centrum voor criminaliteitspreventie en veiligheid

Churchilllaan 11
3527 GV Utrecht
Postbus 14069
3508 SC Utrecht

T (030) 751 67 00
F (030) 751 67 01
I www.hetccv.nl

0

CCV INSPECTION REGULATIONS VEHICLE SECURITY

Version 2.0

Date published
December 1, 2021
Effective date
December 1, 2021

FOREWORD

Theft of, from, and out of vehicles can be mitigated by installing security systems, both ex-factory as well as afterwards (aftermarket). Users and risk bearers both want to be sufficiently assured that the security provided is functional and has been correctly installed in/on the vehicle.
The desired functionality, as well as the installation, can be demonstrated through certification.

This document describes the requirements and assessment methods of Security systems and is used in the CCV Certificatieschema Systemen Voertuigbeveiliging (CCV Certification Scheme for Vehicle Security Systems).

The CCV Certificatieschema Systemen Voertuigbeveiliging (CCV Certification Scheme for Vehicle Security Systems) does not stand alone. Certified security systems are installed by installation companies that are recognized on the basis of the CCV Erkenningsregeling Inbouwbedrijven Voertuigbeveiliging (CCV Recognition Scheme for Vehicle Security Installation Companies).
The CCV Risicomodel Voertuigbeveiliging (CCV Vehicle Security Risk Model) provides guidance regarding which security should be installed.

The CCV is the scheme manager of these documents. These documents are approved by the CCV Commission of Stakeholders Vehicle Security.

This text of this compliance scheme is issued under the auspices of the Centrum voor Criminaliteitspreventie en Veiligheid (Centre for Crime Prevention and Safety) in Utrecht.

TABLE OF CONTENTS

1 SUBJECT AND SCOPE

1.1 SUBJECT AND SCOPE

This document describes the requirements and the inspection method of security systems in vehicles as part of the Keurmerk CCV Voertuigbeveiliging (CCV Vehicle Security Certification Mark).
This document is applied in conjunction with the CCV Certificatieschema Systemen Voertuigbeveiliging (CCV Certification Scheme for Vehicle Security Systems).

1.2 TRANSITIONAL PROVISIONS

This document replaces 'CCV INSPECTION REGULATIONS
VEHICLE SECURITY CCV Inspections Regulations Vehicle Security'version 1.0+C1.
The effective date is December 1, 2021 without a transition period.
In accordance with the provisions of version 1.0+C1, the use of the following documents is permitted until September 1, 2021 for follow-up inspections::

- Keuringsvoorschrift AA04 – Beveiliging personenvoertuigen - Eisen en testmethoden startonderbrekers en alarmsystemen (Inspection Regulations AA04 - Security of passenger vehicles - Requirements and testing methods for immobilizers and alarm systems)
- Keuringsvoorschrift BV03 – Elektronische beveiliging bedrijfsvoertuigen (Inspection Regulations BV03 – Electronic security of commercial vehicles)
- Keuringsvoorschrift MF04 – Elektronische beveiliging motoren (Inspection Regulations MF04 – Electronic security of engines)
- Keuringsvoorschrift WM03 – Beveiliging werk- en land(bouw)materieel (Inspection Regulations WM03 – Security of work and farming equipment)
- Keuringsvoorschriften voor Beveiligingssystemen – AB04 – Administratieve Bepalingen (Inspection Regulations for Security Systems - AB04 - Administrative Provisions)

1.3 OVERVIEW OF THE MOST IMPORTANT CHANGES

The most important changes as compared to version 1.0+C1 are:

- The interpretation decision with regard to paragraph 8.5.1. ("falling asleep") is now included in this version.
- Section 5.1.1 (writing on the DATA BUS) has been amended, and section 7.3.1 has been amended accordingly.
- In the table in section 7.1.5, angle of inclination detection was mentioned twice (different), this has been corrected.
- In Chapter 8, a few paragraphs have been deleted and reworded.

2 NORMATIVE REFERENCES

The following documents that are referred to apply to these inspection regulations.
Only the quoted version applies to dated references (static reference). The latest version of the document (including supplemental and correction sheets) referred to applies to undated references (dynamic reference).
Transition periods referred to in these documents are binding, unless other certification terms and conditions have been laid down in this certification scheme and the inspection regulations.
Other standards or documents mentioned in these standards and documents apply, as indicated herein.
The certification body is in possession of all of the documents mentioned. The supplier is in possession of the documents marked with a *.

CCV Certificatieschema Systemen Voertuigbeveiliging (CCV Certification Scheme for Vehicle Security Systems)		*	CCV Website
CCV Inbouwvoorschrift Voertuigbeveiliging (CCV Installation Regulations for Vehicle Security)		*	CCV Website
Keurmerk CCV Voertuigbeveiliging – termen en definities (CCV Vehicle Security Certification Mark - terms and definitions)			CCV Website
ECE R116	Regulation No 116 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform technical prescriptions concerning the security of motor vehicles against unauthorised use	*	internet
ECE R28	Regulation No 28 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of audible warning devices and of motor vehicles with regard to their audible signals	*	internet

3 TERMS AND DEFINITIONS

For the purposes of this document, the following terms and definitions apply.
All terms and definitions used in and with the documents accompanying the Keurmerk CCV Voertuigbeveiliging (CCV Vehicle Security Certification Mark) are included in the document "Keurmerk CCV Voertuigbeveiliging – termen en definities" (CCV Vehicle Security Certification Mark - terms and definitions).

Attack resistance	Resistance to attacks from the outside with the aim of sabotaging the security system and using the vehicle without authorization.
Ex-factory	A system installed into the vehicle at the factory or factory organization (using OEM parts). An ex-factory system can only be installed after the date of the first authorization if the CCU is already present in the vehicle. The importer must have submitted any additional parts for inspection.
Aftermarket	A system not built into the vehicle at the factory or factory organization that is not Original Equipment Manufacturing (OEM).
Alarm condition	The condition the system is in when a tamper, alarm, or displacement detection has occurred.
Alarm cycle	The period during which audible warning occurs.
Alarm system	An electronic security system for vehicles with an on-board voltage of up to 50 Volt DC, with the aim of detecting the theft of the entire vehicle, or theft inside the vehicle.
Autonomous system	Aftermarket system with own authorization (also called 2nd authorization).
Authorization	Activation/deactivation of the blocking system and/or the alarm system.
Security system	An electronic security system for vehicles with an on-board voltage of up to 50 Volt DC, with the purpose of preventing theft of the vehicle itself, or if applicable, theft from the vehicle.
Interior motion detection	A system that detects movements of the secured object.
Blocking condition	The condition in which blocking is engaged, which prevents the vehicle from moving on its own once the ignition is turned off. This condition never affects the driving state, only the restarting of the vehicle.
Immobilizer/Blocking system	A device that prevents the vehicle from moving on its own.
CCU	Central Control Unit of a security system in which the security functions are brought together.
CCV	Centre for Crime Prevention and Safety. The CCV is the scheme manager and owner of the inspection regulations.
CCV Installation Regulations	The document in which the aftermarket installation requirements for vehicle security have been determined.
Commission of Stakeholders	The committee that provides support for the scheme and is responsible for the content of the inspection regulations. This committee represents interested parties and involved parties.
Code panel	Keypad, installed in the vehicle, through which blocking can be cancelled by entering a multi-digit code.

Code key (Electronically)	A key that, in addition to normal lock access, can also open a lock electronically.
DATA BUS	Vehicle wiring through which various messages are sent digitally to various electronic vehicle components.
Detection	Selectively detecting a signal.
Driver card	An authorization method using a card. In general, this card does not have to be actively operated to (de)activate the security system.
Approved system	A product which, after testing has been conducted, has been determined to meet the requirements of the inspection regulations, and for which an approval number is subsequently assigned by the certification body. This is made visible by publishing the approval number of the product and by placing an approval sticker on the product.
Inclination detection	A system that detects changes in the inclination of a vehicle.
Tilt detection	A system that detects the tilting of the cabin of a commercial vehicle.
Keyless start	The vehicle can be started if the smart key is in the vicinity or in the vehicle.
Keyless entry	The vehicle can be unlocked if the smart key is in the vicinity or in the vehicle.
M.O.	Modus Operandi: How a vehicle is sabotaged/stolen.
Assembly instructions (assembly manual)	Guidelines from the manufacturer or supplier regarding installing the system.
Perimeter detection	**D**etection triggered by switches as soon as one of the doors, hood, trunk lid, tailgate, grill (provided essential parts of the security system can be accessed), or loading door (optional) is opened.
Pre-warning	A system in which early detection of a possible theft attempt is signalled for a short time at a limited volume level.
Relay attack	An attack method in which the signal between the vehicle and the so-called smart key (keyless entry/start) is extended.
Driving state	A state in which the entire (security) system has been disabled and the vehicle can be started and driven normally.
Interior movement detection:	Detection within the vehicle interior that reacts if someone gains access to the interior in any way or if movements are made inside the interior.
Signalling	Visual and audible alarms.
Siren	**A**n electronic acoustic signal generator.
Transponder	A transponder is an electronic device that sends a message in response to a message that has been received. The word transponder is a contraction of the English words transmitter and responder.
Trigger	**A**ny form of input to the alarm that, if the system is in an activated state, will immediately result in an alarm condition.
Type specification	**I**ndividual specification of a system, or a part thereof.
VLG commercial vehicle	Commercial vehicles that are equipped for the transport of dangerous goods by land and that meet the legal requirements of

	the “Regulation on the overland transport of dangerous substances” (VLG) or ADR (international).
Monitoring state	The state in which the entire alarm system, including blocking, is engaged. An interruption of the status of one of the detection inputs will trigger an alarm.
Towing detection	Detection of the movement of the vehicle without the driving state being activated in an authorized manner (ignition off).

4 CLASSIFICATION

4.1 PASSENGER VEHICLES

Classes 1, 2, and 3 are used for passenger vehicles (categories M1 and M2 in accordance with directive 2007/46/EC) and commercial buses, campers, and other vehicle categories up to and including 3,500 kg (N1 - in accordance with directive 2007/46/EC).

4.1.1 CLASS 1

An electronic security device that prevents the vehicle from being moved on its own by unauthorized persons.

This system has been equipped with the following functionality:
- immobilizer/blocking system

4.1.2 CLASS 2

A security system that detects and perceives unauthorized access to and/or the usage of the vehicle. It also prevents the vehicle from being moved on its own by unauthorized persons.

At a minimum, this system has been equipped with the following functionalities:
- immobilizer/blocking system;
- perimeter detection;
- interior movement detection;
- audible warning;
- optical warning.

4.1.3 CLASS 3

A security system that detects and signals unauthorized access to, lifting and towing and/or the usage of the vehicle. It also prevents the vehicle from being moved on its own by unauthorized persons.

At a minimum, this system has been equipped with the following functionalities:
- immobilizer/blocking system;
- perimeter detection;
- interior movement detection;
- audible warning;
- optical warning;
- inclination detection / towing detection

4.2 COMMERCIAL VEHICLES

Classes B1, B2 and B3 are used for commercial vehicles, commercial buses, campers (categories N2, N3, M2, and M4 in accordance with directive 2007/46/EC).

4.2.1 CLASS B1

An electronic security device that prevents the vehicle from being moved on its own by unauthorized persons.

This system has been equipped with the following functionality:
- immobilizer/blocking system
- an expected attack resistance of 5 minutes

4.2.2 CLASS B2

A security system that detects and perceives unauthorized access to and/or the usage of the vehicle. It also prevents the vehicle from being moved on its own by unauthorized persons.

At a minimum, this system has been equipped with the following functionalities:
- immobilizer/blocking system;
- perimeter detection;
- interior movement detection;
- audible warning;
- optical warning;
- cabin tilt detection (if applicable);
- an expected attack resistance of 5 minutes.

4.2.3 CLASS B3

A security system that detects and signals unauthorized access to, lifting and towing and/or the usage of the vehicle. It also prevents the vehicle from being moved on its own by unauthorized persons.

At a minimum, this system has been equipped with the following functionalities:
- immobilizer/blocking system;
- perimeter detection;
- interior movement detection;
- audible warning;
- optical warning;
- cabin tilt detection (if applicable);
- an expected attack resistance of 15 minutes.

4.3 MOTORCYCLES

Classes M1 and M2 are used for mopeds and motorcycles, including quads and other small vehicles with three or four wheels (categories L in accordance with directive EU/168/2013).

4.3.1 CLASS M1

An electronic security device that prevents the vehicle from being moved on its own by unauthorized persons.

This system has been equipped with the following functionality:

- immobilizer/blocking system

4.3.2 CLASS M2

A security system that detects and signals unauthorized access to, lifting and towing and/or the usage of the vehicle. It also prevents the vehicle from being moved on its own by unauthorized persons.

At a minimum, this system has been equipped with the following functionalities:

- immobilizer/blocking system;
- audible warning;
- optical warning;
- inclination detection/towing detection.

4.4 WORK EQUIPMENT

Classes W1 and W2 are used for work equipment (categories T and C in accordance with directive 2003/37/EC).

4.4.1 CLASS W1

An electronic security device that prevents the vehicle from being moved and/or operated by unauthorized persons on its own.

This system has been equipped with the following functionality:

- immobilizer/blocking system;
- an expected attack resistance of 5 minutes.

4.4.2 CLASS W2

An electronic security device that prevents the vehicle from being moved on its own by unauthorized persons.

This system has been equipped with the following functionality:

- immobilizer/blocking system;
- an expected attack resistance of 15 minutes.

5 SYSTEM REQUIREMENTS

5.1 GENERAL

5.1.1
This is regarding security systems that operate with an on-board voltage of a maximum of 50 Volt DC.
The security system must be suitable for the usual nominal on-board voltage that corresponds to the vehicle categories mentioned in chapter 4.

5.1.2
The system must be powered by the vehicle's on-board battery.

5.1.3
All parts that are necessary to guarantee the functioning of the security system are considered as a system component and must also be submitted for inspection.

5.1.4
If the system or system component is integrated with equipment intended for other purposes, this equipment, insofar as it affects the functioning of the system, must meet the inspection requirements.

5.1.5
Components and functionalities which are connected or applied to the security system and which are not described in these inspection regulations, are not part of the product approval.

5.1.6
The security systems referred to in this regulation must meet the requirements of European legislation as stated in Regulation No 116 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform technical prescriptions concerning the protection of motor vehicles against unauthorised use (see Appendix 1).

5.1.7
If a security system uses radio waves, for example, to engage or disengage the security system, it must comply with the relevant European standards (see Appendix 1).

5.1.8
The security system must be designed and installed in such a way that every vehicle equipped with it still meets the technical requirements (type approval).

5.1.9
The security system must not in any way endanger road safety when activated or not activated.

5.1.10
It is not permitted for a system to write on the vehicle's DATA BUS.
Exceptions to this are:

- a written statement from the official importer or the vehicle manufacturer stating that the supplier of the system is allowed to write on the DATA BUS of the vehicle;
- the control of optical signals

5.1.11
Aftermarket security systems that meet the requirements of these inspection regulations are implemented as and identified “with own authorization”.

5.1.12
All requirements apply to ex-factory systems as well as to aftermarket systems.
Based on the information supplied with an application, the certification body can determine how the requirements will be met.

5.1.13
The system, when notified by the certification body, is adapted to the specific M.O. for the specific make and type of vehicle. See appendix 2.

5.2 DESIGN REQUIREMENTS

5.2.1
The systems that are tested in accordance with classes 1/B1/M1 and W1 must at least have the following functionalities:
- aftermarket systems: at least 2 interruptions automatically engaged;
- ex-factory: if the engine management system is interrupted, it counts as double blocking.

5.2.2
The housing of the Central Control Unit (CCU) must be designed in such a way that it meets the installation requirements of the CCV Inbouwvoorschrift Voertuigbeveiliging (CCV Installation Regulations for Vehicle Security).

5.2.3
In accordance with IP54, the housing of a motorcycle security system must be waterproof.

5.2.4
If the system can be mounted on a bracket, the mounting of the CCU on the bracket must be designed in such a way that the CCU cannot be removed in a single movement.

5.2.5
Supplied mounting items must meet the requirements set in the CCV Inbouwvoorschrift Voertuigbeveiliging (CCV Installation Regulations for Vehicle Security).

5.2.6
External relays for blocking are allowed, provided these are controlled encoded by the CCU.

5.2.7
The security system must have a visible signal (e.g. LED) that indicates whether the system is in a driving, blocking, or monitoring state.
This signal is implemented or can be installed in a way that it is clearly visible from the outside as well as from the driver's position within the vehicle.

5.2.8
All system components must comply with these inspection requirements and are only supplied complete.

5.2.9

The type designations and/or brand name under which the approval is issued must be clearly indicated on the CCU.

5.2.10
System parts that are visible outside the vehicle, such as sensors or LED indicators, must not show a recognizable brand or type indication.

5.2.11
During the blocking, monitoring state, or alarm conditions, the (re)programming or replacement of (parts of) the system may not lead to status changes in the system.

5.2.12
During driving and monitoring states, interruptions from 0.1 to 10 seconds from the system's +30 or +15 connections must not let blockings change status.

5.2.13
After and while the ground connection (-31) or the supply voltage (+30) to the system is interrupted at least five (5) times while it is in the blocking or monitoring state or in the alarm condition and the interruption times vary in length between half (0.5) a second to at least 1 minute, the system status should not change.

5.2.14
In the driving state, the system components that engage blocking must not change status if there are variations in a nominal battery voltage of +/- 25%.

5.2.15
Engaging or disengaging blocking must remain possible if there are variations in a nominal battery voltages of +/- 25%.

5.2.16
An attack via the Data Bus, the OBD plug (from the outside or from the inside), or through a wireless connection to the vehicle should never result in the unauthorized partial or total disengaging or the bypassing of the security system.

5.2.17
It must not be possible to program keys while the security system is switched on.

5.2.18
The use of a panic function to activate the optical warning and/or audible warning of the alarm system is only permitted if it has been installed inside the vehicle.

This functionality is independent of the status of the security system and also cannot generate status changes. The vehicle user must be able to disengage the panic alarm.

5.2.19
A production code must be printed onto the circuit board or must be attached to the housing of the CCU and the siren. This can also be software-based.

5.2.20
The system must be supplied with a user manual and assembly instructions that are adapted to the supplied system and must be drawn up in at least the Dutch language.

5.2.21
The user manual must include at least:
- operating conditions;
- operating instructions;
- preventing unnecessary signalling;
- what to do in case of malfunction/defects;
- overview of system components relevant to the user.

5.2.22
The assembly instructions must include at least:
- projection of the system components;
- the method of installation;
  The installation of these parts must not conflict with the CCV Installation Regulations.
- installation and connection diagrams;
- system check (checklist);
- troubleshooting/protocol;
- an overview of the system components.

5.2.23
Classes B1, B2, and W1 systems must have an expected attack resistance of 5 minutes, and classes B3 and W2 systems must have an expected attack resistance of 15 minutes. For this reason, the supplied system and documentation is evaluated by the certification body. Where necessary, the supplier is asked to provide supplemental documentation (or tests).

5.2.24
The engaging and disengaging of an alarm system may be made visible outside of the vehicle through optical warning for a maximum time of 3 seconds.

5.2.25
If the interior movement detection and/or the slope detection can be switched off separately by the user, this may only take place before a maximum amount of time of less than 60 seconds after the system has been engaged.

5.2.26
The power consumption of the entire security system in a blocking and/or monitoring state must be limited to a maximum of twenty (20.0) mA.

5.2.27
The system may not malfunction or become inoperative due to a short circuit of the audible warning and/or optical warning or other system components that must be connected to the CCS.

5.3 ENGAGING

5.3.1
System blocking must engage within 60 seconds or less after the ignition, the (electric) motor, or the driving mode has been disengaged.

5.3.2
If the vehicle is not started after the vehicle’s blocking devices have been disengaged, the blocking devices must be re-engaged after a maximum of 120 seconds.

5.3.3
It must be impossible to engage blocking if the vehicle's (electric) engine is running, the ignition is switched on, or if the driving mode is still operational.

5.3.4
An alarm system may be engaged:
- automatically, after 60 seconds or less after the ignition is switched off;
- automatically, when the vehicle is locked;
- manually, using the same authorization method as for switching off.

5.3.5
If within these 60 seconds, the alarm system can be partially disengaged by opening a door or boot lid (in an unauthorized manner), this part of the alarm system must be fully re-engaged when the relevant door or boot lid is closed.

5.3.6
It must be impossible to program an authorization method using the standard (built-in) software. The reason for this is to prevent a system from being delivered or being modified so that it can switch off without the mandatory authorization of the security system.

5.3.7
All authorization methods that disengage the security system in a passive (without extra action on the remote control/key card/transponder) and wireless manner, must meet the requirements as stated in chapter 8 of these inspection regulations “Inspection requirements for keyless entry/start”.

5.4 DISARMING - GENERAL

5.4.1
The security system may only be disarmed in an authorized way.

5.4.2
All security systems must have an emergency procedure. This is an additional procedure that can be utilized in addition to the standard disarming method to disarm the security system in an authorized way.

5.4.3
When the system is disengaged by an authorized user, the alarm condition must immediately change to the driving state.

5.4.4
Aftermarket systems must always have to disarm “with their own authorization”. It is not allowed for these systems to disarm by, for example, reading signals from the data bus.
This does not apply to approved OEM systems that are installed by the brand dealer after the first authorization.
A trigger delay is allowed under the following conditions:

1. This delay is activated by the OE unlocking command (allowed via data bus). The status that follows does not have a maximum duration.
   Relocking via OE remote will cancel this status, own authorization is not required.
2. Opening the vehicle as well as any other trigger will put the system into a 2nd state.
   - The maximum duration of this is 15 seconds.
   - Before this period has expired, an “own authorization” must take place through an “own authorization” of the alarm system (not via the data bus).
   - If after this period of time there has been no “own authorization”, there will be an alarm condition.
   - An immobilizer must not be deactivated before “own authorization” has been given. This blocking must be installed in such a way that it ensures that the vehicle cannot be moved on its own.
   - This process must be irreversible. Relocking no longer removes the requirement for “own authorization”.
   - This also applies to opening the boot lid separately/exclusively.

5.4.5
It should be impossible to generate the correct code to disable the system within twenty-four (24) hours with a greater probability than one tenth (0.1)%.

5.4.6
Remote controls:
Every time the remote control is used, the code for disengaging must be changed. A randomly chosen code key with a minimum size of sixty four (64) bits must be used for this.

5.4.7
Transponders:
Transponder keys are regarded as remote controls and must, therefore, meet the same (legal) requirements.
Removal of a transponder from a remote control or key must result in permanent visible damage.

5.4.8
Code panels and code keys:
The number of code options for electronic code keys must be at least 50,000, and that for code panels must be at least 10,000.
If the system comes with a standard delivery code of the
code panel that must be changed by the customer, this delivery code may only be used ten (10) times.

5.4.9
Driver cards and smart keys
The maximum distance at which driver cards and smart keys may deactivate the security system is 10 meters, measured from the vehicle.

5.4.10
Smartphone Applications:
If the security system can be disabled with an APP, a code must be entered each time this action is taken. This may be the authorization of the smartphone (fingerprint/code), or a code developed by the APP. The number of code options must be at least 10,000.
The connection, for instance, such as Bluetooth, connecting from the smartphone to the security system, must also have at least 10,000 codes.
When the Bluetooth connection automatically connects to be authorized to switch off, it must meet the requirements as stated in chapter 8 of these inspection regulations “Inspection requirements for keyless entry/start”.

5.4.11
NFC chips.
After each use of the chip, the code for disengaging must change. A randomly chosen code with a minimum size of sixty-four (64) bits must be used for this.

5.4.12
All other disarming methods with which the security system can be disarmed must be submitted for inspection.

6 DETECTION

6.1 GENERAL

6.1.1
After the alarm system has been engaged, it must be in a monitoring state within sixty (60) seconds after all actions needed to activate the system have been taken.

6.1.2
The perimeter and interior movement detection must work independently of each other and must not influence each other's operation.

6.1.3
Perimeter detection must have two detection inputs that operate independently.

6.1.4
Inclination detection or tilt detection is mandatory for B2 and B3 in class 3.
Tilt detection takes place with sensors that react to changes in the tilt angle of the vehicle cabin in relation to the parking position. This applies to both the longitudinal and transverse directions.
The change in tilt angle at which detection must take place is a minimum of two (2) and a maximum of four (4)% = 4 cm. deviation per meter (= 1.1 - 2.3 °).
The position of the vehicle may not affect the tilt detection.
Slow changes in the position of the vehicle (max. 0.2% per sec.) should not affect the tilt detection.
Due to mechanical changes in the parking position of the vehicle, tilt detection may be activated with a delay. This maximum time of this delayed activation is ninety (90) seconds.

6.1.5
Interior motion detection for motorcycles
In the case of motorcycles, any changes from the parking position to a different position of the motorcycle must be detected, after which an alarm must be triggered.

6.1.6
Towing detection must detect unauthorized towing or movement of the vehicle, after which an alarm must be triggered:
- the vehicle is not in driving state (ignition off);
- an alarm must be triggered if the vehicle moves further than 20 meters.

6.1.7
The detection of the opening of the grill (if present,) after which an alarm is triggered, is mandatory for classes B2 and B3.

6.1.8
Interior movement detection must take place using sensors which have to be installed in the vehicle interior.

The certification body tests the interior movement detection as follows:
Place an empty folding box (single sheet) of 270 x 210 x 120 mm +/- 20 mm in the middle of the front seat. Open the front door window 20 cm (+5 cm/-0 cm), close the door, enable the alarm system, and wait for 60 seconds. All other windows are closed. Take the box from the front seat within 4 seconds +/- 2 seconds. The alarm should now go off immediately. Repeat these same steps for the other side. Perform the test on the driver and passenger seats. The system must trigger an alarm in both cases.
When the test is carried out on the rear side windows, the triggering of the alarm is desirable but not mandatory.

6.1.9
In the monitoring state, the alarm condition is triggered as soon as a sensor makes a detection.

6.1.10
Tampering with the interior sensors must result in the alarm being triggered.

6.1.11
The use of adjustable interior movement detection sensors is only permitted if this adjustability cannot easily be changed by the vehicle owner.

6.1.12
Perimeter detection takes place through (original) switch contacts of doors, the boot lid, the hood, the grill, and hatches. If it is not possible to use the original switches, switches approved in accordance with these inspection regulations must be used. The suppliers of the security system must provide these.

6.1.13
For the perimeter detection, all sensors to be used must be tested in accordance with these inspection regulations.

6.1.14
The pre-warning system (optional for class M2) is activated if there are small movements at sensors that may indicate a possible theft attempt.
In the case of pre-warning modules, the sound duration of the signal is limited to five (5) seconds and the volume level is limited to seventy (70) dB(A).

6.1.15
Voltage drop, shock detection, and vibration detection are not allowed

6.2 VLG VEHICLES (AT CLASSES B2/B3)

The following adaptation of the specifications for VLG vehicles is accepted by the RDW (National Road Traffic Service):

6.2.1
The security system must be connected to a VLG current limiter (power consumption maximized and independent of the VLG main switch).

6.2.2
Optical warning must only be connected through the VLG main switch.

6.2.3
Audible signalling must only occur through the emergency power siren.

6.2.4
The maximum power consumption of the current limiter is set at 1 amp at 30 V.

7 SIGNALLING

7.1 GENERAL

7.1.1
Manipulation of the (additional) inputs or outputs of the security system on the vehicle exterior may not lead to more than 10 alarm cycles.

7.1.2
In the monitoring state and alarm condition, the fuses that protect the CCU and the siren cannot be removed without at least audible warning occurring.

7.1.3
The signalling section may not influence blocking in any way.

7.1.4
During an alarm condition, audible warning as well as optical warning is activated immediately.

7.1.5
The requirements for the number and duration of the alarms are indicated below for each detection input.

	Minimum	Maximum	Alarm duration		
			Audible	Visual	Interval
Interior detection	8	10	25-30 sec	0-300 sec	0-15 sec
Inclination detection	8	10	25-30 sec	0-300 sec	0-15 sec
Perimeter detection	8	no maximum	25-30 sec	0-300 sec	0-15 sec
Other sensors	8	no maximum	25-30 sec	0-300 sec	0-15 sec
If the status remains unchanged	1	10	25-30 sec	0-300 sec	0-15 sec

7.2 AUDIBLE WARNING

7.2.1
Audible warning must only occur through an electronic siren that uses an emergency power supply.

7.2.2
Audible warning is immediately activated in the alarm condition for a minimum of twenty-five (25) and a maximum of thirty (30) seconds.

7.2.3
At the end of an alarm cycle, the system should automatically return to the monitoring state, and the reset time should not exceed fifteen (15) seconds.

7.2.4
In the monitoring state and during an alarm condition, it must not be possible to disable the emergency power siren without activating it for a minimum of five (5) minutes or a minimum of ten (10) cycles of twenty-five (25) seconds.

7.2.5
If the siren has a frequency modulation (between 1,800 and 3,550 Hz), it must modulate between 1 and 3 Hertz.

7.2.6
The maximum number of alarms is 10 Cycles, except in the case of perimeter detection. In the case of perimeter detection, the system sounds an alarm indefinitely.

7.2.7
The siren must comply with ECE R28 with a minimum of 105 dB (A) whereby the volume level must be measured after the end of the corrosion test.

7.2.8
The capacity of the siren's emergency power supply must be sufficient to signal for a minimum of five (5) minutes, whereby decreases in volume level may not exceed two (2)%.

7.2.9
The connection between the CCU and the siren must be established through an encrypted signal.

7.2.10
If the wiring between the CCU and the siren is interrupted while in a monitoring state, the system should generate an alarm, and this should not cause the system or siren to shut down.

7.2.11
Use of a wireless siren is permitted under the following conditions:
- Communication at 2 separate frequencies which must be different from those used by the remote control.
- In the event of a cut in or the sabotage of the wireless communication while in a monitoring state, an alarm must be triggered.

7.2.12
In the case of ex-factory systems, if the siren is located in an unsecured zone (for example, behind wheel housing), the siren must be mounted in a way that the siren cannot be disassembled within 5 minutes without alarms being triggered.
It is permitted, for example, to break or cut a plastic part to do so. Using hand tools to do so is permitted.
Breaking mounting brackets is permitted. Cutting open sheet metal is not taken into consideration.

7.3 OPTICAL WARNING

7.3.1
Optical warning may utilize:
- the direction indicators/lights of the vehicle.
- Optical warning that is retrofitted must be provided with an E-mark and a test report and/or certificate that is in accordance with European Regulation No. 6 [1].

[1] In full: Regulation No 6 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of direction indicators for power-driven vehicles and their trailers

- - The direction indicators/lights on the vehicle may be controlled via the DATA bus of the vehicle.

7.3.2
During an alarm condition, optical warning is activated immediately for a duration of up to five (5) minutes.

7.3.3
The minimum length of the optical warning is determined by the length of the audible warning (25 - 30 sec. of the signalling that occurs)

8 TEST REQUIREMENTS KEYLESS ENTRY/START

Requirements and test methods for additional measures to combat relay attacks on vehicles equipped with keyless entry/start.

8.1 GENERAL

8.1.1
Security Systems where no additional measures against relay attacks have been taken, cannot be issued with a CCV Certificaat Voertuigbeveiliging (CCV Vehicle Security Certificate) without additional (manufacturer and/or aftermarket) measures.

8.2 SPECIFIC REQUIREMENTS

8.2.1
With regard to the inspection of an additional measure, a description of the manufacturer regarding the functionality of the additional measure together with a (documented) validation about why it works, and a risk analysis for the possible failure of the additional measure, the ability to influence the additional measure, and possible negative and unintended effects on the additional measure, must be submitted.
Where necessary, additional information is made available at the request of the certification body.

8.3 ATTACK RESISTANCE KEYLESS ENTRY/START

8.3.1
The security system may not be disengaged or bypassed by an attack method in which a keyless remote control signal is extended.

8.3.2
Based on the data supplied with the application, the certification body will:

- Determine whether certification is possible. The application will be rejected if it is possible to indicate in advance why certification is not possible/feasible. For example, solutions that depend on human actions (easy to switch off by human action, or must always be switched on by human action) are not possible.
- Determining the test method. Certification is only possible if the operation itself can be tested by or on behalf of the certification body.
- Determine whether the operation of the supplementary system is definitive, or whether it can be proven that the supplementary system was present and functioning properly.

8.5 ENGAGING AND DISENGAGING

8.5.1
If a supplier of an additional measure has chosen to have the key or the authorization device “sleep” , then the communication between the transmitter/receiver must be automatically been terminated after a maximum of 5 minutes after the key stops moving, for example by putting the key down.
This also applies to keys where such a measure is applied ex-factory systems .

APPENDIX 1 - TESTS

The applicant will provide one or more test reports or certificates showing that the system and the components meet the set requirements.
The tests derived from ECE R116 are legally required for passenger vehicles, and these inspection regulations apply to vehicles other than passenger vehicles.
The tests are performed at the voltage for which the system has been designed. A multi-voltage system is tested at all voltages.
The order in which the tests will be performed is determined by the testing institute, taking into account the provisions in ECE R116, unless otherwise specified in this appendix.
The system components are tested in the condition in which they have been assembled and delivered.
The positioning of the system components during the tests that will be performed is determined by the testing institute and, if possible, in accordance with the CCV installation regulations and/or the supplier's assembly instructions. If there are special requests made by a manufacturer, it must be demonstrated that these are adhered to in the assembly of the position in which the tests have taken place.
During the duration of each test, no unnecessary alarms should be caused, and the system status should not change, except in the usual or intended manner.
After each test, the system components must operate in accordance with the manufacturer's specifications and may not have undergone any distortions and/or changes that may adversely affect the operation of the system components at that time, or over time.
Before and after performing the tests listed below, the system should function normally.

COLD TEST		
Temperature	T = - 40°C ± 2°C	ECE R116, 6.4.2.2.1
Voltage	U = 0.75 x nominal voltage ± 0.2 V	
Acclimatization time	t = 4 hours	

HEAT TEST For parts to be fitted in the passenger or luggage compartments:		
Temperature	T = 85°C ± 2°C	ECE R116, 6.4.2.2.2
Voltage	U = 1.25 x nominal voltage ± 0.2 V	
Acclimatization time	t = 4 hours	

HIGH HEAT TEST For components underneath the hood:		
Temperature	T = 125°C ± 2°C	ECE R116, 6.4.2.2.3
Voltage	U = 1.25 x nominal voltage ± 0.2 V	
Acclimatization time	t = 4 hours	

HIGH VOLTAGE TEST 1	
The system must be exposed to 1.5 x the nominal voltage +/- 2 Volt DC for 1 hour in both the monitoring state as well as in the off state.	ECE R116, 6.4.2.2.4

HIGH VOLTAGE TEST 2	
The system must be exposed to 2 x nominal voltage +/- 2 Volts DC for 1 minute in both the monitoring state as well as in the off state.	ECE R116, 6.4.2.2.5

SAFE OPERATION AFTER WATER TIGHTNESS TESTS	
The system and its components must be protected in accordance with the classes listed below as defined in IEC publication 529-1989: IP40 for system components in the vehicle interior. IP42 for system components in the interior of convertibles and/or sports cars. IP54 for all other system components and motorcycle security systems.	ECE R116, 6.4.2.3

SAFE OPERATION AFTER HEAT TESTS WITH CONDENSATION TESTS	
Heat test with condensation test Weather resistance Seven days in accordance with IEC 68-2-30-1980	ECE R116, 6.4.2.4 ECE R116, 6.4.1.3

SAFE OPERATION AFTER POLARITY REVERSALS	
The system and its components should not fail after performing this test with a voltage of 1.1 x nominal voltage and a duration of 2 minutes.	ECE R116 6.4.2.5

SAFE OPERATION AFTER A SHORT CIRCUIT	
The system and its components should not fail after performing this test with a voltage of 1.1 x nominal voltage.	ECE R116 6.4.2.6

POWER CONSUMPTION	
The power consumption of the complete system must not exceed 20 mA in the monitoring state. The maximum power consumption of motorcycle security systems is 4 mA.	ECE R116 6.4.2.7

SAFE OPERATION AFTER VIBRATION TEST	
Vibration test Type 1: System components mounted onto the vehicle: The frequency should range from 10 Hz to 500 Hz with a maximum amplitude of ± 5 mm and a maximum acceleration of 3 g (peak value). Type 2: System components mounted onto the engine: The frequency should range from 20 Hz to 300 Hz with a maximum amplitude of ± 2 mm and a maximum acceleration of 15 g (peak value). For type 1 and type 2: The frequency variation is 1 octave/min. 10 cycles along each of the 3 axes. Vibrations are applied at a low frequency with a maximum amplitude.	ECE R116, 6.4.2.8 ECE R116, 6.4.2.8.2

SAFE OPERATION ENDURANCE TESTS		
Total number of cycles	250	ECE R116, 6.4.2.9
Test method per cycle	20 times engaging and disengaging 1x driving state 1x blocking condition 1x monitoring state 1x alarm condition	

INTERIOR MOVEMENT DETECTION TEST	
This test must be carried out in accordance with the European inspection regulations.	ECE R116, 6.4.2.9

HF RADIATION (EMC)	
High-frequency radiation tests	ECE R116, Appendix 9

SECURITY AGAINST FALSE ALARMS ON IMPACT	
In this test, we must verify that an impact of a hemispherical orb with an energy of up to 4.5 J, a diameter of 165 mm and a hardness of (70 ± 10) Shore A at any point on the body or the vehicle's glazing does not trigger a false alarm.	ECE R116, 6.4.2.13

TEST FOR FALSE ALARMS INSIDE THE VEHICLE	
The system, which must be installed in accordance with the manufacturer's instructions, must not be activated when it has been subjected to the test described in R116, 6.4.2.13 for five times, each time at an interval of 0.5 s. The presence of a person touching the outside of the vehicle or moving around it (while the windows are closed) should not trigger a false alarm.	ECE R116, 6.4.2.15

VOLTAGE DROP	
In the test, we must verify that a slow drop in the voltage of the main battery due to a continuous discharge at a rate of 0.5 V/h to 3 V/h does not trigger a false alarm.	ECE R116, 6.4.2,14

CORROSION TEST		
Test method per cycle:	conditioned test room	NEN-EN-ISO 9227
System components:	intended to be fitted outside the interior of the vehicle	
Duration per cycle:	144 hours	
Number of cycles:	1	

LOUDNESS TEST	
Measure after corrosion and endurance test. Min. 105 dB (A) max. 118 at a distance of 2 meters with a detachable siren. (85% at 1 meter with installed systems).	ECE R28

RADIO TRANSMISSION	
If the security system is controlled by radio transmission (such as remote controls, but also between the components of the system).	ECE R116, 6.2.3

APPENDIX 2 - M.O. AND INSPECTION REQUIREMENTS

Effective vehicle security is characterized by:

- The correct security measures that are applicable to the risk.
- The correct installation method.

The CCV Risicomodel Voertuigbeveiliging (CCV Vehicle Security Risk Model) indicates which security measures must be applied.
In the addition of functionalities (such as blocking, alarming, detection,) the requirements of the security system are also focused on known M.O.

As scheme manager, the CCV has a Commission for Attack Resistance Assessment (CBA) that has the following tasks:

- Analysing (new and changing M.O.)
- Indicating the extent to which adapted inspection requirements must take effect.

Input for the CBA can be:

- Signalling that the theft percentage exceeds a certain limit, to be determined by the CvB Vehicle Security,
- Signals from the field
- The police determine that new M.O. has been established, or, for example, a location where several vehicles have been stolen is discovered.
- At the request of the parties.

The CBA investigates:

- What the M.O. is and which tools have been used,
- Whether this M.O. is practical and if it can be widely used,
- To what extent the manufacturer has to adapt the system to account for this M.O. and for which brand(s) and type(s).
- To what extent the requirements for the systems or their installation must be adapted.

The CBA records the analysis and conclusions in a report and makes it available to the certification body. With this report, the certification body informs the supplier and specifies within what time period the system must be adjusted.

CENTRE FOR CRIME PREVENTION AND SAFETY

The Centre for Crime Prevention and Safety is the centre that develops and implements coherent tools to increase social security. The CCV encourages cooperation between public and private organisations to integrally reduce crime and forms a link between policy and practice.

With these instruments developed by the CCV, instruments developed by other parties, or (technical) instruments already present at the market level, there may be a need to demonstrate the quality of achieved performances.

The CCV manages compliance schemes for this, for which a structure has been set up with the participation of interested parties.

The Centre for Crime Prevention and Safety is located in Utrecht:
Churchilllaan 11
3527 GV Utrecht
PO Box 14069
3508 SC Utrecht
T (030) 751 6700
F (030) 751 6701
www.hetccv.nl