

# Recommendation of Charging Interface Initiative e.V.

**CharIN implementation guide for TLS with ISO 15118: avoidance and handling of wrong implementations**

Recommendations and implementation guidelines for EV and EVSE manufacturers

Version 1

2026-04-18

Charging Interface  
Initiative (CharIN) e.V.  
EUREF-Campus 10-11  
10829 Berlin

**Contact**

Phone +49 30 288 8388-0  
Mail [coordination@charin.global](mailto:coordination@charin.global)  
Web [www.charin.global](http://www.charin.global)

## Contents

Executive Summary .....	3
1. Introduction .....	4
2. Background and Motivation .....	4
2.1. Evolution of protocols and TLS versions .....	4
3. Scope and Purpose .....	5
4. Technical Problem Statement .....	6
4.1. Missing exchange of TLS version information and supported V2G protocol in startup sequence ...	6
4.2. Mixed TLS configurations in EVSE implementations .....	6
4.3. Dual TLS handshake and downgrade failures .....	6
4.4. Lack of explicit errors and restart rules .....	10
4.5. Identified root causes .....	10
5. Recommendations and best practices .....	11
5.1. ISO 15118-202 (ESDP) implementation as a basis .....	11
5.2. Recommended mapping between protocol and TLS version .....	11
5.3. EVSE TLS version and algorithm selection logic .....	12
5.4. EVSE implementation guidance .....	12
5.5. EV TLS configuration .....	13
5.6. TLS library configuration (example: OpenSSL) .....	13
5.7. Deactivation of TLS 1.3 “Middlebox Compatibility Mode” .....	14
5.8. Initial guidance on restart and fallback .....	14
6. Testing and certification inputs .....	14
6.1. Positive interoperability test cases .....	14
6.2. Suggested certification integration .....	15
7. Harmonization with Standards .....	16
8. Conclusion .....	16
9. Reference .....	17

## Executive Summary

ISO 15118-2 and ISO 15118-20 are being deployed in parallel in the field. ISO 15118-2 requires TLS 1.2 for Plug & Charge, while ISO 15118-20 requires TLS 1.3 with mutual authentication, using different cipher suites and certificate requirements.

Vehicles increasingly support both ISO 15118-2 and ISO 15118-20 and therefore offer TLS 1.2 and TLS 1.3 in the TLS ClientHello. In contrast, many existing public chargers implement only ISO 15118-2 and rely on TLS libraries that enable TLS 1.3 and modern cipher suites by default. As a result, inconsistent combinations of TLS versions, cipher suites, elliptic curves, and certificate chains are selected, leading to TLS handshake failures and loss of Plug & Charge functionality.

Two main classes of interoperability issues are being observed:

- EVSEs respond with TLS 1.3 while using ISO 15118-2 certificate profiles and parameters that are not compatible with the selected TLS 1.3 configuration.
- EVSEs attempt a TLS 1.2 downgrade but select parameters from a TLS 1.3 configuration (e.g. secp521r1 or unsupported signature algorithms), which violates ISO 15118-2 constraints for TLS 1.2 in the context of V2G communication.

In both cases, the EV aborts the handshake with fatal alerts, and charging often continues only via TCP and EIM authentication after several retries, causing user-visible errors and delays.

The document defines the following guiding principles:

- As of now, CharIN recommends that ISO 15118-2 should be implemented with TLS 1.2 only, using the cipher suites and signature algorithms defined in ISO 15118-2. This recommendation might be revised in the future.
- ISO 15118-20 should be implemented with TLS 1.3 only, using the cipher suites and signature algorithms defined in ISO 15118-20.
- TLS libraries should be explicitly configured according to the selected protocol profile, and default library behavior should not be relied upon.
- Clear testing practices and logging mechanisms should be implemented to detect and diagnose interoperability issues prior to deployment.
- Early capability exchange mechanisms, such as ISO 15118-202 (ESDP), should be implemented to improve interoperability and avoid ambiguous TLS and protocol negotiation.

This document provides implementation guidance and test scenarios to mitigate these issues in existing deployments.

## 1. Introduction

This document provides recommendations to harmonize the use of Transport Layer Security (TLS) versions and related cryptographic parameters between Electric Vehicles (EVs) and Electric Vehicle Supply Equipment (EVSEs) in the context of charging communication. It aims to improve interoperability and Plug & Charge robustness during the TLS handshake phase by clarifying how ISO 15118-2 and ISO 15118-20 should be combined with TLS 1.2 and TLS 1.3.

The recommendations focus on the coexistence of multiple protocol generations and TLS versions in the field. They describe the consistent selection of TLS 1.2 and TLS 1.3 together with the corresponding cipher suites and elliptic curves, and the correct application of the Plug & Charge certificate profiles as specified in ISO 15118-2 and ISO 15118-20. The document is built on the requirements defined in ISO 15118-2 and ISO 15118-20, and field experience and interoperability findings reported by CharIN members.

## 2. Background and Motivation

### 2.1. Evolution of protocols and TLS versions

The CCS ecosystem has evolved through two protocol generations:

- **ISO 15118-2 Edition 1 (2014):** Introduced TLS 1.2 with a defined set of cipher suites and signature algorithms, using secp256r1 as an elliptic curve for the PKI used for TLS and Plug & Charge certificates.
- **ISO 15118-20 Edition 1 (2022):** Introduced TLS 1.3 with new cipher suites and the use of secp521r1 and Curve448 for the PKI used for TLS and Plug & Charge certificates.

ISO 15118-2:2014 specifies the cipher suites and signature algorithms to be used for TLS communication. The standard defines the use of the following cipher suites (see ISO 15118-2:2014, Table 7):

Supported cipher suites:

- TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 (IETF RFC 5289)
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 (IETF RFC 5289)

In addition, ISO 15118-2:2014 specifies that, for each V2G entity, the signature operation shall be based on elliptic curve cryptography (ECC) using the curve secp256r1 and the ECDSA signature algorithm (see ISO 15118-2:2014, requirement V2G2-006).

ISO 15118-20:2022 introduces TLS 1.3 for V2G communication and defines updated cipher suites and signature algorithms (see ISO 15118-20:2022, Table 6 and Table 8). The following parameters are specified:

Supported cipher suites:

- TLS\_AES\_256\_GCM\_SHA384 (IETF RFC 5116)
- TLS\_CHACHA20\_POLY1305\_SHA256 (IETF RFC 8439)

Supported signature algorithms:

- ecdsa\_secp521r1\_sha512 (ANSI X9.62)
- ed448 (IETF RFC 8032)

ISO 15118-20:2022 also mentions the possibility of using TLS 1.3 together with ISO 15118-2 communication. ISO 15118-2:2014 does not explicitly prohibit the use of TLS 1.3. However, to avoid interoperability issues, it is recommended to use ISO 15118-2 communication in combination with TLS 1.2 only.

### 3. Scope and Purpose

This implementation guide addresses:

- Handling of TLS version interoperability issues between ISO 15118-2 and ISO 15118-20 on the DC and AC charging interface.
- Standard-conform TLS handshake behavior between EVCC (EV) and SECC (EVSE), including cipher suite and certificate selection.

By providing:

- Implementation guidance for EV, EVSE, and backend systems with a focus on existing field deployments and near-term vehicles.
- Recommendations for test cases and certification input.

This document was created within the CharIN Focus Group Charging Communication and its subgroup Field Issues. It represents the consensus reached in this group at the time of writing and is intended to support ongoing standardization work and to facilitate discussion among OEMs, EVSE manufacturers, charge point operators, backend providers, and test houses. It does not constitute a normative standard but provides system-level guidance and recommendations for implementation and testing.

## 4. Technical Problem Statement

### 4.1. Missing exchange of TLS version information and supported V2G protocol in startup sequence

The communication start-up sequence described in ISO 15118-2 and ISO 15118-20 does not allow the EVCC and SECC to exchange information about the intended TLS version (and cipher suite) and the intended V2G protocol before the TLS channel is setup. In case of implementation errors in the SECC (TLS 1.3 support without implementation of ISO 15118-20 certificates), the TLS handshake will fail.

ISO 15118-202 (ESDP) addresses this limitation by enabling early information exchange about supported security profiles (such as TLS versions) and V2G protocols, but deployment of this new layer will take time and will not address immediate issues in existing field systems.

### 4.2. Mixed TLS configurations in EVSE implementations

EVSEs commonly use OpenSSL or similar TLS libraries. Since OpenSSL 1.1.1, TLS 1.3 has been enabled by default. If EVSE implementations leave the TLS stack in its default configuration, the following situation occurs:

- The EV offers TLS 1.2 and 1.3, and at least secp256r1 and secp521r1 in the ClientHello.
- The EVSE TLS stack automatically selects TLS 1.3 as the highest version and preferred algorithms such as secp521r1, even though the application has been designed as an ISO 15118-2 server expecting TLS 1.2 and secp256r1.
- The certificate chain and signature algorithms configure for ISO 15118-2 (secp256r1) no longer matched the TLS 1.3 cipher suite selection.

This mismatch triggers fatal alerts on the EV side and causes Plug & Charge failures.

These issues highlight that default behavior of TLS libraries cannot be relied upon in the context of ISO 15118-2/-20, because the standards referenced specific cipher suites and algorithms that needed to be enforced explicitly.

### 4.3. Dual TLS handshake and downgrade failures

Vehicle implementations supporting both ISO 15118-2 and ISO 15118-20 offer a “dual TLS handshake” where TLS 1.3 and TLS 1.2 are both proposed in the ClientHello.

Examples of typical protocols/TLS profiles for EVSE types:

EVSE type	Protocols	TLS profile	Target use case
Public HPC DC charger	ISO 15118-2	TLS 1.2 (ISO 15118-2)	Public DC charging with Plug & Charge
DC home / bidirectional wallbox	ISO 15118-20	TLS 1.3 (ISO 15118-20)	Home DC and bidirectional charging
Full multi-protocol EVSE (typically for depot use case)	ISO 15118-2, ISO 15118-20	TLS 1.2 (ISO 15118-2), TLS 1.3 (ISO 15118-20)	Future-proof premium installations

Three representative traces illustrate the resulting behavior:

- **Example A – EVSE attempted TLS 1.3 with ISO 15118-2 certificates:**

The EV receives a TLS 1.3 ServerHello with key\_share secp521r1 and a TLS\_AES\_256\_GCM\_SHA384 cipher suite, but the EVSE sends ISO 15118-2 based certificates and CertificateVerify using secp256r1. The EV reports a TLS 1.3 fatal alert “Bad Record MAC” and aborts.

```

▼ TLSv1.3 Record Layer: Handshake Protocol: Server Hello
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 191
  ▼ Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 187
    Version: TLS 1.2 (0x0303)
    Random: 094fd9793f75cde1c30c62a9f82012581960d187344e01c8bf6797f16990c17d
    Session ID Length: 0
    Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    Compression Method: null (0)
    Extensions Length: 147
    ▼ Extension: supported_versions (len=2)
      Type: supported_versions (43)
      Length: 2
      Supported Version: TLS 1.3 (0x0304)
    ▼ Extension: key_share (len=137)
      Type: key_share (51)
      Length: 137
      ▼ Key Share extension
        > Key Share Entry: Group: secp521r1, Key Exchange length: 133
        [JA3S Fullstring: 771,4866,43-51]
        [JA3S: 15af977ce25de452b96affa2addb10361]
  
```



(a) ClientHello and ServerHello negotiation (TLS 1.3 selection)

```

v TLSv1.3 Record Layer: Handshake Protocol: Certificate Verify
  Opaque Type: Application Data (23)
  Version: TLS 1.2 (0x0303)
  Length: 95
  [Content Type: Handshake (22)]
v Handshake Protocol: Certificate Verify
  Handshake Type: Certificate Verify (15)
  Length: 74
  > Signature Algorithm: ecdsa_secp256r1_sha256 (0x0403)
  Signature length: 70
  Signature: 304402205e85a0910e8a7fbbb1306c5a286098b527b54a103b58e884b721ad2ec2d3803a...
  
```




(b) Certificate and CertificateVerify messages showing mismatch with ISO 15118-2 profile

- Example B – TLS 1.2 downgrade with wrong parameters:

```

v Transport Layer Security
v TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 217
v Handshake Protocol: Server Key Exchange
  Handshake Type: Server Key Exchange (12)
  Length: 213
v EC Diffie-Hellman Server Params
  Curve Type: named_curve (0x03)
  Named Curve: secp521r1 (0x0019)
  Pubkey Length: 133
  Pubkey: 04016fefcf5cf4b141bc0badb0894312ac1272dc0ab9073c9060df5bffb9b56fcadac8b4...
  > Signature Algorithm: ecdsa_secp521r1_sha512 (0x0603)
  Signature Length: 72
  Signature: 3046022100e895153d02e308483bd8e0d76fda01542fa39f476b4e0aa2d4f5dbc3a1591f...
  
```



TLS 1.2 downgrade with non-compliant parameters

The EVSE responds with TLS 1.2 and a correct ServerHello but choose secp521r1 and a TLS 1.3 signature algorithm in ServerKeyExchange. This illegal combination leads to a TLS 1.2 fatal alert “Decode Error” on the EV.

- **Example C – Successful TLS 1.2 downgrade:**

The EVSE correctly downgrades to TLS 1.2, selects a cipher suite allowed by ISO 15118-2 (e.g. TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256) and uses secp256r1 for key exchange and signatures. Plug & Charge succeeds.

```

▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 42
    ▼ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 38
      Version: TLS 1.2 (0x0303)
      > Random: 9cb6bda609720937cd447009c330854d806f49d9173332ab4d3ed5354be55e36
      Session ID Length: 0
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ✓
      Compression Method: null (0)
      [JA3S Fullstring: 771,49187,]
      [JA3S: 433e8944dbb6c575c4166e99747132c0]
  
```

(a) TLS version negotiation and cipher suite selection

```

▼ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 148
  ▼ Handshake Protocol: Server Key Exchange
    Handshake Type: Server Key Exchange (12)
    Length: 144
    ▼ EC Diffie-Hellman Server Params
      Curve Type: named_curve (0x03)
      Named Curve: secp256r1 (0x0017) ✓
      Pubkey Length: 65
      Pubkey: 046e382dfc1222e5f83f284d7421e5a58f49525a555bb592074d1173a4:
      > Signature Algorithm: ecdsa_secp256r1_sha256 (0x0403) ✓
      Signature Length: 71
      Signature: 304502203e6800114b153f423b8d06c367d6eb0034798be23fcf5d5:
  
```

(b) Certificate exchange and successful handshake completion

These examples demonstrate that TLS interoperability depends not only on the TLS version but also on consistent combinations of cipher suite, elliptic curve and certificate chain.

#### 4.4. Lack of explicit errors and restart rules

Current ISO 15118-2 and ISO 15118-20 editions do not contain explicit error handling and restart rules for TLS version negotiation failures between EV and EVSE.

In practice, different implementations behave differently:

- Some EVSEs retry the communication and eventually fall back to TCP without TLS, leading to EIM-only charging.
- Some EVs require a manual re-plug to reset the sequence.
- Some systems terminate with persistent fault indication.

This fragmented behavior reduces user experience and complicates troubleshooting. Harmonized restart and fallback mechanisms are therefore required and will be defined in a future document.

#### 4.5. Identified root causes

Field issues show recurring TLS-related interoperability issues in mixed deployments of DIN/TS 70121:2024-11, ISO 15118-2 and ISO 15118-20.

The following causes of these issues are identified:

- Many observed failures are not caused by an incorrect standard text but incomplete system-level guidance on how to combine multiple protocol generations with two TLS versions.
- Mixed protocol/TLS combinations such as “ISO 15118-2 over TLS 1.3” are theoretically possible but create significant complexity for security certificates, cipher suites and test coverage.
- The reliance on default TLS library behavior leads to inconsistent configurations when not explicitly aligned with ISO 15118 requirements.
- The absence of early capability signaling in current deployments contributes to interoperability issues.

Based on this analysis, the need for an interim CharIN document has been identified with the objective to:

- Provide guidance on protocol/TLS combinations that should be supported or avoided.
- Recommend TLS implementation logic for EVSEs and EVs.
- Support testing and validation through representative test cases.
- Establish a basis for future harmonized restart and fallback mechanisms.

## 5. Recommendations and best practices

### 5.1. ISO 15118-202 (ESDP) implementation as a basis.

ISO 15118-202 (ESDP) enables early capability exchange between EV and EVSE, allowing supported V2G protocols, TLS versions and associated security profiles to be communicated prior to the TLS handshake.

This allows the EV to select a compatible configuration and construct a consistent ClientHello, reducing the risk of mismatched TLS parameters and enabling early detection of incompatible or misconfigured EVSE implementations.

ISO 15118-202 can be deployed alongside existing DIN SPEC 70121, ISO 15118-2 and ISO 15118-20 implementations without requiring modifications to these protocols.

It is recommended to implement ISO 15118-202, and in particular to use the Charging Service extension (ISO 15118-202, Clause 6.5.6) to explicitly declare supported charging services together with their associated security profiles. This improves interoperability between DIN SPEC 70121, ISO 15118-2, and ISO 15118-20 by avoiding implicit or ambiguous assumptions regarding TLS and security behavior.

### 5.2. Recommended mapping between protocol and TLS version

Following mapping is suggested:

- ISO 15118-2: TLS 1.2 only, using cipher suites and signature algorithms as specified in ISO 15118-2 (e.g. secp256r1).
- ISO 15118-20: TLS 1.3 only, using cipher suites and signature algorithms as specified in ISO 15118-20 (e.g. secp521r1).

Implementations are recommended to avoid the following combination, as it does not support ESDP:

- ISO 15118-2 over TLS 1.3.

### 5.3. EVSE TLS version and algorithm selection logic

For EVSE that supports multiple protocols, the following behavior is recommended upon receiving a ClientHello from the EV:

- Evaluate the “supported\_versions” extension and the offered cipher suites and signature algorithms.
- Determine which application protocols (DIN 70121, ISO 15118-2, ISO 15118-20) were supported by this EVSE.
- Select TLS 1.3 only if ISO 15118-20 is supported and the EVSE possesses a TLS 1.3 compatible certificate chain and cipher suites as defined in ISO 15118-20.
- Otherwise, select TLS 1.2 if ISO 15118-2 is supported and a TLS 1.2 profile per ISO 15118-2 is available.
- If neither mapping is possible, a restart mechanism should be applied. Detailed guidance on restart mechanisms will be provided in a separate document.

When TLS 1.2 is selected, the EVSE should limit itself to cipher suites and signature algorithms from ISO 15118-2 and use secp256r1 for certificates and key exchange. When TLS 1.3 is selected, cipher suites and signature algorithms from ISO 15118-20 and secp521r1 should be used consistently.

### 5.4. EVSE implementation guidance

EVSE manufacturers and operators are advised to:

- Define explicit configuration profiles for each supported protocol combination (DIN only, DIN + ISO 15118-2, DIN + ISO 15118-20, all three).
- For each profile, configure the TLS stack with:
  - Allowed TLS versions.
  - Allowed cipher suites and signature algorithms.
  - The correct certificate chain with an appropriate elliptic curve.
- Verify that automatic selection mechanisms in the TLS library do not override these restrictions.
- Implement logging that clearly indicates which TLS version, cipher suite and curve have been selected in each handshake, to support field diagnosis of interoperability issues.
- Disable TLS 1.3 middlebox compatibility mode.
- Clearly communicate supported protocol profiles to customers and operators. In particular, EVSEs that support ISO 15118-20 but not ISO 15118-2 should clearly communicate this limitation to customers.

Operators are encouraged to run the recommended test cases from section 6 as part of acceptance testing when deploying new firmware or TLS library versions.

## 5.5. EV TLS configuration

Vehicle implementations supporting both ISO 15118-2 and ISO 15118-20 are recommended to:

- Offer both TLS 1.3 and TLS 1.2 in the “supported\_versions” extension, with TLS 1.3 listed first.
- Offer cipher suites and signature algorithms required by ISO 15118-20, followed by those required by ISO 15118-2.

Include `secp521r1` and `secp256r1` in the `key_share` and `supported_groups` lists.

EV engineers are advised to:

- Implement flexible ClientHello construction, allowing updates to support cipher suites and curves without changing the core application logic.
- Treat certain TLS alerts as indicators of EVSE misconfiguration and avoid persistent fault states when user-initiated retries could restore service.
- Define clear prioritization of application protocols after TLS setup (for example, preference for ISO 15118-20 when both EV and EVSE supported it, otherwise ISO 15118-2, otherwise DIN 70121).

## 5.6. TLS library configuration (example: OpenSSL)

For EVSE implementations based on OpenSSL:

- Explicitly configuring the set of allowed TLS versions per communication protocol profile instead of using the library default (`TLS_server_method`).
- Restricting cipher suites and signature algorithms to those listed in ISO 15118-2 when the EVSE operated in an ISO 15118-2 profile.
- Restricting cipher suites and signature algorithms to those listed in ISO 15118-20 when operating in an ISO 15118-20 profile.
- Verifying that the certificate chain used by the TLS library matched the selected elliptic curve (`secp256r1` vs `secp521r1`).

Implementing regression tests to ensure that a library update enabling additional features (for instance new TLS 1.3 cipher suites) did not change the effective behavior of the ISO 15118-2 profile.

## 5.7. Deactivation of TLS 1.3 “Middlebox Compatibility Mode”

Some TLS 1.3 stacks support a “middlebox compatibility mode” that inserts ChangeCipherSpec “dummy” messages in the handshake. In environments where the EVCC does not expect such messages, this can lead to handshake failure.

Because EV charging communication typically does not traverse legacy middleboxes, proxies or firewalls, it is recommended to deactivate TLS 1.3 middlebox compatibility mode on both EV and EVSE sides to improve interoperability.

## 5.8. Initial guidance on restart and fallback

A dedicated document will focus on restart mechanism guidelines soon.

# 6. Testing and certification inputs

Testing is considered a critical tool to prevent field issues. The following test cases are proposed:

## 6.1. Positive interoperability test cases

### T1 – ISO 15118-2 EVSE with future EV (TLS 1.2 downgrade)

- EV offers TLS 1.3 and TLS 1.2 and both ECC curves.
- EVSE implements ISO 15118-2 only.
- Expected result: EVSE selects TLS 1.2, choose an ISO 15118-2 compliant cipher suite and secp256r1, processes only –2 TLS extensions, handshake succeeds. and later chooses ISO 15118-2 in SupportedAppProtocol.

### T2 – ISO 15118-20 EVSE with future EV (TLS 1.3 operation)

- EV offers TLS 1.3 and TLS 1.2 and both ECC curves.
- EVSE implements ISO 15118-20 only.

Expected result: EVSE selects TLS 1.3, uses ISO 15118-20 cipher suites and secp521r1 certificates, processes only –20 TLS extensions, handshake succeeds, and later chooses ISO 15118-20 in SupportedAppProtocol.

### **T3 – Multi-protocol EVSE with EV expecting ISO 15118-2**

- EV supports DIN + ISO 15118-2, but not ISO 15118-20.
- EVSE supports all three protocols.
- Expected result: EVSE selects TLS 1.2, handshake succeeds and later chooses ISO 15118-2 in SupportedAppProtocol.

## **6.2. Suggested certification integration**

CharIN and test system providers can integrate these test cases into:

- CCS interoperability events.
- Formal test specifications for EVSE and EV certification.
- Regression test suites for TLS library upgrades.

Test houses can document the exact TLS versions, cipher suites, curves and certificates used in each test to ensure reproducibility.

It is planned to integrate these test cases into CharIN test programs. In the meantime, manufacturers can use the proposed test cases to perform their own testing.

NOTE Above test cases are going to be integrated into the CharIN test program as follows: T1 and T3 as part of the “EVSE Extended” test package, where T3 is not applied to EVSE that have implemented only ISO 15118-2, and T2 as part of the “EVSE Advanced” test package.

## 7. Harmonization with Standards

The recommendations in this implementation guide are aligned with and complemented by the following standards:

- ISO 15118-2 Ed.1: The standard requires at least TLS 1.2 with selected cipher suites if PnC is used. Stronger encryption methods are generally allowed but not specified.
- ISO 15118-20: The standard requires TLS 1.3 for all ISO 15118-20 energy transfer and authorization services and recommends consistent use of defined cipher suites and secp521r1 certificates.

The recommendations do not override any legal or regulatory requirements and are intended to be compatible with AFIR implementation.

## 8. Conclusion

The coexistence of ISO 15118-2 and ISO 15118-20, together with the introduction of TLS 1.3, have created practical interoperability risks in the field. These risks stem from inconsistent mapping between communication protocols and TLS versions, default behavior of TLS libraries and the absence of explicit restart rules in current standards.

Pragmatic principles to mitigate these risks are the following:

- Keep ISO 15118-2 bound to TLS 1.2 and ISO 15118-20 bound to TLS 1.3.
- Configure TLS libraries explicitly and consistently with the chosen protocol profile.
- Adopt clear testing practices and logging to detect issues before deployment.
- To strengthen interoperability between ISO 15118-2 and ISO 15118-20, the security profile information should be implemented via the Charging Service extension defined in ISO PAS 15118-202.

These measures are expected to reduce TLS handshake failures, preserve Plug & Charge functionality, and support a smoother migration towards ISO 15118-20-based solutions.

## 9. Reference

This document was created by the focus group Charging Communication and within the subgroup Field issues of the CharIN association.

The Focus group Charging Communication supports development, specification and tests of charging communication. It closes gaps and provides recommendations for communication protocols of the electric vehicle (EV) charging system.

The Field issues subgroup monitors and analyzes trends, developments, and issues in charging communication. It provides a platform for information exchange and technical discussion among industry stakeholders. It identifies gaps and emerging needs in communication protocols. It supports the alignment of CharIN activities with international standardization. And it facilitates knowledge transfer and best practice sharing.

### Document Status:

This whitepaper represents the consensus reached within the Field issues subgroup as of April 2026. It is intended to support ongoing standardization efforts and facilitate stakeholder discussions.

### Referenced Standards:

- ISO 15118-2:2014 – Road vehicles – Vehicle to grid communication interface – Part 2: Network and application protocol requirements
- ISO 15118-20:2022 – Road vehicles – Vehicle to grid communication interface – Part 20: 2nd generation network layer and application layer requirements
- ISO 15118-202 – Road vehicles – Vehicle to grid communication interface – Part 202: Energy Services Discovery Protocol (ESDP)

### Contributors:

- Xi Zhang (EcoG)
- Celine Rüdiger (Ferchau Automotive)
- Magnus Ilisch (Mercedes-Benz)
- Michael Schwaiger (BMW)
- Olivier Bertin (MAN)
- Alexander Irrgang (Mercedes-Benz)
- Fabian Eisele (Vector)
- Devraj Dutt (Jaguar Land Rover)
- George Gao (Schneider Electric)
- Miguel Rodriguez Escude (ABB)
- Kai Rieger-Grothaus (Shell)
- Thorsten Kuenzig (BMW)
- Maik Schumacher (NOW GmbH)
- Anaïs Bonnard (CharIN e.V.)