



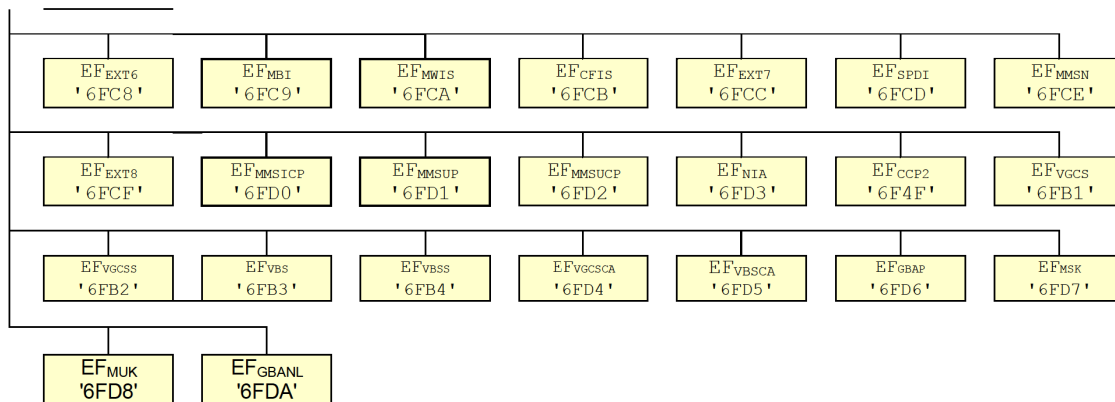


Figure 4.2: File identifiers and directory structures of USIM

5 Application protocol

The requirements stated in the corresponding section of 3GPP TS 31.101 [11] apply to the USIM application.

The procedures listed in clause "USIM management procedures" are required for execution of the procedures in the subsequent clauses "USIM security related procedures" and "Subscription related procedures". The procedures listed in clauses "USIM security related procedures" are mandatory. The procedures listed in "Subscription related procedures" are only executable if the associated services, which are optional, are provided in the USIM. However, if the procedures are implemented, it shall be in accordance with clause "Subscription related procedures".

If a procedure is related to a specific service indicated in the USIM Service Table, it shall only be executed if the corresponding bits denote this service as "service available" (see clause "EF_UST"). In all other cases the procedure shall not start.

5.1 USIM management procedures

If a USIM application is present on the UICC, a 3GPP ME shall only use the USIM application regardless of the radio access technology in use. In this case, a possibly existing SIM application shall never be used by a 3GPP ME.

5.1.1 Initialisation

5.1.1.1 USIM application selection

After UICC activation (see TS 31.101 [11]), the ME selects a USIM application. If no EF_DIR file is found or no USIM applications are listed in the EF_DIR file, the ME may then try to select the GSM application as specified in TS 51.011 [18].

NOTE: there may be cards that need to be reset before selecting the GSM application.

After a successful USIM application selection, the selected USIM (AID) is stored on the UICC. This application is referred to as the last selected USIM application. The last selected USIM application shall be available on the UICC after a deactivation followed by an activation of the UICC.

If a USIM application is selected using partial DF name, the partial DF name supplied in the command shall uniquely identify a USIM application. Furthermore if a USIM application is selected using a partial DF name as specified in TS 31.101 [11] indicating in the SELECT command the last occurrence the UICC shall select the USIM application stored as the last USIM application. If, in the SELECT command, the options first, next/previous are indicated, they have no meaning if an application has not been previously selected in the same session and shall return an appropriate error code.

5.1.1.2 USIM initialisation

The ME requests the emergency call codes. For service requirements, see TS 22.101 [24].

The ME requests the Language Indication. The preferred language selection shall always use the EF_{LI} in preference to the EF_{PL} at the MF unless any of the following conditions applies:

- if the EF_{LI} has the value 'FFFF' in its highest priority position, then the preferred language selection shall be the language preference in the EF_{PL} at the MF level according the procedure defined in TS 31.101[11];
- if the ME does not support any of the language codes indicated in EF_{LI}, or if EF_{LI} is not present, then the language selection shall be as defined in EF_{PL} at the MF level according the procedure defined in TS 31.101[11];
- if neither the languages of EF_{LI} nor EF_{PL} are supported by the terminal, then the terminal shall use its own internal default selection.

The ME then runs the user verification procedure. If the procedure is not performed successfully, the USIM initialisation stops.

The ME performs the administrative information request.

The ME performs the USIM Service Table request.

The ME performs the Enabled Services Table Request.

In case FDN is enabled, an ME which does not support FDN shall allow emergency calls but shall not allow MO-CS calls and MO-SMS.

If BDN is enabled, an ME which does not support Call Control shall allow emergency calls but shall not allow MO-CS calls.

If ACL is enabled, an ME which does not support ACL shall not send any APN to the network.

If all these procedures have been performed successfully then 3G session shall start. In all other cases 3G session shall not start.

Afterwards, the ME runs the following procedures if the ME and the USIM support the related services:

- IMSI request;
- Access control information request;
- Higher Priority PLMN search period request;
- EHPLMN request
- HPLMN selector with Access Technology request;
- User controlled PLMN selector with Access Technology request;
- Operator controlled PLMN selector with Access Technology request;
- GSM initialisation requests;
- Location Information request for CS-and/or PS-mode;
- Cipher key and integrity key request for CS- and/or PS-mode;
- Forbidden PLMN request;
- Initialisation value for hyperframe number request;
- Maximum value of START request;
- CBMID request;
- Depending on the further services that are supported by both the ME and the USIM the corresponding EFs have to be read.

After the USIM initialisation has been completed successfully, the ME is ready for a 3G session and shall indicate this to the USIM by sending a particular STATUS command.

5.1.1.3 GSM related initialisation procedures

If GSM access is enabled the following procedures shall be performed if the applicable service is enabled and if the ME supports the GSM compact access technology.

- Investigation Scan request;
- CPBCCCH information request.

5.1.2 Session termination

5.1.2.1 3G session termination

NOTE 1: This procedure is not to be confused with the deactivation procedure in TS 31.101 [11].

The 3G session is terminated by the ME as follows.

The ME shall indicate to the USIM by sending a particular STATUS command that the termination procedure is starting.

The ME then runs all the procedures which are necessary to transfer the following subscriber related information to the USIM, if the ME and the USIM support the related services:

- Location Information update for CS-and/or PS-domain.
- Cipher Key and Integrity Key update for CS-and/or PS-domain.
- Advice of Charge increase.
- Forbidden PLMN update.
- GSM Termination procedures.

Finally, the ME deletes all these subscriber related information elements from its memory.

NOTE 2: If the ME has already updated any of the subscriber related information during the 3G session, and the value has not changed until 3G session termination, the ME may omit the respective update procedure.

To actually terminate the session, the ME shall then use one of the mechanisms described in TS 31.101 [11].

5.1.2.1.1 GSM termination procedures

If GSM access is enabled the following termination procedures shall be performed if the applicable service is enabled.

- CPBCCCH information update (if the ME supports the GSM compact access technology);

5.1.2.2 3G session reset

The ME shall follow the 3G session termination procedure defined above except that the ME shall use the Application session reset procedure as described in TS 31.101 [11] instead of one of the mechanisms to terminate the session.

5.1.3 USIM application closure

After termination of the 3G session as defined in 5.1.2 the USIM application may be closed by closing the logical channels that are used to communicate with this particular USIM application.

5.1.4 Emergency call codes

Request: The ME performs the reading procedure with EF_{ECC} . If EF_{ECC} does not contain any valid number, the ME shall use the emergency numbers it stores for use in setting up an emergency call without a USIM.

Update: The ME performs the updating procedure with EF_{ECC} .

NOTE: The update procedure is only applicable when access conditions of ADM for update is set to ALW, PIN or PIN2.

5.1.5 Language indication

Request: The ME performs the reading procedure with EF_{LI} .

Update: The ME performs the updating procedure with EF_{LI} .

5.1.6 Administrative information request

The ME performs the reading procedure with EF_{AD} .

5.1.7 USIM service table request

The ME performs the reading procedure with EF_{UST} .

5.1.8 Void

5.1.9 UICC presence detection

The ME checks for the presence of the UICC according to TS 31.101 [11] within all 30 s periods of inactivity on the UICC-ME interface during a call. If the presence detection according to TS 31.101 [11] fails the call shall be terminated as soon as possible but at least within 5s after the presence detection has failed. Here a call covers a circuit switched call, and/or an active PDP context.

5.2 USIM security related procedures

5.2.1 Authentication algorithms computation

The ME selects a USIM application and uses the AUTHENTICATE command (see 7.1.1). The response is sent to the ME (in case of the T=0 protocol when requested by a subsequent GET RESPONSE command).

After a successful AUTHENTICATE command, the ME shall perform cipher and integrity key update procedure.

5.2.2 IMSI request

The ME performs the reading procedure with EF_{IMSI} .

5.2.3 Access control information request

The ME performs the reading procedure with EF_{ACC} .

5.2.4 Higher Priority PLMN search period request

The ME performs the reading procedure with EF_{HPPLMN} .

5.2.5 Location information

Request: The ME performs the reading procedure with EF_{LOC1}.

Update: The ME performs the updating procedure with EF_{LOC1}.

In the case when updating EF_{LOC1} with data containing the TMSI value and the card reports the error '6581' (Memory Problem), the ME shall terminate 3G operation.

5.2.6 Cipher and Integrity key

Request: The ME performs the reading procedure with EF_{Keys}.

Update: The ME performs the updating procedure with EF_{Keys}.

5.2.7 Forbidden PLMN

Request: The ME performs the reading procedure with EF_{FPLMN}.

Update: The ME performs the updating procedure with EF_{FPLMN}.

5.2.8 Void

5.2.9 User Identity Request

The ME selects a USIM and performs the reading procedure with EF_{IMSI}.

5.2.10 GSM Cipher key

Requirement: Service n°27 "available".

Request: The ME performs the reading procedure with EF_{Kc}.

Update: The ME performs the updating procedure with EF_{Kc}.

5.2.11 GPRS Cipher key

Requirement: Service n°27 "available".

Request: The ME performs the reading procedure with EF_{KcGPRS}.

Update: The ME performs the updating procedure with EF_{KcGPRS}.

5.2.12 Initialisation value for Hyperframe number

Request: The ME performs the reading procedure with EF_{START-HFN}.

Update: The ME performs the updating procedure with EF_{START-HFN}.

5.2.13 Maximum value of START

Request: The ME performs the reading procedure with EF_{THRESHOLD}.

5.2.14 HPLMN selector with Access Technology request

Request: The ME performs the reading procedure with EF_{HPLMNwACT}.

5.2.15 Packet Switched Location information

Request: The ME performs the reading procedure with EF_{PSLOC1}.

Update: The ME performs the updating procedure with EF_{PSLOC1}.

5.2.16 Cipher and Integrity key for Packet Switched domain

Request: The ME performs the reading procedure with EF_{KeysPS}.

Update: The ME performs the updating procedure with EF_{KeysPS}.

5.2.17 LSA information

Requirement: Service n°23 "available".

Request: The ME performs the reading procedure with EF_{SAL}, EF_{SLL} and its associated LSA Descriptor files.

Update: The ME performs the updating procedure with EF_{SLL}.

5.2.18 Voice Group Call Services

Requirement: Service n°57 "allocated and activated".

Voice Group Call Service

Request: The ME performs the reading procedure with EF_{VGCS}.

Voice Group Call Service Status

Request: The ME performs the reading procedure with EF_{VGCS}.

Update: The ME performs the updating procedure with EF_{VGCS}.

5.2.19 Voice Broadcast Services

Requirement: Service n°58 "allocated and activated".

Voice Broadcast Service

Request: The ME performs the reading procedure with EF_{VBS}.

Voice Broadcast Service Status

Request: The ME performs the reading procedure with EF_{VBS}.

Update: The ME performs the updating procedure with EF_{VBS}.

5.2.20 Generic Bootstrapping architecture (Bootstrap)

The ME uses the AUTHENTICATE command in GBA security context (Bootstrapping Mode) (see 7.1.1). The response is sent to the ME.

After a successful GBA_U Procedure, the ME shall update the B-TID field and the Key Life Time field in EF_{GBAP}.

5.2.21 Generic Bootstrapping architecture (NAF Derivation)

The ME shall first read EF_{GBAP}. The ME then uses the AUTHENTICATE command in GBA security context (NAF Derivation Mode) (see 7.1.1). The response is sent to the ME.

5.2.22 MSK MIKEY Message Reception

The ME performs the reading of EF_{MUK} and retrieves the Time Stamp Counter Value associated with the involved MUK. Then it proceeds with Timestamp Payload checking as described in TS 33.246 [43].

5.2.23 MTK MIKEY Message Reception

The ME performs the reading of EF_{MSK} and retrieves the Time Stamp Counter Value associated with the involved MSK. Then it proceeds with Timestamp Payload checking as described in TS 33.246 [43].

5.2.24 Void

5.2.25 EHPLMN request

Requirement: Service n°71 "available".

Request: The ME performs the reading procedure with EF_{EHPLMN}.

5.3 Subscription related procedures

5.3.1 Phone book procedures

5.3.1.1 Initialisation

The ME first reads the content of EF_{PBR} to determine the configuration phonebook. If the EF_{IAP} file is indicated in EF_{PBR} following tag 'A8' the ME reads the content of EF_{IAP} in order to establish the relation ship between the content in the files indicated using tag 'A9' and files indicated by tag 'A8'. The ME may read the contents of the phone book related files in any order.

5.3.1.2 Creation/Deletion of information

In order to avoid unlinked data to introduce fragmentation of the files containing phone book data the following procedures shall be followed when creating a new entry in the phone book. The data related to EF_{ADN} is first stored in the relevant record. As the record number is used as a pointer the reference pointer is now defined for the entry. The rule for storing additional information for an entry is that the reference pointer shall be created before the actual data is written to the location.

In case of deletion of a complete or part of an entry the data shall be deleted first followed by the reference pointer for that data element. In case of deletion of a complete entry the contents of EF_{ADN} is the last to be deleted.

5.3.1.3 Hidden phone book entries

If a phone book entry is marked as hidden by means of EF_{PBC} the ME first prompts the user to enter the 'Hidden Key'. The key presented by the user is compared against the value that is stored in the corresponding EF_{Hiddenkey}. Only if the presented and stored hidden key are identical the ME displays the data stored in this phone book entry. Otherwise the content of this phone book entry is not displayed by the ME.

Even if the terminal does not support the Hidden Key Procedures, a hidden phone book entry shall not be displayed by the terminal.

Request: The ME performs the reading procedure with EF_{Hiddenkey}.

Update: The ME performs the updating procedure with EF_{Hiddenkey}.

5.3.2 Dialling numbers

Requirements:

- Service n°1 "available" for ADN located under the local phonebook;
- Presence of EF_{ADN} in EF_{PBR} for ADN located under the global phonebook;
- Presence of EF_{ANR} in EF_{PBR} for ANR;
- Service n°2 "available" for FDN;
- Service n°21 "available" for MSISDN;
- Service n°4 "available" for SDN;
- Service n°6 "available" for BDN;
- Service n°8 "available" for EFOCI;
- Service n°9 "available" for EFICI.

The following procedures may not only be applied to EF_{ADN} and its associated extension files EF_{CCPI} and EF_{EXT1} as described in the procedures below, but also to EF_{ANR}, EF_{FDN}, EF_{MSISDN}, EF_{BDN}, EF_{SDN}, EF_{OCI}, EF_{ICI}, and EF_{MBDN} and their associated extension files. If these files are not allocated and activated, as denoted in the USIM service table, the current procedure shall be aborted and the appropriate EFs shall remain unchanged.

As an example, the following procedures are described as applied to ADN.

Update: The ME analyses and assembles the information to be stored as follows (the byte identifiers used below correspond to those in the definition of the relevant EFs in the present document):

- i) The ME identifies the Alpha-tagging, Capability/Configuration1 Record Identifier and Extension1 Record Identifier.
- ii) The dialling number/SSC string shall be analysed and allocated to the bytes of the EF as follows:
 - if a "+" is found, the TON identifier is set to "International";
 - if 20 or less "digits" remain, they shall form the dialling number/SSC string;
 - if more than 20 "digits" remain, the procedure shall be as follows:
 - The ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted.
 - The first 20 "digits" are stored in the dialling number/SSC string. The value of the length of BCD number/SSC contents is set to the maximum value, which is 11. The Extension1 record identifier is coded with the associated record number in the EF_{EXT1}. The remaining digits are stored in the selected Extension1 record where the type of the record is set to "additional data". The first byte of the Extension1 record is set with the number of bytes of the remaining additional data. The number of bytes containing digit information is the sum of the length of BCD number/SSC contents of EF_{ADN} and byte 2 of all associated chained Extension1 records containing additional data.
- iii) If a called party subaddress is associated to the ADN/SSC the procedure shall proceed as follows:
 - If the length of the called party subaddress is less than or equal to 11 bytes (see TS 24.008 [9] for coding):
 - The ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted.
 - The ME stores the called party subaddress in the Extension1 record, and sets the Extension1 record type to "called party subaddress".
 - If the length of the called party subaddress is greater than 11 bytes (see TS 24.008 [9] for coding):
 - The ME seeks for two free records in EF_{EXT1}. If no such two records are found, the ME runs the Purge procedure. If two Extension1 records are still unavailable, the procedure is aborted.
 - The ME stores the called party subaddress in the two Extension1 records. The identifier field in the Extension1 record containing the first part of the subaddress data is coded with the associated EF_{EXT1}

record number containing the second part of the subaddress data. Both Extension1 record types are set to "called party subaddress".

Once i), ii), and iii) have been considered the ME performs the updating procedure with EF_{ADN}. If the USIM has no available empty space to store the received ADN/SSC, or if the procedure has been aborted, the ME advises the user.

For reasons of memory efficiency, the ME may analyse all Extension1 records to recognise if the additional or subaddress data to be stored is already existing in EF_{EXT1}. In this case, the ME may use the existing chain or the last part of the existing chain from more than one ADN. The ME is only allowed to store extension data in unused records. If existing records are used for multiple access, the ME shall not change any data in those records to prevent corruption of existing chains.

- | | |
|----------|--|
| Erasure: | The ME sends the identification of the information to be erased. The content of the identified record in EF _{ADN} is marked as "free". |
| Request: | The ME sends the identification of the information to be read. The ME shall analyse the data of EF _{ADN} to ascertain, whether additional data is associated in EF _{EXT1} or EF _{CCP1} . If necessary, then the ME performs the reading procedure on these EFs to assemble the complete ADN/SSC. |
| Purge: | The ME shall access each EF which references EF _{EXT1} (EF _{EXT2} , EF _{EXT6}) for storage and shall identify records in these files using extension data (additional data or called party subaddress). Note that existing chains have to be followed to the end. All referred Extension1 (Extension2, Extension6) records are noted by the ME. All Extension1 (Extension2, Extension6) records not noted are then marked by the ME as "free" by setting the whole record to 'FF'. |

The following three procedures are only applicable to service n°2 (FDN).

FDN capability request. The ME shall check the state of service n°2, i.e. if FDN is "enabled" or "disabled". If FDN is enabled, the ME shall only allow outgoing calls as defined in the fixed number dialling description in TS 22.101 [24]. To ascertain the state of FDN, the ME shall check in EF_{UST} and EF_{EST} if FDN is enabled (service activated and available). In all other cases service n°2 is disabled.

FDN enabling is done by activating the FDN service in EF_{EST}.

FDN disabling is done by deactivating the FDN service in EF_{EST}.

The following three procedures are only applicable to service n°6 (BDN).

- BDN capability request. The ME shall check the state of service n°6, i.e. if BDN is "enabled" or "disabled". To ascertain the state of BDN, the ME shall check in EF_{UST} and EF_{EST} if BDN is "enabled" (service available and activated). In all other cases, the BDN service is "disabled".
- BDN enabling is done by activating the BDN service in EF_{EST}.
- BDN disabling is done by deactivating the BDN service in EF_{EST}.

5.3.3 Short messages

Requirement: Service n°10 "available".

Request: The USIM seeks for the identified short message. If this message is found, the ME performs the reading procedure with EF_{SMS}.

If service n°10 is "available" and the status of the SMS is '1D' (status report requested, received and stored in EF_{SMSR}), the ME performs the reading procedure with the corresponding record in EF_{SMSR}. If the ME does not find a corresponding record in EF_{SMSR}, then the ME shall update the status of the SMS with '1S' (status report requested, received but not stored in EF_{SMSR}).

If the short message is not found within the USIM memory, the USIM indicates that to the ME.

Update: The ME looks for the next available area to store the short message. If such an area is available, it performs the updating procedure with EF_{SMS}.

If there is no available empty space in the USIM to store the received short message, a specific MMI will have to take place in order not to lose the message.

Erase: The ME will select in the USIM the message area to be erased. Depending on the MMI, the message may be read before the area is marked as "free". After performing the updating procedure with EF_{SMS}, the memory allocated to this short message in the USIM is made available for a new incoming message. The memory of the USIM may still contain the old message until a new message is stored in this area.

If service n°11 is "available" and the status of the SMS is 'ID' (status report requested, received and stored in EF_{SMSR}), the ME performs the erasure procedure for EF_{SMSR} with the corresponding record in EF_{SMSR}.

5.3.4 Advice of charge

Requirement: Service n°13 "available".

Accumulated Call Meter.

Request: The ME performs the reading procedure with EF_{ACM}. The USIM returns the last updated value of the ACM.

Initialisation: The ME performs the updating procedure with EF_{ACM} using the new initial value.

Increasing: The ME performs the increasing procedure with EF_{ACM} sending the value which has to be added.

Accumulated Call Meter Maximum Value.

Request: The ME performs the reading procedure with EF_{ACMmax}.

Initialisation: The ME performs the updating procedure with EF_{ACMmax} using the new initial maximum value.

Price per Unit and Currency Table (PUCT).

Request: The ME performs the reading procedure with EF_{PUCT}.

Update: The ME performs the updating procedure with EF_{PUCT}.

5.3.5 Capability configuration parameters

Requirement: Service n°14 "available".

Request: The ME performs the reading procedure with EF_{CCP2}.

Update: The ME performs the updating procedure with EF_{CCP2}.

Erase: The ME sends the identification of the requested information to be erased. The content of the identified record in EF_{CCP2} is marked as "free".

5.3.6 User controlled PLMN selector with Access Technology

Requirement: Service n°20 "available".

Request: The ME performs the reading procedure with EF_{PLMNWACT}.

Update: The ME performs the updating procedure with EF_{PLMNWACT}.

5.3.7 Cell broadcast message identifier

Requirement: Service n°15 "available".

Request: The ME performs the reading procedure with EF_{CBMI}.

Update: The ME performs the updating procedure with EF_{CBMI}.

5.3.8 Group identifier level 1

Requirement: Service n°17 "available".

Request: The ME performs the reading procedure with EF_{GID1}.

5.3.9 Group identifier level 2

Requirement: Service n°18 "available".

Request: The ME performs the reading procedure with EF_{GID2}.

5.3.10 Service provider name

Requirement: Service n°19 "available".

Request: The ME performs the reading procedure with EF_{SPN}.

5.3.11 Enhanced multi level precedence and pre-emption service

Requirement: Service n°24 "available".

Enhanced Multi Level Precedence and Pre-emption.

Request: The ME performs the reading procedure with EF_{eMLPP}.

Automatic Answer on eMLPP service.

Request: The ME performs the reading procedure with EF_{AAeM}.

Update: The ME performs the updating procedure with EF_{AAeM}.

5.3.12 Cell broadcast message identifier ranges

Requirement: Service n°16 "available".

Request: The ME performs the reading procedure with EF_{CBMIR}.

Update: The ME performs the updating procedure with EF_{CBMIR}.

5.3.13 Short message status report

Requirement: Service n°11 "available".

Request: If the status of a stored short message indicates that there is a corresponding status report, the ME performs the search record function with EF_{SMSR} to identify the record containing the appropriate status report. The ME performs the reading procedure with EF_{SMSR}.

Update: If a status report is received, the ME first seeks within the SMS record identifiers of EF_{SMSR} for the same record number it used for the short message in EF_{SMS}. If such a record identifier is found in EF_{SMSR}, it is used for storage. If such a record identifier is not found, then the ME seeks for a free entry in EF_{SMSR} for storage. If no free entry is found the ME runs the Purge procedure with EF_{SMSR}. If there is still no free entry, the status report is not stored.

If the ME found an appropriate record in EF_{SMSR} for storage, it updates the record with the status report setting the record identifier in EF_{SMSR} to the appropriate record number of the short message in EF_{SMS}.

The status in EF_{SMS} is updated accordingly by performing the update procedure with EF_{SMS}.

Erasure: The ME runs the update procedure with EF_{SMSR} by at least storing '00' in the first byte of the record. The ME may optionally update the following bytes with 'FF'.

Purge: The ME shall read the SMS record identifier (byte 1) of each record of EF_{SMSR}. With each record the ME checks the corresponding short messages in EF_{SMS}. If the status (byte 1) of the corresponding SMS is not equal '1D' (status report requested, received and stored in EF_{SMSR}), the ME shall perform the erasure procedure with the appropriate record in EF_{SMSR}.

5.3.14 APN Control List

Requirement: Service n°35 "available".

Request: The ME performs the reading procedure with EF_{ACL}.

Update: The ME performs the updating procedure with EF_{ACL}.

Enabling: The ME activates service n°3 in EF_{EST} (bit n°3 set to "1").

Disabling: The ME deactivates service n°3 in EF_{EST} (bit n°3 set to "0").

When the APN Control List service is enabled, the ME shall check that the entire APN of any PDP context is listed in EF_{ACL} before requesting this PDP context activation from the network. If the APN is not present in EF_{ACL}, the ME shall not request the corresponding PDP context activation from the network.

In the case that the APN Control List is enabled and no APN is indicated in the PDP context request, indicating that a network provided APN is to be used, then the ME shall only request the PDP context activation if "network provided APN" is contained within EF_{ACL}.

5.3.15 Depersonalisation Control Keys

Requirement: Service n°36 "available".

Request: The ME performs the reading procedure with EF_{DCK}.

5.3.16 Co-operative Network List

Requirement: Service n°37 "available".

Request: The ME performs the reading procedure with EF_{CNL}.

5.3.17 CPBCCCH information

Requirement: Service n°39 "available".

Request: The ME performs the reading procedure with EF_{CPBCCCH}.

Update: The ME performs the updating procedure with EF_{CPBCCCH}.

5.3.18 Investigation Scan

Requirement: Service n°40 "available".

Request: The ME performs the reading procedure with EF_{InvScan}.

5.3.19 Enabled Services Table Request

Requirement: Service n°34 "available".

Request: The ME performs the reading procedure with EF_{EST}.

Update: The ME performs the updating procedure with EF_{EST}.

5.3.20 Operator controlled PLMN selector with Access Technology

Requirement: Service n°42 "available".

Request: The ME performs the reading procedure with EF_{OPLMNwACT}.

5.3.21 HPLMN selector with Access Technology

Requirement: Service n°43 "available".

Request: The ME performs the reading procedure with EF_{HPLMNwACT}.

5.3.22 Void

5.3.23 Network Parameter information

Request: The ME performs the reading procedure with EF_{NETPAR}.

Update: The ME performs the updating procedure with EF_{NETPAR}.

5.3.24 PLMN network name

Requirement: Service n°45 "available".

Request: The ME performs the reading procedure with EF_{PNN}.

5.3.25 Operator PLMN List

Requirement: Service n°46 "available".

Request: The ME performs the reading procedure with EF_{OPL}.

5.3.26 Message Waiting Indication

Requirement: Service n°48 "available".

Request: The ME performs the reading procedure with EF_{MWIS}.

Update: The ME performs the updating procedure with EF_{MWIS}.

5.3.27 Call Forwarding Indication Status

Requirement: Service n°49 "available".

Request: The ME performs the reading procedure with EF_{CFIS}.

Update: The ME performs the updating procedure with EF_{CFIS}.

5.3.28 Service Provider Display Information

Requirement: Service n°19 and 51 are "available".

Request: The ME performs the reading procedure with EF_{SPDI}.

Update: The ME performs the updating procedure with EF_{SPDI}.

5.3.29 MMS Notifications

Requirement: Service n°52 "available".

- Request:** The ME sends the identification of the information to be read, then the ME performs the reading procedure with EF_{MMSN}. If Service n°53 is available the ME shall analyse the data of EF_{MMSN} to ascertain, whether additional data is associated in EF_{EXT8}. If necessary, then the ME performs the reading procedure on EF_{EXT8} to assemble the complete MMS notification.
- Update:** The ME analyses and assembles the MMS notification to be stored as follows:
- if the MMS notification contains not more bytes than the maximum possible number for EF_{MMSN} then the ME looks for the next available area to store the MMS notification. If such an area is available, it performs the updating procedure with EF_{MMSN}.
 - if the MMS notification contains more bytes than the maximum possible number for EF_{MMSN} then the ME seeks for a sufficient number of free records in EF_{EXT8} to store the complete MMS notification.
 - If there is not a sufficient number of EF_{EXT8} records marked as "free" to store the complete MMS notification, the procedure is aborted.
 - Otherwise, the ME performs the updating procedure and stores as many bytes as possible in EF_{MMSN}. The Extension file record number of EF_{MMSN} is coded with the associated record number in the EF_{EXT8}. The remaining bytes are stored in the selected EF_{EXT8} record where the type of the record is then set to "additional data". The second byte of the EF_{EXT8} record is set with the number of bytes of the remaining additional data. It is possible, if the number of additional digits exceeds the capacity of the additional record, to chain another record inside the EF_{EXT8} by the identifier in the last byte of the record. In this case byte 2 of each record for additional data within the same chain indicates the number of bytes within the same record.
- The ME is only allowed to store extension data in unused records of EF_{EXT8}
- If there is no available empty space in the USIM to store the MMS notification, it is up to ME implementation how the notification is handled.
- Erasure:** The ME will select in the USIM the MMS notification to be erased. Depending on the MMI, the MMS notification may be read before the area is marked as "free". The memory of the USIM may still contain the old MMS notification until a new message is stored. If Service n°53 is available all associated records in EF_{EXT8} are then marked by the ME as "free" by setting them to 'FF'.

5.3.30 MMS Issuer Connectivity Parameters

- Requirement:** Service n°52 "available".
- Request:** the ME performs the reading procedure with EF_{MMSICP}.
- Update:** The ME performs the updating procedure with EF_{MMSICP}.

5.3.31 MMS User Preferences

- Requirement:** Service n°52 "available".
- Request:** the ME performs the reading procedure with EF_{MMSUP}.
- Update:** The ME performs the updating procedure with EF_{MMSUP}.

5.3.32 MMS User Connectivity Parameters

- Requirement:** Service n°52 and n°55 "available".
- Request:** the ME performs the reading procedure with EF_{MMSUCP}.
- Update:** The ME performs the updating procedure with EF_{MMSUCP}.

5.3.33 Network's indication of alerting

- Requirement:** Service n°56 "allocated and activated".

Request: The ME performs the reading procedure with EF_{NIA}.

5.3.34 Multimedia Messages Storage

If the terminal supports Multimedia Message Storage on the USIM, then the following procedures apply.

As defined in TS 23.140 [38] a Multimedia Message consists of content, or multimedia objects, and headers to describe various properties of that content. An MM is stored in EF_{MMDf}, a BER-TLV structured file.

A list of multimedia messages is stored in the BER-TLV file EF_{MML} where each data object identifies one Multimedia Message stored in EF_{MMDf}.

Prerequisite: Service n°67 "available".

Request: The ME performs the reading procedures on EF_{MML} to verify the presence and to get the location information of the targeted MM. Then the ME performs the reading procedure of the EF_{MMDf} file to get the MM.

Update: The ME chooses a free identity (i.e. not listed in EF_{MML}) for the multimedia message and check for available space in the EF_{MMDf} file. This procedure could be done for each update or once at the startup of the UE and after a REFRESH command involving one of the DF_{MULTIMEDIA} files. Then the ME performs the following procedures:

If there is no available empty space in the EF_{MMDf} file to store the MM, the procedure is aborted and the user is notified.

Else, the ME stores the MM in EF_{MMDf}, then updates the information in EF_{MML} accordingly.

Erasure: After a successful deletion of an MM in EF_{MMDf} the terminal updates the information in EF_{MML} accordingly.

5.4 USAT related procedures

5.4.1 Data Download via SMS-PP

Requirement: USIM Service n°28 "available".

The procedures and commands for Data Download via SMS-PP are defined in TS 31.111 [12].

5.4.2 Image Request

The terminal sends the identification of the information to be read. The terminal shall analyse the data of EF_{IMG} to identify the files containing the instances of the image. If necessary, then the terminal performs READ BINARY commands on these files to assemble the complete image instance data.

5.4.3 Data Download via SMS-CB

Requirement: USIM Service n°29 "available".

The ME shall perform the reading procedure with EF_{CBMID}, and add the message identifiers to the Cell Broadcast search list. On receiving a cell broadcast message the procedure defined in TS 31.111 [12] applies.

5.4.4 Call Control by USIM

Requirement: USIM Service n°30 "available".

The procedures and commands for Call Control by USIM are defined in TS 31.111 [12]. It is mandatory for the ME to perform the procedures if it has indicated that it supports Call Control by USIM in the TERMINAL PROFILE command.

5.4.5 MO-SMS control by USIM

Requirement: USIM Service n°31 "available".

The procedures and commands for MO-SMS control by USIM are defined in TS 31.111 [12]. It is mandatory for the ME to perform the procedures if it has indicated that it supports MO-SMS control by USIM in the **TERMINAL PROFILE** command.

5.4.6 Data Download via USSD and USSD application mode

Requirement: Service n°70 "allocated and activated".

The procedures and commands for Data Download via USSD and USSD application mode are defined in TS 31.111 [12].

5.5 MExE related procedures

MExE is an optional feature. The higher level procedures, and contents and coding of the commands are given in TS 23.057 [30]. Procedures relating to the transmission of commands and responses across the USIM/ME interface are given in this clause. A USIM or ME supporting MExE shall conform to the requirements given in this clause.

5.5.1 MExE ST

Requirement: Service n°41 (MExE) "available".

Request: The ME performs the reading procedure with EF_{MExE-ST}

5.5.2 Operator root public key

Requirement: Service n°41 (MExE) "available" and MExE ST service n°1 (EF_{ORPK}) "available".

Request: The ME performs the reading procedure with EF_{ORPK}. The ME shall analyse the data of EF_{ORPK} (clause 4.4.1.4.2) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

5.5.3 Administrator root public key

Requirement: Service n°41 (MExE) "available" and MExE ST service n°2 (EF_{ARPK}) "available".

Request: The ME performs the reading procedure with EF_{ARPK}. The ME shall analyse the data of EF_{ARPK} (clause 4.4.1.4.3) to identify the file containing the certificate instance. If necessary, then the ME performs READ BINARY commands on this file to assemble the complete certificate instance data.

5.5.4 Third Party root public key(s)

Requirement: Service n°41 (MExE) "available" and MExE ST service n°3 (EF_{TPRPK}) "available".

Request: The ME performs the reading procedure with EF_{TPRPK}. The ME shall analyse the data of EF_{TPRPK} (clause 4.4.1.4.4) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

5.5.5 Trusted Key/Certificates Data Files

Requirement: Service n°41 (MExE) "available".

Request: The ME performs the reading procedure with EF_{TKCDF}. The ME shall analyse the data of EF_{TKCDF} and, if necessary, perform READ BINARY commands on these files

5.6 WLAN related procedures

5.6.1 WLAN Selection related Procedures

Prerequisite: service n°62 or n°63 "available"

The ME shall read the User and Operator controlled WSIDs from the corresponding list files (i.e. EF_{UWSIDL} and EF_{OWSIDL}) to perform WLAN selection procedures as described in [40].

The user may change the User controlled WSIDs.

5.6.2 WLAN PLMN Selection related procedures

Prerequisite: service n°60 or n°61 "available"

The ME shall read the User controlled PLMN selector and/or Operator controlled PLMN selector in EF_{PLMNWLAN} and EF_{OPLMNWLAN} respectively for WLAN PLMN Selection procedures as described in [40].

The user may change the User controlled PLMN selector for WLAN.

5.6.3 WLAN access authentication related procedures

Prerequisite: service n°59 "available"

When the ME tries a full authentication, it shall inspect if a valid Pseudonym is available in EF_{Pseudo}, and use it as the user name portion of the NAI for WLAN access authentication following the procedures described in [40].

The ME shall manage pseudonyms as defined in [40].

5.6.4 WLAN access re-authentication related procedures

Requirement: service n°66 "available"

When the ME tries a fast re-authentication, it shall inspect if a valid reauthentication identity is available in EF_{WRI} and use it as the user name portion of the NAI for WLAN access re-authentication following the procedures described in TS 24.234 [40].

The ME shall manage re-authentication identities, Master Key and counter values as described in TS 24.234 [40].

6 Security features

The security aspects of 3G are specified in TS 33.102 [13] and TS 33.103 [14]. This clause gives information related to security features supported by the USIM to enable the following:

- authentication of the USIM to the network;
- authentication of the network to the USIM;
- authentication of the user to the USIM;
- data confidentiality over the radio interface;
- file access conditions;
- conversion functions to derive GSM parameters.

6.1 Authentication and key agreement procedure

This clause gives an overview of the authentication mechanism and cipher and integrity key generation which are invoked by the network. For the specification of the corresponding procedures across the USIM/ME interface see clause 5.

The mechanism achieves mutual authentication by the user and the network showing knowledge of a secret key K which is shared between and available only to the USIM and the AuC in the user's HE. In addition, the USIM and the HE keep track of counters SQN_{MS} and SQN_{HE} respectively to support network authentication. SQN_{HE} is a counter in the HLR/AuC, individual for each user and SQN_{MS} denotes the highest sequence number the USIM has ever accepted.

When the SN/VLR initiates an authentication and key agreement, it selects the next authentication vector and sends the parameters RAND and AUTN (authentication token) to the user. Each authentication token consists of the following components: a sequence number SQN, an Authentication Management Field (AMF) and a message authentication code MAC over the RAND, SQN and AMF.

The USIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the SN/VLR. The SN/VLR compares the received RES with XRES. If they match the SN/VLR considers the authentication and key agreement exchange to be successfully completed. The USIM also computes CK and IK. The established keys CK and IK will be used by the ME to perform ciphering and integrity functions.

A permanent secret key K is used in this procedure. This key K has a length of 128 bits and is stored within the USIM for use in the algorithms described below. Also more than one secret key K can be stored in the USIM. The active key to be used by the algorithms is signalled within the AMF field in the AUTN.

6.2 Cryptographic Functions

The names and parameters of the cryptographic functions supported by the USIM are defined in TS 33.102 [13]. These are:

f1:	a message authentication function for network authentication used to compute XMAC;
f1*:	a message authentication function for support to re-synchronisation with the property that no valuable information can be inferred from the function values of f1* about those of f1, ..., f5, f5* and vice versa;
f2:	a message authentication function for user authentication used to compute SRES;
f3:	a key generating function to compute the cipher key CK;
f4:	a key generating function to compute the integrity key IK;
f5:	a key generating function to compute the anonymity key AK (optional);
f5*:	a key generating function to compute AK in re-synchronisation procedures with the property that no valuable information can be inferred from the function values of f5* about those of f1, f1*, f2, ..., f5 and vice versa.

These cryptographic functions may exist either discretely or combined within the USIM.

6.3 GSM Conversion Functions

To gain GSM access, the USIM provides the conversion functions c2 and c3. These functions derive the required GSM parameters (SRES, cipher key Kc) from available 3G parameters.

6.4 User verification and file access conditions

The security architecture as defined in TS 31.101 [11] applies to the USIM application with the following definitions and additions.

- The USIM application shall use a global key reference as PIN and local key reference as PIN2. For access to DF_{TELECOM} the PIN shall be verified. Access with PIN2 is limited to the ADF(USIM).
- The only valid values for the usage qualifier are '00' (verification requirement is not used) and '08' (user authentication knowledge based (PIN)) as defined in ISO/IEC 7816-9 [26].

Disabling of PIN2 is allowed. This is, however, not the case if PIN2 is mapped to the CHV2 of a GSM application.

7 USIM Commands

7.1 AUTHENTICATE

7.1.1 Command description

The function can be used in several different contexts:

- a 3G security context, when 3G authentication vectors (RAND, XRES, CK, IK, AUTN) are available (i.e. the UE is located in the UTRAN, or in a GSM radio access network which is connected to a 3G or 3G capable VLR/SGSN), or
- a GSM security context, when GSM authentication data are available only (i.e. the UE is located in the GSM radio access network which is connected to a non-3G capable VLR/SGSN)
- a VGCS/VBS security context, when VGCS/VBS authentication data is available
- a GBA_U security context, when a GBA bootstrapping procedure is requested
- a MBMS security context, when a MBMS security procedure is requested

The function is used in GSM or 3G security context during the procedure for authenticating the USIM to its HE and vice versa. In addition, a cipher key and an integrity key are calculated. For the execution of the command the USIM uses the subscriber authentication key K, which is stored in the USIM.

The function is used in VGCS/VBS security context during the procedure for retrieving the VGCS/VBS Short Term Key (VSTK) used by the terminal in establishing VGCS/VBS calls.

The function is used in GBA security context in two different modes:

- a) Bootstrapping Mode: during the procedure for mutual authenticating of the USIM and the Bootstrapping Server Function (BSF) and for deriving bootstrapped key material from the AKA run.
- b) NAF Derivation Mode: during the procedure for deriving Network Application Function (NAF) specific keys from previous bootstrapped key material.

The function is used in MBMS security context in three different modes:

- a) MSK Update Mode: during the procedure for updating an MBMS Service Key (MSK).
- b) MSK Verification Mode: during the procedure for computing the MSK Verification Message previously requested by an MSK update message.
- c) MTK Generation Mode: during the procedure for retrieving the MBMS Traffic Key (MTK) used by the terminal to decrypt MBMS data.

The function is related to a particular USIM and shall not be executable unless the USIM application has been selected and activated, and the current directory is the USIM ADF or any subdirectory under this ADF and a successful PIN verification procedure has been performed (see clause 5).

7.1.1.1 3G security context

The USIM first computes the anonymity key $AK = f_5K(RAND)$ and retrieves the sequence number $SQN = (SQN \oplus AK)$.

Then the USIM computes $XMAC = f_{1K}(SQN \parallel RAND \parallel AMF)$ and compares this with the MAC which is included in AUTN. If they are different, the USIM abandons the function.

Next the USIM verifies that the received sequence number SQN is previously unused. If it is unused and its value is lower than SQN_{MS}, it shall still be accepted if it is among the last 32 sequence numbers generated. A possible verification method is described in TS 33.102 [13].

NOTE: This implies that the USIM has to keep a list of the last used sequence numbers and the length of the list is at least 32 entries.

If the USIM detects the sequence numbers to be invalid, this is considered as a synchronisation failure and the USIM abandons the function. In this case the command response is AUTS, where:

$AUTS = Conc(SQN_{MS}) \parallel MACS$;

$Conc(SQN_{MS}) = SQN_{MS} \oplus f5_K(RAND)$ is the concealed value of the counter SQN_{MS} in the USIM; and.

$MACS = f1_K(SQN_{MS} \parallel RAND \parallel AMF)$ where:

RAND is the random value received in the current user authentication request;

the AMF assumes a dummy value of all zeroes so that it does not need to be transmitted in clear in the resynchronisation message.

If the sequence number is considered in the correct range, the USIM computes RES = f2_K(RAND), the cipher key CK = f3_K(RAND) and the integrity key IK = f4_K(RAND) and includes these in the command response. Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND.

The use of AMF is HE specific and while processing the command, the content of the AMF has to be interpreted in the appropriate manner. The AMF may e.g. be used for support of multiple algorithms or keys or for changing the size of lists, see TS 33.102 [13].

If Service n°27 is "available", the USIM calculates the GSM response parameter K_C, using the conversion function defined in TS 33.102 [13].

Input:

- RAND, AUTN (AUTN := SQN $\oplus$ AK $\parallel$ AMF $\parallel$ MAC).

Output:

- RES, CK, IK if Service n°27 is "not available".

or

- RES, CK, IK, K_C if Service n°27 is "available".

or

- AUTS.

7.1.1.2 GSM security context

USIM operation in an GSM security context is supported if Service n°38 is "available".

The USIM computes RES = f2_K(RAND), the cipher key CK = f3_K(RAND) and the integrity key IK = f4_K(RAND). Next the USIM calculates the GSM response parameters SRES and K_C, using the conversion functions defined in TS 33.102 [13].

Input:

- RAND.

Output:

- SRES; K_C.

7.1.1.3 VGCS/VBS security context

USIM operation in a VGCS/VBS security context is supported if Service n°64 or Service n°65 are "available".

The USIM computes the Short Term Key (VSTK) associated with a particular VGCS/VBS Group Identifier (Group_Id). For this computation, the USIM uses the Voice Group (for VGCS) or Broadcast Group (for VBS) Key

(V_Ki) identified by their respective Group_Id and Master Group Key Identifier (VK_Id). The USIM retrieves the Group_Id and the service flag (VGCS or VBS) from the received Voice Service Identifier (VService_Id).

NOTE: The Group_Id has a variable length according to TS 43.068 [xx].

The USIM shall first search if the Group_Id corresponds to a stored VGCS Group Identifier in EF_{VGCS} or a stored VBS Group Identifier in EF_{VBS}.

Then, the USIM shall retrieve the V_Ki corresponding to the given Group_Id and VK_Id.

Then the USIM uses V_Ki and VSTK RAND as input parameters for the A8_V key derivation function (as defined in 3GPP TS 43.020 [44]) in order to compute and returns VSTK.

Input:

- VService_Id, VK_Id, VSTK RAND

Output:

- VSTK.

7.1.1.4 GBA security context (Bootstrapping Mode)

USIM operations in GBA security context are supported if service n°68 is "available".

The USIM receives the RAND and AUTN. The USIM first computes the anonymity key $AK = f5_K(RAND)$ and retrieves the sequence number $SQN = (SQN \oplus AK) \oplus AK$.

The USIM calculates $IK = f4_K(RAND)$ and MAC (by performing the MAC modification function described in TS 33.220 [42]). Then the USIM computes $XMAC = f1_K(SQN || RAND || AMF)$ and compares this with the MAC previously produced. If they are different, the USIM abandons the function.

Then the USIM proceeds by checking AUTN as in UMTS security context. If the USIM detects the sequence numbers to be invalid, this is considered as a synchronisation failure and the USIM abandons the function. In this case the command response is AUTS, which is computed as in UMTS security context.

If the sequence number is considered in the correct range, the USIM computes $RES = f2_K(RAND)$ and the cipher key $CK = f3_K(RAND)$.

The USIM then derives and stores GBA_U bootstrapped key material from CK, IK values. The USIM shall also stores RAND in the RAND field of EF_{GBAP}.

The USIM stores GBA_U bootstrapped key material from only one bootstrapping procedure. The previous bootstrapped key material, if present, shall be replaced by the new one. This key material is linked with the data contained in EF_{GBAP}: RAND, which is updated by the USIM and B-TID, which shall be further updated by the ME.

NOTE: According to TS 33.220 [42], NAF-specific keys that may be stored on the USIM are not affected by this bootstrapping operation.

RES is included in the command response after flipping the least significant bit.

Input:

- RAND, AUTN

Output:

- RES

or

- AUTS

7.1.1.5 GBA security context (NAF Derivation Mode)

USIM operations in GBA security context are supported if service n°68 is "available".

The USIM receives the NAF_ID and IMPI.

The USIM performs Ks_ext_NAF and Ks_int_NAF derivation as defined in TS 33.220 [42] using the key material from the previous GBA_U bootstrapping procedure.

If no key material is available this is considered as a GBA Bootstrapping failure and the USIM abandons the function. The status word '6985' (Conditions of use not satisfied) is returned.

Otherwise, the USIM stores Ks_int_NAF and associated B-TID together with NAF_ID. The Ks_int_NAF keys related to other NAF_IDs, which are already stored in the USIM, shall not be affected. The USIM updates EF_GBANL as follows:

- If a record with the given NAF_ID already exists, the USIM updates the B-TID field of this record with the B-TID value associated to the GBA_U bootstrapped key involved in this GBA_U NAF derivation procedure.
- If a record with the given NAF_ID does not exist, the USIM uses an empty record to store the NAF_ID and the B-TID value associated to the GBA_U bootstrapped key involved in this GBA_U NAF Derivation procedure.
NOTE: According to TS 33.220 [42], the USIM can contain several Ks_int_NAF together with the associated B-TID and NAF_ID, but there is at most one pair of Ks_int_NAF and associated B-TID stored per NAF_ID.

Then, the USIM returns Ks_ext_NAF.

Input:

- NAF_ID, IMPI

Output:

- Ks_ext_NAF

7.1.1.6 MBMS security context (MSK Update Mode)

The USIM receives the MIKEY packet containing an MSK update message. First, the USIM uses the MUK ID to identify the Ks_int_NAF corresponding with a previous bootstrapping procedure.

The USIM shall check if a new NAF derivation procedure involving the received NAF_ID in the MIKEY message has been performed. In such a case, the USIM shall store the last bootstrapped Ks_int_NAF as the current MUK and update EF_MUK as follows:

- If a record with the received NAF_ID (included in the MUK ID: see TS 33.246 [43]) value is already present, then the MUK ID is stored in the corresponding field of this record, and the associated Time Stamp Counter (TS) field is reset. Additionally, the USIM internally stores the last used MUK (i.e. MUK that was used during the last successful MSK update procedure), along with its MUK ID for further use (e.g. to detect Key freshness failure).
- If a record with the received NAF_ID does not exist, the USIM uses an empty record to include the MUK ID, and reset the associated TS field.

If the received MUK ID does not correspond to the current MUK (i.e. last bootstrapped MUK) then the USIM proceeds as follows:

- If the received MUK ID corresponds to the last used MUK and if the received MIKEY message corresponds to a push solicited pull procedure then the USIM uses this MUK to verify the integrity of the message. If the verification is unsuccessful, the USIM abandons the function and returns the status word '9862' (Authentication error, incorrect MAC). If the verification is successful, the USIM abandons the function and returns the status word '9865' (the BM-SC shall be notified to retrieve the latest Ks_int_NAF: see TS 33.246 [43]).
- Otherwise, this is considered as a bootstrapping failure (incorrect MUK) and the USIM abandons the function. The status word '6A88' (Referenced data not found) is returned.

Otherwise, if the received MUK ID corresponds to the current MUK, the USIM uses the MUK value for MSK validation and derivation functions as described in TS 33.246 [43]. If the validation is unsuccessful, the status word '9862' (Authentication error, incorrect MAC) is returned and the USIM abandons the function.

After a successful MSK Update procedure the USIM stores the received MSK and updates EF_{MSK} as follows:

- If a record with the received Key Domain ID and Key Group part (i.e. Key Group part of the MSK ID) already exists, the 2nd MSK ID and the associated TS shall be replaced by the 1st MSK ID and the associated TS. Then the new MSK ID is stored as the 1st MSK ID and the associated TS is reset.
- If a record with the received Key Domain ID and Key Group part does not exist, the USIM uses an empty record to include those values. The received MSK ID is stored as the 1st MSK ID and the associated TS is reset. The 2nd MSK ID and the associated TS are set to 'FF FF'.

NOTE: The policy of replacing Key Domain records when no more empty records are available in EF_{MSK} is HE specific. (e.g. delete Groups from visited Key Domains first)

Then, the USIM stores the Time Stamp field (retrieved from the MIKEY message) in its corresponding field under EF_{MUK}.

The USIM stores internally the last used MUK along with its MUK ID for further use. This MUK may be used beyond its GBA validity (i.e. after the derivation of a new Ks_{int_NAF} resulting from a new bootstrap procedure) to verify the integrity of the first MIKEY message in order to detect a synchronization failure of a push solicited pull procedure. This may occur if the last derived Ks_{int_NAF} did not reach the BM-SC.

NOTE: The MSK is not necessarily updated in the message, since a MSK transport message can be sent e.g. to update the Key Validity data.

Input:

- MIKEY message

Output:

- None

7.1.1.7 MBMS security context (MSK Verification Mode)

USIM operations in MBMS security context are supported if service n°69 is "available".

The USIM receives the NAF_ID and MIKEY packet containing an MIKEY verification message, with an empty MAC field.

First, the USIM tests if the given MUK ID corresponds to a stored MUK ID in EF_{MUK} and if the Time Stamp field in the given MIKEY message corresponds with the stored Time Stamp Counter (TS) in EF_{MUK}.

If any of these verifications fails, this is considered as a Verification failure and the USIM abandons the function. The status word '6985' (Conditions of use not satisfied) is returned.

Otherwise, the USIM computes the MAC value as defined in TS 33.246 [43] and sends back the complete MIKEY verification message.

Input:

- NAF_ID, MIKEY message

Output:

- MIKEY message

7.1.1.8 MBMS security context (MTK Generation Mode)

USIM operations in MBMS security context are supported if service n°69 is "available".

The USIM receives the MIKEY message containing an MBMS MTK and a Salt key (if Salt key is available). First, the USIM retrieves the MSK with the Key Domain ID and the MSK ID given by the Extension payload of the MIKEY message (as described in TS 33.246 [43]).

If the needed MSK does not exist, this is considered as a MSK failure and the USIM abandons the function. The status word '6A88' (Referenced data not found) is returned.

Otherwise, the USIM performs the MBMS Generation and Validation Function (MGV-F) as described in TS 33.246 [43] using MSK.

If the USIM detects that the given MTK ID is invalid, this is considered as a SEQp freshness failure and the USIM abandons the function. The status word '9865' (Key freshness failure) is returned.

If the integrity validation of the MIKEY message is unsuccessful, the USIM abandons the function and returns the status word '9862' (Authentication error, incorrect MAC).

After successful MGV_F procedure the USIM stores the Time Stamp field (retrieved from the MIKEY message) as the Time Stamp Counter (TS) associated with the involved MSK under EF_{MSK}.

The USIM also stores MTK ID (retrieved from the MIKEY message) as the SEQs associated with MSK.

Then, the USIM returns MTK and Salt key (if Salt key is available).

Input:

- MIKEY message

Output:

- MTK and Salt (if available)

7.1.2 Command parameters and data

Code	Value
CLA	As specified in TS 31.101
INS	'88'
P1	'00'
P2	See table below
Lc	See below
Data	See below
Le	'00', or maximum length of data expected in response

Parameter P2 specifies the authentication context as follows:

Coding of the reference control P2

Coding b8-b1	Meaning
'1-----'	Specific reference data (e.g. DF specific/application dependant key)
'----- X XX'	Authentication context: 000 GSM context 001 3G context 010 VGCS/VBS context 100 GBA context 101 MBMS context

All other codings are RFU.

Command parameters/data:

7.1.2.1 GSM/3G security context

Byte(s)	Description	Length
1	Length of RAND (L1)	1
2 to (L1+1)	RAND	L1
(L1+2)	Length of AUTN (L2) (see note)	1
(L1+3) to (L1+L2+2)	AUTN (see note)	L2
Note: Parameter present if and only if in 3G security context.		

The coding of AUTN is described in TS 33.102 [13]. The most significant bit of RAND is coded on bit 8 of byte 2. The most significant bit of AUTN is coded on bit 8 of byte (L1+3).

Response parameters/data, case 1, 3G security context, command successful:

Byte(s)	Description	Length
1	"Successful 3G authentication" tag = 'DB'	1
2	Length of RES (L3)	1
3 to (L3+2)	RES	L3
(L3+3)	Length of CK (L4)	1
(L3+4) to (L3+L4+3)	CK	L4
(L3+L4+4)	Length of IK (L5)	1
(L3+L4+5) to (L3+L4+L5+4)	IK	L5
(L3+L4+L5+5)	Length of K _C (= 8) (see note)	1
(L3+L4+L5+6) to (L3+L4+L5+13)	K _C (see note)	8
Note: Parameter present if and only if Service n°27 is "available".		

The most significant bit of RES is coded on bit 8 of byte 3. The most significant bit of CK is coded on bit 8 of byte (L3+4). The most significant bit of IK is coded on bit 8 of byte (L3+L4+5).

Response parameters/data, case 2, 3G security context, synchronisation failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

The coding of AUTS is described in TS 33.102 [13]. The most significant bit of AUTS is coded on bit 8 of byte 3.

Response parameters/data, case 3, GSM security context, command successful:

Byte(s)	Description	Length
1	Length of SRES (= 4)	1
2 to 5	SRES	4
6	Length of K _C (= 8)	1
7 to 14	K _C	8

The most significant bit of SRES is coded on bit 8 of byte 2. The most significant bit of K_C is coded on bit 8 of byte 7.

7.1.2.2 VGCS/VBS security context

Byte(s)	Description	Length
1	Length of VService_Id	1
2 to 5	VService_Id	4
6	Length of VK_Id	1
7	VK_Id	1
8	Length of VSTK RAND (L1)	1
9 to L1+8	VSTK RAND	L1

VService_Id is coded in the same way as the octets 2-5 in the Descriptive group or broadcast call reference information element as defined in TS 24.008 [9].

The coding of VK_Id is as follows:

Coding of VK_Id

Coding b8-b1	Meaning
'00000001'	Corresponds to the 1st group key
'00000010'	Corresponds to the 2nd group key

The coding of VSTK RAND is described in TS 43.020 [44].

Response parameters/data, VGCS/VBS security context, command successful:

Byte(s)	Description	Length
1	"Successful VGCS/VBS operation" tag = 'DB'	1
2	Length of VSTK (16)	1
3 to 18	VSTK	16

7.1.2.3 GBA security context (Bootstrapping Mode)

Byte(s)	Description	Length
1	"GBA Security Context Bootstrapping Mode" tag = 'DD'	1
2	Length of RAND (L1)	1
3 to (L1+2)	RAND	L1
(L1+3)	Length of AUTN (L2)	1
(L1+4) to (L1+L2+3)	AUTN	L2

Response parameters/data, GBA security context (Bootstrapping Mode), synchronisation failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

AUTS coded as for UMTS Security context.

Response parameters/data, GBA security context (Bootstrapping Mode), command successful:

Byte(s)	Description	Length
1	"Successful GBA operation" tag = 'DB'	1
2	Length of RES (L)	1
3 to (L+2)	RES	L

RES coded as for UMTS Security context.

7.1.2.4 GBA security context (NAF Derivation Mode)

Byte(s)	Description	Length
1	"GBA Security Context NAF Derivation Mode" tag = 'DE'	1
2	Length of NAF_ID (L1)	1
3 to (L1+2)	NAF_ID	L1
(L1+3)	Length of IMPI (L2)	1
(L1+4) to (L1+L2+3)	IMPI	L2

Response parameters/data, GBA security context (NAF Derivation Mode), command successful:

Byte(s)	Description	Length
1	"Successful GBA operation" tag = 'DB'	1
2	Length of Ks_ext_NAF (L)	1
3 to (L+2)	Ks_ext_NAF	L

Coding of Ks_ext_NAF as described in TS 33.220 [42].

7.1.2.5 MBMS security context (All Modes)

Byte(s)	Description	Length
1	MBMS Security Context Mode	1
2	Length of MIKEY message (L1)	1
3 to (L1+2)	MIKEY message	L1
(L1+3)	Length of NAF_ID (L2) (see note1)	1
(L1+4) to (L1+L2+3)	NAF_ID (see note1)	L2

NOTE 1: Parameter present if and only if in MSK Verification Mode.

Parameter MBMS Security Context Mode specifies the MBMS mode in which MBMS security procedure is performed as follows:

Coding of MBMS Security Context Mode

Coding	Meaning
'01'	MSK Update Mode
'02'	MSK Verification Mode
'03'	MTK Generation Mode

Response parameters/data, MBMS security context (MSK Verification Mode), command successful:

Byte(s)	Description	Length
1	"Successful MBMS operation" tag = 'DB'	1
2	Length of MIKEY (L)	1
3 to (L+2)	MIKEY message	L

Response parameters/data, MBMS security context (MTK Generation Mode), command successful:

Byte(s)	Description	Length
1	"Successful MBMS operation" tag = 'DB'	1
2	Length of MTK and Salt (if Salt key is available) (L)	1
3 to (L+2)	MTK Salt (if available)	L

The coding of parameters is described in TS 33.246 [43].

7.2 Void

7.3 Status Conditions Returned by the USIM

Status of the card after processing of the command is coded in the status bytes SW1 and SW2. This clause specifies the coding of the status bytes in the following tables, in addition to the ones defined in TS 31.101 [11].

7.3.1 Security management

SW1	SW2	Error description
'98'	'62'	- Authentication error, incorrect MAC
'98'	'64'	- Authentication error, security context not supported
'98'	'65'	- Key freshness failure

7.3.2 Status Words of the Commands

The following table shows for each command the possible status conditions returned (marked by an asterisk *).

Commands and status words

Status Words	AUTHENTICATE
90 00	*
91 XX	*
93 00	
98 50	
98 62	*
98 64	*
98 65	*
62 00	*
62 81	
62 82	
62 83	
63 CX	
64 00	*
65 00	*
65 81	*
67 00	*
67 XX – (see note)	*
68 00	*
68 81	*
68 82	*
69 81	
69 82	*
69 83	
69 84	*
69 85	*
69 86	
6A 80	
6A 81	*
6A 82	
6A 83	
6A 86	*
6A 87	
6A 88	*
6B 00	*
6E 00	*
6F 00	*
6F XX – (see note)	*
NOTE: Except SW2 = '00'.	

7.4 Optional commands

The following command is optional for the USIM application:

- GET CHALLENGE command.

8 Void

Annex A (informative): EF changes via Data Download or USAT applications

This annex defines if changing the content of an EF by the network (e.g. by sending an SMS), or by a USAT Application, is advisable. Updating of certain EFs "over the air" such as EF_{ACC} could result in unpredictable behaviour of the UE; these are marked "Caution" in the table below. Certain EFs are marked "No"; under no circumstances should "over the air" changes of these EFs be considered.

File identification	Description	Change advised
'2F00'	Application directory	Caution
'2F05'	Preferred languages	Yes
'2F06'	Access rule reference	Caution
'2FE2'	ICC identification	No
'4F20'	Image data	Yes
'4F20'	GSM Ciphering key Kc	No
'4FXX'	Image Instance data Files	Yes
'4FXX'	Unique identifier	Yes
'4F22'	Phone book synchronisation counter	Yes
'4F23'	Change counter	Yes
'4F24'	Previous unique identifier	Yes
'4F30'	Phone book reference file	Yes
'4FXX'	Capability configuration parameters 1	Yes
'4F30'	SoLSA Access Indicator	Caution
'4F31'	SoLSA LSA List	Caution
'4FXX'	LSA Descriptor files	Caution
'4F52'	GPRS Ciphering key KcGPRS	No
'4F63'	CPBCCCH Information	No
'4F64'	Investigation Scan	Caution
'4FXX'	Additional number alpha string	Yes
'4FXX'	Additional number	Yes
'4FXX'	Second name entry	Yes
'4FXX'	Grouping information alpha string	Yes
'4FXX'	Phone book control	Yes
'4FXX'	E-mail addresses	Yes
'4FXX'	Index administration phone book	Yes
'4FXX'	Extension 1	Yes
'4FXX'	Abbreviated dialling numbers	Yes
'4FXX'	Grouping file	Yes
'4F41'	Pseudonym	Caution
'4F42'	User controlled PLMN selector for WLAN	No
'4F43'	Operator controlled PLMN selector for WLAN	Caution
'4F44'	User controlled WSID List	No
'4F45'	Operator controlled WSID List	Caution
'4F46'	WLAN Reauthentication Identity	No
'4F47'	Multimedia Messages List	Yes
'4F48'	Multimedia Messages Data File	Yes
'6F05'	Language indication	Yes
'6F06'	Access rule reference (under ADF _{USIM} and DF _{TELECOM})	Caution
'6F07'	IMSI	Caution (Note 1)
'6F08'	Ciphering and integrity keys	No
'6F09'	Ciphering and integrity keys for packet switched domain	No
'6F2C'	De-personalization Control Keys	Caution
'6F31'	Higher Priority PLMN search period	Caution
'6F32'	Co-operative network list	Caution
'6F37'	ACM maximum value	Yes
'6F38'	USIM service table	Caution
'6F39'	Accumulated call meter	Yes
'6F3B'	Fixed dialling numbers	Yes
'6F3C'	Short messages	Yes
'6F3E'	Group identifier level 1	Yes

File identification	Description	Change advised
'6F3F'	Group identifier level 2	Yes
'6F40'	MSISDN storage	Yes
'6F41'	PUCT	Yes
'6F42'	SMS parameters	Yes
'6F43'	SMS status	Yes
'6F45'	CBMI	Caution
'6F46'	Service provider name	Yes
'6F47'	Short message status reports	Yes
'6F48'	CBMID	Yes
'6F49'	Service Dialling Numbers	Yes
'6F4B'	Extension 2	Yes
'6F4C'	Extension 3	Yes
'6F4D'	Barred dialling numbers	Yes
'6F4E'	Extension 5	Yes
'6F4F'	Capability configuration parameters 2	Yes
'6F50'	CBMIR	Yes
'6F54'	SetUp Menu Elements	Yes
'6F55'	Extension 4	Yes
'6F56'	Enabled services table	Caution
'6F57'	Access point name control list	Yes
'6F58'	Comparison method information	Yes
'6F5B'	Initialisation value for Hyperframe number	Caution
'6F5C'	Maximum value of START	Yes
'6F60'	User controlled PLMN selector with Access Technology	No
'6F61'	Operator controlled PLMN selector with Access Technology	Caution
'6F62'	HPLMN selector with Access Technology	Caution
'6F73'	Packet switched location information	Caution
'6F78'	Access control class	Caution
'6F7B'	Forbidden PLMNs	Caution
'6F7E'	Location information	No (Note 1)
'6F80'	Incoming call information	Yes
'6F81'	Outgoing call information	Yes
'6F82'	Incoming call timer	Yes
'6F83'	Outgoing call timer	Yes
'6FAD'	Administrative data	Caution
'6FB1'	Voice Group Call Service	Yes
'6FB2'	Voice Group Call Service Status	Yes
'6FB3'	Voice Broadcast Service	Yes
'6FB4'	Voice Broadcast Service Status	Yes
'6FB5'	Enhanced Multi Level Pre-emption and Priority	Yes
'6FB6'	Automatic Answer for eMLPP Service	Yes
'6FB7'	Emergency Call Codes	Caution
'6FC3'	Key for hidden phone book entries	No
'6FC4'	Network Parameters	No
'6FC5'	PLMN Network Name	Yes
'6FC6'	Operator Network List	Yes
'6FC7'	Mailbox Dialling Numbers	Yes
'6FC8'	Extension 6	Yes
'6FC9'	Mailbox Identifier	Caution
'6FCA'	Message Waiting Indication Status	Caution
'6FCB'	Call Forwarding Indication Status	Caution
'6FCC'	Extension 7	Yes
'6FCD'	Service Provider Display Information	Yes
'6FCE'	MMS Notification	Yes
'6FCF'	Extension 8	Yes
'6FD0'	MMS Issuer Connectivity Parameters	Yes
'6FD1'	MMS User Preferences	Yes
'6FD2'	MMS User Connectivity Parameters	Yes
'6FD3'	Network's indication of alerting (NIA)	Caution
'6FD4'	Voice Group Call Service Ciphering Algorithm	Yes
'6FD5'	Voice Broadcast Service Ciphering Algorithm	Yes
'6FD6'	GBA Bootstrapping parameters	Caution

File identification	Description	Change advised
'6FD7'	MBMS Service Keys List	Caution
'6FD8'	MBMS User Key	Caution
'6FD9'	EHPLMN	Caution
'6FDA'	GBA NAF List	Caution
NOTE1: If EF _{IMSI} is changed, the UICC should issue REFRESH as defined in TS 31.111 and update EF _{LOC1} accordingly.		

Annex B (normative): Image Coding Schemes

The following image coding schemes are applicable to rectangular raster images. Raster image points are assumed to be of square shape. They are numbered sequentially from 1 onwards, starting at the upper left corner, proceeding line by line downwards, each line in turn proceeding from left to right, and ending at the image's lower right corner.

The following example illustrates the numbering scheme for raster image points by showing how the corner points are numbered, assuming an image length of x points and an image height of y points.



B.1 Basic Image Coding Scheme

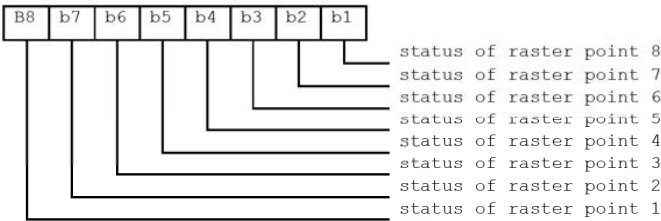
This coding scheme applies to rectangular raster images made up of raster points that are either set or not set. This coding scheme does not support any notion of colour. Image data are coded as follows:

Byte(s)	Description	Length
1	image width = X	1
2	image height = Y	1
3 to K+2	image body	K

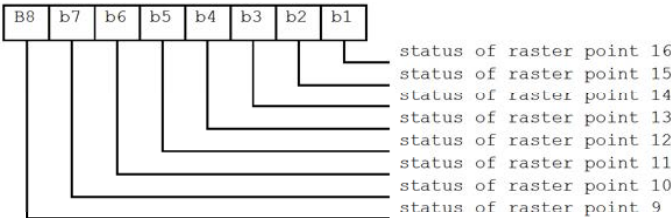
Coding of image body:

- The status of each raster image point is coded in one bit, to indicate whether the point is set (status = 1) or not set (status = 0).

Byte 1:



Byte 2:



etc.

Unused bits shall be set to 1.

B.2 Colour Image Coding Scheme

This coding scheme applies to coloured rectangular raster images. Raster image point colours are defined as references into a colour look-up table (CLUT), which contains a subset of the red-green-blue colour space. The CLUT in turn is located in the same transparent file as the image instance data themselves, at an offset defined within the image instance data.

Image data are coded as follows:

Byte(s)	Description	Length
1	Image width = X	1
2	Image height = Y	1
3	Bits per raster image point = B	1
4	Number of CLUT entries = C	1
5 to 6	Location of CLUT (Colour Look-up Table)	2
7 to K+6	Image body	K

Bits per raster image point:

Contents:

- the number B of bits used to encode references into the CLUT, thus defining a raster image point's colour. B shall have a value between 1 and 8.

Coding:

- binary.

Number of entries in CLUT:

Contents:

- the number C of entries in the CLUT which may be referenced from inside the image body. CLUT entries are numbered from 0 to C-1. C shall have a value between 1 and $2^{**}B$.

Coding:

- binary. The value 0 shall be interpreted as 256.

Location of CLUT:

Contents:

- this item specifies where the CLUT for this image instance may be found. The CLUT is always located in the same transparent file as the image instance data themselves, at an offset determined by these two bytes.

Coding:

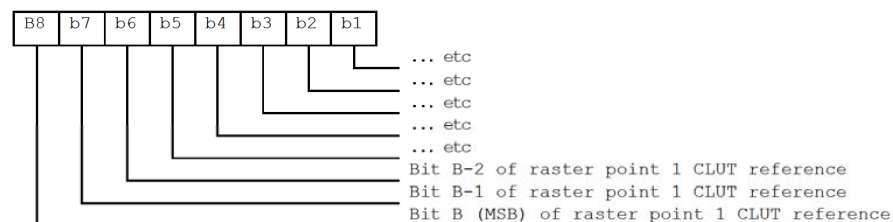
- Byte 1: high byte of offset into Image Instance File.
- Byte 2: low byte of offset into Image Instance File.

Image body:

Coding:

- each raster image point uses B bits to reference one of the C CLUT entries for this image instance. The CLUT entry being thus referenced yields the raster image point's colour. The image body is arrayed as for the Basic Colour Image Coding Scheme, that is, starting with the highest bit of the first raster image point's colour information.

Byte 1:



etc.

Unused bits shall be set to 1.

The CLUT (Colour Look-up Table) for an image instance with C colours is defined as follows:

Contents:

- C CLUT entries defining one colour each.

Coding:

- the C CLUT entries are arranged sequentially:

Byte(s) of CLUT	CLUT Entry
1-3	entry 0
...	...
$3*(C-1)+1$ to $3*C$	Entry C-1

Each CLUT entry in turn comprises 3 bytes defining one colour in the red-green-blue colour space:

Byte(s) of CLUT entry	Intensity of Colour
1	Red
2	Green
3	Blue

A value of 'FF' means maximum intensity, so the definition 'FF' '00' '00' stands for fully saturated red.

NOTE 1: Two or more image instances located in the same file can share a single CLUT.

NOTE 2: Most MEs capable of displaying colour images are likely to support at least a basic palette of red, green, blue and white.

B.3 Colour Image Coding Scheme with Transparency

This coding scheme is identical to the Colour Image Coding Scheme as defined in appendix B.2, with the following exception:

- Entry number C-1 in the colour look-up table (CLUT), where C is the number of entries in the CLUT, defines transparency. Raster image points which point to this entry are transparent, so that the underlying colour in the display is shown.

The three colour-coding bytes of entry number C-1 in the CLUT are of no importance when referenced from images using the '22' coding scheme.

NOTE: Two different descriptors in the EF_{IMG} file with Image Coding Scheme '21' and '22' may point to the same actual image instance. In that case, the descriptor with Image Coding Scheme '21' would describe an image where a raster image point pointing to entry number C-1 in the CLUT would have the colour described in that CLUT entry, while the descriptor with Image Coding Scheme '22' would describe an image where a raster image point pointing to entry number C-1 in the CLUT is transparent.

Annex C (informative): Structure of the Network parameters TLV objects

Structure of the GSM network parameter TLV object, $0 \leq m \leq 32$

Tag	Length	Tag Currently Camped Frequency	Length	BCCH Frequency downlink	Tag Neighbour BCCH Frequency	Length	BCCH Neighbour Frequency 1	BCCH Neighbour Frequency 2		BCCH Neighbour Frequency m
'A0'		'80'	'02'		'81'					

Structure of the FDD network parameter TLV object, $0 \leq m \leq 32$

Tag	Length	Tag Intra frequency carrier	Length	Intra Frequency downlink carrier	Primary Scrambling code 1	Primary Scrambling code m	Tag Inter frequency carrier	Length	Inter Frequency downlink carrier	Primary Scrambling code n1
'A1'		'80'					'81'			

Structure of the TDD network parameter TLV object, $0 \leq m \leq 32$

Tag	Length	Tag Intra frequency carrier	Length	Intra Frequency downlink carrier	Primary Scrambling code 1	Primary Scrambling code m	Tag Inter frequency carrier	Length	Inter Frequency downlink carrier	Primary Scrambling code n1
'A2'		'80'					'81'			

Annex D (informative): Tags defined in 31.102

Tag	Name of Data Element	Usage
'A0'	GSM cell information The following tags are encapsulated within 'A0': '80' GSM Camping Frequency data object '81' GSM Neighbour Frequency Information data object	Network Parameters (EF _{NETPAR})
'A1'	FDD cell information The following tags are encapsulated within 'A1': '80' FDD Intra Frequency data object '81' FDD Inter Frequency Information data object	Network Parameters (EF _{NETPAR})
'A2'	TDD cell information The following tags are encapsulated within 'A2': '80' TDD Intra Frequency data object '81' TDD Inter Frequency Information data object	Network Parameters (EF _{NETPAR})
'A3'	Service provider display information The following tags are encapsulated within 'A3': '80' Service provider PLMN list	Service Provider Display Information (EF _{SPDI})
'A8'	Indicator for type 1 EFs (amount of records equal to master EF) The following tags are encapsulated within 'A8': 'C0' EF _{ADN} data object 'C1' EF _{IAP} data object 'C3' EF _{SNE} data object 'C4' EF _{ANR} data object 'C5' EF _{PBC} data object 'C6' EF _{GRP} data object 'C9' EF _{UID} data object 'CA' EF _{EMAIL} data object	Phone Book Reference File (EF _{PBR})
'A9'	Indicator for type 2 EFs (EFs linked via the index administration file) The following tags are encapsulated within 'A9': 'C3' EF _{SNE} data object 'C4' EF _{ANR} data object 'CA' EF _{EMAIL} data object	Phone Book Reference File (EF _{PBR})
'AA'	Indicator for type 3 EFs (EFs addressed inside an object using a record identifier as a pointer) The following tags are encapsulated within 'AA': 'C2' EF _{EXT1} data object 'C7' EF _{AAS} data object 'C8' EF _{GAS} data object 'CB' EF _{CCP1} data object	Phone Book Reference File (EF _{PBR})
'AB'	MMS Connectivity Parameters: The following are encapsulated under 'AB': '80' MMS Implementation Tag '81' MMS Relay/Server Tag '82' Interface to core network and bearer Tag '83' Gateway Tag	MMS Connectivity Parameters (EF _{MMSICP} / EF _{MMSUCP})
'DB'	Successful 3G authentication	Response to AUTHENTICATE
'DC'	Synchronisation failure	Response to AUTHENTICATE
'DD'	Access Point Name	APN Control List (EF _{ACL})

NOTE: the value 'FF' is an invalid tag value. For ASN.1 tag assignment rules see ISO/IEC 8825 [35]

Annex E (informative): Suggested contents of the EFs at pre-personalization

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

File Identification	Description	Value
'2F00'	Application directory	Card issuer/operator dependant
'2F05'	Preferred languages	'FF...FF'
'2F06'	Access rule reference	Card issuer/operator dependant
'2FE2'	ICC identification	operator dependant
'4F20'	Image data	'00FF...FF'
'4F20'	GSM Ciphering key Kc	'FF...FF07'
'4FXX'	Image instance data files	'FF...FF'
'4FXX'	Unique identifier	'0000'
'4F22'	Phone book synchronisation counter	'00000000'
'4F23'	Change counter	'0000'
'4F24'	Previous unique identifier	'0000'
'4F30'	Phone book reference file	Operator dependant
'4F30'	SoLSA Access Indicator	'00FF...FF'
'4F31'	SoLSA LSA List	'FF...FF'
'4FXX'	LSA Descriptor files	'FF...FF'
'4FXX'	Capability configuration parameters 1	'FF...FF'
'4F52'	GPRS Ciphering key KcGPRS	'FF...FF07'
'4F63'	CPBCH Information	'FF...FF'
'4F64'	Investigation PLMN scan	'00'
'4FXX'	E-mail addresses	'FF...FF'
'4FXX'	Additional number alpha string	'FF...FF'
'4FXX'	Second name entry	'FF...FF'
'4FXX'	Abbreviated dialling numbers	'FF...FF'
'4FXX'	Grouping file	'00...00'
'4FXX'	Grouping information alpha string	'FF...FF'
'4FXX'	Phone book control	'0000'
'4FXX'	Index administration phone book	'FF...FF'
'4FXX'	Additional number	'FF...FF'
'4FXX'	Extension 1	'00FF...FF'
'4F41'	Pseudonym	'00FF...FF'
'4F42'	User Controlled PLMN selector for WLAN	'FF...FF'
'4F43'	Operator Controlled PLMN selector for WLAN	Operator dependant
'4F44'	User Controlled WSID list	'00FF...FF'
'4F45'	Operator controlled WSID list	Operator dependant
'4F46'	WLAN Reauthentication Identity	'FF...FF'
'4F47'	Multimedia Messages List	'FF...FF'
'4F48'	Multimedia Messages Data File	'FF...FF'
'6F05'	Language indication	'FF...FF'
'6F06'	Access rule reference (under ADF _{USIM} and DF _{TELECOM})	Card issuer/operator dependant
'6F07'	IMSI	Operator dependant
'6F08'	Ciphering and integrity keys	'07FF...FF'
'6F09'	Ciphering and integrity keys for packet switched domain	'07FF...FF'
'6F2C'	De-personalization control keys	'FF...FF'
'6F31'	Higher Priority PLMN search period	'FF'
'6F32'	Co-operative network list	'FF...FF'
'6F37'	ACM maximum value	'000000' (see note 1)
'6F38'	USIM service table	Operator dependant
'6F39'	Accumulated call meter	'000000'
'6F3B'	Fixed dialling numbers	'FF...FF'
'6F3C'	Short messages	'00FF...FF'
'6F3E'	Group identifier level 1	Operator dependant
'6F3F'	Group identifier level 2	Operator dependant
'6F40'	MSISDN storage	'FF...FF'
'6F41'	PUCT	'FFFFFF0000'
'6F42'	SMS parameters	'FF...FF'
'6F43'	SMS status	'FF...FF'
'6F45'	CBMI	'FF...FF'
'6F46'	Service provider name	Operator dependant
'6F47'	Short message status reports	'00FF...FF'
'6F48'	CBMID	'FF...FF'
'6F49'	Service Dialling Numbers	'FF...FF'

'6F4B'	Extension 2	'00FF...FF'
'6F4C'	Extension 3	'00FF...FF'
'6F4D'	Barred Dialling Numbers	'FF...FF'
'6F4E'	Extension 5	'00FF...FF'
'6F4F'	Capability configuration parameters 2	'FF...FF'
'6F50'	CBMIR	'FF...FF'
'6F54'	SetUp Menu Elements	Operator dependant
'6F55'	Extension 4	'00FF...FF'
'6F56'	Enabled services table	Operator dependant
'6F57'	Access point name control list	'00FF...FF'
'6F58'	Comparison method information	'FF...FF'
'6F5B'	Initialisation value for Hyperframe number	'F0 00 00 F0 00 00'
'6F5C'	Maximum value of START	Operator dependant
'6F60'	User controlled PLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F61'	Operator controlled PLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F62'	HPLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F73'	Packet switched location information	'FFFFFFFF FFFFFFFF xxxxxx 0000 FF 01' (see note 2)
'6F78'	Access control class	Operator dependant
'6F7B'	Forbidden PLMNs	'FF...FF'
'6F7E'	Location information	'FFFFFFFF xxxxxx 0000 FF 01' (see note 2)
'6F80'	Incoming call information	'FF...FF 000000 00 01FFFF'
'6F81'	Outgoing call information	'FF...FF 000000 01FFFF'
'6F82'	Incoming call timer	'000000'
'6F83'	Outgoing call timer	'000000'
'6FAD'	Administrative data	Operator dependant
'6FB1'	Voice Group Call Service	Operator dependant
'6FB2'	Voice Group Call Service Status	Operator dependant
'6FB3'	Voice Broadcast Service	Operator dependant
'6FB4'	Voice Broadcast Service Status	Operator dependant
'6FB5'	EMLPP	Operator dependant
'6FB6'	AaeM	'00'
'6FB7'	Emergency call codes	Operator dependant
'6FC3'	Key for hidden phone book entries	'FF...FF'
'6FC4'	Network Parameters	'FF...FF'
'6FC5'	PLMN Network Name	Operator dependant
'6FC6'	Operator Network List	Operator dependant
'6FC7'	Mailbox Dialling Numbers	Operator dependant
'6FC8'	Extension 6	'00 FF...FF'
'6FC9'	Mailbox Identifier	Operator dependant
'6FCA'	Message Waiting Indication Status	'00 00 00 00 00'
'6FCB'	Call Forwarding Indication Status	'xx 00 FF...FF'
'6FCC'	Extension 7	'00 FF...FF'
'6FCD'	Service Provider Display Information	
'6FCE'	MMS Notification	'00 00 00 FF...FF'
'6FCF'	Extension 8	'00FF...FF'
'6FD0'	MMS Issuer Connectivity Parameters	'FF...FF'
'6FD1'	MMS User Preferences	'FF...FF'
'6FD2'	MMS User Connectivity Parameters	'FF...FF'
'6FD3'	Network's Indication of Alerting (NIA)	'FF...FF'
'6FD4'	Voice Group Call Service Ciphering Algorithm	'00...00'
'6FD5'	Voice Broadcast Service Ciphering Algorithm	'00...00'
'6FD6'	GBA Bootstrapping parameters	'FF...FF'
'6FD7'	MBMS Service Keys List	'FF...FF'
'6FD8'	MBMS User Key	'FF...FF'
'6FD9'	EHPLMN	'FF...FF' or xxxxxx (see Note 2)
'6FDA'	GBA NAF List	'FF...FF'

NOTE 1: The value '000000' means that ACMmax is not valid, i.e. there is no restriction on the ACM. When assigning a value to ACMmax, care should be taken not to use values too close to the maximum possible value 'FFFFFF', because the INCREASE command does not update EF_{ACM} if the units to be added would exceed 'FFFFFF'. This could affect the call termination procedure of the Advice of Charge function.

NOTE 2: xxxxxx stands for any valid MCC and MNC, coded according to TS 24.008 [9].

Annex F (informative): Examples of coding of LSA Descriptor files for SoLSA

The length of all the records is determined by the LSA descriptor containing the largest number of bytes. Combinations containing different numbers of LSA IDs, LAC+ CI and CI or LAC can therefore be done. Various examples are show. Due to the OTA management of the records it is recommended that the record length is maximum 100 bytes in order to leave room for command descriptor and signature information in the SMS.

This first example contains two LSAs, one described by two LSA IDs and another described by three Cell IDs, giving a record length of 8 bytes.

1st record:

LSA descriptor type = LSA ID and number = 2 (1 byte)	LSA ID (3 bytes)	LSA ID (3 bytes)	Identifier (1 byte)
---	------------------	------------------	---------------------

2nd record:

LSA descriptor type = CI and number = 3 (1 byte)	CI (2 bytes)	CI (2 bytes)	CI (2 bytes)	Identifier (1 byte)
---	--------------	--------------	--------------	---------------------

The second example contains two LSAs, one described by one LSA ID and one described by two Cell Ids, giving a record length of 6 bytes.

1 st record:	LSA descriptor type = LSA ID and number = 1 (1 byte)	LSA ID (3 bytes)	'FF'	Identifier (1 byte)
2 nd record:	LSA descriptor type = CI and number = 2 (1 byte)	CI (2 bytes)	CI (2 bytes)	Identifier (1 byte)

Annex G (informative): Phonebook Example

This example phonebook has more than 254 entries. Additional number (3 additional numbers) information, second name and e-mail information can be added to each ADN entry. In addition each entry has a 2 byte Unique ID (UID) attached to it. The phonebook also contains three files that are shared EF_{EXT1}, EF_{AAS} and EF_{GAS}. These files are addressed from inside a file. EF_{EXT1} is addressed via EF_{ADN}, EF_{ADN1}, EF_{AAS} is addressed via EF_{ANRA}, EF_{ANRA1}, EF_{ANRB}, EF_{ANRB1}, EF_{ANRC}, EF_{ANRC1} and EF_{GAS} is addressed via EF_{GRP}, EF_{GRP1}. The phonebook supports two levels of grouping and hidden entries in EF_{PBC}.

Two records are needed in the phonebook reference file PBR '4F30' for supporting more than 254 entries. The content of the phonebook reference file PBR '4F30' records is as shown in table G.2. The structure of the DF_{PHONEBOOK} is shown in table G.1.

The content of phonebook entries in the range from 1-508 is described in the tables G.3 and G.4.

Table G.1: Structure of EFs inside DF_{PHONEBOOK}

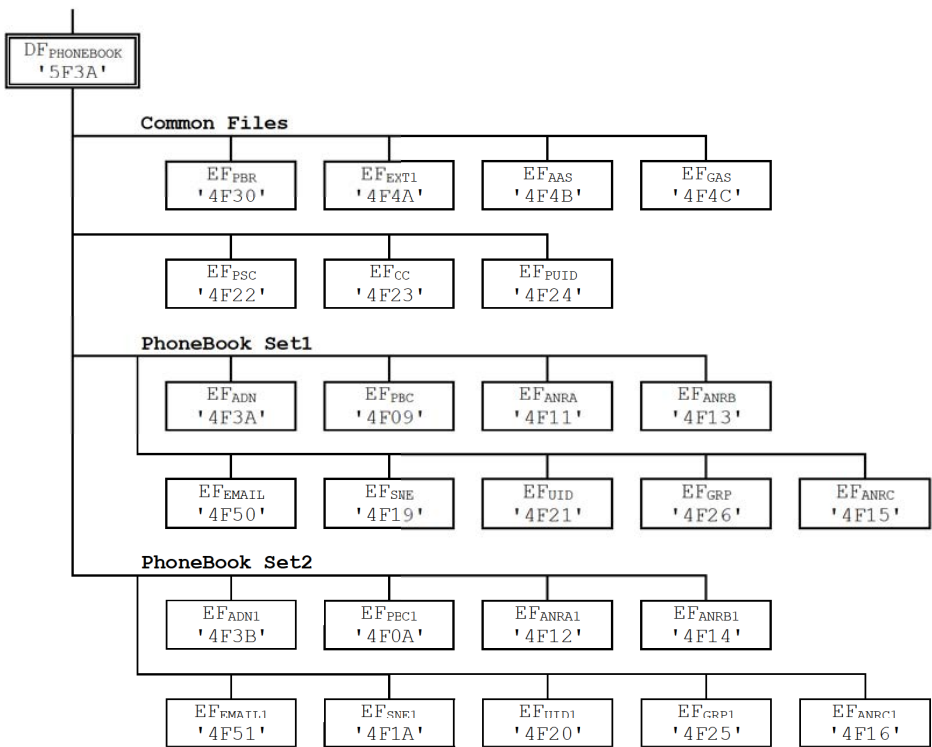


Table G.2: Contents of EF_{PBR}**Rec 1** Tag'A8' L='2D' (for Phonebook Set1)

Tag'C0'	L='03'	'4F3A'	'01'	Tag'C5'	L='03'	'4F09'	'02'	Tag'C6'	L='03'	'4F26'	'03'
Tag'C4'	L='03'	'4F11'	'04'	Tag'C4'	L='03'	'4F13'	'05'	Tag'C4'	L='03'	'4F15'	'06'
Tag'C3'	L='03'	'4F19'	'07'	Tag'C9'	L='03'	'4F21'	'12'	Tag'CA'	L='03'	'4F50'	'09'
Tag'AA'	L='0F'										
Tag'C2'	L='03'	'4F4A'	'08'	Tag'C7'	L='03'	'4F4B'	'14'	Tag'C8'	L='03'	'4F4C'	'15'

Rec 2 Tag'A8' L='2D' (for Phonebook Set 2)

Tag'C0'	L='03'	'4F3B'	'0A'	Tag'C5'	L='03'	'4F0A'	'0B'	Tag'C6'	L='03'	'4F25'	'0C'
Tag'C4'	L='03'	'4F12'	'0D'	Tag'C4'	L='03'	'4F14'	'0E'	Tag'C4'	L='03'	'4F16'	'0F'
Tag'C3'	L='03'	'4F1A'	'10'	Tag'C9'	L='03'	'4F20'	'13'	Tag'CA'	L='03'	'4F51'	'11'
Tag'AA'	L='0F'										
Tag'C2'	L='03'	'4F4A'	'08'	Tag'C7'	L='03'	'4F4B'	'14'	Tag'C8'	L='03'	'4F4C'	'15'

Table G.3: Structure of the 254 first entries in the phonebook

Phone book entry	ADN '4F3A' SFI '01'		PBC '4F09' SFI '02'	GRP '4F26' SFI '03'	ANRA '4F11' SFI '04'	ANRB '4F13' SFI '05'	ANRC '4F15' SFI '06'	SNE '4F19' SFI '07'	UID '4F21' SFI '12'	EXT1 '4F4A' SFI '08'	AAS '4F4B' SFI '14'	GAS '4F4C' SFI '15'	EMAIL '4F50' SFI '09'
# 1	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '02'	Hidden (AID rec N° 3)	Rec n°1 Rec n°3 '00'	ANRA Rec n°1	ANRB Rec n°1	ANRC Rec n°1	Second Name Alpha String	UID	Rec '02'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP	email address
# 2	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '2A'	Not Hidden	Rec n°2 Rec n°1 Rec n°3	ANRA Rec n°2	ANRB Rec n°2	ANRC Rec n°2	Second Name Alpha String	UID	Rec '2A'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP	email address
# 3													
:													
:													
:													
# 254													

Table G.4: Structure of phone book entries 255 to 508 (Rec 1-254)

Phone book entry	ADN1 '4F3B' SFI '0A'		PBC1 '4F0A' SFI '0B'	GRP1 '4F25' SFI '0C'	ANRA1 '4F12' SFI '0D'	ANRB1 '4F14' SFI '0E'	ANRC1 '4F16' SFI '0F'	SNE1 '4F1A' SFI '10'	UID1 '4F20' SFI '13'	EXT1 '4F4A' SFI '08'	AAS '4F4B' SFI '14'	GAS '4F4C' SFI '15'	EMAIL1 '4F51' SFI '11'
#255	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '03'	Hidden (AID Rec n° 3)	Rec n°1 Rec n°3 '00'	ANRA1 Rec n°1	ANRB1 Rec n°1	ANRC1 Rec n°1	Second Name Alpha String	UID	Rec '03'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP1	email address
#256	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '2B'	Not Hidden	Rec n°2 Rec n°1 Rec n°3	ANRA1 Rec n°2	ANRB1 Rec n°2	ANRC1 Rec n°2	Second Name Alpha String	UID	Rec '2B'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP1	email address
#257													
:													
:													
:													
#508													

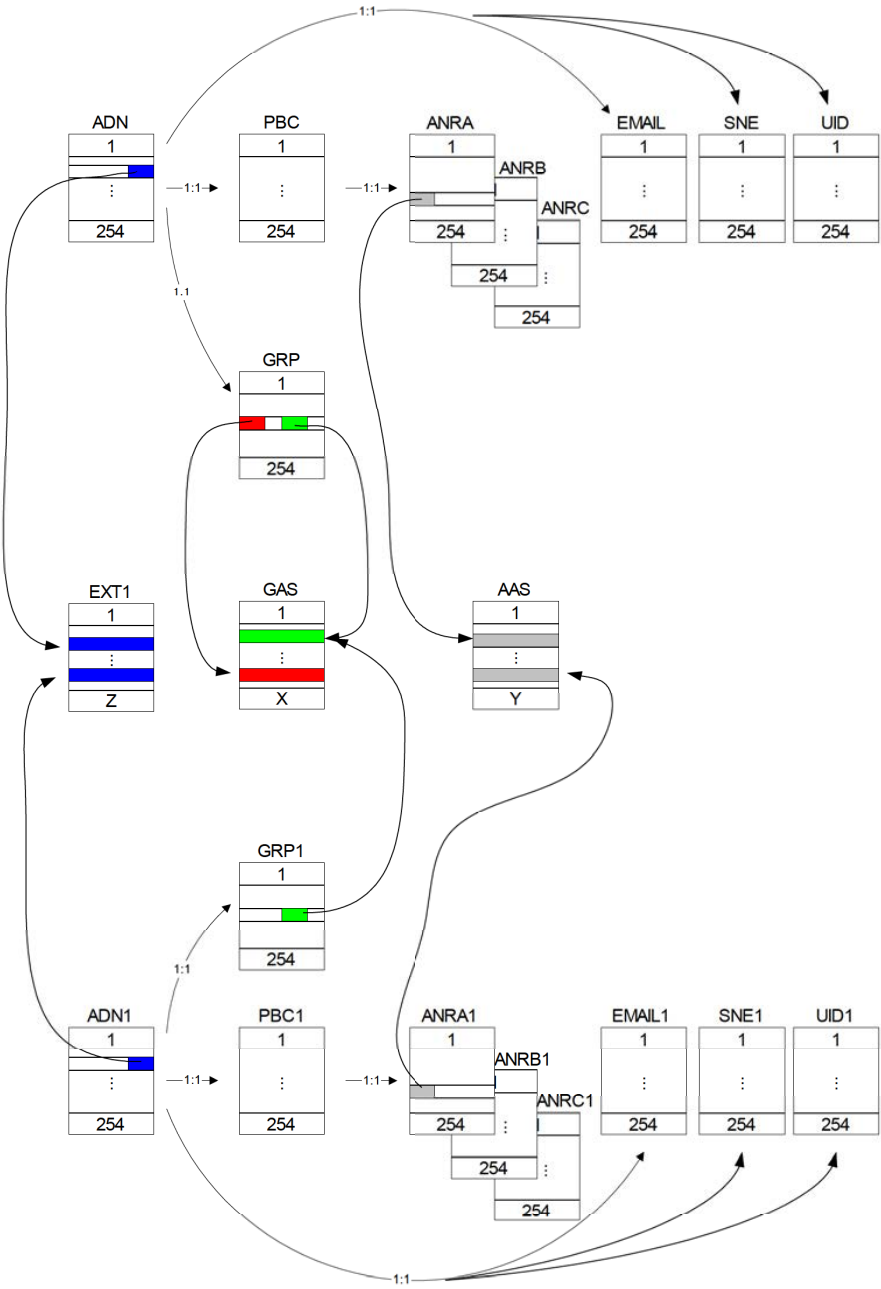


Figure G.1: Structure and Relations of the Example Phone Book

Annex H (normative): List of SFI Values

This annex lists SFI values assigned in the present document.

H.1 List of SFI Values at the USIM ADF Level

File Identification	SFI	Description
'6FB7'	'01'	Emergency call codes
'6F05'	'02'	Language indication
'6FAD'	'03'	Administrative data
'6F38'	'04'	USIM service table
'6F56'	'05'	Enabled services table
'6F78'	'06'	Access control class
'6F07'	'07'	IMSI
'6F08'	'08'	Ciphering and integrity keys
'6F09'	'09'	Ciphering and integrity keys for packet switched domain
'6F60'	'0A'	User PLMN selector
'6F7E'	'0B'	Location information
'6F73'	'0C'	Packet switched location information
'6F7B'	'0D'	Forbidden PLMNs
'6F48'	'0E'	CBMID
'6F5B'	'0F'	Hyperframe number
'6F5C'	'10'	Maximum value of hyperframe number
'6F61'	'11'	Operator PLMN selector
'6F31'	'12'	Higher Priority PLMN search period
'6F62'	'13'	Preferred HPLMN access technology
'6F80'	'14'	Incoming call information
'6F81'	'15'	Outgoing call information
'6F4F'	'16'	Capability configuration parameters 2
'6F06'	'17'	Access Rule Reference
'6FC5'	'19'	PLMN Network Name
'6FC6'	'1A'	Operator Network List
'6FCD'	'1B'	Service Provider Display Information
'6F39'	'1C'	Accumulated Call Meter (see note)
NOTE: When used the value '1C' shall be used as SFI for EF _{ACM} , for compatibility reasons the terminal shall accept other values.		

All other SFI values are reserved for future use.

H.2 List of SFI Values at the DF GSM-ACCESS Level

File Identification	SFI	Description
'4F20'	'01'	GSM Ciphering Key Kc
'4F52'	'02'	GPRS Ciphering Key KcGPRS

All other SFI values are reserved for future use.

H.3 List of SFI Values at the DF WLAN Level

File Identification	SFI	Description
'4F41'	'01'	Pseudonym
'4F42'	'02'	User controlled PLMN for WLAN
'4F43'	'03'	Operator controlled PLMN for WLAN
'4F44'	'04'	User controlled WSID list
'4F45'	'05'	Operator controlled WSID list
'4F46'	'06'	WLAN Reauthentication Identity

All other SFI values are reserved for future use.

Annex I (informative): USIM Application Session Activation/Termination

The purpose of this annex is to illustrate the different Application Session procedures.

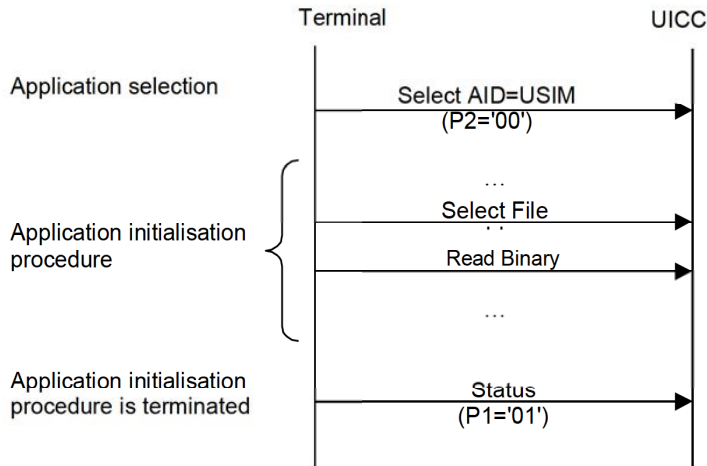


Figure I.1 USIM Application Session Activation procedure

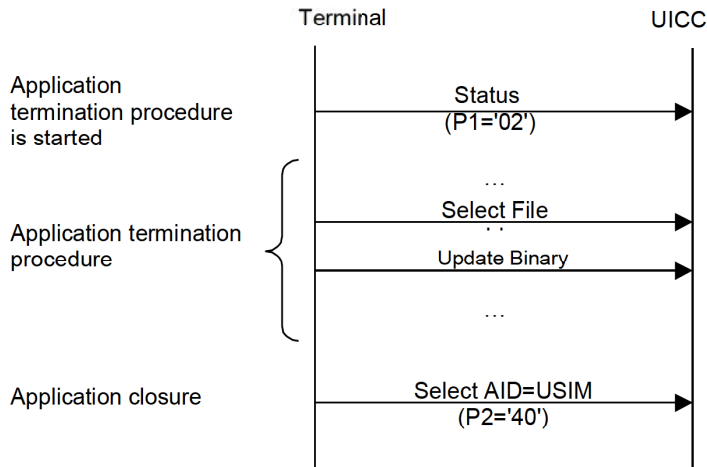


Figure I.2 USIM Application Session Termination procedure

Annex J (informative): Example of MMS coding

This annex gives an example for the coding of MMS User Preferences, while the MMS User Information Preference parameters are coded according to the WAP implementation of MMS.

J.1 Coding example for MMS User Preferences

0x80 MMS Implementation Tag

0x01 (Length = "1")

0x01 (MMS implementation information = "(WAP")

0x81 MMS User Preference Profile Name Tag

0x0E (Length = "14")

43 68 72 69 73 74 6D 61 73 20 43 61 72 64

(profile name = "Christmas Card"; 14 characters, 14 Bytes)

0x82 MMS User Information Preference Information Tag

0x19 (Length = "25")

0x14 0x80 (visibility: = "hide"; 2 Bytes)

0x06 0x80 (delivery report: = "yes"; 2 Bytes)

0x10 0x80 (read-reply: = "yes"; 2 Bytes)

0x0F 0x81 (priority: = "normal"; 2 Bytes)

0x07 0x07 0x80 0x05 0x11 0x22 0x33 0x44 0x55
(Delivery-Time-Tag, Value-Length, Absolute-Token-Tag, Date-Value-Length, Date-Value; 9 Bytes)

0x08 0x06 0x81 0x04 0x55 0x22 0x33 0x44
(Expiry Tag, Value-Length, Relative-Token-Tag, Delta-Second-Value-Length, Delta-Second-Value; 8 Bytes)

J.2 Coding Example for MMS Issuer/User Connectivity Parameters

0xAB MMS Connectivity Parameters Tag

0x81 0x88 (Length = "136") (Length bytes greater than 127 are coded onto 2 bytes according to ISO/IEC 8825 [35])

0x80 MMS Implementation Tag

0x01 (Length = "1")

0x01 (MMS implementation information = "WAP"; 1 Byte)

0x81 MMS Relay/Server Tag

0x17 (Length = "23")

0x68 0x74 0x70 0x3A 0x2F 0x2F 0x6D 0x6D 0x73 0x2D 0x6F 0x70 0x65 0x72 0x61 0x74
 0x6F 0x72 0x2E 0x63 0x6F 0x6D
 (MMS Relay/Server information = "http://mms-operator.com"; 23 characters; 23 Bytes)

0x82 Interface to Core Network and Bearer Tag

0x32 (Length = "50")

0x10 0xAA (bearer = "GSM-CSD"; 2 Bytes)

0x08 0x2B 0x34 0x39 0x35 0x33 0x34 0x31 0x39 0x30 0x36 0x00
 (address = "+495341906"; 12 Bytes)

0x09 0x87 (type of address = "E164"; 2 Bytes)

0x25 0xC5 (speed = "autobauding"; 2 Bytes)

0x0A 0x90 (call type = "ANALOG_MODEM"; 2 Bytes)

0x9A (authentication type = "PAP"; 2 Bytes)

0x0D 0x64 0x75 0x6D 0x6D 0x79 0x5F 0x6E 0x61 0x6D 0x65 0x00
 (authentication id = "dummy_name"; 12 Bytes)

0x0E 0x64 0x75 0x6D 0x6D 0x79 0x5F 0x70 0x61 0x73 0x73 0x77 0x6F 0x72 0x64 0x00
 (authentication pw = "dummy_password"; 16 Bytes)

0x83 Gateway Tag

0x36 (Length = "54")

0x20 0x31 0x37 0x30 0x2E 0x31 0x38 0x37 0x2E 0x35 0x31 0x2E 0x33 0x00
 (address = "170.187.51.3"; 14 Bytes)

0x21 0x85 (type of address = "IPv4"; 2 Bytes)

0x23 0x39 0x32 0x30 0x33 0x00 (port = "9203"; 6 Bytes)

0x24 0xCB (service = "CO-WSP"; 2 Bytes)

0x19 0x9C (authentication type = "HTTP BASIC"; 2 Bytes)

0x1A 0x64 0x75 0x6D 0x6D 0x79 0x5F 0x6E 0x61 0x6D 0x65 0x00
 (authentication id = "dummy_name"; 12 Bytes)

0x1B 0x64 0x75 0x6D 0x6D 0x79 0x5F 0x70 0x61 0x73 0x73 0x77 0x6F 0x72 0x64 0x00
 (authentication pw = "dummy_password"; 16 Bytes)

Annex K (informative): Change history

The table below indicates all CRs that have been incorporated into the present document since it was initially approved.

TSG # / Date	TSG Doc.	WG doc	CR	Rev	Cat	Subject/Comment	New
TP-27						Creation of Rel-7 version based on v6.9.0	7.0.0
TP-27	TP-050018	T3-050189	264	1	F	Correction to overcome IMSI number space limitation – inclusion of EHPLMN	7.0.0