Regulaciones y Certificaciones de Ciberseguridad en el Ecosistema de la Movilidad Conectada y Automatizada

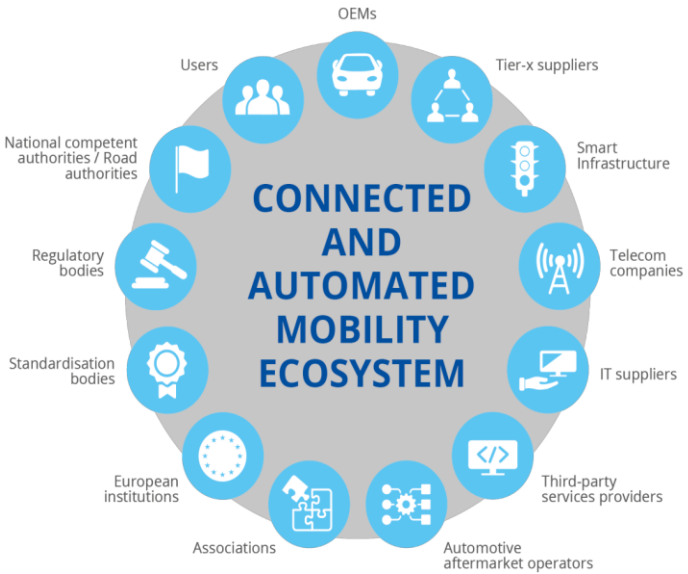
A cyber safe world

Cybersecurity Certifications

Ecosistema de la Movilidad Conectada y Automatizada

PRIMEROS PASOS EN CIBERSEGURIDAD.

- El consenso en los estándares de seguridad
- Regulaciones y certificaciones en el ámbito de la CAM



Principales dificultades que se plantean al abordar este reto

- La CAM un ecosistema muy amplio que engloba muy diferentes industrias
- El vehículo conectado, un sistema extremadamente amplio y complejo
- Un entorno de operación global
  - Sistemas de comunicaciones universales / estandarizados
  - Cadenas de suministros globales

Regulaciones y Certificaciones de Ciberseguridad

PRIMERAS INICIATIVAS EN CERTIFICACIÓN DEL VEHÍCULO AUTÓNOMO CONECTADO

UNECE

UNECE W.29/GRVA- Requisitos de ciberseguridad para la homologación de vehículos

El Foro Mundial para la Armonización de la Reglamentación sobre Vehículos es un grupo de trabajo de la Comisión Económica de las Naciones Unidas para Europa (UNECE W.29) que tiene como objetivo crear un sistema uniforme de reglamentos, para el diseño de vehículos con el objeto de armonizar los requisitos de homologación de vehículos a nivel global y facilitar el comercio internacional.

En junio de 2020 este organismo incluyo por primera vez en su catálogo de reglamentos, dos reglamentos que contienen requisitos de ciberseguridad para el vehículo conectado:

- UN Regulation No 155 - Cyber security and cyber security management system (CSMS) (ISO 21434 CSMS requirements and ISO 5112 audit guidelines)
- UN Regulation No 156 Requirements for Over the Air Software Updates (SUMS) (ISO 24089 SUMS requirements)

DEKRA

Regulaciones y Certificaciones de Ciberseguridad

PRIMERAS INICIATIVAS EN CERTIFICACIÓN DE COMPONENTES DEL VEHÍCULO

COMMON CRITERIA Y LOS ESQUEMAS DE CERTIFICACION SOG-IS Y EUCC

El esquema de certificación SOG-IS y el esquema de certificación Europeo EUCC, (Cybersecurity Act) están basados en una metodología general de evaluación de la seguridad de los productos (Common Criteria / ISO 15408) y en especificaciones concretas de requisitos para cada producto

La industria Automotriz esta dando los primeros pasos en el desarrollo de perfiles de protección para componentes específicos, como por ejemplo:

- PPs para tacógrafos desarrollados por el JRC de la Comisión Europea
- PPs para los elementos mas críticos del vehículo, el modulo HSM y la unidad de comunicaciones V2X en desarrollo por el Car2Car Communication Consortium
- Perfil de protección desarrollado por el BSI Alemán para equipos de señalización en la carretera .
- Perfil de protección desarrollado por la Federación Internacional del Automóvil para una unidad genérica de comunicaciones del vehículo (PP pendiente de certificación en CC).

Regulaciones y Certificaciones de Ciberseguridad

FUTURAS EVOLUCIONES EN LA APLICACIÓN DE COMMON CRITERIA O EUCC EN EL VEHÍCULO CONECTADO

Algunos proyectos en marcha en ISO/IEC JTC 1/SC 27

- ISO/IEC JTC 1/SC 27 WG3 estudio preliminar sobre “Criterios de evaluación de la seguridad de la información de los vehículos conectados basados en la norma ISO/IEC 15408”.
- ISO NWIP “Information security, cybersecurity and privacy protection— Security requirements and evaluation activities for connected vehicle devices

- ¿El vehículo conectado entre los futuros esquemas de certificación a desarrollar en el marco de la Cybersecurity Act ??

Regulaciones y Certificaciones de Ciberseguridad

UN COMPONENTE MUY ESPECIAL: LOS MODULOS CRIPTOGRAFICOS

CERTIFICACIÓN DE MODULOS CRIPTOGRAFICOS

ISO/IEC 19790 y FIPS 140-3

A nivel de esquemas de certificación de módulos criptográficos el más relevante puede considerarse la certificación FIPS-140 desarrollada inicialmente por los gobiernos de Estados Unidos y Canadá, para validar la efectividad de los módulos criptográficos implantados en los equipos.

En su última versión CMVP FIPS-140-3, en un proceso de armonización global de los requisitos técnicos, pasa de estar basado en normas nacionales NIST a basarse en la norma internacional ISO 19790, dando de esta forma un paso de gigante en la generalización de este estándar como base internacional de requisitos técnicos de seguridad para módulos criptográficos

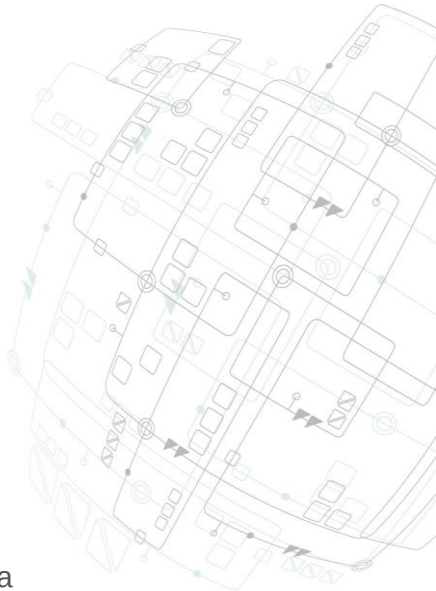
Normas y proyectos

- ISO/IEC 19790:2012 Information Technology. Security techniques. Security Requirements for Cryptographic Modules
- ISO/IEC 24759:2017 Information Technology. Security techniques. Test Requirements for Cryptographic Modules

Regulaciones y Certificaciones de Ciberseguridad

PRIMERAS INICAITIVAS REGULATORIAS INCLUYENDO REQUISITOS DE CERTIFICACION DE COMPONENTES ESPECIFICOS

La industria Automotriz esta dando los primeros pasos en el desarrollo de perfiles de protección para componentes específicos, como por ejemplo:

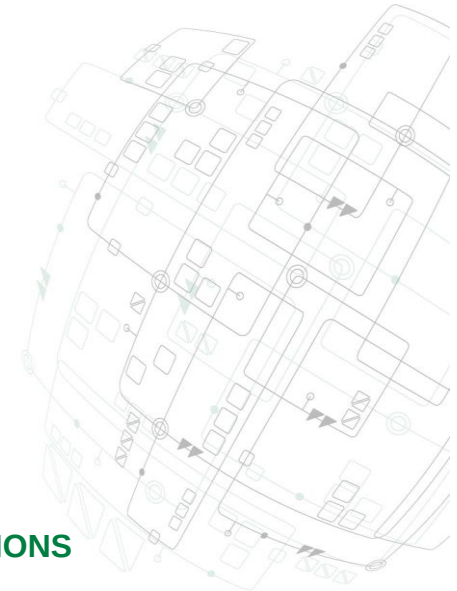


- **C-ITS Delegated Act (en desarrollo)** Regulación europea de sistemas cooperativos e inteligentes de transporte que fueron presentadas en marzo de 2019 y posteriormente retiradas en julio de 2019 tras una objeción del Consejo Europeo al respecto de la neutralidad tecnológica, incluían requisitos de certificación CC para los módulos criptográficos y de comunicaciones tanto del vehículo como de las unidades externas.
- El **Reglamento (UE) 165/2014** del Parlamento Europeo y del Consejo, que establece los requisitos para la construcción, ensayo, instalación, funcionamiento y reparación de los tacógrafos y de sus componentes y que referencia a los requisitos de seguridad de los perfiles de protección del Joint Research Centre de la Comisión Europea para tacógrafos.
- El **Reglamento de Ejecución (UE) 2019/1213** de la Comisión de 12 de julio de 2019 por el que se establecen disposiciones detalladas para garantizar unas condiciones uniformes a efectos de aplicar la interoperabilidad y la compatibilidad de los equipos de pesaje a bordo con arreglo a la Directiva 96/53/CE del Consejo y que incluye requisitos de certificación CC para los módulos de pesaje (OBW) del vehículo y referencia PP de los módulos V2X HSM y Gateway de Car2Car.

Regulaciones y Certificaciones de Ciberseguridad

PRIMERAS INICIATIVAS DE CERTIFICACIONES DE SEGURIDAD EN LAS COMUNICACIONES

REDES CELULARES



- ESQUEMA DE CERTIFICACIÓN 3GPP **SECAM AND SCAS (3G)**
- GSMA ESQUEMA DE CERTIFICACIÓN **5G - NESAS SECURITY ASSURANCE SPECIFICATIONS**
- **FUTURO ESQUEMA DE CERTIFICACIÓN 5G EUROPEO (ENISA)**

Regulaciones y Certificaciones de Ciberseguridad

PRIMERAS INICIATIVAS DE CERTIFICACIONES DE SEGURIDAD EN LAS COMUNICACIONES

REDES DE CORTO ALCANCE

SISTEMAS DSRC

IEEE 802.11:2012	Physical Layer (PHY) & MAC (Transmit & Receive, Power & Sensitivity)
IEEE 1609.2:2017	Security Services (BSMs and WSAs, Certificate Changes/Authentication)
IEEE 1609.3:2016	Network Services (PSIDs/Data Rates/Power/Channels, WSMs, WSAs & IPv6)
IEEE 1609.4:2016	Multi-Channel Operations (Continuous & Alternating, Transmission Rates, WSMs & IPv6 packets)
SAE J2735:2016	Message Dictionary (BSMs for OBUs and BSMs(Rx), SPaT, MAP & TIMs for RSUs)
SAE J2945/1:2016	V2V Minimum Performance (Bench – BSM contents, Field Drive Test Attributes & Location Accuracy) for OBUs
USDOT FHWA-JPO-17-589:2017	RSU 4.1 (Packaging Environment Attributes, Data Logging, SNMP Commands, Time Source accuracy, SPaT/MAP/WSA Messaging, Immediate Forwarding / Store&Repeat) for RSUs

ESQUEMA DE CERTIFICACION

OMNIAIR® CONSORTIUM

Regulaciones y Certificaciones de Ciberseguridad

REGULACIONES MAS RELEVANTES EN LA INDUSTRIA DE LA CAM EN EUROPA

EUROPEAN C-ITS PLATFORM

- En el marco europeo, la Comisión decidió en 2014 establecer una plataforma común para el desarrollo de los sistemas inteligentes de transporte y vehículos conectados, denominada C-ITS Deployment Platform .
- En noviembre de 2016, se presentó por primera vez, la estrategia europea para Sistemas Cooperativos e Inteligentes de Transporte (C-ITS) que basaba la estrategia de seguridad en dos pilares: El desarrollo de una política de seguridad común para los sistemas C-ITS en todos los países europeos y una política de gestión de certificados digitales para los vehículos y demás elementos de los sistemas de C-ITS.
- Finalmente, en marzo de 2019 se presentó la primera iniciativa de regulación de estos sistemas, conocida como la C-ITS Delegated Act.

CYBERSECURITY ACT

- EUCC Primer esquema de certificación Europeo para productos ICT
- ¿Futuro esquema de certificación para vehículos conectados ?

DIRECTIVA EUROPEA 2014/53/UE (RED)

- La directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, más conocida por sus siglas en ingles “Radio Equipment Directive (RED)” establece un marco regulatorio para la comercialización de equipos de radio.
- Actualmente en fase de desarrollo de una nueva versión para incorporar requisitos de ciberseguridad.

Thank you

Jesus Fernandez
Presidente del CTN 26/SC 1/GT 1
“Ciberseguridad” de UNE

jesus.fernandez@dekra.com

DEKRA