

CASE STUDY

Volkswagen Group

How DuoKey MPC KMS embedded on Edge servers enabled \$2B annual savings on Over-The-Air (OTA) vehicle updates by eliminating cloud egress costs

CHALLENGE

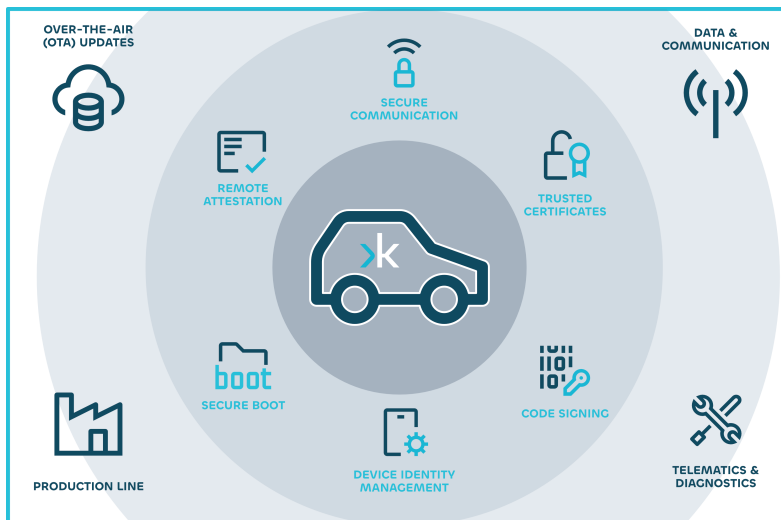
The Business Challenge

The VW Group faces a growing challenge in managing the massive data volumes and frequent over-the-air (OTA) updates required for their software-defined vehicle fleet, with update packages ranging from 500MB to 5GB per vehicle and over 10M+ connected vehicles, resulting in escalating data egress costs from AWS that could reach billions annually.

SOLUTION

How DuoKey Helped

Volkswagen Group manages over 10 million connected vehicles requiring regular OTA firmware and software updates. The traditional cloud-centric architecture generated massive AWS egress traffic costs —estimated at \$2B+ per year. By deploying DuoKey MPC KMS on Edge servers at dealer networks and regional distribution points, VW eliminated the need to route encrypted update packages through centralized cloud, achieving \$2B in annual infrastructure savings while maintaining end-to-end cryptographic security with TISAX-compliant key management.



Architecture Flow

Centralized cloud storage with high egress costs. Edge servers cache updates, reducing egress and latency. DuoKey MPC KMS on cloud and edge provides secure key management without vendor lock-in.



About Volkswagen Group

Volkswagen Group, a leading global automaker, pioneers connected vehicle tech and software-defined vehicles, producing over 10 million cars annually across its diverse brand portfolio.

Results & Impact

- ✓ \$2B in annual infrastructure cost savings
- ✓ 95% reduction in cloud egress costs
- ✓ Zero security compromise with MPC key management
- ✓ 3-month payback period on edge infrastructure investment
- ✓ Improved update delivery latency for global fleet

Key Technology

Multi-Party Computation (MPC) for distributed key management with TISAX AL3 compliance.