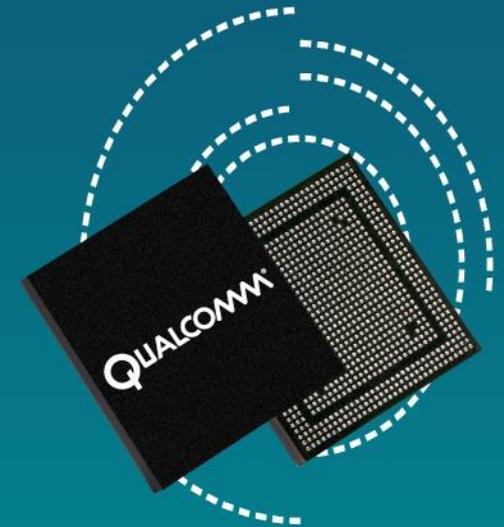




Discussion on UICC Access Optimization

C6-140620



Confidential and Proprietary – Qualcomm Technologies, Inc.

Restricted Distribution: Not to be distributed to anyone who is not an employee of either Qualcomm or its subsidiaries without the express approval of Qualcomm's Configuration Management.

Agenda

- Goal of this presentation is to discuss the proposal from ETSI SCP TEC in SCPTEC(14)000225r1 to provide appropriate response
- Agenda
 - Overview of EFs that would benefit from the proposed change
 - Analysis of EFs that are not PIN protected
 - Analysis of EFs that are PIN protected
 - Conclusions
 - Possible improvements

Which EFs would benefit

There are 3 classes of files that would benefit from the change

- Record-based EFs
 - In case of record based EFs, the terminal needs to perform a SELECT to retrieve the number of records and the record length, and then accesses each record separately.
 - EFs can have up to 255 records: in practice this is valid only for some specific EFs, but it's quite common to see files with 10 or more records.
 - Total number of APDUs: 1 for SELECT + number of records for READ RECORD

- Large binary files
 - Each READ BINARY command can be used to read up to 255 bytes
 - If the EF size exceeds that number, EF needs to be read in chunks with multiple separate READ BINARY commands
 - Initial SELECT needs to be done to retrieve the actual file size
 - Total number of APDUs: 1 for SELECT + ((file size / 255) + 1) for READ BINARY

- Small binary files
 - EFs with a variable length: in order to pass the correct Le value in the READ BINARY command, a SELECT needs to be done
 - EFs with fixed length, but without SFI: in order to read the file, a SELECT needs to be done first
 - In both cases, each file requires 2 APDUs

EFs that are not PIN protected – Emergency related

The following EFs are present on the USIM and are not PIN protected, but are needed for emergency services. For this reason, fast access to them is desirable.

- EF-ECC (Emergency Call Codes)
 - Record based file. It is read at the beginning of USIM initialization.
 - Generally, at least 4 records are present, but some markets have more.

- EF-PWS (Public Warning System)
 - Binary file of variable length and without SFI

- EF-ICE_DN (In Case of Emergency – Dialling Number)
 - Record based EF with dialing numbers in case of emergency

- EF-ICE_FF (In Case of Emergency – Dialling Number)
 - Record based EF with dialing numbers in case of emergency

- EF-ICE_graphics (In Case of Emergency – Graphics)
 - Record based EF with graphics for dialing numbers in case of emergency

EFs that are not PIN protected – Operator name

The following files are present on the USIM and are not PIN protected, but are needed to display correct name to the user. Fast access is required otherwise a wrong information to the user is given until they are read correctly

- EF-SPN (Service Provide Name)
 - This EF is transparent with fixed length of 17 bytes, but does not have any associated SFI

- EF-SPNI (Service Provide Name)
 - This EF is transparent with variable length and does not have any associated SFI

- EF-OPL (Operator PLMN List)
 - 31.102 contains the following text: “Care should be taken not to introduce too many PLMN entries. An excessive number of entries could result in a longer initialisation period.”
 - Cases with large number of records are frequently seen in the field

- EF-PNN (PLMN Network Name)
 - This EF is record based. The number of records normally depends on the content of EF-OPL (see above)

- EF-PNNI (PLMN Network Name Icon)
 - This EF is record based. The number of records normally depends on the size of EF-PNN

EFs that are not PIN protected – Others

- EF-DIR
 - UICC with at least 4 entries are very common in the market, but often have more than 4 records
- EF-LI (Language Indication)
 - Binary file of variable length, needs to be read before completing USIM initialization
- EF-AD (Administrative)
 - Binary file of variable length (4+X)
- EF-UFC (USAT Facility Control)
 - Binary file of variable length and without SFI
- EF-LAUNCH_SCWS (Launchpad for Smart Card Web Server)
 - Binary file of variable length, for terminals with Smart Card Web Server support

EF-ICON (Icon for launchpad for Smart Card Web Server)

- Binary file of variable length, contains the icon for the Smart Card Web Server launchpad

EF-ARR

- In general, terminal only reads required records in the EF-ARR, but anyway these are often a lot
- Different ARR file is present at each level of the UICC on a normal UICC card

EFs that are PIN protected – Controlled by operator

A lot of EFs on the UICC are PIN1 protected, even if the content of those files is not sensitive or confidential. For the most part, these files have the same value on all UICC cards (or at least for specific subsets) of a given operator.

For this reason, protection of those EFs with PIN1 is not strongly required, even if used in specifications: a user could read the from any other UICC of the same operator.

A few examples:

- EF-OPLMNwAct (Operator controlled PLMN selector with Access Technology)
 - There are commercial deployments where this EF is extremely large.
 - For example, an Asian operator has a EF of 3500 bytes
- EF-HPLMNwAcT (HPLMN selector with Access Technology)
 - HPLMN code, or codes together with the respected access technology in priority order
 - Binary file of variable length
- EF-UST (USIM Service Table)
 - Contains list of services provided by the UICC, but not actual values. Has variable size
- EF-OCSGL (Operator CSG Lists)
 - There are deployments with several records, even if not all are already used.
 - Corresponding EF-OCSGT and EF-OHNBN are also present on the USIM
- EF-MMSICP (MMS Issuer Connectivity Parameters)
 - Binary file with parameters for MMS connection

EFs that are PIN protected – Controlled by terminal

Several EFs are PIN1 protected, but are controlled by the terminal and mostly used to guarantee consistent behavior when UICC is moved to a new terminal, so that information is carried to the new terminal.

A few examples:

- EF-EPSLOCI (EPS location information), EF-EPSNSC (EPS NAS Security Context)
 - These files were introduced in Rel.8, but terminal can still use LTE with UICC with previous releases, storing the content in the internal memory
- EF-SMSP (Short message service parameters)
 - Record base file with the SMS parameters set by the user
- EF-PLMNwAcT (User controlled PLMN selector with Access Technology)
 - Transparent file of variable length with preferred PLMNs of the user in priority order
- EF-ACSGL (Allowed CSG Lists), EF-CSGT(CSG Type), EF-HNBN (Home NodeB Name)
 - Record based files with list of allowed CSG cells.
 - These can also be stored in the ME, if the UICC does not have these EFs
- EF-ICI (Incoming Call Information), EF-OCI (Outgoing Call Information)
 - Record based EFs with Incoming/Outgoing Call Information.
 - The information is normally stored on the ME as well
- EF-FPLMN (Forbidden PLMNs)
 - Binary file of variable size with list of forbidden PLMNs
- EF-SMSS (SMS Status)
 - Contains the status of Last Used TP-MR and Memory Capacity Exceeded flag.

User controlled EFs

Several EFs on the UICC are controlled by the user or contain data that belongs to the user:

- Phonebook
- SMS

The storage of these EFs on the terminal for faster UICC initialization does not have one single answer, as it depends on the specific focus of a certain user or operator and might vary depending on the market and the usage of such features in that specific market.

- a fast initialization of phonebook might be seen as an advantage in some markets
 - for example operators deploying UICC cards with 2,000+ entries in the UICC phonebook
- a copy of the information on the terminal might be seen as a potential risk in some markets
- these features on the UICC are not used at all in some markets

For this reason, choice should be given to each operator and the mechanism proposed by ETSI allows this flexibility.

Conclusions

- Even in the most conservative case, there is a significant number of EFs that would benefit from the proposal, which only requires software changes (fast time to market)
 - Optimization of UICC access is important and was already indicated in C6-140106:
 - CT6 agrees that it would be welcome to reduce the time needed for UICC initialisation. CT6 believes that the topic of optimization of the time required by the Terminal to initialize the UICC is an initiative that may positively affect the user experience.

- Adding new features to the USIM in future releases
 - New features are added in each 3GPP release
 - Rel.12 introduced 8 new files for ProSe, all of them would benefit from the proposed change and are needed for Public Safety
 - Time to fully initialize the card increases
 - SFI values are exhausted
 - New EFs in the USIM cannot have SFI, as all possible values (1 to 30) are allocated already

- Other advantages
 - During early LTE roll-outs, it was found that frequent updates of EF-EPSNSC were causing a wear out of the UICC
 - More details are available in S3-110526 and C6-110292
 - A standardized way to easily look into the counter can help detect such conditions early

Improvements

Current proposal in ETSI does not explicitly indicate how the Update Counter is used to improve performances of UICC Access. This might be useful to make sure that final solution is consistent in all implementations:

- Add requirement for the terminal to store content in “secure storage that is not accessible to the user”
- Add requirement for the terminal to delete stored content for a given EF when SELECT is returned with a mismatching Update Counter

Questions?

<https://support.cdmatech.com>

