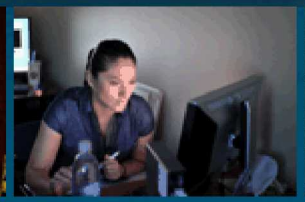
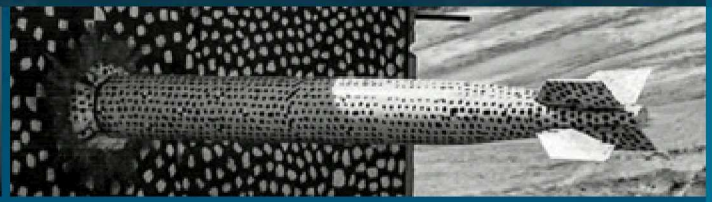
CoCIM Data Authentication





PRESENTED BY

Jay Brotz

SAND2019-6128PE

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Secure Sensor Protocol

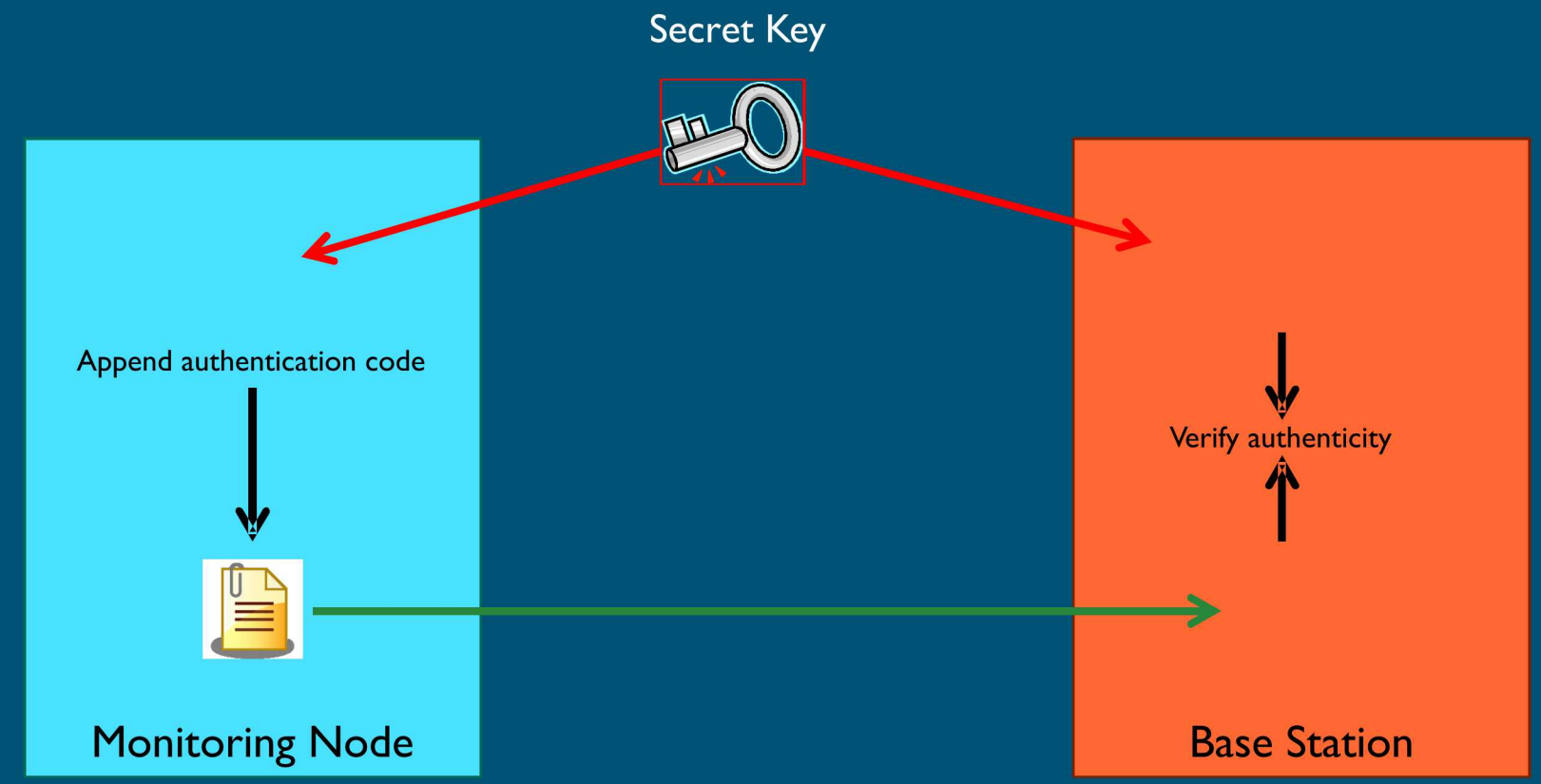
SSP is the base for many potential active monitoring nodes

- Chain of Custody Item Monitor (CoCIM)
- Door Switch
- Motion Detector
- Camera

Trust principles:

- All data is digitally signed at the source
- All data includes an incrementing message counter
- The node is within a tamper indicating enclosure that destroys the private key upon tamper detection

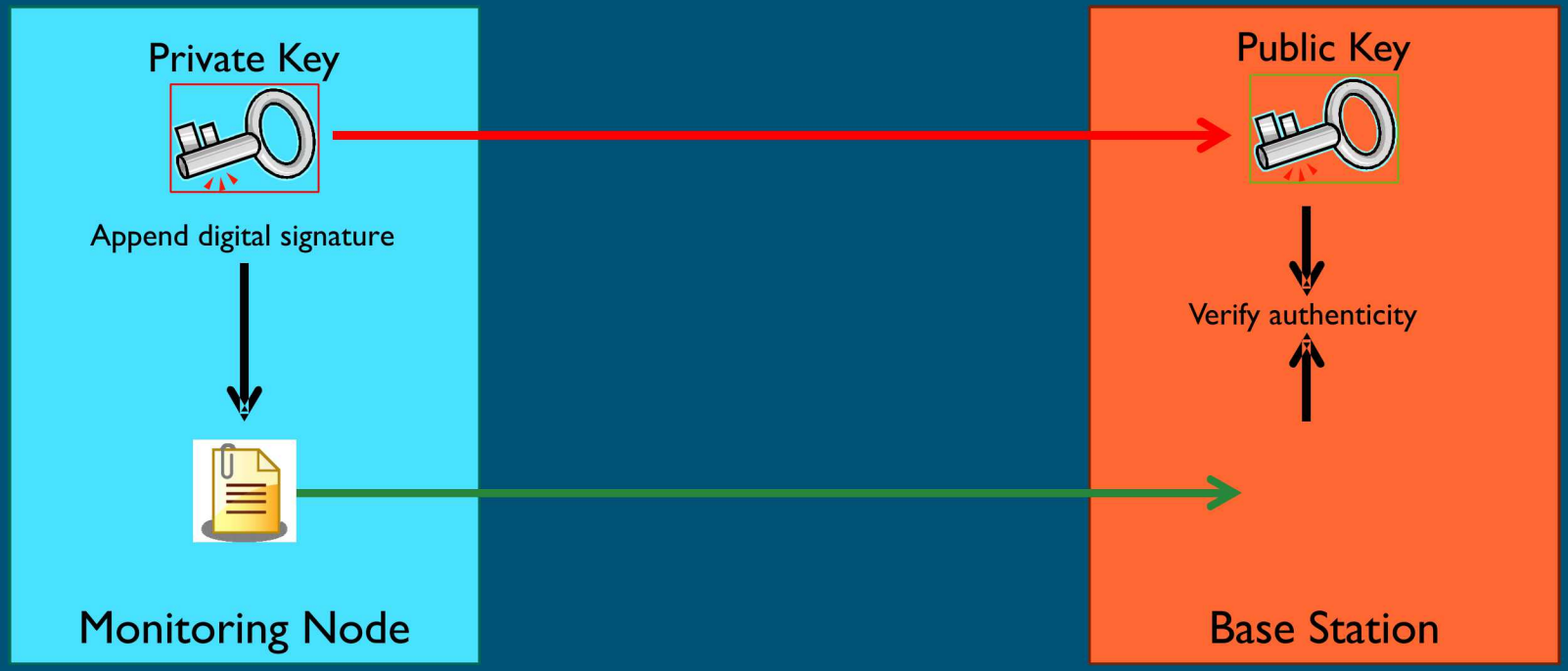
Symmetric Key Authentication



Trusted Channel

Untrusted Channel

Public Key Authentication



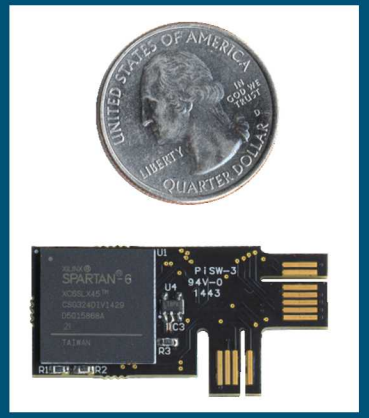
Trusted Channel

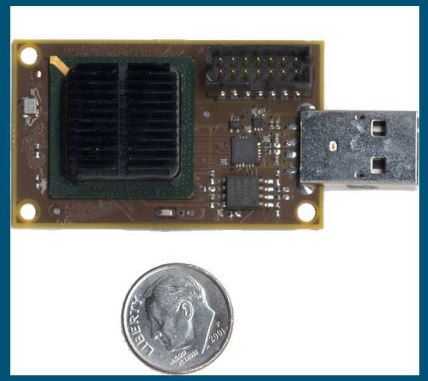
Untrusted Channel

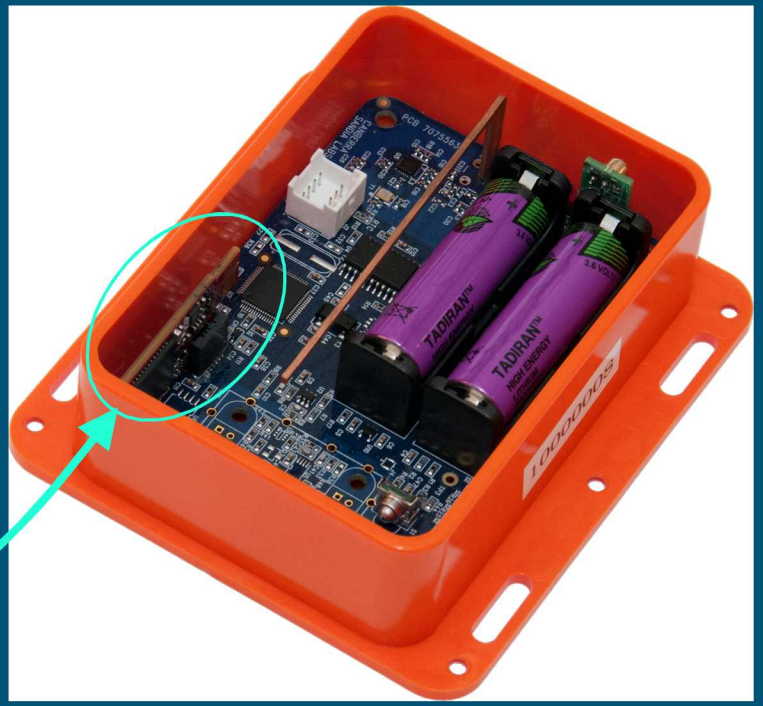
Node Cryptography

A public/private key pair and digital signatures are created with Digital Signature Algorithm (DSA)

- DSA is computationally intensive, but Elliptic Curve DSA (ECDSA) is better
- We have used open source libraries for ECDSA computation in software
- We have developed our own low-power and fast ECDSA processor on an FPGA







Hardware Discussion