draft-richardson-t2trg-idevid-considerations

2025-04-03   slides v7.0

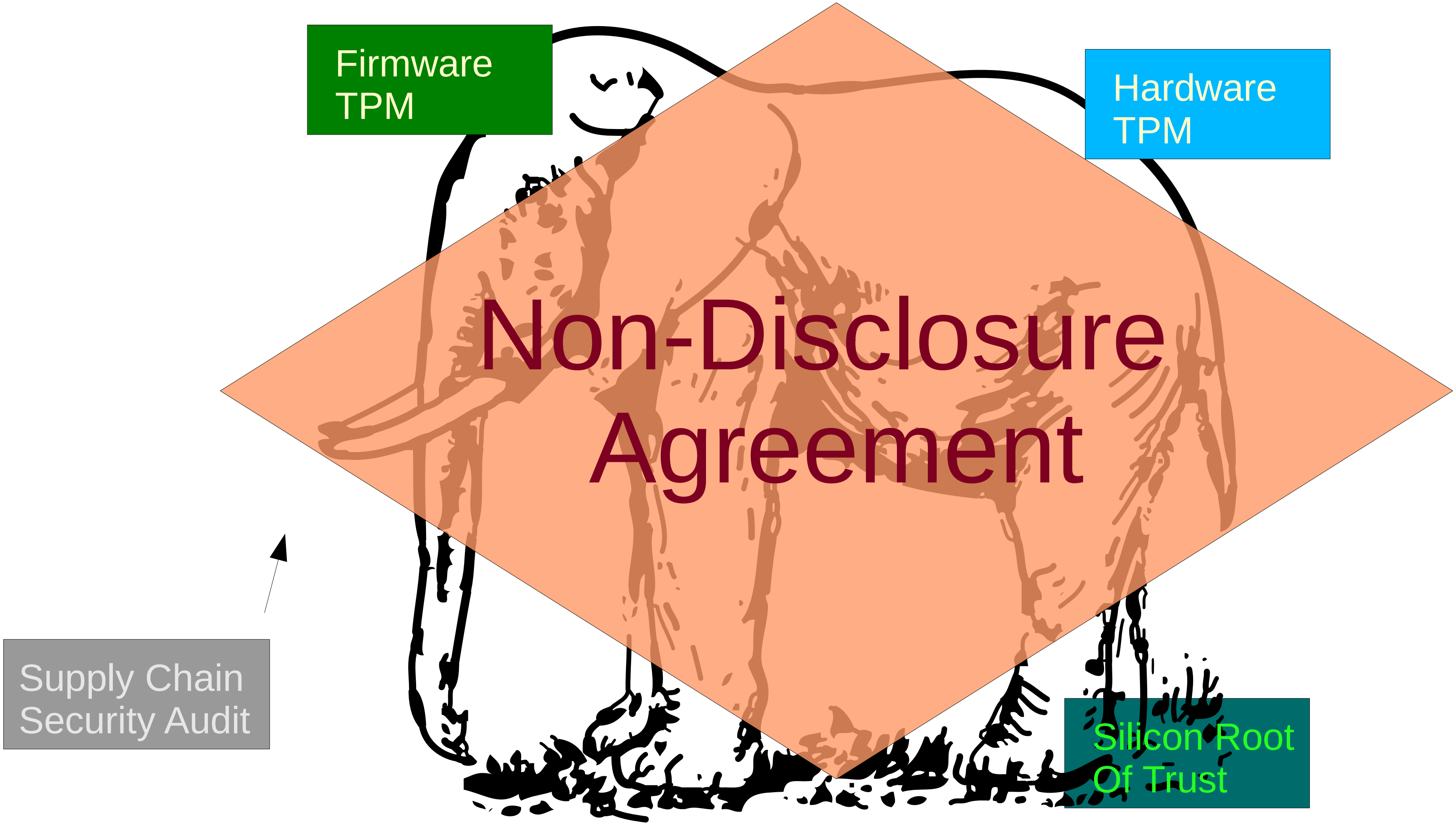
https://www.sandelman.ca/SSW/talks/idevid-considerations

Michael Richardson <mcr+ietf@sandelman.ca>

Why this document is important

- “manufacturers in general have a very bad track record when it comes to managing key materials outside the device”
- “Factoring RSA keys from certified smart cards: Coppersmith in the wild” https://smartfacts.cr.yp.to/smartfacts-20130916.pdf
- And many other comments about poor crypto hygiene my manufacturers.
  - “But not all manufacturers”
  - ... but how to tell, because so many NDAs
  - Your suppliers’ supplier’s supplier might be great... or bad, but how can you know?

Confidentiality of IDevID private key..



Firmware TPM

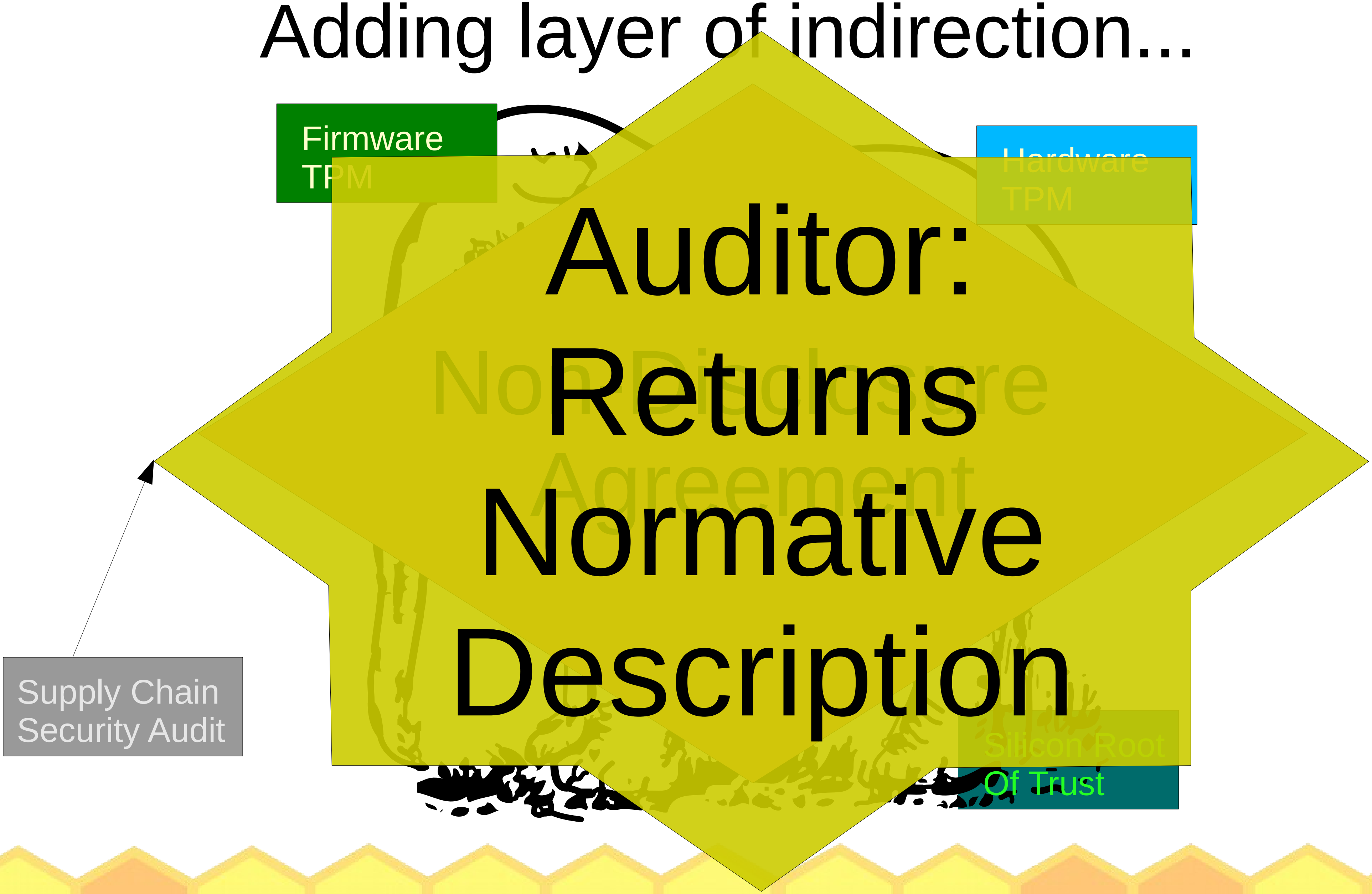
Hardware TPM

Non-Disclosure Agreement

Supply Chain Security Audit

Silicon Root Of Trust

Adding layer of indirection...



Firmware TPM

Hardware TPM

Supply Chain Security Audit

Silicon Root Of Trust

Non-Disclosure Agreement

Auditor: Returns Normative Description

The document so far

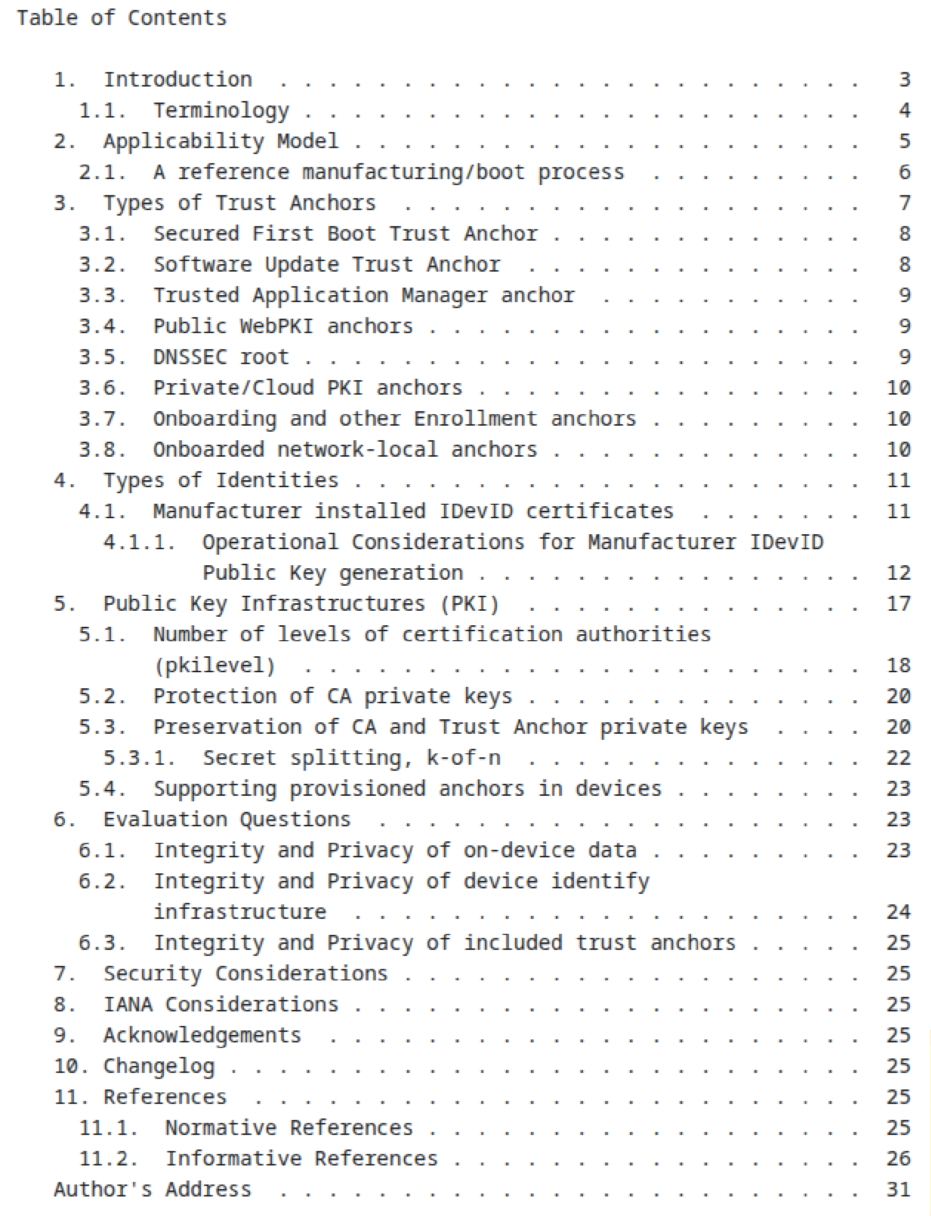


Table of Contents

- Trust Anchor
  - a thing a device uses to verify an external entity’s identity
- IDevID
  - a thing a device uses to prove an identity to an external entity
  - ways of provisioning these key pairs

Key Generation taxonomy

- (A)vocado
- (B)amboo
- (C)arrot
- (S_A)alak
- (S_B)apodilla

Key Generation taxonomy

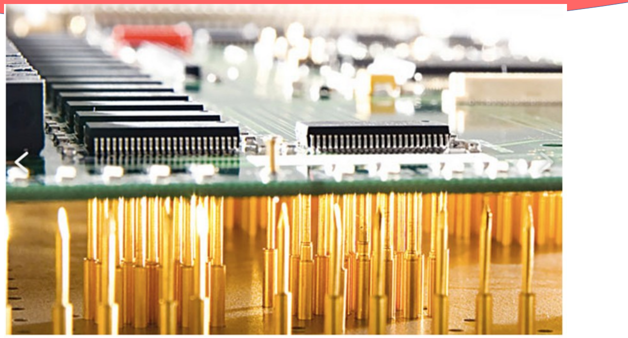
- (A)vocado
- (B)amboo
- (C)arrot
- (S_A)alak
- (S_B)apodilla

Key Generated in Device
CSR generated
Certificate returned to Device

Key Generation taxonomy

- (A)vocado
- (B)amboo
- (C)arrot
- (S_A)alak
- (S_B)apodilla

Key Generated in **Factory**
Factory generates CSR
Certificate + Private Key installed to Device



Key Generation taxonomy

- (A)vocado
- (B)amboo
- (C)arrot
- (S_A)alak
- (S_B)apodilla

Key Generated from pre-loaded seed
Factory also generates key+CSR
Certificate installed to Device

Key Generation taxonomy

- (A)vocado
- (B)amboo
- (C)arrot
- (S_A)alak
- (S_B)apodilla

Key Generated in Secure Element
CSR generated
Certificate returned to Device

Key Generation taxonomy

- (A)vocado
- (B)amboo
- (C)arrot
- (S_A)alak
- (S_B)apodilla

Key Generated in **Factory**
Factory generates CSR
Certificate + Private Key installed to Secure Element

Key Generation taxonomy

- (A)vocado
- (B)amboo
- (C)arrot
- (S_A)alak
- (S_B)apodilla

https://www.nccoe.nist.gov/sites/default/files/2024-05/nist-sp-1800-36-draft.pdf
into section
H.1.1 Device Birth Credential Provisioning Methods

Avocado
Method 1: Key Pair Generated on IoT Device

Bamboo
Method 3: Key Pair Loaded into IoT Device

Carrot
Method 5: Private Key Derived from Shared Seed

Salak
Method 2: Key Pair Generated in Secure Element

Sapodilla
Method 4: Key Pair Pre-Provisioned onto Secure Element

Key Generation taxonomy

- (A)vocado
- (B)amboo
- (C)arrot
- (S_A)alak
- (S_B)apodilla

TOO WHIMSICAL?

PLEASE SUGGEST BETTER TERMS

That’s all folks.
Time to publish?

Properties of PKI

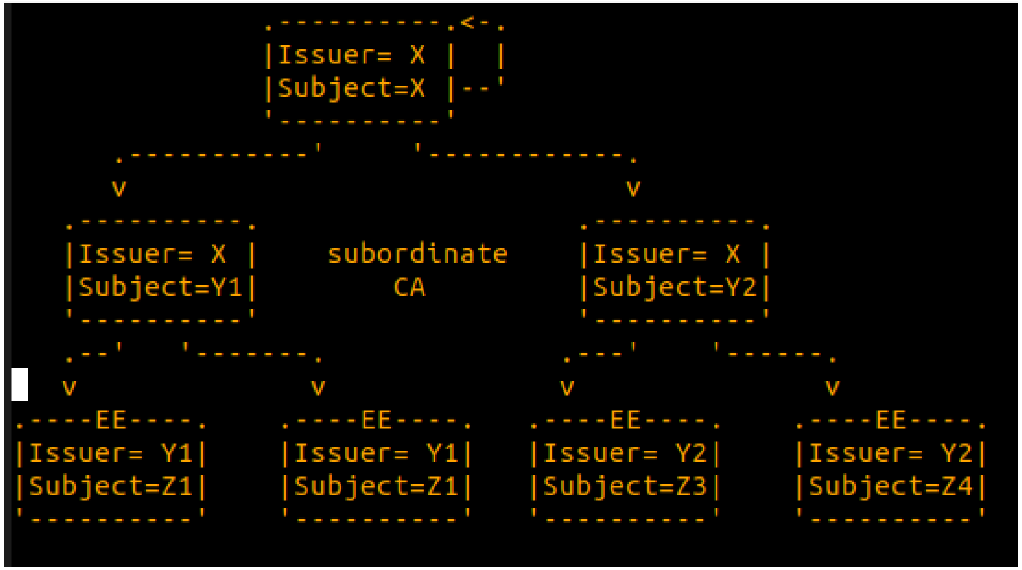
- initial-enclave-location:
- initial-enclave-integrity-key:
- initial-enclave-privacy-key:
- first-stage-initialization:
- first-second-stage-gap:
- identity-pki-level:
- identity-time-limits-per-subordinate:
- identity-number-per-subordinate:
- identity-anchor-storage:
- pki-level:
- pki-algorithms:
- pki-level-locked:
- pki-breadth:
- pki-lock-policy:
- pki-anchor-storage:

- many attributes shown on left
- not at all complete!

- How to deal with level of secret splitting?
  - business continuity vs risk of counterfeit

Public Key Infrastructure

- using “subordinate” rather than “intermediate”
- self-signed certificate is a PKI of level “one”
  - not counting from zero
-
- intermediate used in bridge CA use
- see https://fpki.idmanagement.gov/tools/fpkigraph/



```
                .----------.<-.
                |Issuer= X |  |
                |Subject=X |--'
                '----------'
       .-----------'     '-------------.
       v                               v
   .----------.                    .----------.
   |Issuer= X |     subordinate    |Issuer= X |
   |Subject=Y1|         CA         |Subject=Y2|
   '----------'                    '----------'
   .--'    '-------.               .---'    '------.
   v               v               v               v
.----EE----.     .----EE----.    .----EE----.    .----EE----.
|Issuer= Y1|     |Issuer= Y1|    |Issuer= Y2|    |Issuer= Y2|
|Subject=Z1|     |Subject=Z1|    |Subject=Z3|    |Subject=Z4|
'----------'     '----------'    '----------'    '----------'
```

- This document about the shapes of these things.
- Recovery and Resilience
- How are private keys kept safe?