AUC-10 GARP
Cryptographic Module

HW Version: ROJ 208 16/3 R1A/1
FW Version: CXC 106 0272 R1C

FIPS 140-2
Non-Proprietary Security Policy

Level 1

Revision B
April 30, 2008

ERICSSON

TABLE OF CONTENTS

1 AUC-10 GARP Cryptographic Module Overview

The AUC-10 GARP Cryptographic Module (CM) is a multi-chip embedded module composed of the AGEN2R WCDMA Authentication Generator software binary executing on an Ericsson proprietary Generic Application Regional Processor (GARP) board using the proprietary RAZOR operating system environment. The RAZOR OS includes the OSE Delta kernel along with other extensions such as memory management, error handling or program handling.

The GARP board is a processor designed to operate in the AXE 810 telephony equipment platform.

The AUC-10 GARP Cryptographic Module (CM) consists of the following components:

AUC-10 GARP CM Components	Version	Component Type
GARP Hardware (GARP-1/3)	ROJ 208 16/3 R1A/1	HW
CORE_PBEM_FIPS	CXC 106 0272 R1C	FW

The AGEN2R is the application running the cryptographic services provided by the module and is a component of the CORE_PBEM_FIPS FW component.

The AUC-10 GARP CM is part of the telephony solution that generates data used to provide the main security features in GSM/WCDMA networks as defined by the 3rd Generation Partnership Project (3GPP) which defines that standards used by the telephony industry for standards for the 3G networks (WCDMA and GSM).

The AUC-10 GARP CM cryptographic boundary is the GARP board and the physical boundary is also the GARP board.

The GARP board is placed in the Generic Ericsson Magazine (GEM).

Figure 1: Example of GEM Magazine

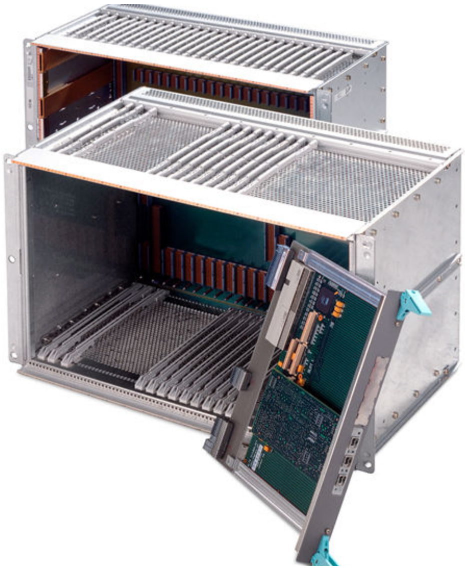


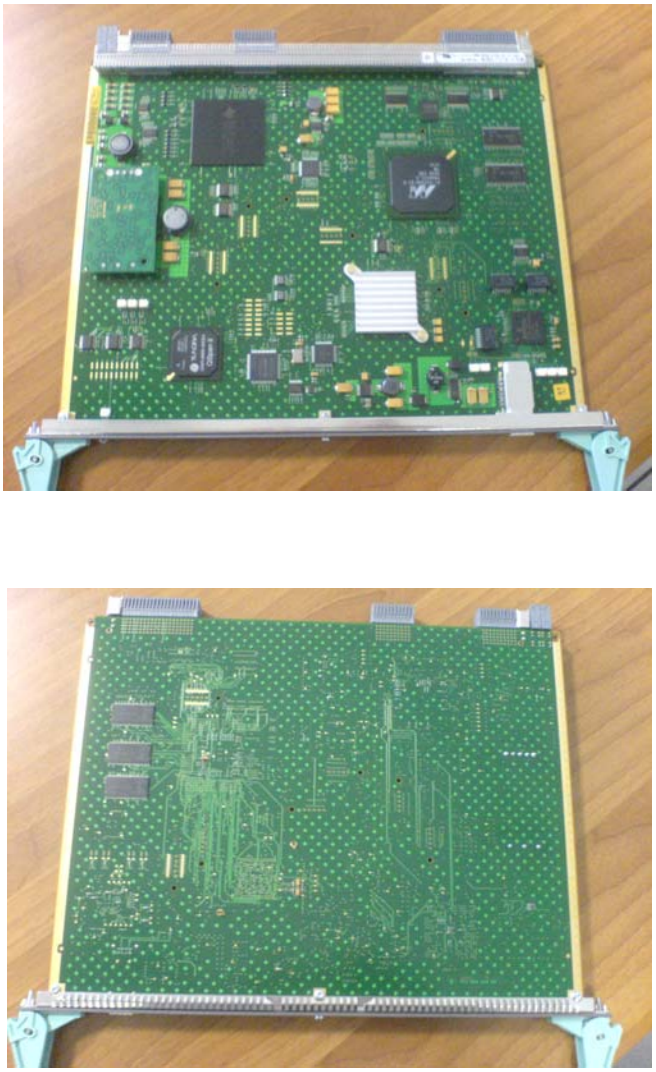
Figure 2: Example of GARP Board Placement in GEM Magazine

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
SCB-RP/3	**Dummy Unit**	**Dummy Unit**	**GARP-1/3 for AuC CM**	**Dummy Unit**	**GARP-1/3 for AuC CM**	**Dummy Unit**	**Dummy Unit**	**Dummy Unit**	**Dummy Unit**	**Dummy Unit**	**Dummy Unit**	**Dummy Unit**	**Dummy Unit**	**GARP-1/3 for AuC CM**	**GARP-1/3 for AuC CM**	**Dummy Unit**	**Dummy Unit**	**Dummy Unit**	**Dummy Unit**	**Dummy Unit**	**Dummy Unit**	**Dummy Unit**	**Dummy Unit**	**Dummy Unit**	**SCB-RP/3**
X02 X05	X08	X11	X14	X17	X20	X23	X26	X29	X32	X35	X38	X41	X44	X47	X50	X53	X56	X59	X62	X65	X68	X71	X74	X77	X80 X83

order of allocation of AUC-10 GARP CM → 3 5 14 15

The device provides network interfaces for data input and output.

Figure 3: GARP Board – Front and Back

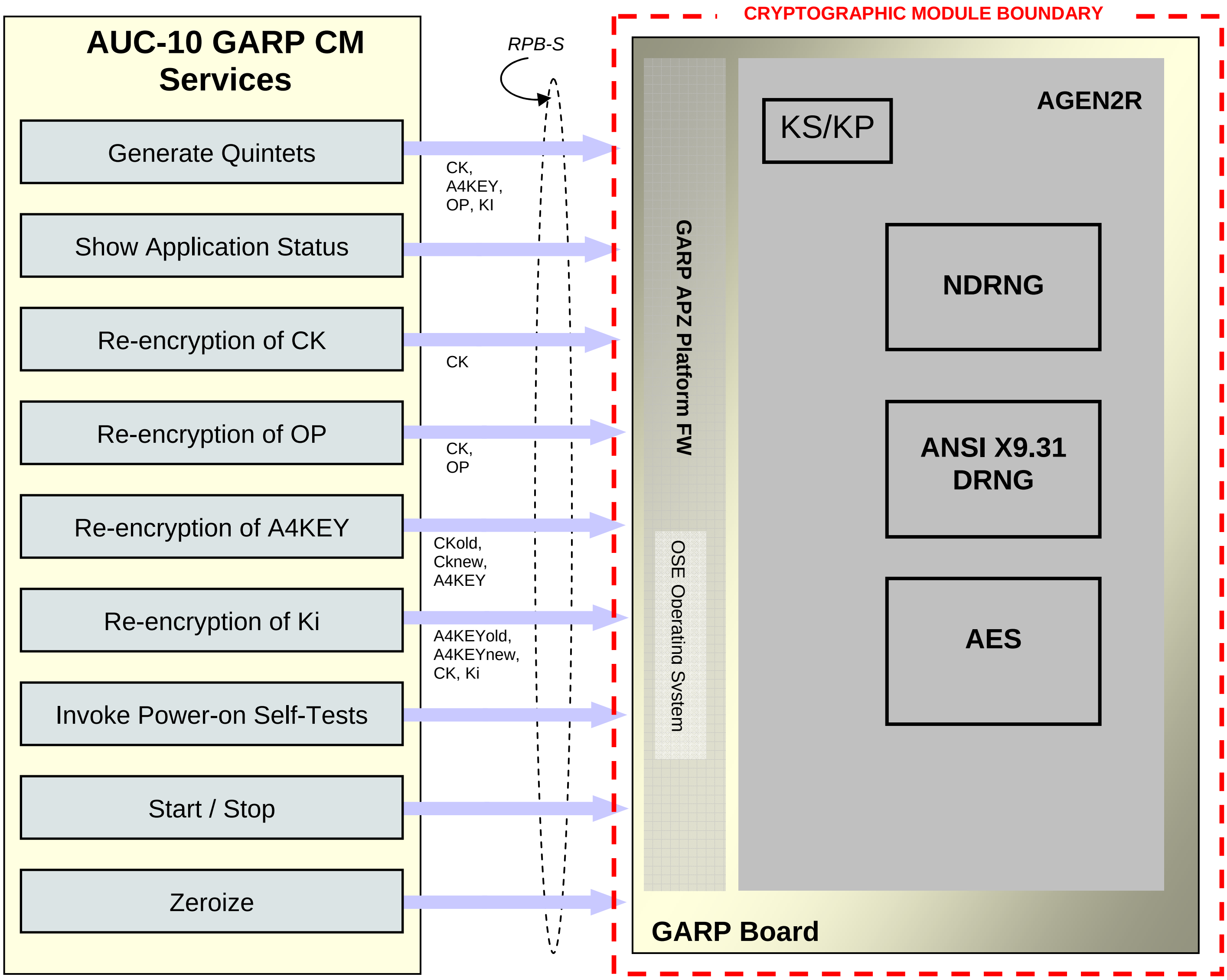


The AUC application firmware and the GARP platform/OS firmware is pre-loaded on the GARP board. New software executables cannot be loaded on the CM. Zeroization makes the GARP board unusable.

The diagram in Figure 4 illustrates the logical interfaces as well as defining the cryptographic boundary.

All cryptographic keys and CSPs that are input to the cryptographic module are entered in an encrypted form.

Figure 4: AUC Cryptographic Module Boundary



2 Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

3 Modes of Operation

Approved mode of operation

The AUC-10 GARP CM only supports the FIPS mode of operation.

The cryptographic module supports the following FIPS Approved algorithm:

- AES 128 ECB for encryption (FIPS-197)
- NIST-Recommended RNG based on ANSI X9.31 Appendix A.2.4 using the AES 128 Algorithm

The cryptographic module supports the following non-approved algorithm:

- Non-approved RNG for seed and seed key generation

Non-FIPS mode of operation

The AUC-10 GARP CM does not support a non-FIPS mode of operation.

4 Ports and Interfaces

The AUC-10 GARP CM physical ports are those provided by the GARP board, including the Ethernet ports and RP bus.

The AUC-10 GARP CM logical interface is an API defined by the Ericsson signals used by the module.

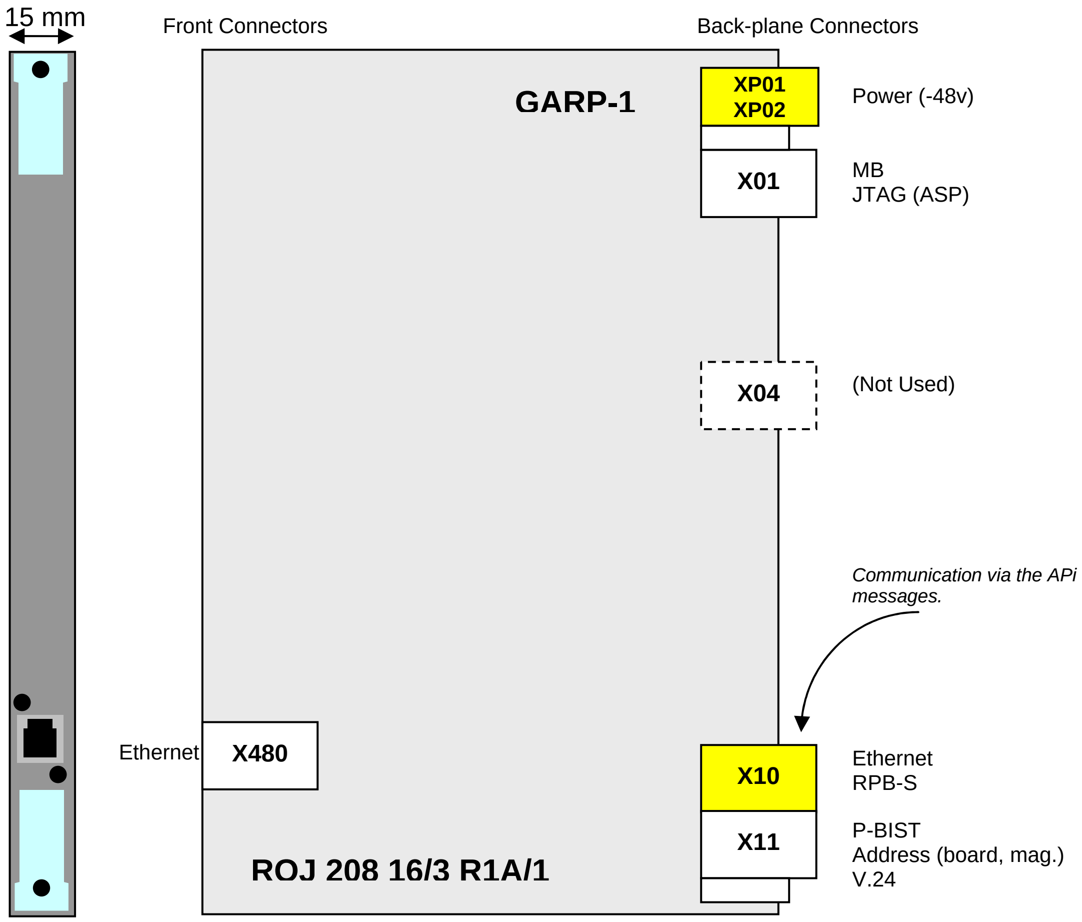
Table 2: AUC CM Logical Interfaces

FIPS 140-2 Logical Interface	**AUC Cryptographic Module Logical Interface**	**GARP Physical Port**
Data Input Interface	The data input is data sent into the module though input API message	RP Bus (Ethernet Port) connected to the backplane in the GEM magazine
Data Output Interface	The data output is data sent out of the module through output API message	RP Bus (Ethernet Port) connected to the backplane in the GEM magazine
Control Input Interface	The control input interface is API messages that controls the module	RP Bus (Ethernet Port) connected to the backplane in the GEM magazine
Status Output Interface	API messages that indicate the status of the module Event log	RP Bus (Ethernet Port) connected to the backplane in the GEM magazine
Power Interface	The power interface to the GARP board.	XP01, XP02 (Power Port) connected to the backplane in the GEM magazine

Data output is inhibited by software. Before any data output is produced the state in the FSM is checked.

The GARP board provides the following physical ports and logical interfaces:

Figure 5: AUC-10 GARP CM Board Ports



The GARP board is provided with the following interfaces to the backplane:

- Two redundant -48 V
- X01: Maintenance Bus: Disabled
- X04: Not used
- X10: Ethernet, 10/100Base-TX (RPB-S, Regional Processor Bus)
- X11: P-BIST. Addressable Scan port
- X480: Ethernet, 10/100 Base-TX port available at the front connector

The AUC-10 GARP CM only uses the power (-48 V) and the X10 Ethernet RPB-S.

5 Identification and Authentication Policy

Assumption of roles

The AUC-10 GARP CM supports two operator roles for accessing the AUC CM (See Table 3).

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Not Applicable	Not Applicable
Cryptographic-Officer	Not Applicable	Not Applicable

Authentication

The AUC cryptographic module itself does not perform authentication of operator or network requests.

6 Access Control Policy

6.1 Roles

The AUC-10 GARP CM module receives requests for services via data input and control input interfaces (API messages). The AUC CM itself does not provide authentication of service requests (not required for FIPS 140-2 Security Level 1).

The roles selected are implicit based on the service requested.

All CSP values entered into the CM are encrypted.

6.2 Services

The AUC-10 GARP CM module receives requests for services via data input and control input interfaces (API messages). All CSP values are entered in encrypted form. All services affecting the CSPs in the AUC-10 GARP CM module are limited to ***User*** and ***Cryptographic Officer (CO)*** roles.

Table 4 –Authorized Module Services

Service	Description	Role
Generate of WCDMA quintets	Request one or more quintets for a specific subscriber.	User
Zeroize CSPs	CSPs stored in the AUC-10 GARP CM are zeroized. All keys, including keys temporarily stored in RAM, are zeroized immediately. Further, the two hardcoded keys, Ks and Kp, are overwritten as well which renders the module unusable.	User
Re-encryption of Customer key (CK)	Re-encrypts CK using AES algorithm and Ks	User
Adaptation of Operator Variant Algorithm Configuration Field (OP)	Re-encrypts OP using AES algorithm and CK	User
Adaptation of the A4KEY	Re-encrypts A4KEYs using AES algorithm and CK	User
Adaptation of the Subscriber key (Ki)	Re-encrypts Ki using AES algorithm (AES) and A4KEY	User
Application status monitoring	Outputs the status of the AUC-10 GARP on the status output interface	User
Start/Stop	Activates/Passivates the CM	Crypto Officer
Invoke Power On Self Tests	Reset the GARP board	User

6.3 Cryptographic Keys and Critical Security Parameters (CSPs)

Table 5 - Cryptographic Keys and CSPs

Key / CSP	Description
Pre-shared Key (***Kp***)	Key used to encrypt and decrypt the encrypted CK entered into the AUC. Known by the AUC-10 GARP CM and the user generating the CK.
Ericsson Secret Key (***Ks***)	Key used to encrypt and decrypt the encrypted CK using AES 128. Known only by the AUC-10 GARP CM.
Customer Key ***(CK)***	This key is used to encrypt and decrypt the CSPs **OP** and **A4KEY** keys used in the AUC.
Operator dependent Variant Algorithm Configuration Field ***(OP)***	This key is used by the customer to personalize those Function Sets (FSETs) which support its usage in the generation of quintets defined by 3GPP[1] standards.
Subscriber Authentication Key (***Ki***)	AES 128 bit key used in the FSET function to derive the authentication vector
A4 Key ***(A4Key)***	A4 encrypt / decrypt Key for the encrypted Subscriber Key.

[1] 3GPP is the 3rd Generation Partnership Project which defines that standards used by the Ericsson AUC in the generation of quintets for authentication and authorization of commercial handsets in the WCDMA network.

6.4 Definition of CSPs Modes of Access

Table 6 defines the relationship between access to CSPs and the different AUC-10 GARP CM services. The details of the service descriptions are shown in Table 4. It should be noted that the actual CSPs are stored outside the AUC-10 GARP CM and are only sent to the AUC-10 GARP CM for generation of quintets and when changing keys used to encrypt other keys, e.g. when the A4KEY value is changed, all subscriber keys (***Ki***s) must be re-encrypted for storage with the new A4KEY.

Table 6 – Specification of Service Access with Inputs & Outputs

Service	Role	Affected Keys and CSPs	Data Input	Data Output
Zeroize CSPs	***User***	***Ks, Kp***	N/A	N/A
Re-encryption of CK	***User***	***CK, Ks, Kp***	Encrypted data	Encrypted data
Adaptation of OP	***User***	***OP, CK***	Encrypted data	Encrypted data
Adaptation of A4Key	***User***	***A4KEY, CK***	Encrypted data	Encrypted data
Adaptation of Ki	***User***	***A4KEY, Ki***	Encrypted data	Encrypted data
Generate Quintet	***User***	***CK, OP, A4KEY, Ki, Ks, Kp***	Encrypted data	Plaintext data[2]
Application status	***User***	N/A	N/A	N/A
Start/Stop	***CO***	N/A	N/A	
Invoke Power Up Self Tests	***User***	N/A	N/A	N/A

[2] The quintet does not contain cryptographic data related to the AUC-10 GARP CM and it is sent out in plaintext form.

7 Operational Environment

The FIPS 140-2 Area 6 *Operational Environment* requirements are not applicable because the AUC-10 GARP CM does not contain a modifiable operational environment.

8 Security Rules

The AUC-10 GARP CM design corresponds to the following cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1 The cryptographic module shall provide at least two distinct operator roles. These are the User role and the Cryptographic-Officer role.

2 Status information shall not contain CSPs or sensitive data that, if misused, could lead to a compromise of the module.

3 The cryptographic module shall perform the following tests:

A. Power up Self-Tests:

1. Cryptographic algorithm tests:
    a. AES Known Answer Test
    b. ANSI X9.31 RNG Known Answer Test
2. Software Integrity Test (16-bit Error Detection Code (EDC))

B. Conditional Self-Tests:

1. Continuous ANSI X9.31 Random Number Generator (RNG) test
2. Continuous non-approved RNG test

4 The results of the Self-Tests are available in the status output interface event log.

5 Data output shall be inhibited during self-tests, zeroization and error states.

6 The operator shall be able to initiate the power-up self-test by resetting the GARP board.

7 The cryptographic module does not support concurrent operators.

.

9 Physical Security Policy

9.1 Physical Security Mechanisms

A multi-chip embedded cryptographic module at Security Level 1 requires the following physical security mechanisms:

- Production-grade components with standard passivation.

The AUC-10 GARP CM uses production-grade components with standard passivation.

9.2 Design Assurances

Ericsson follows highly stabilized and popular design procedures. The design goes through many phases of review and inspections, and implementations undergo rigorous quality assurance testing.

Additionally, ClearCase Version 6.0 is used to provide configuration management for the AUC CM software and documentation. The ClearCase software provides access control, versioning, and logging.

Additional security is added for the AUC software within Ericsson due to the nature of the software in securing the identities of user equipment in large commercial operator environments and government customers.

10 Mitigation of Other Attacks Policy

The mitigation of other attacks is not applicable because the cryptographic module is not designed to mitigate specific attacks beyond the scope of FIPS 140-2.

11 Definitions and Acronyms

Term	Definition
3GPP	3rd Generation Partnership Project which defines that standards used by the telephony industry for standards for the 3G networks (WCDMA and GSM).
AKA	Authentication and Key Agreement – either GSM or UMTS which determines whether triplets or quintets are generated. The FIPS AUC only supports UMTS (quintets).
AUC	Authentication Centre – the network element in a WCDMA system that provides authentication of each UE that attempts to connect to the system.
AGEN2R	AGEN2 is responsible for the generation of the quintets and associated services. AGEN2 is composed of a CP unit (AGEN2U) and a RP unit (AGEN2R). The AGEN2R firmware executes on the GARP board.
AV	Authentication Vector – generated result of the FSETs using AUC CSPs. Also called quintet in 3GPP standards.
AXE	Ericsson proprietary telephony platform used to implement the AUC network element – currently the AXE 810 product line.
A4KEY	Internal AUC keys used to encrypt the Subscriber Key (Ki) for administration purposes. Reference by an A4IND index value.
CK	Internal AUC key used to encrypt and decrypt the OP key and the A4KEYs for administrative purposes.[3]
CP	Central Processor of the AXE 810 platform.
CSP	Critical Security Parameters
EDC	Error Detection Code is a checksum for data. The EDC can be used to identify errors in data based on a specific probability. A typical example of an EDC is the XOR or CRC checksum used in various data transmission protocols.
FSET	Function Set – a group of functions that use CSPs to create a WCDMA quintet used to verify the user equipment attempting to access the WCDMA network the AUC supports.
GARP	Generic Application Regional Processor
GSM	Global System for Mobile Communications - a digital cellular phone technology that is the predominant system in Europe.
IPSec	Internet Protocol Security provides security for transmission of sensitive information over unprotected networks such as the Internet.

[3] The acronym CK is also used by the 3GPP standards to identify the Cipher Key. The 3GPP CK is the result of the generation of the FSET but is not a critical security parameter in the AUC.

Term	Definition
Ki	128 bit Subscriber Key used to identify the device requesting authentication. In a mobile telephony network, this is the identifier programmed into the Subscriber Identity Module (SIM) smart card used to authenticate the mobile phone to the network.
Kp	Internal hard-coded private key used to encrypt and decrypt the **CK**
Ks	Internal hard-coded shared key used to encrypt and decrypt the **CK** for internal storage after receiving the CK from the operator.
OP	128-bit Operator Variant Algorithm Configuration Field that is a component of the functions f1, f1*, f2, f3, f4, f5 and f5* used to generate quintets as defined by 3GPP technical standards.
Quintet	UMTS authentication vector that is generated by using the standard 3GPP FSET and the Ki and OP keys for authentication of the UE. The transmission of the resulting values in the vector is outside the scope of the AUC CM.
RAZOR	An Operating System platform consisting of a number of Ericsson proprietary and OSE components combined into a complete OS for the GARP.
RP	Regional Processor
RPB-S	Serial Regional Processor Bus (Serial RP-Bus). All communication between the CP and the RPs is transported via the RP Bus. The serial RP Bus is divided into several branches.
UE	User Equipment
UMTS	Universal Mobile Telecommunications System - the GSM implementation of the third generation (3G) wireless phone system and will deliver audio and video to wireless devices anywhere in the world through fixed, wireless and satellite systems
WCDMA	Wideband Code Division Multiple Access – a type of 3G cellular network. Both UMTS and GSM are supported. The FIPS AUC is defined for UMTS systems only.