Entity Attestation Token (EAT)

Laurence Lundblade

July 2018

Good Devices CAN

Emulating Real Device Rooted

W

ad 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







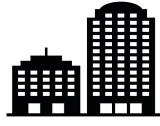
IoT backend



Network infrastructure

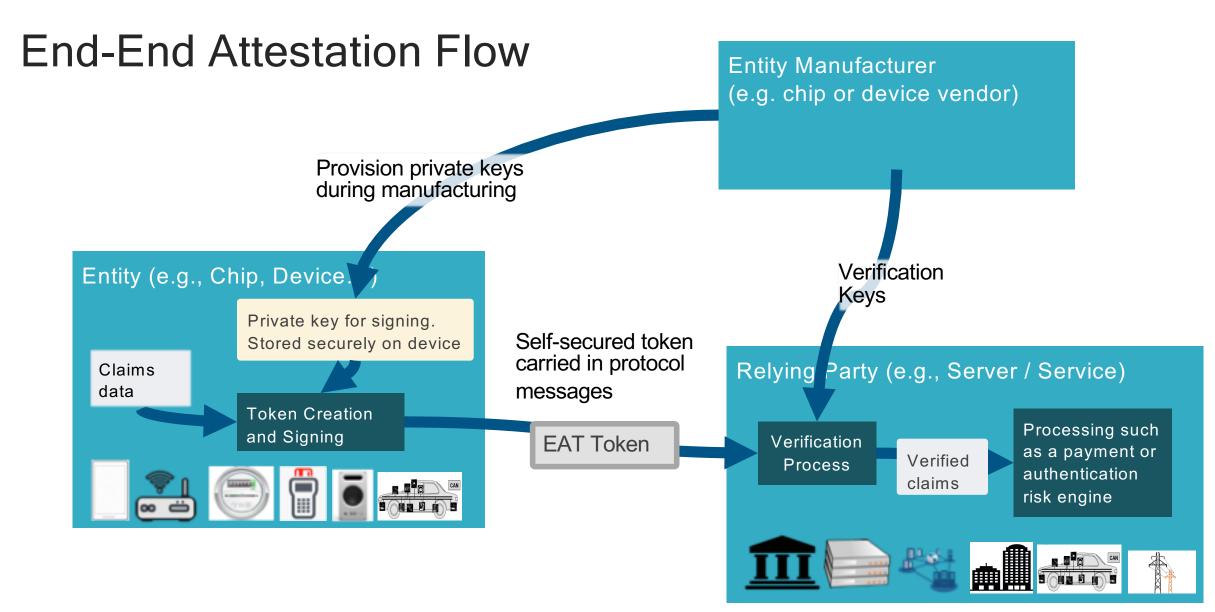


Car components



Enterprise auth risk engine Electric company





Other flows are possible where verification is done by a service or by the entity vendor.

EAT Format

Overall structure: COSE_Sign1

otecter eaders Algorithm -- Examples: ECDSA 256, RSA 2048, ECDAA

Signing Scheme -- Examples: IEEE IDevID, EPID, X.509 Hierarchy

inprotecte headers Key ID -- identifies the key needed to verify signature

Certs (optional) -- to chain up to a root for some signing schemes

Signed payload

- · CBOR formatted map of claims that describe device and its disposition
- Few and simple or many, complex, nested...
- · All claims are optional -- no minimal set
- The format and meaning of a basic set of claims should be standardized for interoperability
- Should be adaptable to cover many different use cases from tiny IoT devices to complex mobile phones
- Privacy issues must be taken into account

sig

signature -- Examples: 64 byte ECDSA signature, 256 byte RSA signature

- COSE format for signing
- Small message size for IoT
- Allows for varying signing algorithms, carries headers, sets overall format

- CBOR format for claims
- Small message size for IoT
- Labelling of claims
- Very flexible data types for all kinds of different claims.
- Translates to JSON
- Signature proves device and claims (critical)
- Accommodate different end-end signing schemes because of device manufacturing issues
- Privacy requirements also drive variance in signing schemes

Similar and Related Technologies

Technology	Use Case
FIDO Attestation	Attestation of FIDO Authenticator implementations
Android Key Store	Attestation key pairs in the key store
NEA	Collect and send endpoint security posture (e.g. anti-virus SW state and config) to enterprise collection / monitoring point
RATS / NSF	Attestation / Measurement of SW on Network Security Functions (e.g., firewalls)
TPM	Attestation / Measurement of SW running on a device
BRSKI / Zero Touch	Authenticates IoT devices for enrollment in IoT management system

More Info

- Non-WG mailing list: eat@ietf.org
- Mail list info: https://www.ietf.org/mailman/listinfo/EAT
- Draft document: https://tools.ietf.org/html/draft-mandyam-eat-00
- Github: https://github.com/eat-ietf-wg