Kapsch SAM-4000: SAM based security solution for DSRC products.

The Kapsch SAM-4000 Secure Application Module is a smartcard that is intended to be used as secure key storage location for Dedicated Short Range Communication (DSRC) based ETC solutions. It provides a high level of fraud protection in operative ETC systems. The SAM-4000 is also available as “add on” for the Kapsch DSRC RF Field product family and offers valuable benefits for system integrators and ETC operators, who integrate these products into their own ETC solutions.

DSRC security basics.
DSRC technology offers a powerful security architecture based on a two-way authentication scheme between the on-board unit and the road side entity. This authentication process complies with “Security Level 1” EN15509 interoperable application profile.

In the downlink direction, the road side entity must present a valid keyset that acts as an access password to the stored data on the OBU. The roadside stored access keys are transformed via cryptographic algorithms, transmitted over the air-interface and then validated by the OBU. This authentication process provides an effective protection against unauthorized access to the OBU memory. The keyset stored locally in the OBU has been either initialized in factory or personalized by the system operator.

In the uplink direction, the OBU is requested to present a mutual known secret key towards the roadside. An authentication mismatch leads to the termination of the DSRC communication due to suspicion of a fraud attempt.

Aspects for secure key storage locations.
The authentication challenge towards the OBU is calculated by deriving a session based temporary value from a so called “master keyset”. Therefore the master keys must be available in the roadside entity. It is imperative for the entire system security, to prevent unauthorized access to the key storage location on the roadside device. This means protection against possible access by manipulated or malfunctioning software modules as well as against unauthorized personnel during operations or maintenance tasks.

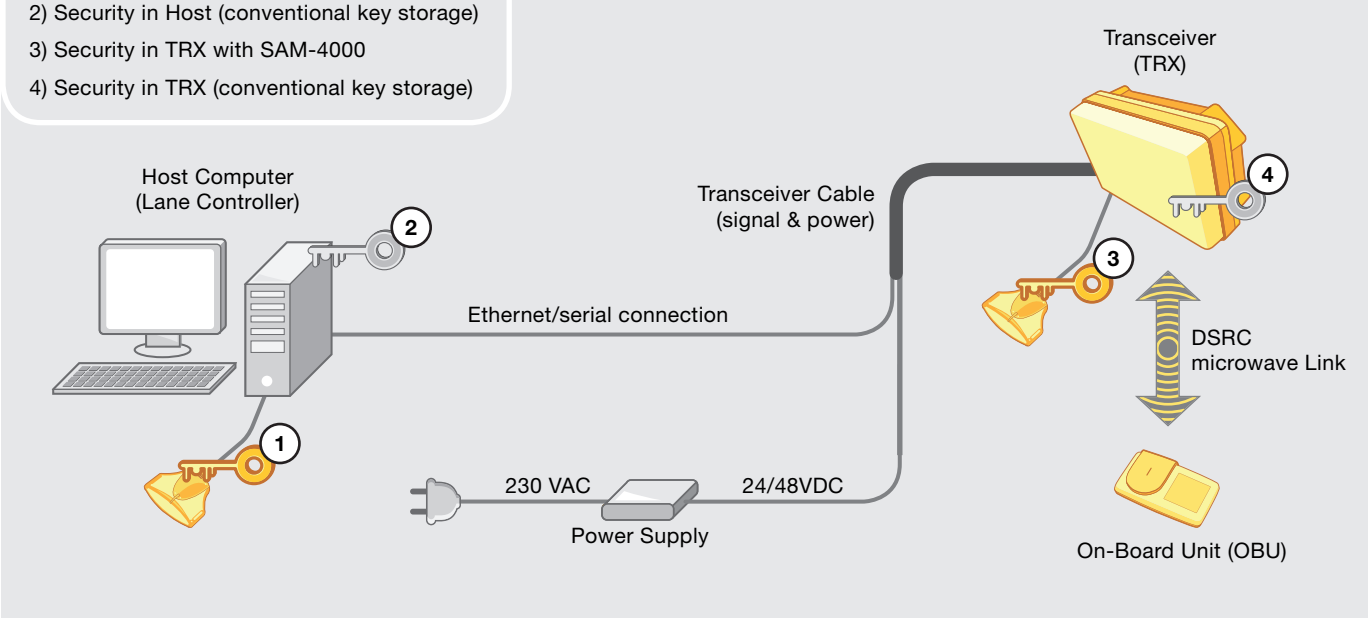
Furthermore, there has to be a secure mechanism to upload the master keys into the DSRC device during start of operation or in case of a system-wide key replacement.

Conventional key storage locations.
When using a conventional key storage location (like an encrypted file on the lane controller or a data field inside the transceiver) it might be inevitable to expose the keys in plain text. This may be necessary, because the transport of newly generated keys from the safe location of the Key Initialization Factory to the tolling site and directly into the roadside device is usually not possible without manual interaction by technical personnel or has to be done via non end-to-end secured communication channels.

The Kapsch solution.
The Kapsch SAM-4000 add on offers an elegant solution against potential security risks by providing a smart card based key storage location, directly connected to the roadside entity. The SAM card prevents the stored keys from any readout attempt and offers the necessary cryptographic operations to be processed directly on the chip. Depending on the project specific environment, the smart card may be connected to the lane controller of the ETC system or directly to the DSRC device (e.g. DSRC transceiver).

Possible key storage locations:
1) Security in Host with SAM-4000
2) Security in Host (conventional key storage)
3) Security in TRX with SAM-4000
4) Security in TRX (conventional key storage)

Example schematics for DSRC transceivers (TRX).



Key benefits of Kapsch SAM-4000:

- There is no possibility to readout the keys from the smartcard processor. The smartcard offers sophisticated and secure methods to update the locally stored keys, even via remote access.
- The SAM-4000 smart card is not only a highly secure storage location for the customers ETC master application keys, it also performs the necessary security calculations directly on the chip. The DSRC roadside device requests the necessary authentication challenge session values directly from the SAM card in realtime without the need of knowing the valuable keys. Vice versa, a presented mutual known encrypted secret key from the OBU is validated inside the SAM card, just answering OK/ NOK towards the roadside device.
- The master keys are never exposed to the host application of the lane controller or the firmware of the transceiver. Software manipulations or manual software maintenance operations are no longer a security threat to the entire system.
- When using the Kapsch OBU Programming Station, OBU key personalization is possible without exposing the keys to the point-of-sales host application.
- The SAM card can be physically removed from the DSRC device and transported to a secure environment. In a closed IT key management system keys are generated and directly written on the SAM card without manual interaction.
- Upgrade of existing conventional ETC systems is often possible without modification of the lane controller software application.

Supported Kapsch products:
The SAM-4000 add on is available for the following DSRC products:

- **TRX-1x20** Single-Lane Transceiver
- **TRX-1x21-A** Access Transceiver
- **OPS-1955** On-Board Unit Programming Station
- **OMR-1734** On-Board Unit Mobile Reader

Key management system.
Security keys are generated in a closed secure environment, the so called Key Initialization Factory (KIF). Kapsch is operating a high security KIF in Sweden and offers key management services including key generation, safe key storage and secure transport channels directly to the clients. Kapsch also offers a complete key management system solution, that may be embedded in the existing infrastructure of the ETC operator or any third party entity. There are several online and offline options for key transportation and key distribution of newly generated keys. The specific solution will be implemented with respect to the customers' requirements and his existing operational processes.

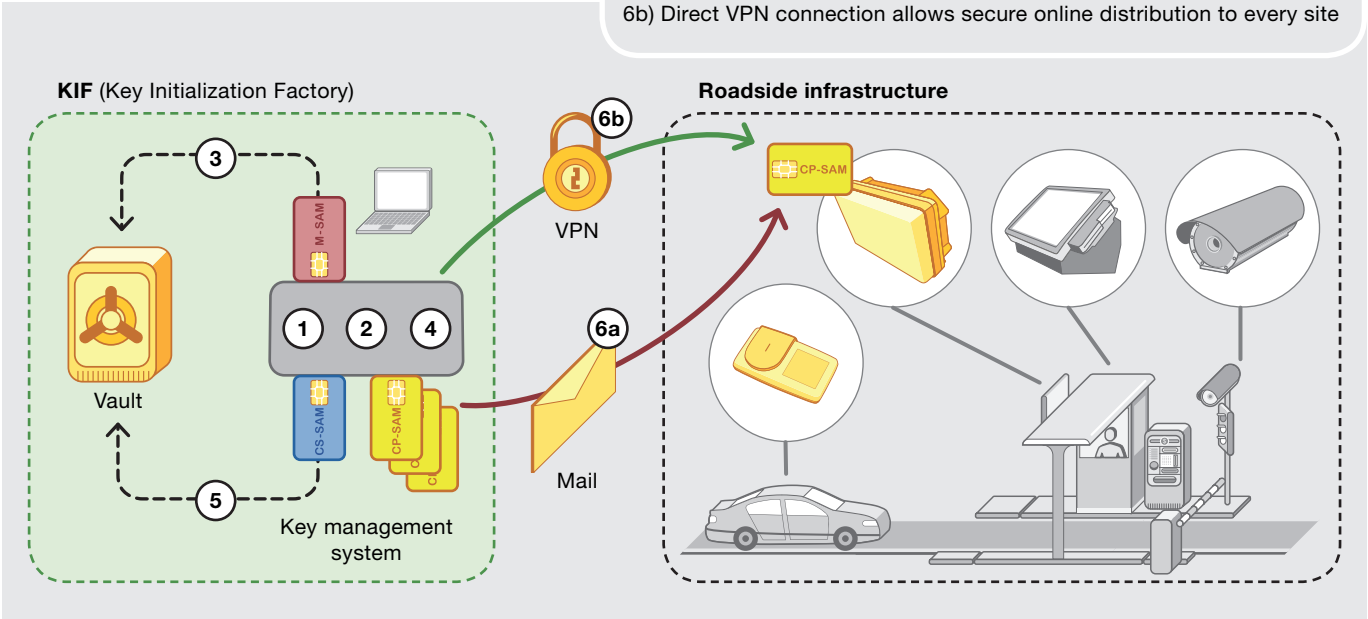
Example of a possible key distribution process.

1) Key generation on M-SAM
2) Write keys on CS-SAM
3) M-SAM is moved into vault
4) Write keys on CP-SAM(s)
5) CS-SAM is moved into vault

6a) CP-SAMs are transported by conventional mail to every single site

Or alternatively:

6b) Direct VPN connection allows secure online distribution to every site



Supported products.

TRX-1x20 Single-Lane & Access Receiver.

OPS-1955 On-Board Unit Programming Station.

OMR-1734 On-Board Unit Mobile Reader.

Technical features

3 Types of SAM-4000 cards:
(3 different variants for different applications)

- M-SAM: Master SAM (red)
- CS-SAM: Central Services SAM (blue)
- CP-SAM: Communication Point SAM (yellow)

Main features SAM-4000:

- DSRC optimized cryptographic operations
- MAC calculation/verification
- Large key storage (>1000 keys)
- Support for remote key distribution
- File encryption/decryption (option)
- High speed baudrate 223 kbaud
- Pre-loaded common hardware key
- Key generation (Master SAM only)
- Digital signature calculation (option)
- Individual assignment of allowed set of commands for each key
- Possible key import from 3rd party key management system
- True random generation
- File access protection according to ISO 7816
- Import/export keys to/from foreign security domains

Physical characteristics:

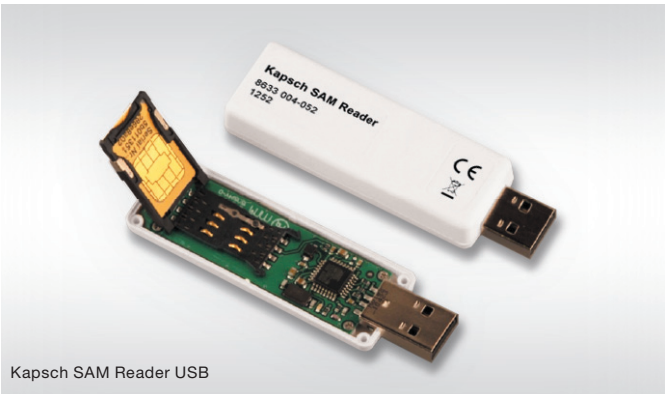
- Card Size: ISO 7810 ID-1, ISO 7810 ID-000
- Pin configuration according ISO 7816
- Supply voltage range: 1.62 V to 5.5 V

Temperature range:

- Storage: -40°C … + 85 °C
- Operation: -25°C … +85 °C

Cryptographic algorithm:

DES	64 bit keys
3DES	128 bit keys
AES	128,256 bit keys
RSA	1024,2048 bit keys
MAC	AES EMAC and CMAC DES MAC
Enc/decryption	ECB mode, CBC mode



Kapsch SAM Reader USB

Kapsch Group

Kapsch is one of Austria's most successful technology corporations, specialized in the future-oriented market segments of Intelligent Transportation Systems (ITS), Railway and Public Operator Telecommunications as well as Information and Communications Technology (ICT). Kapsch. Always one step ahead.

47000000640-01_EN