SAND2016-12207R

SAND2016-XXXX
Unlimited Release
November, 2016

An Overview of Chain of Custody Options for LETTERPRESS

Heidi Smartt and Peter Marleau

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

Sandia National Laboratories is a multi-mission 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.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

1 INTRODUCTION

This purpose of this document is to provide an overview of Chain of Custody (CoC) technology options that could be made available for the LETTERPRESS exercise as part of the Quad Working Group. The Quad Working Group comprises five sub-working groups (Management, Protocol, Simulation, Technology, and Training) with members from the U.S., U.K., Norway, and Sweden having the goal of providing a repeatable, realistic arms control exercise (dubbed LETTERPRESS) to be executed in representative facilities and using non-proliferative but representative treaty items. The Technology Working Group is responsible for supporting the technology requirements of the LETTERPRESS exercise and as such the technologies presented here are possible options to meet those requirements.

2 OVERVIEW

A **seal** is a tamper-indicating device that prevents *undetected* access to an enclosure or other monitored item, typically via recognized openings. The terms seal and tamper-indicating device are synonymous. A **unique identifier (UID)** is an applied identifier or intrinsic feature that is used to facilitate inventory taking, provide security, and protect against counterfeiting. Seals often include UIDs, but UIDs may not be seals.

A loop seal consists of a loop of wire or fiber that is threaded through the item to be secured and a seal body that secures the ends of the wire or cable. Loop seals can be passive or active. Passive loop seals do not require an energy source while the seal is attached; however, they may require a reader for verification. As compared with active loop seals, passive loop seals:

- Are generally less expensive
- Are more environmentally robust
- Could have a longer life
- Often have an increased application space

Verification, however, must be performed manually by a trained inspector, either visually or via custom equipment.

Active loop seals monitor whether the seal is open or closed and, when used with a fiber optic loop, can monitor the integrity of the seal loop. This state-of-health information may be transmitted to a separate monitoring station, or events can be recorded and downloaded by an inspector at the time of seal access. They therefore provide a continuous active monitoring capability. However, these seals require an energy source, usually battery power, and such active monitoring necessarily reduces battery life (note: there is research into energy harvesting techniques that may greatly reduce battery concerns). The timing and frequency of the monitoring should be optimized for the application to allow maximum battery life, which is generally considered 2-4 years for active loop seals. Active loop seals have other advanced capabilities specific to each device. While active loop seals provide greater continuity in monitoring over time, they are often more expensive than passive loop seals, the batteries must be monitored and manually changed, and some applications may not permit the use of active devices or batteries. In some applications, however, the higher purchase cost of the active seal may be offset by the cost of replacing several passive seals.

Adhesive seals, which are sometimes called tape seals or tamper tapes, can be applied across the seam of an enclosure or item to verify that it has not been opened or, if unique features are included, applied to a surface to uniquely identify an item. These seals can also be applied on a surface or over a fastener to provide an indication that tampering was attempted. Adhesive seals are relatively inexpensive and are generally easy to apply and verify, typically requiring limited additional equipment for their use. In comparison to loop seals these seals may require surface preparation and additional time for application, depending on the specific adhesive type and the material to which it is applied, to allow for curing of the adhesive. While easy to use, they are in general not very durable. Adhesive seals work best when applied to clean, smooth surfaces that do not have features that could reduce adhesion. They are generally considered less secure in comparison with loop seals, though they can make an important contribution to overall security when used in conjunction with other seals.

While seals are well-suited to be applied over hasps or other enclosure openings, they are not able to provide evidence of an adversary by-passing that opening completely, for example by drilling through the side of an enclosure. Tamper-indicating enclosures (TIEs), on the other hand, are intended to detect precisely those scenarios. TIEs may be constructed of different materials, from transparent plastics and glass, to metal enclosures, each with strengths and weaknesses. All TIEs can be opened or penetrated, but the essential element of a TIE is that an adversary cannot repair the opening or penetration without detection. Refer to Tolk and Benz[1] for an excellent summary of TIE general options and relative strengths.

3 TECHNOLOGY OPTIONS

Maintaining confidence that items have not been tampered with requires a systematic approach and is broadly termed "containment." Comprehensive containment verification includes sealing systems and also the integrity of the entire enclosure or item, such as welded joints, to ensure there have been no penetrations undetected by the sealing system. There is not one particular containment verification solution for all technologies, equipment, or items and each must be evaluated separately. In this section, the toolbox of containment technologies is described.

3.1.1 Seals

Options for seals include the following: metal cup seal, (future) glass seal, NIC Quickseal (with modification), Cobra seal, adhesive seal, Electronic Optical Sealing System (EOSS), and CoCIM (wired or wireless option). These will be discussed here with advantages and disadvantages.

---

[1] K.M. Tolk and J. Benz, *Options for Tamper Indicating Enclosures in Treaty Verification Equipment*, April 24, 2015.

3.1.1.1 Metal Cup Seal

The metal cup seal is the workhorse of the IAEA—it is a small metal two-part, single-use passive loop seal. It is used in applications that include hasps or the ability to loop a wire to ensure closure—the wire ends are secured inside the seal body. It is extremely robust and low cost. However, verification is labor intensive and not in-situ. The seal receives a unique identity through random solder scratches inside the seal. An inspector images these scratches before application, and then after use verifies the images of the scratches match. This seal is not recommended for use due to the time consuming verification as well as security concerns.

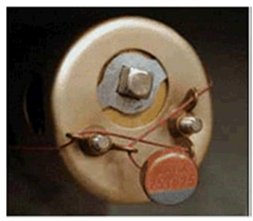

Figure 1: Metal cup seal. Image courtesy IAEA.

3.1.1.2 Glass Seal

The IAEA is currently developing the glass seal as a replacement for the metal seal. It is somewhat larger than a metal seal, perhaps twice the size. Unique identity is formed through colored swirls throughout the glass that will be imaged before, during, and after use. Tamper attempts result in a shattered seal that cannot be easily reassembled. Not enough is known currently about this seal to determine whether it is viable and it may not be available.

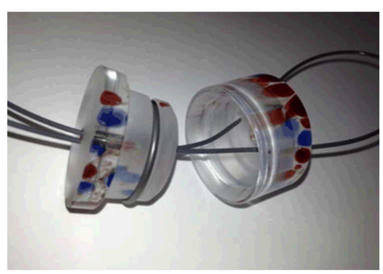

Figure 2: Glass seal prototype

3.1.1.3 NIC Quickseal

The NIC Quickseal XLP (Figure 3) is a simple mechanical loop seal. It has a one-piece transparent polycarbonate plastic body and uses a two or three strand twisted stainless steel wire that can be either independent of the seal or secured to the seal body (as provided by the vendor). The seal cap and the seal body are connected with a plastic tether. Seal installation is accomplished by threading the seal wire through either holes or a hasp on the item to be secured and then placing the wire through a hole, which passes through the center of the seal body and is secured when the seal cap is snapped in place. Excess wire is then trimmed after seal closure. A wire cutter is the only tool required to install the seal. After installation, the seal should be inspected to ensure that it is properly installed.

The seal can be ordered with reflective particles molded into the seal body, providing a unique ID (it otherwise contains no unique ID). However, this method requires a photographic seal reader and image comparison software for contrasting reference and deployed images. Unfortunately, NIC Products does not produce a reader to support this application and thus one would require development. Advantages of the seal are that it is low cost and simple to deploy. Disadvantages are that it does not have a reader that supports the reflective particles, which are required to create a unique ID for the seal.

Figure 3: NIC Quickseal.

3.1.1.4 Cobra Seal

The Cobra seal is a passive fiber optic loop seal. The ends of the fiber optic cable are inserted into a plastic seal body, where a cutting blade cuts into and impedes light flow through arbitrary strands. Images are used to record and verify the distinctive characteristics of light through the cut fiber strands. The Cobra seal is durable, easy to use, small, lightweight, low cost, and verification of seal identity and integrity can be performed in-situ. The latest version includes reflective particles in the seal body for increased tamper-indication. The disadvantage is that the latest seal reader is expensive and based on an iTouch. Older seal readers were based on film cameras.

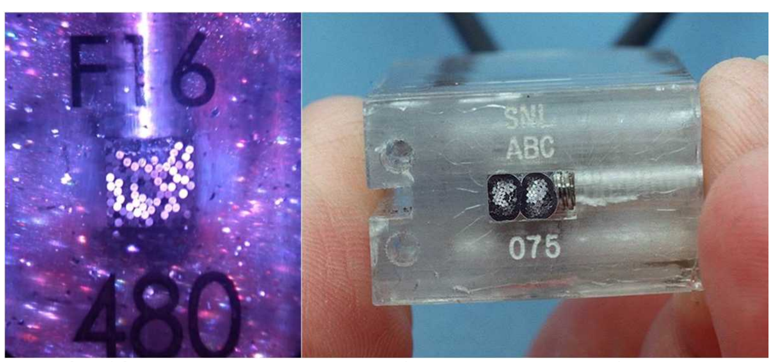

Figure 4: Cobra seal. (Left) illuminated patterns from the spliced fiber optic cable. (Right) Two ends of the fiber optic cable secured inside of the body. Images courtesy SNL.

Figure 5: Old Cobra seal reader, based on Polaroid. Image courtesy SNL.

3.1.1.5 Adhesive Seals

Adhesive seals are made of special materials which cannot be removed without leaving evidence of seal damage nor reattached. They are easy to use and low cost. However, they are typically considered only for short term sealing applications unless they are combined with another type of seal.

3.1.1.6 Electronic Optical Sealing System (EOSS)

The EOSS seal is an active fiber optic loop seal intended for applications that require periodic access. It is reusable, meaning the fiber optic loop can be unattached and attached multiple times, with each change time and date stamped and recorded. Access to the seal case is also recorded, whether or not it is simply opening the battery compartment or unauthorized penetration into the case. These events and state-of-health are recorded in non-volatile memory, and can be sent authenticated and encrypted to a reader (connected physically). The advantages of the seal are the ability to open and close multiple times, to securely record each opening and closing, and remote data transmission capability. The major disadvantage is the cost of the seal, on the order of several thousand U.S. dollars, as well as the need for an external reader. Another disadvantage is that the EOSS seal uses secret key cryptography and there are issues with key management and joint-use (essentially only one party can independently authenticate messages generated by the seal).

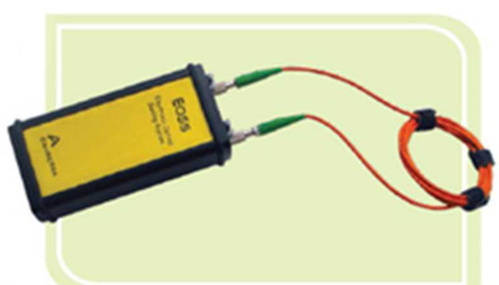

Figure 6: EOSS active fiber loop seal.

3.1.1.7 CoCIM Seals

The Secure Sensing Platform (SSP) based CoCIM, is an active, reusable fiber optic loop seal that can locally store data (tamper events, fiber open/close events, seal state-of-health) and later communicate the data via secure (authenticated and encrypted) RF, infrared, or direct-connected wired link to an associated on-site Coordinator. As with the EOSS, the advantages of the CoCIM are the ability to open and close multiple times, to securely record each opening and closing, and remote data transmission capability. An advantage over EOSS is that CoCIM utilizes public/private key pairs—the private key is generated on the CoCIM seal, and the public key on the reader. This makes key management much simpler than with EOSS.

Figure 7: (Left) CoCIM RF Coordinator (Right) CoCIM. Image courtesy SNL.

3.1.2 Unique Identifiers

Options for extrinsic UIDs include the Reflective Particle Tag (RPT) and the Unique Surface Etched (USE) tag. Depending on requirements, intrinsic UIDs could be utilized. Examples include the use of eddy currents or other ultrasonic techniques to use the intrinsic features of the item itself as a unique identifier.

3.1.2.1 Reflective Particle Tag

RPT is a field applied UID composed of specular hematite particles randomly dispersed in a clear, adhesive polymer matrix. The hematite particles are of size ~80 µm and exhibit flat, reflective facets (Figure 8). The “contact” reader is based on a custom camera and collimated illuminators arranged at multiple different angles. To inspect a UID, the reader is physically attached to the frame (Figure 9, Figure 10) for precise alignment and records images using each of the illuminators. For each of the illumination angles, only a subset of the hematite facets will be oriented in such a manner as to redirect the incident illumination beam toward the aperture of the camera. This subset will appear as small bright spots in the recorded image. In this manner, a sequence of complex and highly unique patterns is obtained that can be used to physically authenticate the UID. In addition, a unique, barcode like identifier (ID) is placed at the midline to identify the UID (Figure 11). Once a UID is set, an inspector can return to the item, attach the reader, compare IDs, then reflective patterns to determine if UID sets match.

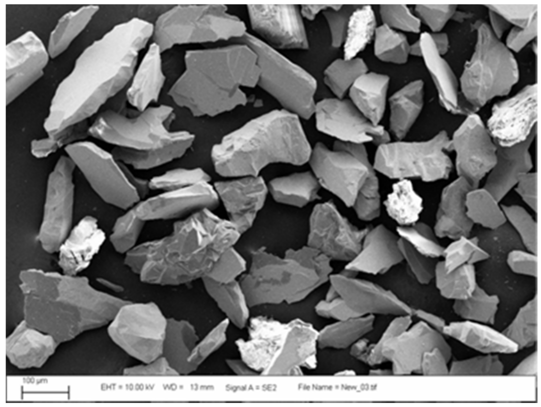

Figure 8: A scanning electron microscope image of the faceted specular hematite particles used in the RPT system. Image courtesy SNL.

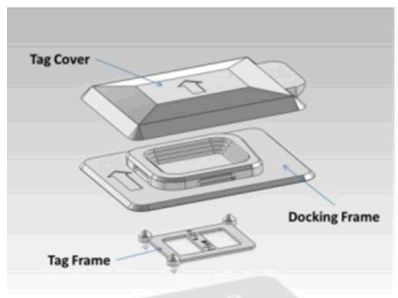

Figure 9: The contact RPT cover, docking frame, and UID frame. Image courtesy SNL.

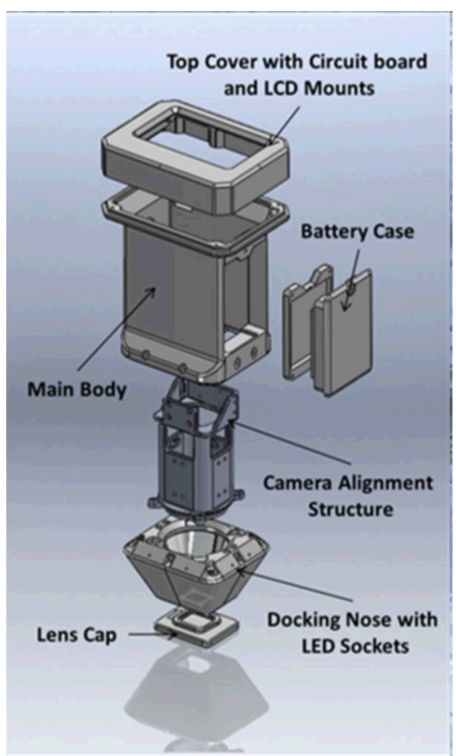

Figure 10: The contact RPT reader. Image courtesy SNL.

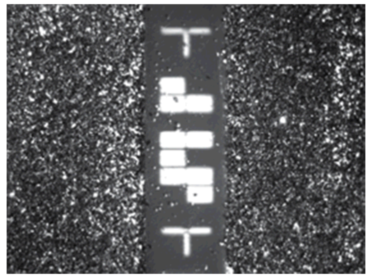

Figure 11: Reflective particles create unique patterns that are difficult to duplicate. A strip located in the middle of the UID contains a unique binary code ID. Image courtesy SNL.

The RPT architecture has proven resistant to counterfeiting and removal without detection. Furthermore, the tag requires no power, and is stable through temperature extremes, rough handling, and years of service. A "non-contact" reader prototype has been developed that allows standoff (~10 cm) imaging and verification, does not require a frame, and can be applied to more complex surfaces including curved surfaces.

3.1.2.2 Unique Surface Etched Tag

The Unique Surface Etched (USE) tag is a unique, non-transferrable UID scribed directly onto the surface of an item via femtosecond laser. The scribing should not impact the performance of the item as the pattern depth is 10-120 nm. Metals that have been scribed include: titanium, SS304, and SS316. The verification features of the UID have been tailored for macro-patterns for easy identification (QR code), and micro-patterns to provide non-reproducible features for authentication. A QR code reader is used to read encoded information such as UID identification and text that may be relevant to the monitoring scenario. The micro-patterns can be read via laser interrogation; however, a reader has not yet been designed for this purpose and thus the UID cannot currently be recommended.

Figure 12: Unique Surface Etched (USE) tag. Image courtesy SNL.

3.1.2.3 Eddy Current

Eddy current is an intrinsic UID possibility, used on the welds at the seams of the metal enclosure or item. Eddy current scans would fingerprint these welds and allow comparison before and after for a unique ID.

3.1.2.4 Ultrasonic Intrinsic Tag

Another option is the Ultrasonic Intrinsic Tag (UIT). This equipment was one of two, along with RPT, originally approved for use in START, to uniquely identify treaty limited items. UIT functions by interrogating a location to measure the reflection of ultrasonic waves as they interact with the subsurface grain structure of the material, and comparing the reference to subsequent measurements. The electronics of the reader are fairly simple. However, the unit would require additional effort to get the reader into a state where it could be used. Therefore, this device cannot currently be recommended. Figure 13 shows a comparison with a non-match between inspection and reference measurement.

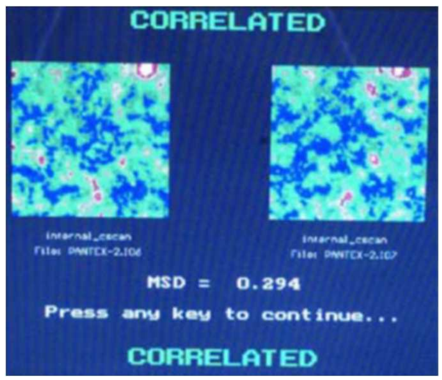

Figure 13: UIT Measurement Comparison

3.1.3 Seal as UIDs

Seals can alternately be used as UIDs if they can be attached to the item in a secure manner. For instance, to uniquely identify the item itself, a seal can be applied to the hasps of the item. The seal acts as a UID as it cannot be removed without leaving evidence.