SAND2015-10382PE

Authentication Issues in Zero Knowledge Protocols

Peter Marleau

JOINT CSGAC-CISAC MEETING

BEIJING
DECEMBER 7-8, 2015

Certification vs. Authentication: It's not just for hardware

Certification – the process by which a host party gains confidence that sensitive information regarding an entity or facility remains secure.

Authentication - the process by which a monitoring party gains confidence that reported characteristics of an entity reflect the true state of that entity

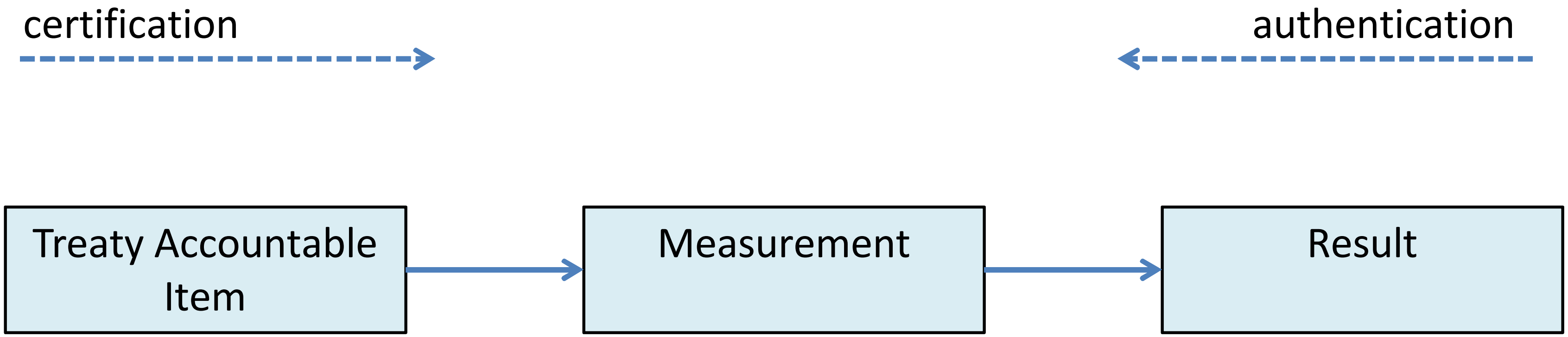
Certification vs. Authentication: It’s for the whole system

Host

- Wants confidence that no sensitive information will be leaked.

Inspector

- Wants confidence that a relevant measurement took place and the result represents the “truth”.



certification

authentication

Treaty Accountable Item

Measurement

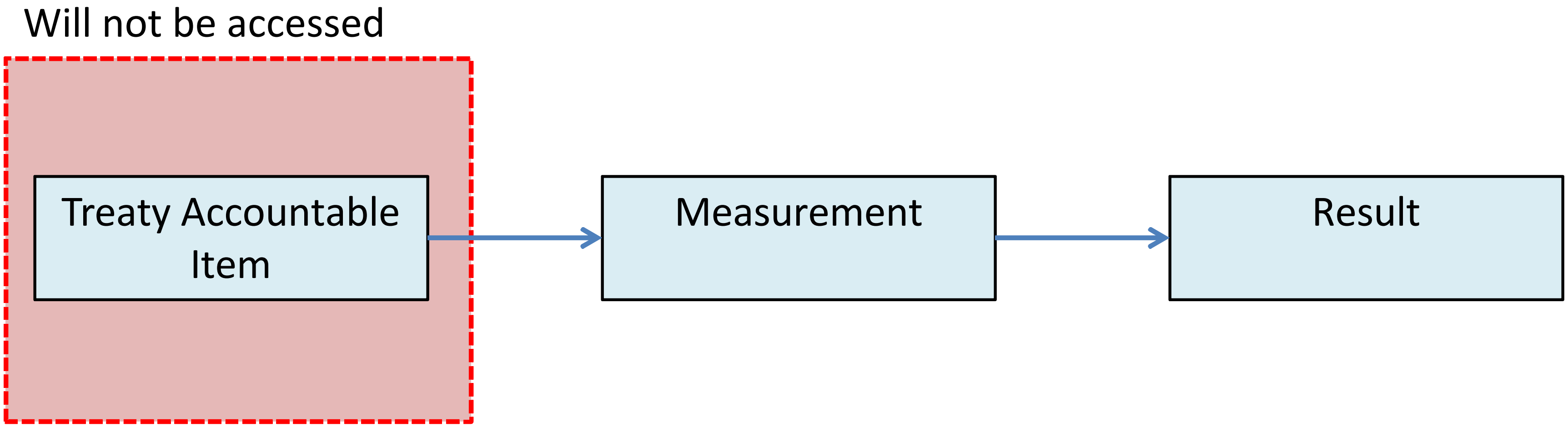
Result

Certification vs. Authentication

Host

- No sensitive information out.

Inspector



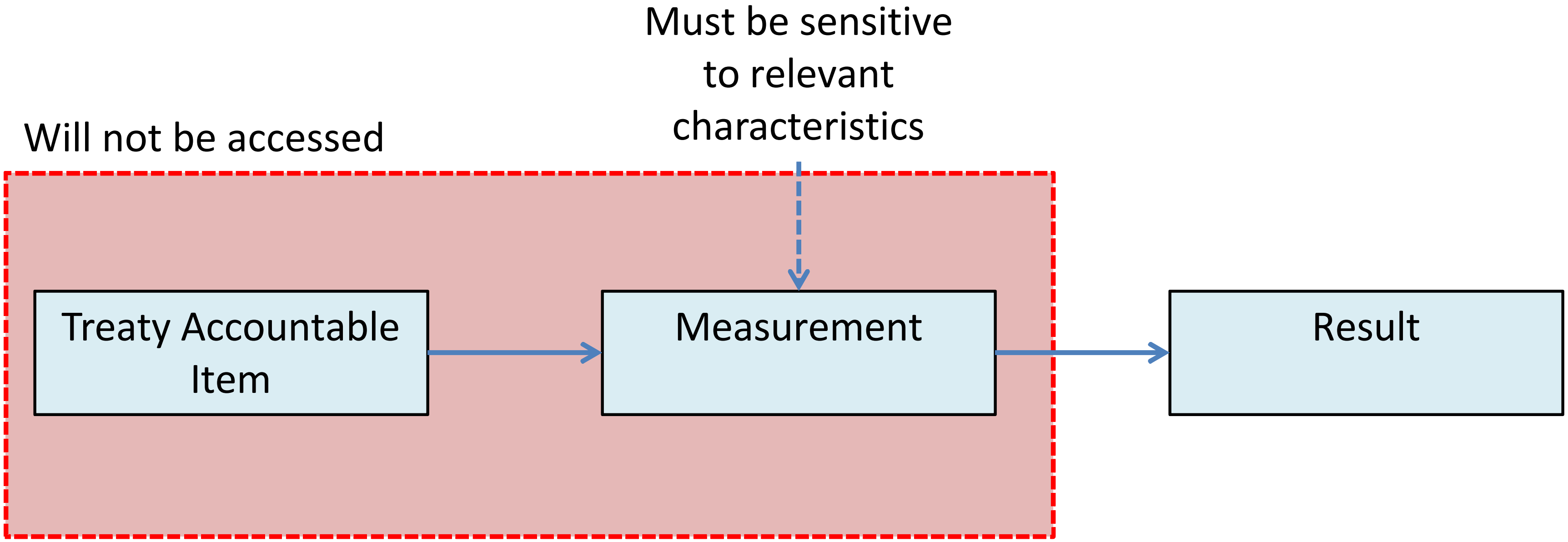
Certification vs. Authentication

Host

- No sensitive information out.
- Relevant characteristics may be sensitive.
  - The host can/should prove this to themselves.

Inspector

- Measurement must be relevant.
  - The inspector can/should prove this to themselves.



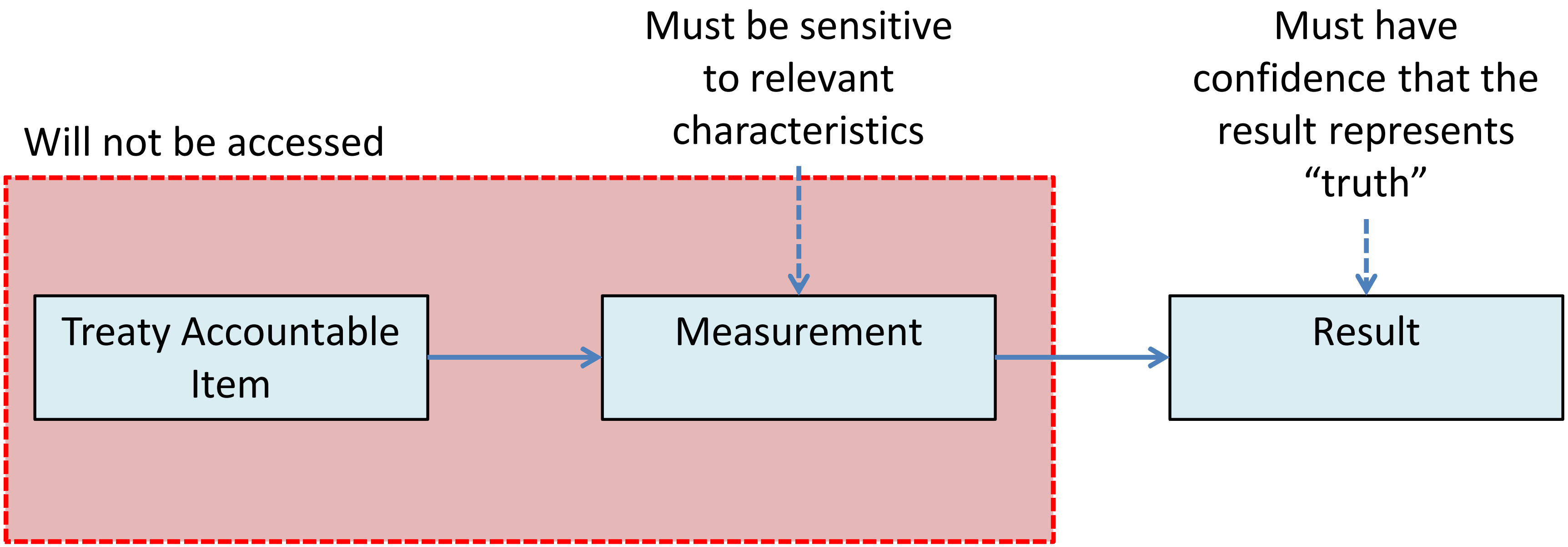
Certification vs. Authentication

Host

- No sensitive information out.
- Relevant characteristics may be sensitive.

Inspector

- Measurement must be relevant.
- Measurement took place.
- Result represents the “truth”.



Will not be accessed

Must be sensitive to relevant characteristics

Must have confidence that the result represents “truth”

Treaty Accountable Item

Measurement

Result

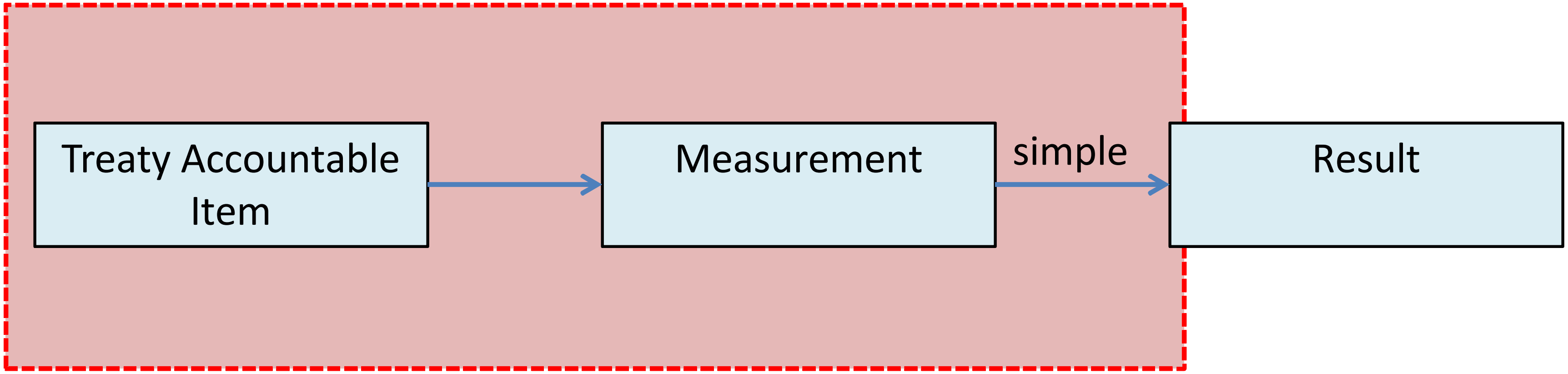
Aside #1 - Digital Computer?

Host

- Malicious firmware, Underhanded-C, etc.
- How can digital code and computers be trusted?
- The host will want to own and strongly vet this.

Inspector

- How does an inspector gain confidence that code is doing what it’s expected to do?
- Encryption and digital keys?



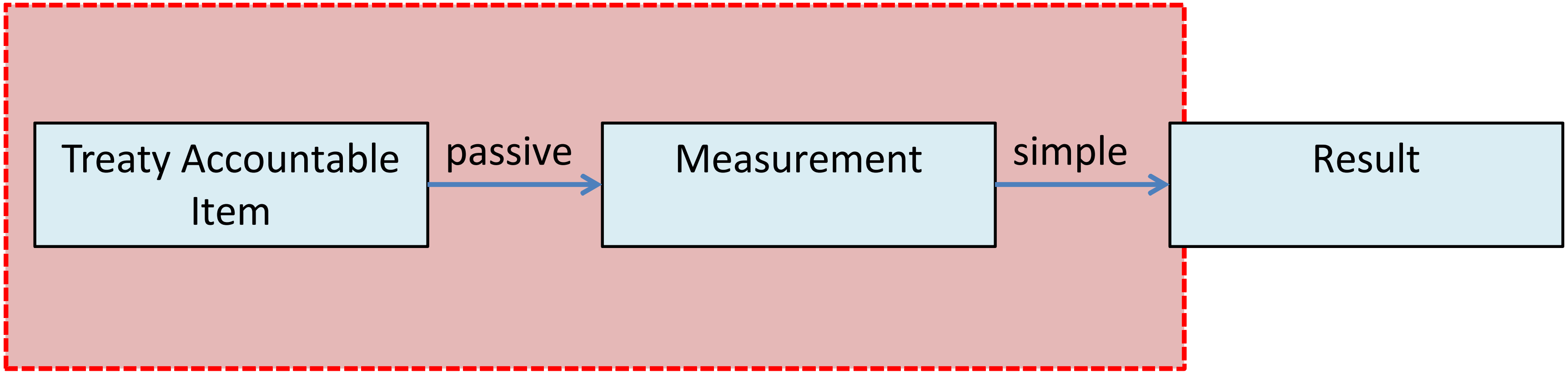
Aside #2 - Active?

Host

- Oh yeah, also don't damage my TAI.
- Might be ok if heading to dismantlement …

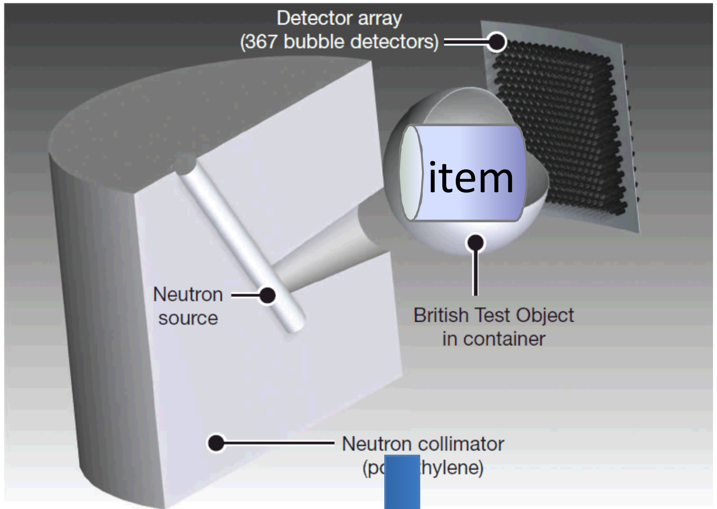
Inspector

- As long as it is sensitive to relevant characteristics …



ZKP – Neutron Radiograph + Bubble Detectors

standard

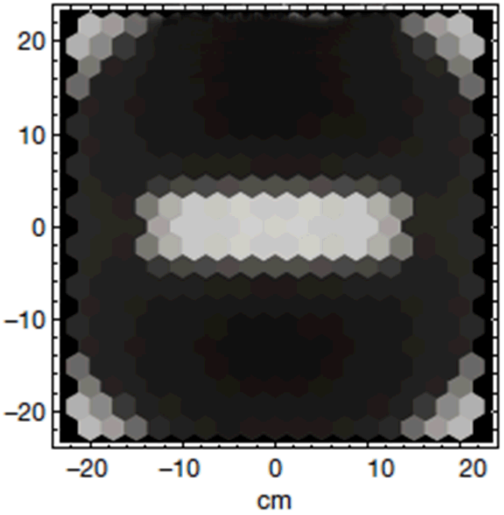


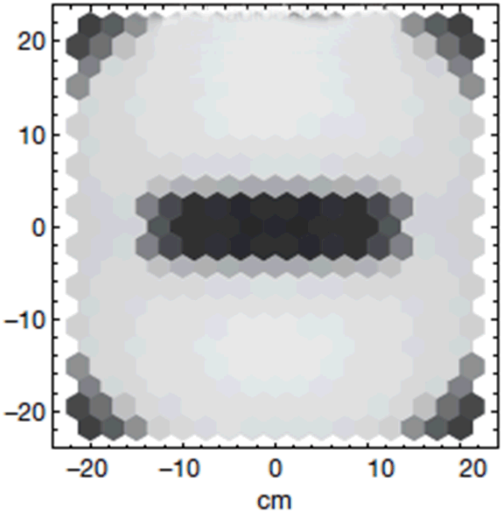
Positive results in NULL

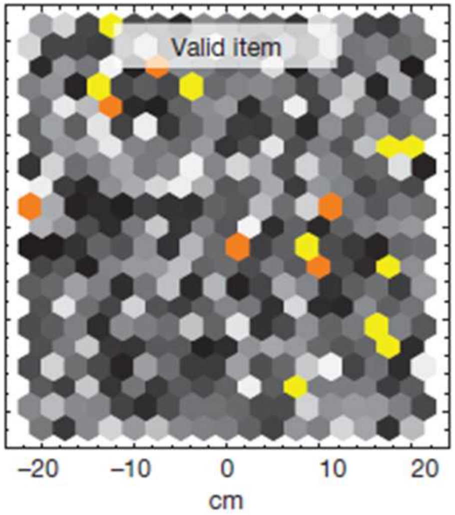
Preloaded counts based on pre-confirmed standard measurements

+ measurement

=

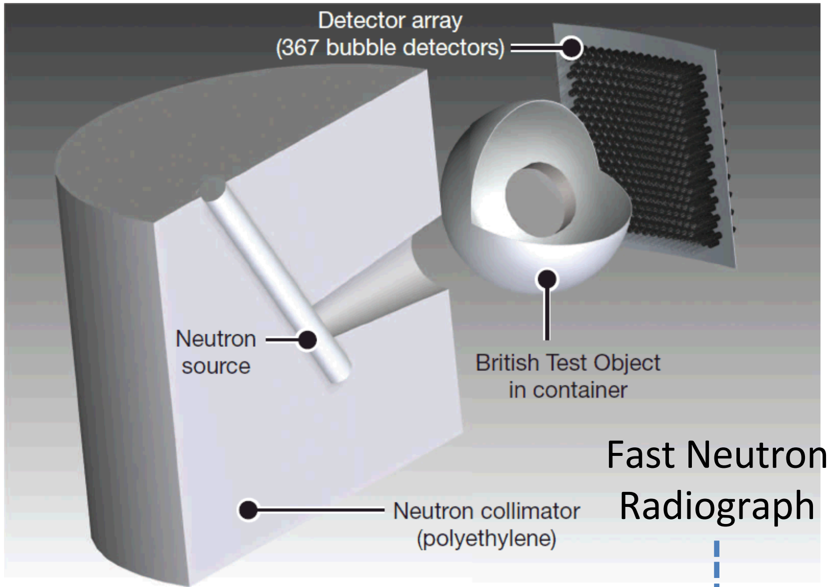




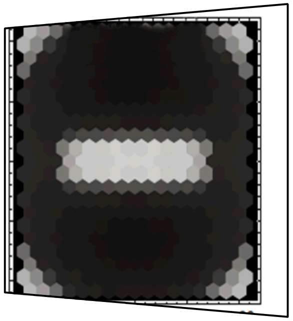


Images borrowed from: Glaser, Barak, and Goldston, “A zero-knowledge protocol for nuclear warhead verification”, doi:10.1038/nature 134557

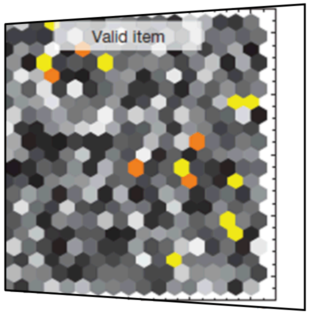
ZKP – Neutron Radiograph + Bubble Detectors


Detector array
(367 bubble detectors)
Neutron source
British Test Object in container
Neutron collimator (polyethylene)

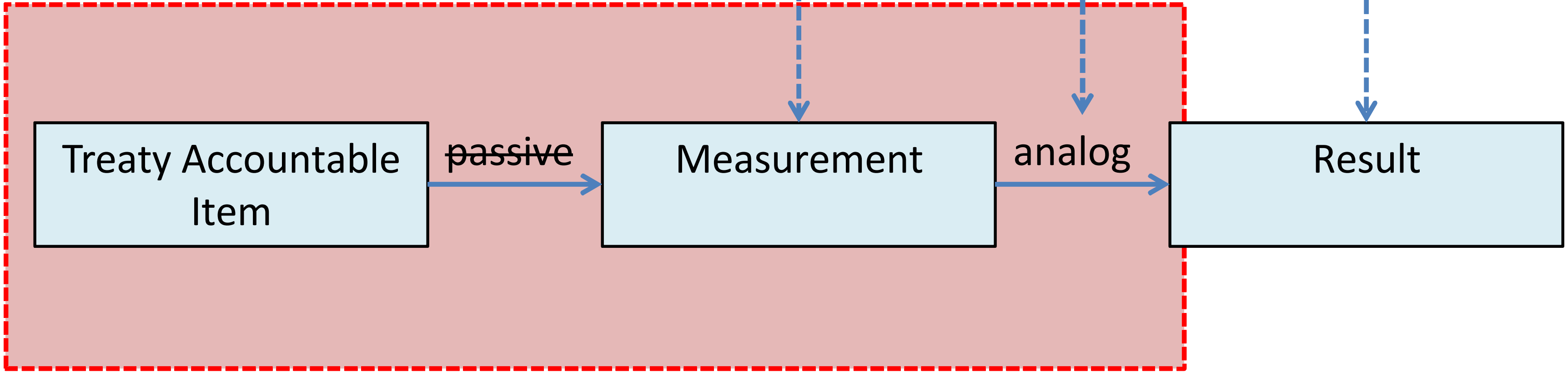
Fast Neutron Radiograph



Analog bubble detectors with preloaded inverse



Flat featured image (NULL) is a true positive.



Treaty Accountable Item

~~passive~~

Measurement

analog

Result

Images borrowed from: Glaser, Barak, and Goldston, “A zero-knowledge protocol for nuclear warhead verification”, doi:10.1038/nature 134557

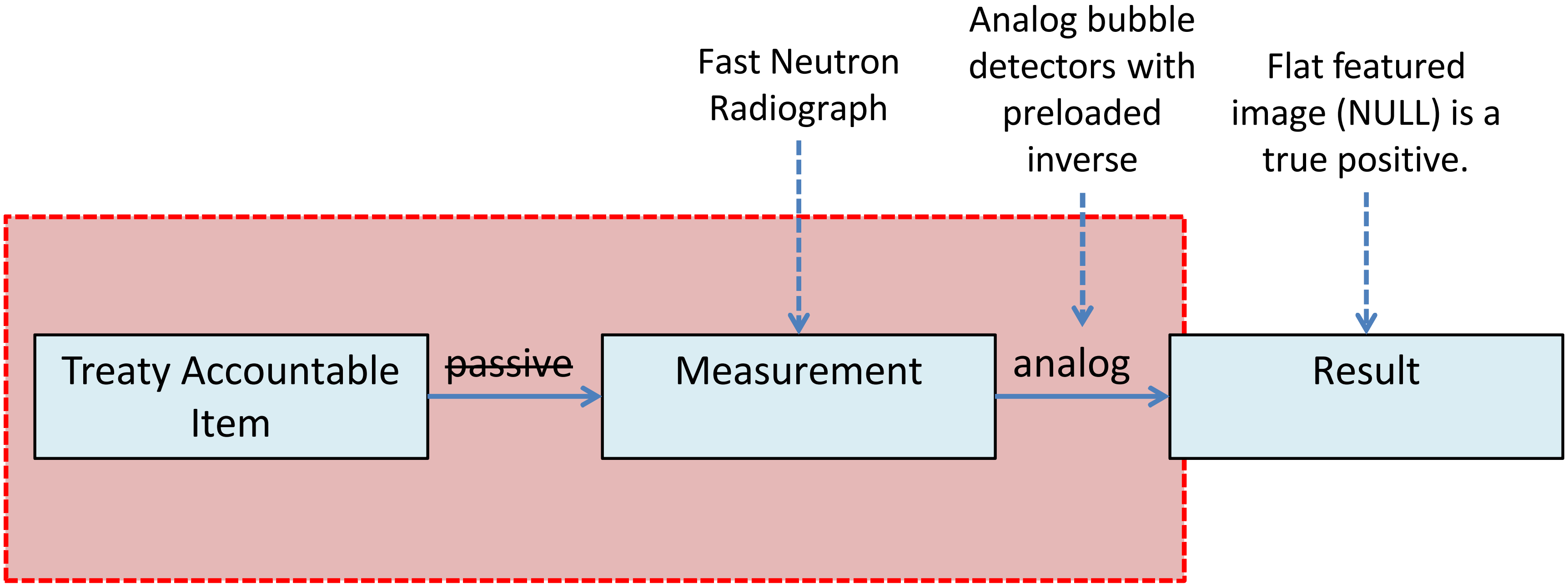
ZKP – What did we gain?

Host

- Owns the preloaded inverse, the measurement, and the result.

Inspector

- How do I know that a relevant measurement took place?
- **Pre-confirmed standard? True Negative?**



Fast Neutron Radiograph

Analog bubble detectors with preloaded inverse

Flat featured image (NULL) is a true positive.

Treaty Accountable Item

~~passive~~

Measurement

analog

Result

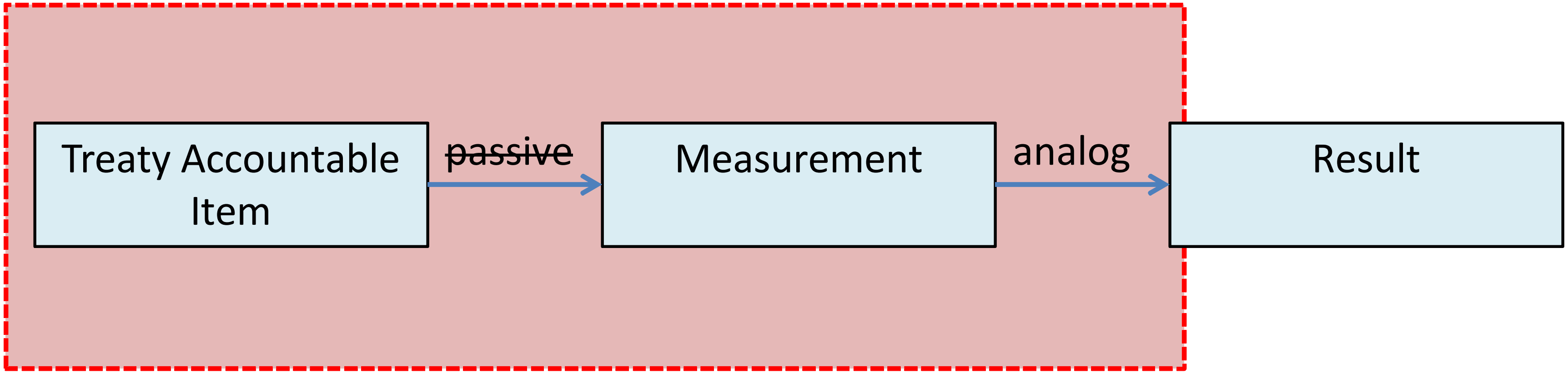
ZKP – Role of inspector choice

Host

- Presents multiple preloaded detectors and multiple items.

Inspector

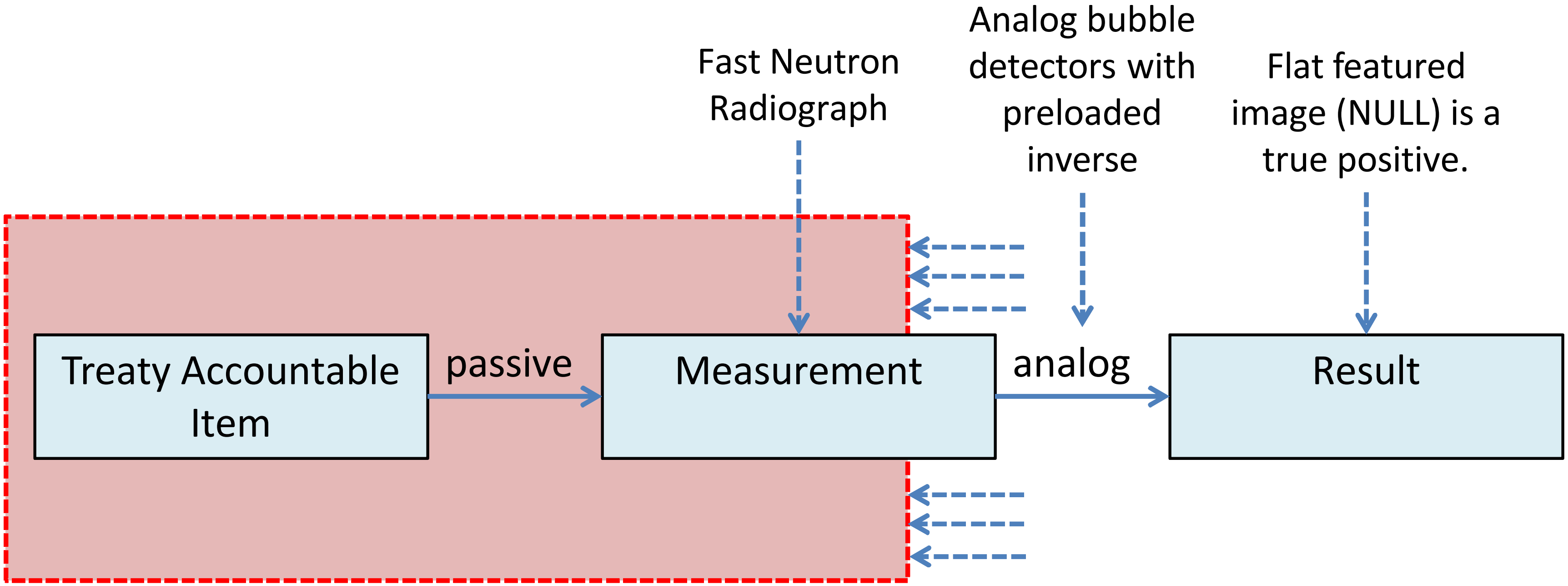
- Pairs detectors to items ensuring all are identical (statistically over time).
- If measurement took place ***and*** the pre-confirmed standard object was present, then I've gained something.



ZKP – authentication measures

Research Questions

- Is there some way to watch the measurement?
- Do we need a preloaded instrument?
- Can an inspector provide a true negative to be measured?


Fast Neutron Radiograph
Analog bubble detectors with preloaded inverse
Flat featured image (NULL) is a true positive.
Treaty Accountable Item
passive
Measurement
analog
Result