DEVICE AUTHORITY

Securing the Automotive Supply Chain:
Establishing Trust in a Software-Defined Ecosystem

Tyler Gannon

Key Challenges Facing the Automotive Supply Chain

Complexity. Connectivity. Risk.

Trust can't be assumed—It must be established.

1. FRAGMENTED IDENTITY MANAGEMENT

Inconsistent or absent device identities across suppliers, manufacturing stages, and operational environments create blind spots and increase risk.

2. INSECURE PROVISIONING PROCESSES

Manual or siloed credential injection increases the risk of compromise during manufacturing and limits scalability and consistency.

3. LACK OF END-TO-END TRUST

Difficulty verifying the authenticity and integrity of hardware and software components across tiers leaves the supply chain vulnerable to tampering and fraud.

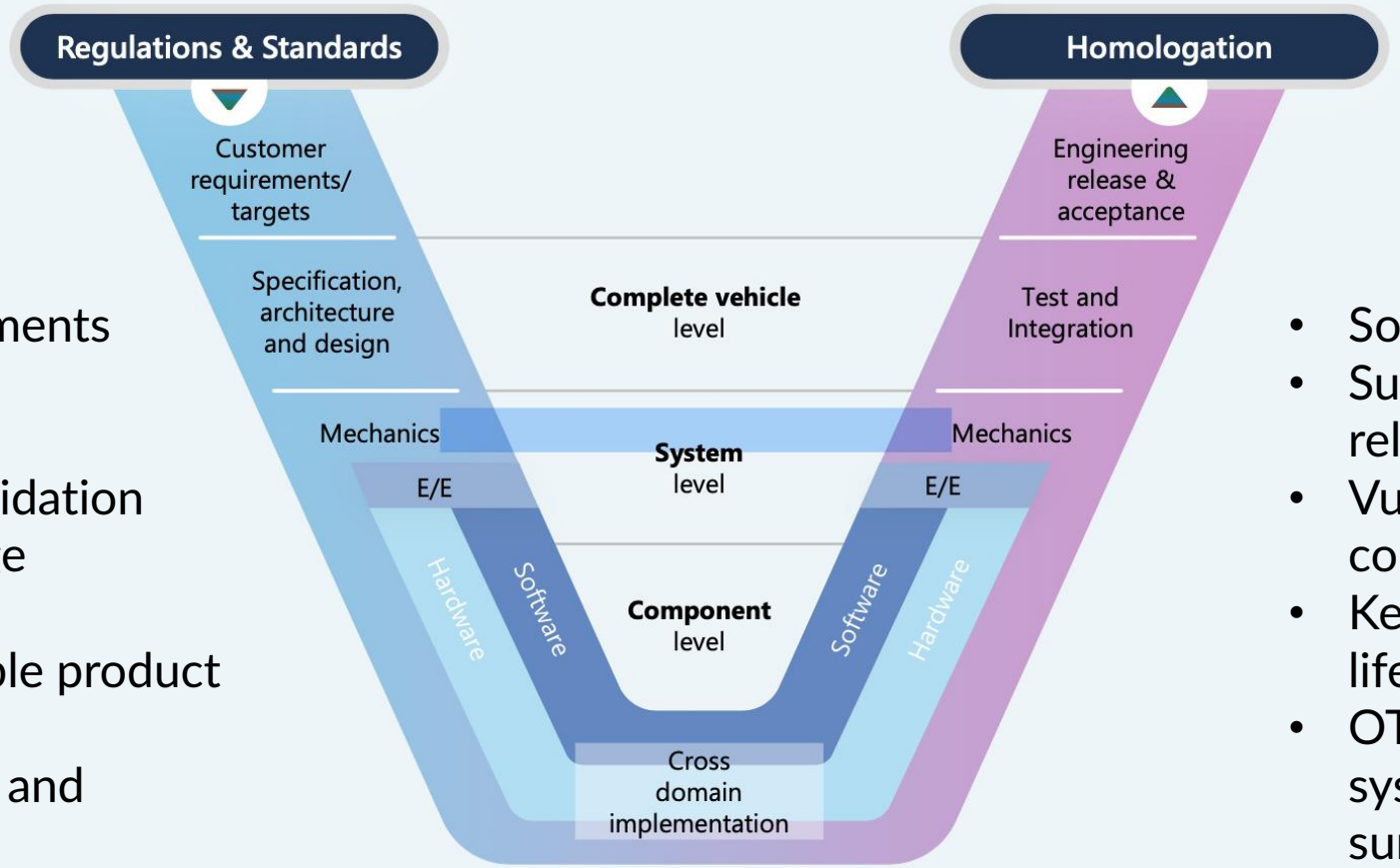
4. CERTIFICATE AND KEY LIFECYCLE COMPLEXITY

Managing PKI at scale across millions of vehicles and components is operationally complex and prone to error without automation.

5. REGULATORY PRESSURE

Meeting evolving standards such as UNECE WP.29 and ISO/SAE 21434 requires stronger security posture, traceability and auditability.

The Standard V-Shaped Model for Vehicle Manufacturing



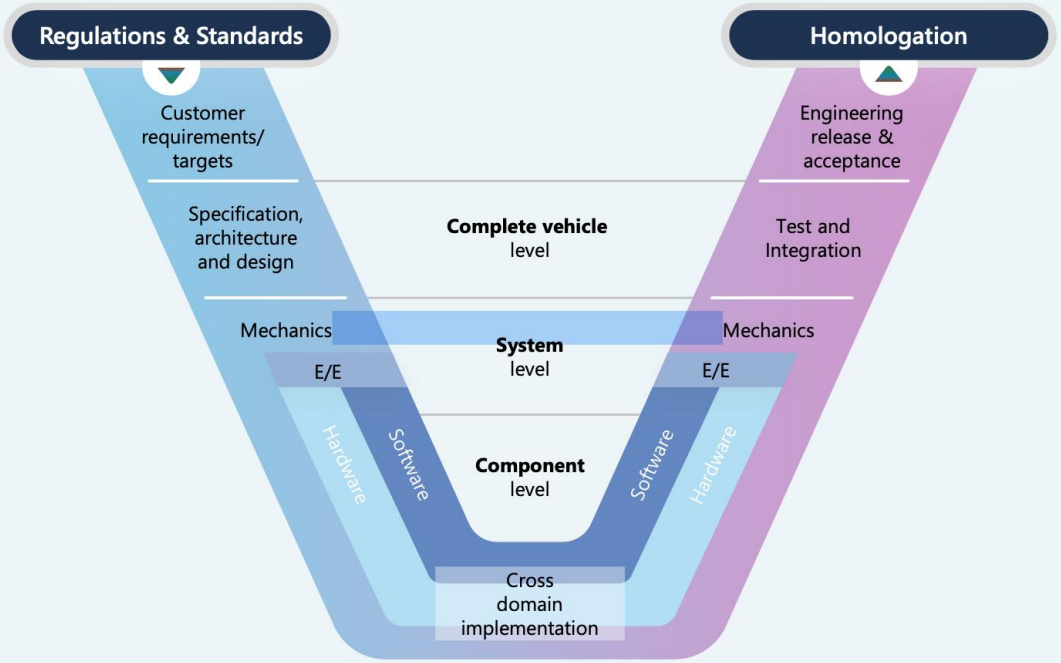
Great Because:

- Structured requirements traceability
- Disciplined design, integration, and validation
- Strong release-stage evidence
- Well suited for stable product baselines
- Effective for safety and quality assurance

Weak Because:

- Software changes after SOP
- Suppliers remain active after release
- Vulnerabilities emerge continuously
- Keys and certificates require lifecycle governance
- OTA, cloud, and service systems expand the attack surface
- Compliance evidence must stay current

But what about…..



The V-model proves the vehicle was built correctly.

SDVs require proof that the vehicle, software, suppliers, and credentials remain trustworthy over time.

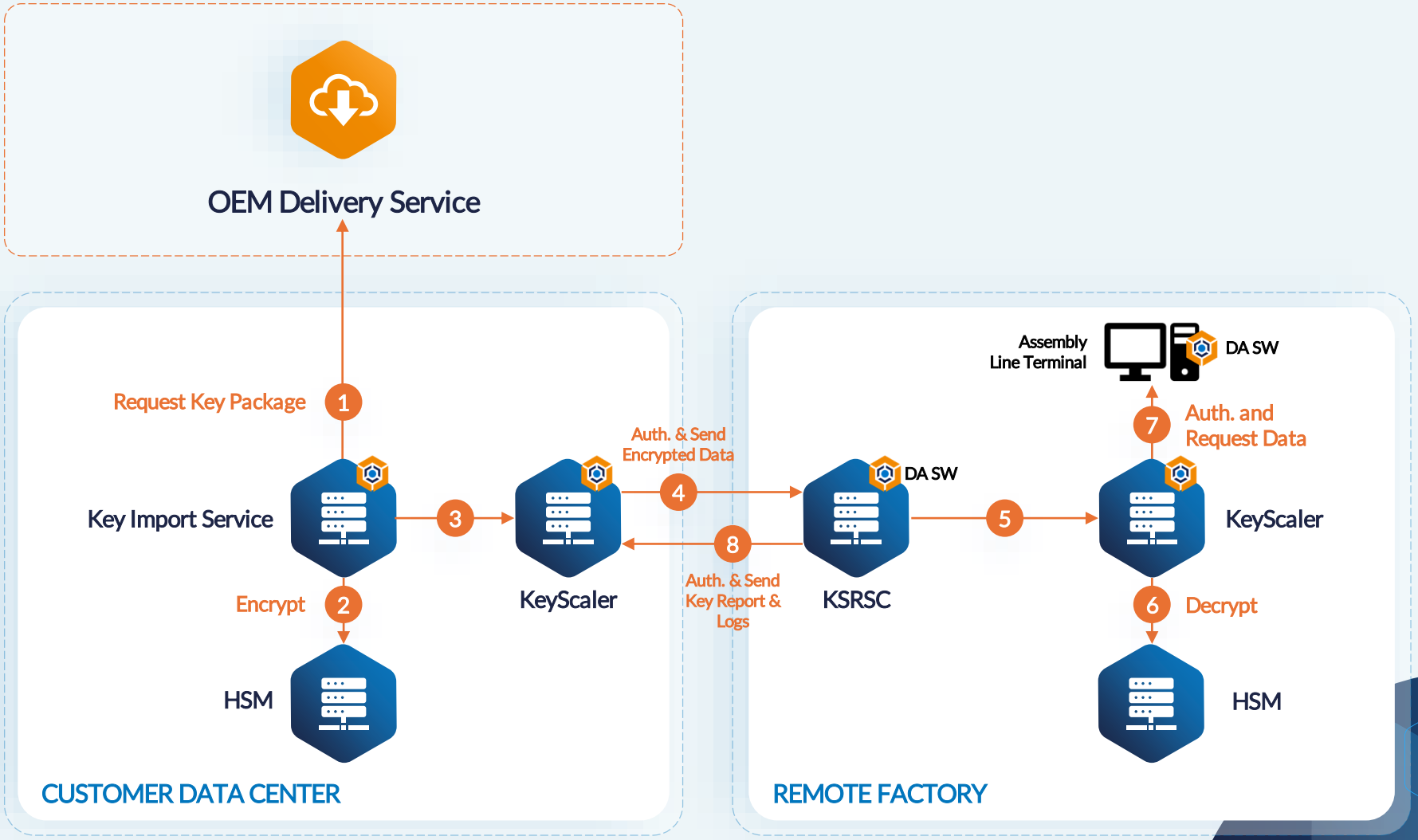
From Release Validation to Lifecycle Trust

Design → Supplier → Manufacturing → Vehicle Assembly → Operation → Service → End of Life

Lifecycle Area	Trust Question
Supplier	Is the component authentic and approved?
Manufacturing	Was key material protected and provisioned correctly?
Vehicle Assembly	Can the ECU or subsystem prove its identity?
Operation	Is the software, certificate, and configuration still trusted?
Service	Is this tool or technician authorized?
End of Life	Can trust be revoked and audited?

Automotive supply chain security becomes a lifecycle trust problem — not a point-in-time validation problem.

Secure Key Generation, Storage, and Distribution



The Customer Solution:

- Client Authentication - DDKG
- End-to-End Data Encryption
- HSM Access Controller
- Secure Key Gen
- Fully Audited Distribution Chain

The complexity of managing the connected lifecycle

KeyScaler

Microsoft Azure

Device Authority Engine

Device Authentication | Policy Management | API Services

Data Security | Certificate & Key Management | Security Events, Alarms, Notifications and Logs

POLICY

- Auto-Rotation:
  - 365 days
- Auto-Revoke
- Store Encrypted

Device Registration/ Cert. Provisioning

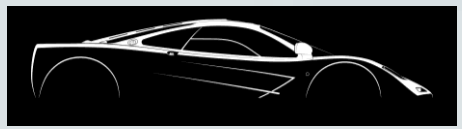
Service Connectors

Certificate Signing

Signed Certificates

TCU Certificate

Device Software



Azure Key Vault

Private CA

Microsoft Azure

IoT Application/ Platform

NTT DATA

Mutual-TLS Connection

DEVICE AUTHORITY

Automotive: PKI Management for Construction Equipment

POLICY
- Auto-Rotation:
  - 365 days
- Auto-Revoke
- Store Encrypted

KeyScaler

Device Authority Engine

- Device Authentication
- Policy Management
- API Services
- Data Security
- Certificate & Key Management
- EPIC

The Customer Solution:
- Client Authentication - DDKG
- End-to-End Data Encryption
- PKI Certificate Provisioning
- AWS connector

Service Connectors

Certificate Signing
Code Signing
Secure Updates

Device Registration/ Cert. Provisioning

Thing Creation/ Cert. Provisioning

ECM

Diesel Engine

ENTRUST

Venafi

AWS IoT Core

Mutual-TLS Connection

DEVICE AUTHORITY

Key Takeaways

Enabling Zero Trust Across the Automotive Supply Chain

1. AUTOMATED IDENTITY PROVISIONING

Establishing unique, cryptographically strong identities for every device and component at manufacture.

2. PKI AND CERTIFICATE LIFECYCLE AUTOMATION

Scalable management of certificates and keys across the entire vehicle lifecycle.

3. SECURE SOFTWARE DELIVERY

Ensuring firmware and OTA updates are authenticated and tamper-proof.

4. SUPPLY CHAIN INTEGRITY AND VISIBILITY

Enabling traceability and attestation of components from factory to field.

5. POLICY-BASED ACCESS CONTROL

Enforcing least-privilege principles across machine-to-machine communications.

DEVICE AUTHORITY

DEVICE AUTHORITY

Thank you!

tyler.gannon@deviceauthority.com