draft-richardson-secdispatch-idevid-considerations-02

IETF108 – secdispatch - 2020-07-30

Michael Richardson <mcr+ietf@sandelman.ca>
JayYang <jay.yang@huawei.com>

http://www.sandelman.ca/SSW/ietf/meeting/ietf108/secdispatch-ietf108-idevid-considerations-expanded.pdf

1972

My Dad (cjr)
[Sociologist!]

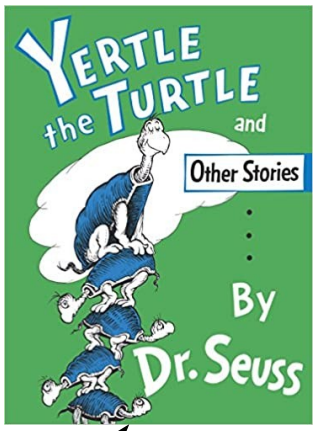
Returned from UK

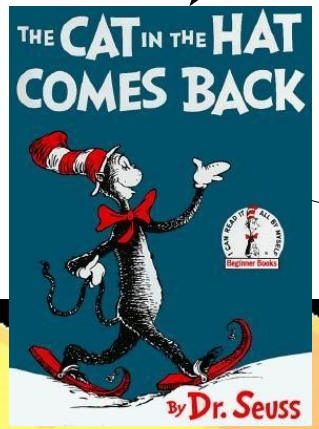
Alpha version of SPSS: Statistical Package for the Social Sciences

With
Baby Boy (mcr)

1975

Got a “computer”





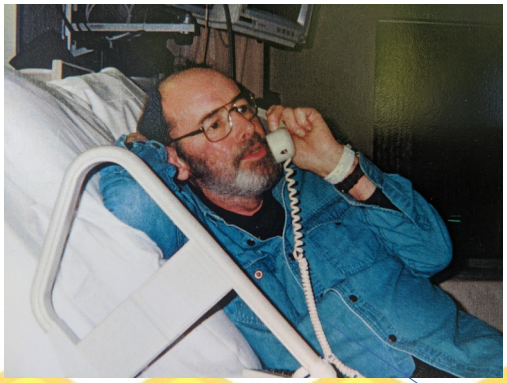
Worn Out copy

1995: for decates, he had been pestering me:

HOW DOES MY COMPUTER KNOW
WHAT TO DO WHEN I TURN IT ON?

HOW DOES IT KNOW IT WHO IT CAN TRUST?

Me, explaining
What a BIOS is



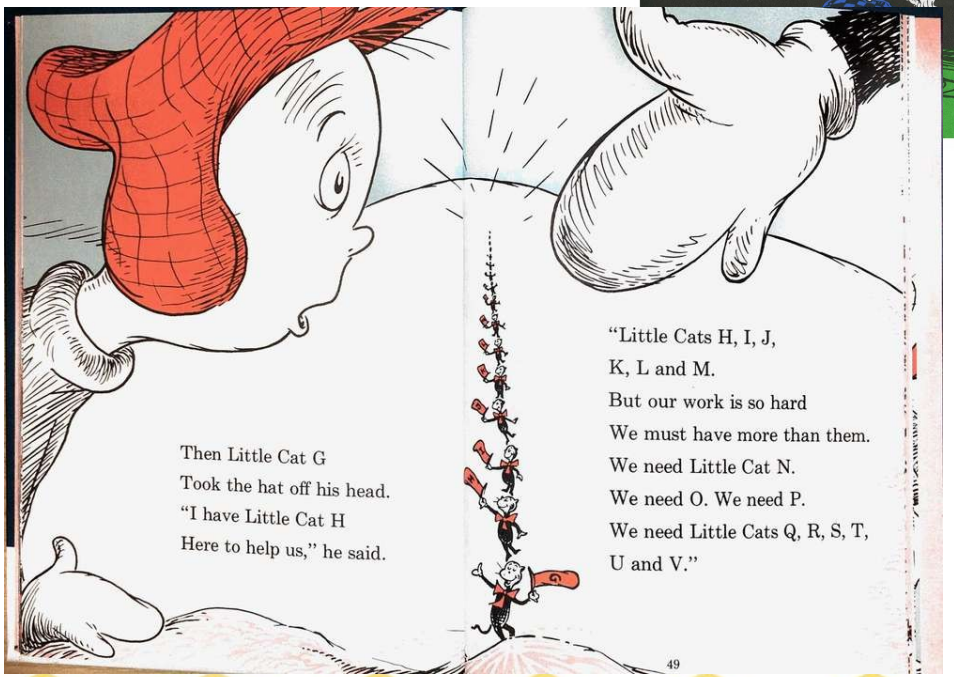
"So, does every
IoT device have
a secure enclave?"

"No, I don't want
to securely update
right now!!"

Turtles all the way down

- Everytime I thought I'd convinced him, he'd just just complain:
  - You've just added a turtle.

At some point, it's gotta stop,
There must something down there, he would complain.

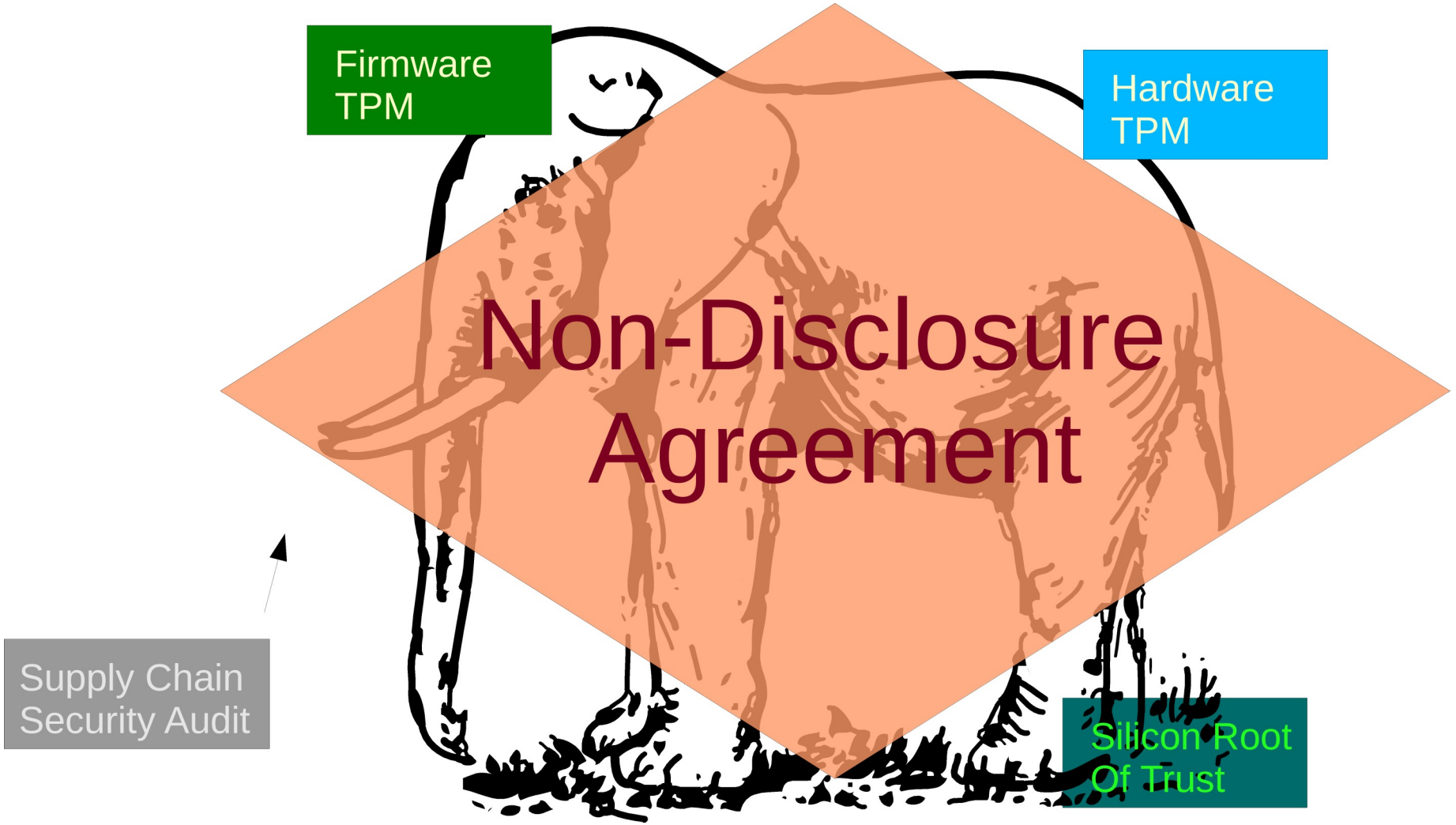


IDevID considerations document

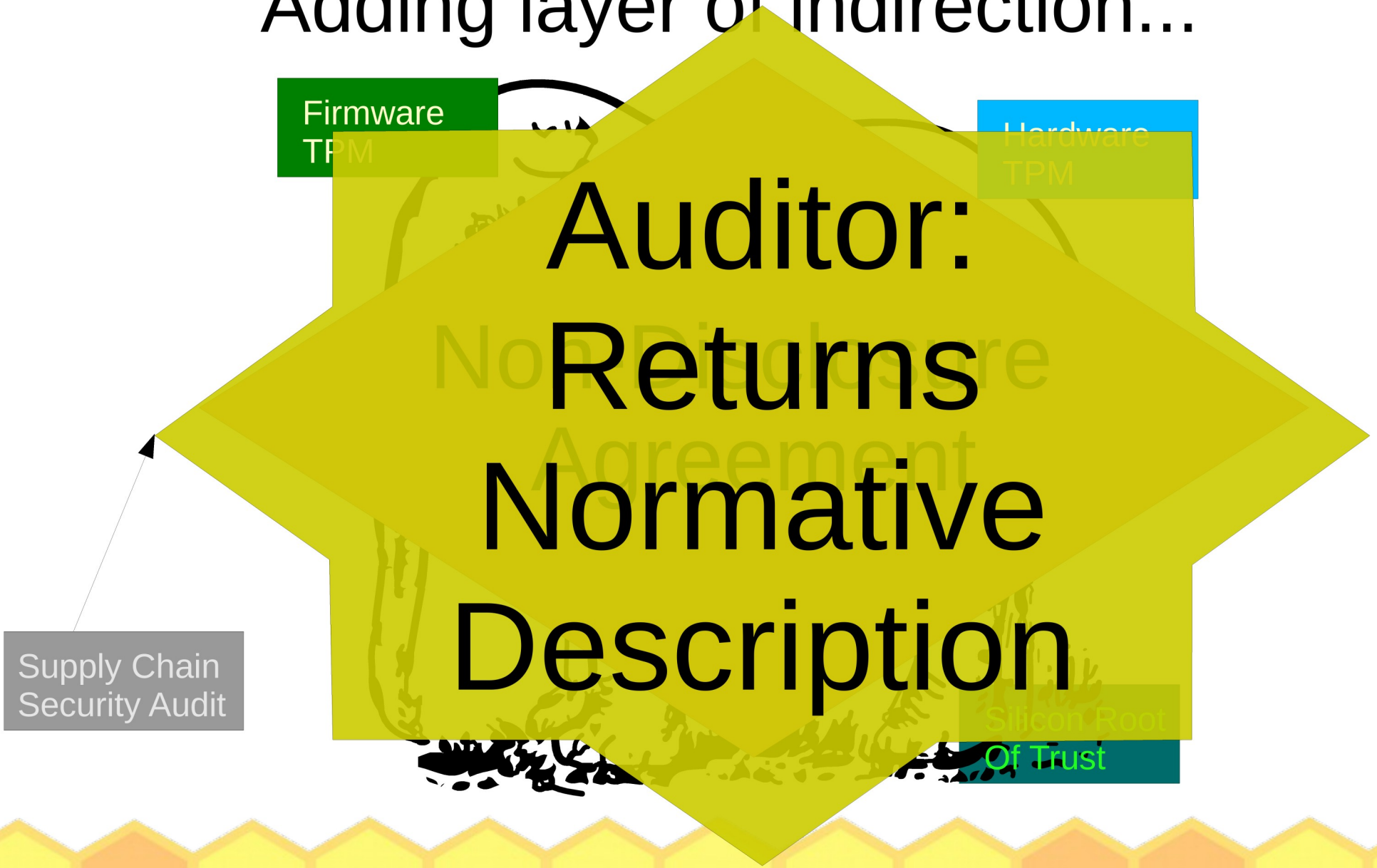
- This document is about the quality of the turtles
  - How do they get there?
  - Can they be trusted?
    - How much?
    - **For what?** (Is the risk mitigation appropriate to the user's threat model?)
- Three fundamental ways to provision initial roots of trust.
- Ultimately, the software update trust anchor **rules everything.**

- Insert parable about blind people examining different parts of an elephant.
- https://en.wikipedia.org/wiki/Blind_men_and_an_elephant

Confidentiality of IDevID private key..



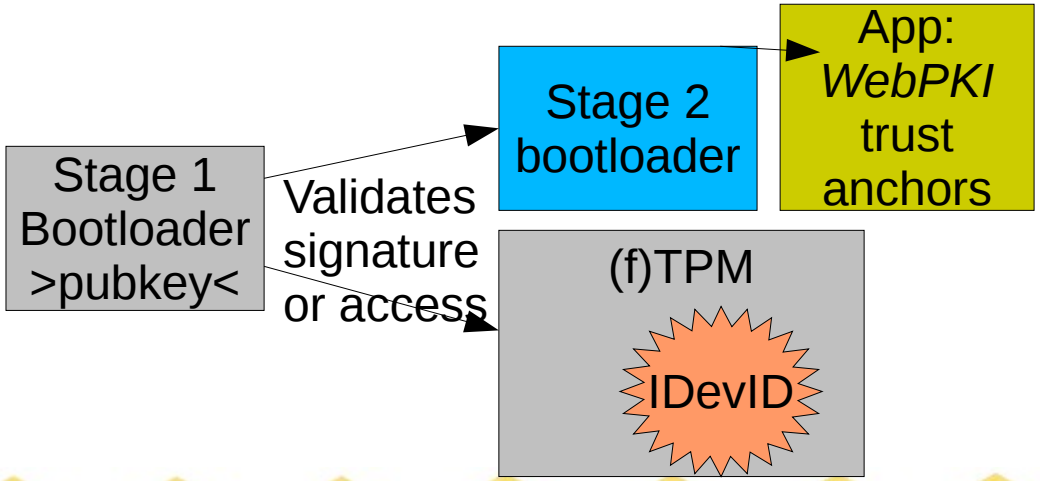
Adding layer of indirection...



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?

Non-Goals of the document

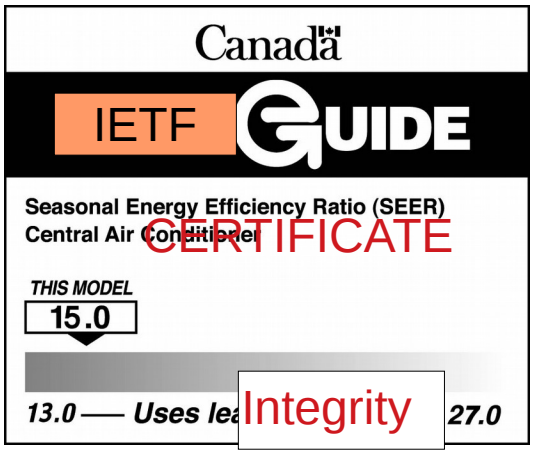
1) Not aiming to write an ISO27001-ish evaluation process.

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

The PKI part of the document
Is still proscriptive, that's a bug
left from splitting.

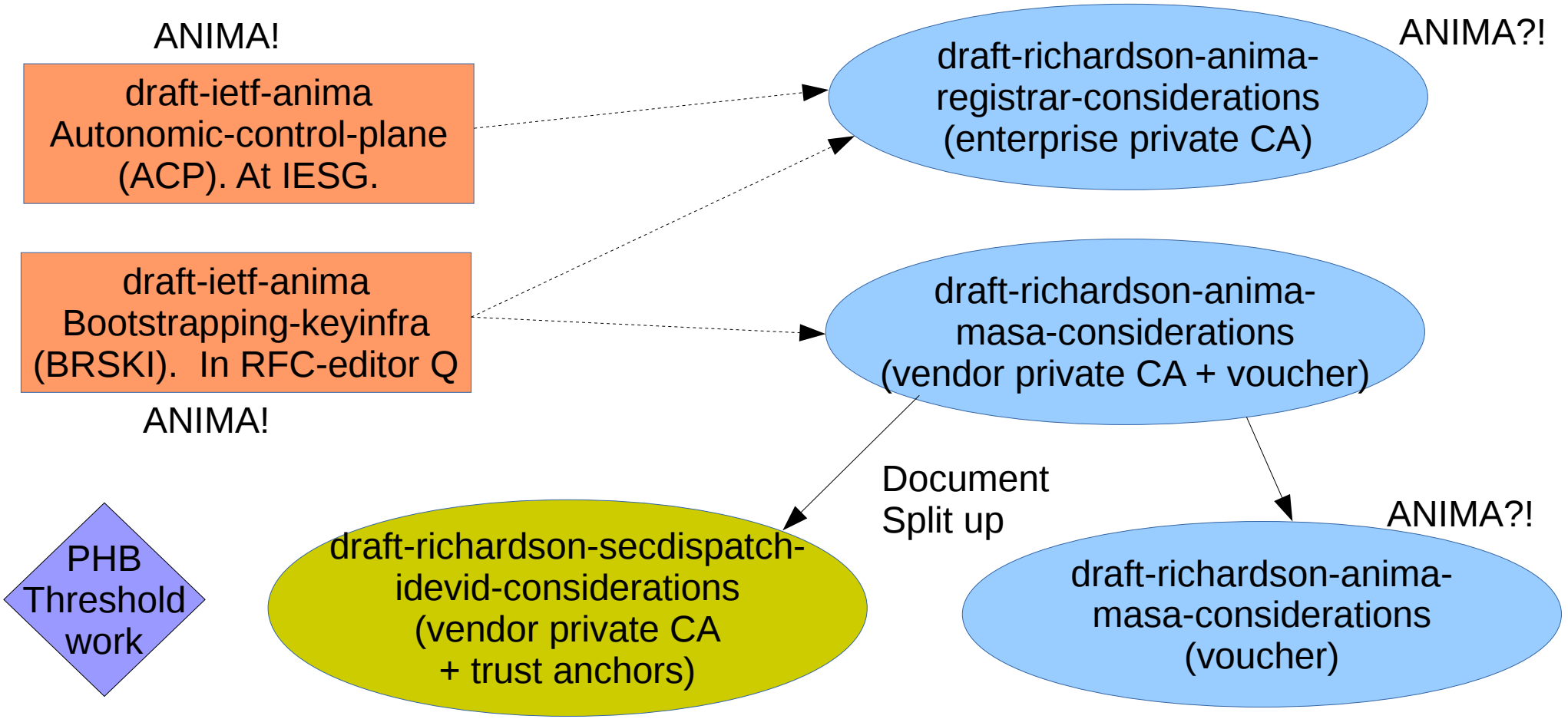
Goals of this document

- 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

History of Document



Useful Links

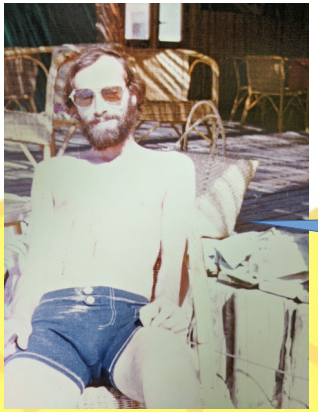
- IDevID discussions
  - https://mailarchive.ietf.org/arch/msg/secdispatch/Hqe1lHG2wnW_9NxJLazEYbmGYN0/
  - https://mailarchive.ietf.org/arch/msg/anima/-2Niz98BNSopDi4GpgxrDfl_Mdc/
  - https://mailarchive.ietf.org/arch/msg/anima/eMOH3NFbEDjZOi5gZgB9EkI6yxw/
  - https://mailarchive.ietf.org/arch/msg/anima/-6-eQJgtUWrz5v067u9Xb030qnQ/
- MASA operational considerations
  - https://mailarchive.ietf.org/arch/msg/anima/PSkpYZs0C_RLzUFD2BSMipEggfQ/

Useless Links and Irrelevant Facts

- Return of Cat in the Hat https://www.youtube.com/watch?v=YJf2f_LqnLo
- Yertle the Turtle https://www.youtube.com/watch?v=xY5vs2WtlKM
  - ..in which the eponymous Yertle, king of the pond, stands on his subjects in an attempt to reach higher than the moon—until the bottom turtle (Mack) burps and he falls into the mud, ending his rule.

Dr. C. James Richardson

1941-2003



Actually, Sardinia, Not London.

Actually, My brother jjrh