SANDIA REPORT
SAND2016-2172
Unlimited Release
Printed March 2016

Final Report for FY15 Spent Fuel Project Task 12: Data Authentication

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

SAND2016-2172
Unlimited Release
Printed March 2016

Final Report for FY15
Spent Fuel Project
Task 12: Data Authentication

George T. Baldwin
Global Technology Engagement, Research & Analysis
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1371

Abstract

The data authentication task is concerned with the ability of a user to trust the output from an unattended measurement of spent nuclear fuel intended for disposal. Five high-level requirements that are driven from a data authentication perspective need to be considered for instrument development: The instrument must be secured. All data emerging from the instrument must be signed. Instrument inputs may also need to be signed and authenticated. The instrument environment needs to be controlled. A vulnerability assessment will be necessary for the full system before deployment. Additional requirements may be necessary, especially if operational scenarios include arrangements for joint use.

None of the prototype instruments currently under development yet satisfies any of these requirements. From a data authentication perspective, the selection of a preferred instrument from among the candidates under development should consider the relative ability to secure the instrument, its relative needs for ancillary instrumentation, and ability of the instrument to self-interrogate its state of health.

Further work is recommended to develop advanced technologies, methods and approaches for tamper indication. Beyond the development of any particular instrument for the nondestructive assay of spent fuel, efforts should be devoted to developing the system for spent fuel verification prior to long term disposal, including likely operational scenarios for routine use of the verification system.

ACKNOWLEDGMENTS

Support to Sandia National Laboratories provided by the NNSA Office of Nuclear Safeguards and Security, Next Generation Safeguards Initiative is gratefully acknowledged. Discussions with Anders and Jan-Olov Stål of the Swedish Nuclear Fuel and Waste Management Co (SKB), Peter Jansson of Uppsala University, and Camilla Andersson and Lars Hildingsson of the Swedish Radiation Safety Authority (SSM) gave helpful guidance regarding the Swedish spent fuel disposal plans. Steve Tobin and Matt Sternat participated also in the visit to Sweden. Sincere thanks to Mike Coram for contributions to the cryptography discussion, and to Matt Sternat for the review of this report.

CONTENTS

INTRODUCTION

We reported the initial work on the "data authentication" problem for the spent fuel project in late 2014.[1] There we defined the "data authentication" problem as follows:

> *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?*

Work in 2015 has extended the previous study by seeking to further clarify the envisioned application for the nondestructive assay instrument. In particular, we have taken an in-depth look at the spent fuel disposal case for Sweden, and posed questions concerning the intended use of a final assay measurement for spent fuel to both the operator (Swedish Nuclear Fuel and Waste Management Co, SKB) and regulator (Swedish Radiation Safety Authority, SSM).

However, a consensus operational scenario ("use case"), which is a critical prerequisite for data authentication, has yet to be defined. There is still no well understood safeguards approach able to inform facility design or operational procedures for spent fuel encapsulation and disposal. Nevertheless, the data authentication task can satisfy at least two important needs of the project immediately:

(1) Define additional high-level requirements for instrument development that will enable data authentication.

(2) Identify criteria that would assist in selecting leading candidate(s) from among the various instrument options.

The primary focus of the instrument developers is clearly on the science involved in the measurement, which ensures that the instrument is able to obtain desired safeguards-relevant information. Other considerations, such as safety, reliability, ease of use and others, including data authentication, are also important for the instrument to be a viable safeguards tool.

This report addresses both of the project needs cited above, i.e., defines high-level requirements for data authentication, and identifies criteria to compare candidate instruments from a trust perspective, both assuming unattended operation.

SYSTEM OPERATION CONSIDERATIONS

Presently, prototype instruments are being used in field tests. They have not been secured, but instead are used in attended mode. In any event, they are being used in a research context, which is not at all the same as the safeguards context. Data are shared with analysts, who use the data in various ways together with sophisticated modeling simulations to characterize selected fuel assemblies. This is not at all how the instrument would be used for safeguards.

Thus far, it is still not clear how an instrument would be employed in a production environment; in particular, as a final measurement station before the encapsulation and disposal of spent fuel assemblies. In this report, we assume that the instrument would be employed with the sole purpose for safeguards verification by the International Atomic Energy Agency (IAEA) and/or Euratom. Other use cases are possible and they would have a critical bearing on the data authentication aspects. We further assume the instrument is in unattended operation, i.e., with no safeguards inspector present.

For safeguards, measurement results are used as a decision support system: Either the inspectorate accepts that a spent fuel assembly is as declared, or it does not accept the spent fuel assembly is as declared. This boils down to “yes, the spent fuel assembly can proceed to disposal,” or “no, we have questions that first need to be resolved.” Nothing has thus far been said about how that decision is communicated to the operator, how much time is available to make that decision, or even whether or not human intervention is needed for the decision. Each spent fuel assembly cannot be a separate research project. There must be a process in place whereby the measurement is made and a decision reported back to the facility operator. For all we know, a decision could be either generated promptly by logic within the instrument itself, rendered by a green or red light; or made entirely apart from the instrument, days after the data had been communicated to Vienna and/or Luxembourg. The operator may be willing to risk proceeding toward disposal before receiving a “green light,” but the greater the delay, the greater the cost of having to “pull” an assembly from the process. More likely, the process must hold until a decision is rendered.

HIGH LEVEL REQUIREMENTS

The following sections cover the essential factors involved in spent fuel nondestructive assay measurements from a "data authentication" perspective. In other words, we describe what is necessary for a safeguards inspectorate to trust the measurement data. The usefulness of those measurement data is an entirely separate question, as are other considerations, such as data confidentiality. Here we concern ourselves only with the assurance that the data are truthful.

Assumptions

1. There is only one "user" of the data. If multiple entities communicate with the instrument, the situation is much more complicated and is beyond the scope of this report.
2. The instrument is operated in an environment that is neither controlled by nor trusted by the user of the instrument data.
3. The instrument is operated in unattended mode. It does not matter whether data are transmitted remotely, or only retrieved intermittently by onsite access.
4. The data actually matter to an international nuclear safeguards conclusion, i.e., altered data in principle might be able to conceal a diversion of nuclear material.

1. The instrument must be secured

By "secured," we mean that it should not be possible to do anything at all to an operational instrument without detection. We may not be able to *prevent* either malicious tampering or inadvertent/ accidental interference (e.g., power disruptions), but we should always *know* when such events happen. Data authentication would be meaningless unless the system has a secure endpoint where the data originate.

Tamper indicating enclosure (TIE)

For an instrument to be properly secured, the volume of space it occupies needs to be fully enclosed within a well-defined, continuous surface perimeter. That surface perimeter must further be capable of revealing any breach in its integrity. Nothing should be able to cross that surface without detection. Such detection is called *tamper indication*, and that enclosing surface is referred to as a *tamper-indicating enclosure* (TIE). The typical TIE is *passive*, meaning that any breach in the surface would be hard to repair and relatively easy to spot visually. However, passive tamper indication assumes that the TIE actually will be inspected periodically. The TIE should also not be obstructed, such as being covered with adhesive labels. All surfaces should be readily visible, or else made to be visible, even a surface in contact with a floor, for example. *Active* detection may also be employed, such as adding a micro switch to a removable cover, which can then trigger an automatic and prompt response, if desired. However, most active detection for tamper indication is only partially effective; it does not cover all tamper scenarios, many of which involve bypassing switches. Active detection usually relies on electrical power with battery backup.

Verification

In almost all cases tamper indication relies on periodic physical access to the instrument for visual inspection of the TIE. The integrity of that perimeter can be verified, preferably *readily*

verified. If the verification reveals no evidence of a possible breach of the instrument containment, then measurement data produced by the instrument prior to the TIE verification can be trusted. If the verification results in any evidence of a possible breach of the containment, then no data released by the instrument since the last positive verification can be trusted, *even if cryptographic authentication of the data had been successful*. In the latter case, one must assume that the private signing key (explained later) had been compromised.

Connections

Any connection between the instrument and the outside world affords an opportunity to bypass the TIE, and thus becomes a potential instrument vulnerability for malicious tampering. The number of connections should therefore be minimized whenever possible. Each connection should be identified and assessed: is there any way that it could be manipulated from outside to affect instrument operation or configuration? If so, modifications to the instrument design may be able to compensate for such vulnerabilities, possibly by monitoring the connection and incorporating automated response logic.

Inevitably mains power will be a connection required by the instrument. For operational reasons, the instrument will need to be resilient to power disruptions. But if that is accomplished with an uninterruptible power supply located *outside* the instrument TIE, one would still need to consider whether or not a deliberate power disruption could be used to manipulate instrument operation.

Any instrument data likely need accurate timestamps. A real time clock may operate within the instrument TIE, but it could also (or alternatively) involve a connection to time information relayed to or from the outside. Any external communication of clock time would require signing and authentication.

State of health

State-of-health messages are one kind of data that are important indication to the user confirming that the instrument remains able to perform measurements. If the instrument is able to monitor tamper status, then any indication of tamper should immediately cause state-of-health status to fail.

Within the instrument

If an instrument has been properly secured, there is no need for authentication of data entirely confined within the instrument. The space within the tamper indicating enclosure is assumed to be a trusted space.

While a tamper indicating enclosure secures the instrument from external influences, it does nothing in the way of monitoring what is going on within the instrument itself. Nevertheless, it is essential that the instrument contains no Trojans or back doors, anything able to manipulate measurement operation or configuration, data, or the signing key. Such malware could have entered the instrument at any stage; whether during instrument design and development, manufacture, delivery, or at any time prior to initial operation. It does not necessarily have to rely on being controlled from the outside, but may be able to operate automatically based on internally available information. (The “hidden switch” able to change operational modes of an automobile engine was a well-publicized accusation of Volkswagen in manipulating the results

of emissions testing, for example.) Proper control of the supply chain through the instrument life-cycle is important; the user will also rely on a vulnerability assessment as an important confirmatory step.

Vulnerability assessment (VA)

Instrument designers and developers need to take tamper indication into consideration, and can incorporate features that help to secure the instrument. However, their primary focus must be on instrument function and performance, as well as many other considerations (e.g., safety).

Ultimately the user of the instrument (a safeguards inspectorate) will require a completely independent "red team" vulnerability assessment (VA) by a third party, which is tasked to evaluate the instrument entirely from the perspective of a sophisticated adversary who is intent on defeating the instrument without detection. The assumption is made that the adversary is a state-level threat, with extensive resources, unfettered access to the instrument, and full knowledge of its design and operation. The results of such an evaluation are usually very sensitive, treated in confidence by the VA team and the user, and may not even be shared with the instrument developer. The user can either request changes to the instrument that improve its security, make procedural accommodations to compensate for weaknesses, or else accept the risk that a tamper event might be successful (i.e., not detected).

What about surveillance?

Reliance on the TIE for the security of the instrument utilizes a "containment" approach to maintain confidence that data from the instrument can be trusted. One might be inclined to consider instead a "surveillance" approach, whereby the instrument is continuously watched by cameras. In this case, surveillance video would provide the assurance that no tampering has taken place. Although conceivable in principle, it is not necessarily a practical approach, for several reasons.

All conceivable means to tamper with the instrument would need to be discernible from the video record. One usually cannot monitor all attackable surfaces of the instrument, even with multiple cameras. The cameras would need to be configured specifically for the purpose of tamper detection, rather than for other reasons, for which tamper detection is only an incidental, supplementary activity. Surveillance detection relies on transient evidence, whereas indication of a containment breach usually persists long after the attack has occurred. Cameras themselves are instruments subject to compromise, and also to interference, such as a temporarily blocked field of view or failure of facility lighting. Review of surveillance records to detect instrument tampering could indeed be a tedious undertaking, and its findings are likely to be ambiguous at best. We are not aware of *any* unattended safeguards instrument that the IAEA approved for use in an unattended operation that relied on surveillance methods to assure instrument security.

2. All data emerging from the instrument must be signed

Before leaving the secured instrument, data must be signed by digital cryptographic means that are acceptable to the user of the data. By "signing," we mean appending to the data a string of bytes that constitute a signature. The signature results from combining the data with a "key" using a cryptographic algorithm. The algorithm is openly shared, but the cryptographic key used by the algorithm is a secret. Data are unchanged by signing. Unless they are separately

encrypted, data bytes are still "in the clear" and thus readable. Yet should even a single bit in either the original data or its signature change (e.g., a zero becomes a one, or vice versa), for any reason, the data would fail authentication.

If the user of the data (the one who needs to trust its authenticity) has direct physical access to the instrument for retrieving the data, then in theory, the data would not need to be signed (or authenticated) at all. Instead, *only the user would need to be authenticated by the instrument*, and then that user could be granted unfettered access to data within the secured instrument. In that case, the user could trust unsigned data due to the security of the instrument itself. However, there would then be no mechanism for later validating the authenticity of any data that the user had taken away from the instrument. For this reason, we rule out making any exception that would permit unsigned data to leave the instrument.

Key management

The security of the key used to sign the data is critical to data authentication. If it could be copied, then that copy enables someone to sign any bogus data and have those data accepted as authentic. The best approach is to employ asymmetric key authentication, where only a single copy of the signing key exists, kept secret within the instrument.[1] A "public key" corresponding to that signing key (together called a key pair) is used to cryptographically authenticate (verify) the data signature. Any number of copies of the public key can exist; it can be shared freely. There is no need to keep the public key a secret, because it cannot be used to sign the data, nor can it be reverse-engineered to reveal the signing key. Such asymmetry ensures that data cannot be signed by any entity other than the instrument, which alone possesses the secret signing key.

It is possible (and advisable) to generate the key pair automatically within the instrument itself, so that the secret key is never revealed outside of the instrument (even to the user of the data). Of course, the user must be assured of possessing the true public key for the instrument, and not a fraudulent impersonation of the public key. The user must receive the instrument public key through a trusted channel, such as with direct physical access to the instrument when the instrument is initialized.[2]

If active tamper indication is employed (see previous section, Requirement 1, "The instrument must be secured"), then the instrument can take defensive action against those tamper events it is able to detect. A common practice is to store the private signing key in volatile memory, and then erase the key immediately if a tamper is detected.

---

[1] We will not consider symmetric key authentication (also called "secret key" authentication), because it entails greater demands on secure key management. In symmetric key authentication, the same key is used to sign and authenticate messages, which makes it possible for anyone in possession of the key to sign (and thus also to impersonate) messages.

[2] Another way for the user to have confidence in the instrument public key is by utilizing a signing authority. The signing authority needs to have a trusted channel to receive the instrument's public key and sign it. Then data authentication by the user involves two steps: validating the instrument's public key (the user has the signing authority's public key), and only then accepting that instrument public key to authenticate the data. See Coram, et al [2].

Type of data

The type of data that can be authenticated is limited to that which can be represented as a digital message. Analog data must first be converted to digital. Timing data, such as logic pulses that convey information according to the precise instant they appear, cannot be authenticated without first being converted into a time-invariant message. ("List mode" data from a nondestructive assay instrument could be signed and authenticated, for example.) Digital data may be produced as a defined data set, having a clear beginning and an end, with either a fixed or a variable number of bytes. In other cases, data could be generated in a continuous or irregular stream. However produced, the data typically are first aggregated into "blocks" of arbitrary length. Each data block is then signed. Authentication reverses the process, first comparing each data block with its associated signature, and then reassembling the original data stream. How to block the data is an important consideration in achieving optimum efficiency for signing and authentication. Available computational power to block and sign instrument data streams is generally fast enough to keep up with most output rates except those of very high bandwidth instruments; nevertheless, it is preferable to minimize the amount of data needing to be sent outside of the instrument.

Data content

It is important that each data block differs from the others, specifically, that it includes some uniquely advancing indicator within the data stream, such as a message counter or the time stamp from an internal real time clock. Otherwise, signed data could be recorded and later played back (e.g., substituting for actual messages). Because data had been signed correctly from a purely cryptographic standpoint, such a replay attack might succeed unless we guarantee that the data content can never repeat.

After signing

Once signed, the data can either be pushed out of the secured instrument immediately, pushed out after some arbitrary time delay, or else stored within the instrument until retrieved by the user, e.g., by polling. Whether data are retrieved by the user during an onsite inspection, or conveyed via remote data transmission, is immaterial to data authentication.

Data backup

The retention period (and capacity) for data within the instrument is an entirely separate question, likely dictated by considerations other than data authentication. For example, there may be a need to retain a copy of data pushed out of the instrument, in case there is any risk of the data being lost and needing to retrieve it again. As long as data stay within the instrument, they can exist with or without signature. It is only critical that data are signed before leaving the secure perimeter of the instrument.

Data authentication is only one element of data security

Other considerations may play a role in dictating additional data security requirements. Data authentication *only* addresses the need for the user of the data to be able to trust its integrity and its origin; to believe that the data are *true*. There may also be other requirements. For example, in some safeguards applications the inspectorate may not want to share the operational status of the instrument with the facility operator. Often a facility operator may impose requirements on the

inspectorate, such as maintaining confidentiality of the data. Such conditions impose other requirements, affecting when the data are transmitted and how they are transmitted.

3. Instrument inputs may also need to be signed and authenticated

The instrument for spent fuel verification does not operate in isolation; instead, it must interact with the outside world, including the operator system for the handling of spent fuel assemblies. There are likely ancillary devices associated with the measurement being made by the instrument. Data from instrument may only be meaningful when combined with other information that the instrument itself is not capable of providing or confirming (e.g. the identification of the fuel assembly being measured). It is not merely results coming *out* of the instrument that must consider the need for data authentication.

External inputs to the instrument, to the extent they can affect the data the instrument generates, may need to be authenticated. If so, the external sending device would sign its message; the instrument would then verify the authenticity of the received message before accepting it as input. Examples could include any triggers to start or stop a measurement, instrument configuration settings, control signals, state of health signals from other instruments, or polling requests from the user to release data.

4. The instrument environment needs to be controlled

Digitally signed data can be determined to have come from the instrument without change ("authentication"). But do those data reflect the assumed measurement conditions? Authentication of the instrument data alone cannot provide that assurance. For operation in unattended mode, any measurement assumptions should be independently verified, so that there is little possibility for correct data to convey the wrong message.

The first step is to list all assumptions that could affect the measurement results. The risk is that we take some environmental conditions for granted. For example, these measurements are conducted under water. But what is in the water? Would it make a difference? What else might be nearby, besides a fuel assembly and the instrument?

In *attended* mode, one does not typically worry about all of the environmental conditions explicitly. For example, if measurements were to be carried out at the mid-plane of the spent fuel assembly, one would probably notice if the assembly had only been partially inserted in the device. But when unattended, how does one know? Do we trust an operator signal? Or is there an independent means of confirming the assembly position? Is that confirmation relayed to the instrument with a secure (signed) message?

All of the ancillary equipment that would be necessary to support an unattended measurement should be understood in a system context. It is important to determine how the user will be able to make an unambiguous connection between authenticated instrument data and the actual measurement conditions. Furthermore, once the measurement data have been collected, it is likely necessary to maintain the association of those data with a particular spent fuel assembly in the encapsulation process. Thus far, that "handoff" of a spent fuel assembly from the instrument to whatever system will maintain continuity of knowledge has yet to be determined.

5. A vulnerability assessment will be necessary for the full system

A vulnerability assessment on the instrument itself, as described under requirement (1), merely evaluates the security of the instrument in isolation, a necessary but not sufficient condition. As should be clear from the previous discussion about the instrument environment, there are many more factors that could affect the ability of the user to trust an unattended measurement. A more comprehensive *system* VA would take all factors into consideration. Ultimately it is not just the security of the individual components involved in the measurement, but also how they interoperate that will enable the user to trust the overall measurement. Data authentication is a critical aspect, not only for the output results, but also the interoperation of system components.

CRITERIA FOR DOWN-SELECTION

Are any of the instruments under development more promising than others from a data authentication perspective? We assert three aspects are important to consider in making such a judgment.

1. Relative ability to secure the instrument

A more easily secured instrument is preferable to one that is more difficult to secure. Most of the instruments being considered all suffer from the same challenges in securing cabling tethers and underwater detector heads. Some differences might be differentiating, however, such as the possibility of incorporating the neutron source within the instrument itself (as in Differential Die Away), rather than requiring a separate tamper indicating enclosure.

2. Relative needs for ancillary instrumentation

An instrument less dependent on external inputs would be preferable. For example, an instrument employing a neutron source located outside of its tamper indicating enclosure requires separate tamper indication for the source, as well as verification of the source positioning, control of the intervening materials between the source and the spent fuel assembly it irradiates, etc. The instrument likely would need to know about the source position before acquiring measurement data, and therefore might need to rely on an external authenticated trigger signal. As another example, if the spent fuel assembly positioning is constrained, such as being confined by detector walls on all four sides, then there is less opportunity for results being affected than if the spacing between the fuel assembly and instrument are not so confined (as with the FORK design). The former case may be a simple matter of assuring that an assembly is either inside the instrument or not. And in that case, an instrument with four fixed walls would be easier than one with a door, for which one also needs to know that the door is closed.

3. Ability to self-interrogate

An instrument that affords a state of health challenge-response capability would be less susceptible to deliberate manipulation. Having a means to artificially generate a measurable signal in the instrument (such as by introducing or removing a neutron source), if and when desired, would be a distinct advantage. This could be commanded by a(n authenticated) control signal from the user, or else a capability built into the system to operate autonomously.

CONCLUSIONS

While this report may appear to cover much more than data authentication, per se, it is important to realize that all of the discussion pertains directly to the ability of a user to trust the measurement. Without considering the broader context, authenticated data would only create a deceptive illusion of being able to trust the measurement.

Development requirements

Instrument development needs to include the following high-level requirements that are driven from a data authentication perspective:

1. The instrument must be secured
2. All data emerging from the instrument must be signed
3. Instrument inputs may also need to be signed and authenticated
4. The instrument environment needs to be controlled
5. A vulnerability assessment will be necessary for the full system

None of the prototype instruments currently under development yet satisfies any of the forgoing requirements. Further details within these broad requirements are not repeated here, but have been discussed in the main report. (For example, a supporting requirement for (2) would be the need to include a time-dependent indicator in any data block to be signed.) Additional requirements may emerge as the operational scenario for the instrument is defined, especially if it involves arrangements for joint use.

Instrument selection criteria

Selection of a preferred instrument from among the candidates under development should consider the following criteria, from a data authentication perspective:

1. Relative ability to secure the instrument
2. Relative needs for ancillary instrumentation
3. Ability to self-interrogate

Of course, these considerations must be weighed against those reflecting other aspects of instrument suitability, reliability, performance and possibly other factors.

RECOMMENDATIONS

The data authentication task forces the consideration of other factors that will be critical for a successful implementation of spent fuel verification, beyond the scope of the scientific development of the nondestructive assay instrument. Specifically, there are supporting activities that can, and should, be undertaken now.

1. Develop advanced technologies, methods and approaches for tamper indication

All of the instruments being considered have extended structures, with an underwater detection component, electronics out of pool, and a cabling tether between them. This is not an easily-secured architecture. It cannot rely on existing solutions for tamper indication such as powder-blue paint and anodized aluminum surfaces. Yet the state of the art in technologies that could be applied for tamper indication has advanced considerably. For example, the advent of additive manufacturing methods involving multilayered materials enables entirely new approaches to tamper indication, which have yet to be exploited for safeguards. The potential exists to create active surfaces, ones that can be sensed by the secure instrument itself. Such prompt detection of a containment breach enables defensive actions to be taken. It would offer a quantum leap in capability over tamper indicating enclosures that must be inspected visually.

2. Develop the spent fuel verification *system*, not just the nondestructive assay instrument

Although cryptographic signing and authentication is a necessary measure for the unattended operation of a spent fuel verification instrument, it is by no means sufficient for an inspectorate to be able to trust the measurement results. The context for the signed data is all-important. If the context can be manipulated without detection, then the signed data might be bit-for-bit correct (the assurance provided by data authentication), but at the same time utterly untrue. For example, if an assumed external californium source happened to be substituted with a source of different intensity, the data would be correct, yet the results entirely misleading. As another example, if the measurement involved scanning the axial length of the assembly, the results likely depend on assumptions made about the scan rate.

Even for the instrument itself, it is not yet clear *what* data actually need to leave the instrument (and thus requiring signing and authentication). It is not yet certain whether neutron measurements will be acquired in list mode, or by using shift register electronics. Active measurements will likely entail separate back-to-back measurements of a spent fuel assembly, with and without a neutron source. Does the instrument process all related data acquisitions internally and only push results out (as “data”), or are the raw data from each acquisition needed? Note that the answer may differ depending on the user’s perspective. An instrument developer may be interested in extensively detailed data for diagnostic reasons; a safeguards inspector may have no need for anything but high-level results.

3. Define the *operational scenario* for routine use of the spent fuel verification system

The previous recommendation focuses on understanding the overall measurement system, including the various ancillary components that are necessary to produce a complete picture of the unattended measurement. An even larger context is important, however. We still do not know how the system would be employed for the final disposal of spent fuel. Various entities are interested; all are potential "users" of the data from the measurement. Yet exactly who participates, and how, is all-important to data authentication.

REFERENCES

[1] George Baldwin, “Spent Fuel NDA Project: Data Authentication Considerations,” Sandia National Laboratories, SAND2014-19460, November 2014.

[2] Michael Coram, Ross Hymel, Michael McDaniel, and Jay Brotz, “Key Management Strategies for Safeguards Authentication and Encryption,” IAEA Symposium on International Safeguards, IAEA-CN-220, 20-24 October 2014.

DISTRIBUTION

6 National Nuclear Security Administration
Attn: A. Belian, A. Dougan, K. Durbin, A. Iyengar, M. Larson, K. Veal

7 Los Alamos National Laboratory
Attn: A. Favalli, D. Henzlova, A. Trahan, A. LaFleur, S. Tobin, H. Trellue, D. Vo

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

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

2 Svensk Kärnbränslehantering AB (Swedish Nuclear Fuel and Waste Management Co)
Attn: A. Sjöland, J-O. Stål

2 Strål säkerhets myndigheten (Swedish Radiation Safety Authority)
Attn: C. Andersson, L. Hildingsson

1 Uppsala Universitet
Peter Jansson

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

1	MS0899	Technical Library	9536 (electronic copy)


Sandia National Laboratories