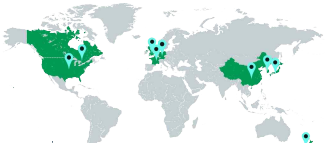
TRUSTONIC

# Designing Security into the heart of your Electric Vehicle

# TRUSTONIC
## Who We ARE

- Founded by ARM & Gemalto in 2012, **now an EMK Capital portfolio company**
  - Focused on accelerating Trustonic's growth
- Deployments in 17m+ vehicles on-road
  - IVI, Connectivity, Telematics,
  - Zero breeches
- Global operations and support



**2 BN** Devices

**120** Patents

**40M+** Vehicles

### GLOBAL CUSTOMERS AND PARTNERS

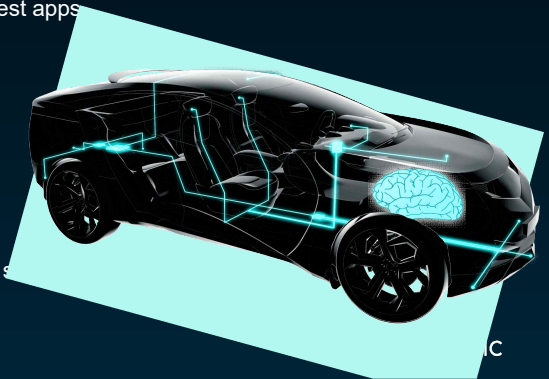
Audi · Porsche · Bentley · Volkswagen · Panasonic Automotive · DENSO TEN · APTIV · HARMAN · LG · JET OPTO · SAMSUNG · MEDIATEK · RENESAS · Texas Instruments · NVIDIA

### HARDWARE BACKED SECURITY: TRUSTED EXECUTION ENVIRONMENT

EMVCo · Common Criteria · FIPS 140-2 · GlobalPlatform

# Software Defined Vehicles ➔➔➔ Cybersecurity Matters

- Autonomous and ADAS *mean* more sensors, actuators and compute power
- Customers expect voice, gestures, and latest apps
- New opportunities for revenue by entering "internet speed" innovation
- But – more software means more opportunities for hackers
- And enhanced connectivity makes attacks s




**775 million consumer vehicles**

will be connected via telematics or by in-vehicle apps by 2023

juniperresearch.com

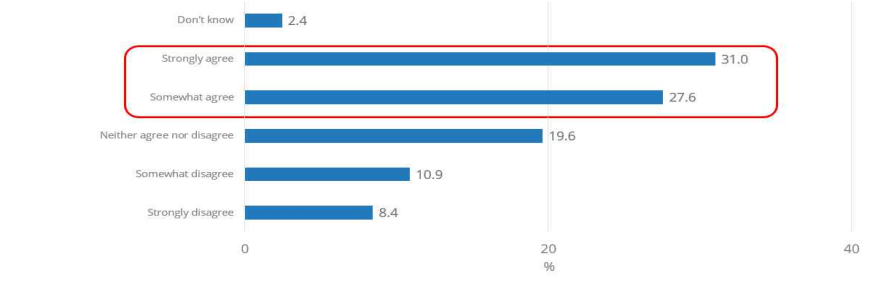
- Cybersecurity has become a consumer and industry focus – much like safety was in previous eras.
- Regulators have rightly demanded that Cybersecurity is taken seriously
- And lapses in Cybersecurity can damage reputations and cause customer harm as seriously as any safety mis-step

TRUSTONIC

# And the latest research highlights that consumer awareness is growing.

58.6% of Respondents Indicate That They Would Consider Paying a Premium for a Brand That Has Demonstrated Leading Cybersecurity Protection and Monitoring; As Vehicles Become More and More Networked and Software Defined, Cybersecurity Can Become a Potential Brand Differentiator

**Q28. Please rate your level of agreement with the following statement. I would be willing to pay a premium for a vehicle or automotive brand that has embraced, implemented, and demonstrated an industry leading level of cybersecurity protection and monitoring.**




n = 1,599
Source: IDC's 2021 U.S. Consumer Automotive and Transportation Survey on Current and Future Vehicle Technologies



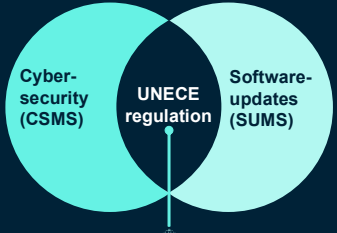


TRUSTONIC

# New Regulation means security is no longer optional

## Cyber-Security

- Manage vehicle cyber risks and design suitable mitigations
- Secure vehicle by design to mitigate cyber risks along the value chain
- Detect and respond to security incidents across the vehicle fleet




Applicable to 60+ countries

## Software-updates

- Provide safe and secure software updates and assure no harm/impact of vehicle safety

UNECE

**Mid 2020** Publication of final regulatory text

**Jul 2020** Mandatory for aut. Level 3-5 in Japan

**Jan 2022** Mandatory for new types in Japan

**Jul 2022** Mandatory for new vehicles types in EU

**Jul 2024** Mandatory for all new registrations in EU

2020 | 2021 | 2022 | 2023 | 2024

Expected dates ( web research, expert interviews)



TRUSTONIC

# Security Uses Case Are Expanding Rapidly

## Protecting assets

FROM

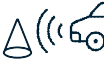
Immobilizer

DRM

## Pro-active management of security & value creation

TO

Secure OTA



V2X

Secure Charge

Privacy & Personalization

Trusted components

Telematics

# New Industry Business models assume security is built-in


## Sharing Economy

New vehicle ownership is declining, while ride share and rental models are growing

## Connected Car Services

OEMs want to monetize the vehicle data and also deliver paid -or premium services over time

## Pay To Play

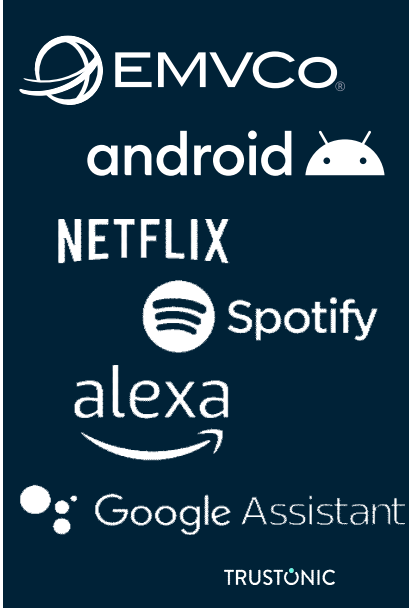
New monetization models for features, including in-vehicle software updates, streaming content services etc.



TRUSTONIC

# 3rd Party Solution Providers expect security as standard

- The payment industry has long set standards for its ecosystem, and in vehicle payments will have to follow existing rules
- Google sets stringent rules for Android security and certification.
- Amazon has recently strengthened security requirements for devices with Alexa capabilities including 3rd party evaluation.
- These requirements are all being set from industries outside of automotive, where automotive is just a small part of larger ecosystems with different expectations and timelines.
- These 3rd party brand holders have as much to gain (or lose) as Automotive OEMs. 3rd party requirements are here to stay.

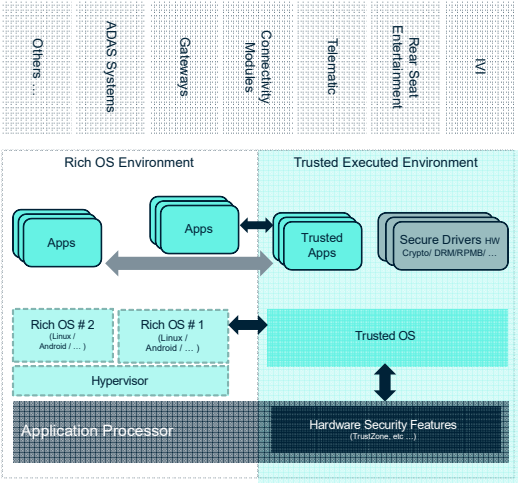


# TRUST IS EVERYTHING

**A Trusted Execution Environment (TEE)** provides a secure enclave to isolate and protect custom code and data by using a special mode of a regular Arm CPU

**Benefits include:**

- Hardware security with zero additional hardware, or hardware cost
- High performance with very large memory, enabling many applications beyond simple crypto
- Ability to run Trusted Applications (TAs) to encapsulate different functions
- Privileged access to ECU peripherals
- Hardware root of trust and attestation capabilities, enabling cloud services to identify and trust individual vehicles






TRUSTONIC

# Summary

Cyber security needs to be at the heart of the OEMs strategy

- “Electric” is not just about drivetrain, it is about a move to **software defined vehicles**
  - Meeting customers expectations shaped by constant mobile app releases and rapid service evolution.
- New opportunities and new risks mean that vehicle software will need **constant** updates.
  - Recall is not a scalable approach.
- There is no silver bullet
  - But technologies such as the Trusted Execution Environment can be used to provide strong security and necessary flexibility – for new service deployment and OTA updates of code, keys and algorithms.

# Thank You

Andrew Till
andrew.till@trustonic.com

TRUSTONIC