



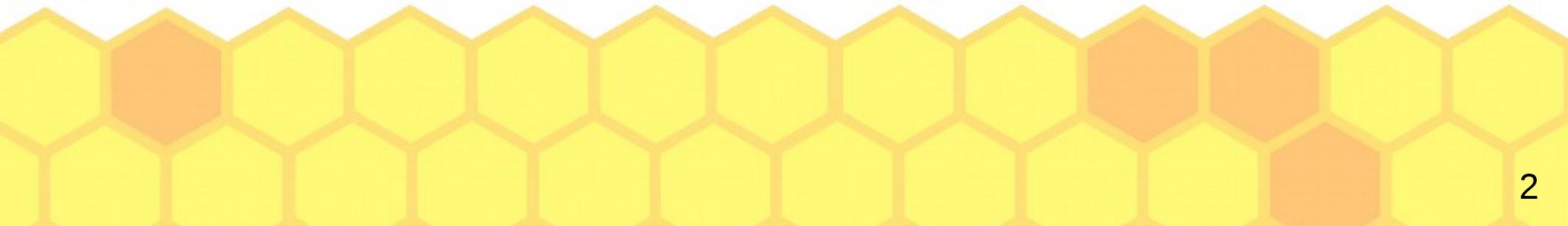
draft-richardson-secdispatch-idevid- considerations-02

IETF108 – secdispatch - 2020-07-30

Michael Richardson <mcr+ietf@sandelman.ca>

JayYang <jay.yang@huawei.com>

1972



1972



My Dad (cjr)
[Sociologist!]

1972



My Dad (cjr)
[Sociologist!]



Returned from UK

1972



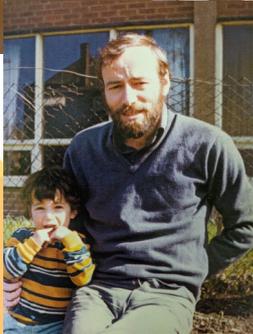
My Dad (cjr)
[Sociologist!]



Returned from UK



With
Baby Boy (mcr)



1972



My Dad (cjr)
[Sociologist!]



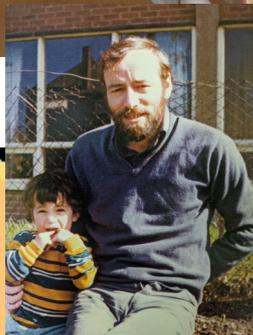
Returned from UK



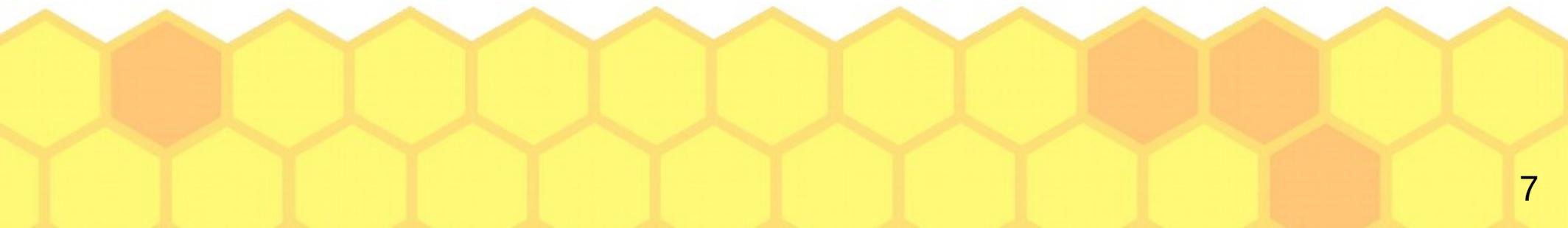
Alpha version of
SPSS: Statistical
Package for the
Social Sciences



With
Baby Boy (mcr)



1975



1975



Got a "computer"



1975



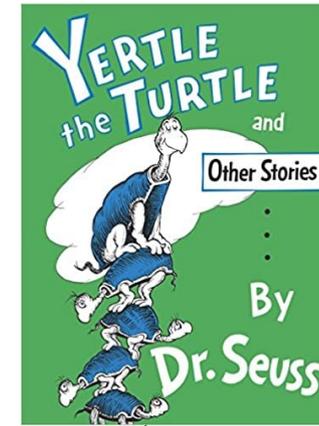
Got a "computer"



1975



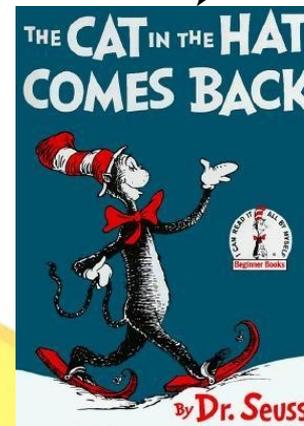
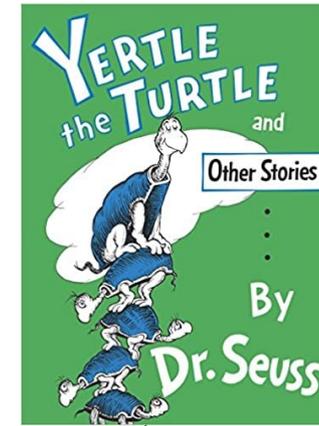
Got a "computer"



1975



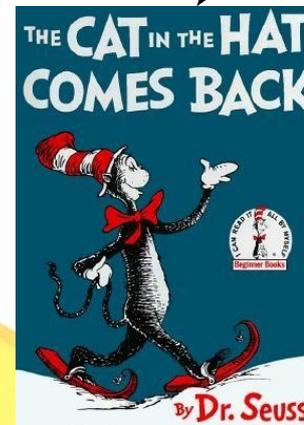
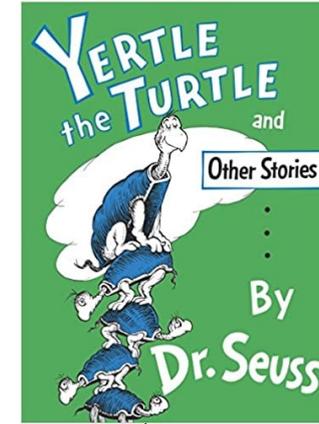
Got a "computer"



1975



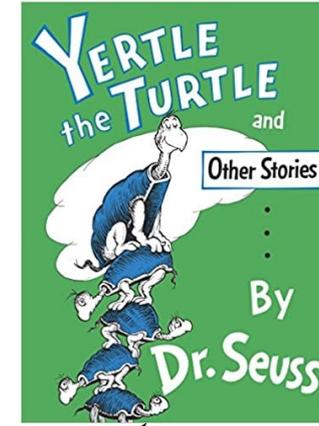
Got a "computer"



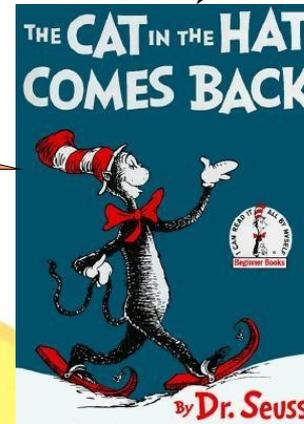
1975



Got a "computer"



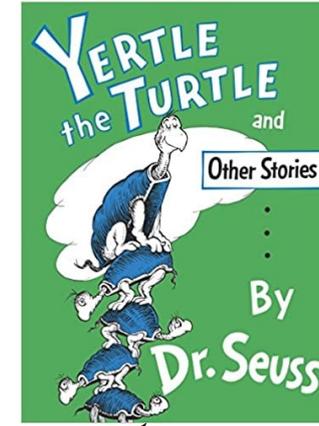
And we read
An awful lot



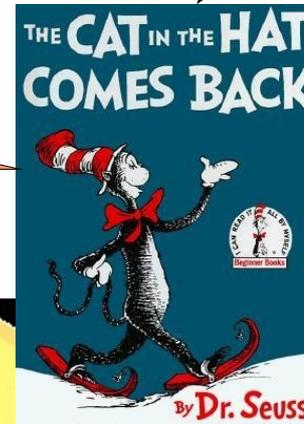
1975



Got a "computer"



And we read
An awful lot



Worn
Out
copy

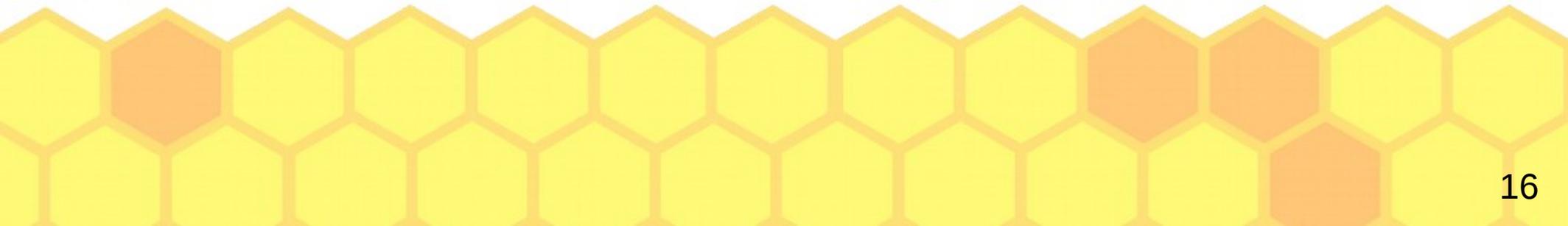


1995: for decades, he had been
pestering me:



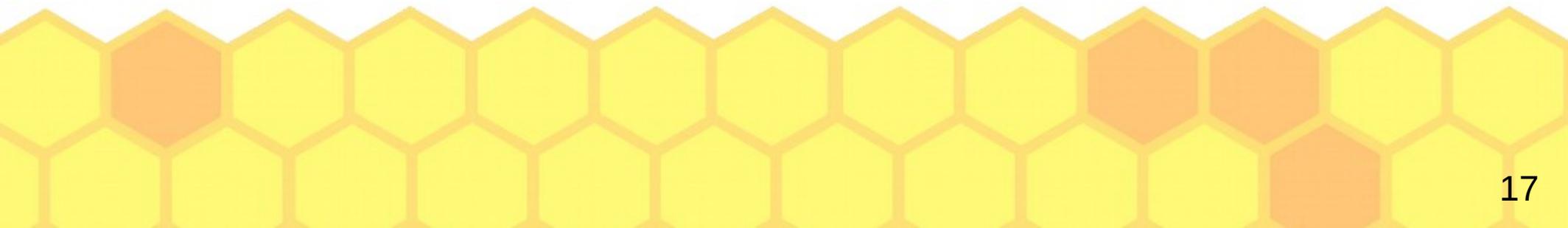
1995: for decades, he had been pestering me:

HOW DOES MY COMPUTER KNOW



1995: for decades, he had been pestering me:

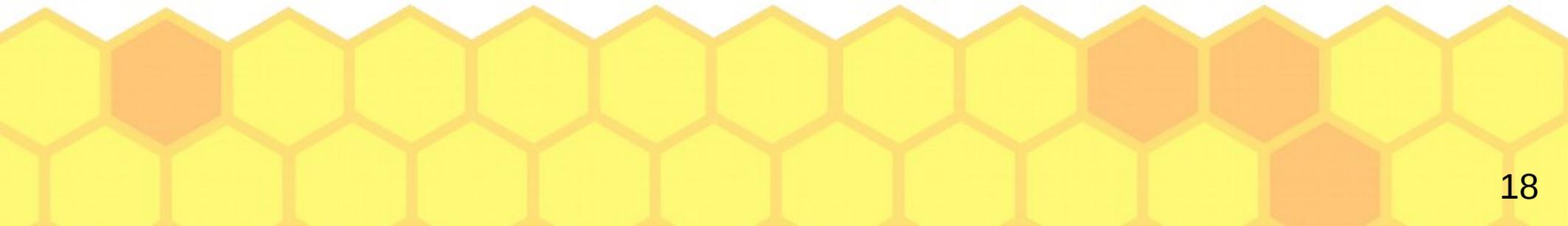
HOW DOES MY COMPUTER KNOW
WHAT TO DO WHEN I TURN IT ON?



1995: for decades, 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?



1995: for decades, 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

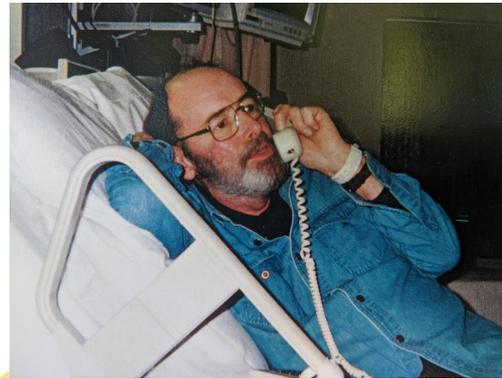


1995: for decades, he had been pestering me:

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



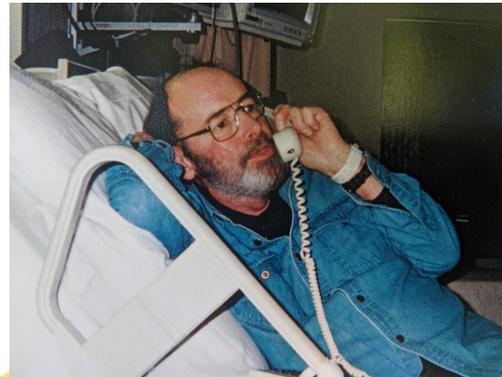
“So, does every
IoT device have
a secure enclave?”

1995: for decades, he had been pestering me:

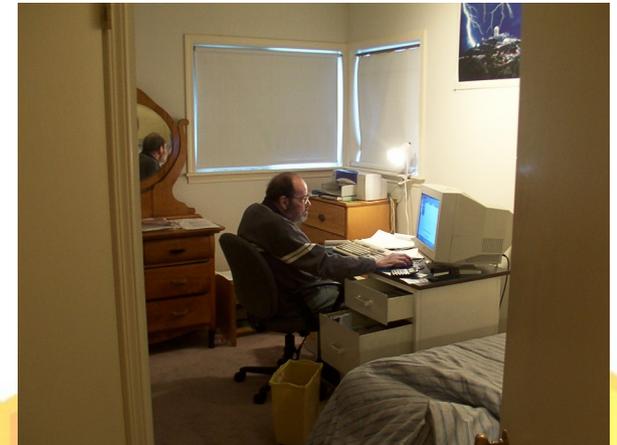
HOW DOES MY COMPUTER KNOW
WHAT TO DO WHEN I TURN IT ON?

HOW DOES IT KNOW IT WHO IT CAN TRUST?

Me, explaining
What a BIOS is



“So, does every
IoT device have
a secure enclave?”

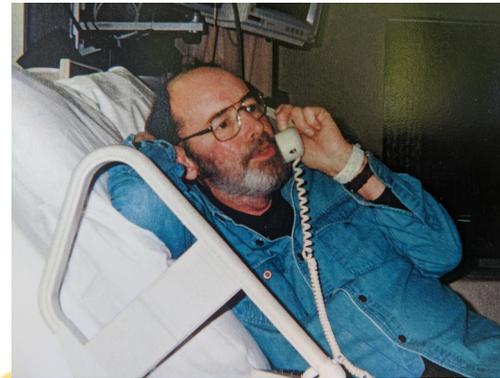


1995: for decades, he had been pestering me:

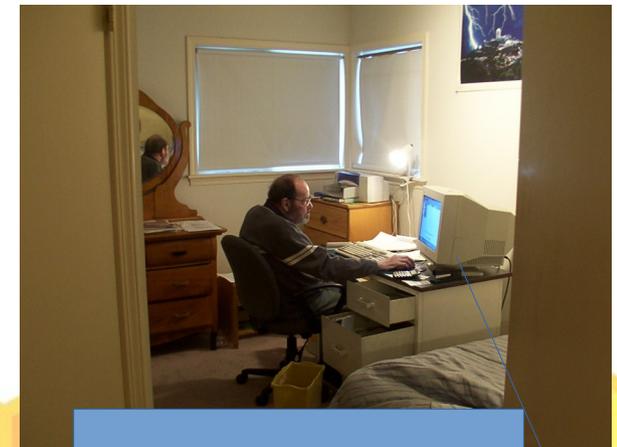
HOW DOES MY COMPUTER KNOW
WHAT TO DO WHEN I TURN IT ON?

HOW DOES IT KNOW IT WHO IT CAN TRUST?

Me, explaining
What a BIOS is



“So, does every
IoT device have
a secure enclave?”



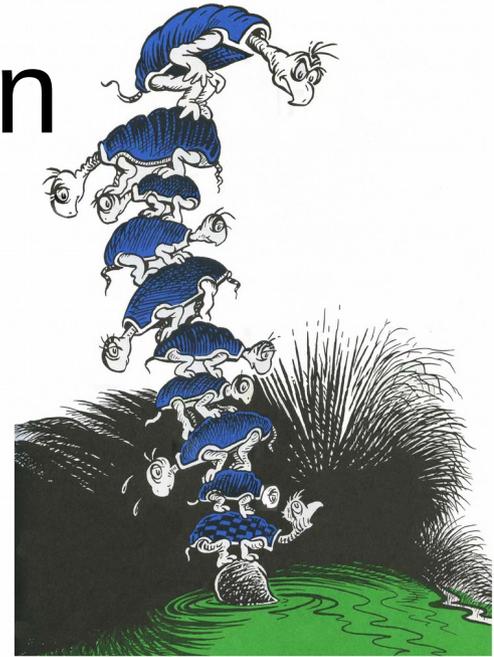
“No, I don't want
to securely update
right now!!”

Turtles all the way down

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

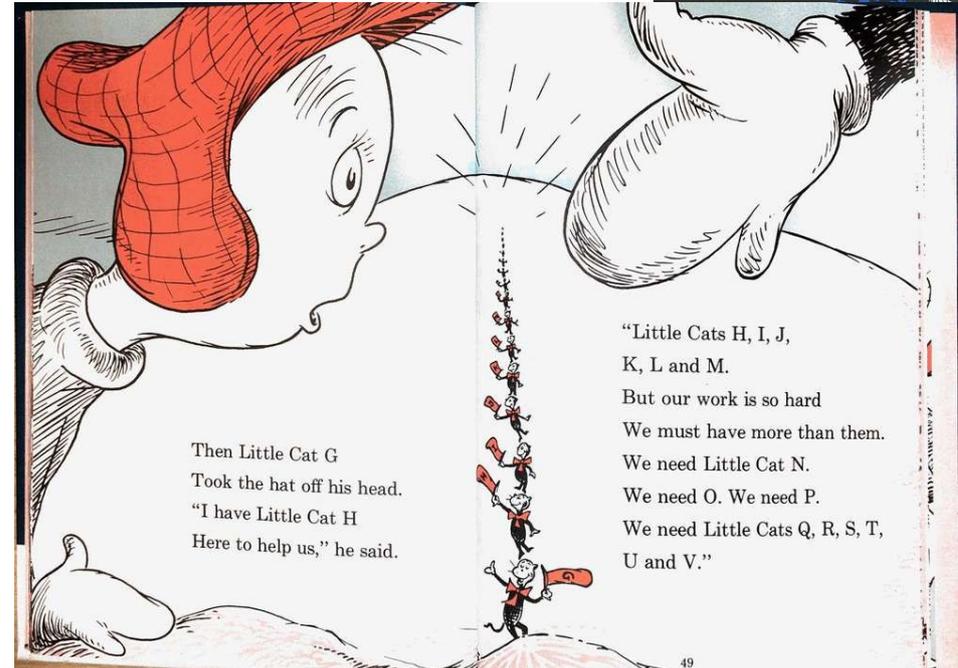
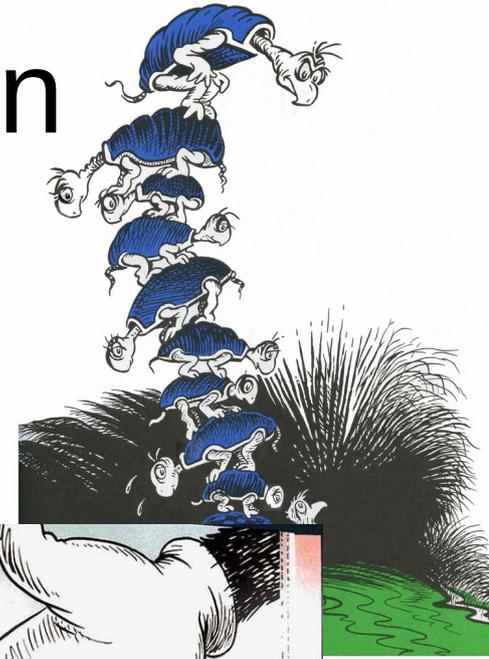
Turtles all the way down

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



Turtles all the way down

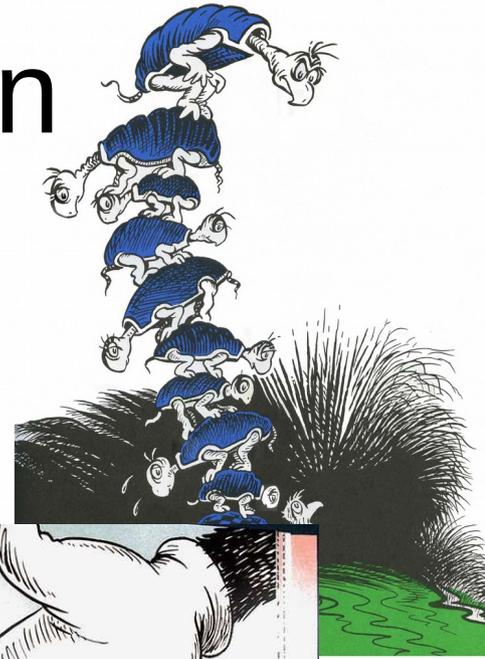
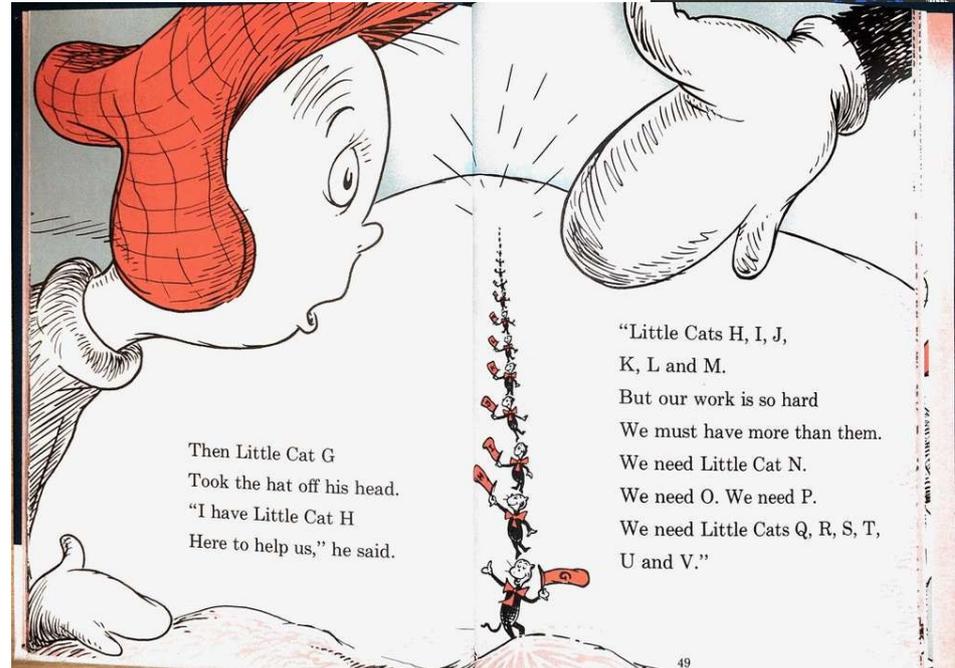
- Everytime I thought I'd convinced him, he'd just just complain:
 - You've just added a turtle.



Turtles all the way down

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

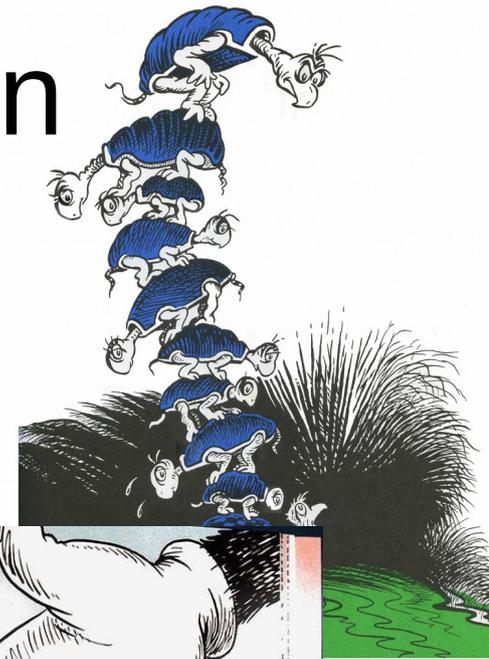
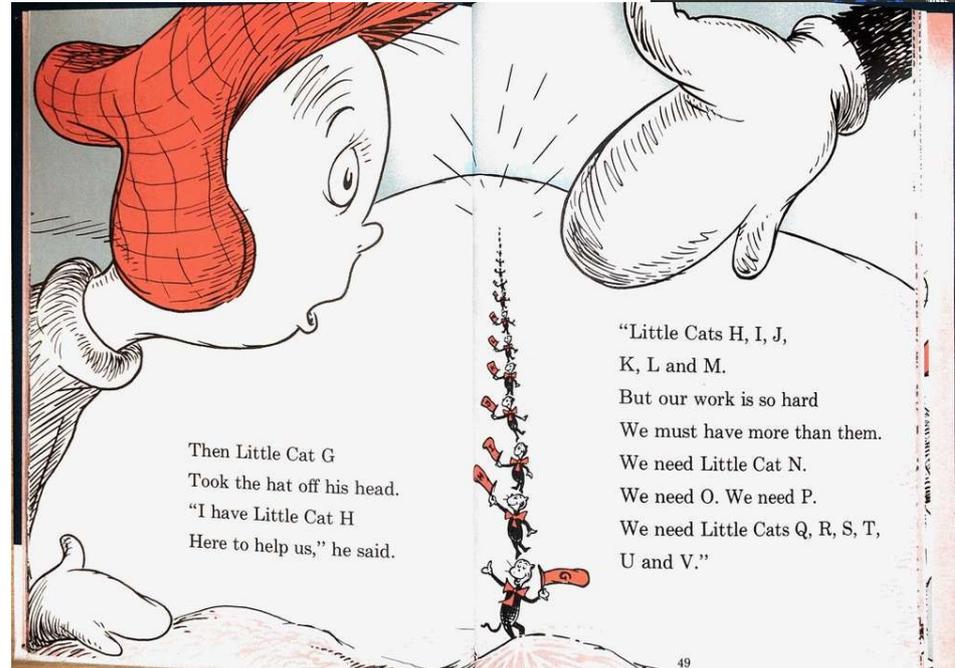
At some point, it's gotta stop,



Turtles all the way down

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

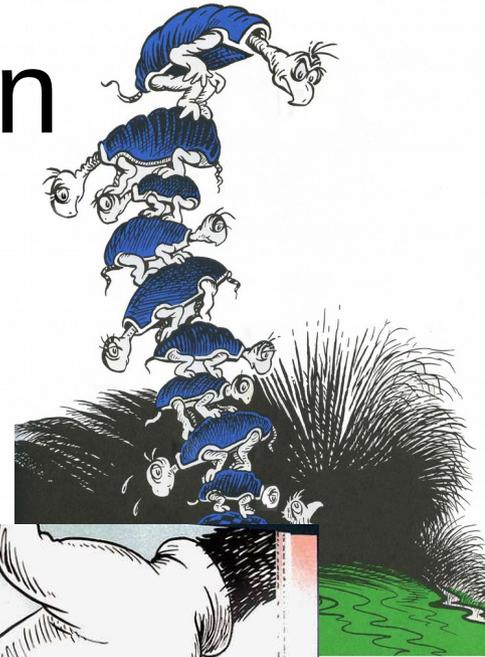
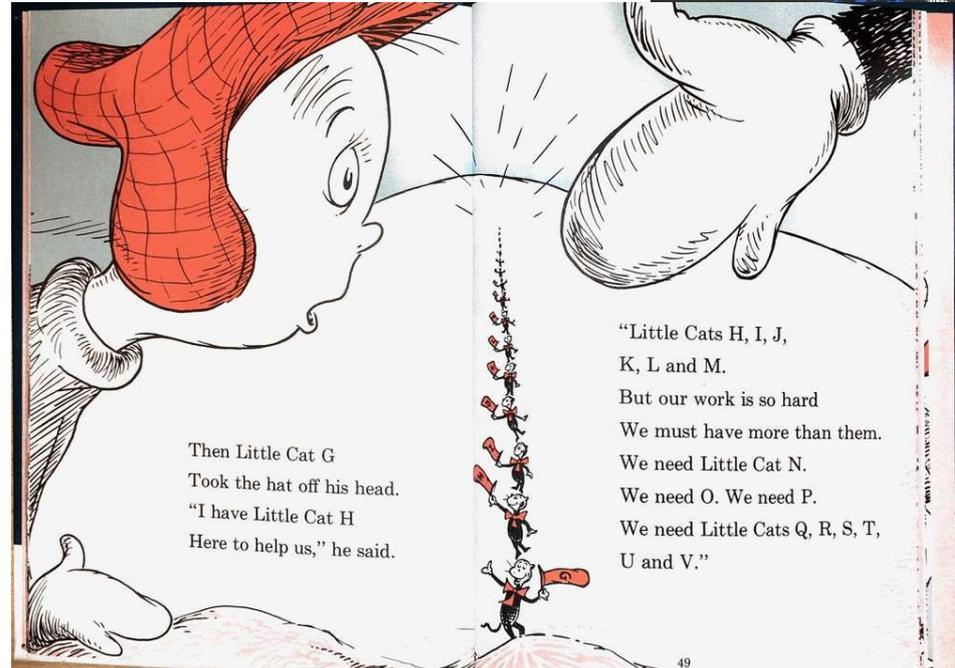
At some point, it's gotta stop,
There must something down



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

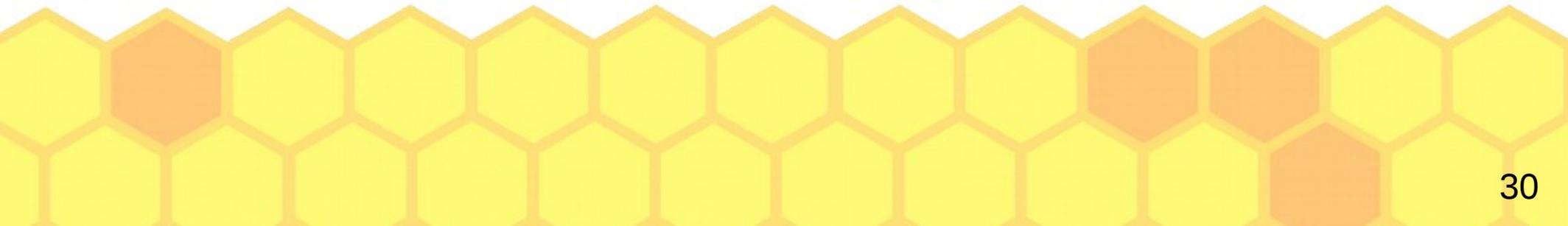
- This document is about the quality of the turtles
 - How do they get there?
 - Can they be trusted?
 - How much?
 - **For what?** (Is the risk mitigation appropriate to the user's threat model?)
- Three fundamental ways to provision initial roots of trust.
- Ultimately, the software update trust anchor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

Firmware
TPM

Hardware
TPM

Auditor:
Returns
Normative
Description

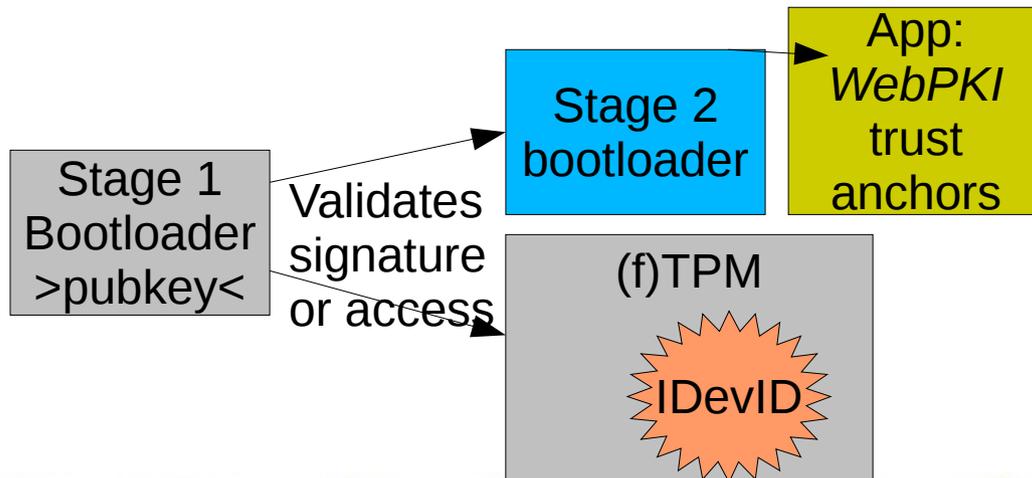
Supply Chain
Security Audit

Silicon Root
Of Trust

Audit Model

Recognize:

Possessor 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

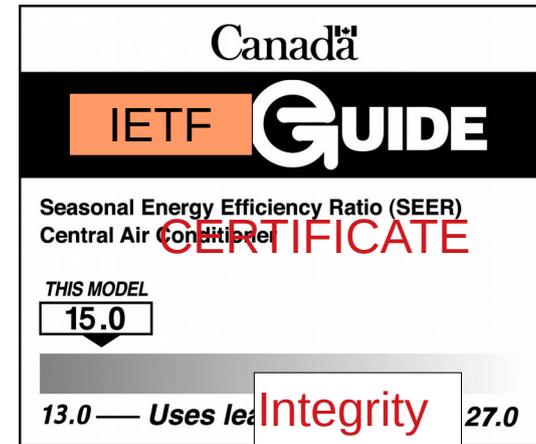
- 1) Not aiming to write an ISO27001-ish evaluation process.
- 2) Not going to make any recommendation as to an appropriate solution for a given risk situation.



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

ANIMA!

draft-ietf-anima
Autonomic-control-plane
(ACP). At IESG.

draft-ietf-anima
Bootstrapping-keyinfra
(BRSKI). In RFC-editor Q

ANIMA!

History of Document

ANIMA!

draft-ietf-anima
Autonomic-control-plane
(ACP). At IESG.

draft-ietf-anima
Bootstrapping-keyinfra
(BRSKI). In RFC-editor Q

ANIMA!

draft-richardson-anima-
registrar-considerations
(enterprise private CA)

ANIMA?!

History of Document

ANIMA!

draft-ietf-anima
Autonomic-control-plane
(ACP). At IESG.

draft-ietf-anima
Bootstrapping-keyinfra
(BRSKI). In RFC-editor Q

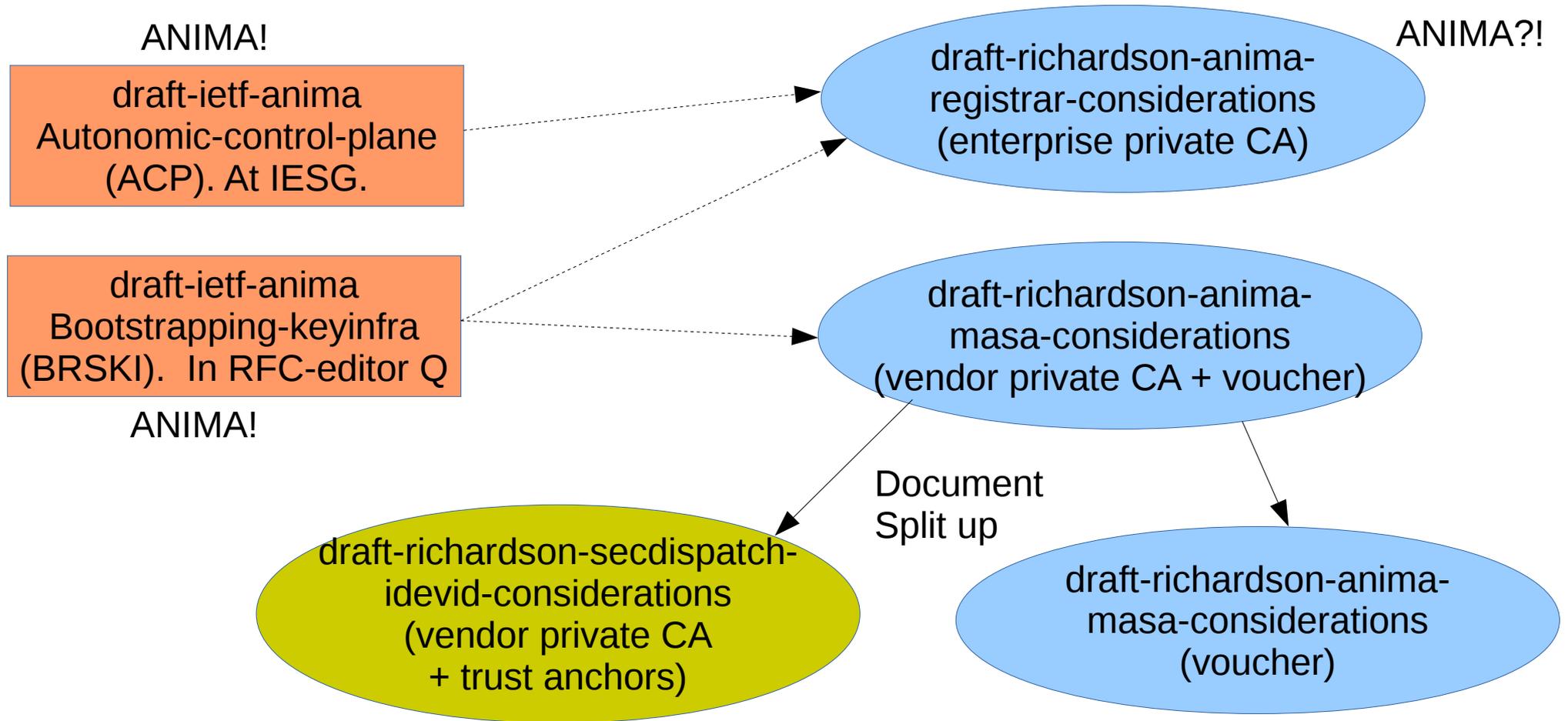
ANIMA!

draft-richardson-anima-
registrar-considerations
(enterprise private CA)

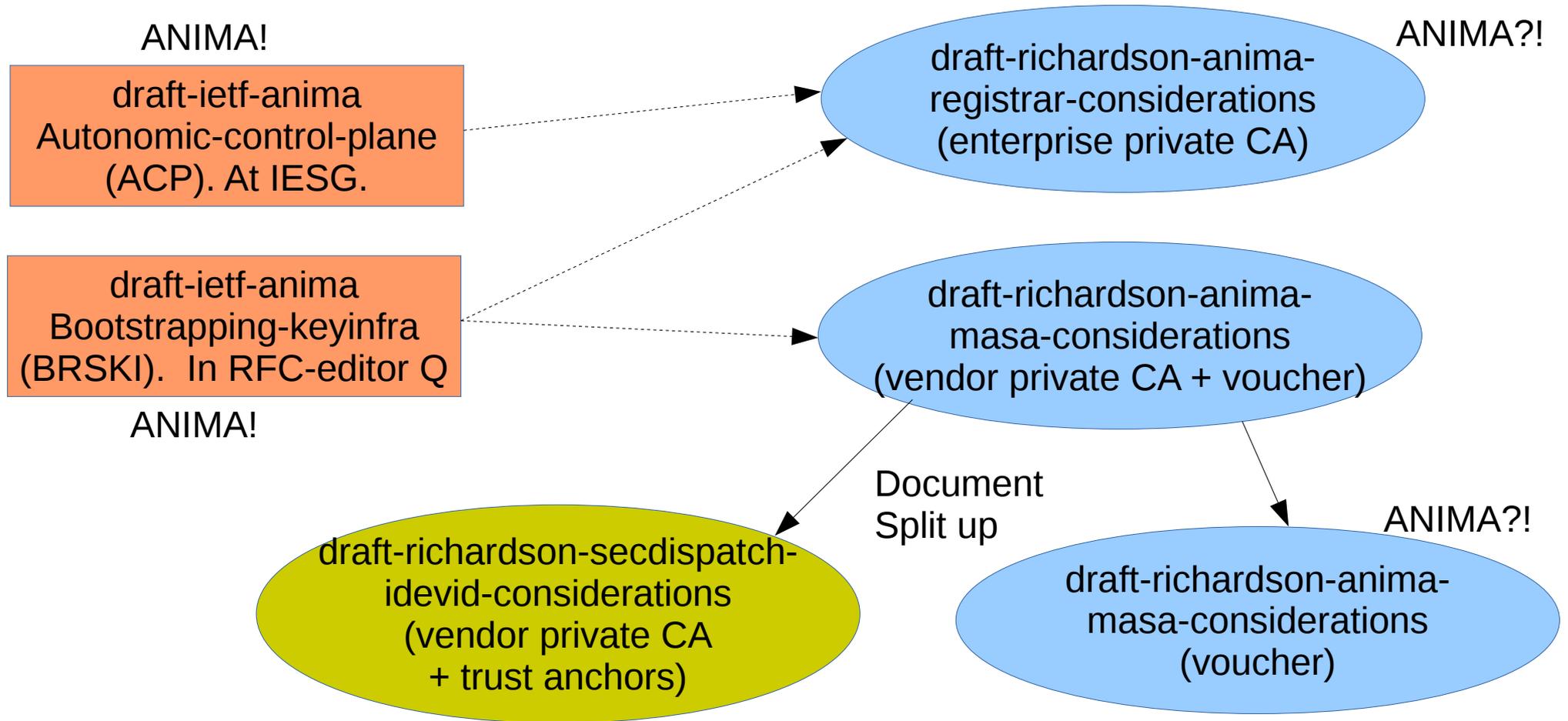
ANIMA?!

draft-richardson-anima-
masa-considerations
(vendor private CA + voucher)

History of Document



History of Document



History of Document

ANIMA!

draft-ietf-anima
Autonomic-control-plane
(ACP). At IESG.

draft-ietf-anima
Bootstrapping-keyinfra
(BRSKI). In RFC-editor Q

ANIMA!

PHB
Threshold
work

draft-richardson-secdispatch-
idevid-considerations
(vendor private CA
+ trust anchors)

draft-richardson-anima-
registrar-considerations
(enterprise private CA)

ANIMA?!

draft-richardson-anima-
masa-considerations
(vendor private CA + voucher)

Document
Split up

draft-richardson-anima-
masa-considerations
(voucher)

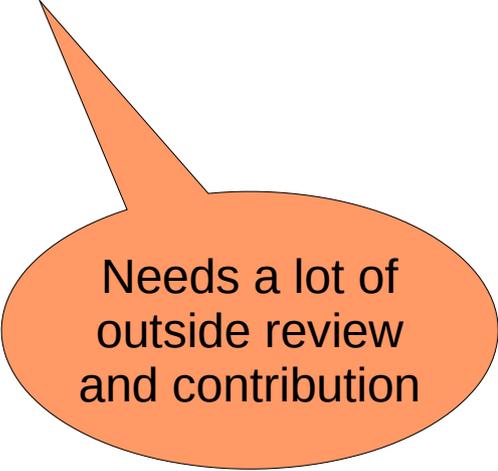
ANIMA?!

What to do?

- Supports work in:
 - SUIT
 - TEEP
 - RATS
 - ANIMA
 - LAMPS (CMP)
 - IPsecME, COSE, TLS,...
- But it is not even close to a protocol.
- Also not an applicability draft.
- It would be **referenced** by an applicability draft
 - Probably one in an outside SDO

What to do?

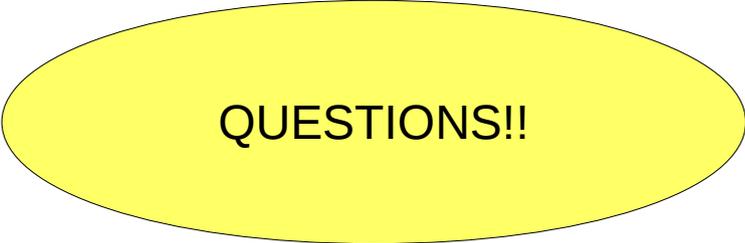
- Do it in SAAG?



Needs a lot of
outside review
and contribution

- AD sponsor

- Would not get enough
review



QUESTIONS!!

Useful Links

- IDevID discussions

- https://mailarchive.ietf.org/arch/msg/secdispatch/Hqe1IHG2wnW_9NxJLazEYbmGYN0/
- https://mailarchive.ietf.org/arch/msg/anima/-2Niz98BNSopDi4GpgxrDfl_Mdc/
- <https://mailarchive.ietf.org/arch/msg/anima/eMOH3NFbEDjZOi5gZgB9Ekl6yxw/>
- <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=xY5vs2WtIKM>

-

..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