U.S.-UK Information Barrier Workshop

SAND2007-1626P

Historical Technical Review
Information Barrier Technology

Trusted Radiation Attribute Demonstration System (TRADS) and Trusted Radiation Identification System (TRIS)

Kevin D. Seager

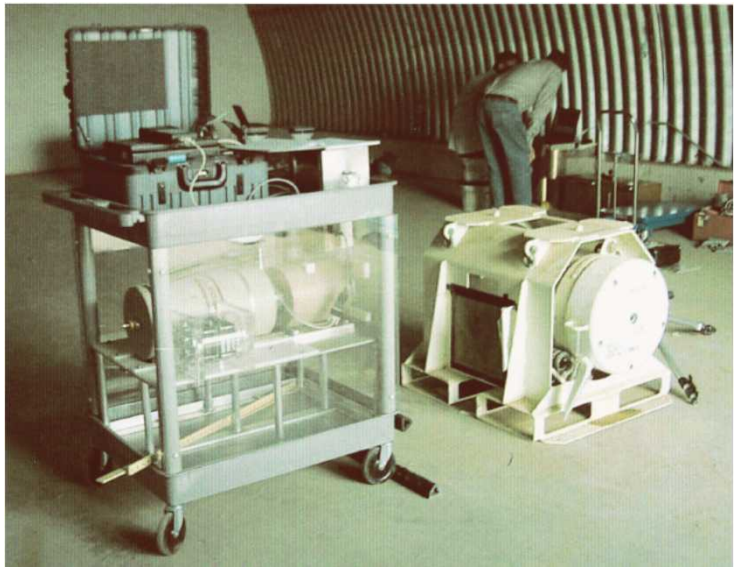
Sandia National Laboratories

April 17, 2007

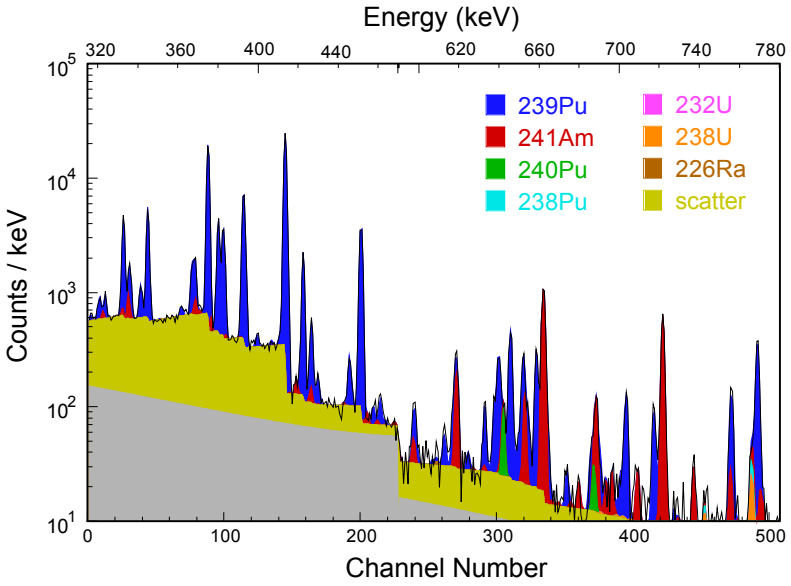
National Nuclear Security Administration

Sandia National Laboratories

Sandia developed the Trusted Radiation Attribute Demonstration System (TRADS) in FY99 to address the needs for nuclear weapons and weapon components authentication under START III.



TRADS being tested at Pantex in 1999.



Spectrum for 400 gm Pu Plate

Sandia National Laboratories

What does "trusted" mean?

- **Design features of the radiation signature inspection system need to satisfy the fundamental requirements for an information barrier:**
  - **Protection of host-country classified information**
  - **Building inspector-country confidence via authentication that the results of measurements accurately reflect the characteristics of the TAI being measured**
- **Ensuring inspector confidence is especially challenging because, unlike inspections under the Intermediate Nuclear Forces (INF) treaty and Strategic Arms Reduction Treaty (START) that utilize *inspector-supplied equipment*, future arms control regimes will likely rely on *host-supplied equipment* for conducting radiation measurements.**

Sandia National Laboratories

TRADS Requirements

- Confirm attributes of plutonium-bearing weapons and weapon components (i.e., classified configurations). Attributes include:
  - the plutonium mass must exceed a declared threshold
  - the ratio of Pu-240 to Pu-239 must be consistent with weapons-grade plutonium
- Protect sensitive information while assuring inspector that measurements are authentic
- The system must be portable and battery powered
- Tamper resistance is important because the system may be moved from dual-secure storage to use location
- Must be capable of measuring complete nuclear weapons

There are unique requirements for the TRADS hardware and firmware.

- **Hardware**
  - **Must ensure that classified information is not compromised**
  - **Must be inspectable and tamper-protected**
- **Firmware**
  - **All source code is available to the inspector; implies no proprietary commercial software**
  - **Verification algorithm required to confirm authenticity of firmware without revealing classified information**
  - **Display only unclassified information and conform to information security requirements; implies automated calibration and self-test**

TRADS Conceptual Design

Tamper Resistant Case

Information Barrier
- architecture
- software
- procedures

Trusted Processor

Red

Black

High Purity Germanium Detector

Multichannel Analyzer

Display and Keypad

Collects and analyzes classified data

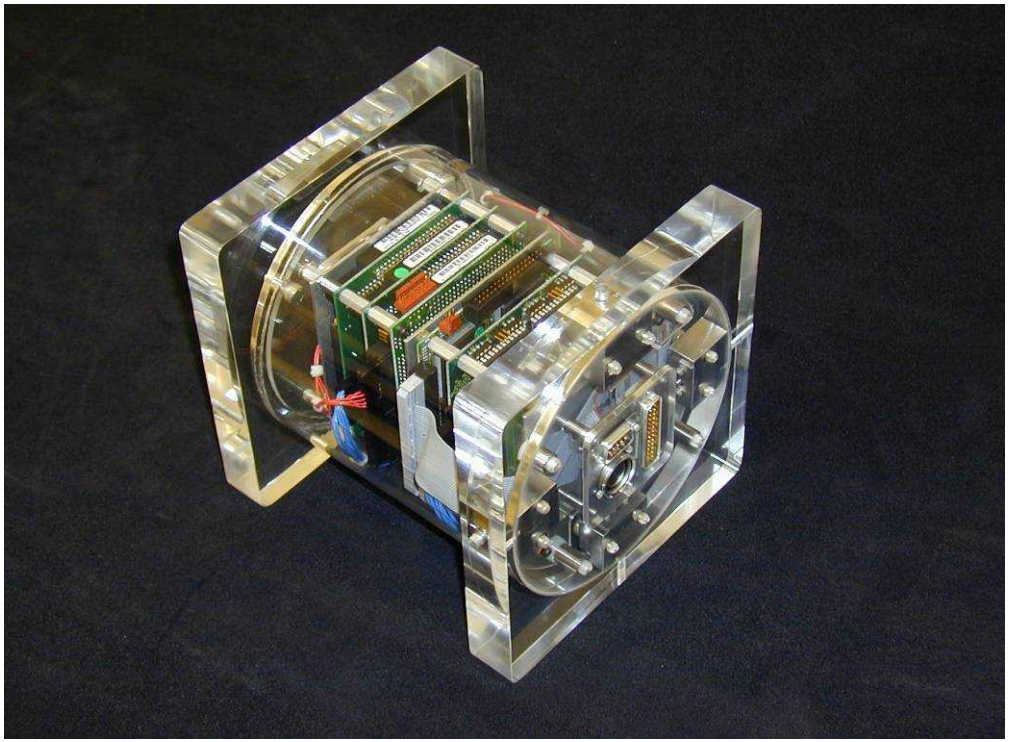
Dedicated serial port

Communicates between keypad and red processor

Hand-held user interface displays "yes/no/failure"

Sandia National Laboratories

Sandia completed development of Version 1 of the Trusted Processor utilized by TRADS in 1999.



Transparent Version

Sandia National Laboratories

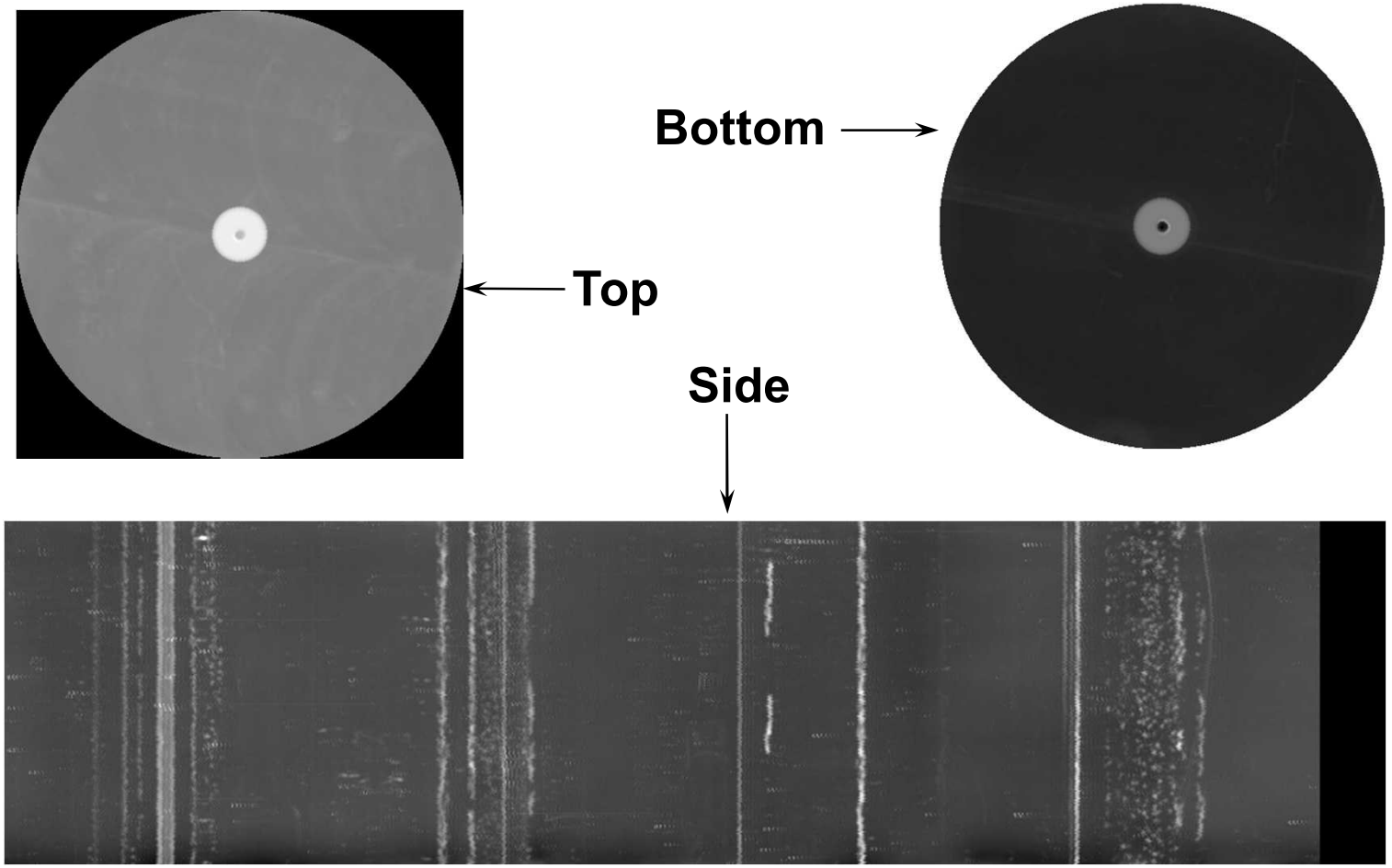
Inspection of Trusted Processor

- Inspector can perform eddy-current scan of trusted processor in ~10 minutes
  - Simultaneous scanning of top, bottom, and side of trusted processor
  - Container can be uniquely identified by eddy-current scan of welds
  - Comparison of subsequent scans with original reveals penetrations not detectable by visual examination

2nd Generation Eddy-Current Scanner

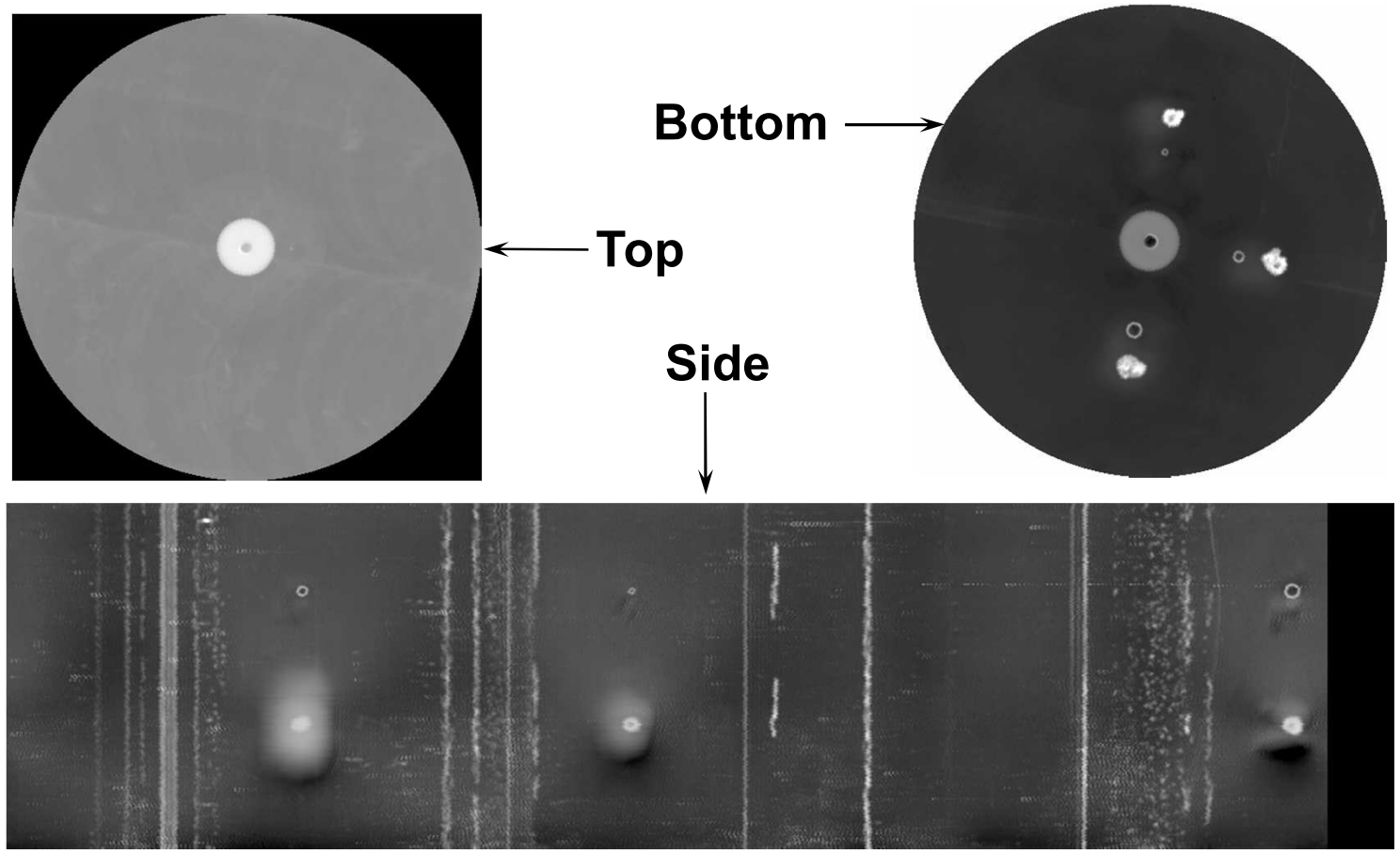
Sandia National Laboratories

Eddy-current Scans of Trusted Processor



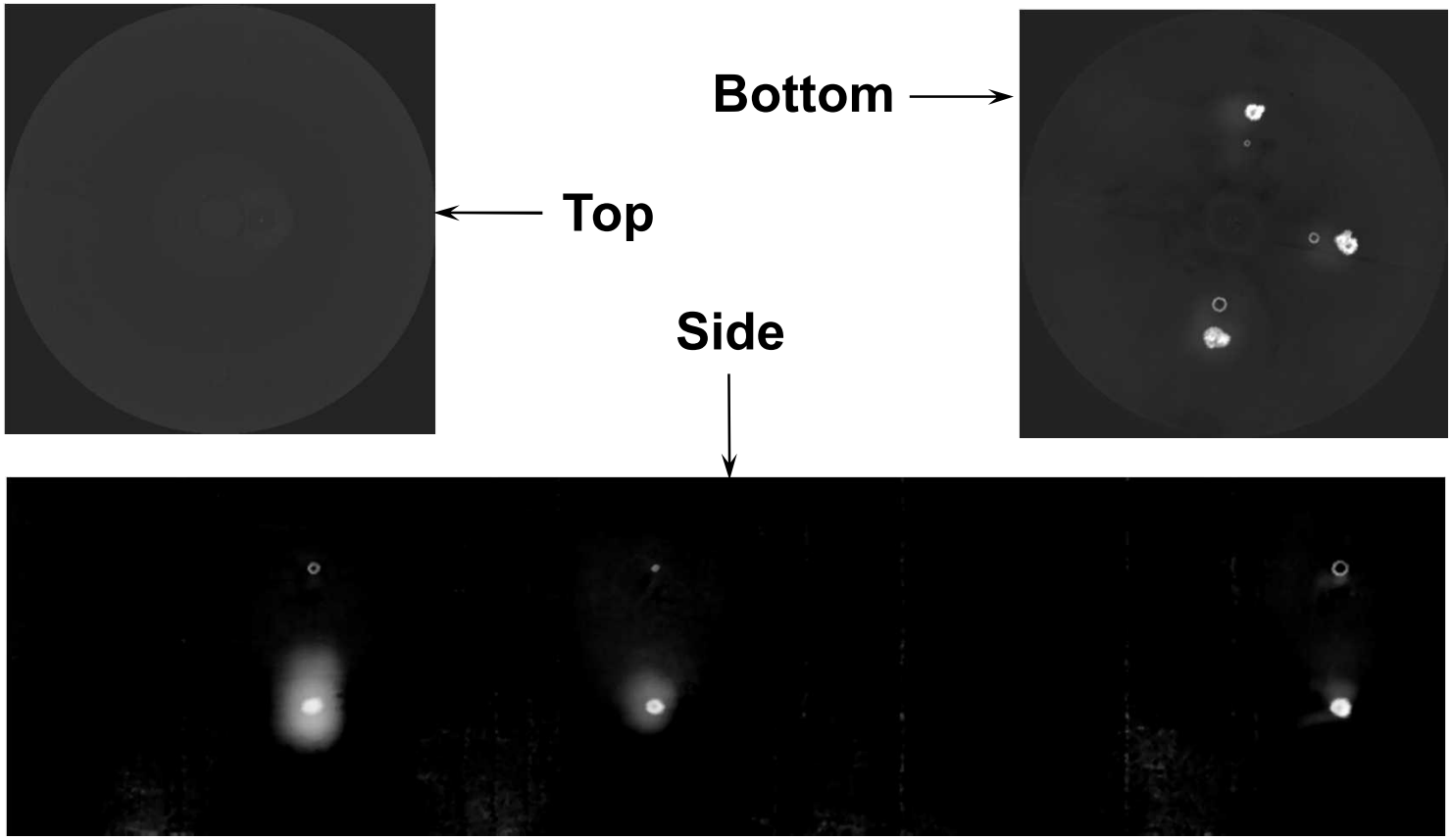
Sandia National Laboratories

Scans of Test Canister After Pairs of 1/16”, 1/8”, and 3/16” dia Holes Were Drilled and Plugged or Welded



Sandia National Laboratories

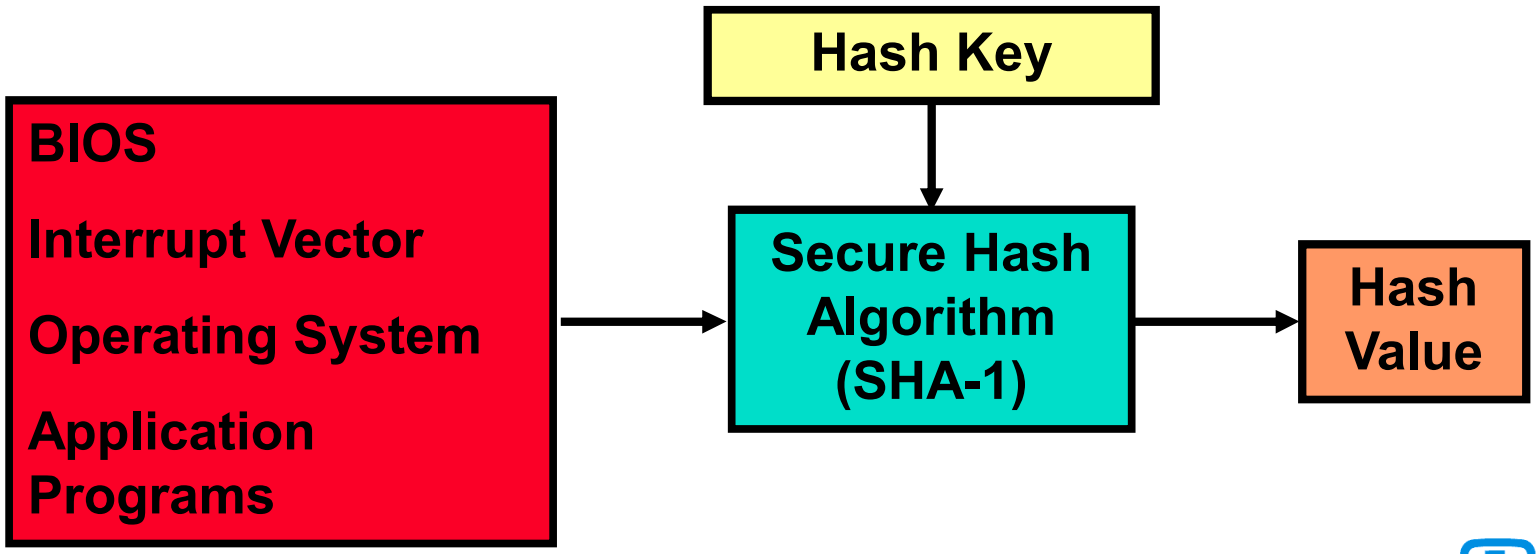
Difference in Eddy-Current Scans Before and After



Sandia National Laboratories

Firmware Integrity Verification

- Inspector performs authentication of trusted processor firmware using hash keys entered via the hand-held user input/output device.
- The hash value generated during the inspection must exactly match the hash value generated earlier using the same hash key on an identical trusted processor with firmware known to be correct.



Sandia National Laboratories

TRADS Summary

- It is possible to confirm plutonium mass and isotopic attributes with high confidence using a portable system utilizing only one HPGe detector.
- Minimum Mass Estimate (MME) method provides robust data analysis algorithm, but it may be necessary to set mass threshold attribute considerably lower than actual mass.
- TRADS demonstrated several applicable technologies including:
  - Divided architecture and software design that protects classified information
  - Tamper-resistant enclosure that provides low RF leakage
  - Keyed hash algorithm

Sandia National Laboratories

Trusted Radiation Identification System

- The Trusted Radiation Identification System (TRIS) was developed in FY00 and FY01 to build on the technology previously demonstrated as the Radiation Inspection System (RIS), while incorporating many of the information barrier features utilized by TRADS.

- TRIS uses radiation template measurements to initialize Treaty Accountable Items (TAIs) into an arms control regime and to maintain continuity of knowledge during storage.

Sandia National Laboratories

Energy group structure used to analyze low-resolution spectral data

Energy Range (keV)	Principal Significance of the Energy Group	Template Uncertainty (%)
80 - 120	U and Pu x-rays	10
120 - 160	continuum	1
160 - 172	sensitivity to energy-calibration error	exclude
172 - 198	^{235}U at 186 keV	1
198 - 230	^{237}U at 208 keV, variable in plutonium	exclude
230 - 290	continuum	1
290 - 350 plus 390 - 500	^{239}Pu full-energy peak region (change in sum of counts is insensitive to energy calibration error)	1
350 - 390	^{239}Pu full-energy peak region	1
500 - 600	continuum	10
600 - 711	^{241}Am at 662 keV, variable in plutonium	20
711 - 821	^{238}U at 766 keV	2
821 - 936	continuum	20
936 -1090	^{238}U at 1001 keV	1
1090 -1200	continuum	5
1200 -2480	continuum from ^{238}U and ^{232}U	20
2480 -2750	^{232}U at 2614 keV, variable in HEU	30

Sandia National Laboratories

TRIS Components

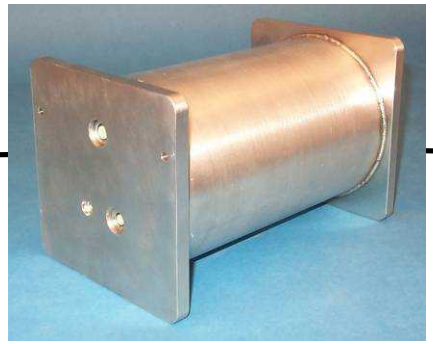
Gamma-Ray Detector

Nal Detector - uses tungsten shutter during functionality tests and background measurements

Multi-channel Analyzer

MCA collects classified gamma-ray spectrum

Trusted Processor



Trusted Processor provides information barrier via divided hardware/firmware architecture

Red Side : Classified processor analyzes spectrum

Black Side: Unclassified processor services operator instructions and sends unclassified messages

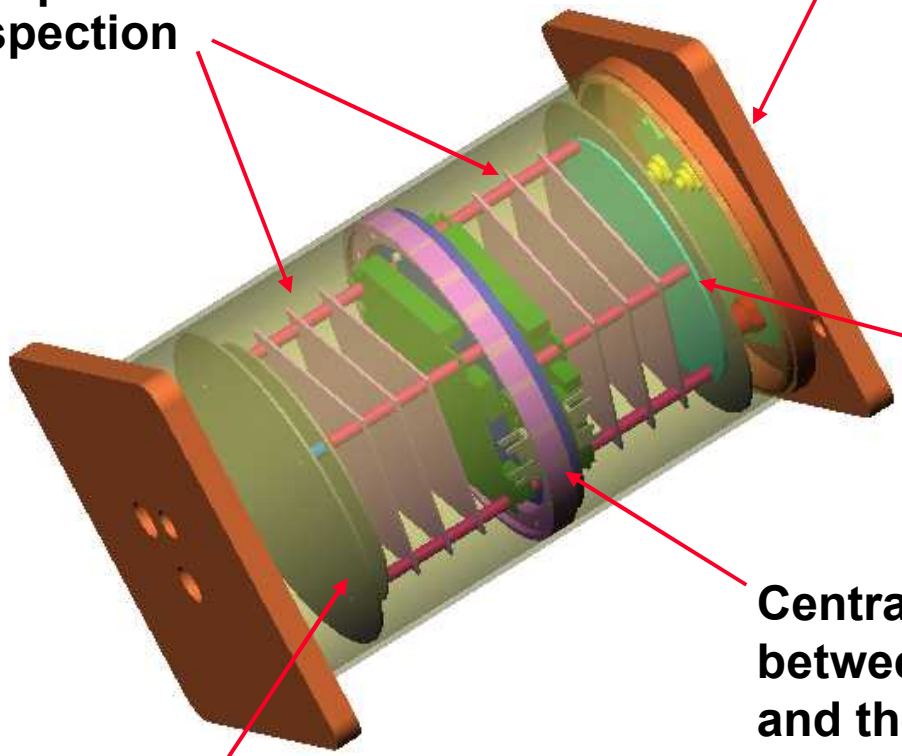
Display and Keypad

Hand-held user input/output (I/O) device displays messages and provides means to communicate instructions to Trusted Processor

Sandia National Laboratories

TRIS Trusted Processor Conceptual Design

Simple PC-104 card computers facilitate inspection



Fully-welded stainless steel case minimizes RF emissions and serves as a tamper-indicating enclosure

Active and passive tamper boards

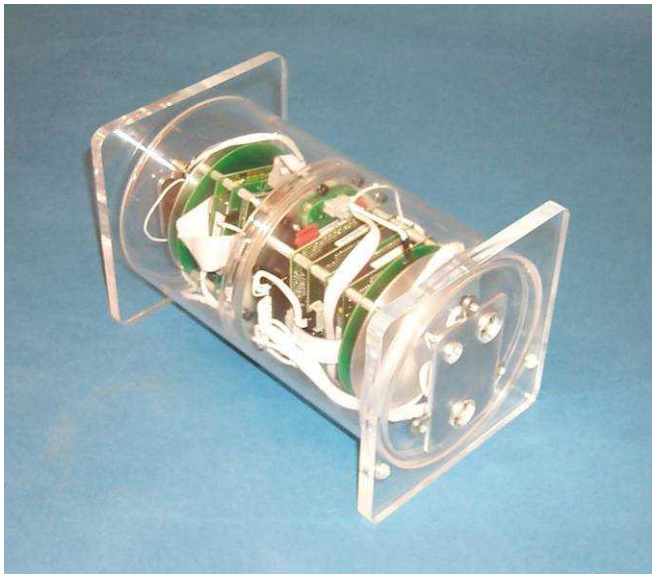
Central plate provides RF-isolation between red and black processors and thermal pads conduct heat from CPU chips to case via central plate

Active and passive tamper boards

Sandia National Laboratories

TRIS Trusted Processor

- Same type CPU (PC-104, 586) used for red and black sides
- Optical communication between red and black sides



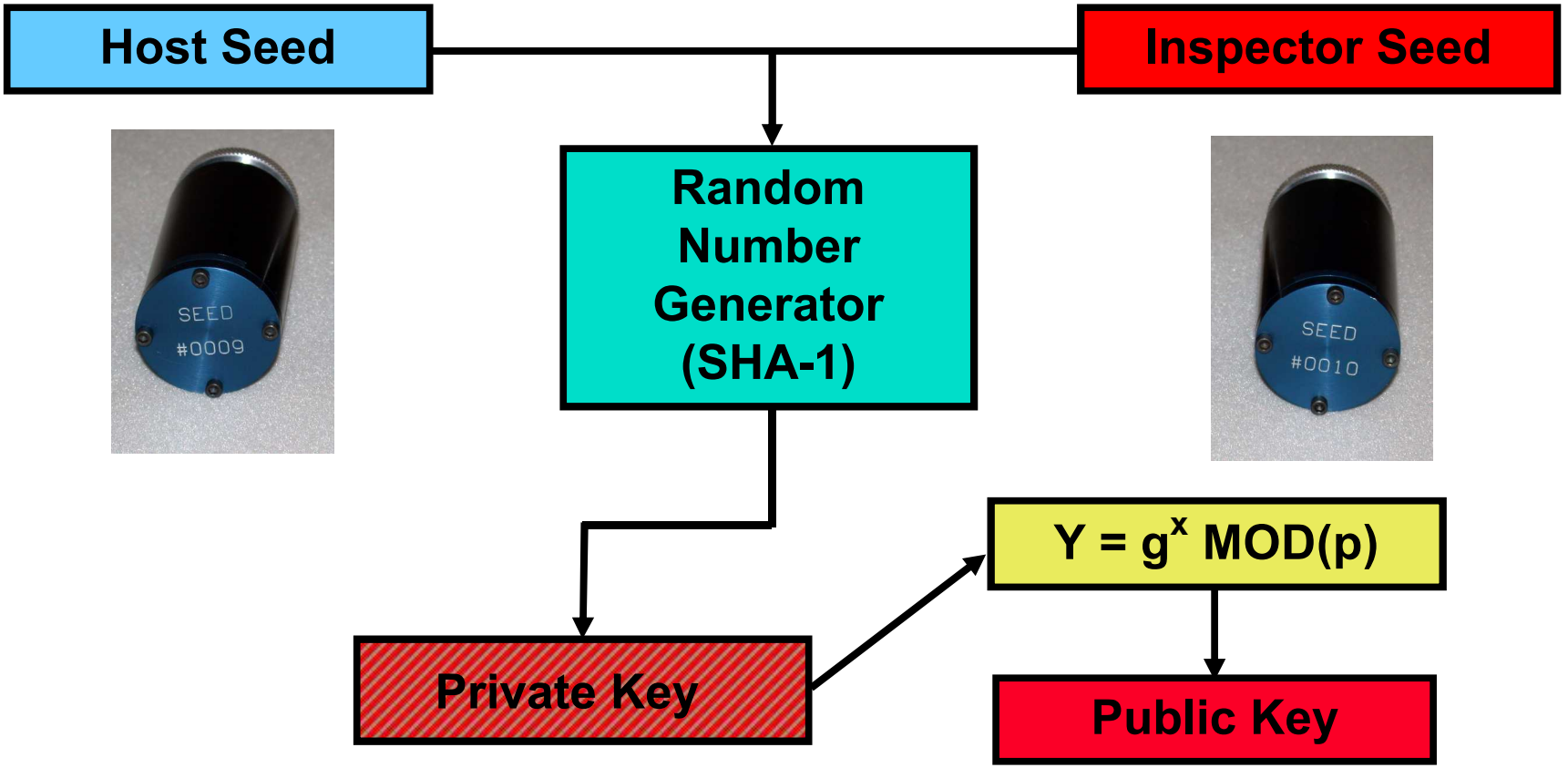
Lucite Version (for illustrative demonstrations only)

Stainless Steel Version

- Power line is filtered
- Connectors are uniquely sized

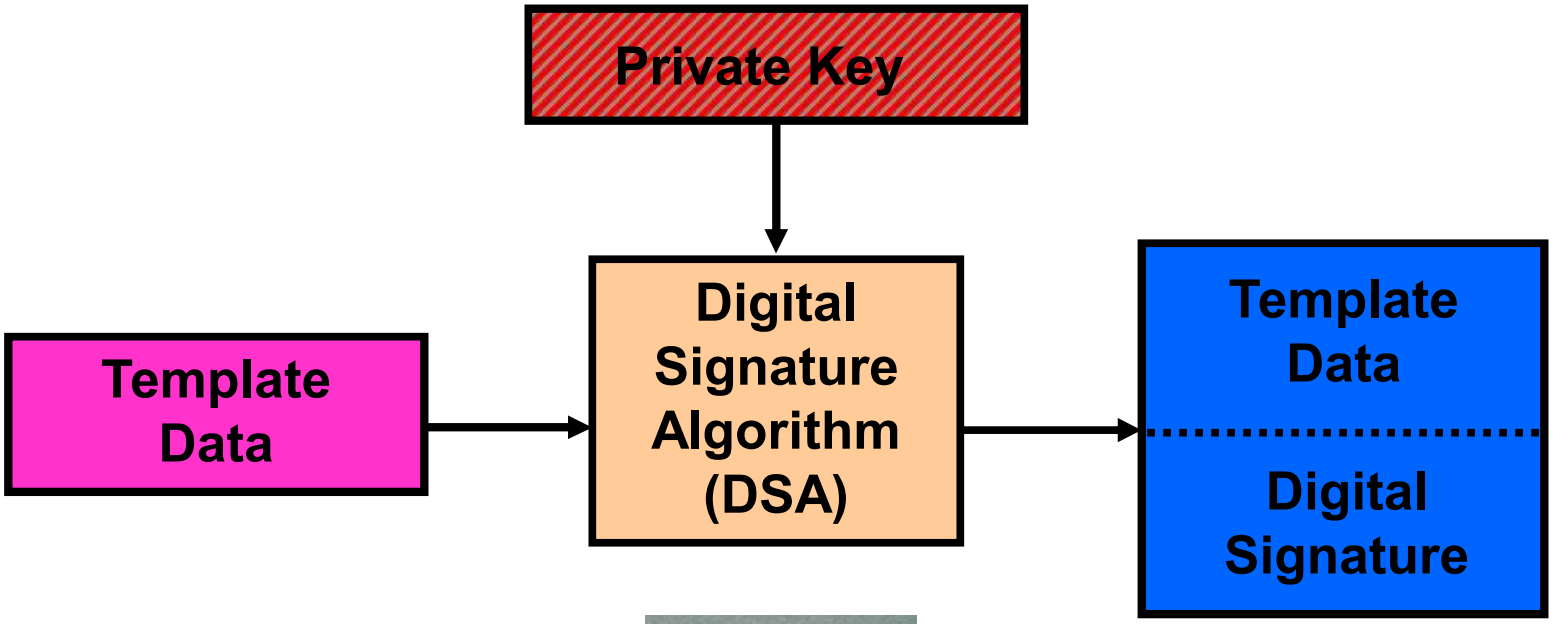
Sandia National Laboratories

Host and inspector use independent random number seeds to generate a Private/Public Key pair.



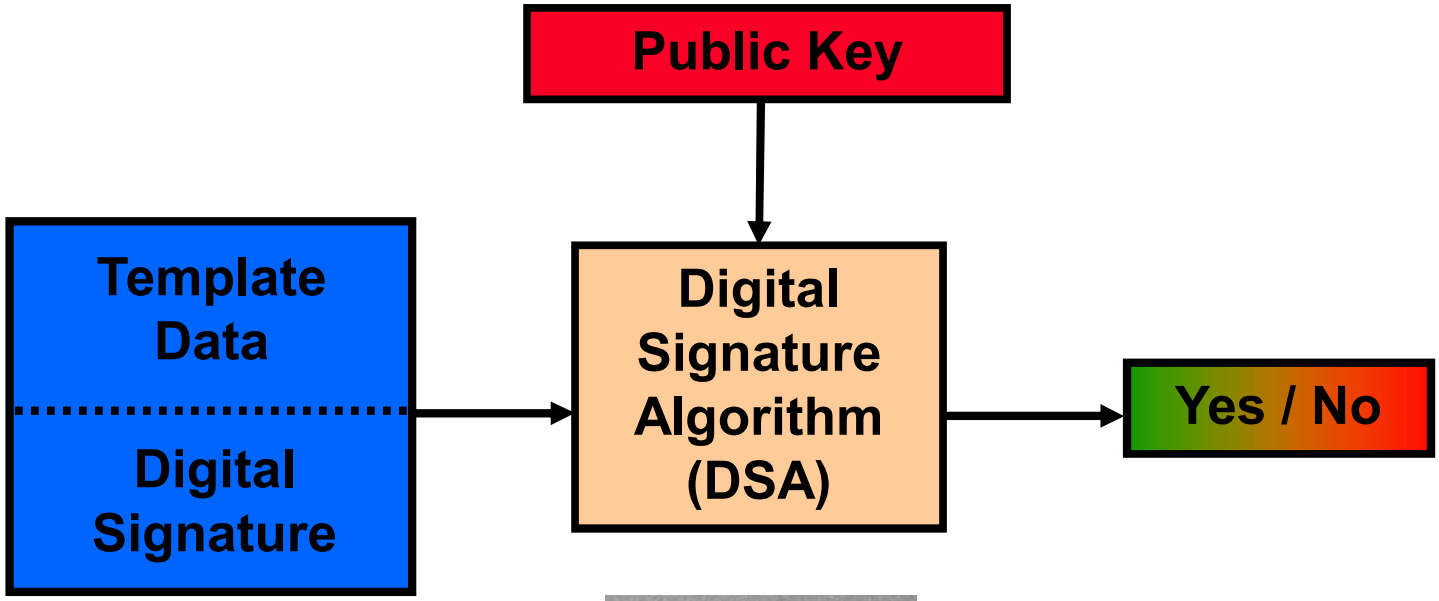
Sandia National Laboratories

Private key is used to digitally sign the template when the template is generated.



Sandia National Laboratories

The public key is used to verify the template signature when the template is confirmed.



Sandia National Laboratories

Continued Evolution of Eddy-Current Scanner

- **SNL has:**
  - **Modified eddy-current scanner to be able to accommodate current trusted processor utilized by TRIS**
  - **Developed a new probe for scanning the side of the trusted processor**
  - **Initiated analysis of sources of variation in process that influences the repeatability of eddy current scans**

3rd Generation Eddy-Current Scanner

Sandia National Laboratories

In summary, TRADS and TRIS address both Host and Inspector Needs

Item	Host	Inspector
Host supplied equipment	✓	
Only volatile memory	✓	
No single-point failure reveals classified information	✓	
Separate wiring and connectors for red and black CPU	✓	
Selective communication between red and black CPU	✓	
Low electromagnetic emission enclosure	✓	
Integrated diagnostics and self-test mechanisms	✓	✓
Battery operated and field portable	✓	✓
Cost-effective and easily maintained	✓	✓
Tamper-indicating enclosure		✓
CPU memory and template authentication		✓
All code in firmware		✓

Sandia National Laboratories