Smart Tachograph G2

Focus on Tachograph Cards

Anibal CASTILLO, Sylvain LHOSTIS

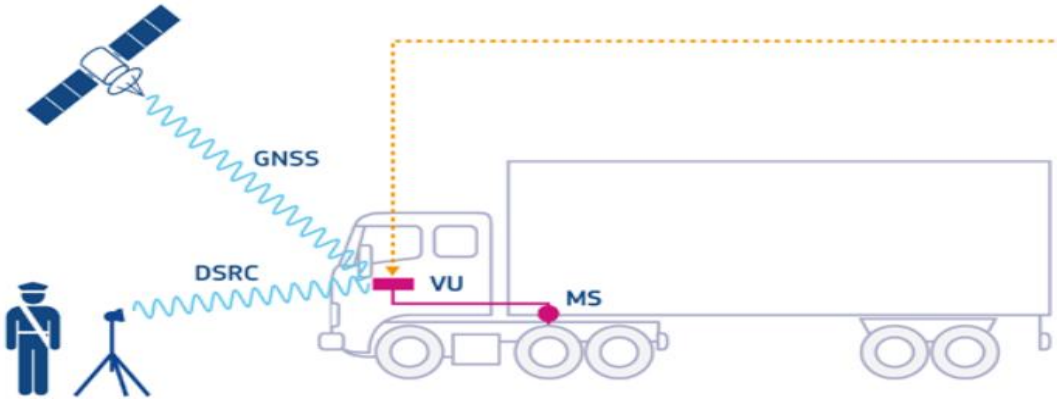
gemalto
security to be free

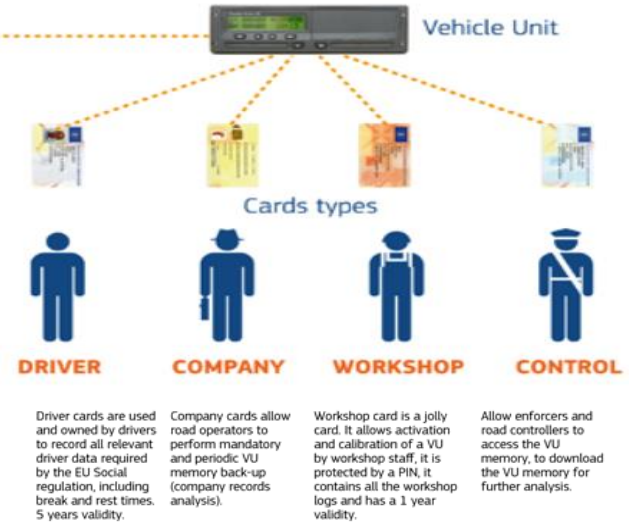
Digital Tachograph Scope

- The Digital Tachograph is a recorder of the professional drivers' activities (rest and driving hours).
- It provides trustworthy information to EU enforcers controlling compliance with Social Regulation (EC) No 561/2006.

The Vehicle Unit (VU) is the brain of the system. It is connected to the secured Motion Sensor (MS). .
The VU contains a printer, 2 slots for the cards, a display and mass storage.
The memory is able to hold data on drivers' activities for about a 12 month period. It also records data relating to faults, attempts to tamper with the system, over speeding, calibration details, when data has been accessed, (e.g. by the Police) etc.

Deployed in 51 Countries (28 EU and 23 AETR)

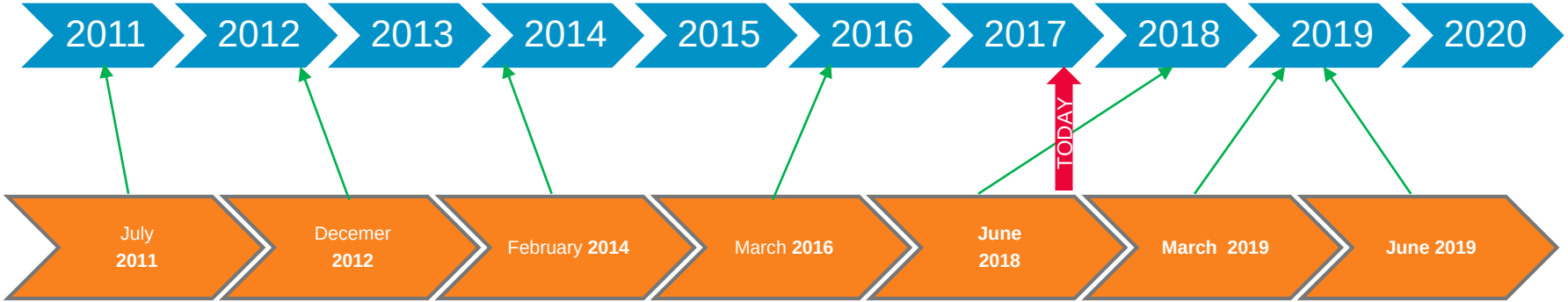




https://dtc.jrc.ec.europa.eu/index.php
https://dtc.jrc.ec.europa.eu/dtc_smart_tachograph.php

gemalto

From digital (Gen1) to ‘smart’ tachographs (Gen 2)



- European Commission proposal to revise tachograph legislation to make fraud more difficult and reduce the administrative burden
- JRC mandated to update the technical specifications
- First workshop sessions with JRC, Industry and Police Enforces started with active Gemalto participation
- Regulation No 165/2014 on Tachographs in road transport
- Repeals Regulation No 3821/85 and amends Regulation (EC) No 561/2006 on the harmonization of certain social legislation relating to road transport
- Entry into force
- Begin of period to migrate to Gen 2 cards
- End of period to migrate workshop cards to Gen 2
- All new cards issued must be Gen 2

gemalto

New Functions on Smart Tachograph

- **Enhanced Cards** compliant to the latest security recommendations to **prevent fraud and backward compatibles with Gen 1 Systems**
- **Satellite Positioning Systems (GNSS)** for tachograph VU to **automatically determine position and record** at least start and end point of work periods
- **Remote Detection (DSRC)** to allow **remote roadside checks** by enforcers. Onboard Weighting information will be available by 2021.
- **ITS Interface (Optional)** allowing **ITS applications to use data** recorded by the tachograph

Tachograph Cards and Security

- Tachograph cards remains key asset for security management.
- **Secure Channel (Mutual Authentication):** Whenever a Card is inserted on a Vehicle Unit (**VU**):

    1. Card and VU demonstrate that they own a valid certificate signed by a Member State Certificate Authority (**MSCA**); whose key is also signed by European Root Certificate Authority (**ERCA**)
    2. Card and VU demonstrate that they own the private key corresponding to the public key presented in the certificate
    3. Both card and VU independently calculate 2 session keys
    4. Both card and VU use agreed session keys to ensure the confidentiality, integrity and authenticity of all exchanged messages.

Tachograph Cards and Security

- Tachograph cards also store sensitive data (Information and other keys)
- Data can only be updated by a trustable VU (using a Secure Channel)

What is new in G2?

- ERCA Policy is updated with state of the art security mechanisms.
  - **RSA1024 (obsolete)** replaced by **Elliptic Curve (ECC) 256 up to ECC 521 bits (Valid above 2020)**
  - **TDES (obsolete)** replaced by **AES 128 up to 256 bits (Valid above 2020)**
  - **Sources:** https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=6
  - https://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf

Impact:

- Tachograph G2 Cards needs to implement much stronger security mechanisms so new chip and new application need to be developed.
- For Issuers:
  - MSCA system needs to be updated using the new ERCA Policy
  - Data Preparation, Key Management System and Perso Script need to be updated.

Tachograph Cards G1/G2 compatibility

- Introducing G2 Cards should not impact the existing installed base of G1 Vehicles.

- **What is new in G2?**
  - Tachograph G2 Cards must work on G1 Vehicle Units and corresponding ecosystem
  - Exception: Workshop Cards must be fully replaced to G2. More details on next slide.
  - Tachograph G2 Cards must be visually identified by adding a “G2 Tag” on the card design

- **Impact:**
  - Tachograph G2 Cards needs to fully operate as a G1 Card. This means we need to implement both G1 and G2 applications and file systems (including G1 Security Policies).
  - For Issuers:
    - Perso Solution needs also to support G1 Personalization services
    - Card Design need to be updated in order to add the “G2 Tag”

Focus on Workshop Cards

- Due to security increase, only Workshop G2 cards can calibrate VU G2 & Motion Sensor G2
  - Note that Workshop Gen2 cards hold former TDES motion sensor key, so can be used to maintain existing Gen1 VU

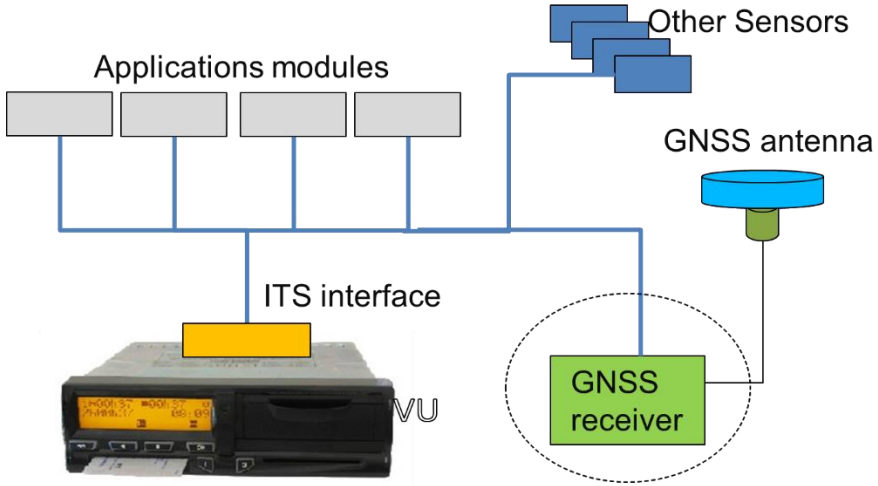
- Workshop Gen2 cards hold a part of the Motion Sensor Gen2 key
  - Mandatory for VU to start a calibration or maintenance process

- **As a consequence:**
  - All countries need to have their workshop equipped to be able to repair G2 VU before the delivery of the first vehicle with VU G2
  - Vehicle manufacturers need Workshop Gen2 cards to fully set up the vehicle before its delivery
    - They claim 6-9 months before June 2019.

Global Navigation Satellite System (GNSS)

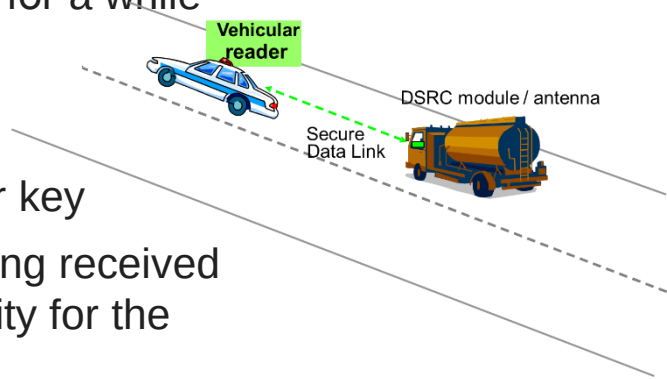
- **What is new in G2?**
  - Automate the process of recording the start and end locations by connecting the tachograph to a satellite navigation system
  - Independent data source to prevent tempering with the Motion Sensor
  - Additional info to identify cabotage

- **Impact:**
  - No direct impact on the G2 Card



Remote Detection (DSRC)

- **What is new in G2?**
  - Enable law enforcers to read remotely some tachograph information from passing vehicles at a road side control
  - Increase efficiency and allow for better enforcement by stopping only those vehicles for a more detailed control that show some irregularities or haven't been checked for a while
  - Based on DSRC 5.8 GHz band
- **Impact:**
  - Tachograph G2 Control Card stores DSRC Master key
  - Tachograph G2 Control Card in charge of decrypting received data and guarantee data confidentiality and integrity for the enforcer

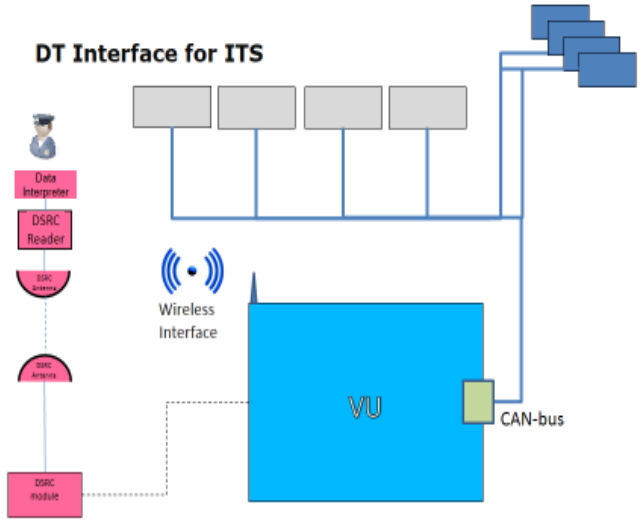


gemalto

New: Intelligent Transport Systems (ITS)

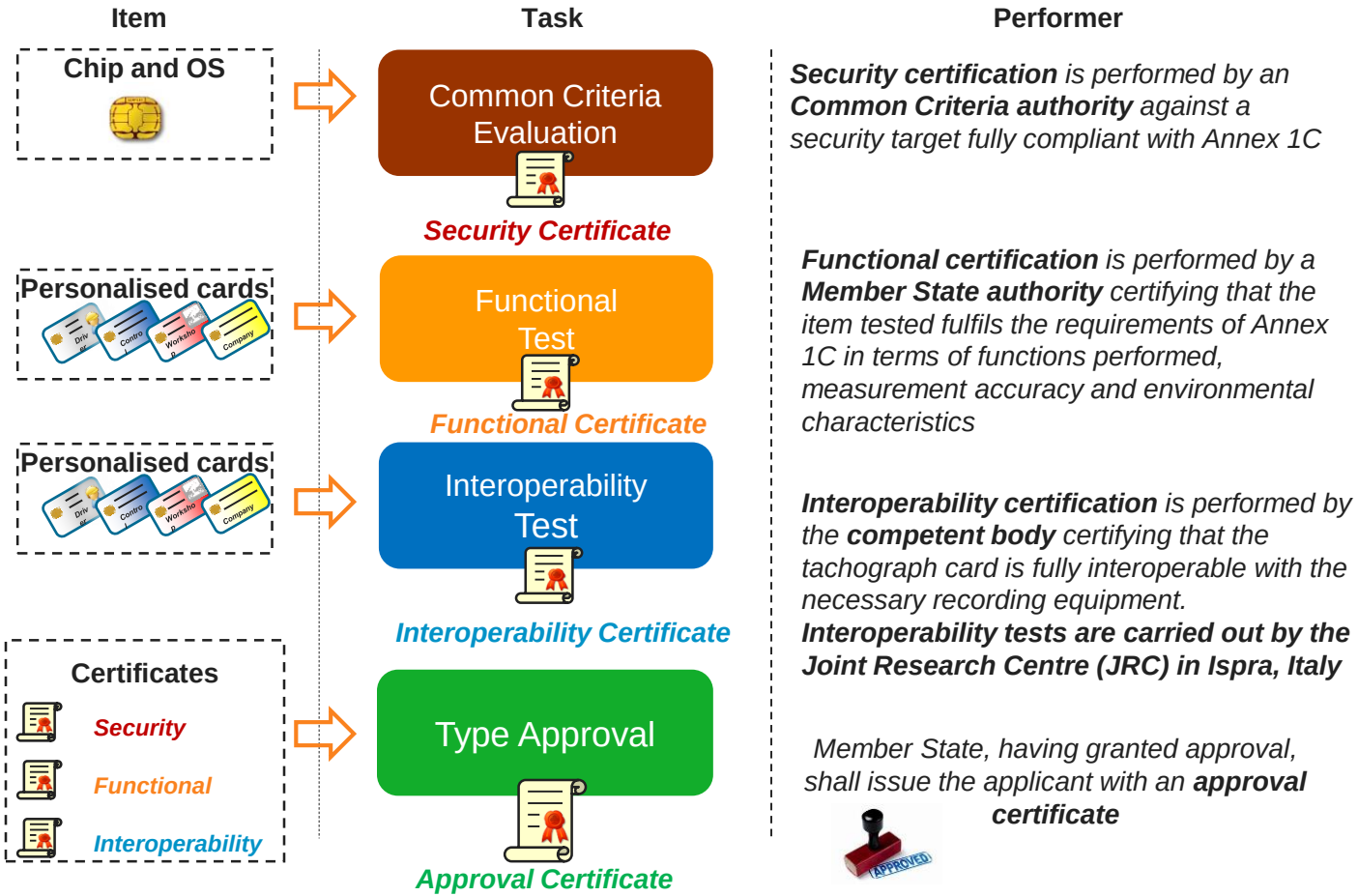
- **What is new in G2?**
  - Allow a tachograph to share its data with other approved vehicle telematics systems
  - Access to personal data, including geo-positioning data, after the verifiable consent of the driver to whom the data relates

- **Impact:**
  - No impact on the G2 Card



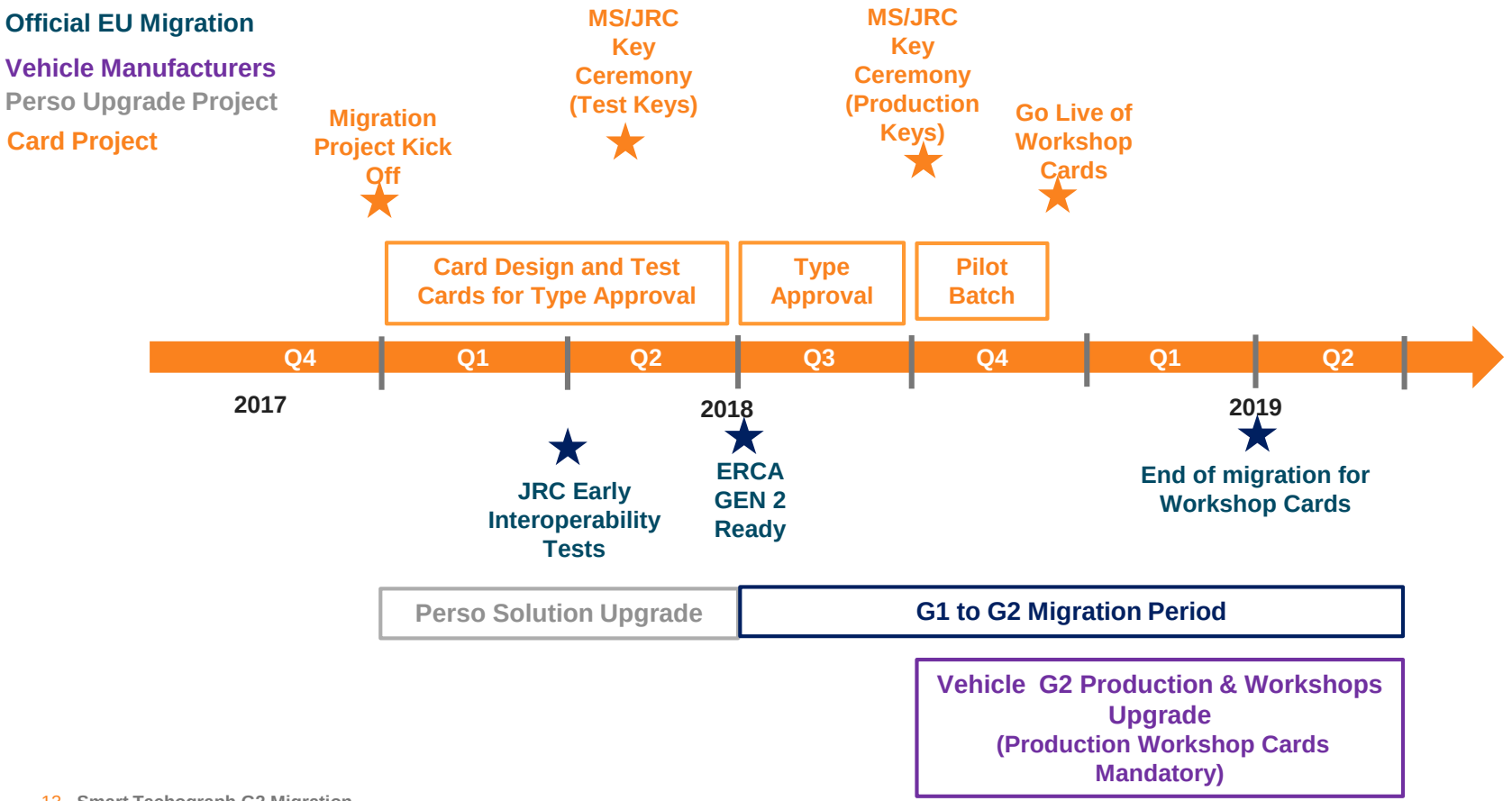
gemalto

Type Approval process



gemalto

Key Milestones & Planning



gemalto

Thank you