

Jan. 19th, 2022

Online

@FuTURE Forum

Qualcomm

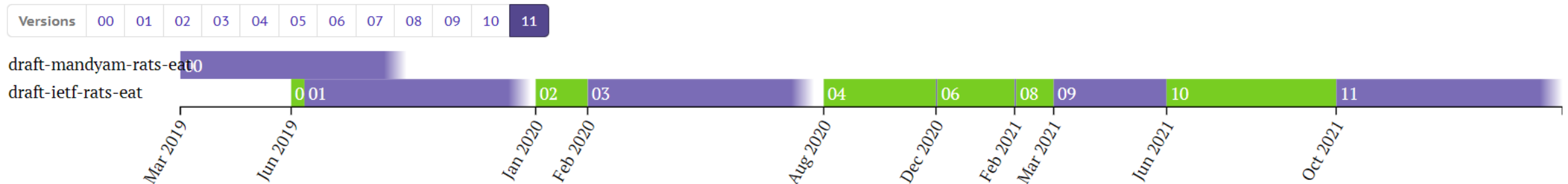
Updates on IETF EAT

Zhimin Du Ph.D.

Director, Technical Standards
Qualcomm

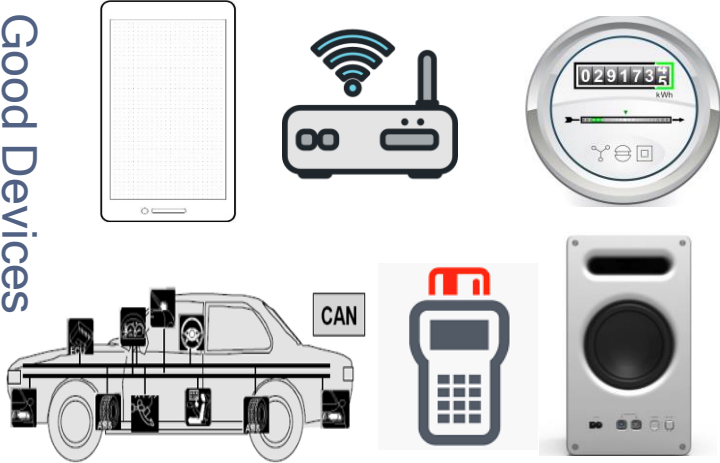
IETF EAT Standardization Progress

- EAT is a standards-track I.-D. in the IETF Remote Attestation Procedures (rats) Working Group

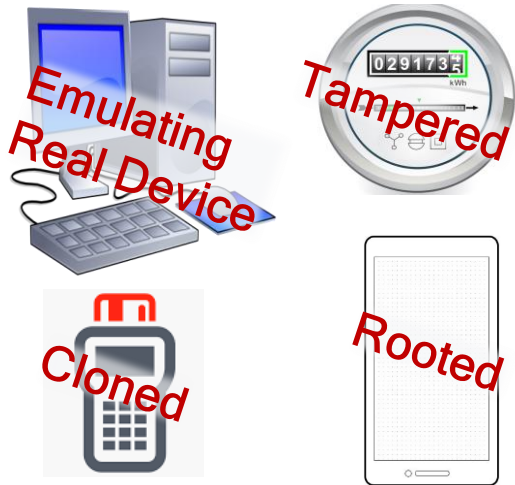


- In WG Last Call state
- Core function
 - An Entity Attestation Token (EAT) provides a signed (attested) set of claims that describe state and characteristics of an entity, typically a device like a phone or an IoT device. These claims are used by a relying party to determine how much it wishes to trust the entity
- EAT profiles have also been created
 - ARM PSA Token - <https://tools.ietf.org/id/draft-tschofenig-rats-psa-token-05.txt>
 - QWES Token - <https://tools.ietf.org/id/draft-mandyam-rats-qwestoken-00.txt>
- Open issues, public review comments and open-source implementation being tracked in GitHub
 - <https://github.com/ietf-rats-wg/eat/>

Good Devices



Bad Devices



Entity Attestation Token

- Chip & device manufacturer
- Device ID (e.g. serial number)
- Boot state, debug state...
- Firmware, OS & app names and versions
- Geographic location
- Measurement, rooting & malware detection...

All Are Optional

Cryptographically secured by signing



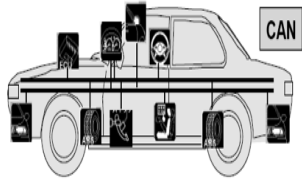
Banking risk engine



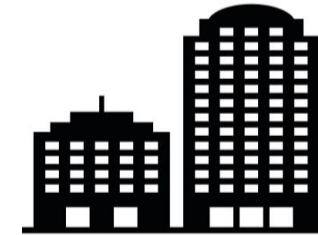
IoT backend



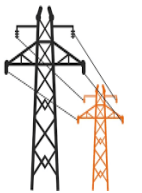
Network infrastructure



Car components



Enterprise auth risk engine



Electric company

EAT: Core Designs

- **Overall**

- An extensible and crypto-agile container for transporting Claims about a device state
 - Use Certificate or directly Private/Public Key pairs
- Built on the IETF CDDL (Concise Data Definition Language) over IETF COSE (CBOR Object Signing and Encryption) or JSON data structures standards
- Inherits from CWT (CBOR Web Token) claims, later also adds JWT claims
 - IANA administers claim definitions and numbering for both specifications

- **Claims**

- Token ID, Timestamp, Nonce, Universal Entity ID, Origination, OEM ID, Security Level, Boot State, Location, Age, etc.
 - All optional
- Also extensible to add in other claims
 - Via CWT or JWT registry through IANA

EAT Adoption in Other SDOs





- Baseline attestation solution for FIDO Device Onboard (FDO)
 - <https://fidoalliance.org/specs/FDO/fido-device-onboard-v1.0-ps-20210323/fido-device-onboard-v1.0-ps-20210323.html>
- GlobalPlatform has adopted EAT for TEE's EntityAttestation API

EAT Commercialization

- All products requiring support for Alexa Voice Services (AVS) require EAT support
 - This is due to requirement for PSA Certification - TOE (target-of-evaluation) must be attestable either via EAT token or PSA token
- QCC 710, targeted to Electronic Shelf Label (ESL) market, supports EAT in the device onboarding protocol
 - Mutual attestation between device owner (cloud service “Mgmt. Entity” - ME) and ESL device
- QC WES (Qualcomm Wireless Edge Services) remote attestation solution is EAT-compliant
- All products supporting ARM Trusted FW (ATF) for TrustZone support ARM PSA Token out of the box
 - PSA Token is EAT compliant
 - <https://community.arm.com/arm-community-blogs/b/internet-of-things-blog/posts/how-psa-apis-will-enable-secure-devices-and-a-consistent-developer-experience>



Thank you

Follow us on:    

For more information, visit us at:

www.qualcomm.com & www.qualcomm.com/blog

All data and information contained in or disclosed by this document is confidential and proprietary information of Qualcomm Technologies, Inc. and/or its affiliated companies and all rights therein are expressly reserved. By accepting this material the recipient agrees that this material and the information contained therein will not be used, copied, reproduced in whole or in part, nor its contents revealed in any manner to others without the express written permission of Qualcomm Technologies, Inc. Nothing in these materials is an offer to sell any of the components or devices referenced herein.

©2018-2021 Qualcomm Technologies, Inc. and/or its affiliated companies. All Rights Reserved.

Qualcomm is a trademark of Qualcomm Incorporated, registered in the United States and other countries. Other products and brand names may be trademarks or registered trademarks of their respective owners.

References in this presentation to "Qualcomm" may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable. Qualcomm Incorporated includes our licensing business, QTL, and the vast majority of our patent portfolio. Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of our engineering, research and development functions, and substantially all of our products and services businesses, including our QCT semiconductor business.