OTA Software Management Uptane Metadata Signing with Code Signing Server

Safeguarding Automotive OTA Updates

An increasing dependency on software, electronic control units (ECUs), and microprocessors to power modern vehicle systems and features, combined with the rising intricacy and complexity of managing software updates, requires automotive OEMs to adopt state-of-the-art processes and security standards such as the Uptane Secuity Framework. A central tenet of Uptane is compromise-resilience which is achieved by distributing responsibility for the signing of metadata, requiring a threshold of signatures to attest authenticity of a file, and using both online and offline signing of Uptane metadata.

Pre-Integrated Solution for Uptane Metadata Signing

Airbiquity® and Blackberry Certicom have integrated their OTAmatic® and Code Signing Server products to help OEMs quickly adopt Uptane and deploy Metadata signing processes into operational workflows to ensure safe and secure OTA updates. The integration automates Uptane root keys, associated image signing and timestamp keys, and Metadata updates. Although automated, access to signing key operations is strictly enforced. As a result, supporting a quorum of signatures for a key update or signing operation can be hassle free but remain highly secure.

Airbiquity OTAmatic® Software Management Platform

BlackBerry | certicom

OTA Software Management

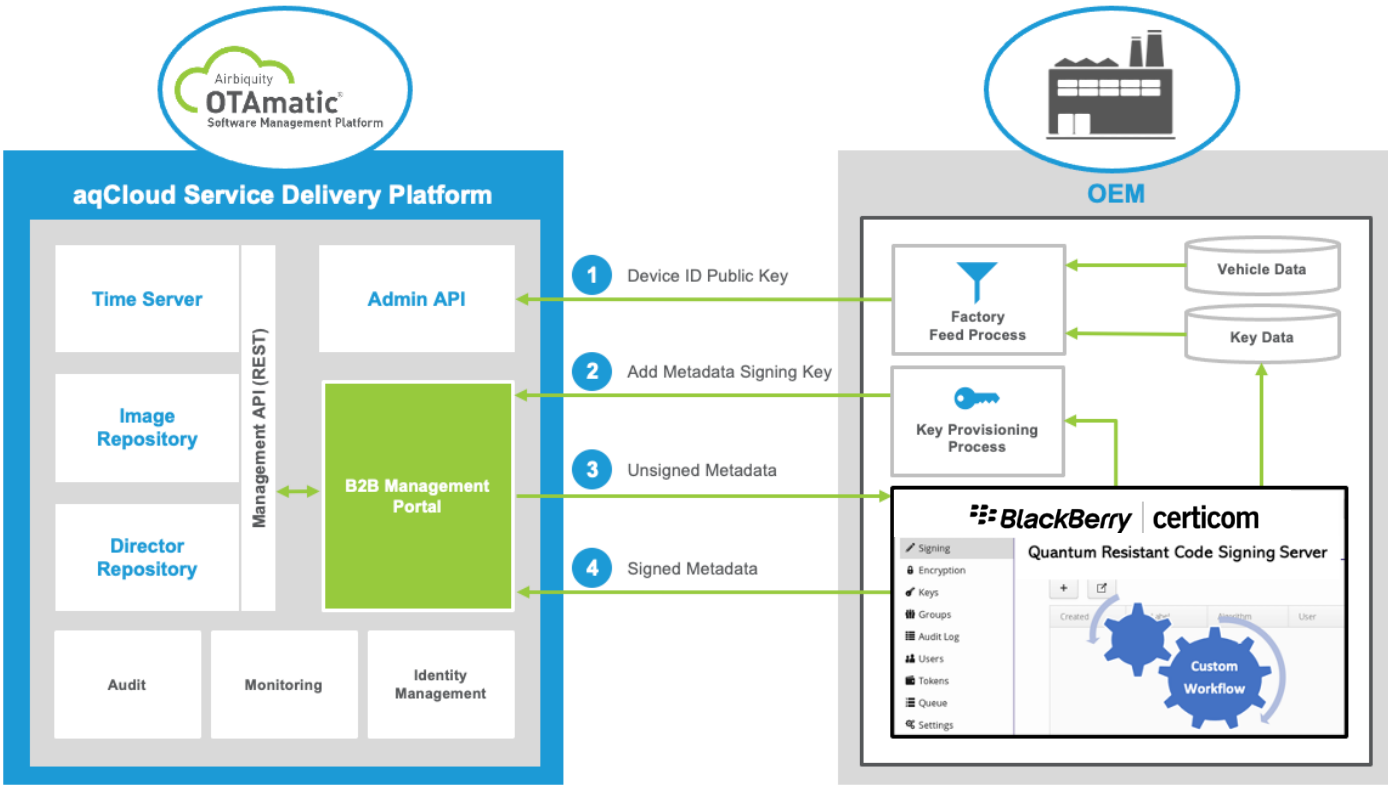
Airbiquity's OTAmatic Software Management Platform securely orchestrates and automates connected vehicle software update campaigns from the cloud. OTAmatic provides a fully-featured back-end management portal allowing manufacturers to efficiently execute multi-ECU software update campaigns—at scale—with highly refined vehicle and device targeting, discrete policy and privacy controls, customizable consumer communications, and solution deployment option flexibility. OTAmatic also has enhanced multi-layer cybersecurity protection via integration of the compromise-resilient Uptane Security Framework.

Code Signing Server

BlackBerry's Code Signing Key Server supports traditional cryptosystems as well as new post-quantum crypto algorithms to enable crypto-agile next generation devices. The system has been designed with key access control flexibility to support R&D, test, and production operations for OEMs and Tier 1s. It can be used by numerous groups within an enterprise, with users and authorized systems getting access to only their own group restricted keys for signing or encryption operations. REST APIs and a plug-in architecture are part of the product's extensible design to support custom workflows while maintaining robust security for a variety of use cases.

Uptane

Airbiquity-Certicom Multi-ECU OTA Software Update Solution
— Functional View —



Airbiquity OTAmatic Software Management Platform

- Single and Multi-ECU Software Updates
  - Unified Diagnostic Services (UDS) Updates for Secondary and Legacy ECUs
- Advanced OTA Software Update Orchestration
  - Preconditions, Priorities and Dependencies
  - Fault and Error Detection, Recovery and Rollback
- Standard-Based Security Integration
  - PKI, PSK, and TLS 1.2
  - Uptane-Based Security Design
- Back-End Service Management Portal
  - Step-by-Step Campaign Configuration Process
  - Separate Software and Data Management Campaign Tracks
- Comprehensive Campaign Reporting

Certicom Code Signing and Key Management Server

- Security of Signing keys: reduce risk of key compromise with a hardened signing server
- Ease of Use: local, web or REST based access to registered key group users and system administrators
- Increased Policy and Audit Compliance: an audit trail of individuals or applications using keys for signing or encryption
- HSM-backed key stores with a range of key protection options
- REST API integration for signing, encryption and MAC operations
- Add or revoke signing keys
- RSA, ECDSA & quantum resistant digital signature algorithms
- Yubikey option for key holder authentication
- A/D integration support

For Additional Information

Airbiquity

Email sales@airbiquity.com

BlackBerry | certicom

Email sales@certicom.com