Communication for ERTMS

General

To run on lines with ERTMS Level 2, the railway vehicle must be able to communicate securely with the signalling system. The railway vehicles use a dial-up data connection over GSM-R or GPRS to communicate. The Onboard unit (OBU) must have a SIM card with an ETCS profile and encryption keys to secure the communication between the railway vehicle and the Radio Block Centre (RBC).

The required encryption key is associated with the unique ETCS ID (NID_ENGINE) that each OBU is assigned. The ETCS ID is assigned by the vendor of the onboard equipment. The KMAC encryption key is assigned by the Key Management Center in Bane NOR.

Ordering encryption keys

Bane NOR manages encryption keys for Radio Block Centres (RBC) in Norway and vehicles that have Bane NOR's Key Management Center (KMC) as their home KMC. Bane NOR supports offline distribution of keys to vehicles via files in the SUBSET-114 format and the UAC format (Bombardier Eastern Line). SUBSET-38 format is used for communication with other KMCs. Online Key Distribution uses SUBSET-137.

Two types of encryption keys are used: KMAC and KTRANS. KMAC is used to secure the communication between the OBU and the RBC, and is updated relatively often. KMAC is encrypted with the KTRANS encryption. This encryption makes the change of the KMAC possible without risk of compromise. Online key distribution will replace KTRANS with a digital certificate.

Procedure for vehicle/onboard unit registration

Vehicles that are to receive keys offline or online must be registered in Bane NORs KMC. Registration is done by sending contact information for the person responsible for the vehicle's encryption keys, vehicle data and the ETC ID to kmc@banenor.no. Contact data must be kept up-to-date to ensure that Bane NOR can quickly give notification of abnormal situations, such as suspected compromise or other conditions related to validity and security.

After registration has been approved, the KTRANS encryption key is issued along with a password used for ordering a certificate for online key distribution.

Procedure for ordering KMAC

Encryption keys (KMAC) can be ordered for:

1. Østfoldbanen's Eastern Line – Pilot line for ERTMS
2. ETCS Norge – Provides access to lines in Norway with ETCS, with the exception of the Eastern Line.
3. Foreign countries – the country and route must be specified in the order. Bane NOR will contact the

KMC for the area in question and have keys sent.

Keys are ordered by contacting kmc@banenor.no and are normally valid for a period of five years.

Secure encryption key management

- Two types of encryption keys are used: KMAC and KTRANS. KMAC is used to secure the communication between the OBU and the RBC and is replaced relatively often. This key is encrypted and requires the lowest level of security management. KTRANS is used for the encryption of KMAC. This key is not encrypted and safeguards against it being compromised are based on procedures that must be followed. Nonencrypted keys should be handled only by a limited number of people.
- These individuals must be registered and have completed training and been approved.
- If it is suspected that information concerning the keys may be compromised, this must be reported immediately to Bane NOR.

Ordering encryption keys for guest vehicles

Vehicles that do not have Bane NOR’s KMC as its home KMC shall order keys from their home KMC. Bane NOR will then exchange keys with the vehicle’s home KMC.

Exchange of information

ERTMS is a distributed system in which driver, rail traffic controller, onboard unit, balises, GSM-R, RBC and safety systems communicate for safe train operation. To ensure optimal interaction, log files from the onboard unit shall be made available to Bane NORs troubleshooting team.

Ordering SIM cards for ETCS

The ETCS SIM card is ordered from OPM user support. See Appendix 3.3.3.3

From:
http://networkstatement.jbv.no/ - **Network statement**

Permanent link:
http://networkstatement.jbv.no/doku.php?id=vedlegg_communication_ertms

Last update: **2020/06/02 10:02**