INSTITUT VEDECOM

Empowering sustainable mobilities

mobena

Next generation EV charging

SECURING THE CHARGING STATION

WHITE PAPER

A Comprehensive Cybersecurity Recommendations for EV Charging Ecosystem

About Mobena-X

Mobena-X is a collaborative R&D initiative designed to accelerate the deployment of next-generation electric vehicle (EV) charging solutions.

Building on a successful first phase (2021–2023), the current phase (2024–2026) brings together a consortium of 15 industrial partners - including EV manufacturers, charging infrastructure providers, cybersecurity experts, and testing organizations - united by a shared goal: creating a secure, interoperable, and user-centric EV charging ecosystem.

In response to the rapid growth of EV adoption and the increasing integration of intermittent renewable energy sources, Mobena-X addresses critical challenges such as energy flexibility, charging infrastructure interoperability, and EV ecosystem cybersecurity.

The project promotes advanced services such as Plug & Charge and Smart Charging, leveraging the ISO 15118 standard to simplify user authentication and enable a wide range of smart charging capabilities.

As a cross-sector catalyst, Mobena-X bridges the traditionally fragmented domains of mobility, energy, and buildings, offering a collaborative framework for innovation, testing, and standardization. Through quarterly demonstrations, strategic dissemination activities, and contributions to European regulatory frameworks, the project not only enhances the EV user experience but also positions electric vehicles as key assets within future smart and flexible energy grids. Mobena-X remains open to welcoming new partners during the current phase or in future phases of the initiative.

Mobena is a project by VEDECOM co-financed by a consortium with the support of ANR.

The Institute for Energy Transition (ITE) VEDECOM is dedicated to Accelerate the transition towards sustainable mobility by acting on mobility systems and practices.

Based in Versailles, the institute conducts R&D projects in collaboration with industry, local authorities, and academia, carries out exploratory studies, delivers turnkey services, and fosters the mobility ecosystem.

Operational partners

Institutionnal partners

A Comprehensive Cybersecurity Recommendations for EV Charging Ecosystem

As Electric Vehicle (EV) adoption scales, the charging infrastructure has emerged as a high-value target for cyber-attacks. The ecosystem is a complex intersection of physical hardware, network protocols, and backend management systems. Securing EV charging infrastructure requires a shared responsibility model. Charge Point Operators (CPOs), charging station's OEM, and equipment suppliers must align their security postures to mitigate risks that threaten both consumer data and national energy grid security.

This whitepaper synthesizes the results of a comprehensive EBIOS RM–based risk assessment conducted in the context of MOBENA initiative to provide concrete mitigation strategies tailored to the EV Charging ecosystem. The goal is to offer high-level guidance, without implementation-level detail, to decision-makers who must balance operational constraints, interoperability, regulatory compliance, and security requirements.

The Threat Landscape: Key Risk Vectors

The EV charging ecosystem faces risks across four primary domains.

1

Governance and Insider Threats

Improperly vetted contractors and the public exposure of maintenance schedules or internal organizational charts provide attackers with the reconnaissance needed for targeted strikes.

2

Communication Protocols

Vulnerabilities in legacy protocols, such as using OCPP with low security Profile, allowing une ncrypted data transmission and man-in-the-middle (MITM) attacks.

3

Physical Infrastructure

Publicly accessible charging stations are susceptible to hardware and software tampering, unauthorized debug port access, and the installation of payment skimming devices.

4

Supply Chain and Production

Compromises on the production line or during firmware flashing can result in the deployment of "tainted" devices across an entire fleet.

Strategic Mitigation Recommendations

To address these risks, a multi-layered security approach is required, focusing on the following core pillars:

1 - Governance and compliance

Security begins with organizational and personnel controls in the level of the organization to prevent reconnaissance and insider threats.

Public information hygiene

Avoid exposing maintenance schedules, organization charts,
firmware versions and contractor. The organizations must treat internal organizational details as confidential. Publicly accessible documents should not reveal staff contact details or internal reporting lines.

Contractor Management

Strict contractor governance, including background checks, NDAs, Tool hardening and security attestations.

Security Awareness

Mandatory cybersecurity training is required for all employees and contractors before they receive access to any charging point.

Internal specifications and hardware documentation

They must be restricted to mitigate the risk of targeted exploitation enforced through a strict "Need-to-Know" access policy.

2 - Secure Communication and Network Resilience

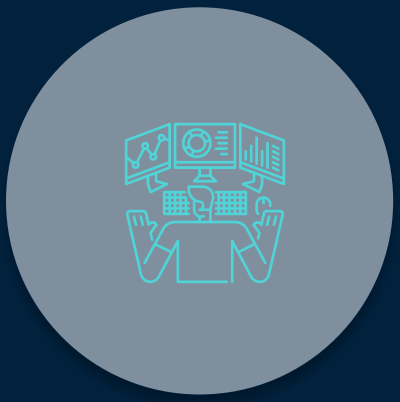
The integrity of the connection between the charging station and the Charging Station Management System (CSMS) is the backbone of the ecosystem.

Communication Hardening

OCPP Profile 1 and 2 must be deprecated. All communication must be used in encrypted WebSocket with mutual authentication (OCPP Profile 3) to support high level protection.

Encryption and Authentication

Deploy TLS 1.2/1.3 for all connections and implement Mutual TLS (mTLS) where both the station and the CSMS present valid certificates.



Advanced Monitoring

Utilize a Security Information and Event Management (SIEM) system equipped with packet inspection to detect protocol violations and malicious message injections within OCPP traffic.

Segmentation

The charging network should be logically separated into security zones using VLAN isolation between stations, backend systems, and maintenance tools.

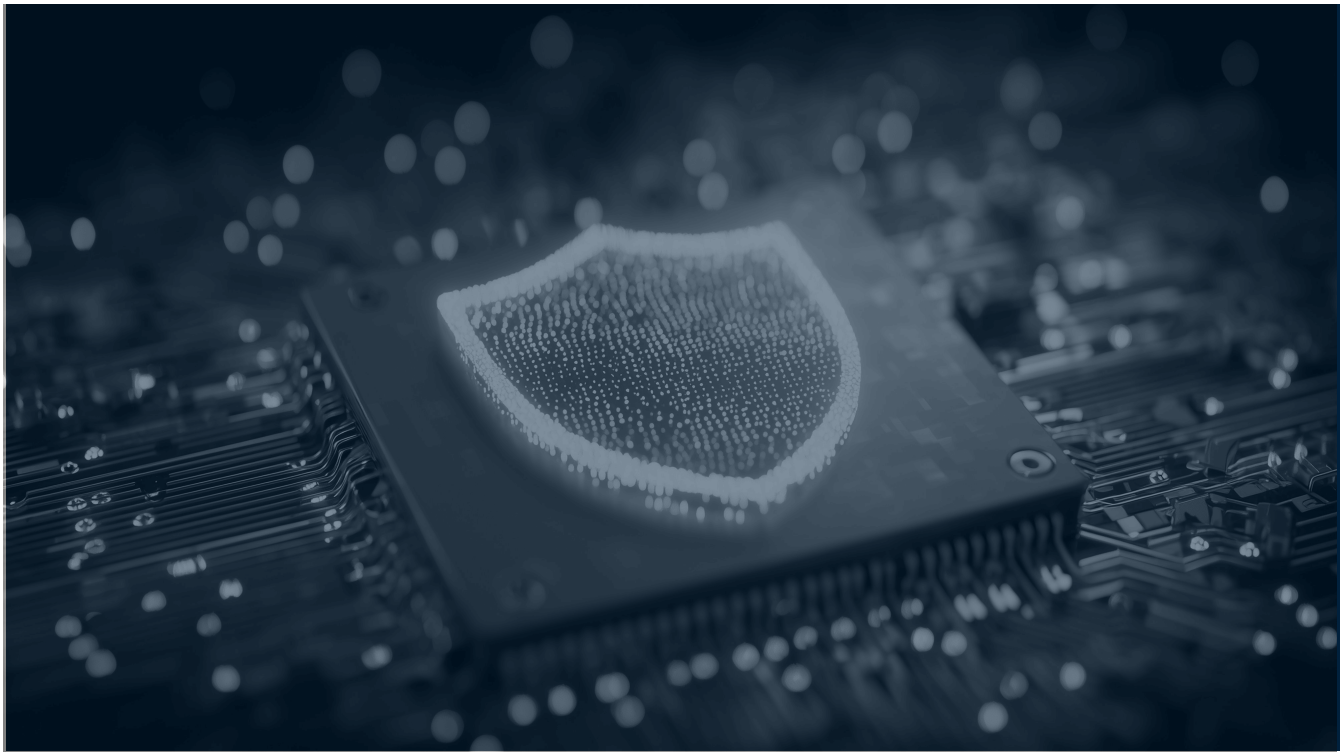
3 - Firmware & Software Security

1 Secure Firmware Lifecycle
Implement non-bypassable secure boot and cryptographically signed firmware updates to prevent the execution of malicious code. Firmware/Code readout protection (RDP/CRP) must be enabled on microcontrollers to prevent memory dumping.

2 Encrypted firmware storage
Protects firmware images using AES encryption to prevent extraction or reverse engineering. Adds Code obfuscation feature to reinforce anti–reverse-engineering protections to make firmware analysis significantly harder for attackers.

3 Hardened software stack with secure coding practices
Apply strict development standards (static analysis, vulnerability scanning, input validation) to reduce exploitable bugs and ensure robust, secure EVSE software.

4 Regular software updates with secure OTA mechanisms
Ensure charging stations receive authenticated, signed, and integrity-verified updates to patch vulnerabilities and maintain long-term security.



4 - Secure Storage and Configuration

Implement secure and isolated data storage based on Tamper resistant Hardware technology: Secure Elements (SE), TPMs, or HSMs for key generation, storage, certificate protection and avoid storing cryptographic materials (keys, certificate) in plaintext to prevent certificate cloning, MITM attacks, and Plug-and-Charge abuse.

Protect configuration parameters and files (network settings, OCPP endpoints, logs and data) using encryption and integrity-protection -to prevent unauthorized modification or tampering.

Maintain detailed audit trail mechanisms, tamper-evident logs (immutable) of all configuration changes, administrative actions, and access attempts to support traceability, accountability, and incident investigation.

Enforce strict data retention and minimization policies and store only the data strictly required for operation, retain it for the minimum duration necessary, and regularly purge old or unused data to reduce exposure in case of breach.

5 - Physical and Hardware Protection

Charging stations are often located in public, unsupervised areas, making physical access much easier.

Enclosure Security

Use high-security locks and uniquely numbered tamper-evident seals on all access panels. Stations should have intrusion detection sensors that trigger real-time alerts to the CSMS if an enclosure is opened.

Board-Level Security

Production PCBs should have silkscreen labels removed to hide debug port locations. All hardware debug interfaces (JTAG, UART, SWD, ...) must be permanently disabled or cryptographically locked in production.

Payment Terminal Integrity

Maintenance of payment systems requires a two-person rule (dual control). Technicians should use RF detection and scanning to identify unauthorized wireless skimming devices post-maintenance.

Surveillance

High-value or risk sites like high power DC charging stations require mandatory video surveillance with motion detection and at least 30 days of recording retention to monitor activity around the equipment.

6 - Identity and Access Management

Protecting administrative access is critical to preventing fleet-wide compromises.

The enforcement of individual and unique credentials and the elimination of shared accounts are mandatory to mitigate the insider threat risk.

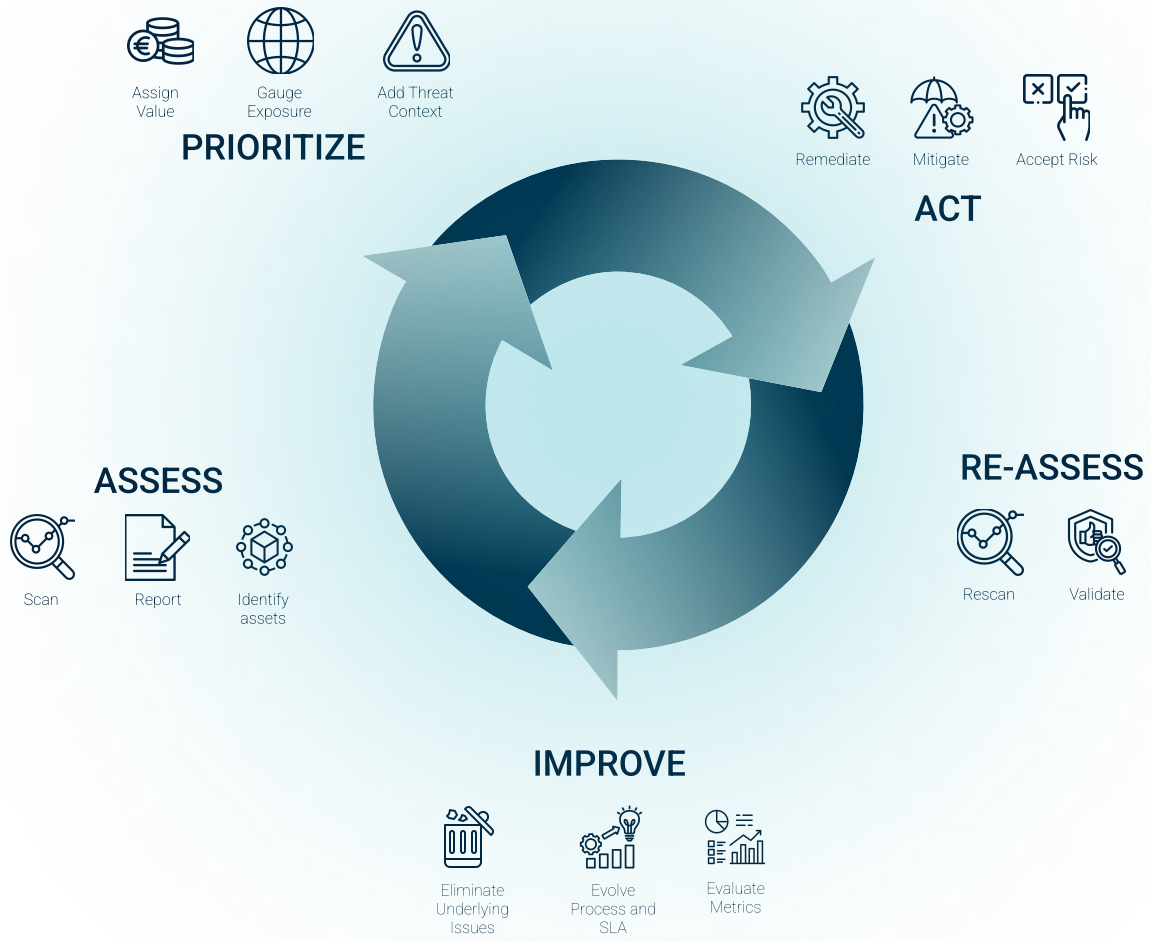
Access Controls

Enforce Multi-Factor Authentication (MFA) for all high-privilege administrative accounts. Implement the principle of least privilege via Role-Based Access Control (RBAC) to ensure that personnel only have access to functions required for their specific responsibilities.

Dual Authorization

Require mandatory dual authorization for "mass operations," such as fleet-wide configuration changes or firmware flashing on the production line.

7- Vulnerability Management, Incident Response, and Monitoring



A proactive posture is required to manage emerging threats.

Vulnerability Management: Maintain a program that actively monitors CVE databases for protocols implementations, embedded system components and firmware. Critical patches should be applied within a defined window, such as 30 days post-disclosure.

Deploy a centralized SIEM to collect and correlate logs from charging stations, backend systems, and network infrastructure, enabling real-time anomaly detection and rapid incident response.

Implement network and host-based IDS/IPS to continuously monitor traffic, detect intrusions, and block malicious activity such as DoS or protocol manipulation.

Incident Recovery: Establish a comprehensive disaster recovery plan covering mass charging station compromise and ransomware scenarios. Ensure that immutable audit trails and logs are maintained for forensic analysis.

Conclusion: Building A Secure and Resilient EV Charging Future

Cybersecurity in the EV charging ecosystem is not a feature; it is a fundamental requirement for the viability of the grid and users. The conducted risk analysis demonstrates that a defensible future depends on a rigorous lifecycle of hardware-level roots of trust, technical protocol hardening, and continuous operational vigilance.

The security of the EV charging ecosystem depends on the continuous application of these mitigation strategies across the entire lifecycle of the infrastructure. By focusing on governance, encrypted communications, and physical integrity, stakeholders can build a resilient network that supports the future of electric mobility.

By adhering to these recommendations and the upcoming European cybersecurity directives, the automotive and energy industries can ensure that the transition
to electric mobility remains resilient against an increasingly sophisticated threat landscape.

Contributors

- VEDECOM
- Thales
- ETAS

Continue the conversation

Cybersecurity in EV charging is a collective challenge that requires ongoing dialogue, shared expertise, and coordinated action across the ecosystem.

Further discussion with MOBENA partners

If you would like to explore the topics covered in this white paper, discuss specific use cases, or engage with MOBENA experts, we invite you to get in touch with :

→Yassir Dahmane, EV Charging Technology Expert - yassir.dahmane@vedecom.fr

→Ahmed Amine Melhaoui, Project Manager - ahmedamine.melhaoui@vedecom.fr

Join the consortium

Do you want to be in the premium starting block to drive the access and deployment of new generation of interoperable EV recharge service ?

Mobena continues to welcome new industrial partners from the e-mobility ecosystem who are interested in positioning themselves in Plug and Charge and Smart Charging and contributing to the structuring of the offer. The project is also open to institutional partners, who will help prepare for the seamless introduction of these offers to the European market and promote the project's resulting orientations

CONTACT US

Mobena-X

23 bis Allée des Marronniers, 78000 Versailles (France)

contact@mobena.org

www.mobena.org