An Object-Oriented Approach to Mobility Service Creation

Ivaylo Atanasov[1]

Abstract - **The paper presents an object-oriented approach to modeling mobile value-added services. Service capabilities are set of building blocks that can be used to implement value-added services. The service capability features are common utility features that provide such things as authentication, authorization, registration, and notification services. The paper investigates how security features can be implemented using an object-oriented approach on the Intelligent network platform. It exploits the Service independent building block (SIB) concept of the IN conceptual model for service creation.**

Keywords – **Intelligent network services, SIBs, objects, authentication, ciphering**

I. Introduction

The three service classes (bearer services, teleservices and supplementary services) are all standardized in 2G and 3G mobile networks and their functionality is strictly specified. This means that no matter which operator provides them, they are always the same from the subscriber's perspective. Operators have longed for a set of tools which to build unique services, a means to distinguish themselves from the competition. Service capabilities are set of building blocks that can be used to implement value-added services. As the value added services themselves are not standardized, but only the building blocks, it is possible to implement them in a way that produces unique services. Service capabilities are accessible to applications via a standardized application interface. Various toolkits and mechanisms such as the SIM Application Toolkit (SAT), Mobile station Execution Environment (MExE), Customized Application for Mobile Enhanced Logic (CAMEL) and Intelligent network (IN) provide them.

Framework service capability features are common utility features that are used by nonframework features. They provide such things as authentication, authorization, registration, and notification services. Nonframework features are used by the applications as building blocks for value-added services. These features should be as generic as possible, so that the applications using the features are easily portable.

The paper investigates how security nonframework features may be implemented using an object-oriented approach on the Intelligent network platform.

To create services the IN conceptual model uses the Service independent building block (SIB) concept. It defines services as composition of features, which in turn are composed of elementary SIBs. An IN service creation environment allows even inexperienced service engineers to create services by clicking together elementary SIBs in a plug-and-play fashion.

II. SIBs supporting mobility procedures

By modularizing the GSM mobility procedures it is possible to identify commonality within the various procedures. Examples of common sub-procedures are authentication, new TMSI assignment, ciphering and database updating. These sub-procedures are self contained and identical irrespective of the mobility procedure using it. Each of these sub-procedures may be converted to a Service independent building block (SIB). The following list of SIBs may be identified:

- Authentication SIB – generates data required for authentication and checks the calculated value against the returned value.
- Ciphering SIB – instructs the radio access network to cipher a channel to the mobile telephone (MT).
- TMSI assignment SIB – issues a new TMSI to MT.
- Service data management SIB (SDM SIB) – used for creating, updating and deleting records on database.
- Location update SIB – if location area updating procedure is successful then the user is informed accordingly or else the SIB is used to process any errors that may have been occurred during the procedure.
- Mobile originating call SIB (MOC SIB) – checks the compatibility service requested by the user with the subscription for the user. Instructs MSC capture a radio channel to the MT and forwards instructions on call completion to Service Switching Function (SSF).
- Mobile terminating call SIB (MTC SIB) – instructs SSF to check compatibility of incoming call with the mobile terminal and capture a radio channel to the MT.
- Paging SIB – instructs radio access network to page a MT in a specified area.

For example, the mobile terminating call service in GSM uses Paging SIB, SDM SIB, Authentication SIB, Ciphering SIB, TMSI assignment SIB and MTC SIB. It proceeds in the following way. Receiving an *Initial address message* from the GMSC the MSC/SSF treats it as a service trigger and sends an *InitialDP message* to the Service Control Point (SCP). The SCP starts service logic with the Paging SIB in order to contact with the MT. The SCP also sends a *requestReport* message to the SSF, indicating the detection point (DP) where it wants to be notified. When the MT answers the paging, the SSF sends an *eventReport* message. The SCP proceeds with

[11] Ivaylo Atanasov is with Faculty of Communications, Technical University of Sofia, 8 Kl. Ohridski Blvd., 1000 Sofia, Bulgaria, e-mail iia@tu-sofia.bg

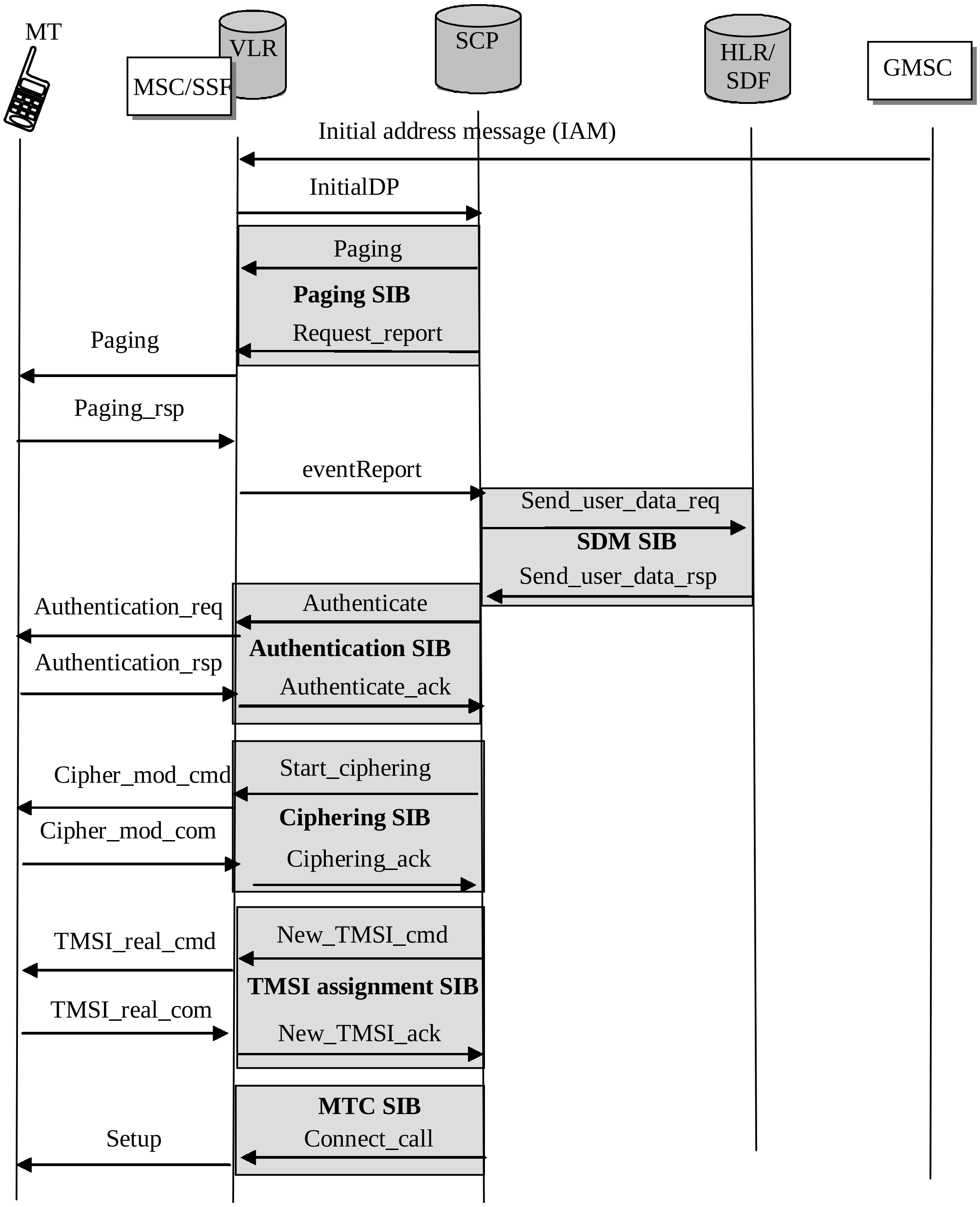

Figure 1 Mobile terminating call service by the use of SIBs supporting mobility

service logic execution starting the SDM SIB to request authentication data for the subscriber from the HLR/SDF. Having the needed information the SCP invokes the Authentication SIB and instructs the MSC to send *Authentication_req* message to the MT. The MT returns the authentication result. If authentication succeeds the SCP invokes the Ciphering SIB which instructs the MSC to start ciphering over the air interface. A new TMSI is assigned to the MT by the use of the TMSI assignment SIB. The SCP instructs the SSF to check compatibility of the incoming call with the MT and capture a radio channel to the MT using the MTC SIB. Figure 1 shows the mobile terminating call service created with the use of identified SIBs.

The appropriate SIB set can be used to create the mobile originating call service and the location update service.

The mobility procedures in GPRS and UMTS follow almost the same steps as those in GSM. The main deference is in the security sub-procedure, which is more complicated in UMTS. UMTS uses mutual authentication, more advanced radio access network encryption and integrity protection.

III. Security in mobile environment

The most important security features in the GSM system are:

- Authentication of the user
- Encryption of communication in radio interface
- Use of temporary identities.

As GSM system became more and more successful, the usefulness of these basic security features also becomes more and more evident. Naturally, it has been a leading principle in specification work of UMTS security to carry these features over to the new system.

The success of GSM also emphasised finally the limitations of its security. A popular technology is also tempting for intruders. The properties of GSM that have been most criticized on the security front are the following:

- Active attacks towards the network are possible in principle: it refers to somebody who has the required equipment to deviate communication from legitimate network/ terminal equipment.
- Sensitive control data, e.g. keys used for radio interface ciphering, are sent between different networks without ciphering.
- Some parts of the security algorithms are kept secret but they trend to be revealed sooner or later.
- Keys used for radio interface ciphering become eventually vulnerable to massive attacks where somebody tries all the possible keys until one matches.

In UMTS countermeasures for perceived weaknesses in GSM are developed. The most important security features of UMTS are the following:

- Mutual authentication of the user and the network
- Use of temporary identities
- Radio access network encryption
- Protection of signaling integrity inside UTRAN.

Publicly available cryptographic algorithms are used for encryption and integrity protection. Algorithms for mutual authentication are operator-specific.

IV. From SIBs to objects

Defining the generic functionality of GSM mobility procedures by the use of SIB object types, it is possible to extend the model with GPRS and UMTS mobility procedures. For example, a new UMTS object type can inherit basic properties from an already existing GSM type and extend it with new features. Common objects as the TMSI assignment SIB and the Service data management SIB can be reuse in many service scripts.

The focus in the paper is on security sub-procedures: Authentication SIB and Ciphering SIB.

Considering the common parts in GSM and UMTS security functions the following object types can be defined.

- *User identity request* object type– allows the identification of a user on radio path by means of IMSI. The mechanism should be invoked by the serving network when the user registers for the first time in a serving network or when the serving network cannot retrieve the IMSI from the TMSI. This object types is used to negotiate whether the authentication is necessary. For GSM and UMTS the specializations use CKSN (Cipher key sequence number) and KSI (key set identifier) accordingly.
- *User authentication* object type - generates user authentication vector that is temporary authentication and key agreement (AKA) data enabling a VLR/SGSN to engage AKA with a particular user. The specializations of this object types are for GSM and UMTS authentication procedures. GSM authentication vector consists of three elements: a) network challenge RAND, b) an expected user response SRES and c) a cipher key Kc. UMTS authentication vector consists of five elements: a) network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) network authentication token AUTN.
- *Security algorithm decision* object type – for GSM determines which ciphering algorithm is to be used and for UMTS which UMTS Encryption algorithms (UEAs) and UMTS Integrity algorithms (UIAs) are allowed to be used in order of preference.
- *Start security mode* object type – sends a start security command to the BSC/SRNC. For GSM to activate ciphering the value Kc and the reference to the chosen A5/X algorithm is sent. For UMTS an ordered list of allowed UEAs and IK to be used are sent. The message contains the ordered list of allowed UEAs and CK to be used too.
- *Start ciphering* object type – starts ciphering.
    - For GSM at BSS the Kc and information about cipher algorithm is retrieved and a message is forwarded to MT. This message triggers the MT to enable ciphering of all outgoing data and deciphering all incoming information. The MS confirms the change to ciphering mode to the MSC/VLR.
    - For UMTS the SRNC decides which algorithm to use, generates a random value FRESH and initiates downlink integrity protection. The SGSN sends a security mode command message including user equipment security capability, the UIA and FESH to be used. Before sending this message the SRNC generates the MAC-I and attaches this information to the message. At reception of the message the MT controls that the user equipment security capabilities received is equal to the user equipment security capabilities sent in the initial message. The MT verifies the integrity of the message by calculating the XMAC-I. If all controls are successful, the MT compiles a message that confirms the security mode and generates MAC-I for this message. At the reception of response message the SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I. The SRNC acknowledges the security mode to the VLR/SGSN.

The Authentication SIB can be defined as a generic object type composed of the *User identity request* object type and the *User authentication* object type. The Ciphering SIB can be defined as a generic object type composed of the *Security algorithm decision* object type, the *Start security mode* object type and the *Start ciphering* object type. Figure 2 illustrates the generic definitions of the Authentication SIB and the Ciphering SIB.

For GSM and UMTS these generic object types are inherited by specializations representing the specific features of the security procedures.

For example, the GSM Authentication SIB is composed of the *GSM User identity request* object type that inherits the *User identity request* object type and the *GSM User authentication* object type that inherits the *User authen-*

tication object type. The GSM Ciphering SIB is composed of the *GSM Security algorithm decision* object type that inherits the *Security algorithm decision* object type, the *GSM Start security mode* object type that inherits the *Start security mode* object type and the *GSM Start ciphering* object type that inherits the *Start ciphering* object type. Figure 3 illustrates the adopted approach.

Similar definitions of the UMTS Authentication SIB and UMTS Ciphering SIB can be done.

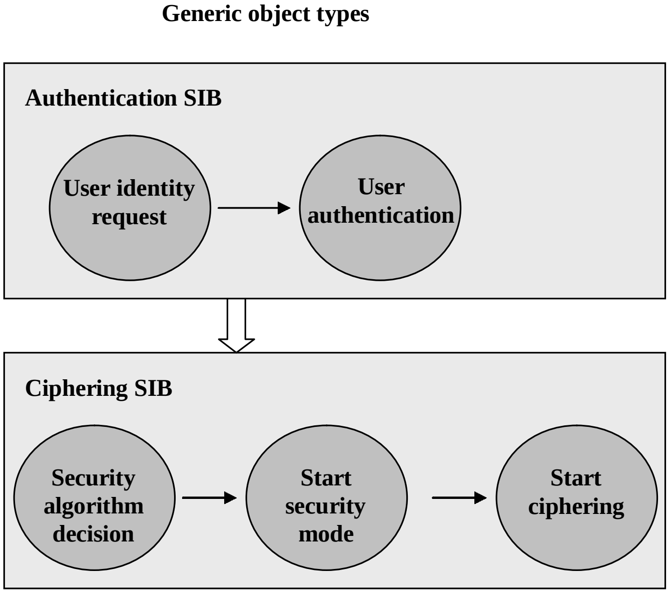

Figure 2 The generic object types:
Authentication SIB and Ciphering SIB

V. Conclusion

A new approach to provisioning mobile value-added services is suggested. The service capabilities can be offered as a composition of SIBs defined as object types. The generic object types represent the common parts in mobility management procedures for GSM, GPRS and UMTS systems. The specific parts are defined by the use of specialized object types that inherit communality in the generic object types. The approach is illustrated with concern of the security procedures in GSM and UMTS. Both systems apply common security functions as: authentication of the user, encryption of communication in radio interface, use of temporary identities. Adding to that, UMTS applies integrity check of the signaling data. By identification of common parts some generic object types are defined and to consider the specifics for GSM and for UMTS some object types are redefined and new ones are defined.

The approach suggests a flexible way of capability service feature implementation that exposes all the advantages of object-oriented programming.

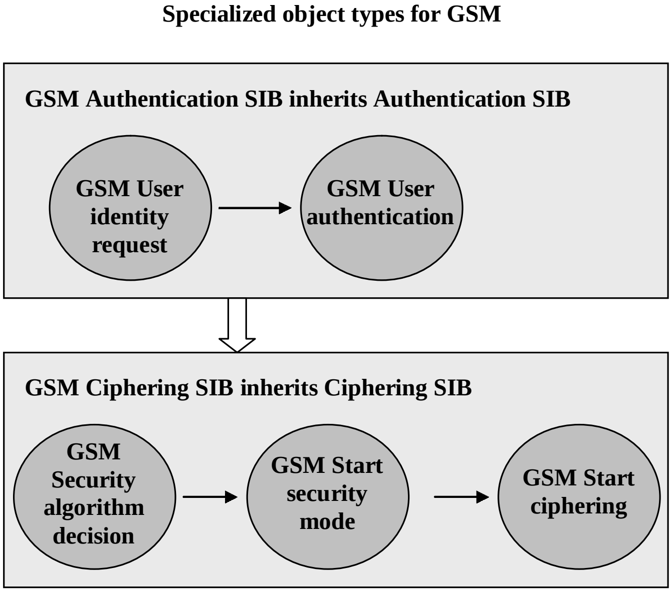
Specialized object types for GSM
GSM Authentication SIB inherits Authentication SIB
GSM User identity request
GSM User authentication
GSM Ciphering SIB inherits Ciphering SIB
GSM Security algorithm decision
GSM Start security mode
GSM Start ciphering

Figure 3 The specialized object types:
GSM Authentication SIB and GSM Ciphering SIB

Reference

[1] ITU Q.1223, IN Global Functional Plane Architecture for Capability Set 2.

[2] ETSI TS 123 121, Universal Mobile telecommunications System, Architectural Requirements for Release 1999

[3] ETSI TS 123 060, General Packet Radio Service, Service Description.

[4] Gunnar Heine, GSM Networks: Protocols, Terminology, and Implementation, 1999.