Constrained voucher

`draft-ietf-anima-constrained-voucher-15`

Michael Richardson, Peter van der Stok,
Panos Kampanakis, Esko Dijk

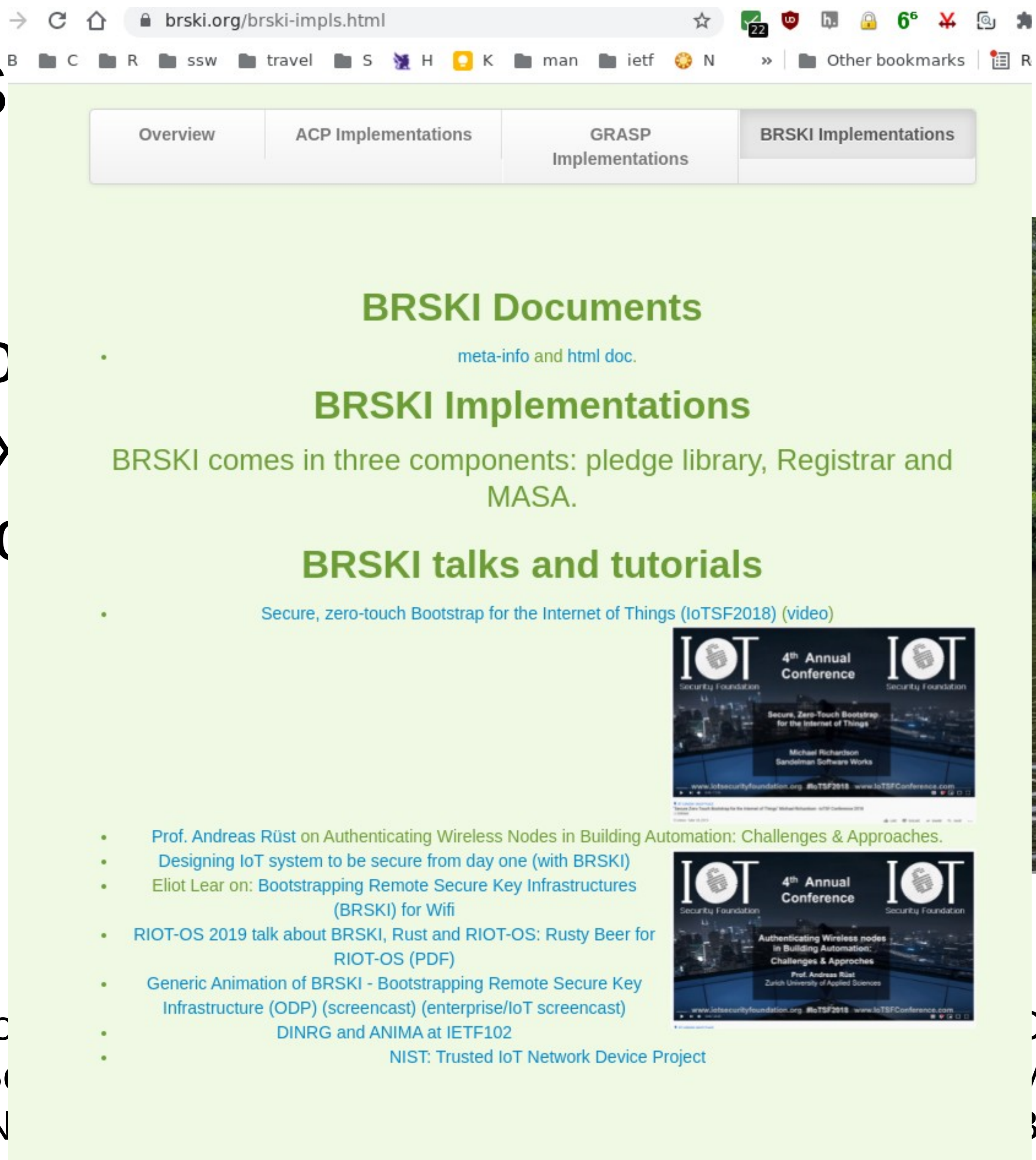
IETF 113
ANIMA Working Group

Constrained Voucher

BRS

This

- co
- Ex
- Co



BRSKI Documents

- meta-info and html doc.

BRSKI Implementations

BRSKI comes in three components: pledge library, Registrar and MASA.

BRSKI talks and tutorials

- Secure, zero-touch Bootstrap for the Internet of Things (IoTSF2018) (video)
- Prof. Andreas Rüst on Authenticating Wireless Nodes in Building Automation: Challenges & Approaches.
- Designing IoT system to be secure from day one (with BRSKI)
- Eliot Lear on: Bootstrapping Remote Secure Key Infrastructures (BRSKI) for Wifi
- RIOT-OS 2019 talk about BRSKI, Rust and RIOT-OS: Rusty Beer for RIOT-OS (PDF)
- Generic Animation of BRSKI - Bootstrapping Remote Secure Key Infrastructure (ODP) (screencast) (enterprise/IoT screencast)
- DINRG and ANIMA at IETF102
- NIST: Trusted IoT Network Device Project

IoT Security Foundation
4th Annual Conference
Secure, Zero-Touch Bootstrap for the Internet of Things
Michael Richardson
Sandelman Software Works
IoT Security Foundation
4th Annual Conference
Authenticating Wireless nodes in Building Automation: Challenges & Approaches
Prof. Andreas Rüst
Zurich University of Applied Sciences
www.iotsecurityfoundation.org #IoTSF2018 www.IoTSFConference.com

s

EST: Enro

BRSKI: Bo

SID: YAN

SE: CBOR Signing and Encryption (RFC 8152)

MS: Cryptographic message Syntax (RFC 5652)

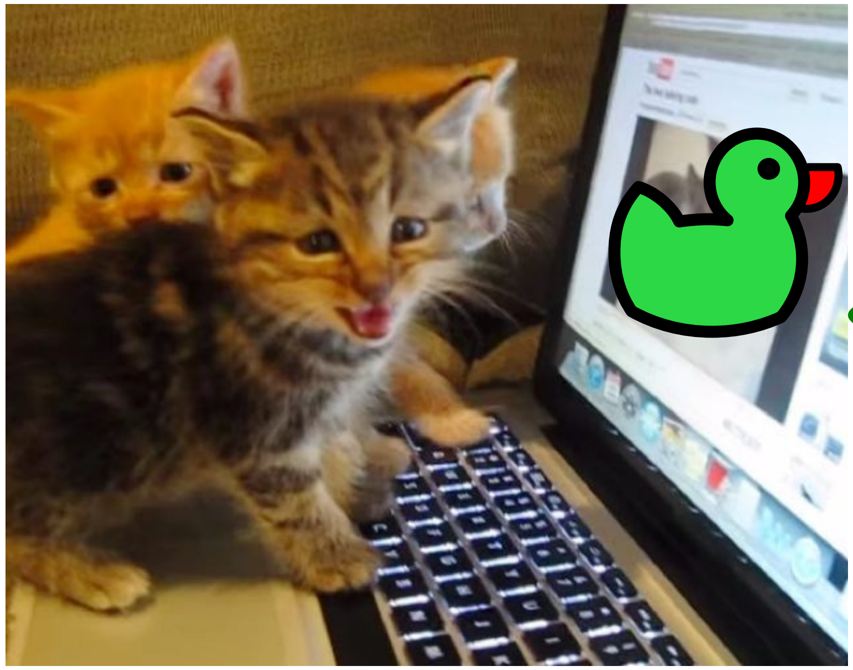
OR: Concise Binary Object Representation (RFC 7049)

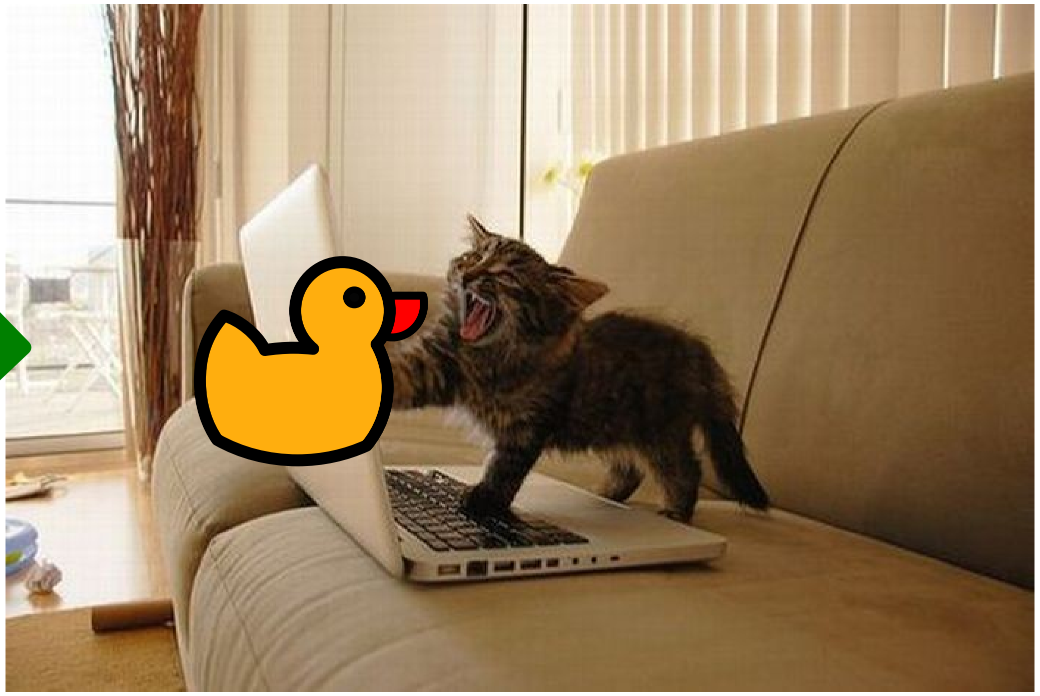
Changes since IETF112

- https://www.ietf.org/rfcdiff?url1=draft-ietf-anima-constrained-voucher-14&url2=draft-ietf-anima-constrained-voucher-16
- Many small edits
  - IANA fixes
- Fixes to examples.
- Added table for mapping of assertion values to integers (not strings)
- Interop efforts

Hackathon Results

- IETF113 interop testing, online and via IETF VPN. In the weeks up to meeting.
- Participants: Esko (IOT-Consultancy), Peter, Michael (Sandelman), Thomas (Siemens),
  - Will repeat at next Hackathon, but also participants want to continue between events.
  - IETF L2 VPN (used)
- Same cats as last time, different bugs





List of Hackathon Issues (1)

- Still need **Early Allocation of TBD3** - previous efforts used 65502 (private use value) for Content-Format

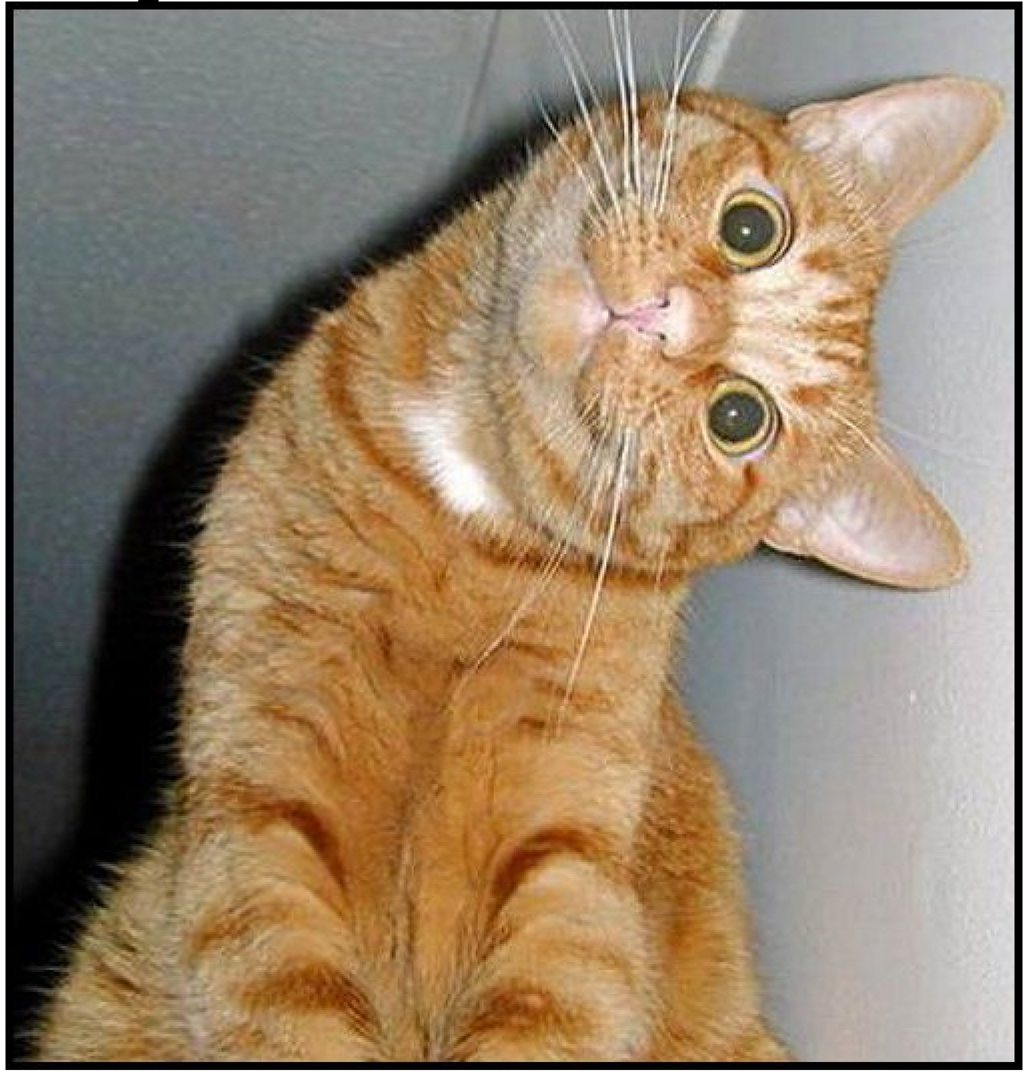
- **SNI must be used for Registrar/MASA connection**
- **still have to get AuthorityKeyIdentifier correct for IDevID**
-

Much external distraction to participants

- **in-room, right-now, right-here work is superior to vague on-line efforts**

Discussion
Ready for WGLC!

-



Thanks to weekly discussions in BRSKI design team on Thursday
Will resume in April