Date of hosting on website: 28th December 2023
Last date for comments: 10th January 2024

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

Revised 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)	i) Amendment is related to insertion of digital key related optional provisions.
2.0	Indicate details of base reference standard (amendments).	UN Regulation 116.
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.

Revised 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)

1. Page 1/34, Add a new Clause 1.6 after Clause 1.5. as below,

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

Note: *Digital solutions which cannot be used to operate the 'alarm system' and/or the 'immobilizer' for the purpose of normal driving away of a vehicle under its own motive power are not covered under Digital Key requirements.*

2. Page 3/34, Replace Clause 2.7 as below,

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 a new clause 2.12. to 2.14 as below,

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, Replace Clause 15.6 as below,

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 a new clause 15.11. to 15.13 as below,

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."

6. Page 33/34, Add new ANNEX 6 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.

4.4. 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. *Till the implementation of AIS-189 for complete vehicle level Cyber security requirements, vehicle manufacturer shall, at least comply with system level requirements for digital key system as per paragraph 5.1.*

5.1 *The vehicle Manufacture shall identify threats associated with digital key operation and its external interfaces (like GSM, GPS, Bluetooth, RF, etc.). Proportionate mitigations shall be implemented to protect the vehicle type in which digital key is implemented. The vehicle manufacturer shall demonstrate that the processes used to ensure cyber security for Digital key is adequately considered, including risk and mitigations listed in Annex D of AIS-189 as applicable.*

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.

7. Page 34/34, Renumber existing ANNEX 6 as ANNEX 7.

***(Justification for amendment:** Harmonization with UNECE Regulation 116 Amd. 9)*

***