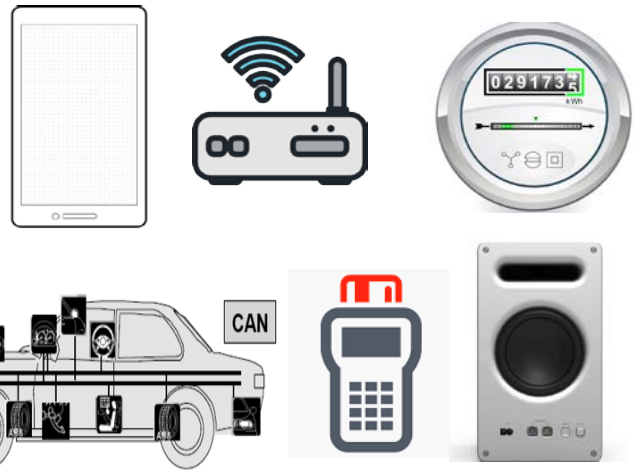
Entity Attestation Token (EAT)

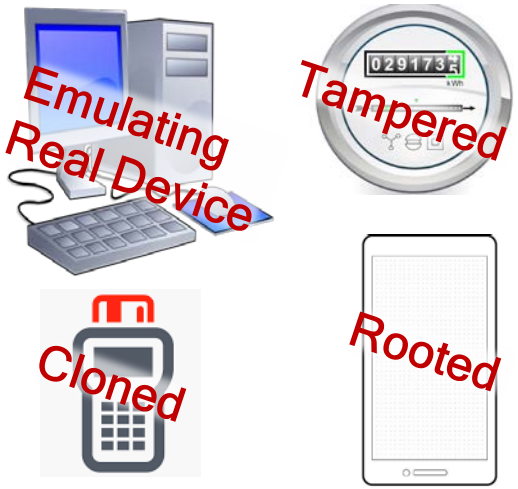
Laurence Lundblade

July 2018

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…

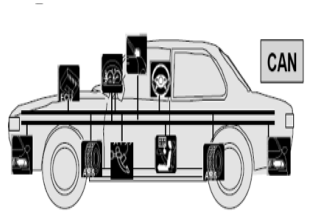
All Are Optional

Cryptographically secured by signing

Banking risk engine

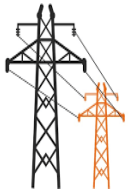
IoT backend

Network infrastructure



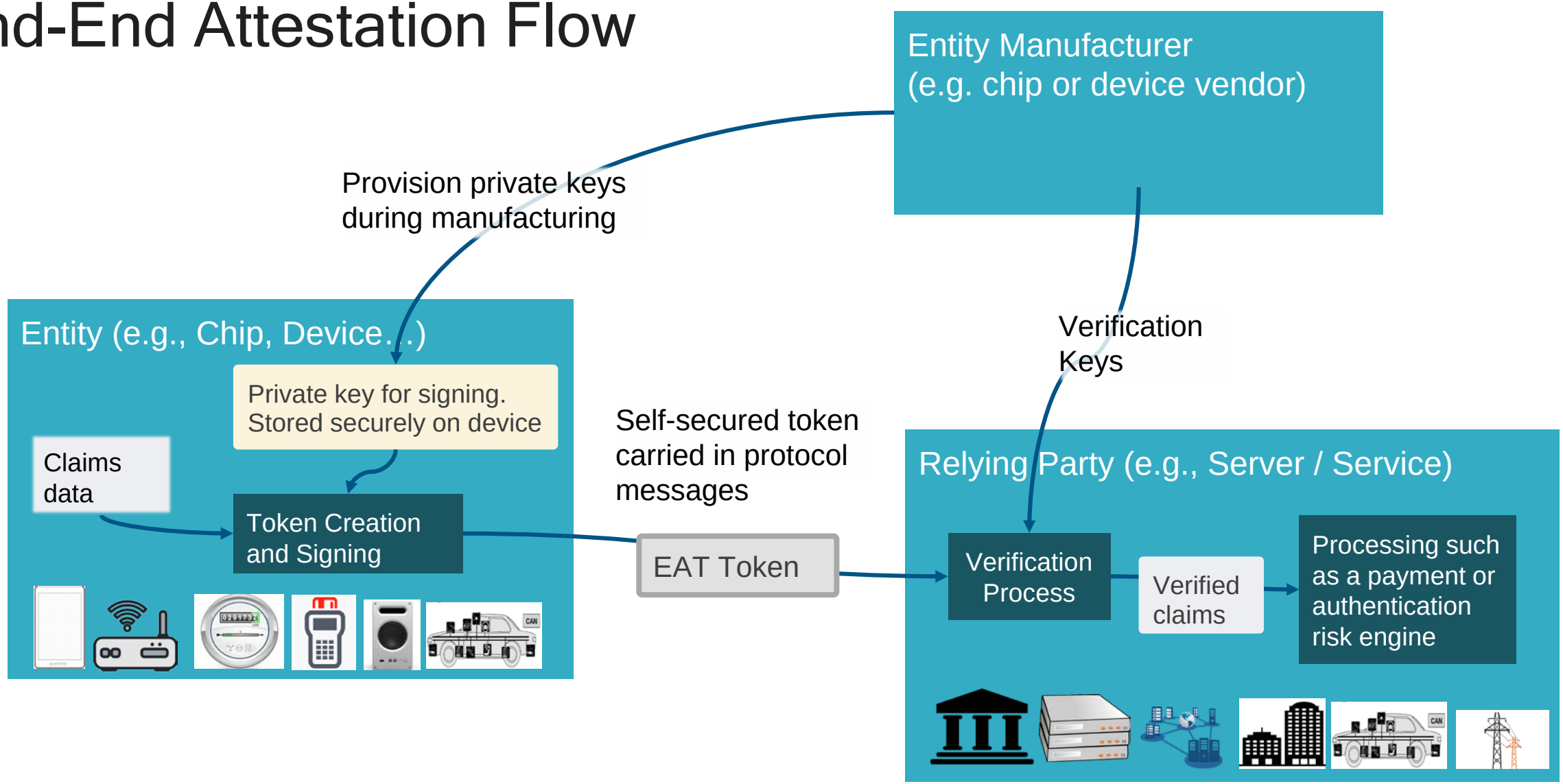
Car components

Enterprise auth risk engine



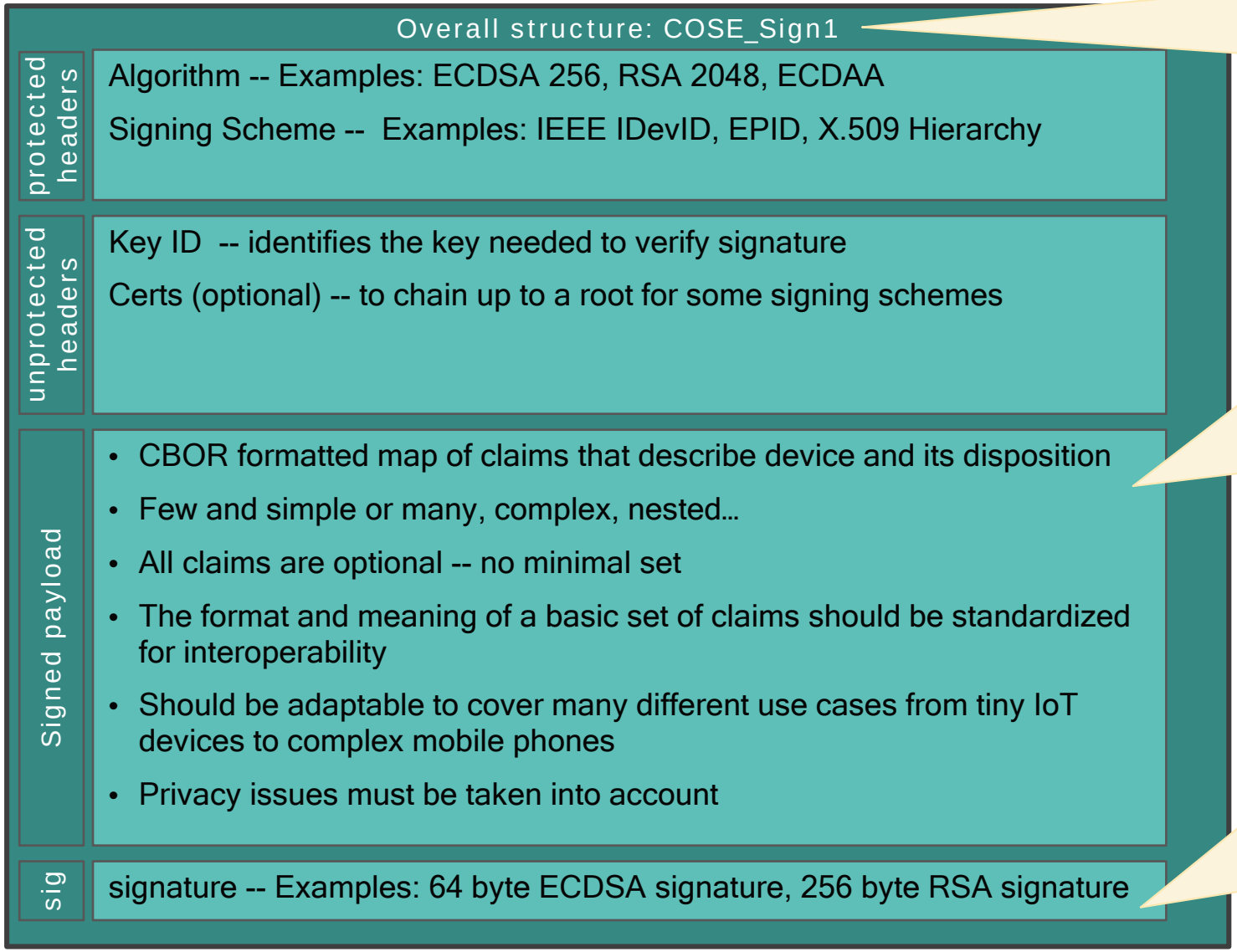
Electric company

End-End Attestation Flow



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

EAT Format



- 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