



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>

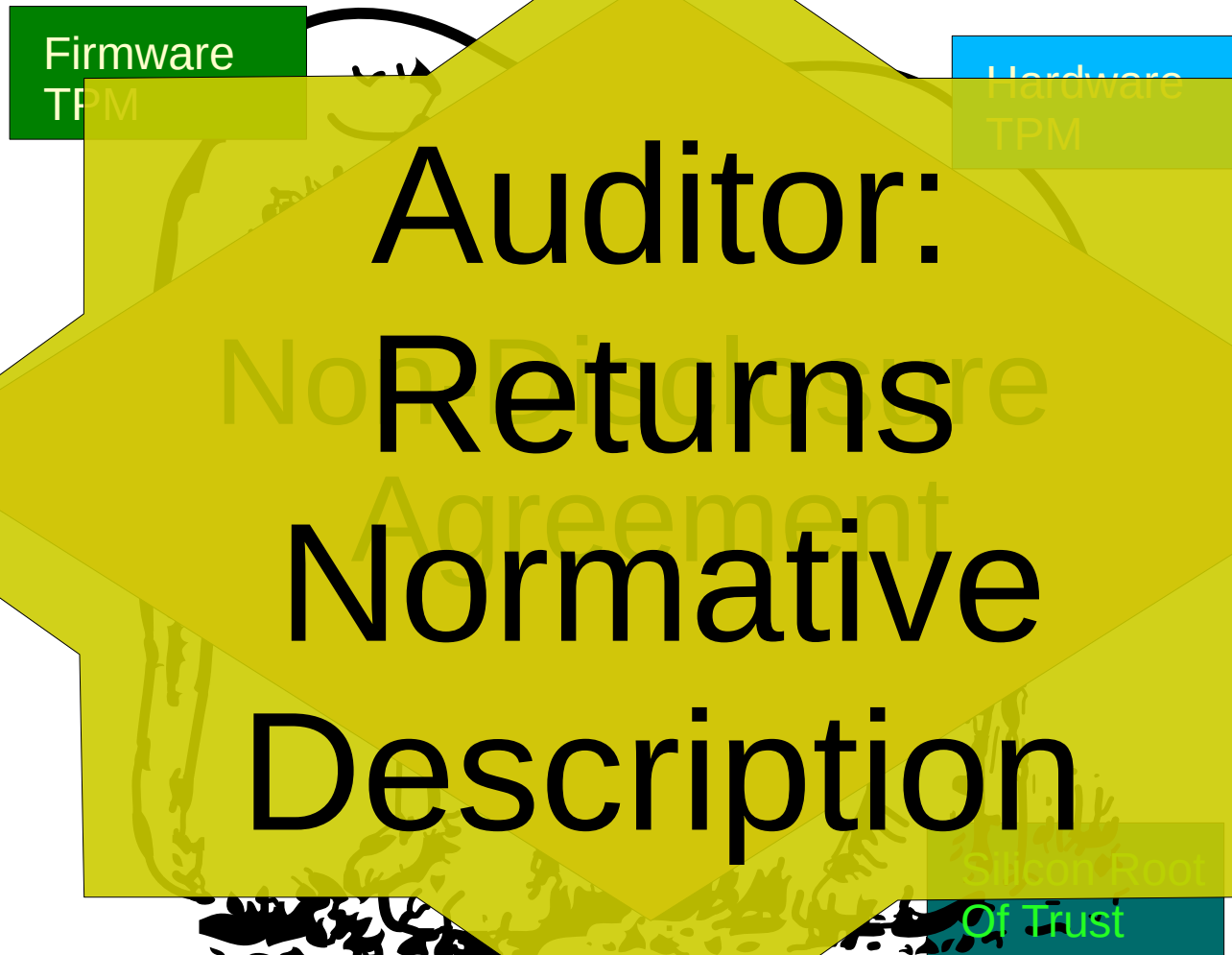
Why this document is important

- “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..



Adding layer of indirection...



Supply Chain
Security Audit

The document so far

Table of Contents

1. Introduction	3
1.1. Terminology	4
2. Applicability Model	5
2.1. A reference manufacturing/boot process	6
3. Types of Trust Anchors	7
3.1. Secured First Boot Trust Anchor	8
3.2. Software Update Trust Anchor	8
3.3. Trusted Application Manager anchor	9
3.4. Public WebPKI anchors	9
3.5. DNSSEC root	9
3.6. Private/Cloud PKI anchors	10
3.7. Onboarding and other Enrollment anchors	10
3.8. Onboarded network-local anchors	10
4. Types of Identities	11
4.1. Manufacturer installed IDevID certificates	11
4.1.1. Operational Considerations for Manufacturer IDevID Public Key generation	12
5. Public Key Infrastructures (PKI)	17
5.1. Number of levels of certification authorities (pkilevel)	18
5.2. Protection of CA private keys	20
5.3. Preservation of CA and Trust Anchor private keys	20
5.3.1. Secret splitting, k-of-n	22
5.4. Supporting provisioned anchors in devices	23
6. Evaluation Questions	23
6.1. Integrity and Privacy of on-device data	23
6.2. Integrity and Privacy of device identify infrastructure	24
6.3. Integrity and Privacy of included trust anchors	25
7. Security Considerations	25
8. IANA Considerations	25
9. Acknowledgements	25
10. Changelog	25
11. References	25
11.1. Normative References	25
11.2. Informative References	26
Author's Address	31

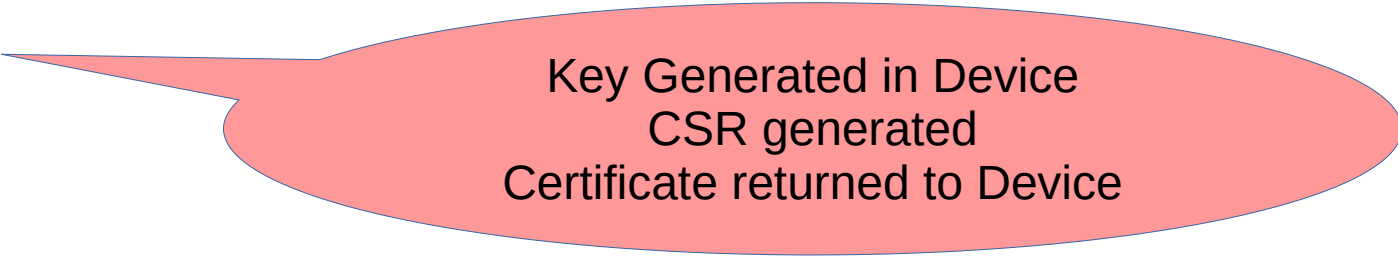
- Trust Anchor
 - a thing a device uses to verify an external entity's identity
- IDevID
 - a thing a device uses to prove an identity to an external entity
 - ways of provisioning these key pairs

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

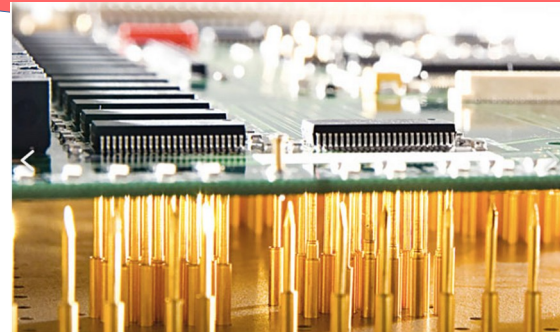


Key Generated in Device
CSR generated
Certificate returned to Device

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

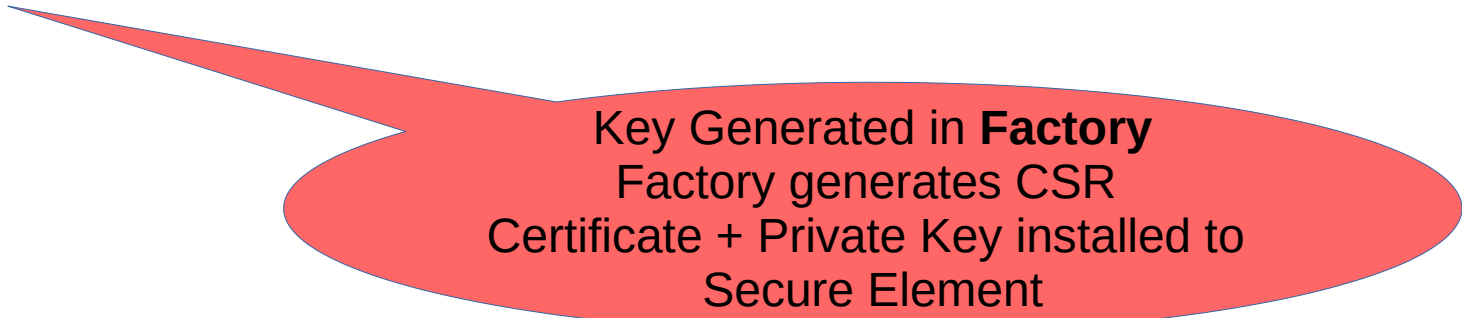
- (A)vocado
- (B)amboo
- (C)arrot
- (S_A)alak
- (S_B)apodilla



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

<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

- (A)vocado

Avocado

Method 1: Key Pair Generated on IoT Device

- (B)amboo

Bamboo

Method 3: Key Pair Loaded into IoT Device

- (C)arrot

Carrot

Method 5: Private Key Derived from Shared Seed

- (S_A)alak

Salak

Method 2: Key Pair Generated in Secure Element

- (S_B)apodilla

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

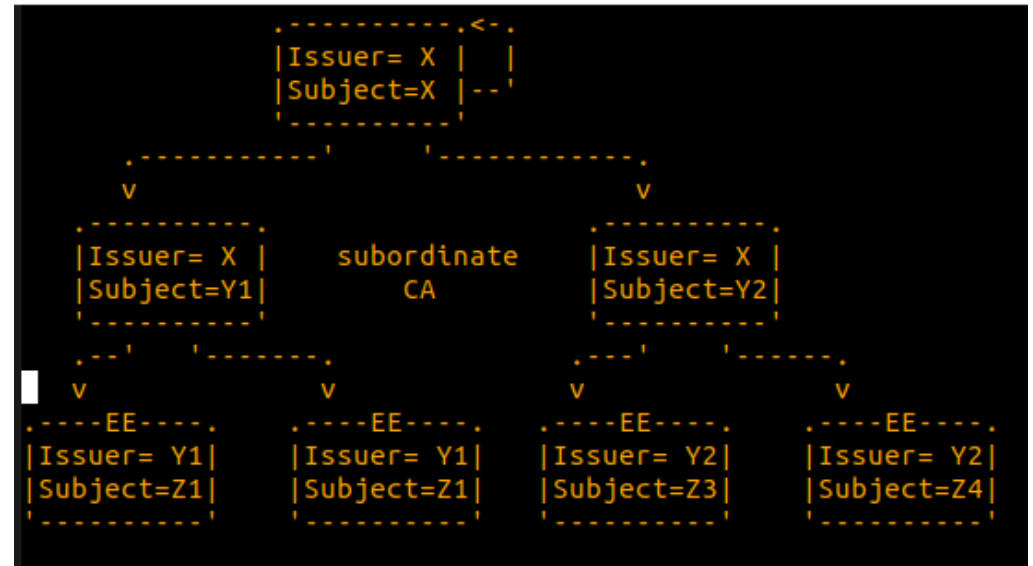
- initial-enclave-location:
- initial-enclave-integrity-key:
- initial-enclave-privacy-key:
- first-stage-initialization:
- first-second-stage-gap:
- identity-pki-level:
- identity-time-limits-per-subordinate:
- identity-number-per-subordinate:
- identity-anchor-storage:
- pki-level:
- pki-algorithms: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



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