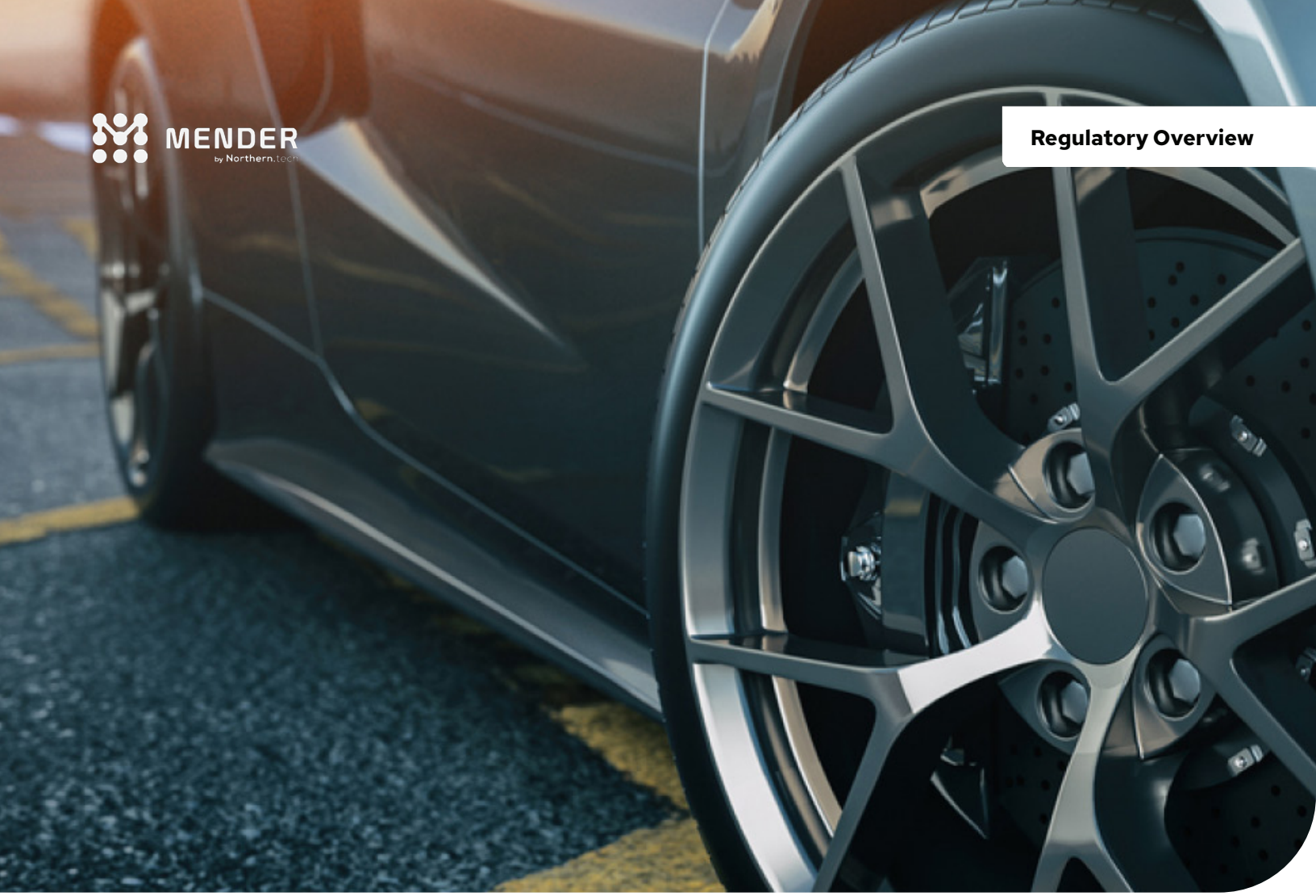


MENDER by Northern.tech

Regulatory Overview

ISO/SAE 21434 & UNECE R155/R156 Compliance.

Automotive Cybersecurity

Executive Summary

The automotive industry continues to evolve towards a software-centered and -defined vehicle. With autonomous, fully self-driving technologies on the horizon, the industry has transformed from a kinetic, physical-focused product to one indistinguishable from the software within. In this transformation, cybersecurity becomes as important as current safety requirements, such as reliable airbags and braking hoses.

ISO/SAE 21434[1] is rapidly gaining acceptance as the global industry benchmark for automotive cybersecurity practices. In Europe and Japan, corresponding legislation is coming into force through the work of the United Nations Economic Commission for Europe (UNECE Working Party / WP 29[2]). While these new requirements can seem daunting at first glance, ISO/SAE 21434 represents a formalization of existing best practices for cybersecurity engineering. Implementing the ISO standard alone also substantially fulfills UNECE R155/R156 compliance requirements. For organizations still defining and developing their internal cybersecurity culture, these standards provide rigorous and actionable guidelines for implementing robust processes around cybersecurity.

Software updates are a mandatory part of a modern cyber-secure product development cycle and are mandated by these standards and regulations. The ability to update embedded and connected devices in a robust and secure manner is essential for the innovation and security of vehicles. Mender provides the technology to deliver updates economically, rapidly, and securely over the air to vehicles. Leveraging Mender for over-the-air (OTA) software updates accelerates implementation and compliance with ISO/SAE 21434 and UNECE R155/R166.

In the backend, Mender vehicle software inventory, campaign management, and reporting directly implements many of the ISO/SAE 21434 and UNECE R155[3] requirements for cybersecurity threat monitoring and incident response. For ISO/SAE 21434, Mender is part of an organization's overall Cybersecurity Management System (CSMS); Mender's OTA technology constitutes a Software Update Management System (SUMS) as defined and required by UNECE R156[4].

In the vehicle, the Mender client can be integrated directly into vehicle software platforms. In doing so, Mender supplies the necessary evidence and cybersecurity process alignment to directly meet ISO/SAE 21434 and UNECE R155 requirements for Mender's on-platform software components.

Continuous cyber-secured technological innovation requires efficient, robust, and secure OTA updates. Without it, innovation and, thereby, competitiveness fail to progress. OTA updates are foundational components organizations need to ensure to comply with industry regulations and succeed in a new, technology-focused environment.

1 https://www.iso.org/standard/70918.html
2 https://unece.org/wp29-introduction
3 https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
4 https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

Glossary

API	Application programming interface
CA	Certificate authorities
CSMS	Cybersecurity Management System as defined in ISO/SAE 21434
DoS	Denial-of-service
ECU	Electronic control unit
IP	Internet Protocol
ISO	International Organization for Standardization
HTTP	Hypertext transfer protocol
HSM	Hardware security module
mTLS	mutual transport layer security
OEM	Original equipment manufacturer
OTA	Over-the-air
OTP	One-time password
PKCS	Public-key cryptography standards
R155	UN Regulation 155 - Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system
R156	UN Regulation 156 - Uniform provisions relating to the approval of vehicles with regards to software update and software updates management system
RASIC	Responsible, approving, supporting, informed, and consulted matrix
RBAC	Role-based access control
REST	Representational state transfer
RFQ	Request for quotation
RXSWIN	RX software identification number (RXSWIN) in the sense defined by UNECE R155
SAE	Society of Automotive Engineers
SAML	Security assertion markup language
SSO	Single sign-on
SUMS	Software Update Management System as defined by UNECE R156
TLS	Transport layer security
TPM	Trusted platform module
UI	User interface
UNECE	United Nations Economic Commission for Europe
URL	Unified resource locator
2FA	Two-factor authentication

Cybersecurity and the automotive industry

Software are eating the car. Modern vehicles contain over 100 million lines of code running on hundreds of electronic control units (ECUs). With the deployment of autonomous driving, the vehicle codebase is expected to expand to more than 500 million lines.

During the development of the vehicle, it is impossible to catch every bug in such a large codebase. But software bugs in an automobile can be safety-critical. As such, the reliability and safety of vehicles rely on fixing bugs rapidly after production when the vehicle is already on the road. Lives depend on it.

Over-the-air (OTA) software updates are a critical part of the modern automotive development lifecycle, despite manufacturers' historical caution in deploying the technology; while a software update infrastructure makes it possible to mitigate software defects in the field, it can also increase the risk of cybersecurity attacks targeting vulnerabilities in the update mechanism itself. Manufacturers are still defining and improving their processes around software vulnerability identification, protection, detection, response, and remediation— while balancing the risks and costs of moving beyond traditional dealership-based software updates.

Complying with new cybersecurity standards

In August 2021, the International Organization for Standardization (ISO) released ISO/SAE 21434 to standardize how automotive vehicle manufacturers implement cybersecurity in their organizations. Passing an ISO/SAE 21434 audit gives consumers the confidence that cybersecurity threats have been considered and addressed during vehicle conception, manufacture, and ongoing operation. Passing an ISO/SAE 21434 audit also provides significant support for compliance with UNECE Regulations R155 and R156; enforcement of these regulations started in the summer of 2022 for Europe and Japan.

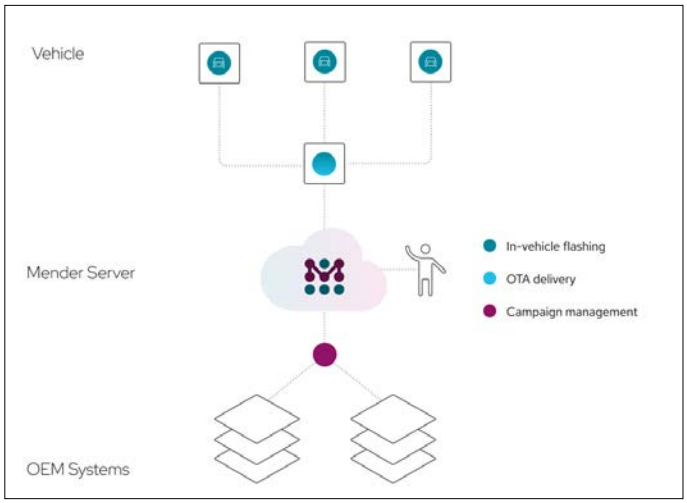
Organizations hoping to achieve compliance must develop a comprehensive approach to cybersecurity risk management across all stages of the vehicle lifecycle. Organizations must live in a culture of cybersecurity. The cybersecurity policies and governance model must be documented and reviewed, and comprehensive evidence of threat modeling and mitigation must be created and validated by independent auditors.

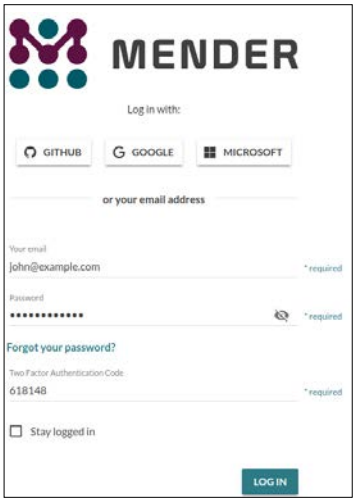
Software updates are a mandatory part of mitigating cybersecurity vulnerabilities in the field. Mender provides automotive original equipment manufacturers (OEMs) with an ISO/SAE-21434-ready solution for rapidly and economically implementing those updates with secure security over-the-air (OTA) software updates.

5 https://spectrum.ieee.org/software-eating-car

Mender for the automotive industry

As part of an organization's implementation of cybersecurity monitoring in their products' lifecycles (ISO/SAE 21434[6], §8), cybersecurity events (ibid., §8.4) may be triggered where mitigation according to the risk treatment decision (ibid., §15.9) requires releasing an update to vehicle software (ibid., §13.4)





Campaign management

Through the Mender user interface (UI), vehicle update campaigns can be defined and launched to mitigate identified cybersecurity threats in affected vehicles.

On the server side, security is particularly important, as controlling campaigns can have a significant impact across a vehicle fleet. Mender implements a defense-in-depth security model to limit the impact of a breach on any given level.

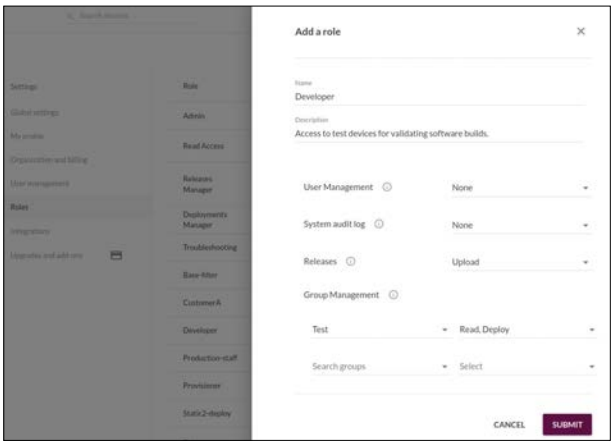
Secure user authentication and authorization

As the first step, the Mender UI (for users) and application programming interface (API) access (for programs such as OEM systems) requires authentication for all users. Mender user authentication has several layers. Two-factor authentication (2FA) using a one-time password (OTP) token (e.g., from a smartphone app) is a common method. 2FA plus an OTP token adds an additional layer of security to logging in so that stealing or phishing a password is not enough to compromise user authentication.

6 https://www.iso.org/standard/70918.html

For enterprise deployments, Mender integrates with existing secure identity providers via the industry-standard security assertion markup language (SAML) protocol for single sign-on (SSO) support, ensuring no user accounts are left unmanaged as internal staff change over time.

Role-based access control (RBAC) is an additional authorization layer that limits the potential impact in the scenario that a user or attacker is authenticated with the server. For example, if the user is part of a "Developer" role, they can only control and deploy to the Test Devices Group without impacting production.



Availability and denial-of-service (DoS) protection

For enterprise deployments, the Mender server supports configurable API rate limits. When a device or a user crosses the rate limit threshold, it will receive the hypertext transfer protocol (HTTP) status code: 429 Too Many Requests. Organizations can configure the server to enforce these limits based on the client internet protocol (IP) and the identity of the API caller, either device or user. Rate limits can apply to all the API calls or be customized for specific API endpoints.

Secure binary storage

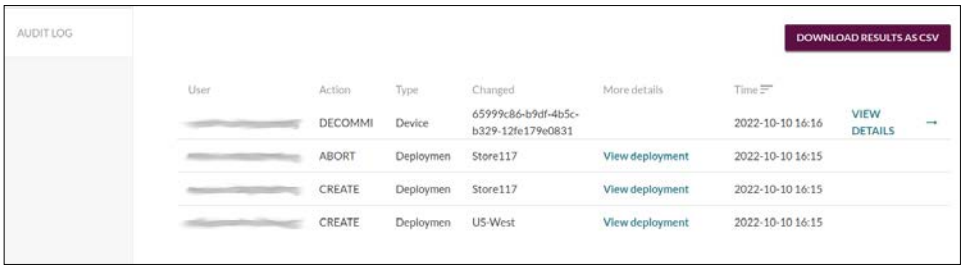
The Mender server comes with an integrated secure binary storage (ibid., §5.4.6, RQ-05-16) as software binaries, packaged as Mender artifacts, are stored behind the server API gateway and are only accessible for authenticated users and devices. Amazon S3 can be used as well as S3-compatible services such as Minio. The Mender server structure enables several standard layers of infrastructure-level security, such as storage encryption. As the binary storage service is decoupled from the rest of the server infrastructure, Mender also supports independent geolocation of the storage service.

Device downloads for software binaries are secured with time-limited signed unified resource locators (URLs); each device must uniquely authenticate to download each software binary. This prevents devices from accessing software binaries they do not strictly need access to, as the device will only obtain a signed URL once a user has explicitly created a software deployment for the given device.

Audit log

If suspicious activity is detected or an operational incident has occurred, Mender audit logs will help identify the root cause, assess the impact, and create a remediation plan.

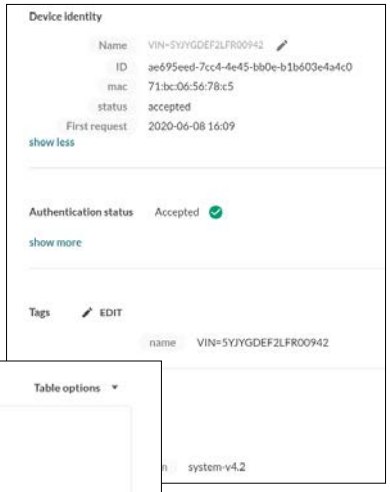
Audit logs are a security feature that immutably logs key user actions that impact the devices or other users, such as creating a software deployment campaign, decommissioning a device, or changing user permissions.

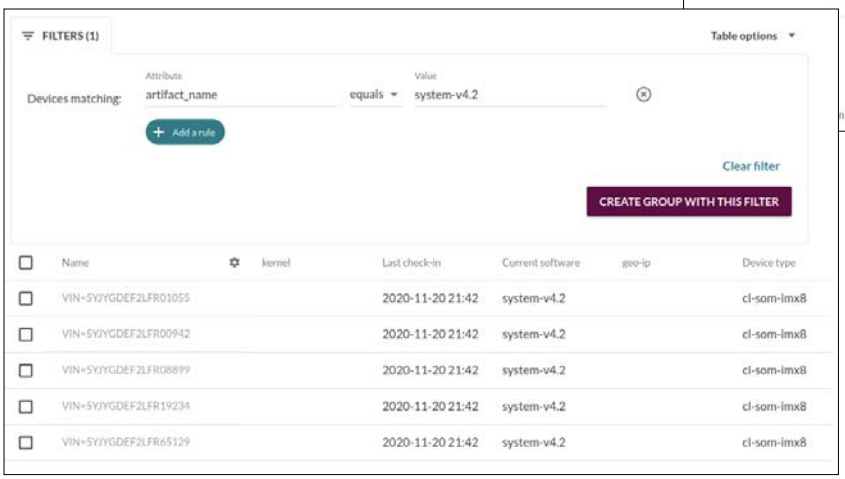


Software bill of materials

Mender keeps an up-to-date online software bill of materials for each vehicle (ibid., §5.4.4, RQ-05-12) as part of Mender's software inventory.

Vehicles can be filtered based on inventory attributes, including installed software versions. Based on this data, dynamic groups can be created, for example, to target vehicles with software versions possessing a known issue, such as a security vulnerability.





Over-the-air delivery

Mender takes care of the secure over-the-air delivery of the software updates.

Secure transport layer security (TLS) communication

The security of Mender's over-the-air delivery starts with a secure communication channel set up with the industry standard, battle-tested TLS protocol. This ensures that the infamous man-in-the-middle attack is impossible to carry out against products using Mender.

Communication between the client and server happens via a representational state transfer (REST) API over a TLS-encrypted channel. The Mender client relies on the operating system's root certificate authorities (CAs) to verify the server identity by default. Organizations can also configure the client to use a specific certificate for chain validation, such as when the server uses a self-signed certificate.

The server is always authenticated using TLS; the client may use TLS to authenticate itself as well, in which case, the connection will be secured with mutual TLS (mTLS). Otherwise, the client can use an application-layer method to authenticate, as described below.

Secure client authentication

Mender has several layers of security to ensure that only authenticated clients will be able to obtain software updates.

At the first layer, Mender enterprise requires all clients to have a secret tenant token. This maps the given client to a valid organization (the tenant) on the Mender server. The client will not be able to authenticate to the server without providing a valid tenant token.

As the second layer of security, client-side (mutual) TLS can be used. In this case, hardware security through the hardware security module (HSM) and trusted platform module (TPM) is also supported, as described below.

If mutual TLS is not practical for the given project, such as a lack of a CA, two simpler options can also be used. First, preauthorizing devices rely on a list of trusted public keys associated with devices. Second, accepting devices on their first request is also possible, often used in smaller-scale environments to simplify the infrastructure.

Support for hardware security module (HSM) and trusted platform module (TPM)

The Mender client can utilize private keys stored in an HSM or in a TPM. This is an additional layer of security that eliminates the storage of private keys (secrets) as plain text files on the device, making it harder for an attacker to gain access to keys to impersonate devices.

This protection is relevant for devices in hostile environments where attackers can gain physical access and attempt to read the storage device, such as by connecting it to a different device.

For maximum operability, Mender supports the industry-standard public-key cryptography standards (PKCS) #11 and OpenSSL engine implementations of HSMs.

In-vehicle flashing

Mender's in-vehicle update client takes care of the reprogramming and validation of ECUs targeted by update campaigns (ibid., §5.4.5, RQ-05-14).

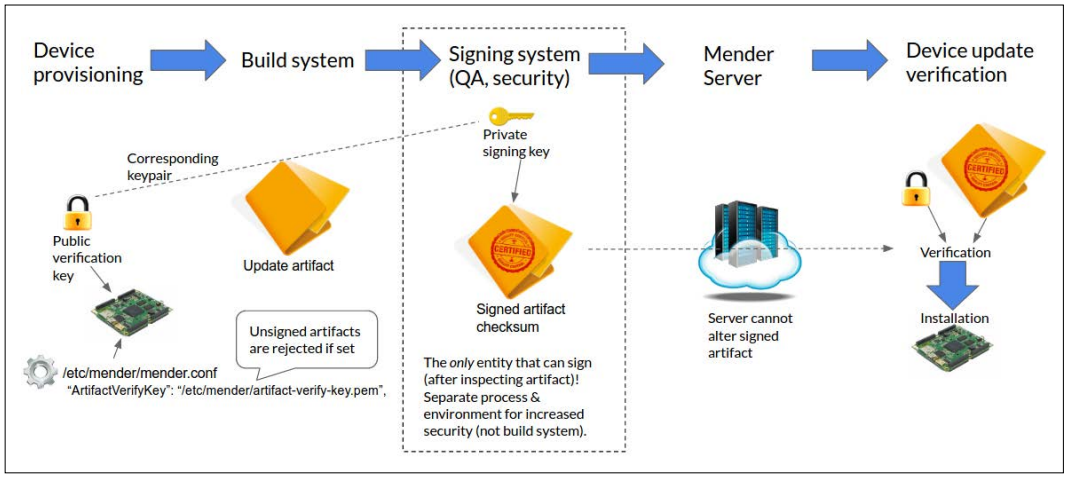
Seamless A/B updates

Mender preserves the safety properties of the vehicle with atomic updates: an update either fully installs or fully rolls back. The vehicle will never end in an intermediate, half-updated, or unpredictable state. This is implemented as part of the proven design of A/B updates (UNECE R156[7], §7.2.2.1.1), where the previous working version of the software is preserved while the new update is installed in a different location and tested before being made permanent. In case of failure, the previous working version of the software is started again (rollback).

End-to-end cryptographic code signing

End-to-end code signing serves as an independent layer of security and continues in force even if the complete server infrastructure is compromised by an attacker, such as the impersonation of a high-privileged user account.

By enabling code signing, the Mender client software will only allow the installation of Mender artifacts that pass the verification with its public key. The corresponding private key used for signing artifacts can be kept offline and manually used, such as by the security or quality assurance team, to achieve the highest level of security.



7 https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

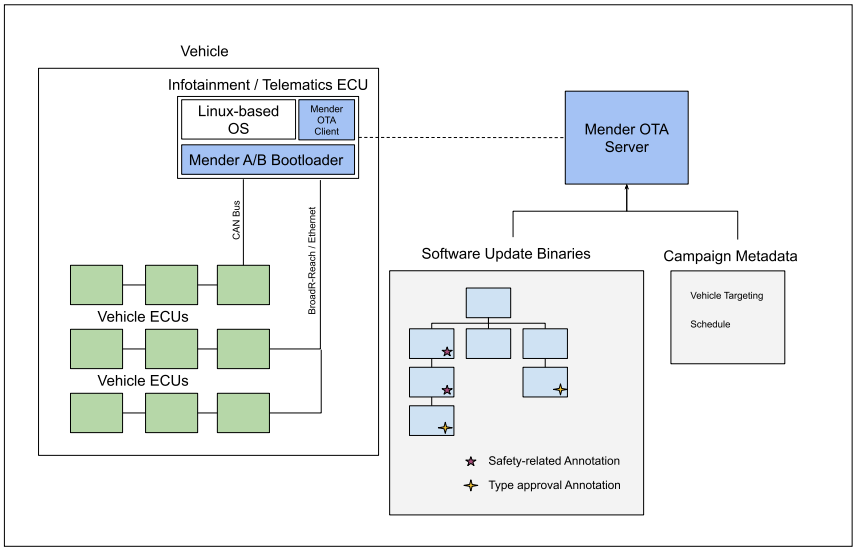
Use native flashing tools

Mender uses fully customizable software components called *Update Modules* to carry out the installation and any rollback of different types of software. For example, there are existing *Update Modules* to install A/B system updates, package, file, and container type updates.

Vehicle ECUs often have native diagnostic and update tools that are used to install new software. This flow can easily be integrated into the Mender client by creating an ECU-specific *Update Module* that leverages this device-native flashing tool.

UNECE R156 compliance

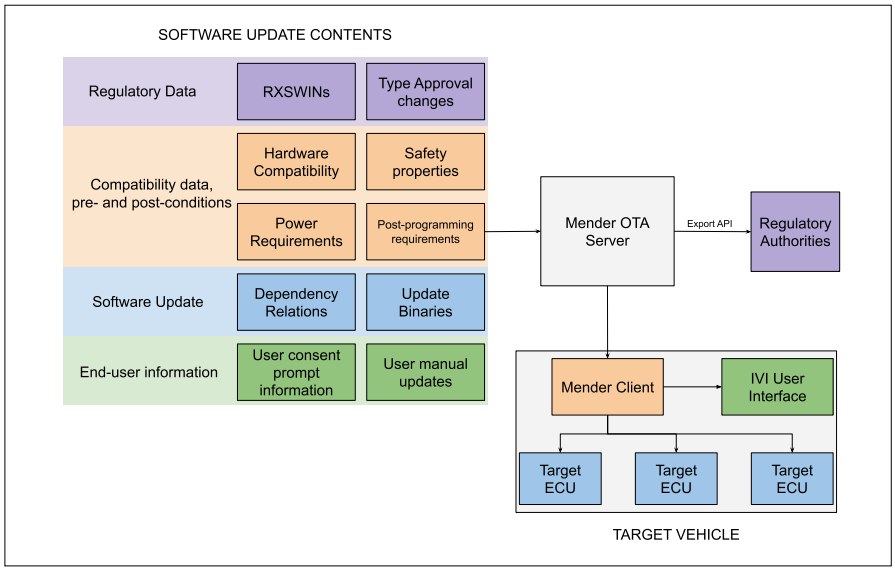
As well as storing software version information and cryptographic signatures for binaries, Mender can store and process type-approval-relevant software identifiers (RXSWINs) for a vehicle's software components to assemble a software bill of materials for each vehicle; the software bill of materials is then made available in the Mender server (ibid., §7.1.1.3). The Mender client validates that the software is installed in the vehicle, preserving the integrity of the binaries during the flashing process (ibid., §7.1.1.4) with checksum and signature verification.



The Mender server can store and process information about dependencies between software components (ibid., §7.1.1.5) and their compatibility with hardware module types and versions. Individual vehicles or groups of vehicles can be targeted for updates (ibid., §7.1.1.6), with the server checking the compatibility of the proposed updates with the currently installed hardware and software in the vehicle (ibid., §7.1.1.7) before scheduling a campaign to any specific vehicle. For hardware compatibility, Mender ensures the device type of the ECU is in the list of compatible devices of the given software. Software compatibility can be ensured using device provides and depends attributes of Mender.

Where information about the impact on type approval of the update is made available, that can also be tracked through Mender campaign management (ibid., §7.1.1.8 / §7.1.1.9 / §7.1.1.10). Likewise, artifacts can be annotated with safety and validation-related properties to ensure that safety-critical updates are only applied when the vehicle is not driving (ibid., §7.1.4.1, §7.2.2.3, §7.2.2.1.3) and that updates requiring skilled or complex post-programming intervention are not applied over the air (ibid., §7.1.4.2). This is implemented using *State Scripts* in Mender, which is a powerful framework to customize the workflow of installing updates.

Using the flexibility of *State Scripts*, the campaign can be annotated with power budget information to ensure that the client does not initiate an update on a vehicle with insufficient power to complete its installation (ibid., §7.2.2.1.2). Information that should be presented to the user as a prompt before the update (ibid., §7.2.2.2.2) and campaign-specific post-update documentation (ibid., §7.2.2.4) can also be attached to a campaign to be made available in the user interface of the vehicle before and after the update is complete. If updates to the end user manual are required, a download link for the new manual can also be included in the campaign metadata (ibid., 7.2.2.4(b)).



Based on the information supplied in the campaign, the integration of the Mender client can ensure that all update pre-conditions (e.g., safety and power-related factors) are met before initiating the update (ibid., §7.2.2.5). Mender A/B updates also mean that atomic rollbacks (ibid., §7.2.2.1.1) of all supporting ECUs can be performed in the event that part of the update fails.

Mender stores comprehensive audit logs that include details of the vehicle's software configuration before and after updates, including any changes to RXSWINs (ibid., §7.1.2.2, §7.1.2.3). This information is available over REST APIs

7 https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

and can be exported on a per-vehicle (ibid., §7.1.2.4) or per-type (ibid., §7.1.2.5) basis to be made available to type-approval authorities (ibid., §7.1.1.12).

The update binaries are securely stored on the Mender server, with strong role-based user authentication and cryptographic signatures to prevent unauthorized modification of the binaries that are to be flashed (ibid., §7.1.3.1). The Mender server and client have been developed with security at the core; threat modeling and risk assessments for the client code, server code, client-server interaction, and in-vehicle flashing are also available (ibid., §7.1.3.2).

This comprehensive coverage of the UNECE R156 requirements for software updates and software update management systems ensures that clients leveraging Mender can quickly and easily comply with the new regulations in Europe and Japan.

Mender as an ISO/SAE 21434-compliant parter

ISO/SAE 21434 requires that all suppliers responding to requests for quotations (RFQs) also conform to the standard (ISO/SAE 21434[8], §7.4.2). As a trusted automotive partner, the Mender team is ready to support clients with compliant process implementation and provide the necessary evidence to meet the requirements of an ISO/SAE 21434 audit.

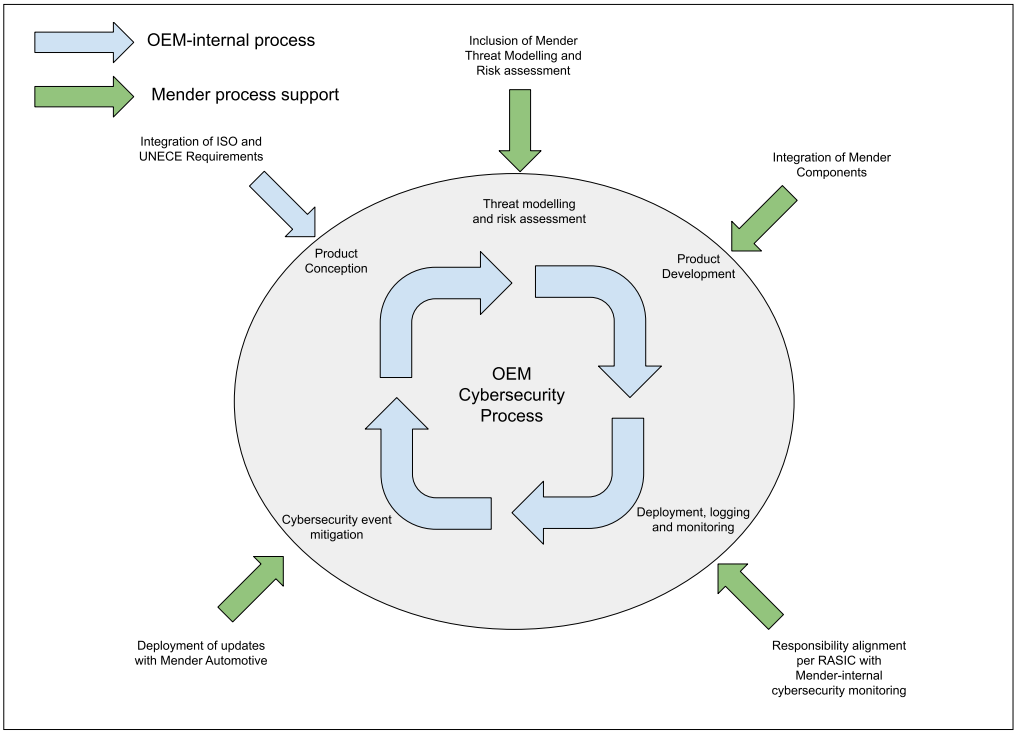
Compliant software components

Mender is supplied as an off-the-shelf component, and its integration into vehicle projects falls under the category of reuse (ibid., §6.4.4). As such, Mender can support customers with the *Reuse* analysis (ibid., §6.4.4, RQ-06-15), including the identification of any tailoring of cybersecurity activities that might be required (ibid., §6.4.3). The Mender team can also provide existing references to support the development of the cybersecurity case for integrating the Mender client (ibid., §6.4.7, RQ-06-23).

In line with ISO/SAE 21434, Mender has a security concept for the client and server (ibid., §9), which can be adapted to match the specific circumstances of the integration in a vehicle project, including a reference set of cybersecurity goals and requirements (ibid., §7.4.2(c)). Working from a template threat analysis and risk assessment for the Mender solution (in line with ibid., §15), robust evidence for cybersecurity threat modeling, mitigation, and validation can be developed quickly in cooperation with the client security teams.

8 https://www.iso.org/standard/70918.html

Compliant security processes



The Mender team continually monitors its own product development to ensure that cybersecurity threats and risks are modeled, detected, and mitigated (ibid., §7.4, RQ-07-02). Mender monitors vulnerability disclosures from defined sources (ibid., §8, RQ-08-01) and cross-references those with the libraries and dependencies of the Mender client and server to detect potential cybersecurity events related to Mender. According to defined triggers, collection, and triage processes (ibid., §8, RQ-08-02, RQ-08-03), the Mender team is able to respond to incidents rapidly and notify customers that might be affected.

On commencement of a commercial engagement, the Mender team works with customer teams to align responsibilities for cybersecurity events related to Mender (ibid., §7.4.3, RQ-07-04), defining and agreeing on a project- and customer-specific responsible, accountable, supportive, informed, and consulted (RASIC) matrix for each deployment (ibid., §7.4.3, RQ-07-08). This alignment reduces the effort required on the part of the customer to monitor their code base for meaningful cybersecurity events and provides peace of mind throughout the lifetime of the deployment that any events related to Mender will be handled following the established cybersecurity policies.

UNECE R155 compliance

Organizations wishing to achieve compliance with the UNECE R155 regulation are required to have considered cybersecurity throughout the development of their product and have personnel with specific automotive cybersecurity skills. The regulation makes specific reference to ISO/SAE 21434 (UNECE R155[9], §5.3.1(a)); the specifications of UNECE R155 (ibid., §7) substantially overlap with the ISO/SAE 21434 standard.

During the internal development process of Mender and in the development of threat and risk models for the Mender client and server, the threats and mitigations detailed in the regulation (ibid., Annex 5) have been considered; documentation can be provided on the implementation and validation of controls for all the threats that apply to Mender and its integration into vehicle projects.

The Mender team recommends that our customers and partners adopt cybersecurity processes aligned with ISO/SAE 21434, as doing so substantially covers the requirements of the UNECE R155 regulation. The Mender team can provide documentation to support a UNECE R155 audit, and the documentation artifacts and processes that are implemented for Mender ISO/SAE 21434 alignment can also be used in support of our clients' UNECE R155 compliance process.

The R155 regulation makes numerous references to the requirement for software updates as mitigation for multiple cybersecurity threats (ibid., Annex 5). The Mender implementation of an R156-compliant Software Update Management System (SUMS) supports our clients' compliance with this requirement.

9 https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

Northern.tech | MENDER by Northern.tech

Mender offers robust, secure, and customizable over-the-air (OTA) software updates for smart devices. Powering OTA software updates for more than a million devices worldwide over nearly a decade, Mender boasts a proven track record with Fortune 1000 clients, including Siemens, Thales, and ZF Group.

Learn more about OTA software update management.

Mender is developed and maintained by Northern.tech. Founded in 2008, Northern.tech is the leader in device lifecycle management with a mission to secure the world's connected devices.

Learn more about Mender for your vehicle platform

Learn more about Northern.tech for your device security needs