| DOCKETED | |
|---|---|
| **Docket Number:** | 19-TRAN-02 |
| **Project Title:** | Medium- and Heavy-Duty Zero-Emission Vehicles and Infrastructure |
| **TN #:** | 236569 |
| **Document Title:** | Interoperability Testing Events RFP Workshop Comment - AUTOCRYPT |
| **Description:** | N/A |
| **Filer:** | Spencer Kelley |
| **Organization:** | California Energy Commission |
| **Submitter Role:** | Commission Staff |
| **Submission Date:** | 2/2/2021 1:11:10 PM |
| **Docketed Date:** | 2/2/2021 |

Interoperability Testing Events
19-TRAN-02

January 24, 2021

**About AUTOCRYPT**

AUTOCRYPT is the leading player in transportation security technologies. Beginning in 2007 as an in-house venture at Penta Security Systems Inc., AUTOCRYPT spun off as a separate entity in 2019 as its presence expanded worldwide. Recognized by TU-Automotive as the Best Auto Cybersecurity Product/Solution of 2019, AUTOCRYPT continues to pave the way in transportation and mobility security through a multi-layered, holistic approach. Through security solutions for V2X/C-V2X, V2G (including PnC security), in-vehicle security, and Fleet Management, AUTOCRYPT ensures that security is prioritized before vehicles hit the road.

**Comment #1: Interconnectivity Events**

Interconnectivity events encourage the participation of private sector players, thereby building trust that is essential between such players and government agencies before the commercial release of new technology. Organizations such as the OmniAir Consortium run V2X interconnectivity events for both WAVE and C-V2X technologies. ISO 15118, which oversees communications between electric vehicles and CCS EV chargers, also run the ISO 15118 Testing Symposium. The Testing Symposium also extends to communications between EV chargers and the backend infrastructure, which is governed by OCPP. Such events have been administered for years, and may serve as good benchmarking for California's own initiatives in EV charging.

**Comment #2: Security as a Vehicle for Trusted Communications**

The California Energy Commission's *Assembly Bill 2127 Electric Vehicle Charging Infrastructure Assessment (Staff Report)* and *Notice of Remote-Access Staff Solicitation of Scoping Workshop* illustrate a variety of different factors to reach its goals, which include 100 percent of passenger vehicles sales to be zero emissions by 2035. The concept of security is not addressed as a necessary component of building an EV charging infrastructure to encourage widespread EV adoption in these documents, however. For future technologies such as bidirectional charging and other EV-charging-related services, it seems to us that all market participants must trust the security of the communications that will occur. As such, we would like to suggest the concept of security as an essential component of establishing trust between all the software-based endpoints (as well as hardware components that increasingly rely on such software) prior to launching such services. We strongly encourage the California Energy Commission to include the idea of trust and security in these documents.

Thank you in advance for allowing us to contribute to this very important topic.

Sincerely,
Jaeson Yoo
Chief Strategy Officer
Autocrypt Co. Ltd.
Phone: +82-10-5188-3550
E-mail: jyoo@autocrypt.io