Certicom's Vision

- Authenticate <u>everything</u>
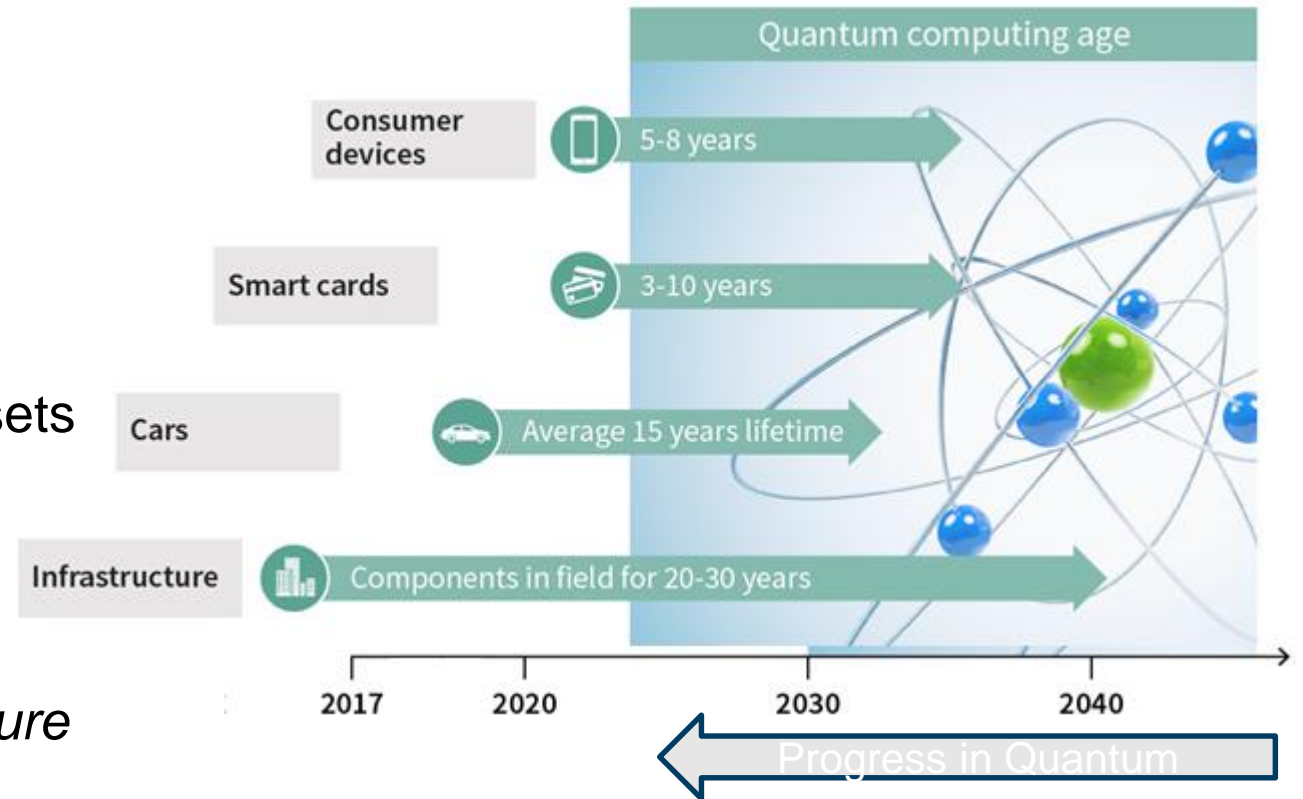
- Within the vehicle: any device on any bus
  - Component authentication
  - Message integrity validation
  - Gateway key master supports multiple protocols & session key rules

- External connections
  - Validate diagnostics & service requests
  - Secure V2X messages

- External services
  - Extend to vehicle attestation
  - Ensure your vehicle is <u>not</u> the weakest link

Instrument cluster
Body ECU
Driver seat control
Engine ECU
Head unit
Restraint control ECU
Data link
Rear view camera
TPMS ECU
Side obstacle detection ECU
Driver door control
Parking aid module
Telematics box
Keyless entry ECU

https://technology.ihs.com/Services/420404/teardown-automotive-intelligence-service
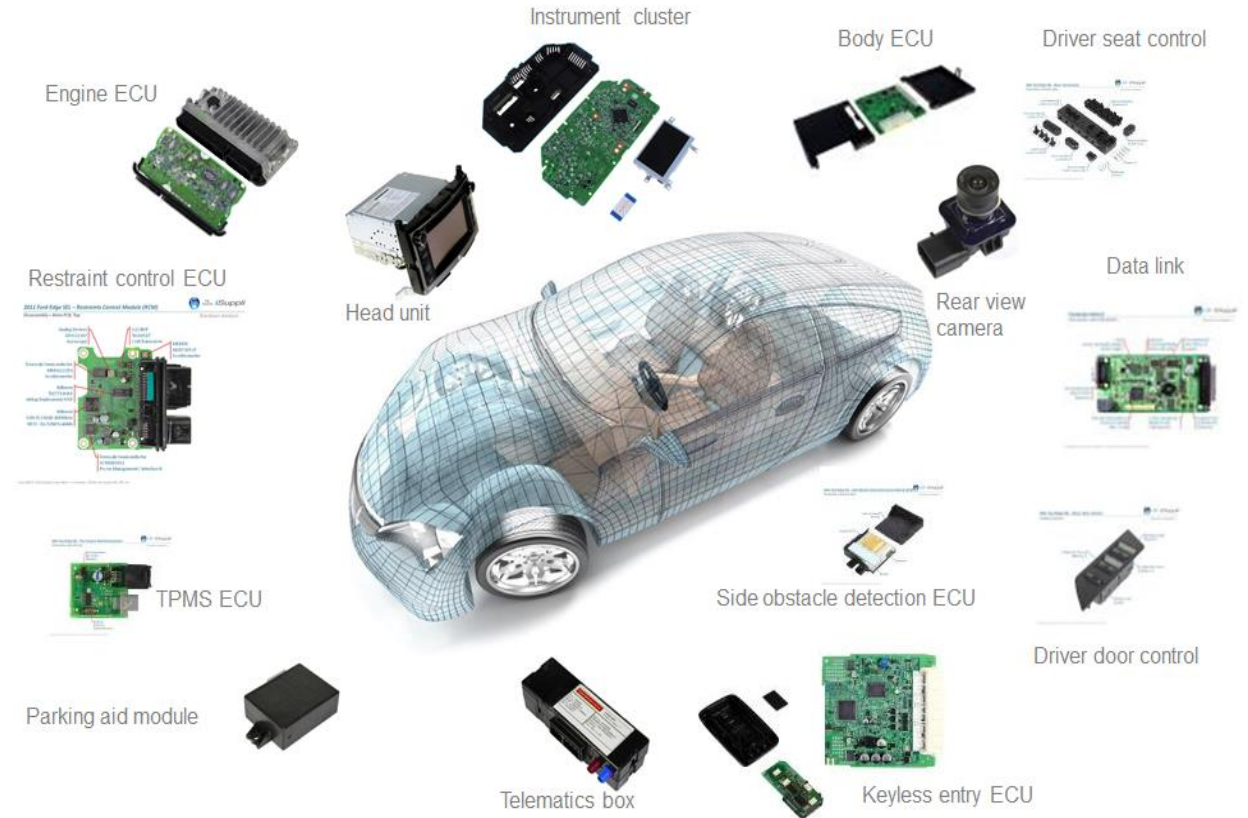
Recently Announced: Quantum-Safe Signing Appliance

- Quantum Attack Resistant Code Signing
  - *Used to overcome limitations of classical public key cryptosystems*
  - *Can sign QNX & Linux filesystem images, RTOS & firmware images for secure boot*
  - *Also supports traditional cryptosystems, signing & encryption key management*

- Ideal for industries deploying long-lived assets
  - *Application processors & MCUs*
  - *Mil-Aero Systems*
  - *Smart Grid/Critical Infrastructure*
  - *Automotive & Transportation Infrastructure*
  - *Telecommunications Infrastructure*

- Product availability: November 2018

Quantum computing age

Consumer devices — 5-8 years

Smart cards — 3-10 years

Cars — Average 15 years lifetime

Infrastructure — Components in field for 20-30 years

2017   2020   2030   2040

Progress in Quantum

IBM says 5 years away from a practical machine