EAT Update

Laurence Lundblade

IETF 113 March 2022
Planned Contents of an EAT - The Claims

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, profile claim

GPS Location

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

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

Nested EATs
- One signed EAT inside another

Formal Device Certifications
- For example, Common Criteria certification; format is GP’s DLOA

Results Codes
- Overall Verification Results, Measurement Results
Level of Completion in EAT Draft

- **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, profile claim
- **GPS Location**
- **Submodules**
  - HW subsystems, TEE, SW process and apps...
- **Nested EATs**
  - One EAT inside another, Detached Bundles
- **Formal Device Certifications**
  - For example, Common Criteria certification; format is GP’s DLOA
- **Public Keys**
  - Attestation of private keys on the device (e.g., Android key store)
- **Result Codes**
  - Overall Verification Results, Measurement Results

• Ready for last call, no open issues
• Near completion, reviewed
• Draft text
• Proposed, Interest in

Progress & change since IETF 112. In draft -12
Important changes in the -12 draft (since IETF 112)

- Use normative language consistently
- Better definition of “entity”
- Lots of wording improvements
- Added HW Model claim
- Added boot odometer claim
- Added privacy considerations for replay protection
- Make HW Version one claim instead of three (3 were for chip, circuit board and device)
- Fill in IANA section with descriptions of all claim registrations (both early allocation and standard allocation)
Improved grouping of claims (PR #171)

- Claims about the entity
  - Identity – HW OEM, Model, Version, UEID, SUEID
  - Running state – debug and boot status, uptime, boot odometer
  - Composite devices – submods and token nesting
  - SW Manifests
  - Measurements and measurement results
  - Certification
  - Attestation results code(s)

- Claims about the token
  - Profile
  - Intended use
  - Time stamp
  - Nonce and Freshness
  - Recommendations for including public keys
Work in the EAT queue

- Complete the CDDL
  - Use JC<> CDDL generic to ease definitions that vary between CBOR and JSON
  - A few bug fixes
- Rearrange sections to group claim definitions better
Topics Requiring Work Group Consensus

◦ Resolve relationship to UCCS (Separate Presentation)
◦ Resolve security-level claim
◦ Attestation Results
  ◦ EAT’s role in AR
  ◦ A separate profile document?
  ◦ Add general result code?
  ◦ Relation to ar4si