Regulation n°116

Discussions on Digital Keys,
Task Force February 18th, 2020

Presentation of Digital Key (Virtual Key) Concept

Background:
- Discussions at GRSG-117 revealed different understandings about proposed functionalities.
- The presentation is intended to clarify the technical concept of digital key/virtual keys working with smart devices.
UN-R116 aims to ensure safety by preventing unauthorized use of a motor vehicle:

- Locking the steering or transmission or gearshift control or brakes systems
- Locking the vehicle power
- Indicating intrusion into or interference with the vehicle

UN-R116 key is a device designed and constructed to provide a method of operating the above locks or the alarm system. The UN-R116 locks or alarm system are designed and constructed to be operated only by the intended UN-R116 key for the specific lock or alarm system.

Without that key, the steering or transmission or gearshift control or brakes systems or the vehicle power system or the alarm system can not be unlocked.

UN-R116 does not have requirements on door locking/unlocking.

UN-R116 does not restrict the use of a vehicle to a specific driver.

UN-R116 does not define how the vehicle power is switched on.
A car KeyFob containing a digital key is paired with a specific vehicle by the manufacturer.

A car KeyFob containing a digital key connects a specific keyfob/device to the inactivation/activation of the device to prevent unauthorized use, alarm, immobilizer and start system of a specific vehicle.

The KeyFob can prove that it holds the correct paired digital car key by using the key to sign commands that are sent from and to the vehicle.

A car KeyFob containing a digital key can enable detection of the device in close proximity to the vehicle using short range radio communication, RF.

Unsetting of the device to prevent unauthorized use / immobilizer is only allowed:

- From inside the vehicle (e.g. by pressing the vehicle start button) if the car KeyFob containing a digital key is detected inside the vehicle, or
- From outside the vehicle (e.g. at Automatic Park Out) if the car KeyFob containing a digital key is detected in the proximity of the vehicle.

Setting/Unsetting the Alarm System is allowed from outside of the vehicle if the car KeyFob containing a digital key is detected outside of the vehicle.

* Remark:
A digital key in a car KeyFob is called “Electronic code” under UN Regulation No. 116.
Car KeyFob technology principle is also used in other technologies as Smart Cards, the digital key is handed on a vehicle manufacturer hardware device to the customer.
Digital Car Key ("Code only")

- A digital car key in a mobile phone also has to be securely paired with a specific vehicle.
- A digital car key connects a specific device to the inactivation/activation of the device to prevent unauthorized use, alarm, immobilizer and start system of a specific vehicle.
- The device can prove that it holds the correct paired digital car key by using the key to sign commands that are sent from and to the vehicle.
- A device containing a digital car key can enable detection of the device in close proximity to the vehicle using short range radio communication, RF
- Unsetting of the device to prevent unauthorized use / immobilizer is only allowed*:
  - From inside the vehicle (e.g. by pressing the vehicle start button) if a digital car key is detected inside the vehicle, or
  - From outside the vehicle (e.g. at Automatic Park Out) if a digital car key is detected outside of the vehicle (e.g. within driver’s eye contact when driver is in charge)
- Setting/Unsetting the Alarm System is allowed from outside of the vehicle if the digital car key is detected outside of the vehicle.

* Remarks:
1) A second authentication inside the vehicle is needed before control is released to the driver if the vehicle was started from outside.
2) The device shall only be able to allow for unlocking the device to prevent unauthorized use. The actual unlocking and locking command needs to come from user input.
3) Restrictions could be defined in terms of Speed, Time, Allowed distance, etc.
4) Demands by market for digital services, e.g. Amazon Key Service requires alarm system unset, therefore the vehicle owner must give Amazon a key for the alarm system (US experience)
5) Detection inside the vehicle can be by vehicle scanning for key or driver authenticating through other means like NFC, UWB, rolling QR, PIN code, etc.
Access for both solutions is **proximity based**, i.e. the device has to be placed close to or inside the vehicle

- When the device is in close proximity of the vehicle, it is possible to:
  - Press a button on the key or phone to lock or unlock the vehicle and its alarm system
  - Unlock the device to prevent unauthorized use/immobilizer (e.g. at Automatic Park Out) if a digital car key is detected just outside (e.g. within driver’s eye contact when driver is in charge) of the vehicle. Restrictions could be defined.

- When the device is inside the vehicle, it is possible to:
  - Activate start to unlock the device to prevent unauthorized use/immobilizer and enable the propulsion system

**Authorized Vehicle Access**

Both can only **allow start, not request start or shut down vehicle**

- Propulsion activation requires:
  - Device to be detected - vehicle scans for key or drivers authenticates through other means like NFC, UWB, rolling QR, PIN code, etc..
  - Digital key authentication – vehicle identifies and authorizes the key
  - A start request from the driver – vehicle sets ignition on and the device to prevent unauthorized use is unset

- An attacker has to manipulate both the device detection system and the driver input system in order to start the vehicle, which is the same for a system using digital key in a mobile phone as one using a traditional car KeyFob containing a digital key.
Thank you for your attention