Tachograph Forum
Meeting 28 November 2016

Bernardo MARTÍNEZ
Road Transport Unit (DGMOVE)
bernardo.martinez@ec.europa.eu
Agenda (main points)

- **Smart tachograph (EC)**
  - Smart tachograph and Galileo network
  - Security
  - Implementation milestones

- **Enforcement (ECR, CORTE)**
Smart tachograph

- Adopted by Regulation 165/2014
- In all new vehicles registered as from 15 June 2019
- GNSS module
  - Automatic recording of the location of the vehicle (cabotage)
  - Second motion sensor
- DSRC module for communication tachograph - control officers
- New cryptography
- Enhanced seal
OUR VISION: A ROBUST GNSS CAN ACT AS A SINGLE LOCATION “ENGINE” FOR MULTIPLE ROAD APPLICATIONS

Digital Tachograph (DT)

Pay As You Drive (PAYD)

Road User Charging (RUC)

Intelligent car sharing

Advanced Driver Assistance Systems (ADAS)

Fleet Management Systems (FMS)

In-vehicle Systems (including eCall)

Dangerous Goods Transport
✓ **Multi-constellation**: When buildings block the signal and reduce the number of visible satellites, the availability of more constellations ensures a **much more accurate final position**

Automotive chipset suppliers leaders support Galileo

GALILEO UNIQUE DIFFERENTIATOR: SIGNAL AUTHENTICATION

- **Security** is a **major concern** in the Smart Tachograph
- Galileo provides an **efficient**, **resilient** and **low-cost solution** against jamming or spoofing attacks

Authentication

- Ability of the system to guarantee to the users that they are utilizing signals from the Galileo satellites and not from any other source

Authentication of Galileo signals in the Open Service looks **more convenient for the industry** than the signal encryption between GNSS receiver and VU
GNSS

- Satellites
- OS Navigation
- Commercial Service

Timeline:
- 2016: Initial Service Start
- 2017: Enhanced Service
- 2018: 23+3
- 2019: 23+3
- 2020: 30


text

- Ranging
- Positioning
- OS INAV MSG Improv.
- OS Authentication
- Initial CS Service

Transport

European Commission
Security

New Cryptographic Algorithms

- Cryptographic algorithms to secure the communication links completely renewed
- Public key cryptography → Elliptic Curve Cryptography (ECC), Symmetric-key cryptography → AES, Hash → SHA-2
- New format for digital certificates

AES
Pairing and secure communication

ECC, SHA-2, AES, Digital Certificates

Mutual authentication and secure communication

External GNSS (optional)

Secure communication

Digital signatures on downloaded data

Early Remote Detection (DSRC)

AES, SHA-2

ECC, SHA-2, Digital Certificates
Timeline

ERCA SERVICES (CERTIFICATES) GEN 1
IOT GEN 1 in REGIME

SPECIFICATIONS ERCA GEN 2
DEVELOPMENT ERCA GEN 2
TESTS KEYS GEN 2 FOR MS
SAMPLE TEST KEYS FOR INDUSTRY
MS POLICIES + INFRASTRUCTURES DEVELOPMENT
MS TEST KEYS
MS PRODUCTION KEYS
SMART TACHOGRAPH COMPONENTS DEVELOPMENT
SMART TACHOGRAPH DEPLOYMENT
1 CARD + 1 VU CERTIFIED
SPECIFICATIONS IOT GEN 2
DEVELOPMENT IOT GEN 2
IOT GEN 2 CERTIFICATIONS

2016
Entry into force Reg 799/2016
NOW

2017
Start of Certification Processes

2018
START UP CERT. IOT GEN 2
ERICA GEN 2 KEY CEREMONY

2019
WSC
STC
Smart Tachographs mandatory
Enforcement

- Detection of tachograph manipulation has risen from 5 to 10% of the total of breaches to Reg 561/2006
- More and more sophisticated
- Tachograph tampering is beneficial
- Request for software type-approval
- Tachograph should remain an enforcement tool
Thank you