(1) Introduction

To allow vehicles to undertake journeys at ETCS Level 2, secure communication must be ensured between the ETCS onboard units (OBUs) and the ETCS radio block centres (RBCs). The required cryptographic authentication keys (KMAC) and the unique ETCS-identifier of the vehicle (NID-ENGINE) must be installed on the OBU and at the RBC. DB Netz AG runs a Key Management Centre (KMC DB) for this purpose from which RUs can request keys for DB Netz routes. The e-mail address to be used for exchanging data with KMC DB is

DB.KMC.ETCS@deutschebahn.com

A Key Management Centre (KMC) is a technical database that fulfils all the functional and cryptography-related requirements of UNISIG SUBSET-038 (from Commission Decision 2015/14/EU of 05/01/2015 amending Decision 2012/696/EU on the technical specifications for interoperability relating to the control-command and signalling subsystems of the trans-European rail system) and the normative references named there. Consequently, the KMC must in particular satisfy the following additional criteria:

- UNISIG EURORADIO FIS Subset-037 (from Commission Decision 2015/14/EU)
- ANSI X9.52 – 1998 Triple Data Encryption Algorithm Modes of Operation
- ANSI X3.92 – 1981 Data Encryption Standard (DES) algorithm

The KMC ensures the secure storage and management of the vehicle keys issued to the railway undertaking (RU) in order that they can be reinstalled onboard the vehicle where necessary (for example, following maintenance work) and also enables standardised communication with other KMCs via a preassigned e-mail address.

Since the annex does not differentiate between authorised and non-authorised vehicle keepers, RU is understood to include non-authorised vehicle keepers.

If the RU does not have its own KMC, it can have its vehicles managed by a third-party KMC. Where this is the case, the third-party KMC must be registered with KMC DB. The RU or vehicle keeper can also commission DB Netz AG with managing its vehicles for a charge; see Section 4 "Managing ETCS onboard units".

(2) "Register KMC" procedure

An RU or RIU can use the "Register KMC" request to register its Key Management Centre (KMC) with KMC DB. Only when this registration has been performed can keys be registered for communication between OBUs and DB Netz RBCs.

The request must contain information on the KMC such as name and e-mail address, as well as the details of the party submitting the request. All following key requests must be assigned to the KMC specified here and will only be accepted if the specified e-mail address is used. For communication or the exchange of subset messages between KMC DB and the customer's KMC, a cryptographic key (K-KMC) is required. This key is generated and distributed when the request is processed. The key must be encrypted to be sent and must be saved securely on the customer's KMC (for further information see Section 4).

The request must be sent to the e-mail address provided in Section 1 above. Requests are processed in the order in which they are received. DB Netz AG undertakes to process each request within four weeks.

(3) Distribution of keys (K-KMC)

K-KMC keys must not be distributed unencrypted online. K-KMC keys are distributed using openSSL. Both parties use openSSL to generate one private and one public key and each sends the public key to the other party. The K-KMC is encrypted with this public key and sent exclusively to the e-mail address of the KMC. The K-KMC can only be decrypted with the private key.

Where asymmetric e-mail encryption (e.g. PGP) is available, this can also be used.

The method to be applied must be agreed with DB Netz AG.

(4) "Managing ETCS onboard units" procedure

If the RU does not have its own KMC, DB Netz AG can manage the cryptographic ETCS keys in a Key Management Centre in accordance with SN 6.4.8.

In order to register OBUs with DB Netz AG, the "Assign OBU" request can be used after commissioning. Once the OBUs have been assigned, the required keys can be requested.

For further information please contact DB.KMC.ETCS@deutschebahn.com.

(5) "Request key" procedure

Once the customer's KMC is registered, keys for communication between OBUs and RBCs can be requested using the "Request key" request. Where several vehicles are to be entered for a route, a list of the OBUs can be entered in the request. In addition, the route on which the OBUs are to be used must be entered, as is the validity period. Keys are generated and issued only for routes operated by DB Netz.

If DB Netz AG has not been commissioned to manage the KMCs by the RU, the keys for routes operated by other RIUs in other countries must be requested from them directly. The steps necessary for exchanging keys are to be agreed on by the two parties and are not the responsibility of DB Netz AG.

If the OBUs are managed by DB Netz AG, the key requests are forwarded to the responsible KMCs. If the route lies outside the area operated by DB Netz, the other countries affected are to be entered in the request.

If the RBCs are known, these can be entered along with the route. If they are not known, KMC DB determines which RBCs are relevant from the route information and creates the key accordingly.

The required validity period for the key must be entered in the request and must not exceed five years. Where a longer period is entered, a validity period of only five years will be granted. Where no period is entered, the validity period of five years begins when the key is issued.

The customer must request a new key in good time before the validity period for the current key ends. The key will not be replaced automatically.

The request must be sent to the e-mail address provided above. Requests are processed in the order in which they are received. DB Netz AG undertakes to make the requested keys available within eight weeks.

When a key has been sent to the e-mail address of the customer's KMC, receipt of the e-mail must be confirmed by the customer via the KMC e-mail address within one week, where possible with a subset-compliant confirmation message. If no confirmation has been received within a week, the key is automatically withdrawn and can no longer be used. In this case, the party submitting the request is informed of this measure by e-mail.

(6) "Withdraw key" procedure

If a key is to be withdrawn, the corresponding subset message ("Delete key" request) must be sent to the e-mail address provided above. KMC DB then deletes the key irrevocably in the RBC and KMC and sends the subset-compliant confirmation message.

(7) "Delete OBU" procedure

If the DB KMC serves as the RU KMC, the RU can use the "Delete OBU" request to have the complete OBU deleted. This will mean that all assigned keys and the OBU itself will be deleted. If keys were provided by foreign RIUs, these RIUs will be informed immediately that the keys are no longer used. In the event that such an OBU is later put back into service, it is treated as if it were a new vehicle (see Procedure 4).

(8) Customers' data protection measures

After the key has been received on the KMC, each of the customer's authorised parties is obligated to ensure data security by guaranteeing that only authorised employees use it. Keys must be distributed only as e-mail attachments between the known KMC e-mail addresses and must not be forwarded or sent as a carbon copy, except to the OBU or RBC.

The RU or RIU confirms that the selected KMC undertakes to meet the following requirements:

- Unencrypted keys are handled by a limited number (normally <5) of trustworthy persons only.
- These trustworthy persons must be explicitly nominated within their organisation.
- The handling of keys must be documented and the name of the handling person noted.
- Unauthorised access to keys must be prevented with the use of suitable operational processes and technical environments.
- Outside the protected environment, keys must be encrypted using methods that are comparable at least with the 3DES cryptography of KMC-KMC communication.
- All keys must be stored on fail-safe electronic storage media that are cryptographically secured. The methods used in this must correspond to the latest standard in cryptographic techniques.

The customer undertakes to report any loss or compromising of a key to the above e-mail address without delay and have the key withdrawn. The key must be deleted irrevocably from the OBU at

once. Once it has received the message, DB Netz AG withdraws the key immediately and asks the customer to check whether it is complying with the above provisions.

If a customer repeatedly reports that keys have been lost or compromised, DB Netz AG will assume that the above provisions are not being complied with. The customer will then be requested to have its Compliance unit audited by DB Netz AG or another certified company in the form of a vulnerability analysis in order to identify and eliminate these deviations. If lost or compromised keys pose a direct threat to operations on DB Netz's rail network, DB Netz AG is entitled to take all necessary measures to avert the threat even without the consent and notification of the affected RU. A threat arises if a key is disclosed to unauthorised third parties, since these parties are then able to interfere with ETCS controlling of the vehicle for which the key was provided. If the vehicle at risk is in use, the threat is considered an imminent danger to operations. The Operations Management unit of DB Netz AG will stop this vehicle immediately or prevent it from continuing its journey.

If the vehicle is not yet in use, the Operations Management unit of DB Netz AG will refuse operations on (no movement authorisation from traffic controllers at ETCS centre) or transfers to DB infrastructure. In such a case the RU shall be notified immediately of the reasons why operation was refused.

In addition to these operational measures, operation can be prevented technologically by deleting the relevant keys on the RBCs.

(9) Allocation of the ETCS-identifier (NID-ENGINE)

Each OBU needs a unique ETCS-identifier (NID-ENGINE) which must only be allocated once. The NID-ENGINE will be used for registration of the vehicle at the RBC. The RU is responsible for obtaining the NID-ENGINE which will usually be provided by the manufacturer of the OBU or the vehicle. The manufacturer will take the number from the group of numbers allocated to him and provide this number when handing over the OBU or when handing over the vehicle to the RU.

In case no group of numbers is allocated to the manufacturer or if all numbers are already in use or if other reasons prevent the allocation of the identifier, a RU with head office in the Federal Republic of Germany may request the allocation of a NID-ENGINE at DB Netz AG.

A justified request has to be submitted to: DB.KMC.ETCS@deutschebahn.com

If the request for the NID-ENGINE is reasonable, DB Netz AG will provide the identifier within one month after receipt of the request. The RU is obliged to provide DB Netz AG with all data of the vehicle necessary for allocation and management of the NID-ENGINE. The allocated NID-ENGINE must only be used with the corresponding OBU.

The RU the identifier was allocated to will be responsible to prevent any misuse, especially multiple usage, usage by a vehicle or OBU not indicated in the request or usage of the identifier by third parties.

DB Netz AG is entitled to withdraw the allocated NID-ENGINE in case of misuse or to prohibit all involved vehicles to run on the infrastructure of DB Netz AG.

12 months after allocation of the NID-ENGINE at the latest, the RU must present an authorisation by a member state of the European Union for putting the vehicle into service as a proof of usage of the identifier, or he has to return the NID-ENGINE. A non-formal e-mail will be sufficient and has to be submitted to: DB.KMC.ETCS@deutschebahn.com

(10) Obligations of the RU

The distributed keys serve for cryptographic encoding between RBC and EVC and shall mainly prevent unauthorized access to the communication system by third parties. These keys do not ensure that a vehicle is approved, qualified or authorized to use a specific line safely. To evaluate and ensure this is responsibility of the RU.

Thus, cryptographic keys created and provided by DB Netz AG may only be used without restrictions in vehicles approved for ETCS in Germany.

In case keys were requested for vehicles without approval for ETCS in the area of DB Netz AG, the following points must be considered:

- With ETCS SIM card inserted, the use of ETCS must be technically excluded (except for test or trial runs)
- The activation for use of ETCS may only be done shortly before the beginning of test or trial runs or together with ETCS approval.
- The RU is responsible to provide instructions for the loco driver what to do if in unpredicted cases a change to ETCS mode is proposed. The loco driver must not confirm the change to ETCS Level 0, 1 or 3 on the DMI and must bring the vehicle to a safe stop immediately. Then he has to inform the traffic controller without delay.
- In case the keys were only activated for test or trial runs of a vehicle, they must be deleted at the end of the test or trial runs until the final approval for usage of ETCS in Germany. Alternatively or in addition, a change to ETCS mode for this vehicle may be prevented by software or hardware locks.

Upon receipt of the ETCS keys the RU recognizes these obligations.

(11) Liability

1) DB Netz AG shall be liable without restriction for intent or gross negligence.

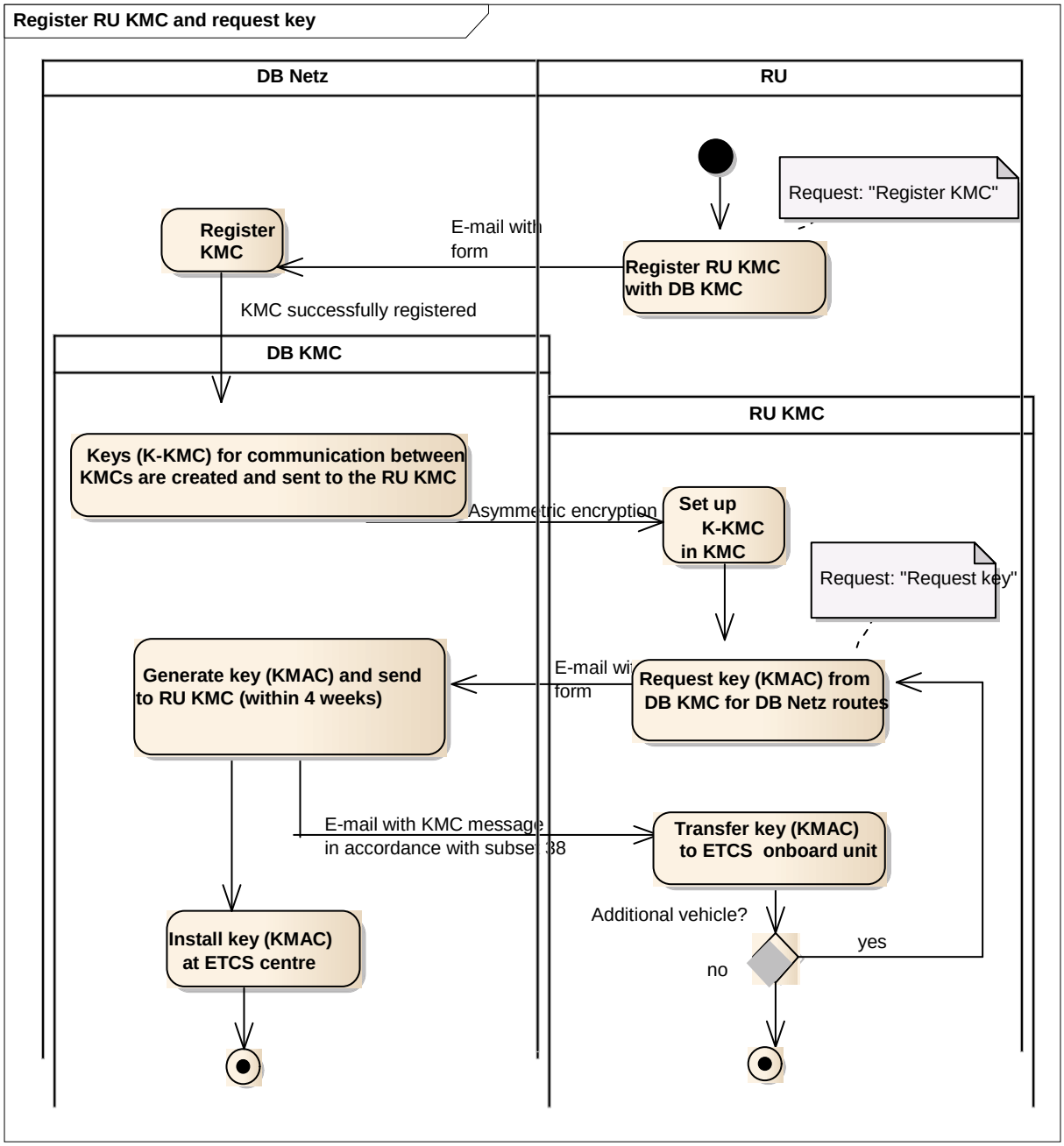
2) DB Netz AG shall only be liable for ordinary negligence—except in the case of harm to life, limb or health—if essential obligations under the provisions of this annex (cardinal duties) are not met. The liability shall be limited to foreseeable damage that is typical for the contract.

3) The liability for indirect and unforeseeable damage, production downtimes and losses, loss of profit, lost savings and financial loss caused by third-party claims shall be excluded in the case of ordinary negligence, except in the case of harm to life, limb or health.

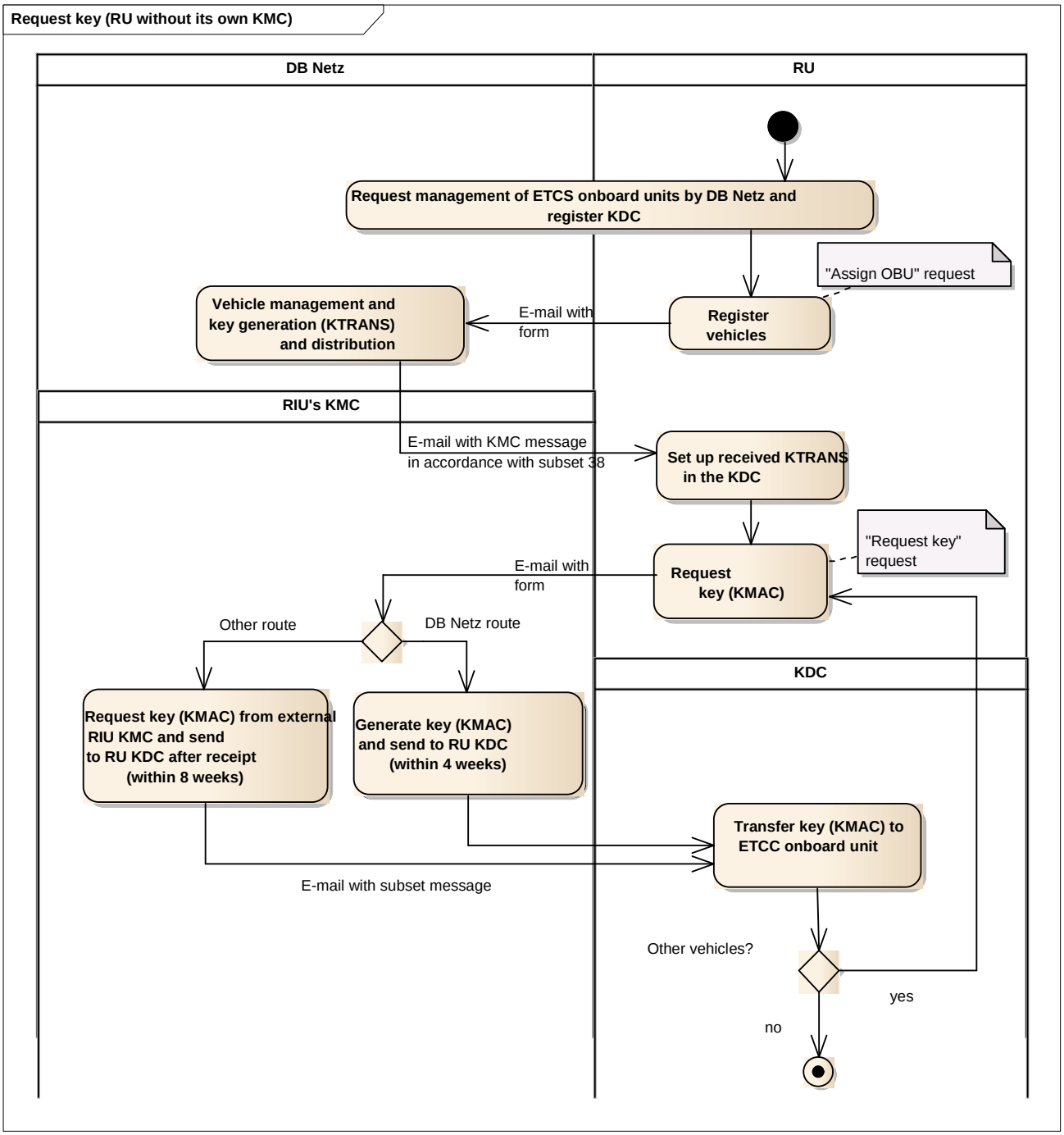
4) Any liability that goes beyond the provisions in this annex shall be excluded irrespective of the legal nature of the claim made. However, the liability limitations or exclusions do not apply to fault-based liability as stipulated by law or liability arising from a fault-based guarantee.

5) Insofar that liability as stipulated under 2 and 3 is excluded or limited, the same applies to the personal liability of employees, representatives, executive bodies and performing agents of DB Netz AG.

(12) Procedure 1: RU registers its own KMC with DB and requests keys for DB Netz routes



(13) Procedure 2: RU has its vehicles managed by DB Netz AG and requests keys for routes



(14) Document overview

- **Requests**
  - **"Register KMC"**
  - **"Request key"**
  - **"Assign OBU"**
  - **"Delete OBU"**

❑