

Specifications for the Smart-Card Operating System for Transport Applications (SCOSTA)

Addendum to Version 1.2b dated March 15, 2002

Dated: July 31, 2002

**National Informatics Centre
Ministry of Communication and
Information Technology
Government of India**

**Ministry of Road Transport and
Highways
Government of India**

Indian Institute of Technology Kanpur

Scope

This addendum specifies the meaning of the RFU bit (bit b3) of the key type field in the records storing keys in EF2 under the MF or any DF.

Details

The bit b3 (previously RFU) of the key type field in the records that store keys in EF2 under the MF or any DF shall now be interpreted as follows (cf. sec. 6.2.2, SCOSTA specifications version 1.2b, page 15).

The bit b3 of the key type field will now be called the KD bit (Key Derivation bit). If the KD bit is 1 in the key type field of any key, this means that only a key derived from this key can be used for any operation (internal auth, external auth, encryption etc., depending on other bits of the key type). The key derivation can be performed by first restoring the SE that specifies the key (using tag 84) by using the MSE RESTORE command and then using the MSE SET command to set the data item for key derivation. The original key cannot be used for any operation other than key derivation if the KD bit is 1.

If the KD bit of the key type field of a key is 0, this means that no key derivation is possible using this key, and that this key will always be used for any other operation directly.

Implementation of this meaning of the KD bit is mandatory for any SCOSTA compliant operating system for smart cards.