



**Navigating Automotive Cybersecurity:
SAE J3201_202409 for Key & Credential Management**
Ensuring Trust and Security in the Connected Vehicle Ecosystem

Rita Barrios, PhD
Sr. Cybersecurity Engineer/Security Manager
Bosch LLC, NA

Work Experience

2022 - Present: Security Manager & Sr. Cybersecurity Engineer

- Patent Submitted: Dynamic approach to real-time CVE/CWE analysis during cybersecurity threat analysis and risk assessment (TARA)
- Chaired SAE J3201 Committee (published 2024); ISO/SAE 21434 & 8475 JWG Member

2020 - 2022: Sr. Cybersecurity Engineer – BlackBerry QNX

2016 - 2020: Sr. Cybersecurity Engineer – Ford Motor

- Patent: Dynamic relay attack prevention using time of flight and RF fingerprinting

2006 - 2016: Assoc. Prof. & Dept. Chair – Cybersecurity & Information Systems - UDM

- On-Going: Adjunct Professor in Vehicle Cybersecurity Engineering and Computer Science

1990 - 2006: Sr. Software Engineer & Sr. Database Administrator – Ford Motor Credit

Academic Education

PhD: Computer Science; Cybersecurity. Thesis: Database Intrusion Detection – Detecting Insider Threat

Graduate Certificates: Cybersecurity, Data Science, Embedded Systems

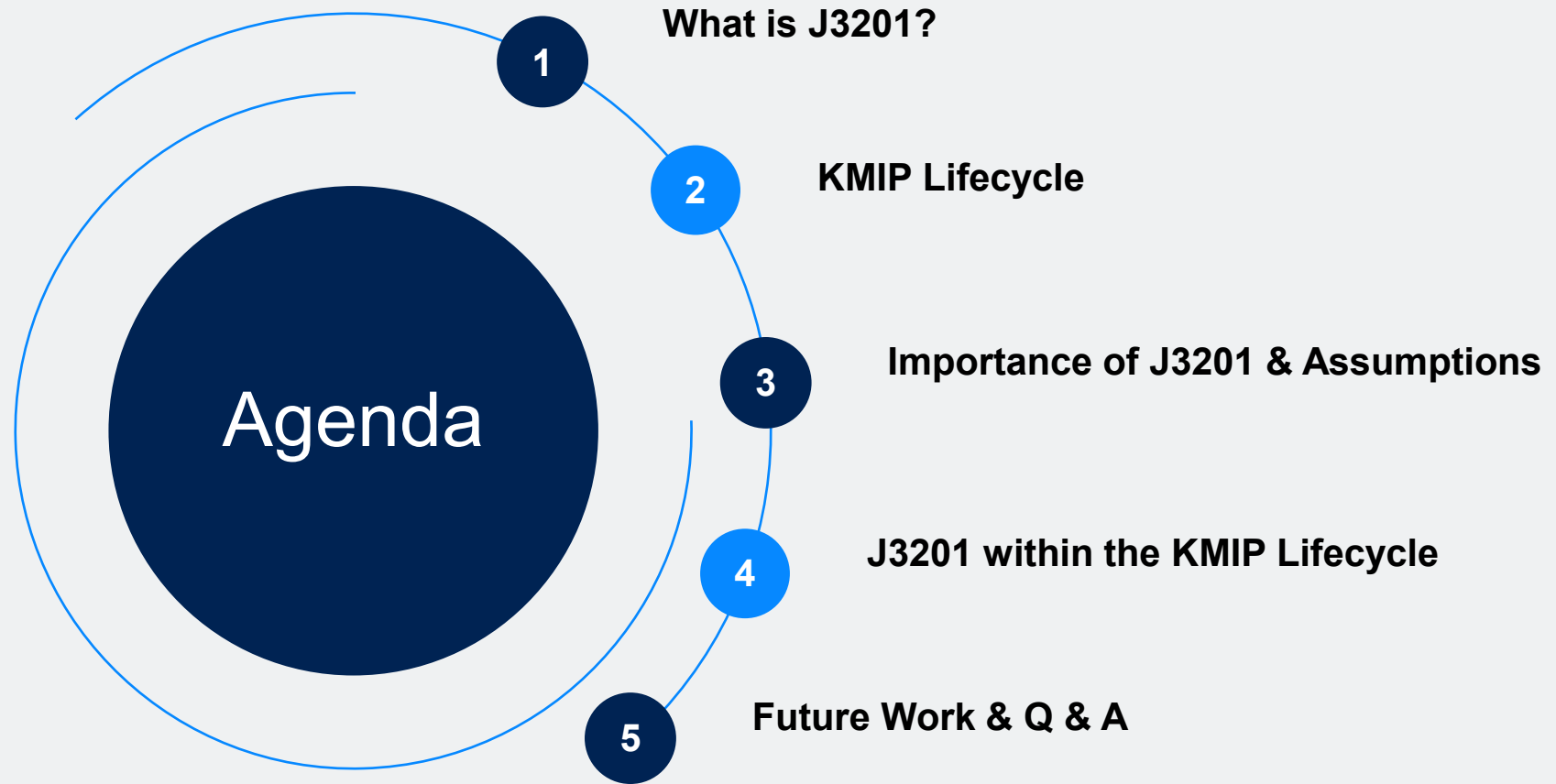
Personal Information

Hobbies: STEM Outreach, running, cooking, travel, Red Wings fan



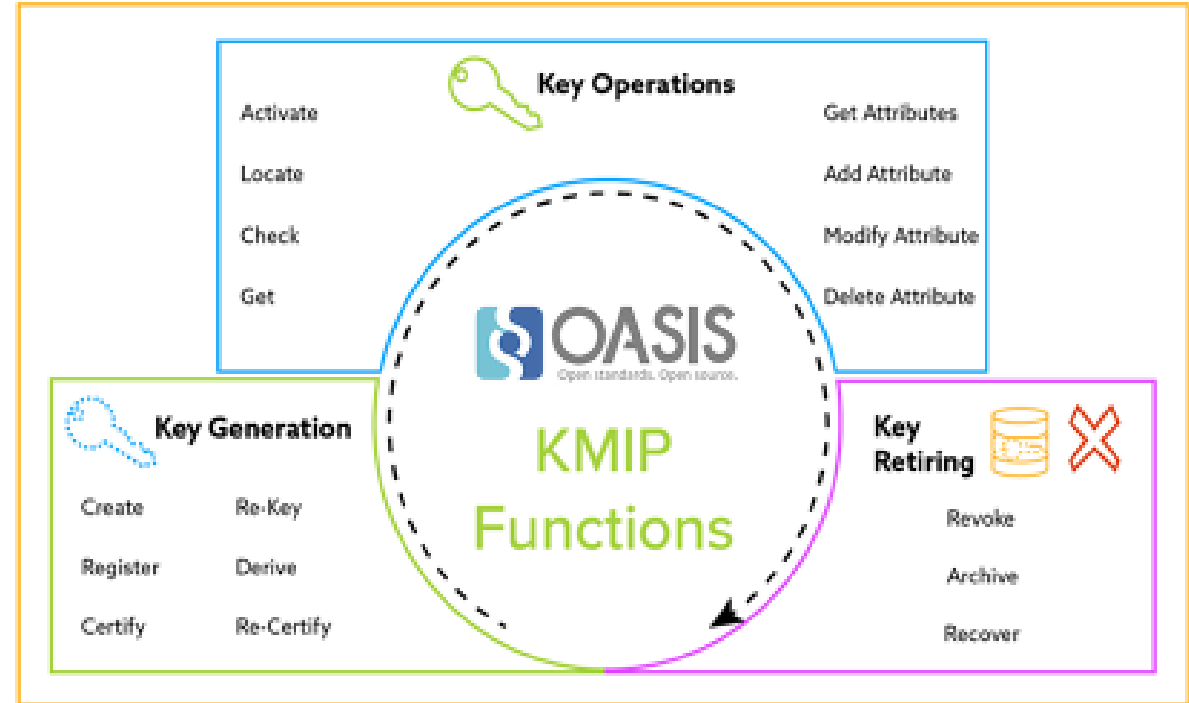
Rita M. Barrios, PhD.

Agenda



SAE J3201_202409 Guidelines for Automotive Environment Cybersecurity Key Management and Credential Distribution

- **Purpose:** Provides a comprehensive framework to facilitate the exchange of critical cryptographic assets throughout the vehicle's lifecycle → based on the **KMIP Protocol**
- **Core Need:** Creates a **standardized approach** to manage the exchange process for keying material for automotive
- **Focus:** Credential management exchanges (keys, certificates, and other cryptographic material) between two different parties in an **automotive setting**



Supports ISO/SAE 21434 and UN R155

Importance of J3201

- Gives guidance and implements a well-known framework for credential exchange put into an automotive context
- Generic enough to support OEM to T1 or any other two-party exchange – following the KMIP nomenclature of client-server relationship
- Based on the KMIP Service Profiles: Baseline Server, Baseline Client, & Complete Server
- Build Service Definitions (use cases) are Auto Industry focused
- Roles include Key Server (server), Key Generator (generator), Key Requestor (client), Key Installer (installer)

Assumptions of J3201

- **Only focuses on the exchange** → KMS, Backup Strategies and Recovery Strategies should follow SP800-53; Storage should follow RFC 4107, ISO 27000-1:2022 and/or SP800-171
- Uses the terms Client and Server in accordance with the KMIP specification to denote the two parties in the exchange – depending on the flow of the exchange – assumes both clients and servers agree to implement and use KMIP
- v1 of J3201 focused on the OEM → T1 exchange – can be extended to Tx → Tx
- Focused on key management during or post vehicle production and the environment is trusted
- OEM SHOULD implement the root CA for the software and firmware signing PKI, since the OEM owns the liability
- Multiparty exchanges were out of scope
- Access controls to services were out of scope
- Transport Layer Protections (TLS or VPN) were out of scope

Organized Around the Service Definitions of the KMIP Lifecycle

Generation:

Includes symmetric key, asymmetric key, X.509 certificate, feature locking/unlocking code, or other objects

7.2.5.1 ECU Generates Its Own Asymmetric Key Pair

Provisioning/Distribution:

7.2.2 Provisioning of Software and Firmware Signing Keys for Build System

7.2.4.3 Client Asynchronously Requests Key Injection for Production Run Batch

7.2.4.5 Client Asynchronously Requests Key Injection for Specifically Identified ECU

7.2.5.4 Provisioning Security Credentials to In-Vehicle ECUs via Gateway ECU

Storage/Protection:

7.2.4.6 Register Feature Locking/Unlocking Codes to Server

7.2.5.2 ECU Requests Intermediate Server to Validate and Forward Its CSR to a CA Server for Processing and Pushes the Certificate to the ECU

Usage:

7.2.4.1 Client Associates Existing Object to ECU Type

7.2.4.2 Client Registers Objects Associated with Production Run Batch (foundational KMIP)

7.2.4.4 Server Associates Injected, Managed Objects to Recipient ECU

7.2.4.7 Client Obtains Status on One or More ECU Injection Requests

7.2.4.8 Client Obtains Injection DateTime for ECU in Production Run Batch

7.2.4.9 Client Associates Object to Vehicle Identification Number (VIN)

7.2.5.3 Registering Security Objects per Element of an ECU

Revocation/Destruction:

Future service definitions of J3201

Future Work for J3201: Potential Service Definitions

COMPROMISE OF OBJECTS

- An entity within the OEM or Tier-1 discovers that a key, or series of keys, has been compromised. The state of these keys can be managed via the KMIP attributes on the key objects. Either the OEM or the Tier-1 can take on the role of the Client or Server. The Client with knowledge of the compromise, performs KMIP SET_ATTRIBUTE on the life-cycle state of the compromised object to set the attribute to “compromised.”

Testing KMIP

- Identification of best practices when testing the service definitions in conjunction with the KMIP framework.

Post-Production

- Key provisioning and exchange in scenarios that involve Vehicle-to-Everything (V2X), OEM-to-OEM, OEM-to-infrastructure (traffic management, emergency services, buildings), and infrastructure-to-OEM.

Application Updates

- Accepting updates to keying material from trusted applications such as those from third party vendors, best practices for updates requested by repair facilities and skilled persons

End of Life

- Identification of best practices when the component containing the key material reaches end of life such as if the component is discarded to a junk yard, it is decommissioned, or remanufactured.

Enables Trust

- Essential for safe and reliable exchange of crypto materials between two parties
- Mitigates Risks

Facilitates Innovation

- Provides a secure foundation for V2X, OTA, Plug & Charge key exchanges

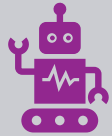
Supports Compliance

- Common exchange mechanism that is auditable



Post-Quantum Cryptography (PQC)

J3201 will need to be revisited



Advanced AI/ML Threats:

New attack methods requiring more dynamic key management.



Global Harmonization:

Continued effort to align standards internationally.

J3201_202409: A guide for securing automotive key and credential exchanges

KMIP Lifecycle Approach:

- Revocation and Destruction will have to be addressed in v2

Foundational:

- Underpins trust

Critical for Industry:

- Drives safety, compliance, and innovation.





**Global
Platform[®]**

Securing the digital future

Thank You!

Rita M. Barrios, PhD.
rita.barrios@us.bosch.com

→ globalplatform.org