GSM Authentication Centre

Contents

- Please note that this description includes details of both basic and optional products. This description does not necessarily correspond to any specific release or delivery time.

1 Introduction

This document describes the functionality and the system architecture of Ericssons GSM AuC, including services, interfaces, element management and characteristics.

The main function of the AuC is to provide to HLR the triplets needed by the authentication and ciphering processes used within GSM system.

Key characteristics of the Ericsson AuC:

- High capacity and high availability
- Designed for flexible configurations
- Authentication and ciphering data provided in real time
- Use of distributed processors for authentication triplets generation
- Use of mechanisms to minimize the risk of fraud

The Ericsson AuC is built to guarantee high capacity and high availability. As the Home Location Register (HLR) is also built on the same platform, the Ericsson AuC gains well proven operational and maintenance benefits.

A common platform offers advantages like common maintenance and development methodology and well-proven process for introducing new and enhanced functionality. But this platform also offers trouble-free and seamless interworking between different nodes.

The platform undergoes continuous extensive development, taking advantage from the general platform development as well as from other parts of Ericsson's UMTS based systems. The Ericsson AuC closely interworks with the HLR, which means that new functionality in the AuC and the HLR will be developed tightly together, optimising interworking and performance.

2 Overview

The AuC generates authentication and ciphering data according to the European Telecommunications Standards Institute (ETSI) GSM specifications.

The AuC supports a wide range of services and functionality. Beside the services and functionality developed for GSM, the Ericsson AuC also supports functionality already developed and implemented for UMTS networks.

UMTS AuC is described Product Description "UMTS Authentication Centre".

3 Functionality

3.1 General

The AuC complies with the GSM phase 1, GSM phase 2 and GSM phase 2+ requirements.

The purpose of the authentication security feature is to protect the network against unauthorised use. It also enables protecting subscribers by denying the possibility for intruders to impersonate authorised users.

The authentication data is used to ensure that the subscribers accessing the system are the ones they claim to be, and not others using the same International Mobile Subscriber Identity (IMSI).

The ciphering data is used to ensure that confidentiality and integrity is kept on the physical radio channels. Ciphering prevents user information and signalling to be available or disclosed to unauthorised individuals.

3.2 AuC Administration

Standard MML is used for subscription handling and to operate locally the node. Operators dealing with subscriptions can handle subscriber-associated data using customer administrative centre connected to the AuC.

The AuC service administration is divided into:

- administrating key data
- administrating subscription data

Administration of key data

The operator gives AuC specific operations in order to perform:

- definition of key data
- change of key data
- deletion of key data
- printing of key data
- changing of customer key

The key data operations can be made restricted for use.

Administration of subscription data

The operator gives AuC specific operations in order to perform:

- initiation of subscriptions
- deletion of subscriptions
- printing of subscription data
- printing of subscription status

The subscription data operations can be made restricted for use.

3.3 Operation and maintenance

The Operation and Maintenance (O&M) may be done either via the AuC built-in O&M functionality, via the optional Operation Support System (OSS), or via the optional Circuit switched Network Operation Support system (CNOS).

3.4 Statistics

The statistical measurement functions in the AuC collect; store, process and present AuC related statistics. The function enables the operator to evaluate the use of certain functions in the AuC. Statistics and measurement data are available and sorted for:

- MAP operations in AuC
- authentication in AuC
- number of subscriptions registered in AuC
- traffic sensitive size alteration events in AuC

3.5 Triplet generation

The purpose of Triplet Generation function is to generate triplets requested to AuC by HLR nodes.

The "triplets" consists of the following elements:

RAND	Random number
Kc	Ciphering Key
SRES	Signed RESponse

When the HLR sends its request to the AuC via the internal Mobile Application Part (MAP) interface (if it is combined with the HLR) or via the external MAP interface). When a triplet is received, the AuC searches for the International Mobile Subscriber Identity (IMSI) given in the MAP operation.

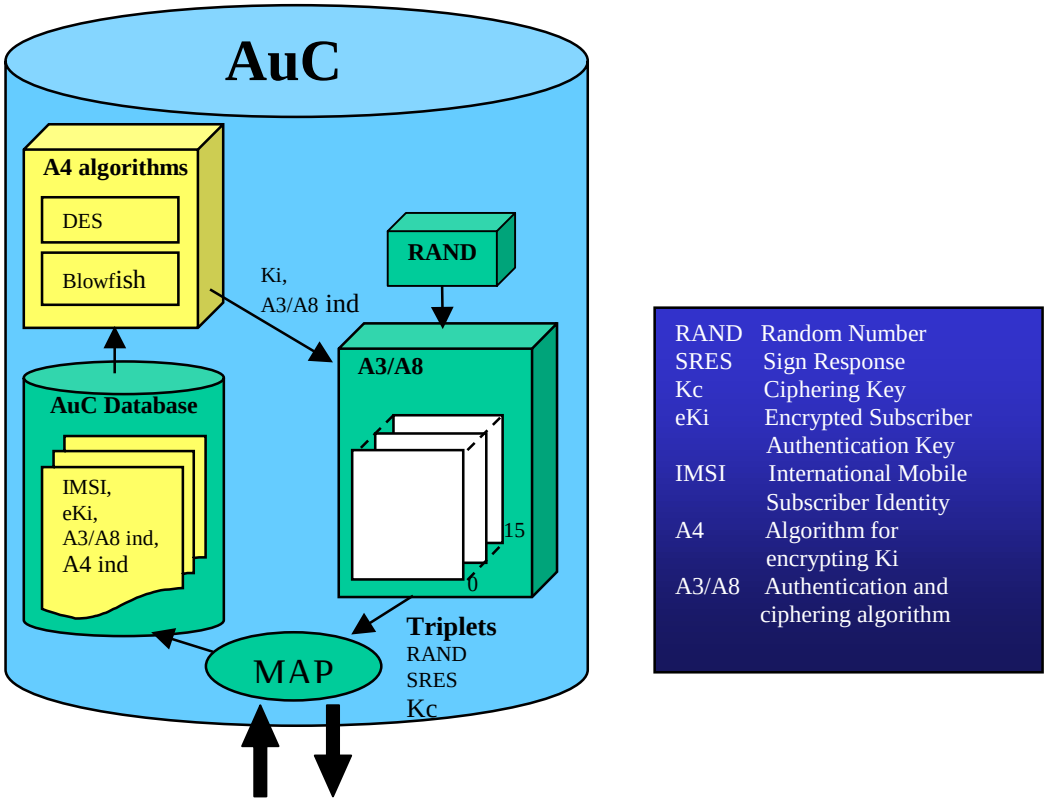

Figure 1. The AuC structure

When the IMSI is found, the encrypted secret authentication key (eKi) is decrypted with an A4 algorithm using the A4 key. At the same time, the random number (RAND) is calculated in the random generator. Using the decrypted Ki and RAND as input, the Sign Response (SRES) and the ciphering key (Kc) are calculated by the A3 and A8 algorithm, respectively. The AuC can respond with up to five triplets per IMSI and request. Finally, the generated triplets (SRES, RAND and Ki) are sent to the HLR.

3.6 MAP Policing

The AuC may accept or reject incoming MAP operations depending on the origin of the request. This function is used mainly to protect security-sensitive data from being accessed by an unauthorised remote access. This is a user function of CCITT Signalling System Transaction Capabilities User Policing.

3.7 Load regulation

Load Regulation function provides regulation mechanisms to control the processor load in situations of extensive signalling towards the AuC node. Typically, such situations may occur at busy hour traffic peaks.

Load regulation makes sure a high throughput of signalling traffic during overload conditions.

3.8 Security

Authentication key

The secret subscriber keys are stored encrypted in the AuC database.

Authority

The AuC has a built-in security function, which allows only authorised personnel to handle key and subscription data. A login procedure with password is required.

Triplet generating functions

The authentication triplet generating functions are included in distributed processor software in order to make efficient use of available resources and at the same time, provide a secure way of data handling.

4 Interfaces

The AuC is basically connected to HLR(s), Operation and Maintenance systems and administration systems.

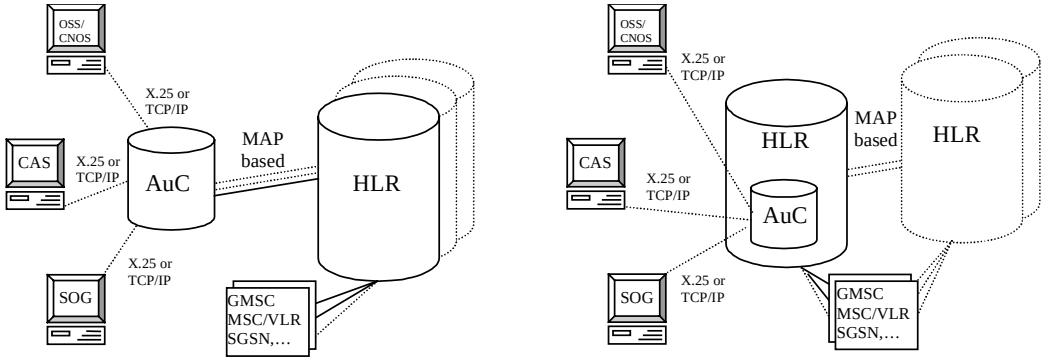

Figure 2. Logical view of AuC in the network.

4.1 Administrative interfaces

The AuC supports the following administrative interfaces:

- Service Order Gateway (SOG). SOG is a product providing Customer Administration System (CAS) to exchange information with Ericsson network elements containing service information.
- Operations Support System (OSS), or Circuit switched Network Operation Support system (CNOS). Used for operation and maintenance purposes. The AuC is also equipped with built in O&M functionality, which makes OSS/CNOS optional.
- Customer Administration System (CAS). AuC may receive orders from an operator's CAS directly connected to the I/O device.

4.2 AuC-HLR interface

The AuC uses a MAP based protocol for the communication towards HLR.

Combined HLR/AuC

The combined AuC and HLR share Common Channel Signalling Subsystem (CCS) resources. The CCS consists of Message transfer Part (MTP) Signalling Connection Control Part (SCCP) and Transaction Capabilities Application Part (TCAP) products. In combined configurations the MTP layer is not used, in this case the HLR/AuC uses an internal SCCP loop.

External HLRs

A stand-alone AuC can of course support other HLRs, but also an AuC combined with an HLR (HLR/AuC) can support other external HLRs than those it is combined with. When HLRs external to the AuC are supported, there are needs for external signalling.

5 Implementation

The AuC is built as an independent Application Module (AM). The AM concept allows for a number of telecommunication applications to be placed on the same platform, of which one is the AuC application; another example is the HLR.

The AuC is implemented on an AXE 10 platform. The node is based on the same processor that is used in Ericsson's well-proven GSM system.

The AuC consists of the following functions realised in Central Processor (CP) and Regional Processor (RP) software:

1. administration of subscriptions and data bases
2. Mobile Application Part (MAP) interface
3. generation of triplets

(1) and (2) are realised in CP software, while (3) is realised in RP software

The Mobile Application Part (MAP) receives messages and replies upon requests for authentication data. For communication with HLR, Ericsson MAP is used, and it is implemented as an internal interface when the AuC and HLR are combined. When the HLR is external to the AuC, the AuC accepts requests from the HLR through an external Ericsson MAP interface. Requests from external HLRs may be rejected by parameter settings.

The AuC authentication and ciphering data generator is implemented in the Regional Processor (RP) to guarantee high capacity and high security.

6 Element Management

The AuC node supports the following management applications:

- Subscription management
- Fault management (e.g. alarm handling)
- Software management (e.g. locally or remotely SW upgrades and backups)
- Hardware equipment management (e.g. inventory support)
- Performance management (e.g. control of statistical real time counters)
- Configuration management (e.g. activation/deactivation SW and HW)
- Security management (e.g. user identification)

7 Capacity

7.1 General

When dimensioning an AuC it is essential to know the capacity figures for the specific network. The node must be able to handle not only busy hour traffic, but also peak load. The Ericsson AuC is designed as a high capacity node in order to cope with these extreme situations.

The AuC can handle up to 8 million subscribers. The capacity of an AuC has to be calculated for each network and for each functional level. The AuC capacity is dependent on the processor limit, but also on the required memory amount. The following factors have influence on the maximum capacity of the AuC:

- Dimensioning
- Node configuration

7.2 Dimensioning

The number of subscribers supported in the AuC node depends on the behaviour of the subscribers, the services used and the network design. The dimensioning of the HW families of AuC product packages has been based on a default traffic model.

8 Configuration

The HW Platform is shared by the different SW applications residing in the node, either an AuC combined with HLR or HLR/FNR node or a stand-alone AuC. The hardware structure also permits several applications residing in the same node, occupying a small footprint, and offering a powerful and reliable product.

8.1 Combined AuC

Using a configuration where the AuC is combined with the HLR (or HLR/FNR) means that the HW resources can be efficiently shared. For example it is possible to share signalling resources and to communicate with the HLR internally without need of any extra signalling links or signalling HW. It is also possible to share operation and maintenance equipment.

Observe that when the number of subscribers grows in the network and in the AuC, the AuC does not significantly increase the processor load on the HLR, since AuC authentication triplet generation is distributed to regional processors.

When combined, AuC may also serve other external HLRs, apart from the one it is combined with, through external interfaces.

8.2 Stand-alone AuC

AuC can be defined in a stand-alone configuration taking benefit from all the platform advantages. The existing AuCs can be moved from the combined nodes and put them into stand-alone.

Depending on how big the network reaches it can in many cases be useful to have a stand-alone AuC supporting other HLR configurations. Using a stand-alone AuC, operators benefit from all the AXE 10 advantages, but at the same time, free up resources from the HLR, even though the AuC application is not very capacity consuming, per se.

Consequently, with stand-alone AuCs, the subscriber data is concentrated- thus facilitating security management.

9 Acronyms and abbreviations

AM	Application Modularity
AuC	Authentication Centre
A3	Cryptographic algorithm that produces SRES using RAND and Ki
A8	Cryptographic algorithm that produces Kc using RAND and Ki
CAS	Customer Administration System
CCS	Common Channel Signalling Subsystem
CNOS	Circuit switched Network Operation Support system
HLR	Home Location Register
Kc	Cipher Key
Ki	Subscriber Authentication Key
IMSI	International Mobile Subscriber Identity
MAP	Mobile Application Part
MTP	Message Transfer Protocol
OSS	Operation and Support System
RAND	Random Number
SCCP	Signalling Connection Control Part
SOG	Service Order Gateway
SRES	Sign Response
TCAP	Transaction Capabilities Application Part

