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

Addendum to Version 1.2b dated March 15, 2002

Dated: January 23, 2003

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 clarifies certain issues related to the security architecture and other details relevant to SCOSTA.

Security Architecture in SCOSTA

SCOSTA supports specification of security conditions for accessing various resources in the card. In particular the card resources that can be protected are:

- Files (EFs and DFs). Blank SCOSTA cards will have a pre-existing MF with no security conditions specified for it.
- Commands. In SCOSTA it is possible to protect the execution of various commands as per the application needs. Thus an application may specify that some of the commands may be executed only when some specified security conditions are met.

In order to execute a command, first the command level security will be checked and if permitted then the referred file's FCP will be checked for the protection against the operation being performed. The command can execute successfully only if both these conditions are satisfied.

Security Status

As the security related commands are executed, the card is expected to maintain a *security status* in volatile memory. The security status indicates:

- Which PINs have been verified using the VERIFY command, CHANGE REFERENCE DATA command or DISABLE VERIFICATION REQUIREMENT commands. In the case of the last two commands, the status will be updated only when the provided verification data (PIN from the user) is successfully verified with the stored reference data (PIN in the corresponding EF1 file) wherever applicable.
- Knowledge of which keys the user has proved to the card using the EXTERNAL AUTH and MUTUAL AUTH commands.

The security status is maintained for each node of the path from the MF to the currently selected DF. When the currently selected DF is changed to another DF, the security status for all nodes from the MF till the common ancestor of the old current DF and the new current DF in the directory tree is maintained and the security status for all other nodes is discarded.

Security specifications

The security may be specified for the following two resources.

Files (EFs and DFs): The security for the operations performed on the files is provided in the FCP of the file during the CREATE FILE command.

These specifications can be in the compact format or in the expanded format.

- In the compact format, the security is put under the FCP with a tag of 8C. Under this tag, there can be several access rules. Each rule has one AM Byte as per tables 6 and 7 of ISO/IEC 7816-9 standard. After the AM byte there are several SC bytes as per table 10 of the ISO/IEC 7816-9 standard. The number of SC bytes depends upon the number of bits set to 1 in the AM Byte. If an operation is covered by several access rules specified in the compact form (under tag 8C), any one of them should be satisfied to perform the selected operation (they represent an OR condition). If the operation to be performed is not covered by any of the AM bytes, it will mean that the compact form of the security is satisfied.
- In the expanded format, the security is put under the FCP with a tag of AB. Under this tag also there are several access rules. Each rule has one AM_DO and several SC_DOs. In SCOSTA, all SC_DOs in an access rule must be satisfied for an access rule to be satisfied. The only relevant AM_DO for the security specifications on the files is with tag 80. Multiple access rules represent an OR condition and any one of the matching access rules must be satisfied for the command to be permitted. If no access rule matches the specified operation, it will mean that the security condition is satisfied.

Among the compact and expanded forms of the security attributes, there will be an OR condition. Thus if the security for an operation on a file is specified in compact and expanded form both, any one of them must be satisfied.

For the DELETE FILE operation, the condition, if any, specified for the DELETE FILE (self) operation in the FCP of the file to be deleted *and* the condition, if any, specified for the DELETE FILE (child) operation in the FCP of the parent DF of the file to be deleted must both be satisfied for the command to be executed successfully.

Commands: The security for the execution of the command can only be specified using the expanded form of the security attributes. In the expanded form, there can be several access rules each with one AM_DO and one or more SC_DOs. The AM_DOs for the command security are specified with tag 81 to 8F (Ref: Table 11 of ISO7816-9). If the issued command (CLA, INS, P1 and P2) matches one of the AM_DOs, all the SC_DOs must be satisfied (AND condition) for that particular AM_DO. If the issued command matches several AM_DOs, any one of them must be satisfied (OR condition among the access rules) before the command may be executed.

The command security is specified only in the FCP of the currently selected DF. If there is no specified security, the command will be permitted to execute. Once the command is permitted to execute, if the command refers to a file explicitly (using any of the file referencing mechanism) then the selected operation is permitted only if the security specified in the FCP of that file (and in the FCP of the parent DF, in case of the DELETE FILE operation) is satisfied. A security condition specified in an EF with the expanded form that provides the

security against a command (i.e. AM_DOs with tag between 81 to 8F) has no meaning in SCOSTA and should be ignored.

Examples:

The examples are discussed with the following sub-tree of the files.

MF → DF_1 → DF_2 → EF

If the currently selected file is DF_1 then the commands may be executed only if they satisfied the command level security as specified in the expanded form in the FCP of the DF_1. Only those access rules will be applicable that have the AM_DO with tag between 81 to 8F.

Suppose that the relevant FCP portion for the security attributes for DF_1 is the following.

8C 05 40 23 41 17 19 (Compact Form to say that Delete Self under Ext Auth of SE#3 or User Auth of pin specified in SE#7. Also, Delete child under User Auth of pin specified in SE#9)

AB 11 80 01 40 9E 01 27 80 01 40 9E 01 22 84 01 22 97 00

(Expanded form that says

Delete self under External Auth of SE#7 or External Auth of SE#2.

Command MSE (INS=22) can never be executed.)

Thus, combining the compact form and expanded form security conditions: the DF can be deleted only if one of the four conditions is satisfied:

1. External auth using SE#3
2. User auth using SE#7
3. External auth using SE#7
4. External auth using SE#2

In addition, if DF_1 is the current DF, the MSE command cannot be executed under any circumstances.

Meaning of various tables in ISO7816-9.

Table 10:

Secure messaging is not in use in SCOSTA and therefore bit b7 is ignored. (except when the SC byte is FF).

Bits b4 to b1 specify the SE number (except for the value being 0 or F). The various possible values for bits b8 to b5 have the following meanings.

0, 8 → Meaningless condition

1, 5, 9, D → User auth (password)

2, 6, A, E → External Auth

3, 7 → Either User Auth or External Auth (one of them must satisfy)

4, C → Not used in SCOSTA

B, F → User Auth and External Auth (both must satisfy)

Table 11 and 12:

Tag 80: Length = 1 is the only possibility. Specify the protection for an operation on a file.

Tag 81: Length = x. Provides protection for commands (x number of them with only P2 being specified for each of them).

Tag 82: Length = x. Provides protection for commands (x number of them with only P1 being specified for each of them).

Tag 83: Length = 2x. Provides protection for commands (x number of them with P1 and P2 being specified for each of them).

Tag 84: Length = x. Provides protection for commands (x number of them with only INS being specified for each of them).

Tag 85: Length = 2x. Provides protection for commands (x number of them with INS and P2 being specified for each of them).

Tag 86: Length = 2x. Provides protection for commands (x number of them with INS and P1 being specified for each of them).

Tag 87: Length = 3x. Provides protection for commands (x number of them with INS P1 and P2 being specified for each of them).

Tag 88: Length = x. Provides protection for commands (x number of them with only CLA being specified for each of them).

Tag 89: Length = 2x. Provides protection for commands (x number of them with CLA and P2 being specified for each of them).

Tag 8A: Length = 2x. Provides protection for commands (x number of them with CLA and P1 being specified for each of them).

Tag 8B: Length = 3x. Provides protection for commands (x number of them with CLA P1 and P2 being specified for each of them).

Tag 8C: Length = 2x. Provides protection for commands (x number of them with CLA and INS being specified for each of them).

Tag 8D: Length = 3x. Provides protection for commands (x number of them with CLA INS and P2 being specified for each of them).

Tag 8E: Length = 3x. Provides protection for commands (x number of them with CLA INS and P1 being specified for each of them).

Tag 8F: Length = 4x. Provides protection for commands (x number of them with CLA INS P1 and P2 being specified for each of them).

An AM_DO with tag between 81 to 8F only can be used for specifying the security on the commands. AM_DOs with tag 80 will provide the security only for the file against various operations.

In an access rule, there can be one AM_DO with several SC_DOs. In that case an AND condition will be implied among the SC_DOs. That is all of them must be satisfied.

Table 13:

SC_DOs with tag 90 and 97 are similar to the SC byte being 00 or FF respectively. These SC_DOs will have length = 00.

SC_DOs with tag A4 will be used for the authentication. The value of the DO is an AT CRT. The CRT must include a CRT usage qualifier (tag 95) and the value of the CRT usage qualifier must be either 80 (external auth) or 08 (user auth). If multiple key references are given within the CRT, then any one of them must be satisfied. (This also holds true in defining the SEs).

SC_DOs with tag B4, B6 and B8 are not meaningful with the current SCOSTA, as it does not support secure messaging.

SC_DOs with tag 9E will be valid in SCOSTA with length = 1 and the data will be one SC byte.

SC_DOs with encapsulation (i.e. tag A0 and AF) will refer to several SC_DOs with OR, or AND condition. These tags will not be found in the SC_DOs that are encapsulated within the SC_DOs with tag A0 and AF. That is, an AND or an OR template cannot be embedded within another AND or OR template.

Equivalence of compact form and expanded form of the security attributes:

The compact form of the security attributes can all be specified using the expanded form. However the reverse is not always true. For example, the following two definitions are equivalent.

8C 05 40 23 44 17 19, and

AB 11 (80 01 40) (A0 06 (9E 01 23) (9E 01 17)) (80 01 04) (9E 01 19).

Terminated and Deactivated Life Cycle States of DFs and EFs

If a DF or EF is in the terminated state, the only operations possible on it are selection and deletion. If a DF or EF is in the deactivated state, the only operations possible on it are selection, activation, termination, and deletion.

Further, *no* commands are permitted if a DF in the terminated or deactivated state is the current DF. Any command that specifies a file (EF or DF) by path shall fail if a terminated or deactivated DF is one of the components but not the final component in the path.