Dynamic Assurance of Vehicle Integrity

*“When you see vehicles in harsh conditions in the field for over 10 years, you are bound to see problems” (**NTHSA**)*

Challenge

ACCELERATE TIME TO MARKET

Rapid evolution of security risks (keeping up with the fast evolving threat landscape)

Growing competition from tech giants & new software driven OEMs (accelerating the pace of releases to keep up with the smart & connected features)

Continuous development and deployment mean more fragmentation and lack of standardisation.

MARKET ACCESS

Fragmented standards regimes.

For example, capabilities regulation for automotive cybersecurity is underdevelopment by EU and

METI & NHTSA are watching the work from WP29 in UNECE

How do you guarantee the integrity of the data coming out of the vehicle?

INCREASING COMPLEXITY & LIABILITIES

Systems are empowered with more critical and complicated operations e.g. autopilots for cars and planes.

Inevitable increase in potential liabilities for failure without demonstration that duty of care standards and procedures were in place and followed

COST OF RECALLS

increasing sophistication and capabilities of hackers and cyber attackers

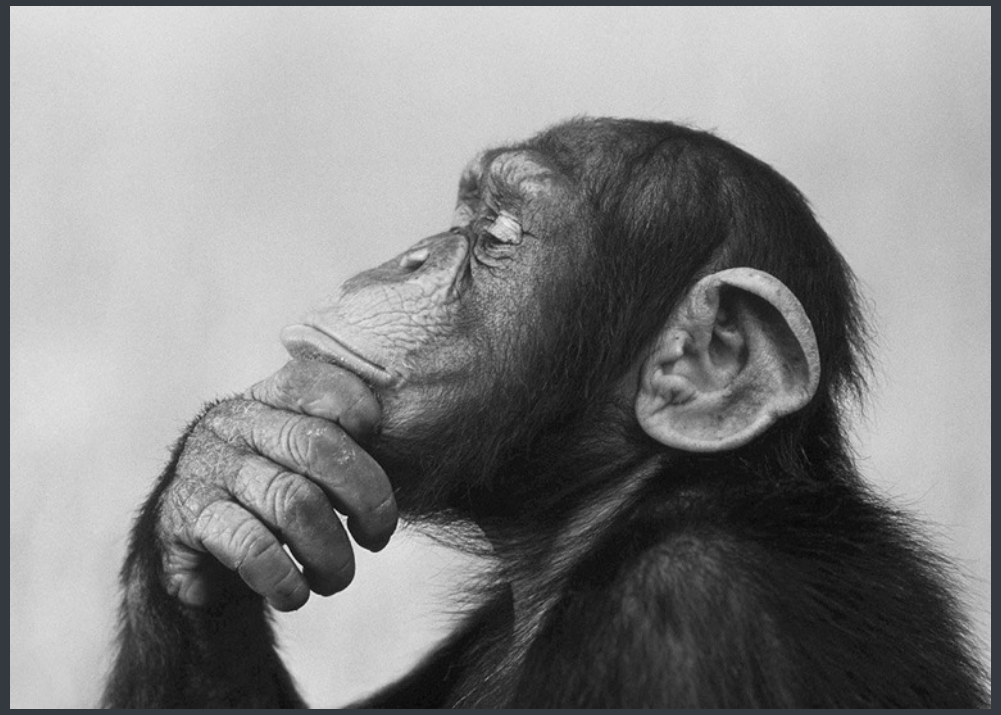
Bad publicity from recalls hurt a brand

Even with self certification, recalls are enforced and costly, driving demand for third party testing

Need Statement: Manage data integrity risk despite complex supply chain

HOW TO:

+ **Ensure my systems are in compliance?**
  With internal and external procedures, standards and traceability
+ **Ensure the software deployed matches the best standards?**
  For both home-grown software and that sourced from OED suppliers
  + **Ensure the Integrity of my Data & System?**
    Ensure software is up to date, not running malware, not hacked
  + **Identify products at risk after deployments?**
    In case of inevitable failure
+ **Provide post-incident analysis?**
  Mitigate legal risk - demonstrate I have taken reasonable steps



QUESTION:

Can I trust data coming from another organisation I don't have a business relationship with?

Manage cyber security risk in a cost efficient manner

Data compliance and dynamic integrity validation

- How can we track data integrity and software compliance from production throughout entire lifecycle (with FOTA /SOTA updates, ECU replacements, parts replacement)
- Vehicle has to comply with automotive regulations, so does mounted parts.
- How modifications/changes could be monitored and tracked?

Can a vehicle gain value over time?

Dynamic attestation of compliance provides trust in connected vehicles

Market access

+ **Ensure my systems are in compliance**
  Compliance data standards and security frameworks
  Supplier provenance tracking

Managing complexity

+ **Ensure the Integrity of my System?**
  Know your compliance, Trust your device, Trust your data
  Ensure single version of the truth (post incidence forensics)

Cost of recall

+ **Identify products at risk after deployments?**
  In case of malicious activity (including unauthorized update or unauthorized part replacement),
  in case of inevitable failure or unexpected behavior,
  in case of new vulnerabilities impacting certain components only

COMPLIANCE ATTESTATIONS

Compliance Attestation

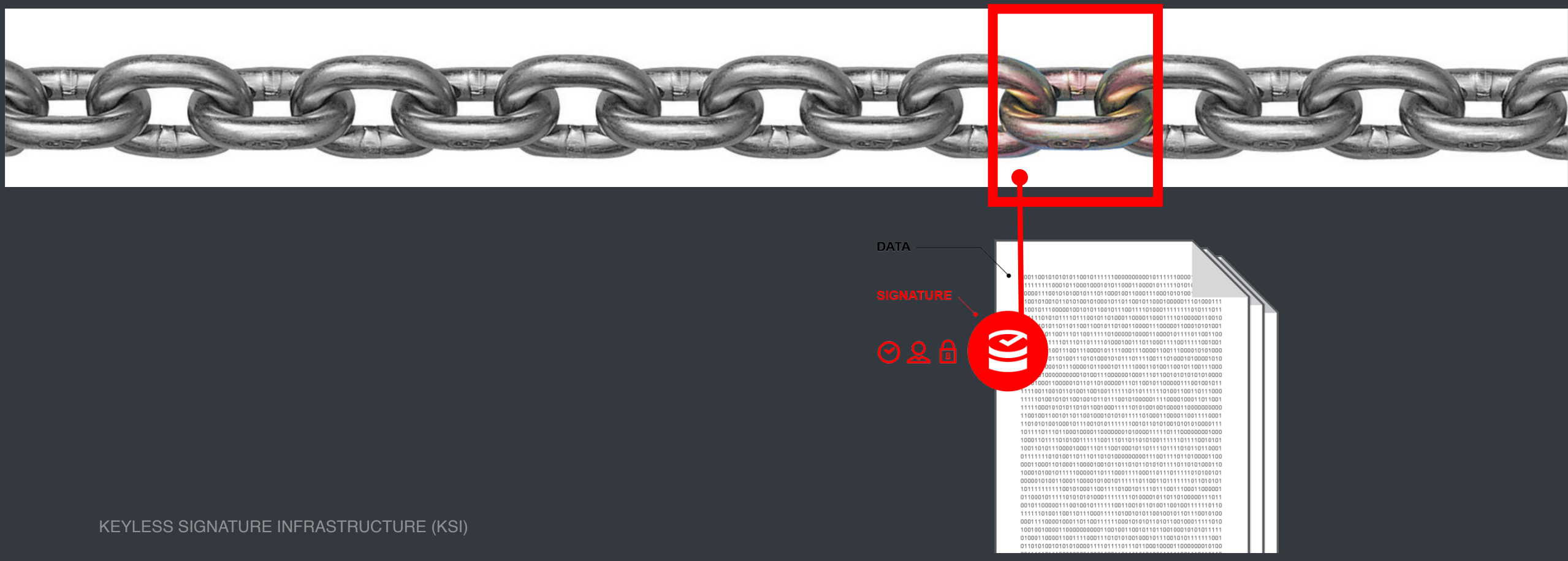
+ **Why?**
  Today, trust is build via business relationships (that may or may not include key management), going forward smart ecosystems are large complex puzzles where everything is connected and one need to find a way to trust strangers.
+ **What is it?**
  Provide visibility on your current (up-to-date) threats, risks and impacts.
  A mechanism to allow for various claims to be made or attested about an asset (code) produced by a third party.
+ **Why do we need it?**
  Manage the risk from suppliers, component and systems
  For critical systems, it allows a third party to make claims relating to the quality of the software it has released (e.g. standard)
  c.f. standards mark on physical asset.
  The owner may then rely on these attested claims as part of their dynamic risk analysis of the systems it is running.
+ **Trust**
  Attestation has signature from registration into the KSI blockchain
  Traceability for forensics.

Compliance Attestation Components

+ **Attestation**
  Claim of compliance status of asset (code) e.g.
  - **Compliant to "XXX" standard**
  - **Sourced to "YYY" developer**
  - **Tested**
+ **Cryptographically Signed**
  Attestation contains KSI signature which holds identity of attester, and time of attestation – cannot be denied.
+ **Immutable Link to Asset (Code)**
  Attestation contains code version information and Hash.
+ **Proof Mechanism**
  Attestation may contain a Hash of a Proof of Process or Evidence.
+ **Constraints**
  Attestation may contain constraints e.g. valid for 60 days.
  Process may be constrained (who can deliver update, which replacement parts are allowed, validated the integrity of my system).
  Monitor and report on the threat landscape and rate their risk.

Keyless Signature (blockchain)

KSI Blockchain provides a tagging system for electronic data: Keyless Signature.
These signatures prove the time, integrity and provenance (human or machine) of the data without relying on trusted third parties, public/private keys or credentials



What Can a KSI Signature Prove?

Hash - Data is signed by cryptographically linking a KSI signature to the data.

Participate - The data's signature is cryptographically linked in a chain

Verify - The KSI Blockchain provides a distributed Trust Anchor

Verifying the signature allows one to assert:

- Signing time: when was the data signed
- Signing entity: who signed the data
- **Data integrity**: the data has not been changed since signing