AVL List GmbH (Headquarters)

Impulse statement: Quantum Cryptography and Connected Cars

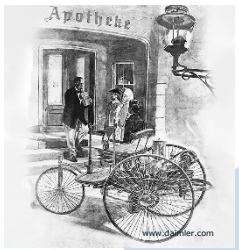
Quantenforschung und -technologien: Potenziale für Wirtschaft und Wissenschaft

21. December 2017

Ma, Zhendong

Innovation in mobility

5000
years



1886

1996

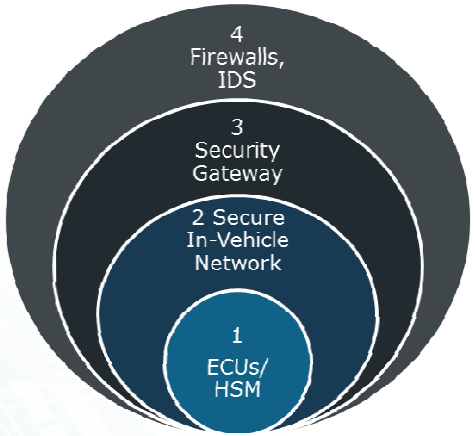
2000

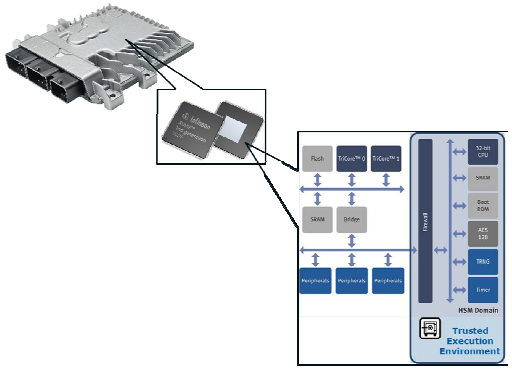
2006

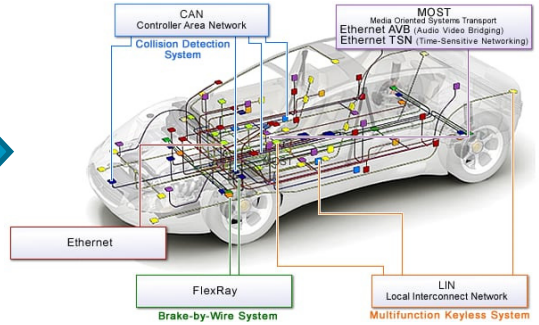
CARTALK.

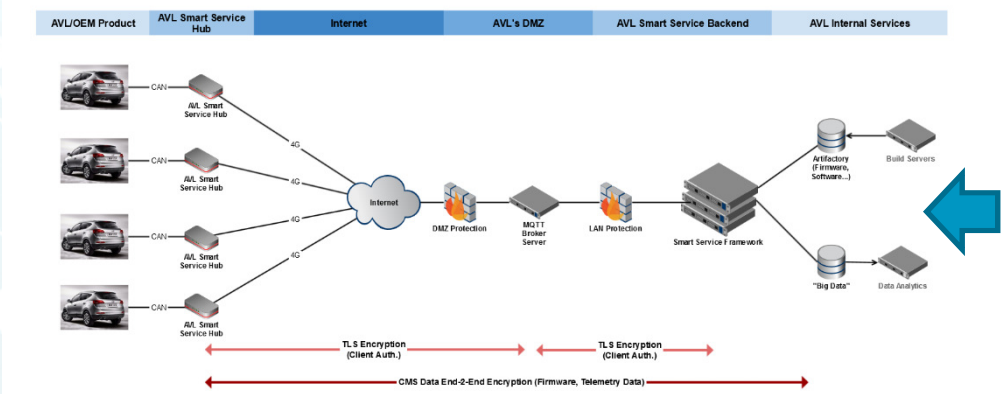
Cadillac Offers A High-tech Guardian Angel

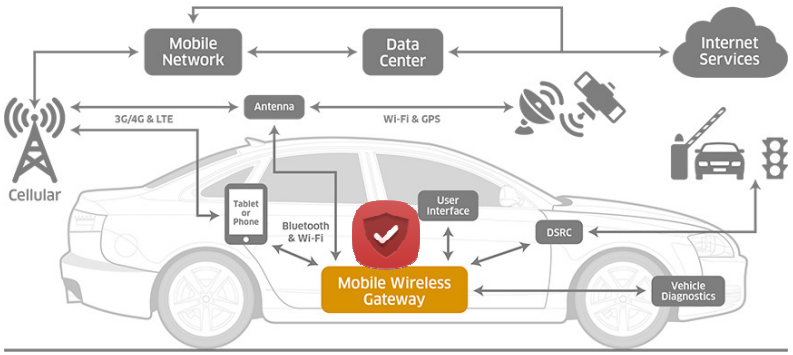
Cybersecurity of connected cars











http://telematicswire.net

Cybersecurity in post-quantum era

- Post-quantum cryptography

Cryptographic algorithm	Type	Purpose	Impact from Quantum Computing
AES	symmetric key	encryption	larger key sizes (double key size)
SHA-2, SHA-3	hash	hash function	larger output (double the key size)
RSA	public key	signature, key establishment	no longer secure
ECDSA, ECDH	public key	signature, key exchange	no longer secure
DSA	public key	signatures, key exchange	no longer secure

- Cryptographic longevity and agility
- Evidence of known attack on existing cryptographic algorithms
- Security concept taking into account post-quantum cryptography
  - Quantum-resistant cryptographic algorithms
  - How to design security that is able to cope with post-quantum cryptography?
  - How to ensure security in a car‘s lifetime?
  - How to (securely) update/upgrade in-vehicle security-critical modules?


Thank You
AVL
www.avl.com