Date of hosting on website: 23rd June 2023

Last date for comments: 7th July 2023

CHECK LIST FOR PREPARING AMENDMENT TO AUTOMOTIVE INDUSTRY STANDARD (AIS)

Draft Amendment 3 to AIS-076: Approval of Vehicle Alarm Systems (VAS) for M1 and N1 Category of Vehicles and of these Vehicles with regard to their Alarm Systems (AS)

SR. NO.	PARTICULARS	REMARKS
1.0	Is the amendment related to : i) Changes in technical requirements; ii) Corrigendum iii) Any other (Pl. specify)	Amendment is related to insertion of digital key related optional provisions and optional guidelines (Annex 7) approved in earlier AISC meeting.
2.0	Indicate details of base reference standard (amendments).	Regulation UN R116.
3.0	Add an explanatory note indicating deviations from the above base referred standard (amendments) in Sr. 2.	N.A.
4.0	If amendment is for provisions in technical requirements :	
4.1	a) Does amendment call for re-type approval of component / vehicle, which is already type approved? b) Is amendment applicable to fresh type approval of component / vehicle c) Do components / vehicles manufacturers / Test agencies require lead time to meet requirements of amendment?	No Yes No
4.2	If amendment is related to corrigendum : a) Whether changes are required in previous approvals	--
5.0	What are the test equipment for establishing compliance to amendment?	No additional equipment required
6.0	If possible, identify such facilities available in India.	ARAI, CIRT, ICAT,VRDE
7.0	Are there any points on which special comments or information is to be invited from AISC/ CMVR-TSC If yes, are they identified?	NA
8.0	Recommendation of date for implementation of amendment.	With date of approval in AISC.

Explanatory note based on ECE/EEC Directive practices:

1. Amend.X = an amendment issued to the text of the AIS.
2. Rev.X = a Revision of the text comprising all previous text(s) of the AIS.
3. Corr.X = a Corrigendum consists of editorial corrections of errors in the issued texts.

Draft Amendment No. 3

To

AIS-076:2007: Approval of Vehicle Alarm Systems (VAS) for M1 and N1 Category of Vehicles and of these Vehicles with regard to their Alarm Systems (AS)

***(Justification:** Harmonization with UNECE R 116 Amendment 9)*

1. Page 1/34, Add following Clause 1.6 after Clause 1.5

"1.6 In addition, digital keys shall comply with the provisions of Annex 6."

2. Page 3/34, Substitute following text for existing text of Clause 2.7

"2.7 **"Key"** means any mechanical and/or electronic solution designed and constructed to provide a method of operating a locking system which is designed and constructed to be operated by that mechanical and/or electronic solution."

3. Page 3/34, Add following clauses 2.12. to 2.14 after Clause 2.11,

"2.12. **"Primary user"** is a user who is able to authorize digital keys. There can be more than one primary users.

2.13. **"Digital key"** means a key designed to be transferred to multiple devices by the primary user(s) through dedicated processes.

2.14. **"Close proximity"** means a distance of less than 6 m."

4. Page 21/34, Substitute following text for existing text of 15.6

"15.6. **"Key"** means any mechanical and/or electronic solution designed and constructed to provide a method of operating a locking system which is designed and constructed to be operated by that mechanical and/or electronic solution."

5. Page 21/34, Add following new clauses 15.11. to 15.13 after Clause 15.10

"15.11. **"Primary user"** is a user who is able to authorize digital keys. There can be more than one primary users.

15.12. **"Digital key"** means a key designed to be transferred to multiple devices by the primary user(s) through dedicated processes."

15.13. **"Close proximity"** means a distance of less than 6 m."

7. Page 33/34, Renumber existing Annex 6 as Annex 8 and Add new ANNEX 6 & 7 after ANNEX 5,

“ANNEX 6
(See 1.6)
Safety provisions for digital keys

1. General

The purpose of this annex is to specify the requirements for documentation and verification for digital keys used to operate the ‘device to prevent unauthorized use’ and/or the ‘alarm system’ and/or the ‘immobilizer’ of the vehicle.

2. Definitions

2.1. "*Authorization process*" means any method to provide the digital key which can operate the ‘device to prevent unauthorized use’ and/or the ‘alarm system’ and/or the ‘immobilizer’ of the vehicle.

2.2. "*Revocation process*" means any method to prevent the digital key to operate the ‘device to prevent unauthorized use’ and/or the ‘alarm system’ and/or the ‘immobilizer’ of the vehicle.

2.3. "*Boundary of functional operation*" defines the boundaries of the external physical limits (e.g. distance) within which the digital key is able to operate the ‘device to prevent unauthorized use’ and/or the ‘immobilizer’ of the vehicle.

3. Documentation

The vehicle manufacturer shall provide the following documentation for type approval:

3.1. A description of the authorization process.

3.2. A description of the revocation process.

3.3. A description of the boundary of functional operation.

3.4. A description of the safety measures designed within the digital key revocation process to ensure safe operation of the vehicle.

4. Requirements for Safe Operation

4.1. A digital key shall only be transferred to a device via the authorization process.

4.2. There shall be a revocation process.

4.2.1. Revocation of a digital key shall not result in an unsafe condition.

A risk reduction analysis using functional safety standard such as ISO 26262 and safety of the intended functionality standard such as ISO/PAS 21448, which documents the risk to vehicle occupants caused by revocation of a digital key and documents the reduction of risk resulting from implementation of the identified risk mitigation functions or characteristics.

4.2.2. It shall be possible for the primary user(s) to identify the number of authorized registered digital keys.

4.3. Boundary of functional operation for the device to prevent unauthorized use and the immobilizer:

4.3.1. Unlocking of the device to prevent unauthorized use shall require that an authorized registered digital key is detected in the interior of the vehicle, or in close proximity of the vehicle.

4.3.2. Unsetting of the immobilizer shall require that an authorized registered digital key is detected in the interior of the vehicle, or that an actuation is triggered by user intent in close proximity of the vehicle.

The limitation of the distance for unsetting of the immobilizer by detection in the interior of the vehicle shall be verified using the following procedure including a tolerance of 2000 mm around the vehicle perimeter:

(a) The vehicle shall be parked in a secure condition in unobstructed free field condition, this means engine off and all windows, doors and roof shall be closed.

(b) The vehicle manufacturer will provide a typical user device for test in agreement with the test agency. The digital key device battery state of charge shall be at maximum.

(c) The test agency will define four test points around the vehicle perimeter at a distance not less than 2000 mm. Distance means the distance between the nearest point of the motor vehicle and the user device.

(d) The user device is placed at each of the test points. During the attempt to operate the vehicle under its own power, the vehicle door shall be closed. If at one of the test points the vehicle can be operated under its own power, the requirement is not met.

4.3.3. The requirements in paragraph 4.3.1. and paragraph 4.3.2. shall not apply during a remote-control manoeuvring and remote-control parking as defined in AIS-193.

4.3.4 In order to verify safety performance of vehicle with digital key with regards to existing provision of AIS-075 and AIS-076, test conditions as defined in informative Annex 7 may be referred.

4.4. Detailed information shall be contained in the owner's manual of the vehicle, or by any other communication means in the vehicle; as a minimum, this information shall include:

(a) The method(s) for authorization of the digital key

(b) The method(s) for revocation of the digital key

5. The effectiveness of the system shall not be adversely affected by cyber-attacks, cyber threats and vulnerabilities. The effectiveness of the security measures shall be demonstrated by compliance with AIS-189.

6. Verification

Verification of the functionality of the digital key shall be conducted with support of manufacturer's documentation as specified in paragraph 3.

7. Assessment Authority:

The assessments under this Annex shall only be conducted by test agencies as specified in CMV Rule No 126.

*(**Justification for Annex 7:** added guidelines to be referred by test agencies, which were also approved in earlier meeting of AISC)*

ANNEX 7

Verification of safety performance of vehicle with "digital key"

1.0 Remote Engine Start and related features

Sr. No.	Feature, if applicable	Technical information about feature	Requirement Guideline / Acceptance Criteria
1	**Remote Engine Start with HVAC control	In this function, a digital key starts engine and HVAC system Activation is for limited time to get desired temperature inside vehicle to provide thermal comfort.	Digital Key control shall be possible only when • Vehicle shall be in stationary conditions and not in drive mode. • For Automatic transmission - Vehicle shall be in Parking Mode and all doors in Locked condition. • For Manual transmission- Parking brake shall be in applied condition (Notch position as defined by vehicle Manufacturer) with all doors in locked condition. Gear shall be in Neutral position. Additional gateway-electronics / specific hardware for digital key connectivity installed in vehicle shall also meet AIS 076 and AIS 075 requirements (except for smart phone), as applicable. "Remote Engine Start" once activated, engine is allowed to run for maximum 20 minutes. In absence of next action within activation period, engine shall shut down automatically and steering shall get locked to ensure antitheft. During "Remote Engine Start" active mode vehicle shall meet all the conditions specified in Table 1 below to ensure safety.
2	Remote door Lock / unlock	In case driver forget to lock door, a digital permits door locking In case driver want to unlock door for removing something from vehicle, limited time unlocking permitted by a digital key.	Remote door locking / unlocking shall be permitted only when vehicle is in stationary condition. Unlocking shall not be for more than 60 seconds. Within 60 seconds, if no door is opened, vehicle shall lock all the doors automatically.

Sr. No.	Feature, if applicable	Technical information about feature	Requirement Guideline / Acceptance Criteria
3	Stolen Vehicle tracking with car blockage	If the vehicle is reported stolen, Telematics center can initiate the vehicle Immobilization activation process remotely	Immobilization activation shall be possible only through vehicle manufacturer telematics centre on the basis of proper request from vehicle owner. In such case, Engine shall not start or vehicle shall not run after 1st ignition cycle. Such immobilization activation process shall not result in engine stoppage while vehicle in motion. The functioning process of this features shall incorporate secure means to prevent any risk of blocking or accidental malfunctioning which could compromise the safety of the vehicle.
4	Remote Audible device / Lights activation	Digital key can activate Audible device / lights remotely assisting driver to identify vehicle in parking	Activation of Audible device and/or lights shall not be for more than 30 seconds. Vehicle Alarm System activation shall override remote activation

**Remote Engine start with HVAC Control function may be activated by standard vehicle key, provided it meets all Requirement Guideline / Acceptance Criteria, mentioned above.

Table 1: Conditions and requirements for "Remote Engine Start"

Sr. No	Tampering / vehicle theft situations	Requirement
1	When the side doors are unlocked by any means (without key)	"Remote Engine Start" shall be deactivated (i.e) engine shall be switched off automatically. VAS, if fitted shall be operational as per vehicle manufacturer strategy and shall meet AIS-076 requirements.
2	When the rear door or trunk is unlocked by any means (without key)	
3	When window is broken and someone tries to unlock doors from inside	Unlocking door from inside, pressing any of the pedal (as decided by the manufacturer) and shifting gear shall deactivate "Remote Engine Start" (i.e) engine shall be switched off automatically. VAS shall be operational as per vehicle manufacturer strategy and shall meet AIS 076 requirements
4	When Stranger breaks window and enters vehicle and tries to drive the vehicle by using any appropriate pedal (Accelerator/ Clutch) or tries to shift the gear	
5	Stranger entered vehicle and operates gear shift control (Manual Transmission) or Drive mode "D" (for Automatic Transmission) from Parking mode "P".	For Manual Transmission: "Remote Engine Start" shall be deactivated when there is unauthorized operation like • Pedal press (A/B/C) • Gear lever in Non-Neutral Position • Change parking brake lever position (Notch position as defined by vehicle Manufacturer). For Automatic Transmission: "Remote Engine Start" shall be deactivated when there is unauthorized operation like • Gear shift control change from 'P' to any of the mode D/N/R.

2.0 Vehicle driving using a digital key

S No	Feature	Technical information about feature	Requirement Guideline / Acceptance Criteria
1.	Vehicle driving using a digital key	All the functions of existing key	Driving the vehicle shall be possible a digital key, only when the digital key is physically present inside the protected cabin compartment of vehicle (Range of smart phone detection shall be restricted to vehicle compartment similar to existing technology of LF-RF based vehicle key.) The functioning process of this features shall incorporate secure means to prevent any risk of blocking or accidental malfunctioning which could compromise the safety of the vehicle. Vehicle manufacturer shall ensure the security for the feature of smartphone key with proper undertaking at the time of type approval.