38th International Electric Vehicle Symposium and Exhibition (EVS38) Göteborg, Sweden, June 15-18, 2025

CharIN e.V. – OPNC, a unified and open protocol for Plug & Charge and global EV interoperability

Daniela Soler[1], Jeremy Schofield

[1] *CharIN Academy GmbH, EUREF-Campus 10-11, 10829 Berlin, Germany*, *coordination@charin.global*

Executive Summary

As the global electric vehicle (EV) market continues to grow, the demand for secure and user-friendly charging solutions has become increasingly important. Plug & Charge, as standardized under ISO 15118, was introduced to simplify the charging process by enabling automatic authentication and billing. However, real-world deployments have revealed fragmented ecosystems, limited interoperability, and vendor-specific implementations.

To address these challenges, CharIN launched the Open Plug and Charge (OPNC) protocol initiative—a collaborative, vendor-agnostic framework designed to unify backend communication in ISO 15118-based Plug & Charge systems. OPNC defines open procedures for trust anchor resolution, certificate provisioning, and backend integration, enabling compatibility across multiple Public Key Infrastructures (PKIs) and actors such as OEMs, CPOs, MOs, and Certificate Authorities.

Developed through an open governance model, OPNC supports secure and scalable Plug & Charge deployments while preserving technical flexibility. This paper presents the motivation, architecture, and governance structure of OPNC, outlines its current capabilities in version 1.0, and provides a roadmap for future developments.

Keywords: Electric Vehicles, Standardization, International Networking, Smart Charging

1. Introduction

The Charging Interface Initiative e.V. (CharIN) is a registered non-profit association founded in 2015 to promote the Combined Charging System (CCS) as a global standard. Its core mission includes supporting the evolution of CCS-related standards, enabling the certification of CCS-based products, and guiding the development of next-generation high-powered solutions such as the Megawatt Charging System (MCS). Since then, CharIN has grown to include over 300 international members across the entire e-mobility value chain.

Operating under a neutral and collaborative umbrella, CharIN brings together stakeholders from across the industry spectrum, including automakers, charging station manufacturers, component suppliers, energy

providers and grid operators. Their collective goal: advancing interoperable charging solutions where vehicles, chargers, and digital systems integrate seamlessly to deliver a consistent and intuitive user experience [1].

As the e-mobility ecosystem continues to evolve, several key stakeholders play fundamental roles in enabling seamless Plug & Charge experiences [5]:

- V2G Root Operators manage the V2G Root Certificate Authority, the highest trust anchor defined in ISO 15118-2. They are responsible for securely creating the V2G root certificates and provisioning certificates for electric vehicle supply equipment (EVSE) and mobility operators, ensuring the validity and security of trust chains across the ecosystem.
- Charge Point Operators (CPOs) are responsible for managing and maintaining charging stations. Beyond providing physical infrastructure, they operate IT systems that support authentication, authorization, and billing—either directly to EV drivers or through mobility operators. CPOs are critical for ensuring ISO 15118 compliance at the station level.
- Mobility Operators (MOs) offer a wide range of charging-related services, including helping drivers locate charging stations, authenticate charging sessions, and manage billing. They conclude commercial contracts with EV owners or drivers and are responsible for issuing contract certificates required for Plug & Charge authentication.
- Original Equipment Manufacturers (OEMs) produce ISO 15118-compatible electric vehicles and provision them with certificates that enable automated authentication and billing processes. By installing OEM provisioning certificates during production, they ensure EVs are ready for seamless Plug & Charge integration upon delivery.

Understanding the distinct responsibilities of each stakeholder highlights the importance of interoperability at every level—from vehicle manufacturing to backend integration.

Beyond the key stakeholders, the Plug & Charge ecosystem defined by ISO 15118 relies on several critical system components that ensure secure communication and certificate management [5]:

- Root Certificate Pool (RCP): Repository for exchanging root certificates between Certificate Authorities (CAs) of ISO 15118 participants (V2G, OEM, MO), enabling validation across trust chains.
- Provisioning Certificate Pool (PCP): Interface where OEMs publish vehicle provisioning certificates after production. Mobility Operators retrieve these certificates to create contract data specific to each EV.
- Contract Certificate Pool (CCP): Main storage point for signed contract data, accessible by OEM and CPO backends. Supports online, backend-driven, and offline provisioning of certificates to EVs.
- Certificate Provisioning Service (CPS): Entity responsible for signing contract data, ensuring authenticity and integrity before storing it in the CCP.
- PKI Services: Organizations managing certificates must maintain secure storage, certificate management tools, and revocation infrastructure in compliance with ISO 15118 guidelines.

These components together form the technical foundation that enables automated authentication, secure billing, and interoperability within the Plug & Charge ecosystem.

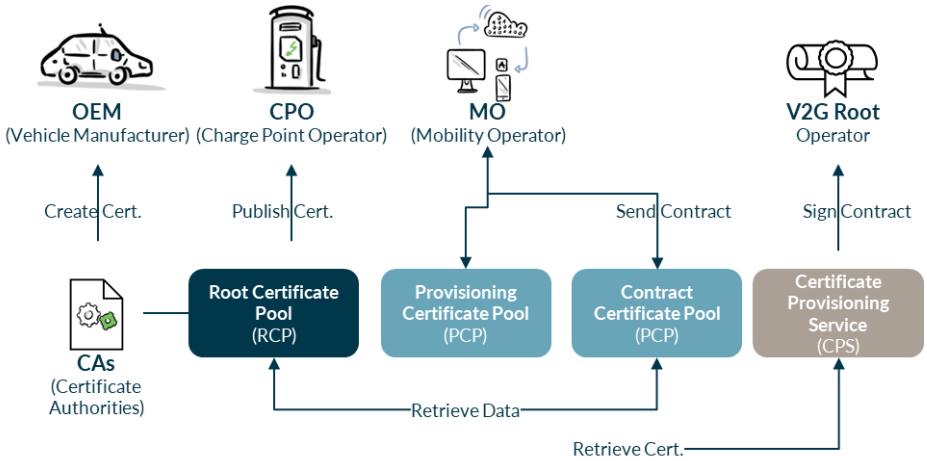

Figure 1: Ecosystem actors and components

As the electrification of transport accelerates, Plug & Charge has emerged as a cornerstone technology. By enabling automated authentication and billing between vehicles and charging points, it simplifies the user interaction dramatically. However, delivering this experience consistently across markets requires resolving one of the most complex underlying challenges: interoperability within fragmented and decentralized Public Key Infrastructure (PKI) ecosystems. These involve multiple CAs, Mobility Service Providers (MSPs), CPOs, and OEMs -often operating under different trust frameworks and implementation assumptions.

Without harmonized processes for trust anchor resolution, certificate provisioning, and cross-platform integration, Plug & Charge implementations risk becoming siloed and non-interoperable. To overcome this, CharIN launched the Open Plug and Charge (OPNC) protocol: a community-driven effort to provide a secure, standardized, and interoperable solution designed to support increasingly diverse trust environments [2]. OPNC establishes scalable trust relationships, enabling cross-vendor compatibility and a seamless user experience.

2. The motivation for OPNC protocol

EV charging introduces numerous advanced features beyond simply recharging the battery. As new players enter the market, some building proprietary systems from scratch, both opportunities and challenges emerge. To ensure reliability and scalability, CharIN advocates for a common set of requirements for high-power charging infrastructure, with particular focus on CCS and MCS, which support long-range e-mobility at scale [3].

Beyond these core systems, CharIN also supports the development of enabling features such as Plug & Charge, smart charging, and wireless charging. These technologies aim to improve the overall charging experience by minimizing user interaction and maximizing system efficiency.

Plug & Charge, specified in the ISO 15118 standard, enables vehicles to authenticate and initiate charging automatically, without the need for physical cards, apps, or manual interaction. When a contract certificate is pre-installed in the vehicle and the charging station is compliant, the system can securely identify the EV and start charging instantly, offering users a true "plug-in-and-go" experience.

The recently released ISO 15118-20 builds upon ISO 15118-2, offering enhanced capabilities such as support for bidirectional charging (Vehicle-to-Grid, V2G), more sophisticated energy management, and improved

contract handling mechanisms. However, even ISO 15118-20 does not standardize the backend communication protocols between MOs, MSPs, CPSs, and CAs.

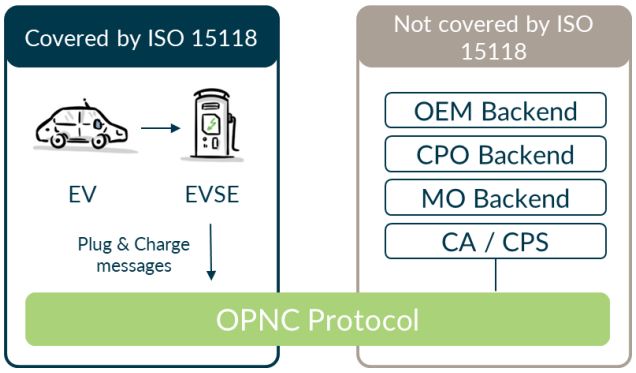

Figure 2: ISO 15118 Scope vs Backend Gap

As a result, the Plug & Charge ecosystem remains fragmented. The absence of clear, enforceable standards on backend integration, certificate governance, and trust anchor selection has led to isolated implementations and vendor-specific solutions, limiting interoperability and increasing complexity for OEMs, CPOs, and backend operators alike.

Recognizing this industry-wide challenge, CharIN initiated the OPNC protocol Task Force. This initiative seeks to:

- Minimize vendor lock-in by promoting open processes.
- Define standardized procedures for certificate provisioning and management.
- Establish interoperable methods for trust anchor resolution.
- Ensure end-to-end security aligned with ISO 15118 best practices.

By formalizing these processes into a shared protocol, OPNC provides a technically robust and operationally scalable foundation for Plug and Charge implementations across diverse ecosystems.

3. OPNC Protocol and its purpose

OPNC is a vendor-neutral API specification developed to harmonize backend flows and trust relationships in Plug & Charge ecosystems. Its main objective is to enable secure, standardized communication between backend systems, such as those used by OEMs, CPOs, and MSPs, ensuring that EV users enjoy consistent charging experiences across different platforms and markets [4].

Designed to work on top of ISO 15118, OPNC focuses specifically on backend-level integration and certificate-based trust models. It outlines how actors within the ecosystem can discover trust anchors, manage contract certificates, and maintain cryptographic security across organizational boundaries. The protocol is grounded in several core principles:

- Full compatibility with ISO 15118-2 and ISO 15118-20 standards.
- Clearly defined responsibilities for each participating actor.
- Transparent governance and public documentation and community input.
- Scalability to accommodate evolving PKI infrastructures and operational models.
- Defined procedures for certificate issuance, validation, and revocation.
- Interoperable workflows that minimize integration complexity and redundancy.

In practice, OPNC bridges backend processes across organizational boundaries by defining clear, vendor-neutral interfaces and trust establishment procedures.

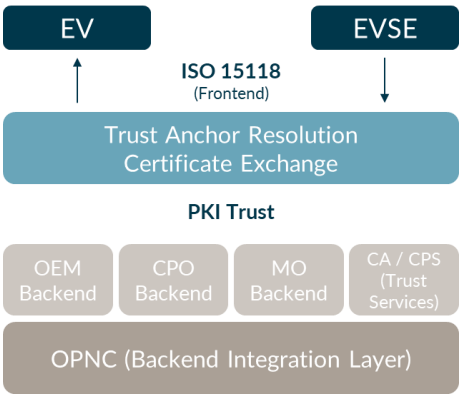

Figure 3: OPNC Layered Architecture Diagram

For example, a vehicle from OEM A should be able to authenticate and charge at a station operated by CPO B, even if their contract certificate was issued by MSP C, as long as all parties comply with the protocol's requirements. This is achieved through a harmonized approach to trust anchor resolution, secure certificate exchange, and consistent handling of edge cases and errors.

The design of OPNC builds upon lessons learned from previous implementations and serves as an evolutionary step forward. It draws from the earlier OPCP protocol and is also compatible with the PNCP protocol, enabling backward compatibility and facilitating adoption within existing systems. One of the defining advances of OPNC is its focus on supplier-agnostic integration, allowing seamless interoperability in environments with multiple V2G PKIs (Vehicle-to-Grid Public Key Infrastructures) and Mobility Operator PKIs. This supports a flexible and future-ready architecture that can adapt to diverse market needs.

Additionally, OPNC introduces a unified API approach, ensuring that stakeholders across the EV charging value chain can communicate through a jointly defined interface -an important step toward a globally aligned Plug & Charge ecosystem. Its open, international character ensures the protocol is suited for global deployment while addressing regional requirements, such as those identified in North America.

Finally, OPNC offers not just technical specifications, but practical guidance. It includes best practices for certificate lifecycle management, backend integration, and regulatory alignment. It serves as both a technical guide and a governance blueprint, accelerating the industry's transition to scalable, cross-provider Plug & Charge solutions.

4. Development and Governance

The development of the OPNC protocol is managed through an open, member-driven process within CharIN's established governance framework [4]. To ensure broad representation and technical depth, the OPNC Task Force was created, bringing together stakeholders from across the e-mobility ecosystem, including OEMs, CPOs, backend system providers, PKI experts, and cybersecurity specialists.

CharIN serves as a neutral platform for this collaboration, where decisions are made through regular meetings, consensus-building, and iterative reviews. Specification drafts are circulated among the participants and refined based on real-world implementation feedback and testing results.

The publication of OPNC version 1.0 in 2024 marks a significant milestone in this process. It represents the initial deliverable of the Task Force and serves as a stable foundation for adoption, testing and further evolution. The protocol is maintained under CharIN's governance, which includes structured change management procedures, transparent versioning, and close alignment with CharIN's broader Working Group, which ensures compatibility is tested and validated through industry-wide events.

This collaborative and iterative model ensures that the protocol evolves in line with industry needs, balancing innovation with practical feasibility, and enabling long-term support for secure, scalable Plug & Charge implementations.

5. Key Features of OPNC version 1.0

The OPNC protocol is designed to support secure Plug & Charge operations within a complex, multi-stakeholder ecosystem. This includes vehicle manufacturers (OEMs), charge point operators (CPOs), mobility service providers (MSPs), certificate authorities (CAs), and backend providers. Each actor plays a distinct role—from issuing digital credentials and managing trust anchors to validating identities and exchanging authorization data.

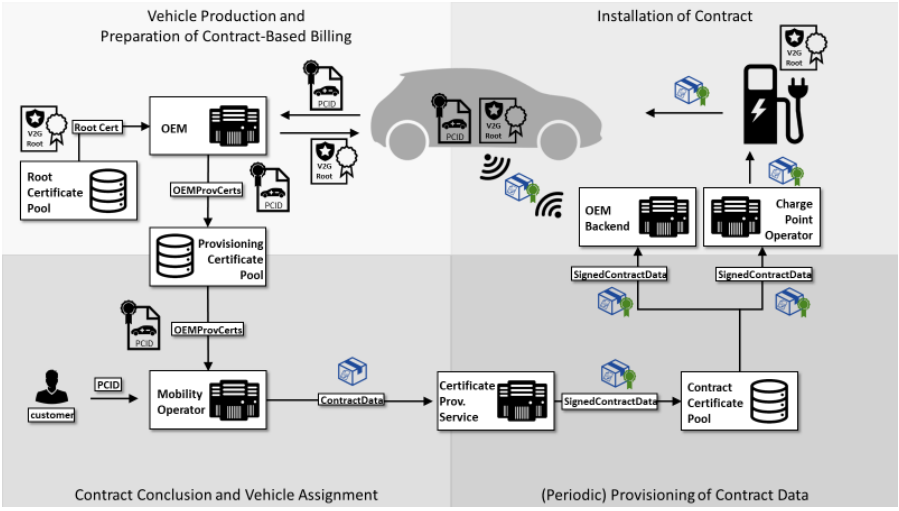

Figure 4: Plug & Charge eEcosystem description [5]

Version 1.0 of the protocol offers a focused set of specifications that directly address integration barriers observed in early implementations. These foundational features promote technical consistency while preserving the flexibility needed to accommodate varying trust models and regional architectures.

Trust Anchor Resolution: OPNC defines a decentralized, implementation-neutral mechanism to discover and validate the appropriate trust anchor based on the vehicle's contract certificate. This ensures that EVs and charging stations can dynamically identify trusted authorities without relying on hardcoded configurations or proprietary logic.

Contract Certificate Handling: The protocol introduces a flexible approach to contract certificate recognition and management, supporting diverse PKI setups while preserving security and interoperability. This enables users to seamlessly authenticate with their preferred service provider, regardless of which PKI issued the certificate.

Certificate Enrolment Flow: OPNC outlines a robust and simplified process for enrolling new certificates, including secure provisioning of cryptographic credentials to vehicles. This reduces onboarding time for end users and simplifies certificate management for OEMs and backend operators.

Backend Communication Guidance: To support interoperability at the backend level, the protocol specifies how different actors (e.g., OEMs, CPOs, MSPs) should exchange authentication data and validate credentials. These recommendations align with existing standards while closing gaps in backend-to-backend interactions.

Together, these features serve as the technical foundation for scalable Plug & Charge ecosystems, reducing fragmentation and enabling secure, automated charging across vendors and borders.

Contract Provisioning Process: The protocol defines a structured approach for provisioning contract certificates across multiple backend systems. The process begins with the OEM generating a provisioning certificate during vehicle production and preloading a trust store with root certificates. Once a user signs a charging contract, the Mobility Operator associates it with the vehicle's provisioning certificate and forwards the relevant data to a backend certificate service. This contract data is then securely signed and stored in a dedicated certificate pool. Finally, the signed certificate is distributed to the OEM and CPO backends to enable authentication at the charge point.

This end-to-end process illustrates the trust layering and interoperability mechanisms at the heart of OPNC. By codifying each step, the protocol ensures consistency across implementations while maintaining the flexibility to evolve alongside new trust models and certificate handling approaches.

6. Implementation and Testing

OPNC has been developed with real-world implementation in mind. To ensure robustness and practical applicability, CharIN supports a comprehensive testing and validation framework, emphasizing collaboration across the EV industry.

Companies can implement OPNC by referring to publicly available specifications and supporting documentation. Backend systems are expected to incorporate trust anchor resolution, contract certificate handling, and authorization flows, in alignment with the protocol. To support this, CharIN provides implementation guidance and promotes the use of shared tools across the community.

A central pillar of the validation process is the CharIN OPNC Task Force and the global interoperability Testival events [6]. These events bring together OEMs, CPOs, MSPs, and backend providers to test interoperability implementations in realistic, cross-company environments. Testivals serve not only as technical verification points but also as collaborative forums where protocol assumptions are examined, interoperability gaps are identified, and improvements are proposed [4].

The OPNC Task Force integrates feedback from Testivals and ongoing implementation experience to continuously improve the protocol. This active feedback loop reinforces the transparency of the development process and accelerates consensus-building across the industry.

7. Challenges and Insights

The development and implementation of the OPNC protocol have brought to light a range of challenges that reflect the complexity of real-world Plug & Charge ecosystems. While the protocol is grounded in the ISO 15118 standard, its deployment in diverse environments has highlighted areas where additional guidance, alignment, and tooling are still needed.

A primary challenge lies in reconciling the perspective of various stakeholders -OEMs, CPOs, MSPs, and backend providers- who often operate within different regulatory contexts, legacy infrastructures, and business priorities. Establishing agreement on processes such as trust anchor resolution, certificate lifecycle handling, and backend interoperability has required sustained dialogue and compromise.

Another key insight is the importance of maintaining a clear boundary between policy and implementation. OPNC must serve as a stable foundation or interoperability while remaining adaptable to local market dynamics and regulatory requirements. This reinforces the need for a modular protocol design that allows for optional extensions without disrupting baseline compatibility.

Technical challenges have also emerged around certificate management in multi-PKI environments. Ensuring interoperability across domains requires consistent interpretation of trust models, naming conventions, and fallback procedures. Variations in these areas can lead to implementation gaps that affect user experience and system reliability.

Perhaps most notably, the collaborative approach adopted within the OPNC community has proven essential. The protocol's progress to date owes much to the openness with which stakeholders have shared implementation insights, challenged assumptions, and responded to real-world feedback. This shared commitment is critical to supporting the long-term scalability and evolution of Plug & Charge systems.

These challenges and lessons learned highlight the need for an ongoing, feedback-driven development process—one that remains grounded in operational realities while supporting a global vision for interoperable EV charging.

8. Roadmap on OPNC new developments

Building on the foundation laid by version 1.0, CharIN is actively collaborating with industry stakeholders to shape the next evolution of the OPNC protocol. The development of version 2.0 is informed by

implementation feedback, insights gathered from Interoperability Testivals, and emerging requirements from global deployment scenarios. The primary aim is to expand OPNC's functionality while preserving interoperability and ensuring backward compatibility.

A major area of focus for OPNC v2.0 is improving certificate security and lifecycle management. In parallel, the OPNC Task Force is establishing a formal governance structure to oversee protocol operations. This body will provide clear guidance on data sharing and storage responsibilities, ensuring full compliance with GDPR [7] and other relevant data protection frameworks. Initially, the model will rely on a manageable number of distributed certificate pools to enable rapid deployment.

As participation in the ecosystem expands and the current model reaches its scalability limits, the governance body will assess a potential transition to a centralized pool platform. This shift would support further growth while maintaining technical and procedural consistency across implementations.

Future considerations also include support for more advanced use cases, such as bidirectional charging, fleet-oriented charging sessions, and managed energy services. These scenarios will require the definition of new roles and enhancements to the authentication logic, moving beyond the single-user paradigm used in earlier stages.

Additional architectural improvements will focus on strengthening fault tolerance -particularly around error handling and fallback behavior- while also improving diagnostic capabilities. The updated protocol will remain aligned with evolving regulatory frameworks, such as the EU's Alternative Fuels Infrastructure Regulation (AFIR) [8], to ensure legal compliance across jurisdictions.

CharIN remains committed to open development and encourages contributions from all stakeholders. The governance structure supporting OPNC v2.0 will continue to function as a transparent, inclusive forum, with interoperability, security, and usability as its guiding principles. Beyond technical refinements, OPNC v2.0 aims to enable the next generation of Plug & Charge experiences, more scalable, more flexible, and more attuned to the growing demands of a global e-mobility ecosystem.

9. Conclusion

The OPNC protocol represents more than a technical specification—it is a coordinated, industry-wide effort to establish reliable, secure, and interoperable Plug & Charge functionality across a global electric mobility landscape. Developed within CharIN's neutral and open framework, OPNC addresses real-world implementation challenges by standardizing trust relationships, certificate flows, and backend integration procedures.

As electric vehicle adoption grows and backend complexity increases, OPNC offers a scalable and adaptable foundation for managing interoperability across PKI environments and diverse stakeholders. It empowers OEMs, CPOs, MSPs, and certificate authorities to collaborate within a common framework that evolves with market demands.

With version 1.0 already in use and version 2.0 focused on governance, scalability, and advanced use cases, OPNC is well positioned to shape the future of seamless and secure Plug & Charge worldwide. CharIN welcomes all stakeholders to participate in this evolving initiative and help realize a more unified and user-centric charging ecosystem.

10. References

[1] *CharIN e.V.,* https://www.charin.global, *accessed on 2024-10-29*

[2] *CharIN e.V.,* https://www.charin.global/news/charin-unveils-opnc-protocol/, *accessed on 2024-10-29*

[3] *CharIN e.V.,* https://www.charin.global/technology/, *accessed on 2024-10-29*

[4] *CharIN e.V., https://github.com/charinev/opnc, accessed on 2024-10-29*

[5] *CharIN e.V., https://www.charin.global/media/pages/technology/knowledge-base/09ce9fd6d5-1649174817/charin_implementation_guide_to_plug_and_charge_v1_2.pdf, accessed on 2024-10-29*

[6] *CharIN e.V., https://www.charin.global/events/global-testivals/, accessed on 2025-04-16*

[7] *European Union Law, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng, accessed on 2025-04-16*

[8] *European Commission, https://transport.ec.europa.eu/transport-themes/clean-transport/alternative-fuels-sustainable-mobility-europe/alternative-fuels-infrastructure_en, accessed on 2025-04-16*

Presenter Biography

Jeremy Schofield

Jeremy Schofield is a seasoned technology executive with deep expertise in the automotive and manufacturing sectors, currently serving as Director of Technology at CharIN Academy.

With leadership roles at Tesla, Rivian, Czinger Vehicles, and Ford, he brings over 15 years of experience in product innovation, global program management, and strategic development across electric vehicle and mobility industries.

Daniela Soler

Daniela Soler is a Technical Project Manager at CharIN, which develops and promotes CCS and MCS charging standards for electric vehicles.

She has an Electric Engineering degree from the University of Chile, an MBA in Energy Management at TU Berlin, and serves on AVEC's board (Chilean Association of Electric Vehicles).

Previously, she led the Efficient Transportation Unit at Chile's Ministry of Energy, overseeing vehicle efficiency regulations, charging infrastructure standards, and the National Electromobility Strategy.