A Taxonomy of Operational Security Issues for Manufacturer installed Keys and Trust Anchors

draft-richardson-t2trg-idevid-considerations

2020-10-21 slides v5.0

Michael Richardson <mcr+ietf@sandelman.ca>

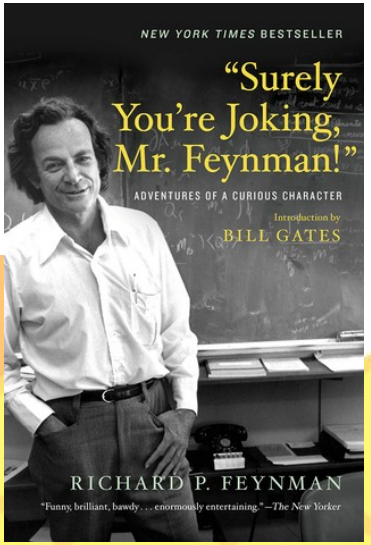
https://www.sandelman.ca/SSW/talks/idevid-considerations/

“It’s turtles all the way down”

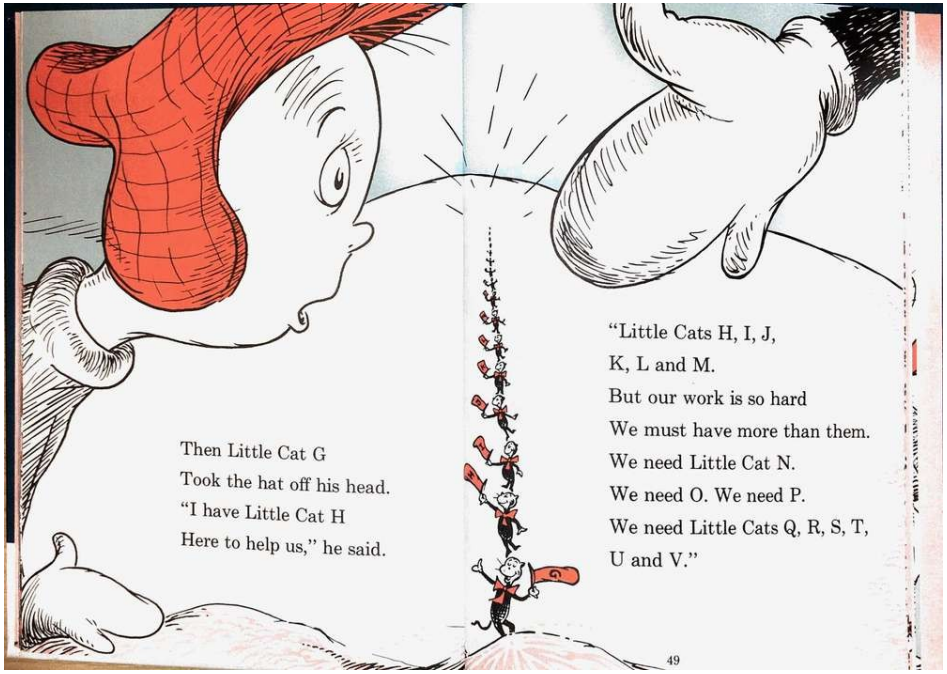
- I first heard this in [Surely You’re Joking Mr. Feynmann]

"The world, marm," said I, anxious to display my acquired knowledge, "is not exactly round, but resembles in shape a flattened orange; and it turns on its axis once in twenty-four hours."
"Well, I don't know anything about its axes," replied she, "but I know it don't turn round, for if it did we'd be all tumbled off; and as to its being round, any one can see it's a square piece of ground, standing on a rock!"
"Standing on a rock! but upon what does that stand?"
"Why, on another, to be sure!"
"But what supports the last?"
"Lud! child, how stupid you are! There's rocks all the way down!"[1]

1838 New York Mirror. https://en.wikipedia.org/wiki/Turtles_all_the_way_down



The Return of the Cat in The Hat



Yertle the Turtle

About those Turtles

1) Provisioning Identities (Roots of Trust)
2) Manufacturer installed Trust Anchors
3) Structures for Key Infrastructure(s)
4) Discussion

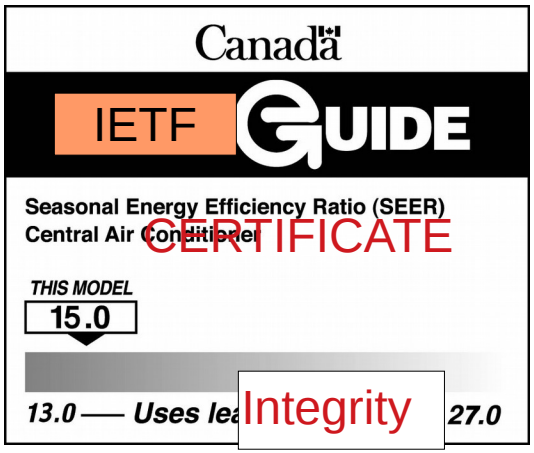
Non-Goals of the document

1) Not aiming to write an ISO27001-ish evaluation process.

2) Not going to make any recommendation as to an appropriate solution for a given risk situation.

Goals of this document

- Enumerate the reasonable, and maybe some less reasonable ways to provision and secure keys, and give them **names**.
- Not just the most secure way, because it is not always worth it.

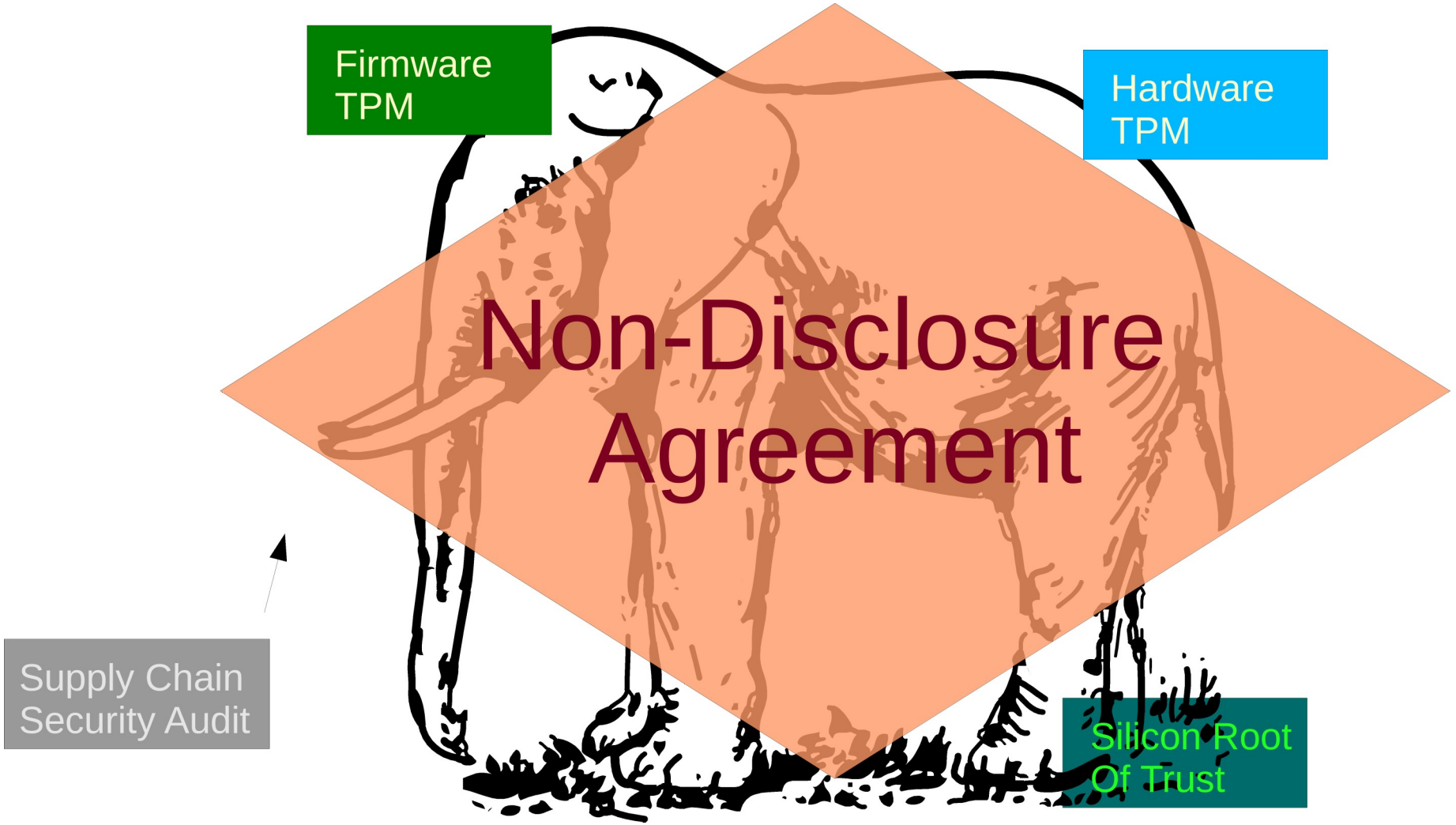


admin:password

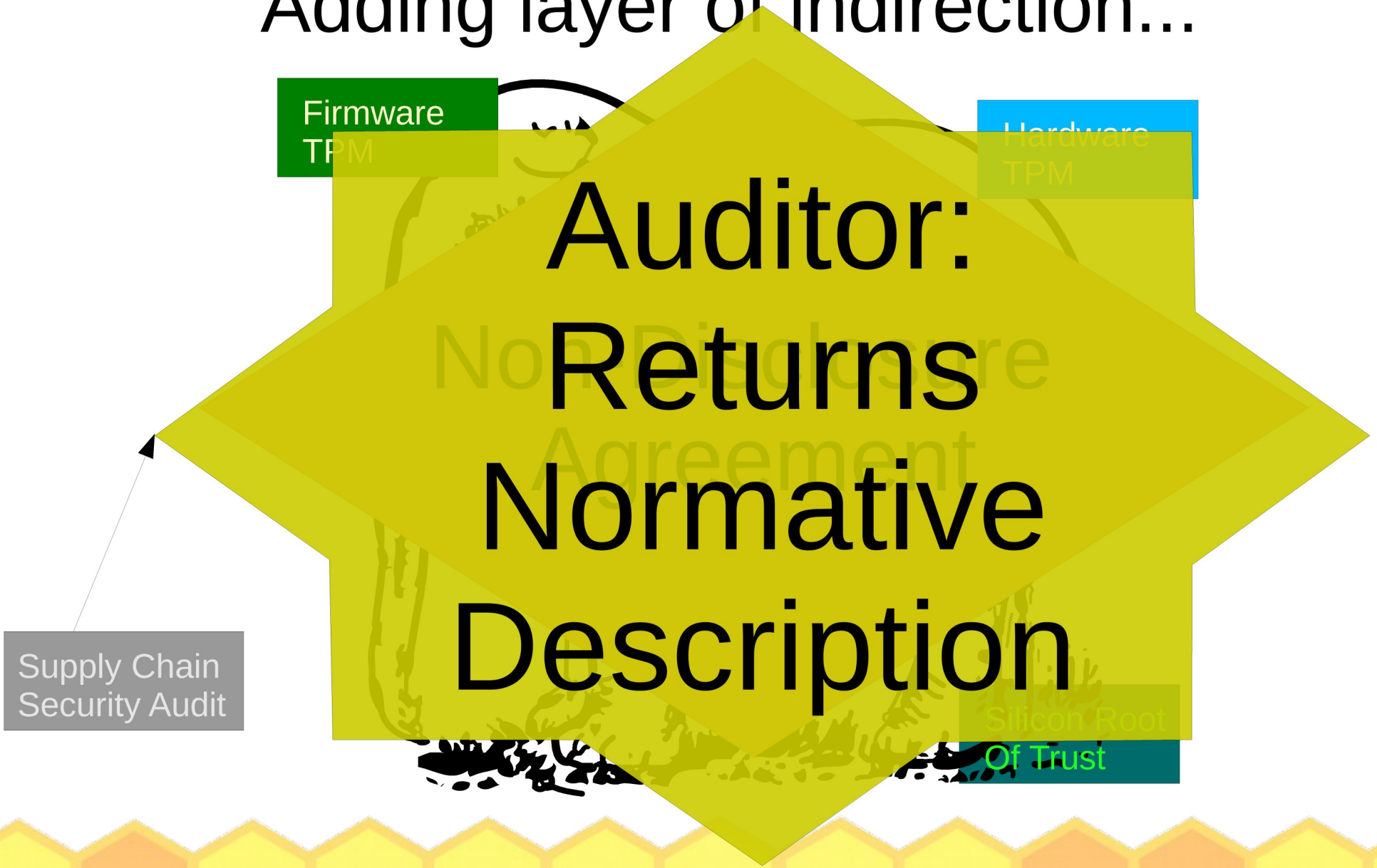
Roots of Trust

- How are they provisioned?
  - What would be involved in compromising that process?
    - assume: bribery, kidnapping, might be used
  - How can we qualify the different processes?
    - Not every process is appropriate for every end use.
- NDAs abound, but Supply Chain considerations mean some of these things need to get through anyway

Confidentiality of IDevID private key..



Adding layer of indirection...



Provisioning Identities

- Password generated by factory, installed by JTAG
- Password generated locally, retrieved by JTAG
- Password generated, uploaded by secure HTTPS
- Password co-generated from silicon provisioned secret
  - Physically Unclonnable Function (PUF), Silicon Root of Trust, Intel SDO, ARM Pelion

“infrastructure-generated-identity-mechanically-installed”

“device-generated-identity-mechanically-retrieved”

“device-generated-identity-network-retrieved”

“device-factory-co-generated-identity”

from Laurence Lundblade slides
from Feb SUIT/RATS/TEEP hackathon

Factory Generated Private Keys

Certificate installed by JTAG

```
if(first_boot) {
  * read certificate from ROM *
}
```

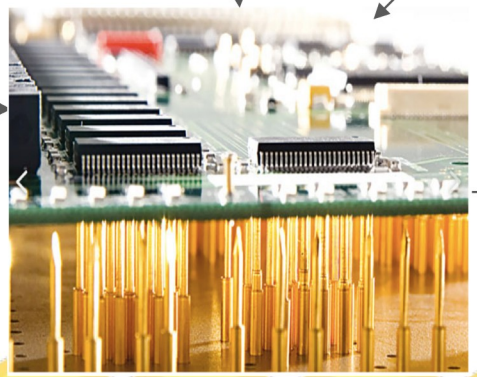
Code compiled to Golden image

Generate keypair, Sign Certificate

Initial environment settings

Also macaddr, serialno

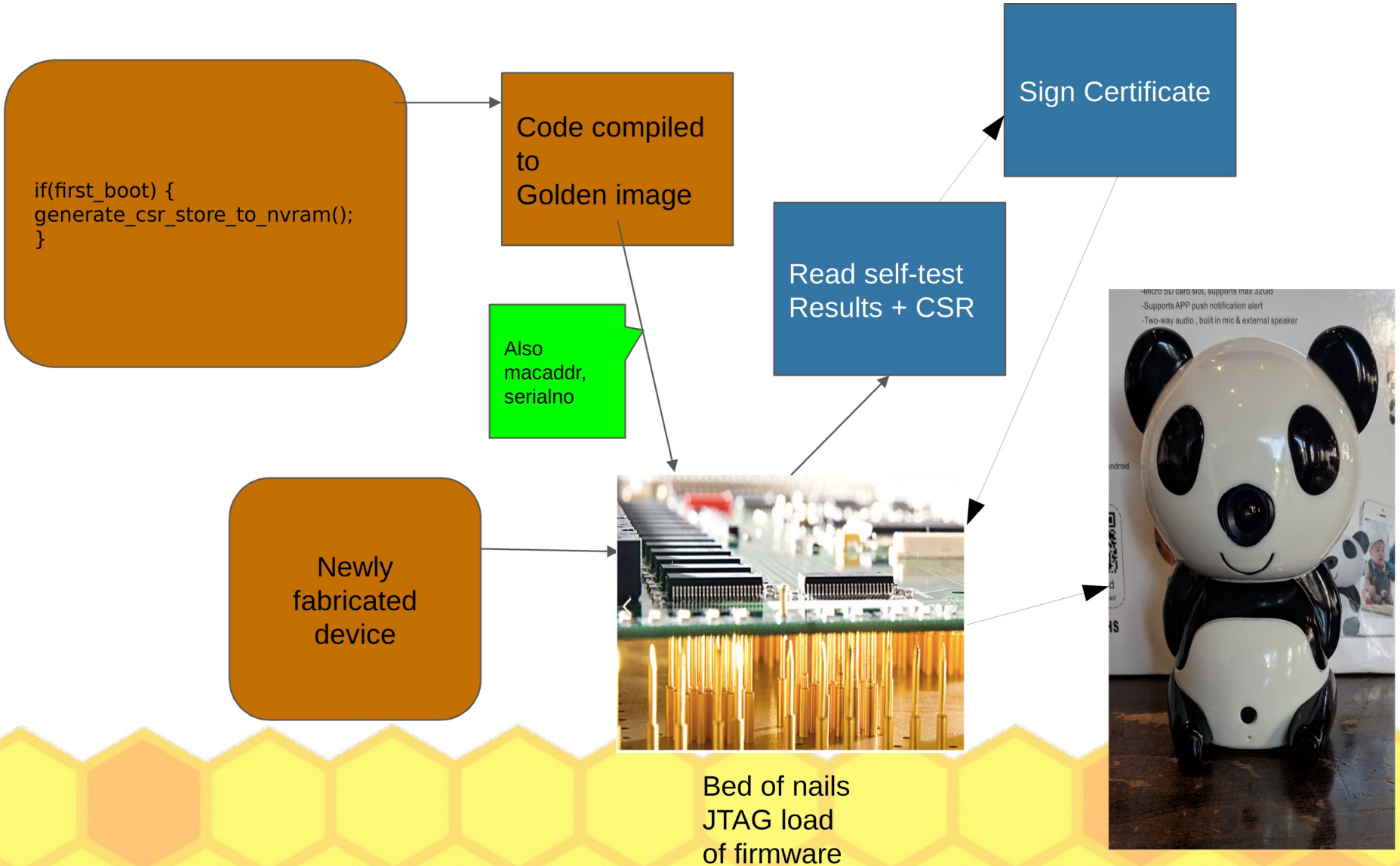
Newly fabricated device



Bed of nails JTAG load of firmware

Device generated keys

Private key generated locally, retrieved by JTAG



Device generated CSR, network provisioning

Device generated, uploaded by secure HTTPS

```
if(first_boot) {
Csr = generate_csr();
https_post(“https://
factory.local/”);
}
```

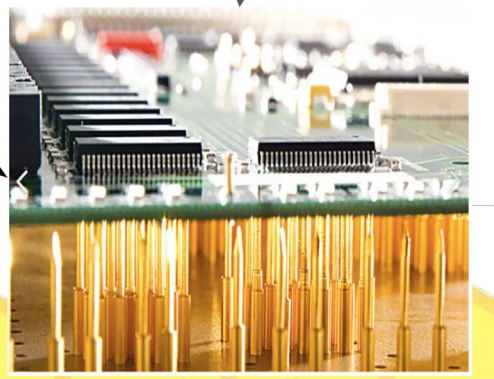
Code compiled to Golden image

Certificate Signing

Factory web service

POST

Newly fabricated device

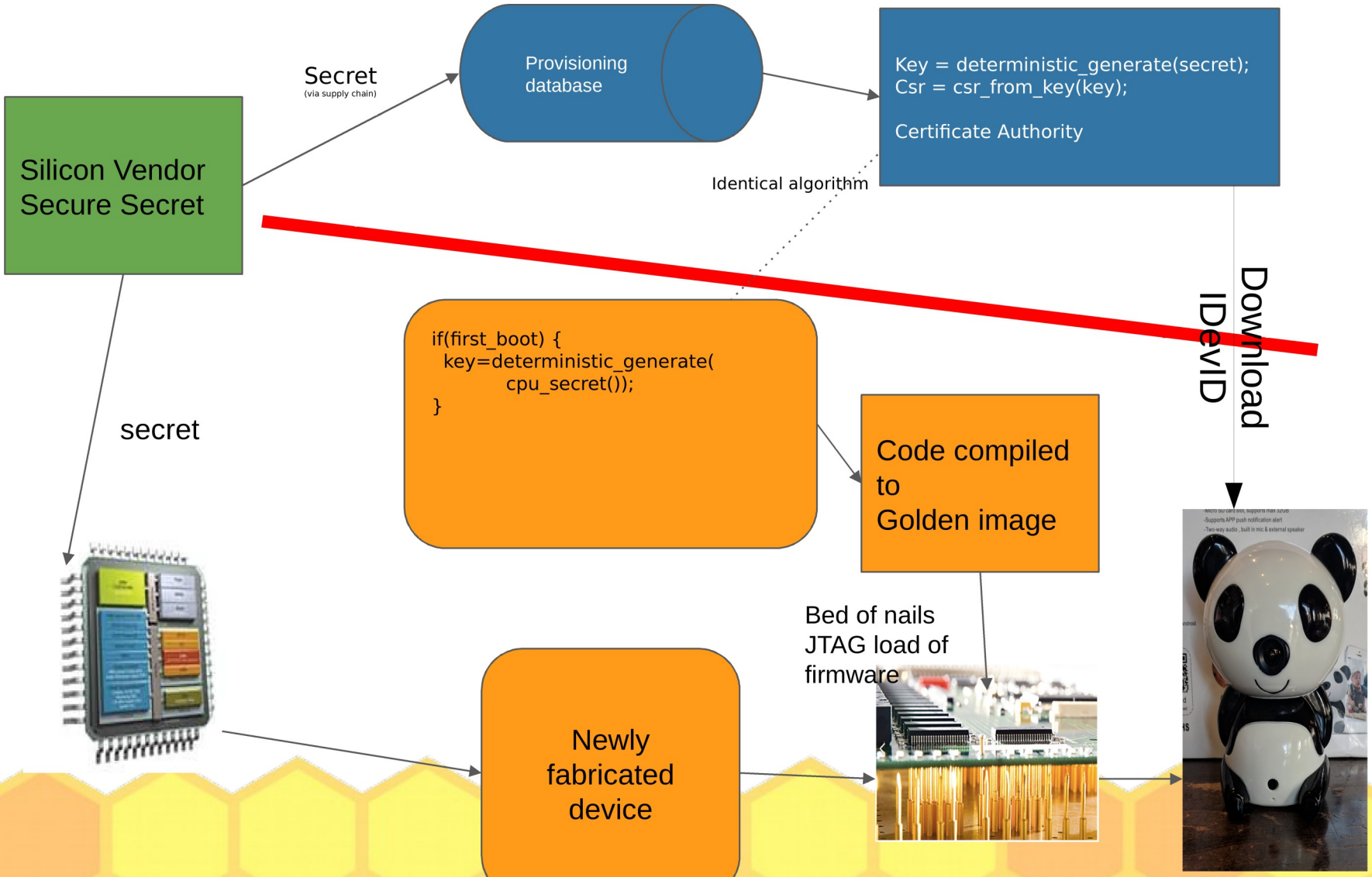


Bed of nails JTAG load of firmware

Also macaddr, serialno

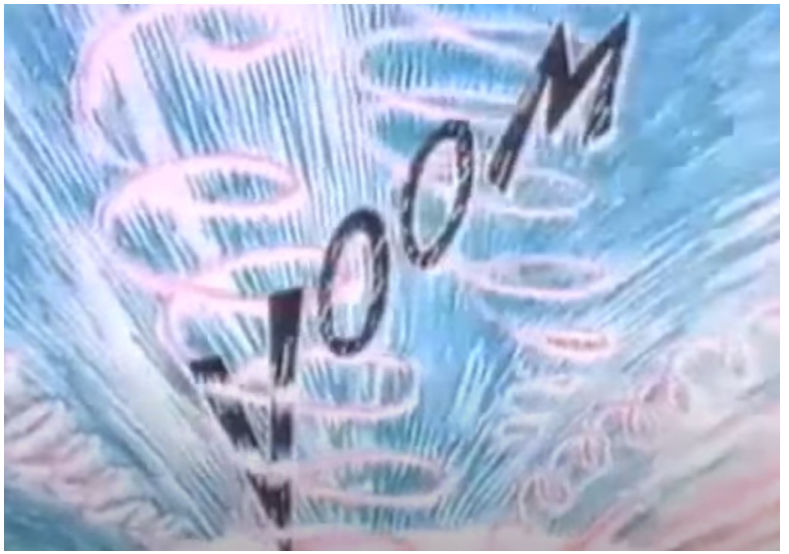
reply

Leveraging CPU provisioned secrets: Password co-generated from silicon provisioned secret



This has been about the VOOM

- “Three” ways to generate certificate that matches private key
  - Device-generated
  - Factory generated
  - Co-generated from smaller Turtle



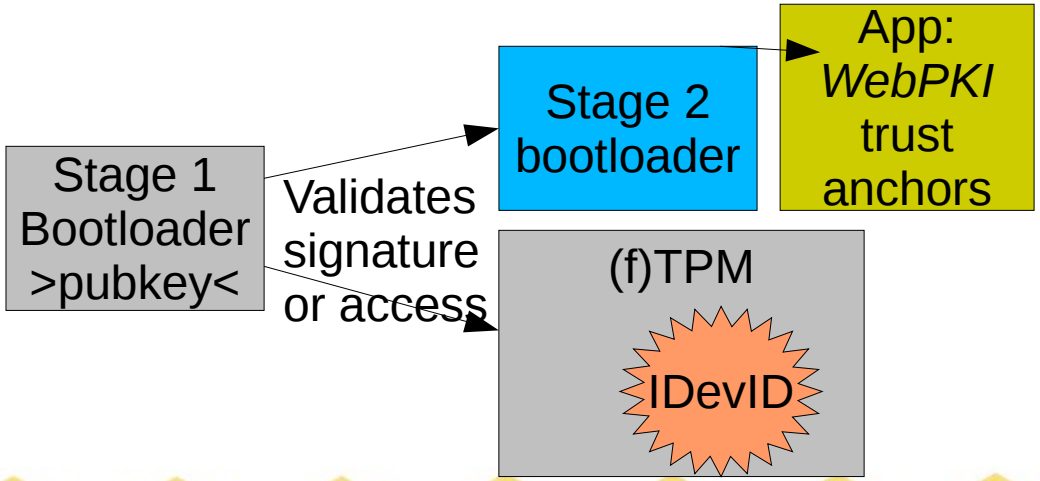
What about Trust Anchors?

- In the device: Software Update anchor
- In the device: TLS anchors for Cloud Things
- In the device: Debug Enable
- In the device: Owner Identity

Audit Model

Recognize:

Posessor of Bootloader software update key wins all battles.



- However >pubkey< is provisioned determines in-system risk of entire system.
  - This is the bottom turtle, “Mack”, and he’d better not burp.
- **Even more critical: how is the private key that can sign code kept?**

Public Key Infrastructure(s)

1) IDevID structure
   a) root/HSM?
   b) Intermediate CAs?
   c) How is factory connected?
2) Software Signing Key
   a) Same root? Different?
   b) Any Intermediate CAs?
   c) R&D signing, QA signing?
      How many secret splits?

Discussion