränslehantering AB (Swedish Nuclear Fuel and Waste Management Company)
Attn: H. Liljenfeldt

1	MS 0747	B. Cipiti	6225
1	MS 1375	R. Wilson	6800
1	MS 1373	M. Sternat	6821
1	MS 1371	P. Garcia	6830
1	MS 1374	M. Coram	6831
1	MS 1371	G. Baldwin	6832
1	MS 1371	D. Blair	6832
1	MS 1371	R. Haddal	6832
1	MS 1371	H. Smartt	6832
1	MS 1371	M. Thomas	6832

1	MS0899	Technical Library	9536 (electronic copy)


Sandia National Laboratories