

Moving Europe towards a sustainable and  
safe railway system without frontiers.

To  
OLTIS Group a.s.,  
Miroslav Fukan  
OLTIS Group Executive Director  
Dr. Milady Horákové 1200/27a  
779 00 Olomouc  
Czech Republic  
(Sent by email)

Valenciennes, 10.10.2023

### Request for Certification of the K\_modul as the Common Interface alternative implementation

To whom it may concern,

I confirm and certify herewith that the following TAF TSI Common Interface functionality implemented by the company OLTIS (Czech Republic), is compliant with the appropriate provisions of the TAF-TSI Regulation (EU) 2021/541 and its Technical Documents.

The detailed results of the verification process are concluded as follows:

OLTIS has sent to the European Union Agency for Railways on 30 August 2023, for verification, the letter "EUAR\_OG\_K\_modul\_certification\_request\_letter\_signed.pdf" accompanied by the technical annex "Annex\_1\_EUAR\_OG\_K\_modul\_certification\_request.pdf", see details in Annex. In this letter OLTIS asked for a verification of the K\_modul, an implementation of the TAF TSI common interface according to the technical document ERA TD-104, Appendix E, Common interface. The applicant would like to ensure, that the K\_modul has been developed in line with the European legislation.

ERA has verified the compliance of the document for the following points from the TAF/TAP TSI regulation:

- a. *message formatting of outgoing messages according to the metadata,*
- b. *signing and encryption of outgoing messages,*
- c. *addressing of the outgoing messages,*
- d. *authenticity verification of the incoming messages,*
- e. *decryption of incoming messages,*
- f. *conformity checks of incoming messages according to metadata,*
- g. *handling the single common access to various databases.*

The applicant has demonstrated, that above functions of the K\_modul are compliant with chapter "4.2.11.5. Common Interface" of the TAF/TAP TSI regulation.

Yours sincerely,



Stefan JUGELT  
European Union Agency for Railways  
Operational Data Unit  
Project Officer

Enclosures: Annex – Compliance report

## Annex – Compliance report

Oltis has sent by email to the European Union Agency for Railways on 30 August 2023, for verification, the following attached document “Annex\_1\_EUAR\_OG\_K\_modul\_certification\_request.pdf”. The document describes the different functions of the K-Module - an implementation of the Common interface - required by the regulation (EU) 1305/2104 (TAF TSI)[1], chapter 4.2.12.6. Common Interface and specified further in the technical document ERA-TD-104 TAF TSI - ANNEX D.2: APPENDIX E - COMMON INTERFACE [4].

In this letter Oltis has requested a certification of the K-module implementation of the common interface, as specified in the TAF TSI. The module shall be verified if the essential requirements of the TSI for this component are fulfilled.

### Basis of the analysis

The TAF TSI specifies in the basic parameter 4.2.12.6. the key requirements of the common interface:

#### *4.2.12.6. Common Interface*

*A Common Interface is mandatory for each actor in order to join the rail interoperability community.*

*A Common Interface has to be able to handle:*

- message formatting of outgoing messages according to the metadata,*
- signing and encryption of outgoing messages,*
- addressing of the outgoing messages,*
- authenticity verification of the incoming messages,*
- decryption of incoming messages,*
- conformity checks of incoming messages according to metadata,*
- handling the single common access to various databases.*

*Each instance of a Common Interface will have access to all the data required according the TSI within each Wagon keeper, LRU, RU, IM, etc., whether the relevant Databases are central or individual (see also document ‘TAF TSI — Annex A.5: Figures and Sequence Diagrams of the TAF TSI messages’, Chapter 1.6, listed in Appendix I).*

*Where a Common Interface is in common use with the TAP TSI (2), the development and changes must be in line with TAP TSI (2), in order to achieve optimum synergies. Based on the results of authenticity verification of incoming messages, a minimum level of message acknowledgement can be implemented:*

- (i) positive send ACK;*
- (ii) negative send NACK.*

*A common interface uses the information in the central repository in order to manage the above tasks.*

*An actor may implement a local ‘mirror’ of the central repository to shorten response times.*

Further requirements are defined in the technical document ERA TD-104 [4].

### Verification procedure

The implementation of the K\_modul has been verified, based on the document “Annex\_1\_EUAR\_OG\_K\_modul\_certification\_request.pdf” [2] provided by OLTIS. The verification has been done based on the information provided by OLTIS in the document above. No further investigation was made by the Agency, such as the installation of the component “K-Modul” on Agency premises or the verification

of an installed K\_modul based on IT test procedures. The document [2] describes several use cases of the K-modul based on the TAF TSI common interface specification. This includes the various messages sent for the example of a PathRequest message according to chapter 4.2.2. Path Request and path allocation of the TAF TSI. The use cases are accompanied by screenshots and example messages. The information provided is used for the analysis of the compliance of the K-Module.

The messages contained in the certification request document have been verified against the specification of the common interface "ERA-TD-104 - TAF TSI - ANNEX D.2: APPENDIX E - COMMON INTERFACE" [4] and the document "ERA\_TD-105 - TAF TSI — ANNEX D.2: APPENDIX F — TAF TSI DATA AND MESSAGE MODEL" [5].

### Verification of the K\_modul

The analysis of the K\_modul based on the certification request document [2] was done by ERA as desk research. The examples provided in the document were checked and compared against the specifications [4] and [5]. During the analysis the agency asked for the clarification of the following points by the submitter:

- *in the chapter "1. Message formatting of outgoing messages according to the metadata"*
  - o *"Message received from CI" the response message was incomplete*
- *in the chapter "2. Signing and encryption of outgoing messages" the following question appeared*
  - o *the encryption of the messages within the SOAP header on the application level was not shown by the applicant.*
- *In the chapter "3. Addressing of the outgoing messages" the following questions appeared*
  - o *The list of the addressed undertakings did not address the railway undertakings*
- *In the chapter "4. Authenticity verification of the incoming messages"*
  - o *The message signature was not explained and documented*
- *In the chapter "5. Decryption of incoming messages" only the HTTPS encryption has been described, but not the encryption of the SOAP payload, as described in [4].*
- *In the chapter "7. Handling the single common access to various databases" the explanation about the implementation of this function was not provided.*
- *The implementation and examples of the heartbeat reply could not be identified in the document*

To cover these points the applicant submitted on 9. October 2023 a revised version of the certification request document [3] to the Agency. In the document the answers concerning the questions above have been given in a satisfactory manner.

It could not be demonstrated that the tool fulfilled the requirement to provide access to common databases, as required by the technical document ERA-TD-104 [4], chapter "2.5 Reference Files and Databases". The explanation of the requestor is, that this function has not been requested by their customers.

### Conclusion

The conclusion of the analysis is that the K-Modul is mostly in line with the common interface specification of the corresponding ERA technical document ERA-TD-104 [4]. The messages required by the TAF TSI common interface, e.g. heartbeat messages, are implemented by the software K\_modul.

The deliverable is in line with the requirements from the TAF TSI.

### Lessons learned

The agency used the opportunity as well to analyse if the feedback of the implementer of the common interface could be used to improve the technical documents of the TAF TSI.

The agency identified the following points to be improved:

1. *Encryption/signing of the Common interface SOAP envelope needs to be better documented.*  
*The requestor commented the question concerning the implementation of the encryption as follows: "The encryption could be provided on 2 different levels: 1, we can use HTTPS connection and the whole communication link between servers is encrypted by the system using the SSL certificate. 2, we can*

*use as you mentioned CI Envelope: <encrypted> and use the internal CI encryption algorithm to encrypt the message. To be able to encrypt the message we need to know: how to generate a key, salt and what is the iteration number. "*

The agency will submit a corresponding change request for the ERA technical document ERA-TD-104 [4] for the further discussion.

## Reference documents

Table 1 - documents used for the compliance assessment.

Index	Document	Version
[1]	Commission Regulation (EU) No 1305/2014 of 11 December 2014 on the technical specification for interoperability relating to the telematics applications for freight subsystem of the rail system in the European Union and repealing the Regulation (EC) No 62/2006	11.12.2014
[2]	Annex_1_EUAR_OG_K_modul_certification_request.pdf	V1 (30.08.2023)
[3]	Annex_1_EUAR_OG_K_modul_certification_request.pdf - update	V2 (09.10.2023)
[4]	ERA-TD-104 - TAF TSI - ANNEX D.2: APPENDIX E - COMMON INTERFACE	3.0
[5]	ERA_TD-105 - TAF TSI — ANNEX D.2: APPENDIX F — TAF TSI DATA AND MESSAGE MODEL".	3.4.0
[6]	K_modul functionalities description	09.10.2023