Social and Technical metrics for Trust Anchor resilence

or: measuring the Trust in your Trust Anchors

Michael Richardson
<mcr@sandelman.ca>

https://www.sandelman.ca/SSW/talk/2022-iotsf-anchor-reputations/

“The future is already here — it's just not very evenly distributed.”

Usually attributed to William Gibson

Outline of the Talk

Outline of the Talk

Tell you who I am
Tell you why I am here
Tell you about the problem

Outline of the Talk

Tell you who I am
Tell you why I am here
Tell you about the problem

Tell you about the challenges
Tell you about what I propose

Outline of the Talk

Tell you who I am
Tell you why I am here
Tell you about the problem

Tell you about the challenges
Tell you about what I propose

Show you some of the results so far, giving examples

Outline of the Talk

Tell you who I am
Tell you why I am here
Tell you about the problem

The part where you tell me which part I did wrong, and how you have a better idea

he results so far, giving examples

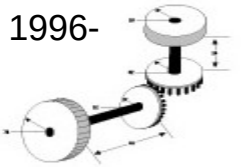
Who am I?

Xelerance Corp 2003-2007,2014-2018

Internet technologist, doing IP since 1988. “Garage Entrepreneur”

SOLIDUM (1998-2001)

SANDELMAN SOFTWARE WORKS 1996-



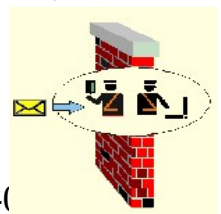
SIMtone CORPORATION (2007-2009)

CREDIL CENTRE DE RECHERCHE ET DÉVELOPPEMENT EXPÉRIMENTAL EN INFORMATIQUE LIBRE / CENTRE FOR RESEARCH AND EXPERIMENTAL DEVELOPMENT IN INFORMATICS LIBRE 2009-

RFC8995 BRSKI RFC8366

FreeS/WAN (2001-2004)

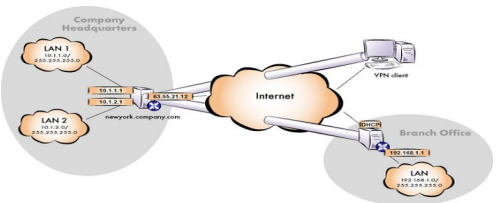
#4 at Milkyway Networks (1994)



ROLL – RFC6550 2012-

RFC4322
RFC4025
RFC5386
RFC8415
RFC7416
RFC8366
RFC8995(BRSKI)
constrained-BRSKI

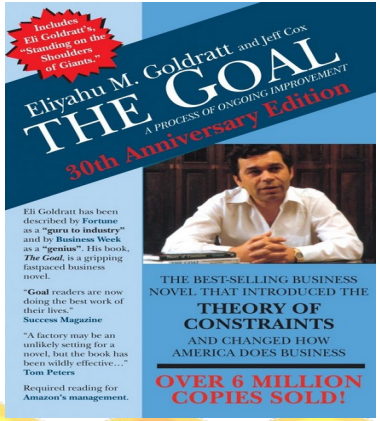
20+ RFCs



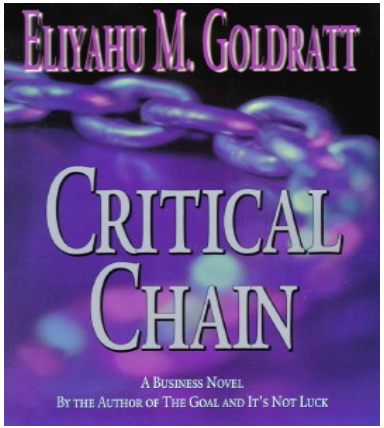
IETF standard security:IPsec/VPN

Metrics come before evaluation

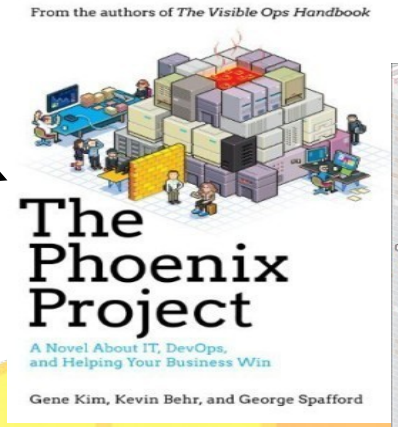
“Tell me how you will measure me, and then I will tell you how I will behave. ...” – Eli Goldratt



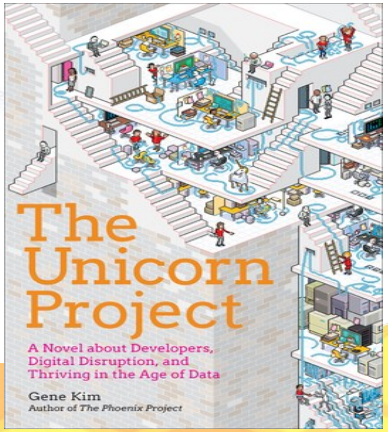
1980s



2000s



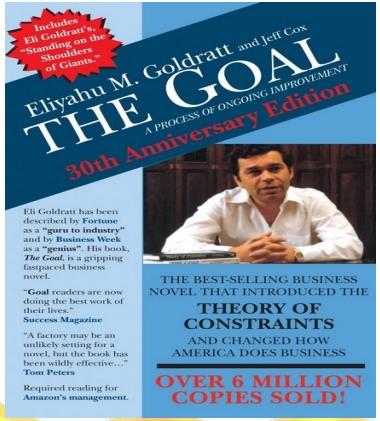
2013



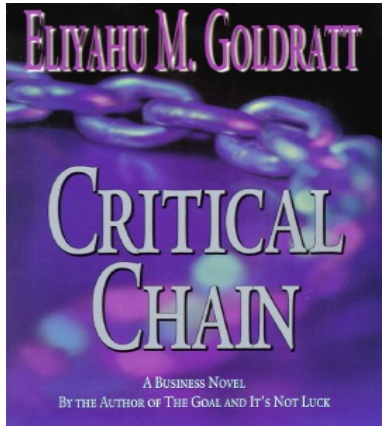
2019

Metrics come before evaluation

“Tell me how you will measure me, and then I will tell you how I will behave. ...” – Eli Goldratt



1980s



2000s

BUT, I’m here to talk about my document.
It needs your feedback.

It’s at
https://datatracker.ietf.org/doc/draft-richardson-t2trg-idevid-considerations/

It’s called

A Taxonomy of operational security considerations for manufacturer installed keys and Trust Anchors

IoTSP / Sandelman

2019

Metrics come before evaluation

“Tell me how you will measure me, and then I will tell you how I will behave. ...” – Eli Goldratt

BUT, I’m here to talk about my document.
It needs your feedback.

It’s at
https://datatracker.ietf.org/doc/draft-richardson-t2trg-idevid-considerations/

It’s called

A Taxonomy of operational security considerations for manufacturer installed keys and Trust Anchors

IoTSP / Sandelman

Metrics c

“Tell me how you will mea… will behave. ...” – Eli Goldratt

Workgroup: T2TRG Research Group
Internet-Draft: draft-richardson-t2trg-idevid-considerations-07
Published: 16 August 2022
Intended Status: Informational
Expires: 17 February 2023
Author: M. Richardson
Sandelman Software Works

A Taxonomy of operational security considerations for manufacturer installed keys and Trust Anchors

Abstract

This document provides a taxonomy of methods used by manufacturers of silicon and devices to secure private keys and public trust anchors. This deals with two related activities: how trust anchors and private keys are installed into devices during manufacturing, and how the related manufacturer held private keys are secured against disclosure.

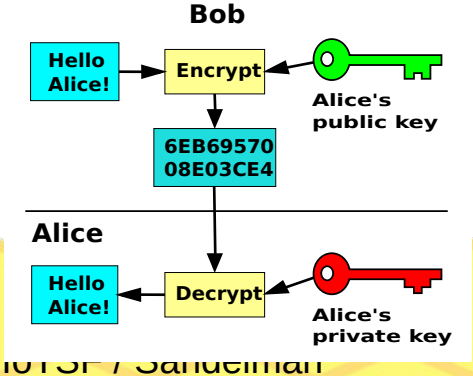
It’s at
https://datatracker.ietf.org/doc/draft-richardson-t2trg-idevid-considerations/

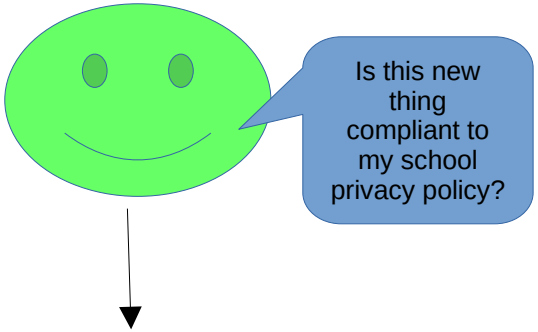
It’s called

A Taxonomy of operational security considerations for manufacturer installed keys and Trust Anchors

IoTSF / Sandelman

Cryptography!

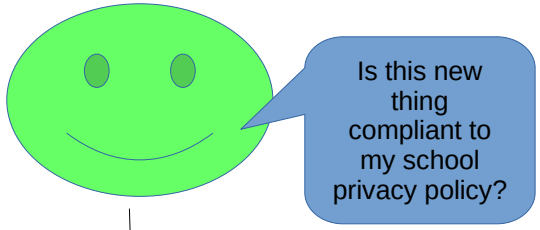




Chains of suppliers (Non-transitive Trust)

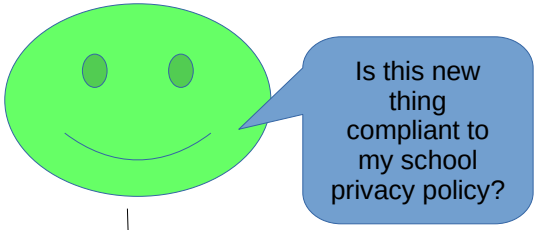
New Killer-App IoT Device

Chains of suppliers (Non-transitive Trust)



New Killer-App IoT Device

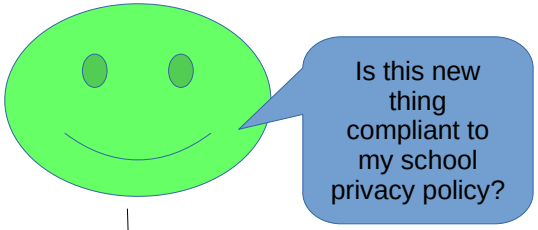
Chains of suppliers (Non-transitive Trust)



New Killer-App IoT Device

- Refrigerant MCU Coolant leaks?
- Arms Flaying wildly
- Walking Legs Internal GPS?
- facial recognition (customer recog)
- Credit Card processor

Chains of suppliers (Non-transitive Trust)

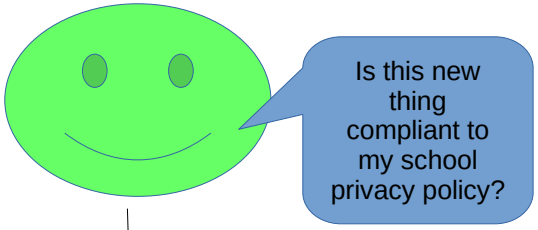


New Killer-App IoT Device

- Refrigerant MCU Coolant leaks?
- Arms Flaying wildly
- Walking Legs Internal GPS?
- facial recognition (customer recog)
- Credit Card processor

- Trust Anchor for SUIT
- No Leak Remote Attestation Key

Chains of suppliers (Non-transitive Trust)



New Killer-App IoT Device

Refrigerant MCU Coolant leaks?

Arms Flaying wildly

Walking Legs Internal GPS?

facial recognition (customer recog)

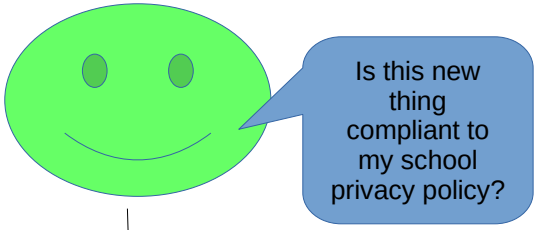
Credit Card processor

Trust Anchor for SUIT

No Leak Remote Attestation Key

Confidential Computing for Face ML engine

Chains of suppliers (Non-transitive Trust)



New Killer-App IoT Device

Refrigerant MCU Coolant leaks?

Arms Flaying wildly

Walking Legs Internal GPS?

facial recognition (customer recog)

Credit Card processor

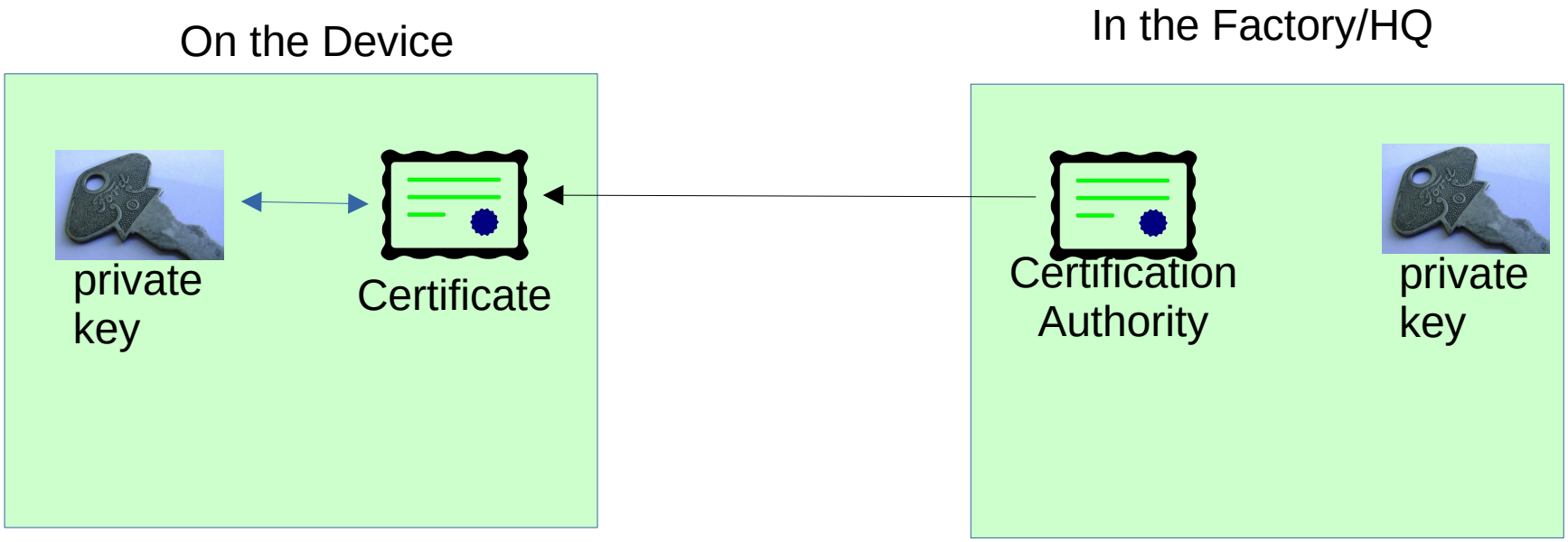
Trust Anchor for SUIT

No Leak Remote Attestation Key

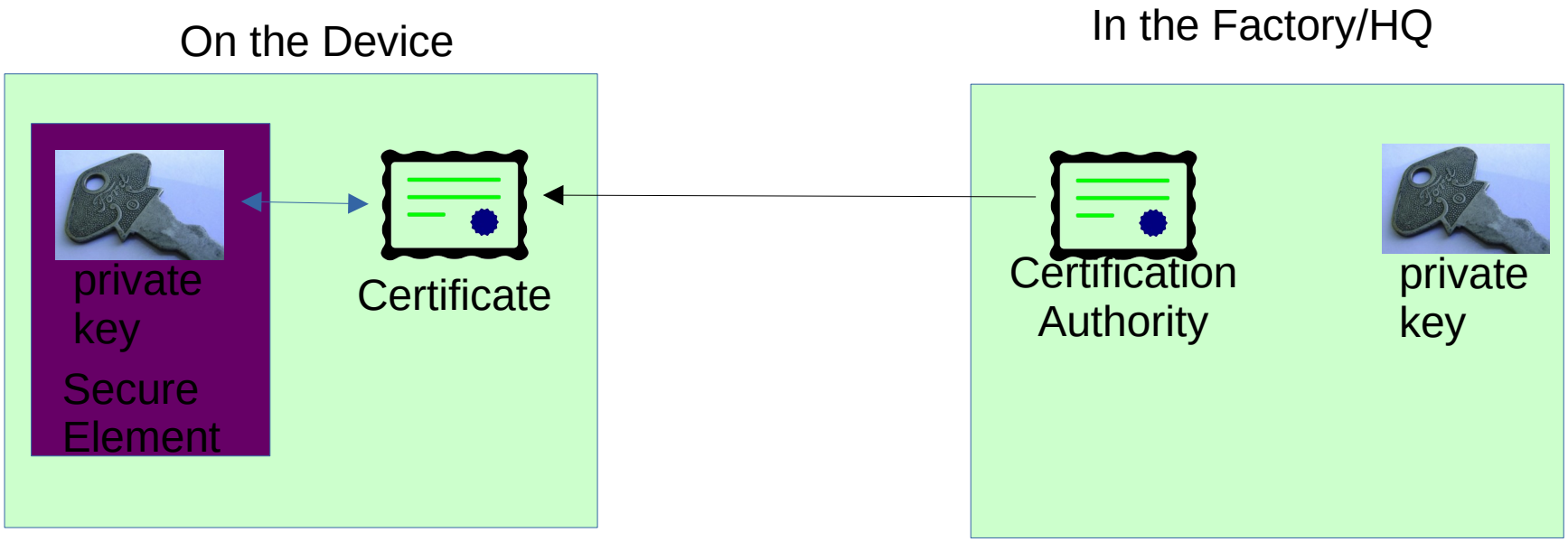
How can happy guy know how this key was created?

Confident… for Face ML engine

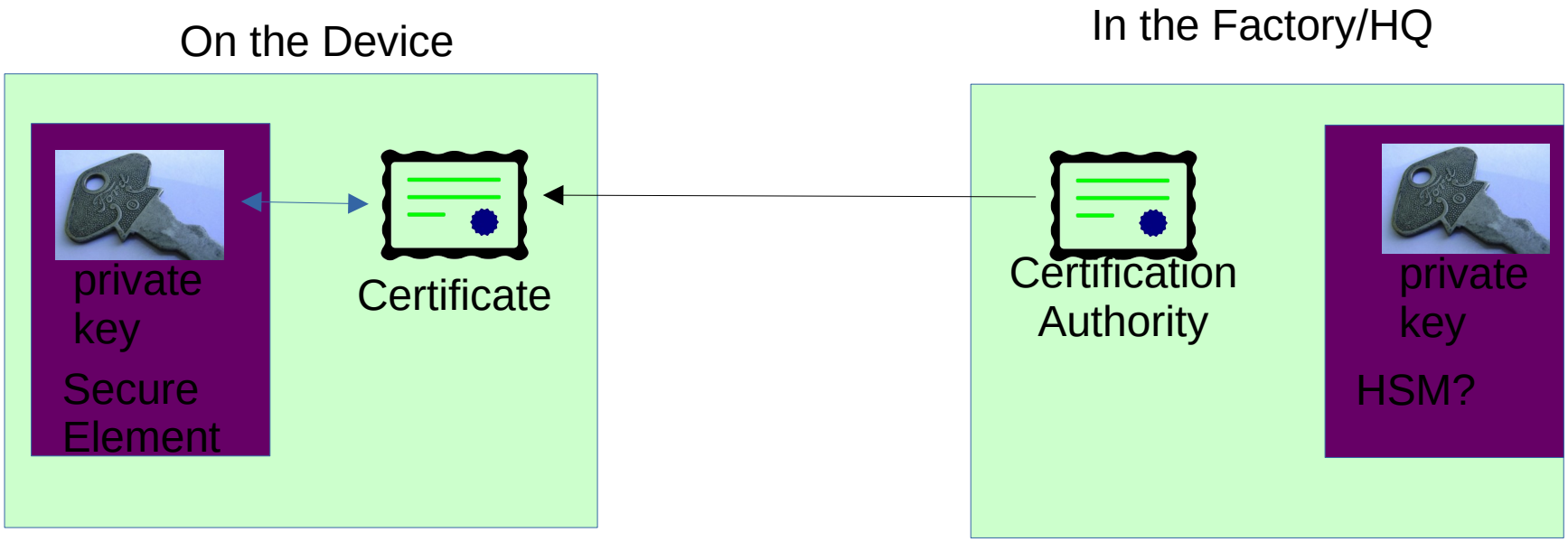
A simple setup, some simple symbols



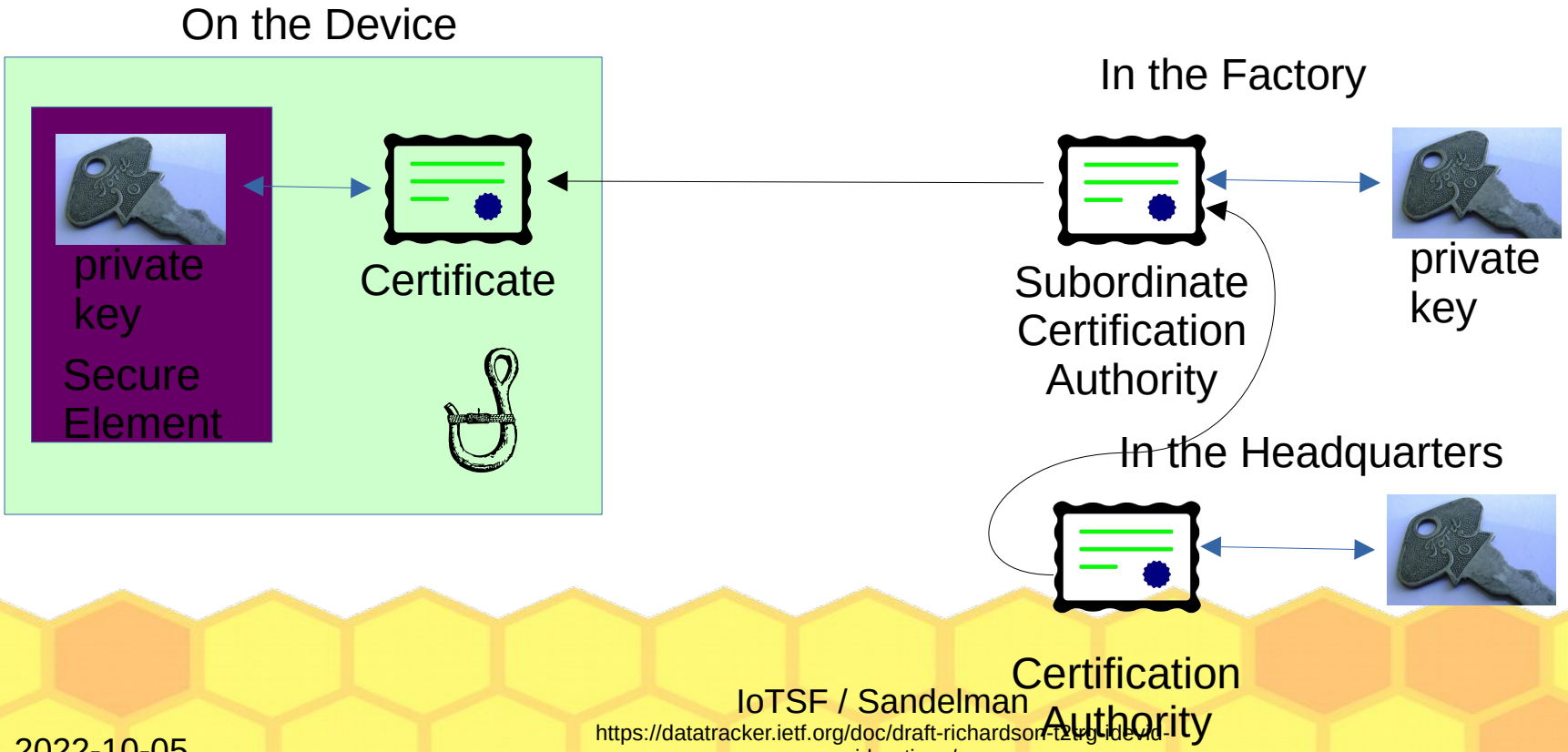
A simple setup, some simple symbols



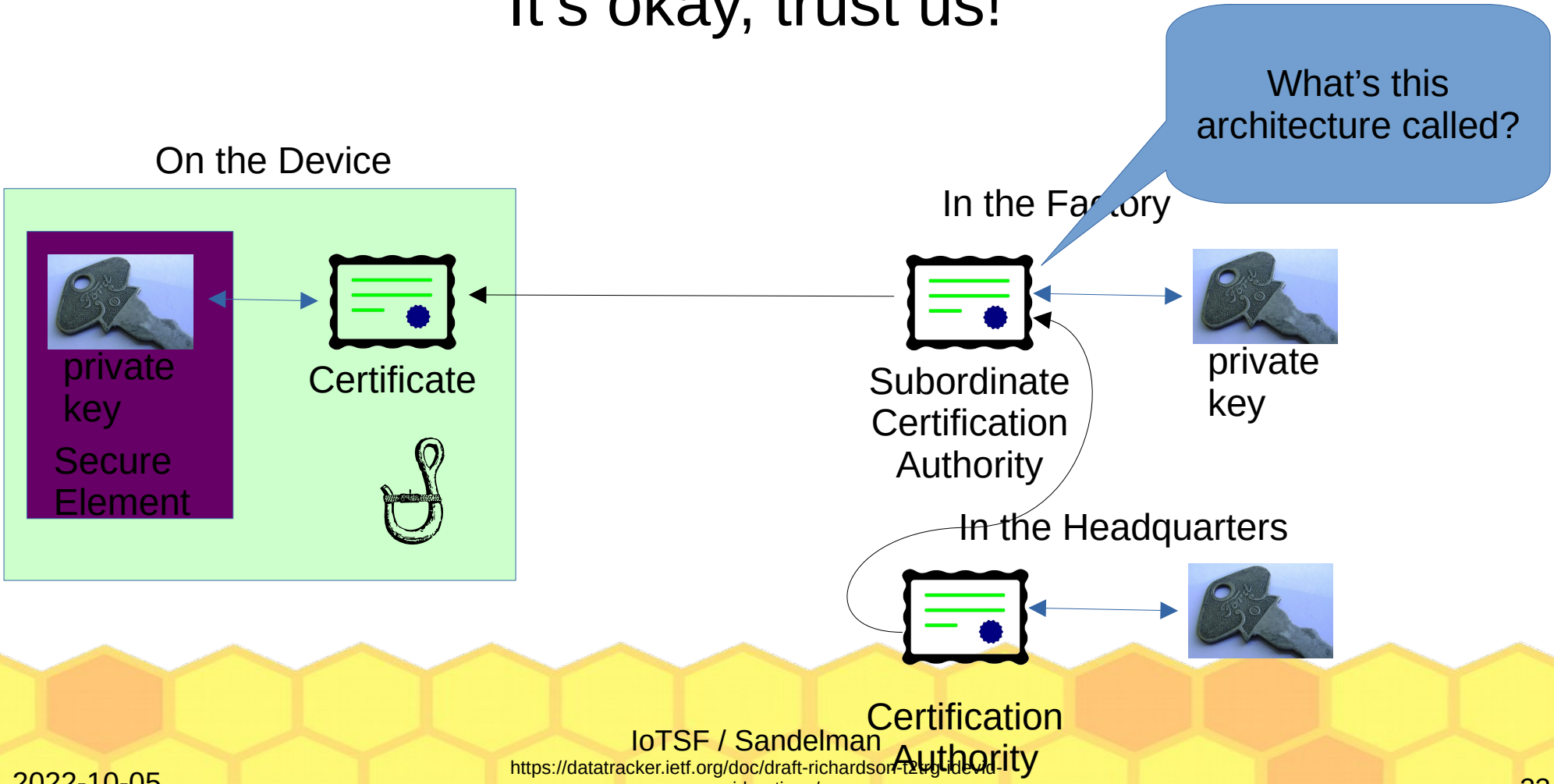
A simple setup, some simple symbols



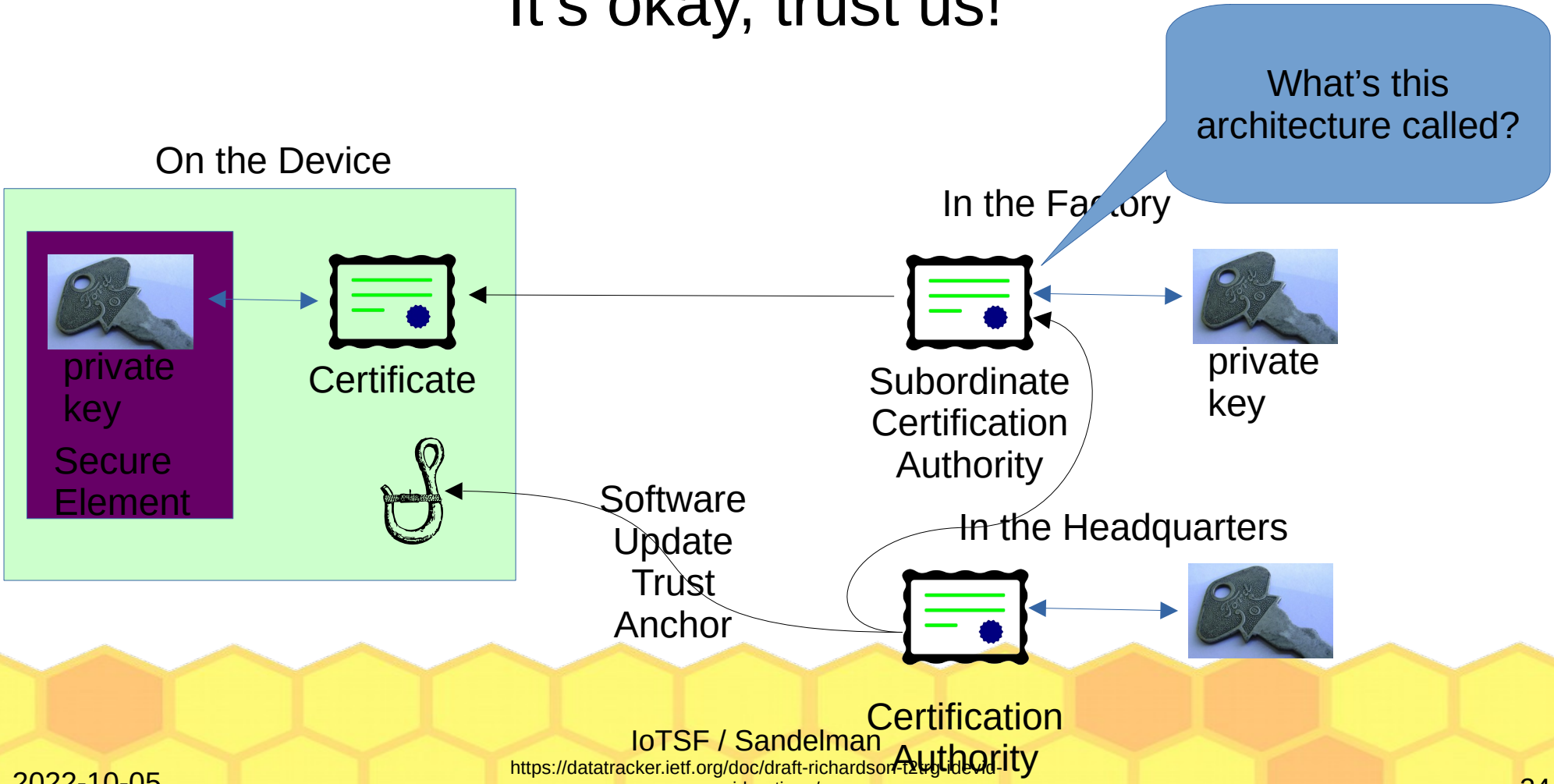
It’s okay, trust us!



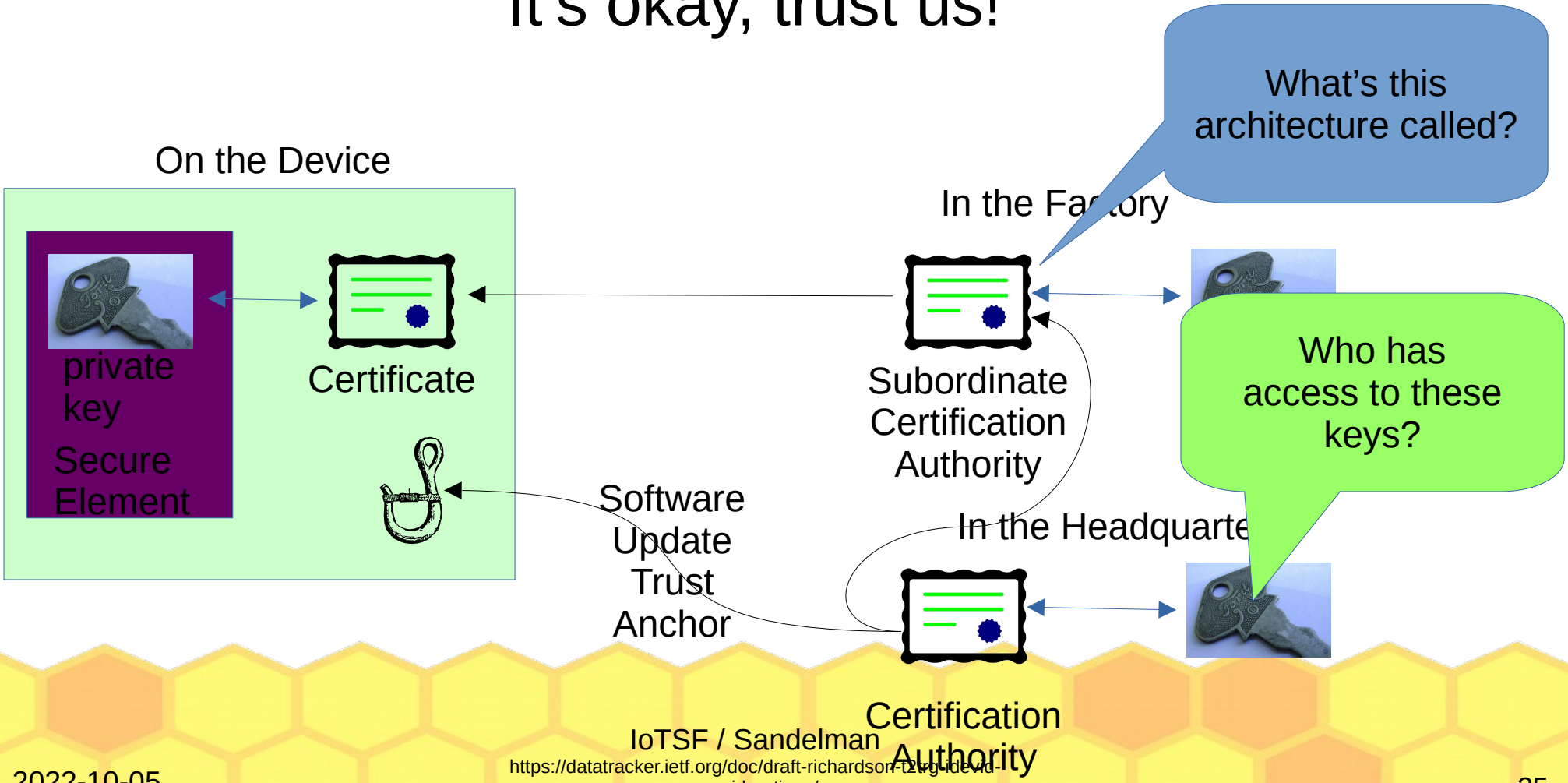
It’s okay, trust us!



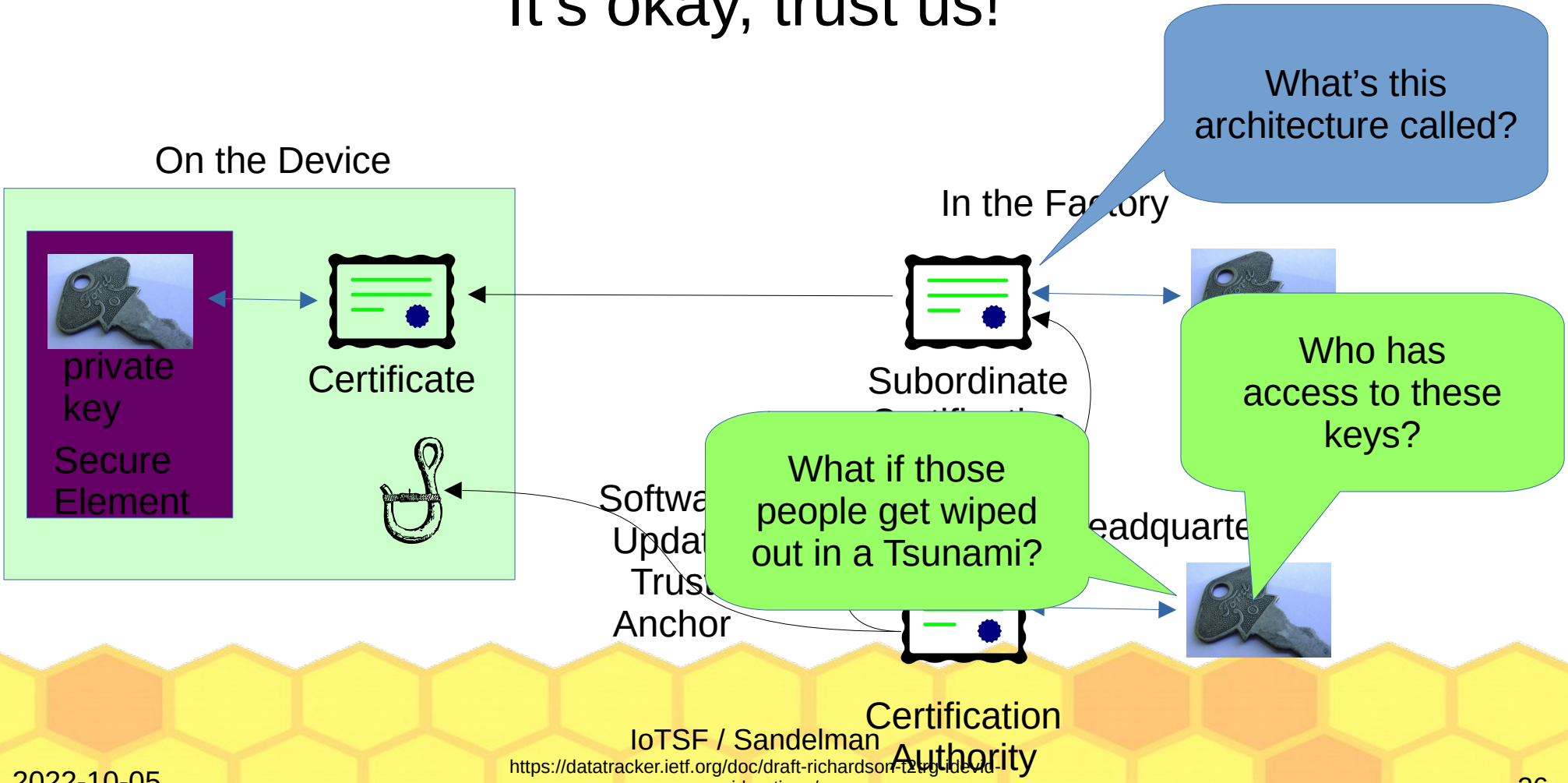
It’s okay, trust us!



It’s okay, trust us!



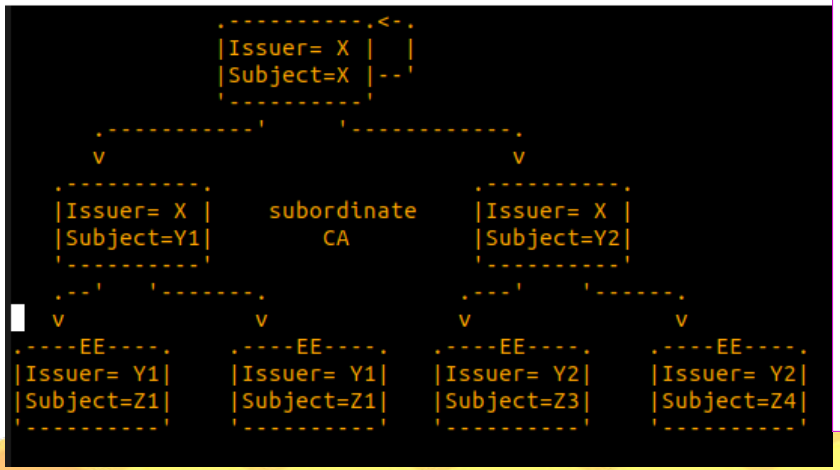
It’s okay, trust us!



Challenges of doing measurements/evaluation: paranoia leads to secrecy

Taxonomy: Public Key Infrastructure Depth

- self-signed certificate is a PKI of level “one”
  - **not** counting from zero
-



6.2. Integrity and Privacy of device identify infrastructure

For IDevID provisioning, which includes a private key and matching certificate installed into the device, the associated public key infrastructure that anchors this identity must be maintained by the manufacturer.

identity-pki-level: how deep are the IDevID certificates that are issued?

identity-time-limits-per-subordinate: how long is each subordinate CA maintained before a new subordinate CA key is generated? There may be no time limit, only a device count limit.

identity-number-per-subordinate: how many identities are signed by a particular subordinate CA before it is retired? There may be no numeric limit, only a time limit.

identity-anchor-storage: how is the root CA key stored? How many people are needed to recover the private key?

6.3. Integrity and Privacy of included trust anchors

For each trust anchor (public key) stored in the device, there will be an associated PKI. For each of those PKI the following questions need to be answered.

pki-level: how deep is the EE that will be evaluated (the trust root is at level 1)

Taxonomy: Key Generation Process

- where/how is the device key generated
  - internal?
  - external/factory?
  - CPU provisioned seed?
  - threashold methods?
-

4.1.2. Key Generation process

4.1.2.1. On-device private key generation

Generating the key on-device has the advantage that the private key never leaves the device. The disadvantage is that the device may not have a verified random number generator. [factoringrsa] is an example of a successful attack on this scenario.

4.1.2.2. Off-device private key generation

Generating the key off-device has the advantage that the randomness of the private key can be better analyzed. As the private key is available to the manufacturing infrastructure, the authenticity of the public key is well known ahead of time.

If the device does not come with a serial number in silicon, then one should be assigned and placed into a

4.1.2.3. Key setup based on 256 bit secret seed

A hybrid of the previous two methods leverages a symmetric key that is often provided by a silicon vendor to OEM manufacturers.

Each CPU (or a Trusted Execution Environment [I-D.ietf-teep-architecture], or a TPM) is provisioned at fabrication time with a unique, secret seed, usually at least 256 bits in size.

This value is revealed to the OEM board manufacturer only via a secure channel. Upon first boot, the system (probably within a TEE, or within a TPM) will generate a key pair using the seed to initialize a Pseudo-Random-Number-Generator (PRNG). The OEM, in a separate system, will initialize the same PRNG and generate the same key pair. The OEM then derives the public key part, signs it and turns it into a certificate. The private part is then destroyed, ideally never stored or seen by anyone. The certificate (being public information) is placed into a database, in some cases it is loaded by the device as its IDevID certificate, in other cases, it is retrieved

lacks good name

Taxonomy:
Private Key access / Business Continuity

- who/how many has access to/control over the private key?
  - how many people need to be threatened/blackmailed?
- what can the auditor say/reveal?
- how is the private key backed up, and how does business continuity work?
  - tsumani destroy keys, probably more often than black hats

5.3. Preservation of CA and Trust Anchor private keys

A public key (or certificate) is installed into target device(s) as a trust anchor. Is it there in order to verify further artifacts, and it represents a significant investment. Trust anchors must not be easily replaced by attackers, and securing the trust anchor against such tampering may involve burning the trust anchor in unchangeable fuses inside a CPU.

Replacement of the anchor can involve a physical recall of every single device. It therefore important tha trust anchor is useable for the entire lifetime of every single one of the devices.

The previous section deals with attacks against the infrastructure: the attacker wants to get access to the private key material, or to convince the infrastructure to use the private key material to their bidding. Su event, if undetected would be catastrosphic. But, when detected, would render almost every device usele potentially dangerous) until the anchor could be replaced.

Intended vs Unintended Business Continuity

- Use Shamir Secret Sharing on PKI keys
  - 4 out of 7 pieces
    - generallly n of k
- how to distribute pieces?
- do they reconstruct the PKI private key,
  - or do they just restruct the HSM secret that unlocks the private key?

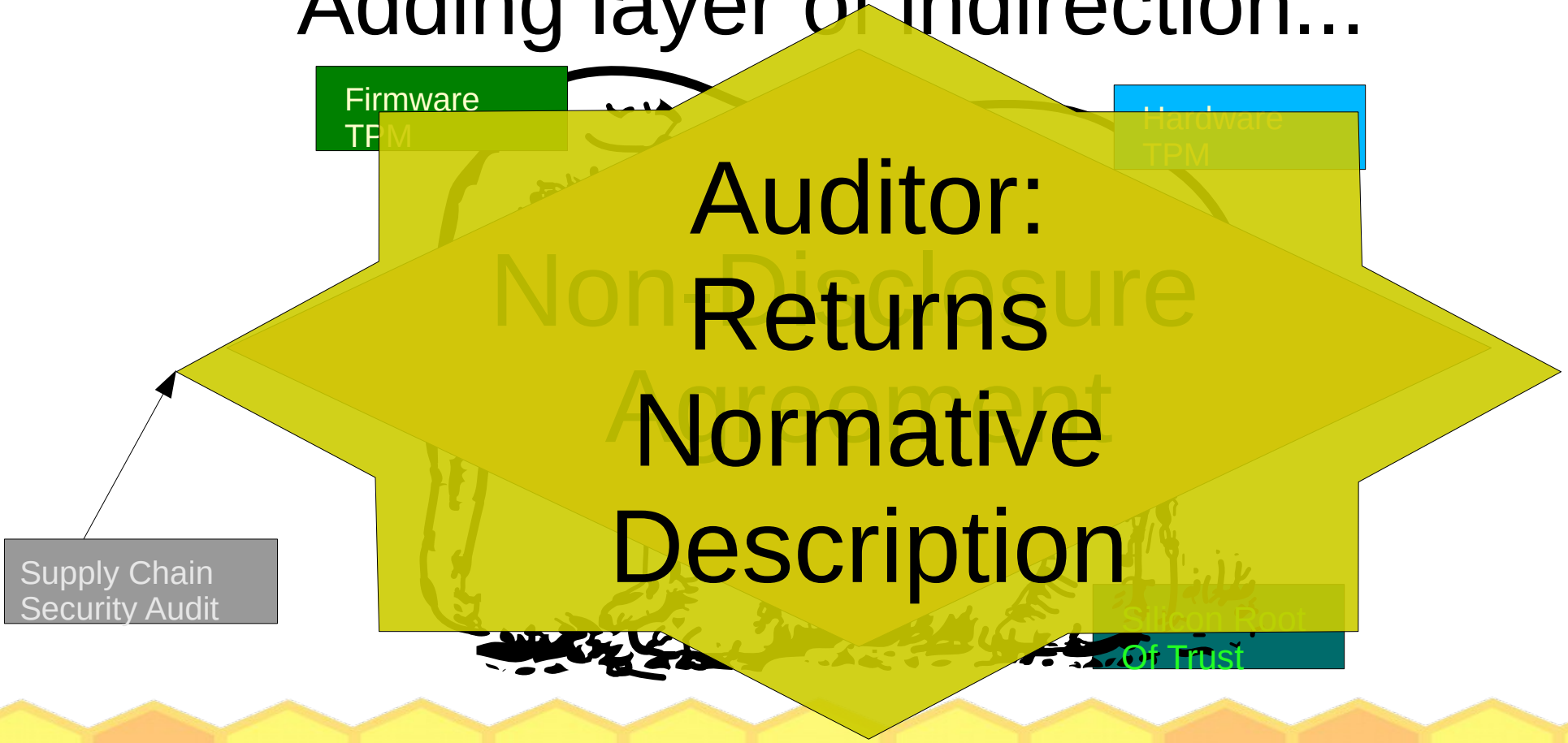
More pieces => more resiliency to “bus events”

higher threshold => more resitence to corruption, bribery, extortion?

If operations are spread across continents, should key pieces too?

HSMs are great, but expensive, and one needs two or three vs a bootable CDrom and any PC?

Adding layer of indirection...



Conclusions

1. In order to make security judgements, we first need a way communicate about the options, in a consistent way.
2. We don’t get to see fundamental data (NDA), so we need abstractions in the descriptions
3. Measuring comes first, judgement as to what is best is later.
4. One size does not fit all! One organizations over-the-top is another organizations’ minimum requirement

Read my document, please send comments/additions.

mcr@sandelman.ca

Questions!