### **EAT Draft Status and Discussion**

Laurence Lundblade

IETF 109 November 2020

### Proposed Contents of an EAT

#### **HW Identification**

OEM, model, version... Unique device identification

### SW Identification - CoSWID

Author, package, version... Measurement

#### Security Characterization High-level OS, TEE, secure element, TPM...

#### Running State Boot and debug state

### Measurement of Running SW

Runtime integrity check

#### Nonce and Timestamps Freshness, prevent replay

Identify Verifier Input Endorsements, key ID, reference values...

Context, Purpose, Profile Intended use cases

### Submodules

HW subsystems, TEE, SW process and apps...

#### Nested EATs One signed EAT inside another

#### Public Keys Attestation of private key stored on the device

**GPS** Location

# Level of Completion in EAT Draft

HW Identification

OEM, model, version...

Unique device identification

Author, package, version...

Measurement

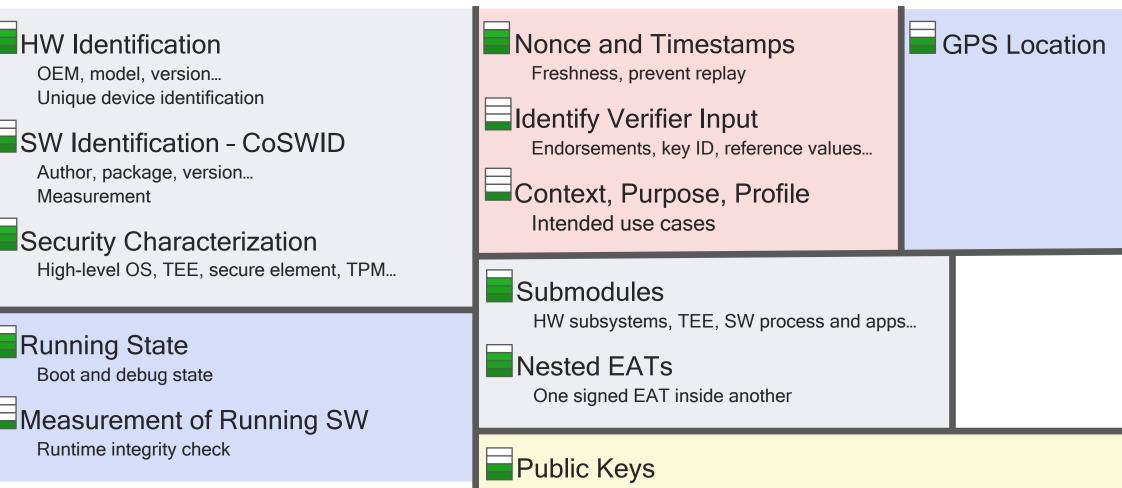
**Running State** 

Boot and debug state

Runtime integrity check

Ready for last call, no open issues

- Near completion, reviewed
- Draft text
- Proposed, Interest in



Attestation of private keys on the device (e.g., Android key store)

### Other EAT Work

- Rework introduction and related with respect to RATS Architecture
  - Use Architecture terminology: "Attester", "Verifier"...
  - $\,\circ\,$  Remove most of the architecture-related text currently in EAT
- More examples
- Should a verification procedure be included?

### Discussion: EAT use for Attestation Results

- · Clear interest and consensus that EATs can be used for attestation results
  - CWT, JWT and UCCS formats all useful
- EAT draft must discuss use as Attestation Results
  - Perhaps only briefly
- Many EAT claims will pass through the Verifier into Attestation Results
  - Reuse as many claims as possible
  - Don't define new variants of EAT claims in Attestation Results
    - If existing EAT claims aren't right for Attestation Results, let's fix the EAT claims
- New "claims" for Attestation Results are needed
  - Overall success of verification
  - Results of checking claims against reference values
    - SW and HW version, measurements...
  - Certifications received by the Attester
  - Other?
- Should new Attestation Result claims be in EAT document or elsewhere?

## Discussion: Work on Identifying Verifier Input

- Add discussion on key identification to EAT draft
  - By COSE kid
  - By COSE X509 draft (include certs, identify certs by thumbprint, URL for certs)
  - Using claims like UEID
- Add definition of COSE Header Parameters to identify Endorsements
  - Thumbprint / opaque bytes as identifier
  - URL
  - Will not define format or content type for Endorsements
- Add definition of COSE Header Parameters to identify Reference Values
  - Thumbprint / opaque bytes as identifier
  - URL
  - Will not define format or content type for Reference Values

## **Discussion: Public Key Inclusion**

- FIDO, IoT onboarding and Android Attestation all include public keys in Attestation Evidence
  - $\,\circ\,$  Critical to the use cases
- Proposed text in pull request
  - Keys SHOULD be in COSE\_Key or JWK format
  - Use cases should define claims for their particular semantics for the key
  - Can use RFC 8747 Confirmation Claim
    - · Semantics of Confirmation Claim in an EAT are not defined; left up to use case
- Possible information about security level of key protection
  - High-level OS, TEE, secure element
  - Biometric authentication to use a key
- Possible information about intended use of key

### Discussion: Context, Purpose, Profile

- ARM PSA defines a profile claim
  - String names a profile document to which the EAT complies
  - $\circ$  Could this be combined with Endorsements? A profile ≈ endorsement?
- Qualcomm QWES Token defines a Context Claim
  - On-demand, Registration, Provisioning, Certificate Issuance, Proof-of-possession

## **Discussion: Measurement of Running State**

- Example (e.g. Samsung TIMA)
  - TEE periodically measures high-level OS at run time
  - Results are evaluated:
    - In TEE and a claim just indicates success or failure
    - TEE sends measurements to Verifier that evaluates results
- More valuable than measurement only once at boot
  - Especially when devices run for months without a reboot in a place very far away
- Can CoSWID report measurements?
- Need new claims would be needed for reporting results evaluated by the device