3GPP TSG SA WG3 Security — S3#29 **S3-030316**
15 - 18 July 2003
San Francisco, USA

3GPP TSG-T2 #21
San Diego, CA, USA
12 -16 May 2003

T2-030263

Title: **UE security aspects of the GUP architecture**
Response to: -
Release: Release 6
Work Item: Data Description Method (GUP)

Source: T2
To: SA3
Cc: SA2

Contact Person:
Name: Henrik Thuvesson
Tel. Number: +46 70 598 5122
E-mail Address: henrik.thuvesson@teliasonera.com

Attachments:

T2-020221 (S2-031000), T2-030035

Overview:

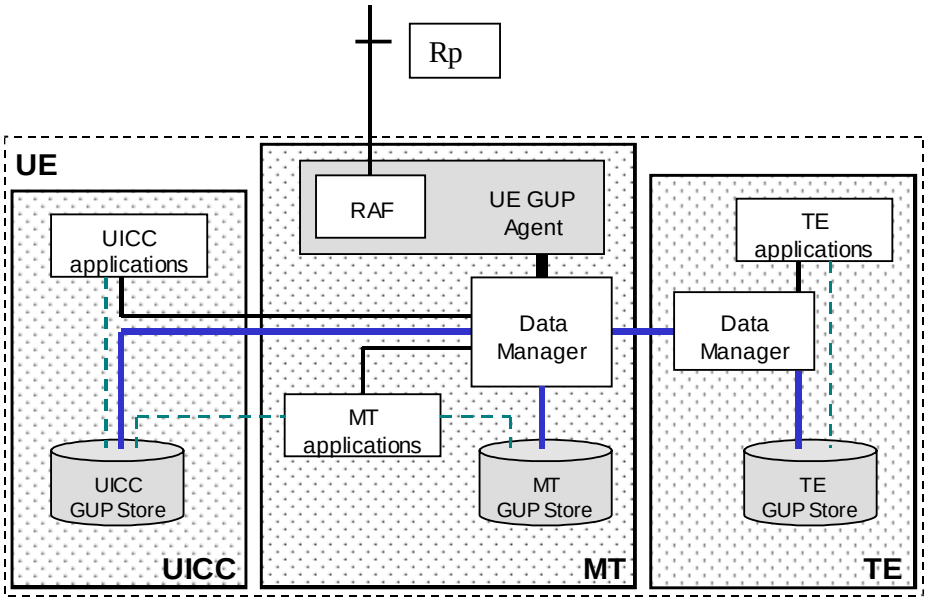
T2 has sent LS T2-030035 to SA2 regarding the implications of UE architectural internal elements and use cases related to GUP operation within these UE elements. SA2 has sent a response LS T2-030221 (S2-031000). In that LS, SA2 raises questions which have implications and questions relating to security, especially items 3d,e.

T2 would like to request SA3 to kindly address these questions which are further elaborated in this LS and respond to T2 with cc to SA2.

GUP security implications on UE Terminal Architecture:

The following figure extracted from T2-030035 (see also TS23.240) illustrates a possible approach for the incorporation of UE components into the current SA2 GUP architecture. This document is intended as a basis for identifying and highlighting a relevant terminal GUP use case and terminal security aspects. T2 intends to continue this effort and to liaise with SA2 and SA3 in order to assist SA2 in defining the GUP Architecture from a Terminal perspective.
(Please also refer to 22.240v600 for synchronization model requirements, especially regarding changes made to GUP data in UE-disconnected mode which would need to be subsequently synchronized).

Security is not yet covered by the use case descriptions. What are the security implications? In Use Case 1 it is not clear how the security of the TE applications can be guaranteed. In Use Case 2 security check is not included. There probably exist many more security implications.



Elements of the GUP UE architecture

- **RAF (Repository Access Function):** This part of the current SA2 GUP architecture (as specified in TS 23.240) realizes the GUP Harmonized Access interface and must be met by the lower layers regardless of a particular UE architecture. Therefore the RAF must be located at the R_p reference point on UE side.
- **UE GUP Agent:** It is assumed that the MT acts as a GUP "single point of entry" in the UE. Then the MT must contain a module to perform this task. The module is called *UE GUP Agent*.
- **Data Manager:** This element is responsible for the data management within the UE. The functions of the Data Manager comprise for instance security, synchronization, and the data handling between UE entities like MT and TE. In the MT the Data Manager is closely linked with the UE GUP Agent.

Use Case 1: TE applications access UE-external GUP data

This use case covers all scenarios where UE applications access UE-external GUP data. In each case the application would have to trigger the MT Data Manager which would initiate the necessary actions in the UE GUP Agent. In the examined case the applications run in the TE what requires the involvement of a second Data Manager. Therefore this use case is the more challenging one.

Actors:

1) external TE
2) GUP network architecture with a GUP Server
3) MT

Pre-Conditions:

1) A radio link is established between UE and GUP Server.
2) The GUP server manages the GUP access policy for the UE.

Flow:

1. The TE application does not distinguish between data stored in the MT, on the UICC or outside of the UE. Always the TE application triggers the TE Data Manager that has to run the necessary protocol with the MT Data Manager.
2. The MT Data Manager forwards the request to the UE GUP Agent.
3. Now the UE GUP Agent contacts the GUP Server according to the R_g protocol and informs about the intended operation.
4. The GUP Server helps to establish a connection between the UE and the device that contains the right GUP data store.

5. Afterwards the MT Data Manager and the Data Manager of the external data store run the protocol to execute the data operation. The source of the commands would be the TE Data Manager which could be more or less involved in the process.

Alternatives:
The TE Data Manager might directly communicate with the Data Manager of the device of the UE-external application. This means that the protocol would be tunnelled through the MT Data Manager. Nevertheless the UE GUP Agent needs to be involved as in the scenario above.

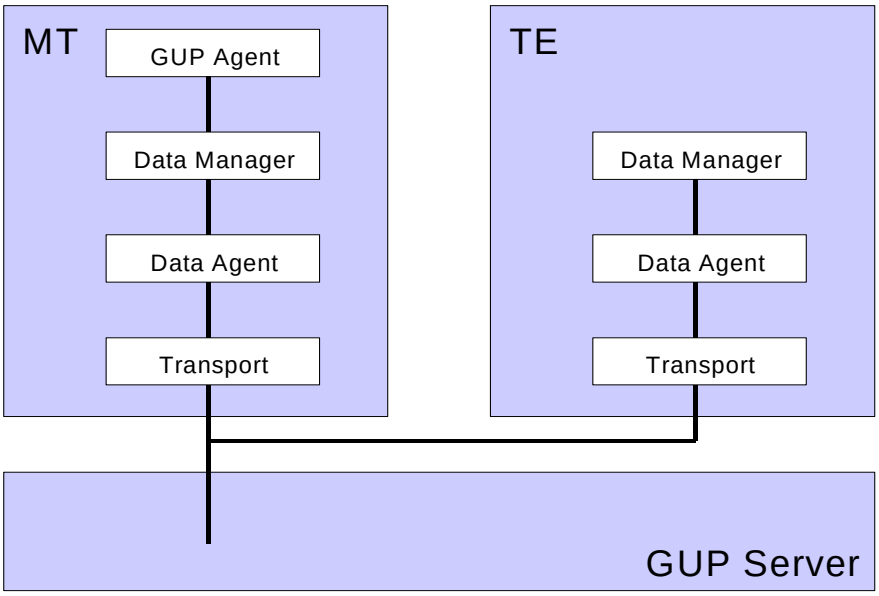
Use Case 2: External applications access UE GUP data via the GUP Server
The GUP Server does not know the current components of the UE or the distribution of the UE GUP data over the different UE GUP stores. The GUP Server merely contacts the UE as a whole entity and the UE GUP Agent has to address the correct UE component. Therefore this use case can cover all scenarios where UE-external applications access data in MT, TE, or UICC GUP repositories.

Actors:
1) Applications outside of the UE
2) GUP network architecture with a GUP Server
3) UE (comprising MT and UICC but not necessarily a TE)

Pre-Conditions:
1) A radio link is established between UE and GUP Server.
2) The GUP server manages the GUP access policy for the UE.

Flow:
1. The GUP Server forwards a request of a UE-external application to create, read, modify, or delete user profile data in the UE. The request is received by the UE GUP Agent.
2. The RAF module in the UE GUP Agent interprets the received commands and data.
3. Together with the Data Manager the UE GUP Agent checks the data location within the UE. If the data are stored in an external TE then the data may be not accessible.
4. The UICC and the MT GUP stores can be accessed directly (accessing device-internal data) by the UE GUP Agent. For the access to the TE GUP store the Data Manager is required.
5. When the UE GUP Agent was requested to read data then these data are sent to the GUP Server. Before the transmission the RAF transforms the data to the right transport format.

The following picture shows the layer diagram related to the UE architecture in the use cases 1-2.



Remarks to the picture:

- The requirements of the RAF block (as specified in TS 23.240) must be met by the lower layers regardless of a particular UE architecture.
- The Data Agent terminates the protocol between two devices that is used for the data operations.
- The Data Manager is located above the Data Agent in the layer hierarchy. The Data Manager is responsible for data operations that are required to provide the input (control, data) for the Data Agent and to process the results of the Data Agent operations.
- The GUP Agent is an additional module for the higher level data management. In contrast to the Data Manager the GUP Agent executes only GUP-specific tasks. At least for the discussions it may be beneficial to have a clear differentiation between GUP-specific functions and functions that are already implemented in a system without GUP. The required functionality of the GUP Agent is not yet discussed.

Actions:

To SA3 group.

ACTION: T2 asks SA3 to review the Terminal GUP Use Cases and GUP security implications on the Terminal architecture and provide T2 with information (cc to SA2) on the results of that discussion. It is hoped that a response is received in a timely fashion to facilitate this work in the Release 6 timeframe.

To SA2 group.

ACTION: None.

3. Date of next T2 Meetings:

T2#22	25-29 Aug 2003	Cambridge, UK

3GPP TSG-T2 #21
San Diego, CA, USA
12 -16 May 2003

T2-030221

3GPP TSG-SA2 Meeting #30 **S2-031000**
Milan, Italy, 24 - 28 February 2003

Title: LS on T2 GUP Co-ordination Progress Report to SA2
Response to: T2-030156 (= S2-030519)

Source: SA2
To: T2
Cc: TSG T

Contact Person:
Name: Harri Koskinen
Tel. Number: +358 40 504 0780
E-mail Address: harri.o.koskinen@nokia.com

Attachments: none

---

1. Overall Description:

This LS is sent to T2 for ACTION.

SA2 would like to thank T2 on their progress report on their GUP work, and for the work done so far. We would like to respond on your actions to us as follows:

1. Comments on your LS and the attached documents

SA2 do not have any specific comments on the Consensus Proposal for GUP in T2-020985. SA2 understand that it is a framework for your work item on Data Description Method and thus also a framework for the new structure of TS 23.241. For the comments on the other attached document T2-030035, please refer to item 3 in this LS.

2. Comments on methods for keeping the Information Model work in our respective Groups synchronised

SA2 have already responded at SA2 #29 in January your earlier LS in T2-020982 (= S2-030049), the response is in S2-030441. Please refer to it on SA2 comments on methods for keeping the Information Model work synchronised in our working groups.

3. Review of the Terminal GUP Use Cases and GUP implications on the Terminal architecture

SA2 have the following comments on the UE Use Cases for the GUP Architecture:

a) General: The relationship between the Rp reference point and SyncML DM is not understood.

b) Use Case 2: There is no GUP Data Repository specified in UICC (NB. SA2 are specifying GUP concretely for Rel6), and also concerns were expressed about the different formats of the GUP data in the UICC and the MT. Also the functionality is not understood, if the same data resides both in the UICC and the MT.

c) Use Case 3: If the TE tries to access the data residing in the UICC, what are the requirements for API? In the flow, it is not clear in item 2) which Data Manager must determine the current location of the data.

d) Use Case 4: In the leading paragraph a second Data Manager is referred to, where it is located and what are its requirements? Additionally, it is not clear how the security of the TE applications can be guaranteed.

e) Use Case 5: Security check seems to be missing in this use case. In the flow, it is not understood in item 3) which Data Manager checks the data location together with the UE GUP Agent. Additionally, it was not understood in item 4) how the UICC and the MT GUP stores can be accessed directly by the UE GUP Agent. Furthermore the MT GUP store (i.e. data repository) is not specified.

f) Questions in the discussion part of the contribution: Concerning the question if the UE is a black box for the GUP server, one company commented that the GUP reference architecture should not specify the internal architectures of the entities involved, while another company expressed their view that the role of the UICC in the GUP architecture needs to be clarified. On the other detailed questions it was felt by SA2 that the

questions cannot be responded yet due to the current status of the development of GUP reference architecture, e.g. synchronisation has not yet been discussed by SA2.

2. Actions:

To T2 group.

ACTION: SA2 ask T2 group to discuss and take into consideration SA2's comments on the terminal GUP Use Cases.

3. Dates of Next TSG-SA2 Meetings:

TSG-SA2 Meeting #31	7 - 11 April 2003	Seoul, Korea
TSG-SA2 Meeting #32	12 - 16 May 2003	San Diego, USA

3GPP GUP TSG-T2#20 SWG2 T2-030035
San Francisco, USA
20th – 24th January, 2003

Source: **Siemens**

Title: **UE Use Cases for the GUP Architecture**

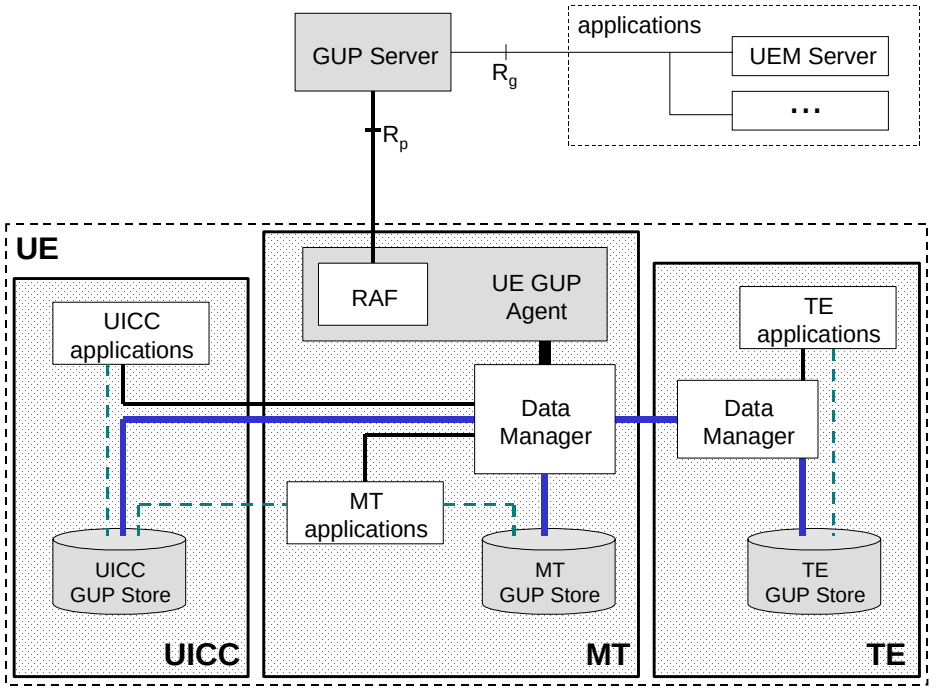
Agenda item: **GUP**

Document for: **Discussion (T2 SWG2 Action Item from Bundang)**

Introduction

During the T2 meeting #19 in Bundang the UE aspects of the GUP architecture were discussed in SWG2. It was concluded that specific terminal aspects still need to be considered in the SA2 GUP architecture draft specification. With an LS T2 informed SA2 about this potential shortcoming and volunteered to provide more detailed information about important terminal use cases. This document is intended as a basis for identifying and highlighting relevant use cases and terminal aspects.

The following figure illustrates a possible approach for the incorporation of UE components into the current SA2 GUP architecture that can be used as a starting point for the necessary discussions.



Elements of the GUP UE architecture

- **RAF (Repository Access Function):** This part of the current SA2 GUP architecture realizes the GUP Harmonized Access interface. Therefore the RAF must be located at the R_p reference point on UE side.
- **UE GUP Agent:** It is assumed that the MT acts as a GUP "single point of entry" in the UE. Then the MT must contain a module to perform this task. The module is called *UE GUP Agent*.
- **Data Manager:** This element is responsible for the data management within the UE. The functions of the Data Manager comprise for instance security, synchronization, and the data handling between UE entities like MT and TE. In the MT the Data Manager is closely linked with the UE GUP Agent.

Use Cases

Use Case 1: MT applications access GUP data in an external TE

An MT application creates, reads, modifies, or deletes user profile data that are stored in a TE.

Actors:
1) MT
2) external TE

Pre-Conditions:
1) An MT is connected with an external TE.
   (The transport protocol may vary and does not matter for the use case.)
2) No radio access to the 3GPP network is required.
   (Thus the UE may not be able to access the GUP Server.)
3) Each TE uses the same data exchange mechanisms.
   (Beside of the protocol this provides the required local access policy.)

Flow:
1) As the MT application does not have a direct link to TE data repositories the MT must involve the Data Manager which provides access to the TE data. Therefore the MT application sends a request for the data operation to the MT Data Manager.
2) The MT Data Manager determines the location of the TE data and provides the needed functionality for authentication, integrity, and confidentiality. The UE GUP Agent may assist.
3) Now the MT Data Manager performs the requested data operation by sending the appropriate commands to the TE Data Manager.
4) The TE Data Manager has direct access to the TE GUP data repository and executes the MT commands. Results are sent to the MT application via the MT Data Manager.

Alternatives:
1) The MT application could be able to access the TE data repositories directly without involving a Data Manager. In this case either no access policy is applied or a non-standardized protection is used. Therefore the case would not differ from the access of MT-internal data by the MT.
2) All TE GUP data might be copied to the MT. When needed the Data Manager would have to synchronize the data repositories in order to update the TE GUP data located in the MT. In this case the MT applications could handle MT and TE GUP data in nearly the same way.

Use Case 2: MT applications access GUP data on the UICC

An MT application creates, reads, modifies, or deletes user profile data that are stored on the UICC. The MT-UICC scenario differs from the MT-TE scenario as the UICC must be always present for a 3GPP radio access. The MT and UICC are also tied together on application level (e.g. MMS parameter storage on the USIM).

Actors:
1) MT
2) UICC

Pre-Conditions:
1) The UICC is located within the terminal device.
2) There is a trusted relationship between the MT and the UICC.
   (Accordingly no GUP access policy is needed to access the UICC GUP store.)

Flow:
1) MT applications (e.g. MMS client) may access the UICC GUP store directly via the standardized MT-UICC interface.
2) Alternatively the MT applications can utilize the capabilities of the MT Data Manager. For instance the Data Manager could help to prevent data inconsistency problems or to locate a particular piece of information.

Use Case 3: TE applications access GUP data on the UICC

In contrast to the MT the UICC does not contain a Data Manager for the data exchange with a TE. Thus the TE depends on the support of the MT Data Manager that is able to access UICC GUP data.

Actors:
1) external TE
2) UICC
3) MT

Pre-Conditions:
1) The UICC is located within the terminal device.
2) The TE has to access the UICC GUP data store via the MT.

Flow:
1) First the TE signals a request to the MT Data Manager that it wants to create, read, modify, or delete user profile data stored on the UICC.
2) Not in all cases the TE will know the location of particular GUP data. Then the Data Manager must determine the current location of the data.
3) The Data Manager ensures the security of the data operation. The UE GUP Agent may have to support the MT Data Manager. For instance the UE GUP Agent could maintain GUP-specific access policies which must be applied at GUP-related operations.
4) Now the MT Data Manager executes the needed operations on the UICC GUP data and sends the results back to the TE application via the TE Data Manager.

Alternatives:
1) The TE applications could contact the UE GUP Agent instead of the Data Manager. Then the UE GUP Agent would act as the master of the process and coordinate the different tasks. The MT Data Manager would become a proxy.

Use Case 4: TE applications access UE-external GUP data

This use case covers all scenarios where UE applications access UE-external GUP data. In each case the application would have to trigger the MT Data Manager which would initiate the necessary actions in the UE GUP Agent. In the examined case the applications run in the TE what requires the involvement of a second Data Manager. Therefore this use case is the more challenging one.

Actors:
1) external TE
2) GUP network architecture with a GUP Server
3) MT

Pre-Conditions:
1) A radio link is established between UE and GUP Server.
2) The GUP server manages the GUP access policy for the UE.

Flow:
1) The TE application does not distinguish between data stored in the MT, on the UICC or outside of the UE. Always the TE application triggers the TE Data Manager that has to run the necessary protocol with the MT Data Manager.
2) The MT Data Manager forwards the request to the UE GUP Agent.
3) Now the UE GUP Agent contacts the GUP Server according to the R_g protocol and informs about the intended operation.
4) The GUP Server helps to establish a connection between the UE and the device that contains the right GUP data store.
5) Afterwards the MT Data Manager and the Data Manager of the external data store run the protocol to execute the data operation. The source of the commands would be the TE Data Manager which could be more or less involved in the process.

Alternatives:
1) The TE Data Manager might directly communicate with the Data Manager of the device of the UE-external application. This means that the protocol would be tunneled through the MT Data Manager. Nevertheless the UE GUP Agent needs to be involved as in the scenario above.

Use Case 5: External applications access UE GUP data via the GUP Server

The GUP Server does not know the current components of the UE or the distribution of the UE GUP data over the different UE GUP stores. The GUP Server merely contacts the UE as a whole entity and the UE GUP Agent has to address the correct UE component. Therefore this use case can cover all scenarios where UE-external applications access data in MT, TE, or UICC GUP repositories.

Actors:
1) Applications outside of the UE
2) GUP network architecture with a GUP Server
3) UE (comprising MT and UICC but not necessarily a TE)

Pre-Conditions:
1) A radio link is established between UE and GUP Server.
2) The GUP server manages the GUP access policy for the UE.

Flow:

1) The GUP Server forwards a request of a UE-external application to create, read, modify, or delete user profile data in the UE. The request is received by the UE GUP Agent.
2) The RAF module in the UE GUP Agent interprets the received commands and data.
3) Together with the Data Manager the UE GUP Agent checks the data location within the UE. If the data are stored in an external TE then the data may be not accessible.
4) The UICC and the MT GUP stores can be accessed directly by the UE GUP Agent. For the access to the TE GUP store the Data Manager is required.
5) When the UE GUP Agent was requested to read data then these data are sent to the GUP Server. Before the transmission the RAF transforms the data to the right transport format.

Discussion

- Typically the Data Manager would have to be based on SyncML DM and may comprise more than one module. For instance the UE Data Manager may act as a master for the UE data management and could consist of an agent module and a more basic module for the data operations. In light of SyncML DM the relationship and functional split between the Data Manager and the UE GUP Agent must be analyzed in more detail.
- The first agreements should clarify the general role of the UE in the GUP architecture. Is the UE a black box for the GUP Server? Does the GUP Server handle the data access policy for the UE or would the usage of SyncML favor a UE-based access policy? Who has to carry out the synchronization of UE GUP data copies? Which UE-related interfaces would be specified in GUP? Afterwards more detailed aspects like the data operations for TE data could be analyzed in accordance with the general understanding.