3GPP TSG SA WG3 Security — S3#32 **S3-040062**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda Item: SAGE

Source: TeliaSonera

Title: Specification of the A5/4 Encryption Algorithms for GSM and EDGE, and the GEA4 Encryption Algorithm for GPRS

Document for: Approval

1. Introduction

A5/3 and GEA3, as defined in TS 55.216, were originally designed such that it was possible to use different key lengths from 64 to 128 bits, through a parameter KLEN. However SA3 has agreed that it is sufficient that two key lengths are supported by the system, i.e. 64 bits and 128 bits. Thus a CR to TS 55.216.was approved to restrict A5/3 and GEA3 to 64 bit keys, in San Francisco (S3-030438)

A new algorithm identifier has also been defined for A5/4 and GEA4 with a key length set to 128 bits (in co-operation with CN1). A new specification - for A5/4 and GEA4 - was then needed and SA3 # 29 decided in San Francisco that this should be developed. This contribution offers the TS for A5/4 and GEA4.

2. Implications

For ciphering algorithms according to A5/4 and GEA4 to be implemented other specifications regarding signalling interfaces need tobe changed to allow for Kc with 128-bit size.

3. Proposal

The new TS for A5/4 and GEA4, as proposed here, to be approved by SA3 and then go to SA for approval.

4. References

TS 55.216

3GPP TSG SA WG3 Security — S3#32 **S3-040062**
09 - 13 February 2004, Edinburgh, Scotland, UK

3GPP TS ~~33~~.~~234~~ V0.~~7~~18.0 (2004~~3~~-02~~11~~2)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Service and System Aspects;
3G Security;
Specification of the A5/4 Encryption Algorithms for GSM and ECSD, and the GEA4 Encryption Algorithm for GPRS;
~~Wireless Local Area Network (WLAN) Interworking Security;~~
(Release 6)

Keywords

<keyword[, keyword]>

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

~~Introduction~~

~~WLAN is not a single radio technology, several different technologies fall into the category called WLAN. Existing industry standard is IEEE 802.11b operating at 2,4 GHz ISM band. New entrant for this same band is Bluetooth and technologies such as IEEE 802.11a and ETSI BRAN Hiperlan2 are being developed for the 5GHz band.~~

~~Despite the different radio technologies, all these WLAN systems are commonly used for transportation of IP datagrams. The specific WLAN technology used in each wireless IP network is not very visible for the layers above IP.~~

~~TSG SA WG3 will need to understand the models and mechanisms under which these technologies can be used to securely interwork with 3GPP networks.~~

1 Scope

This specification of the **A5/4** encryption algorithms for GSM and ECSD, and of the **GEA4** encryption algorithm for GPRS has been derived from ref [1]: 55.216 Specification of the **A5/3** Encryption Algorithms for GSM and ECSD, and the **GEA3** Encryption Algorithm for GPRS. The only essential change is the change of external key length input from 64 bits to 128 bits.

This document should be read in conjunction with the entire specification of the **A5/3** and **GEA3** algorithms:

- Specification of the **A5/3** Encryption Algorithms for GSM and ECSD, and the **GEA3** Encryption Algorithm for GPRS.
  Document 1: **A5/3** and **GEA3** Specifications.
- Specification of the **A5/3** Encryption Algorithms for GSM and ECSD, and the **GEA3** Encryption Algorithm for GPRS.
  Document 2: Implementors' Test Data.
- Specification of the **A5/3** Encryption Algorithms for GSM and ECSD, and the **GEA3** Encryption Algorithm for GPRS.
  Document 3: Design Conformance Test Data.

The normative part of the specification of the block cipher (**KASUMI)** on which the **A5/3, A5/4, GEA3** and **GEA4** algorithms are based can be found in [5].

~~The present document specifies the security architecture, trust model and security requirements for the interworking of the 3GPP System and WLAN Access Networks.~~

~~Recommendations of the appropriate mechanisms for user and network authentication, key management, service authorization, confidentiality and integrity protection of user and signalling data are also provided.~~

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] Specification of the **A5/3** Encryption Algorithms for GSM and ECSD, and the **GEA3** Encryption Algorithm for GPRS;
Document 1: **A5/3** and **GEA3** Specifications.

[2] Specification of the **A5/3** Encryption Algorithms for GSM and ECSD, and the **GEA3** Encryption Algorithm for GPRS;
Document 2: Implementors' Test Data.

[3] Specification of the **A5/3** Encryption Algorithms for GSM and ECSD, and the **GEA3** Encryption Algorithm for GPRS;
Document 3: Design Conformance Test Data.

[4] Specification of the 3GPP Confidentiality and Integrity Algorithms;
Document 1: *f8* and *f9* specifications.

[5] Specification of the 3GPP Confidentiality and Integrity Algorithms;
Document 2: **KASUMI** specification.

~~[1] 3GPP TR 22.934: " Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking;".~~

~~[2] 3GPP TR 23.934: "3GPP system to Wireless Local Area Network (WLAN) Interworking; Functional and architectural definition".~~

~~[3] RFC 2284, March 1998~~ Draft-ietf-eap-rfc2284bis-06.txt, October 2003 ~~"PPP Extensible Authentication Protocol (EAP)".~~

~~[4] draft-arkko-pppext-eap-aka-06~~11, ~~November~~ October ~~2002~~ 2003, ~~"EAP AKA Authentication".~~

~~[5] draft-haverinen-pppext-eap-sim-07~~12, ~~November~~October ~~2002~~2003, ~~"EAP SIM Authentication".~~

~~[6] IEEE Std 802.11i/D2.0, March 2002, "Draft Supplement to STANDARD FOR Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".~~

~~[7] RFC 2716, October 1999, "PPP EAP TLS Authentication Protocol".~~

~~[8] SHAMAN /SHA/DOC/TNO/WP1/D02/v050, 22-June-01, "Intermediate Report: Results of Review, Requirements and Reference Architecture".~~

~~[9] ETSI TS 101 761-1 v1.3.1B "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 1: Basic Data Transport".~~

~~[10] ETSI TS 101 761-2 v1.2.1C "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 2: Radio Link Control (RLC) sublayer".~~

~~[11] ETSI TS 101 761-4v1.3.1B "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 4 Extension for Home Environment".~~

~~[12] ETSI TR 101 683 v1.1.1 "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview".~~

~~[13] 3GPP TS 23.234 "3GPP system to Wireless Local Area Network (WLAN) Interworking System Description".~~

~~[14] RFC 2486, January 1999, "The Network Access Identifier".~~

~~[15] RFC 2865, June 2000, "Remote Authentication Dial In User Service (RADIUS)".~~

~~[16] RFC 1421, February 1993, "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures".~~

~~[17] Federal Information Processing Standard (FIPS) draft standard, "Advanced Encryption Standard (AES)", November 2001.~~

~~[18] 3GPP TS 23.003: "Numbering, addressing and identification".~~

~~[19] IEEE P802.1X/D11 June 2001, "Standards for Local Area and Metropolitan Area Networks: Standard for Port Based Network Access Control".~~

~~[20] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".~~

~~[21] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".~~

~~[22] SIM Access Profile, Interoperability Specification, version 0.95VD - d. Document no. CAR 020 SPEC/0.95cB~~

~~[23] draft-ietf-aaa-eap-023.txt, June October 2003, " Diameter Extensible Authentication Protocol (EAP) Application".~~

~~[24] RFC 3588, September 2003, "Diameter base protocol".~~

~~[25] RFC 3576, July 2003, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)".~~

~~[26] RFC 3579, September 2003, "RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)".~~

~~[27] draft-ietf-eap-keying-01.txt, November 2003, "EAP Key Management Framework".~~

~~[28] E. Barkan, E. Biham, N. Keller, "Instant Ciphertext-Only Cryptoanalysis of GSM Encrypted Communication", Crypto 2003, August 2003~~

3 INTRODUCTORY INFORMATION ~~Definitions, symbols and abbreviations~~

3.1 Introduction

In this document are specified three ciphering algorithms: **A5/4** for GSM, **A5/4** for ECSD, and **GEA4** for GPRS (including EGPRS). The algorithms are stream ciphers that are used to encrypt/decrypt blocks of data under a confidentiality key $\mathbf{K_C}$. Each of these algorithms is based on the **KASUMI** algorithm that is specified in reference [5]. The three algorithms are all very similar. We first define a core keystream generator function **KGCORE** (section 2); we then specify each of the three algorithms in turn (sections 3, 4 and 5) in terms of this core function.

Note that

- GSM A5/4 is the same algorithms as GSM A5/3 but with KLEN changed from 64 to 128 bits
- and ECSD A5/4 is the same algorithms as ECSD A5/3 but with KLEN changed from 64 to 128 bits
- and GEA 4 is the same algorithms as GEA3 but with KLEN changed from 64 to 128 bits

3.2 Notation

3.2.1 Radix

We use the prefix **0x** to indicate **hexadecimal** numbers.

3.2.2 Conventions

We use the assignment operator '=', as used in several programming languages. When we write

<*variable*> = <*expression*>

we mean that <*variable*> assumes the value that <*expression*> had before the assignment took place. For instance,

$$x = x + y + 3$$

means

(new value of x) becomes (old value of x) + (old value of y) + 3.

3.2.3 Bit/Byte ordering

All data variables in this specification are presented with the most significant bit (or byte) on the left hand side and the least significant bit (or byte) on the right hand side. Where a variable is broken down into a number of sub-strings, the left most (most significant) sub-string is numbered 0, the next most significant is numbered 1 and so on through to the least significant.

For example an n-bit **STRING** is subdivided into 64-bit substrings $\mathbf{SB_0}$,$\mathbf{SB_1}$**…**$\mathbf{SB_i}$ so if we have a string:

0x0123456789ABCDEFFEDCBA987654321086545381AB594FC28786404C50A37…

we have:

$\mathbf{SB_0}$ = 0x0123456789ABCDEF
$\mathbf{SB_1}$ = 0xFEDCBA9876543210
$\mathbf{SB_2}$ = 0x86545381AB594FC2
$\mathbf{SB_3}$ = 0x8786404C50A37…

In binary this would be:

00000001001000110100010101100111100010011010101111001101111011111111110…

with $\mathbf{SB_0}$ = 0000000100100011010001010110011110001001101010111100110111101111
$\mathbf{SB_1}$ = 1111111011011100101110101001100001110110010101000011001000010000
$\mathbf{SB_2}$ = 1000011001010100010100111000000110101011010110010100111111000010
$\mathbf{SB_3}$ = 10000111100001100100000000100110001010000101000110111…

3.2.4 List of Symbols

= The assignment operator.

$\oplus$ The bitwise exclusive-OR operation

|| The concatenation of the two operands.

KASUMI[x]$_k$ The output of the **KASUMI** algorithm applied to input value **x** using the key **k**.

X[i] The ith bit of the variable **X**. (**X = X[0] || X[1] || X[2] || ….. **).

Y{i} The ith octet of the variable **Y**. (**Y = Y{0} || Y{1} || Y{2} || ….. **).

Z$_i$ The ith 64-bit block of the variable **Z**. (**Z = Z_0 || Z_1 || Z_2 || …. **).

3.2.5 List of Variables

A a 64-bit register that is used within the **KGCORE** function to hold an intermediate value.

BLKCNT a 64-bit counter used in the **KGCORE** function.

BLOCK1 a string of keystream bits output by the **A5/4** algorithm — 114 bits for GSM, 348 bits for ECSD.

BLOCK2 a string of keystream bits output by the **A5/4** algorithm — 114 bits for GSM, 348 bits for ECSD.

BLOCKS an integer variable indicating the number of successive applications of **KASUMI** that need to be performed.

CA an 8-bit input to the **KGCORE** function.

CB a 5-bit input to the **KGCORE** function.

CC a 32-bit input to the **KGCORE** function.

CD a 1-bit input to the **KGCORE** function.

CE a 16-bit input to the **KGCORE** function.

CK a 128-bit input to the **KGCORE** function.

CL an integer input to the **KGCORE** function, in the range 1…2^{19} inclusive, specifying the number of output bits for **KGCORE** to produce.

CO the output bitstream (**CL** bits) from the **KGCORE** function.

COUNT a 22-bit frame dependent input to both the GSM and EDGE **A5/4** algorithms.

DIRECTION a 1-bit input to the **GEA4** algorithm, indicating the direction of transmission (uplink or downlink).

INPUT a 32-bit frame dependent input to the **GEA4** algorithm.

K_C the cipher key that is an input to each of the three cipher algorithms defined here. Although at the time of writing the standards specify that K_C is 64 bits long, the algorithm specifications here allow it to be of any length between 64 and 128 inclusive, to allow for possible future enhancements to the standards.

KLEN the length of K_C in bits, between 64 and 128 inclusive (see above).

KM a 128-bit constant that is used to modify a key. This is used in the **KGCORE** function.

KS[i] the ith bit of keystream produced by the keystream generator in the **KGCORE** function.

KSB$_i$ the ith block of keystream produced by the keystream generator in the **KGCORE** function. Each block of keystream comprises 64 bits.

M an input to the **GEA4** algorithm, specifying the number of octets of output to produce.

OUTPUT the stream of output octets from the **GEA4** algorithm.

~~3.1 Definitions~~

~~For the purposes of the present document, the following terms and definitions apply:~~

~~**Data origin authentication:** The corroboration that the source of data received is as claimed.~~

~~**Entity authentication:** The provision of assurance of the claimed identity of an entity.~~

~~**Key freshness:** A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.~~

~~**WLAN coverage:** an area where wireless local area network access services are provided for interworking by an entity in accordance with WLAN standards.~~

~~**WLAN-UE:** user equipment to access a WLAN interworking with the 3GPP system, including all required security functions.~~

~~[Editors note This WLAN-UE definition needs to be reflected in related specifications]~~

~~3.2 Abbreviations~~

~~For the purposes of the present document, the following abbreviations apply, [20] contains additional applicable abbreviations:~~

~~AAA Authentication Authorisation Accounting~~
~~AKA Authentication and Key Agreement~~
~~EAP Extensible Authentication Protocol~~
~~WLAN Wireless Local Area Network~~

4 CORE FUNCTION KGCORE~~Security Requirements for the 3GPP-WLAN Interworking~~

4.1 Introduction

In this section we define a general-purpose keystream generation function **KGCORE**. The individual encryption algorithms for GSM, GPRS and ECSDwill each be defined in subsequent sections by mapping the relevant inputs to the inputs of **KGCORE**, and mapping the output of **KGCORE** to the relevant output.

4.2 Inputs and Outputs

The inputs to **KGCORE** are given in table 1, the output in table 2:

Parameter	Comment
CA	8 bits **CA[0]…CA[7]**
CB	5 bits **CB[0]…CB[4]**
CC	32 bits **CC[0]…CC[31]**
CD	A single bit **CD[0]**
CE	16 bits **CE[0]…CE[15]** (see Note 1 below)
CK	128 bits **CK[0]….CK[127]**
CL	An integer in the range 1…2^{19} inclusive, specifying the number of output bits to produce

Table 1. **KGCORE** inputs

Parameter	Comment
CO	**CL** bits **CO[0]…CO[CL-1]**

Table 2. **KGCORE** output

Note 1: All the algorithms specified in this document assign a constant, all-zeroes value to **CE**.

More general use of **CE** is, however, available for possible future uses of **KGCORE**.

4.3 Components and Architecture

(See fig 1 Annex B)

The function **KGCORE** is based on the block cipher **KASUMI** that is specified in [2]. **KASUMI** is used in a form of output-feedback mode and generates the output bitstream in multiples of 64 bits.

The feedback data is modified by static data held in a 64-bit register **A**, and an (incrementing) 64-bit counter **BLKCNT**.

4.4 Initialisation

In this section we define how the keystream generator is initialised with the input variables before the generation of keystream bits as output.

We set the 64-bit register **A** to **CC** || **CB** || **CD** || **0 0** || **CA** || **CE** i.e. **A = CC[0]…CC[31] CB[0]…CB[4] CD[0] 0 0 CA[0]…CA[7] CE[0]…CE[15]**

We set the key modifier **KM** to 0x55555555555555555555555555555555

We set $\mathbf{KSB_0}$ to zero.

One operation of **KASUMI** is then applied to the register **A**, using a modified version of the confidentiality key.

$$\mathbf{A = KASUMI[\ A\ ]_{CK \oplus KM}}$$

4.5 Keystream Generation

Once the keystream generator has been initialised in the manner defined in section 0, it is ready to be used to generate keystream bits. The keystream generator produces bits in blocks of 64 at a time, but the number **CL** of output bits to produce may not be a multiple of 64; between 0 and 63 of the least significant bits are therefore discarded from the last block, depending on the total number of bits specified by **CL**.

So let **BLOCKS** be equal to (**CL**/64) rounded up to the nearest integer. (For instance, if **CL** = 128 then **BLOCKS** = 2; if **CL** = 129 then **BLOCKS** = 3.)

To generate each keystream block (**KSB**) we perform the following operation:

For each integer **n** with 1 ≤ **n** ≤ **BLOCKS** we define:

$$\mathbf{KSB_n = KASUMI[\ A \oplus BLKCNT \oplus KSB_{n-1}]_{CK}}$$

where **BLKCNT = n-1**

The individual bits of the output are extracted from $\mathbf{KSB_1}$ to $\mathbf{KSB_{BLOCKS}}$ in turn, most significant bit first, by applying the operation:

For **n** = 1 to **BLOCKS**, and for each integer ***i*** with 0 ≤ ***i*** ≤ 63 we define:

$$\mathbf{CO[((n-1)*64)+i] = KSB_n[i]}$$

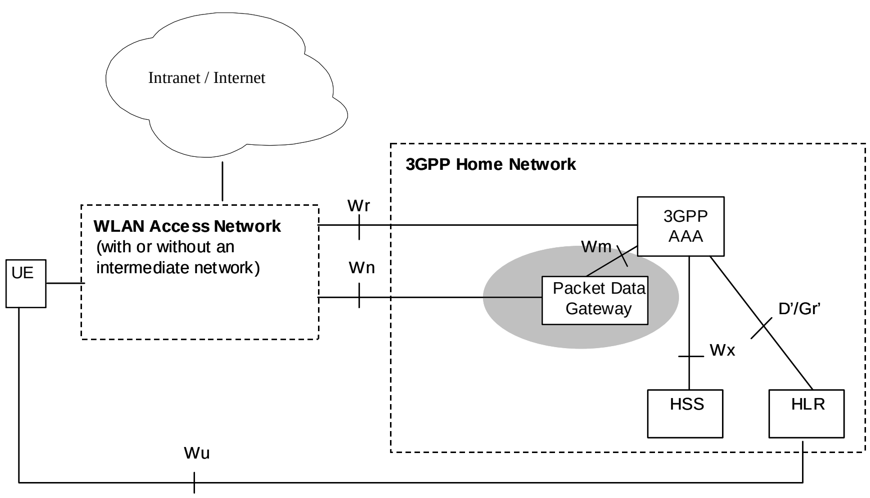
~~[Editor's note: This section shall have a description of the overall architecture for the 3G-WLAN interworking system and a list of the identified security requirements]~~

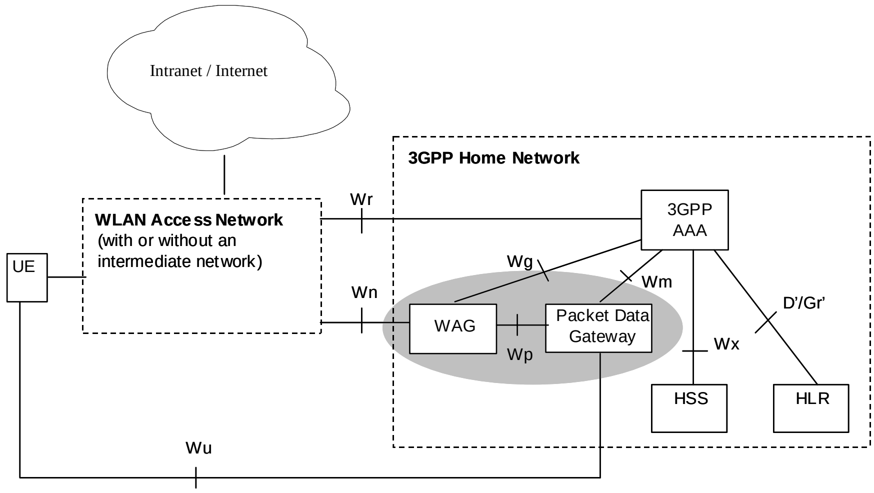
~~4.1Security architecture and Roles~~

~~Note: the pictures in this chapter may contain a shaded area, which surrounds the entities for scenario 3.~~

~~4.1.1Non roaming WLAN interworking Reference Model~~

~~The home network is responsible for access control and tunnel establishment.~~

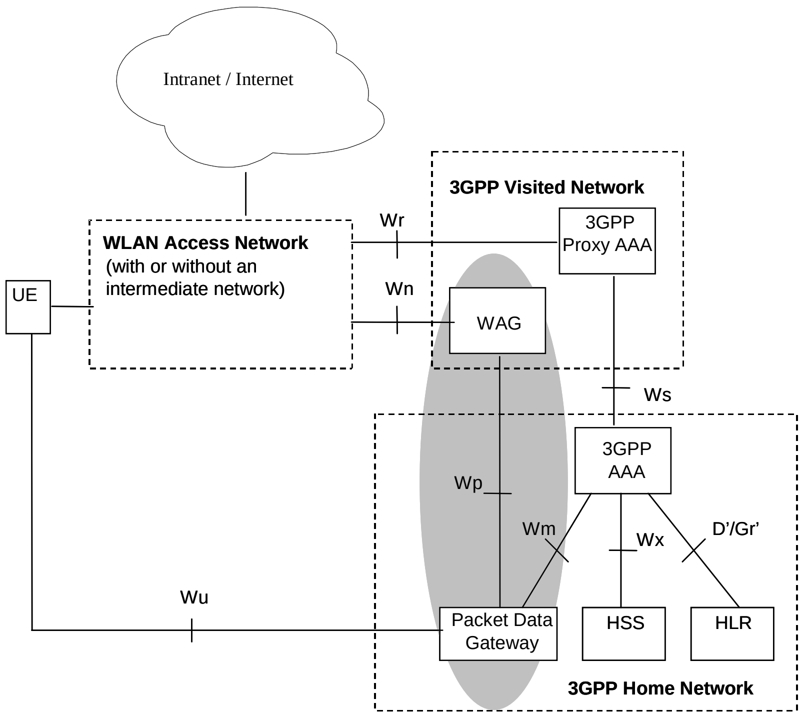


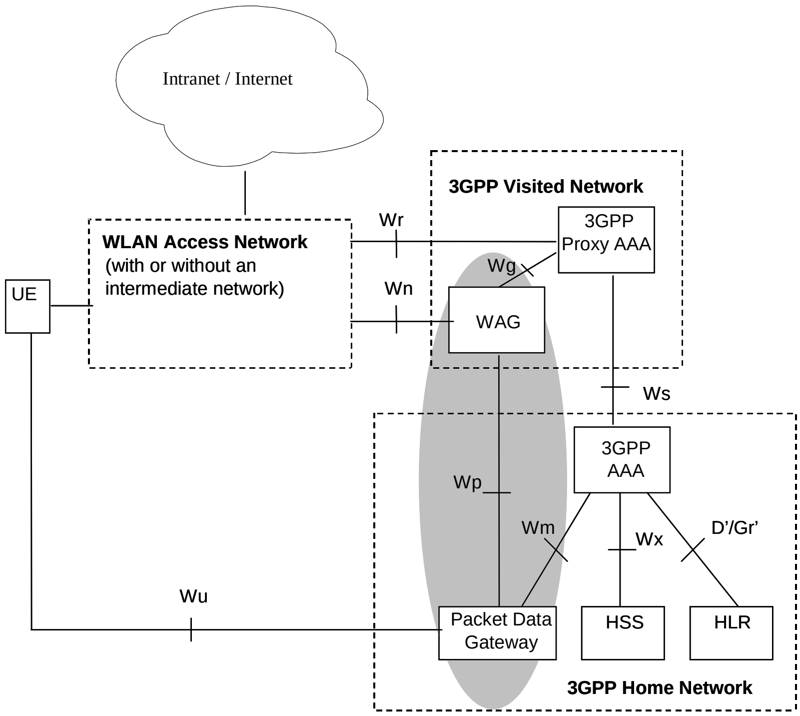


~~**Figure 4.1 Non roaming reference model**~~

~~4.1.2 Roaming WLAN Interworking Reference Model, access to HPLMN services~~

~~The home network is responsible for access control and tunnel establishment. The traffic is routed through the visited network (using the WAG).~~

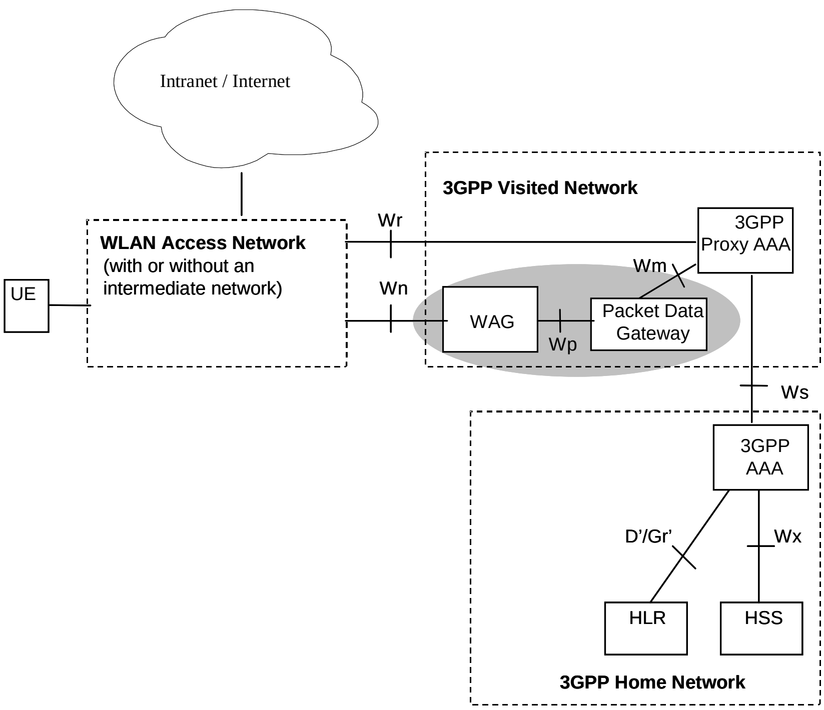


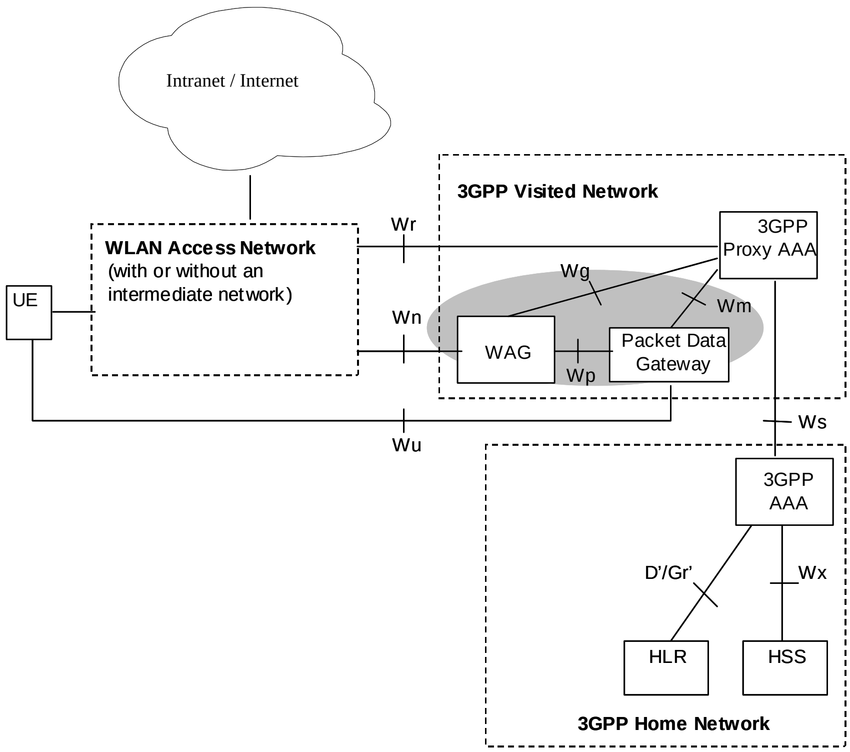


~~Figure 4.2 Roaming reference model, services in the HPLMN~~

~~4.1.3Roaming WLAN Interworking Reference Model, access to VPLMN services~~

~~The home network is responsible for access control, but the authorization decision of tunnel establishment will be taken by the 3GPP proxy AAA based on own information plus information received from the home network. The VPLMN will take part in tunnel establishment (either the WAG or the PDGW).~~





~~**Figure 4.3 Roaming reference model, services in the VPLMN**~~

~~4.1.4 Network elements~~

~~The list below describes the access control related functionality in the network elements of the 3GPP-WLAN interworking reference model:~~

- ~~the **WLAN UE,** equipped with a UICC (or SIM card), for accessing the WLAN interworking service):~~
  - ~~may be capable of WLAN access only;~~
  - ~~may be capable of both WLAN and 3GPP System access;~~
  - ~~may be capable of simultaneous access to both WLAN and 3GPP systems;~~

~~[Editors note: definition of simultaneous access still TBA with SA1- LS in S3-030169] Reply to SA2 in S3-030188 provides some clarification~~

  - ~~May be a laptop computer or PDA with a WLAN card, UICC (or SIM card) card reader, and suitable software applications;~~
  - ~~May be functionally split over several physical devices, that communicate over local interfaces e.g. Bluetooth, IR or serial cable interface;~~

~~[Editors Note: All these alternatives must be carefully studied from a security perspective.]~~

- ~~the **AAA proxy** represents a logical proxying functionality that may reside in any network between the WLAN and the 3GPP AAA Server. These AAA proxies are able to relay the AAA information between WLAN and the 3GPP AAA Server.~~
  ~~The number of intermediate AAA proxies is not restricted by 3GPP specifications. The AAA proxy functionality can reside in a separate physical network node, it may reside in the 3GPP AAA server or any other physical network node;~~

- ~~the **3GPP AAA server** is located within the 3GPP network. The 3GPP AAA server:~~
  - ~~retrieves authentication information from the HLR/HSS of the 3GPP subscriber's home 3GPP network;~~
  - ~~authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signalling may pass through AAA proxies;~~
  - ~~communicates authorisation information to the WLAN potentially via AAA proxies.~~
- ~~The **Packet Data Gateway (PDGW)** enforces tunnel authorization and establishment with the information received from the 3GPP AAA via the Wm interface.~~

~~*Note: The **WLAN Access Gateway (WAG)** responsibilities for security issues are related to tunnel establishment but this decision is pending to be taken.*~~

~~4.1.5 Reference points description~~

~~**Wr**~~

~~The reference point Wr connects the WLAN Access Network to the 3GPP Network (i.e. the 3GPP AAA Proxy in the roaming case and the 3GPP AAA server in the non-roaming case). The main purpose of the protocols implementing this interfaces is to transport authentication and keying information (WLAN UE - 3GPP network), and authorization information (WLAN AN – 3GPP network). The reference point has to accommodate also legacy WLAN Access Networks and thus should be Diameter [23,24] or RADIUS [15,26] based.~~

~~**Wx**~~

~~This reference point is located between 3GPP AAA Server and HSS. The main purpose of the protocols implementing this interface is communication between WLAN AAA infrastructure and HSS, and more specifically the etrieval of authentication vectors, e.g. for USIM authentication, and retrieval of WLAN access-related subscriber information from HSS. The protocol is either MAP or Diameter based.~~

~~**D'/Gr'**~~

~~This optional reference point is located between 3GPP AAA Server and pre-R6 HLR/HSS. The main purpose of the protocol implementing this interface is communication between WLAN AAA infrastructure and HLR, and more specifically the retrieval of authentication vectors, e.g. for USIM authentication, from HLR.. The protocol is MAP-based.~~

~~**Wn**~~

~~The definition of this reference point is for further study~~

~~**Wm**~~

~~This reference point is located between 3GPP AAA Server and Packet Data Gateway. The functionality of this reference point is to retrieve tunnelling attributes and UE's IP configuration parameters from/via Packet Data Gateway.~~

~~Ws~~

~~The reference point Ws connects the 3GPP AAA Proxy to the 3GPP AAA Server. This interface is similar to Wr, its main purpose is to transport authentication, authorization and related information in a secure manner.~~

~~4.2 Security Requirements~~

~~4.2.1 General~~

- ~~The authentication scheme shall be based on a challenge response protocol.~~
- ~~All long-term security credentials used for subscriber and network authentication shall be stored on UICC or SIM card.~~
- ~~Long term security credentials, which are stored on the UICC or SIM card, shall not leave the UICC or SIM card.~~
- ~~Mutual Authentication shall be supported.~~

~~4.2.2 Signalling and user data protection~~

- ~~The subscriber should have at least the same security level for WLAN access as for his current cellular access subscription.~~
- ~~3GPP systems should support authentication methods that support protected success/failure indications. Editors note: FFS if this is possible.~~
- ~~The selected WLAN (re-) authentication mechanisms for 3GPP interworking shall provide at least the same level of security as [33.102] for USIM based access.~~
- ~~The selected WLAN (re-authentication mechanism for 3GPP interworking shall provide at least the same level of security as [43.020} for SIM based access.~~
- ~~Selected WLAN Authentication mechanisms for 3GPP interworking shall support agreement of session keying material.~~
- ~~3GPP systems should provide the required keying material with sufficient length and the acceptable levels of entropy as required by the WLAN subsystem~~

~~[Editors note: LS (S3-030166) sent to IEEE 802.11 task group i on their requirements over key length and entropy of keying material]~~

- ~~Selected WLAN key agreement and key distribution mechanism shall be secure against man in the middle attacks.~~
- ~~Protection should be provided for WLAN authentication data and keying material on the Wr, Ws and Wx interfaces.~~
- ~~The WLAN technology specific connection between the WLAN-UE and WLAN AN shall be able to utilise the generated session keying material for protecting the integrity of an authenticated connection.~~

~~[Editor's note: Threats on the Wr interface are not clear yet, so protection on this interface is FFS]~~

~~4.2.3 User identity privacy~~

- ~~Any secret keys used in 3G AAA servers for the generation of pseudonyms should be infeasible for an attacker to recover.~~

~~-It shall be infeasible for an attacker to recover the corresponding permanent identity, given any pseudonym(s).~~

~~-It should be infeasible for an attacker to determine whether or not two pseudonyms correspond to the same permanent identity.~~

- ~~It shall be infeasible for an attacker to generate a valid pseudonym.~~

~~4.2.4 WLAN-UE Functional Split~~

~~4.2.4.1 General~~

~~In the case when the WLAN-UE, equipped with a UICC (or SIM card), for accessing the WLAN interworking service, is functionally split over several physical devices one device holding the card, and one device providing the WLAN access,, that communicate over local interfaces e.g. Bluetooth, IR or serial cable interface, then is shall be:~~

~~Possible to re-use existing UICC and GSM SIM cards; and~~

~~The UE functional split shall be such that attacking the CS or PS domain of GSM or UMTS by compromising the device providing the WLAN access is at least as difficult as attacking the CS or PS domain by compromising the card holding device.~~

~~[Editors note: The requirement is fulfilled if at least the master keys for EAP-AKA and EAP-SIM, as specified in [4] and [5], are computed either on the card or in the card holding device.]~~

~~[Editor's note: The termination point of EAP is for further study e.g. if. if EAP-AKA and EAP-SIM shall terminate in the TE e.g. laptop computer }. The decision on the termination point shall take into account the requirements in this subsection.}.LS sent to Bluetooth Architecture Review Board (BARB), Bluetooth CAR group and Bluetooth Security Expert Group in S3-030780]~~

~~4.2.4.2 Security requirements on local interface~~

~~The security functionality required on the terminal side for WLAN-3G interworking may be split over several physical devices that communicate over local interfaces. If this is the case, then the following requirements shall be satisfied:~~

- ~~Any local interface shall be protected against eavesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.~~

- ~~The endpoints of a local interface should be authenticated and authorised. The authorisation may be implicit in the security set-up.~~

- ~~The involved devices shall be protected against eavesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.~~

~~[*Editor's note:* New work item approved at SA3#28" U(SIM) Security Reuse by Peripheral Device on local Interfaces" (S3-030307). The Local interface" undetected modification" requirement - cryptographic requirement for short range e.g. Bluetooth is FFS pending the completion of this WI]~~

~~[Editors note: It was agreed at SA3#31 that for WLAN interworking, modification of EAP parameters on the Bluetooth interface will cause EAP to fail in the network or on the USIM. It was therefore agreed to remove the "undetected modification" requirement from this TS.]~~

~~4.2.4.3 Communication over local interface via a Bluetooth link~~

~~For SIM access via a Bluetooth link, the SIM Access Profile developed in BLUETOOTH SIG forum may be used, see [22].~~

~~[Editor note: The version of the SIM Access Profile specification in the reference needs to be updated, if SA3 decides that a new version is required.]~~

~~4.2.5 Link layer security requirements~~

~~[Editors note: This section is FFS, LS (S3-030167) sent to SA2 group. On 1) the need for requiring 802.11i in TS 23.234. SA2 to explain the impact (if any) a change of technology from 802.11i to WPA would have on the standardisation work. 2) SA2 to study the architectural impacts of implementing protection on Wr interface 3) SA2 to Investigate the importance of specifying specific WLAN technologies to be used for the WLAN access network]~~

~~Most WLAN technologies provide (optional) link-layer protection of user data. Since the wireless link is likely to be the most vulnerable in the entire system, 3GPP-WLAN interworking should take advantage of the link layer security provided by WLAN technologies. The native link-layer protection can also prevent against certain IP-layer attacks.~~

~~In order to set the bar for allowed WLAN protocols, 3GPP should define requirements on link layer security. The existing and work-in-progress WLAN standards can then be evaluated based on these requirements.~~

~~Areas in which requirements should be defined are:~~

~~4.2.5.1 Confidentiality and integrity protection of user data~~

- ~~Can user data be sent in the clear or is some kind of protection required?~~
- ~~Is it enough to integrity protect user data or should it be encrypted as well?~~
- ~~How strong must the WLAN security protocols be? Compare e.g. WEP, TKIP and CCMP in the case of 802.11 WLAN.~~

~~4.2.5.2 Protection of signalling~~

- ~~What implications on 3GPP-WLAN security does it have if the WLAN control signalling is unprotected? (Currently 802.11 management frames are not protected by 802.11i).~~

~~4.2.5.2 Key distribution, key freshness validation and key ageing~~

- ~~Can encryption keys generated during EAP authentication be used directly as encryption keys for the link layer or must there be a handshake between UE and AP to e.g. ensure freshness? (Like the 4-way handshake of 802.11i).~~

~~-What are the security implications of not having a UE-AP key handshake?~~

~~4.2.6UE-initiated tunneling~~

~~The security features that are expected in a tunnel from the UE to the VPLMN or HPLMN will be:~~

~~-Data origin authentication and integrity must be supported.~~

~~-Confidentiality must be supported.~~

~~-The 3GPP network has the ultimate decision to allow tunnel establishment, based on:~~

~~oThe level of trust in the WLAN AN and/or VPLMN~~

~~oThe capabilities supported in the WLAN UE~~

~~oWhether the user is authorized or not to access the services (in the VPLMN or HPLMN) the tunnel will give access to.~~

~~-The 3GPP network, in the setup process, decides the characteristics (encryption algorithms, protocols,...) under which the tunnel will be established.~~

~~*Note: Authorization for the tunnel establishment is decided by the 3GPP AAA and enforce by the PDGW or WAG. Whether this authorization information is protected or not is FFS.*~~

~~Working assumptions:~~

~~1.IPsec ESP will be used to protect the tunnels between UE and PDG required by scenario 3.~~

~~1.The security mechanisms used in context with the IP tunnel in scenario 3 are to be independent of the link layer security in scenario 2.~~

~~[Editors note: The independence requirement is not for security reasons). If the solution developed implies significant inefficiencies then this would be reported to SA WG2 for possible revision of this independence requirement.]~~

~~3.Further study will concentrate on IKE and IKEv2 for setting up the keys for IPsec ESP.~~

~~Further work identified for SA3~~

~~1.Define a profile of IPsec ESP for use with scenario 3.~~

~~2.Standardise the set-up of security associations for IPsec ESP between UE and PDG.~~

5 A5/4 ALGORITHM FOR GSM ENCRYPTION~~Security features~~

~~[Editor's note: This section shall explain the provided security features in detail]~~

5.1 Introduction

The GSM **A5/4** algorithm produces two 114-bit keystream strings, one of which is used for uplink encryption/decryption and the other for downlink encryption/decryption.

We define this algorithm in terms of the core function **KGCORE**.

5.2 Inputs and Outputs

The inputs to the algorithm are given in table 3, the output in table 4:

Parameter	Size (bits)	Comment
COUNT	22	Frame dependent input **COUNT[0]…COUNT[21]**
$\mathbf{K_C}$	KLEN	Cipher key $\mathbf{K_C}$**[0]…** $\mathbf{K_C}$**[KLEN-1]**, where **KLEN** is in the range 64…128 inclusive (see Notes 1 and 2 below)

Table 3. GSM **A5/4** inputs

Parameter	Size (bits)	Comment

BLOCK1	114	Keystream bits **BLOCK1[0]…BLOCK1[113]**
BLOCK2	114	Keystream bits **BLOCK2[0]…BLOCK2[113]**

Table 4. GSM **A5/4** outputs

Note 1: The specification of the **A5/4** algorithm only allows KLEN to be of value 128.

Note 2: It must be assumed that $\mathbf{K_C}$ is unstructured data — it must not be assumed, for instance, that any bits of $\mathbf{K_C}$ have predetermined values.

5.3 Function Definition

(See fig 2 Annex B)

We define the function by mapping the GSM **A5/4** inputs onto the inputs of the core function **KGCORE**, and mapping the output of **KGCORE** onto the outputs of GSM **A5/4**.

So we define:

CA[0]…CA[7] = 0 0 0 0 1 1 1 1

CB[0]…CB[4] = 0 0 0 0 0

CC[0]…CC[9] = 0 0 0 0 0 0 0 0 0 0

CC[10]…CC[31] = COUNT[0]…COUNT[21]

CD[0] = 0

CE[0]…CE[15] = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

CK[0]…CK[KLEN-1] = $\mathbf{K_C}$**[0]…**$\mathbf{K_C}$**[KLEN-1]**

If **KLEN** < 128 then

CK[KLEN]…CK[127] = $\mathbf{K_C}$**[0]…**$\mathbf{K_C}$**[127 – KLEN]**

(So in particular if **KLEN** = 128 then **CK =** $\mathbf{K_C}$)

CL = 228

Apply **KGCORE** to these inputs to derive the output **CO[0]…CO[227]**.

Then define:

BLOCK1[0]…BLOCK1[113] = CO[0]…CO[113]

BLOCK2[0]…BLOCK2[113] = CO[114]…CO[227]

6 A5/4 ALGORITHM FOR ECSD ENCRYPTION

6.1 Introduction

The **A5/4** algorithm for ECSD produces two 348-bit keystream strings, one of which is used for uplink encryption/decryption and the other for downlink encryption/decryption.

We define this algorithm in terms of the core function **KGCORE**.

6.2 Inputs and Outputs

The inputs to the algorithm are given in table 5, the output in table 6:

Parameter	Size (bits)	Comment
COUNT	22	Frame dependent input **COUNT[0]…COUNT[21]**
$\mathbf{K_C}$	KLEN	Cipher key $\mathbf{K_C}$**[0]…** $\mathbf{K_C}$**[KLEN-1]**, where **KLEN** is in the range 64…128 inclusive (see Notes 1 and 2 below)

Table 5. ECSD **A5/4** inputs

Parameter	Size (bits)	Comment
BLOCK1	348	Keystream bits **BLOCK1[0]…BLOCK1[347]**
BLOCK2	348	Keystream bits **BLOCK2[0]…BLOCK2[347]**

Table 6. ECSD **A5/4** outputs

Note 1: The specification of the **A5/4** algorithm only allows KLEN to be of value 128

Note 2: It must be assumed that $\mathbf{K_C}$ is unstructured data — it must not be assumed, for instance, that any bits of $\mathbf{K_C}$ have predetermined values.

6.3 Function Definition

(See fig 3 Annex B)

We define the function by mapping the ECSD **A5/4** inputs onto the inputs of the core function **KGCORE**, and mapping the output of **KGCORE** onto the outputs of ECSD **A5/4**.

So we define:

CA[0]…CA[7] = 1 1 1 1 0 0 0 0

CB[0]…CB[4] = 0 0 0 0 0

CC[0]…CC[9] = 0 0 0 0 0 0 0 0 0 0

CC[10]…CC[31] = COUNT[0]…COUNT[21]

CD[0] = 0

CE[0]…CE[15] = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

CK[0]…CK[KLEN-1] = $\mathbf{K_C}$**[0]…**$\mathbf{K_C}$**[KLEN-1]**

If **KLEN** < 128 then

CK[KLEN]…CK[127] = K_C[0]…K_C[127 – KLEN]

(So in particular if **KLEN** = 128 then **CK = K_C**)

CL = 696

Apply **KGCORE** to these inputs to derive the output **CO[0]…CO[695]**.

Then define:

BLOCK1[0]…BLOCK1[347] = CO[0]…CO[347]

BLOCK2[0]…BLOCK2[347] = CO[348]…CO[695]

7 ~~Authentication of the subscriber and the network and Key Security Association Management~~

~~[Editor's note: This section shall deal with subscriber identity and authentication of the subscriber and Home Network/Serving Network. The authentication and key management mechanisms fulfilling the requirements in chapter 4 shall be listed here]~~

~~5.1.1 End to End WLAN Access Authentication (Scenario 2)~~

~~WLAN access A authentication signalling is executed between WLAN-UE and 3GPP AAA Server. This authentication signalling shall be independent on the WLAN technology utilised within WLAN Access network.. WLAN authentication signalling for 3GPP-WLAN interworking shall be based on Extensible Authentication Protocol (EAP) as specified in RFC 2284 (ref. [3])~~

~~5.1.2 Transport of authentication WLAN Access signalling over the WLAN Radio interface~~

~~WLAN authentication signalling is carried between WLAN-UE and WLAN Access Network by WLAN Access Technology specific protocols. These WLAN technology specific protocols shall be able to meet the security requirements set for WLAN Access control in 3GPP-WLAN interworking. To ensure multi-vendor interoperability these WLAN technology specific protocols shall conform to existing standards of the specific WLAN access technology. For IEEE 802.11 type of WLAN radio interfaces the WLAN radio interface shall conform to IEEE 802.11i standard (ref. [6]).~~

~~5.1.3 Transport of WLAN Access authentication signalling between the WLAN access network and the 3GPP AAA proxy server~~

~~WLAN Authentication signalling shall be transported over Wr reference point by standard mechanisms, which are independent on the specific WLAN technology utilised within the WLAN Access network. The transport of Authentication signalling over Wr reference point shall be based on standard Diameter[23,24] or RADIUS [15,26]protocols.~~

~~5.1.4 Transport of authentication signalling between the 3GPP AAA proxy server and the 3GPP AAA server~~

~~WLAN Authentication signalling shall be transported over Ws reference point by standard mechanisms.~~

~~5.1.5 Transport of WLAN Access authentication signalling between the 3GPP AAA server and the HSS~~

~~WLAN Authentication signalling shall be transported over Wx reference point by standard mechanisms.~~

5.1.6 User Identity Privacy in WLAN Access

User identity privacy (Anonymity) is used to avoid sending the cleartext permanent subscriber identity (NAI) and make the subscriber's connections unlinkable to eavesdroppers.

User identity privacy is based on temporary identities, or pseudonyms. The procedures for distributing, using and updating temporary identities are described in ref. [4] and [5]. Support of this feature is mandatory for implementations, but optional for use.

The AAA server generates and delivers the pseudonym to the WLAN-UE as part of the authentication process. The WLAN-UE shall not interpret the pseudonym, it will just store the received identifier and use it at the next authentication. Clause 6.4 describes a mechanism that allows the home network to include the user's identity (IMSI) encrypted within the pseudonym.

To avoid user traceability, the user should not be identified for a long period by means of the same temporary identity. On the other hand, the AAA server should be ready to accept at least two different pseudonyms, in case the WLAN-UE fails to receive the new one issued from the AAA server. The mechanism described in Clause 6.4 also includes facilities to maintain more than one allowed pseudonym.

If identity privacy is used but the AAA server cannot identify the user by its pseudonym, the AAA server requests the user to send its permanent identity. This represents a breach in the provision of user identity privacy. It is a matter of the operator's security policy whether to allow clients to accept requests from the network to send the cleartext permanent identity. If the client rejects a legitimate request from the AAA server, it will be denied access to the service.

[Editor's note: The use of PEAP with EAP/AKA and EAP/SIM is currently under consideration. If PEAP is used, the temporary identity privacy scheme provided by EAP/AKA and EAP/SIM is not needed.]

5.1.7 Re-authentication in WLAN Access

WLAN 802.1x/AAA re-authentication is performed between WLAN-UE and AAA server, through Ws and Wr interfaces.

NOTE:

The WLAN-AN maycan initiate the 802.1x/AAA re-authentication process periodically. The frequency of the 802.1x/AAA re-authentications is determined by a a timer counter which normally is set by O&M procedures in the WLAN-AN but it may can be sent to the WLAN-AN by the AAA server in a RADIUS or Diameter message (in the attribute RADIUS Session Timeout) or Diameter AVP Authorization-Lifetime).

The WLAN UE may initiate the 802.1x/AAA re-authentication process for example upon moving to a new access point. The WLAN UE may also initiate the 802.1x/AAA re-authentication periodically; however it is out of the scope how the UE determines the frequency of periodic 802.1x/AAA re-authentications.

The 3GPP AAA server may initiate the 802.1x/AAA re-authentication process upon some event (for example the amount of data reported in accounting messages exceeds some limit), or periodically, alternatively to the usage of the Session Timeout/Authorization-Lifetime. The frequency of periodic 802.1x/AAA re-authentications is determined by a timer, which is normally set by O&M procedures in the 3GPP AAA server.

NOTE:

If several elements (UE, WLAN AN, 3GPP AAA server) maintain timers for periodic 802.1x/AAA re-authentications, then the element that has the shortest timer will determine the frequency of periodic 802.1x/AAA re-authentications, because each element is able to initiate an 802.1x/AAA re-authentication.

At reception of the Session Timeoutthis attribute, or the Authorization-Lifetime AVP the, the WLAN-AN may substitute the previously set counter by the received one. Nevertheless, the 3GPP network does not have the certainitycertainty that the counter sent by the AAA server is enforced by the WLAN AN, since the latter may not support this feature (the reception and acceptance of the Session Timeout this attribute

~~or AVP). In this case, the WLAN AN will discard it and trigger the re-authentications in the period set by O&M procedures as mentioned before.~~

~~The 802.1x/AAA re-authentication process initiated by the WLAN AN will be performed either with an EAP SIM/AKA full authentication process or with an EAP SIM/AKA fast re-authentication process (from now on it will be simply called called EAP SIM/AKA re-authentication). When the process is triggered by the WLAN AN, it is the client's UE's decision to perform either a EAP SIM/AKA full authentication or a EAP SIM/AKA re-authentication (fast). This is indicated to the WLAN AN by sending either a pseudonym (EAP SIM/AKA full authentication) or a re-authentication id EAP SIM/AKA re-authentication(fast). Both processes are described in this TS.~~

~~The EAP SIM/AKA re-authentication process shall must be implemented together with the full authentication procedure, although its use is optional and depends on operators' polices.~~

~~NOTE:~~

~~These policies depend on the level of trust of the 3GPP operator and the WLAN AN, and the possible threats detected by an operator whichoperator, which may require a periodic refresh of keys. The full process description can be found in ref. [4] and [5].~~

~~*Note: it is still pending to define how the re-authentication id is generated.*~~

~~5.1.8 Security Association Management for UE-initiated tunnels (Scenario 3)~~

~~The tunnel endpoints, the UE and the PDG, are mutually authenticated when setting up the tunnel;~~

~~The tunnel set-up procedure results in security associations, which are used to provide confidentiality and integrity protection, as required according to sections 5.2 and 5.3, for data transmitted through the tunnel.~~

~~5.2 Confidentiality protection~~

~~[Editor's note: This section shall deal with what confidentiality protection that is provided between different nodes both inter domain, intra domain and the WLAN-UE. It shall justify the selected mechanisms (hop-by-hop or end-to-end) and protection at different layers]~~

~~5.2.1 Confidentiality protection in scenario 2~~

~~*Text to be added*~~

~~5.2.2 Confidentiality protection in scenario 3~~

~~It shall be possible to protect the confidentiality of IP packets sent through a tunnel between the UE and the PDG.~~

~~5.3 Integrity protection~~

~~[Editor's note: This section shall deal with what integrity protection that is provided between different nodes both inter domain, intra domain and the WLAN-UE. It shall justify the selected mechanisms (hop-by-hop or end-to-end) and protection at different layers]~~

~~5.3.1 Integrity protection in scenario 2~~

~~*text to be added*~~

~~5.3.2 Integrity protection in scenario 3~~

~~The integrity of IP packets sent through a tunnel between the UE and the PDG shall be protected.~~

~~5.4 Visibility and configurability~~

~~[Editor's note: This section shall contain what the subscriber shall be able to configure and what is visible for the subscriber regarding the actual protection the subscriber is provided with.]~~

~~5.5 Immediate Service Termination~~

~~The AAA server initiates immediate service termination when some events may require stopping user's activity (end of subscription, expiration of charging account, etc.). This process can be initiated at any time by the AAA server with the Diameter command Diameter-Abort-Session-Request and Diameter-Abort-Session-Answer (the Ws interface is implemented with Diameter protocol) as specified in [24]. The AAA proxy will just forward this procedure to the WLAN AN through Wr interface if the latter supports Diameter. If it supports appropriate RADIUS extensions,, the AAA proxy will map the procedure to the RADIUS messages Disconnect-Request and Disconnect-Response as specified in [25].~~

GEA4 ALGORITHM FOR GPRS ENCRYPTION

7.1 Introduction

The GPRS **GEA4** algorithm produces an M-byte keystream string. M can vary; in this specification we assume that M will never exceed 2^{16} = 65536.

We define this algorithm in terms of the core function **KGCORE**.

7.2 Inputs and Outputs

The inputs to the algorithm are given in table 7, the output in table 8:

Parameter	Size (bits)	Comment
INPUT	32	Frame dependent input **INPUT[0]…INPUT[31]**
DIRECTION	1	Direction of transmission indicator **DIRECTION[0]**
$\mathbf{K_C}$	KLEN	Cipher key $\mathbf{K_C}$**[0]…** $\mathbf{K_C}$**[KLEN-1]**, where **KLEN** is in the range 64…128 inclusive (see Notes 1 and 2 below)
M		Number of octets of output required, in the range 1 to 65536 inclusive

Table 7. **GEA4** inputs

Parameter	Size (bits)	Comment
OUTPUT	8**M**	Keystream octets **OUTPUT{0}…OUTPUT{M-1}**

Table 8. **GEA4** outputs

Note 1: The specification of the **GEA4** algorithm only allows KLEN to be of value 128.

Note 2: It must be assumed that $\mathbf{K_C}$ is unstructured data — it must not be assumed, for instance, that any bits of $\mathbf{K_C}$ have predetermined values.

7.3 Function Definition

(See fig 4 Annex B)

We define the function by mapping the **GEA4** inputs onto the inputs of the core function **KGCORE**, and mapping the output of **KGCORE** onto the outputs of **GEA4**.

So we define:

CA[0]…CA[7] = 1 1 1 1 1 1 1 1

CB[0]…CB[4] = 0 0 0 0 0

CC[0]…CC[31] = INPUT[0]…INPUT[31]

CD[0] = DIRECTION[0]

CE[0]…CE[15] = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

CK[0]…CK[KLEN-1] = K_C[0]…K_C[KLEN-1]

If **KLEN** < 128 then

CK[KLEN]…CK[127] = K_C[0]…K_C[127 – KLEN]

(So in particular when **KLEN** = 128 then **CK = K_C**)

CL = 8**M**

Apply **KGCORE** to these inputs to derive the output **CO[0]…CO[8M-1]**.

Then for 0 ≤ ***i*** ≤ **M-1** define:

OUTPUT{*i*} = CO[8*i*]…CO[8*i* + 7]

where **CO[8*i*]** is the most significant bit of the octet.

ANNEX A (informative)
Specification of the 3GPP Confidentiality Algorithm *f*8

A.1 Introduction

The algorithms defined in this specification have been designed to have much in common with the 3GPP confidentiality algorithm, to ease simultaneous implementation of multiple algorithms. To clarify this, a specification of ***f*8** is given here in terms of the core function **KGCORE**. For the definitive specification of ***f*8**, the reader is referred to [5].

A.2 Inputs and Outputs

The inputs to the algorithm are given in table A.1, the output in table A.2:

Parameter	Size (bits)	Comment
COUNT	32	Frame dependent input **COUNT[0]…COUNT[31]**
BEARER	5	Bearer identity **BEARER[0]…BEARER[4]**
DIRECTION	1	***Direction of transmission*** *DIRECTION[0]*
CK	128	Confidentiality key **CK[0]…CK[127]**
LENGTH		The number of bits to be encrypted/decrypted (1-20000)

Table A.1. ***f8*** inputs

Parameter	Size (bits)	Comment
KS	1-20000	Keystream bits **KS[0]…KS[LENGTH-1]**

Table A.2. ***f8*** output

Note: The definitive specification of ***f*8** includes a bitstream **IBS** amongst the inputs, and gives the output as a bitstream **OBS**; both of these bitstreams are **LENGTH** bits long. **OBS** is obtained by the bitwise exclusive-or of **IBS** and **KS**. We present just the keystream generator part of ***f*8** here, for closer comparison with **A5/4** and **GEA4**.

A.3 Function Definition

(See fig 5 Annex B)

We define the function by mapping the ***f*8** inputs onto the inputs of the core function **KGCORE**, and mapping the output of **KGCORE** onto the outputs of ***f*8**.

So we define:

CA[0]…CA[7] = 0 0 0 0 0 0 0 0

CB[0]…CB[4] = BEARER[0]…BEARER[4]

CC[0]…CC[31] = COUNT[0]…COUNT[31]

CD[0] = DIRECTION[0]

CE[0]…CE[15] = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

CK[0]…CK[127] = CK[0]…CK[127]

CL = LENGTH

Apply **KGCORE** to these inputs to derive the output **CO[0]…CO[LENGTH-1]**.

Then define:

KS[0]…KS[LENGTH-1] = CO[0]…CO[LENGTH-1]

ANNEX B (informative) Figures of the Algorithms

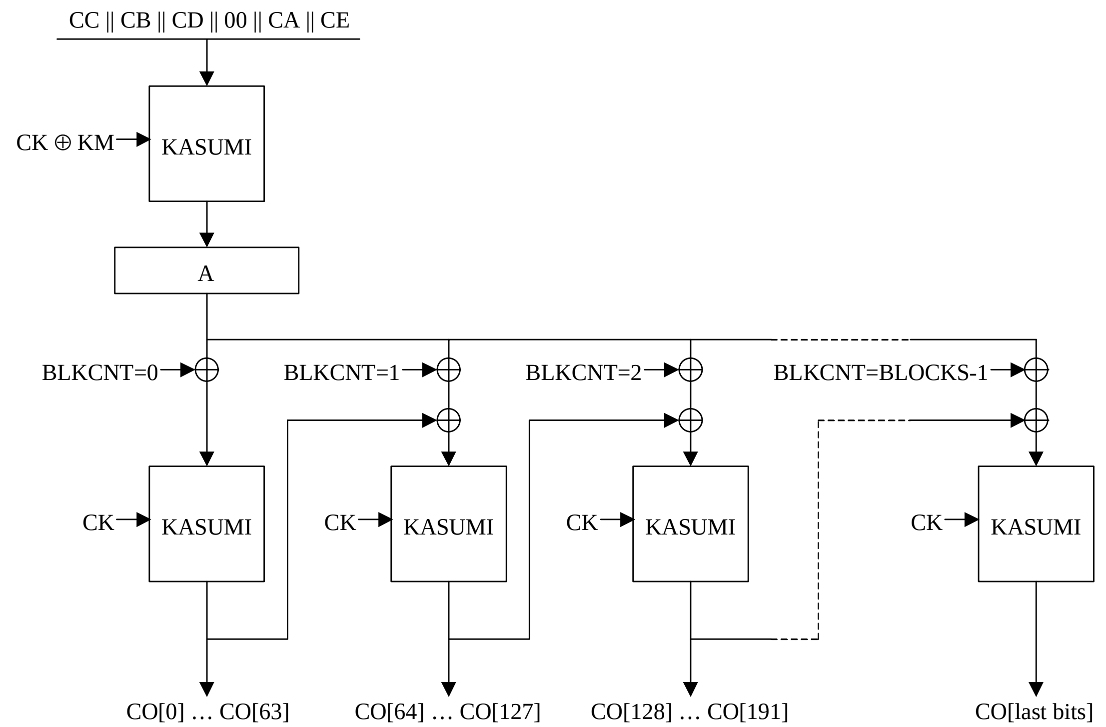


Figure 1: **KGCORE** Core Keystream Generator Function

Note: **BLKCNT** is specified as a 64-bit counter so there is no ambiguity in the expression **A ⊕ BLKCNT ⊕ KSB**$_{n-1}$ where all operands are of the same size. In a practical implementation, where the keystream generator is required to produce no more than a certain number of bits, only the least significant few bits of the counter need to be realised.

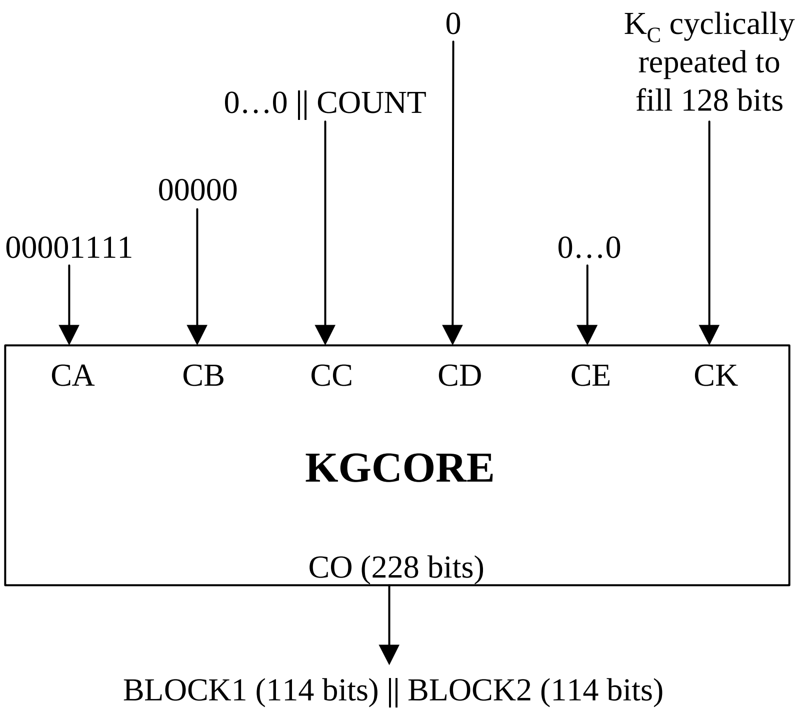


Figure 2: GSM **A5/4** Keystream Generator Function

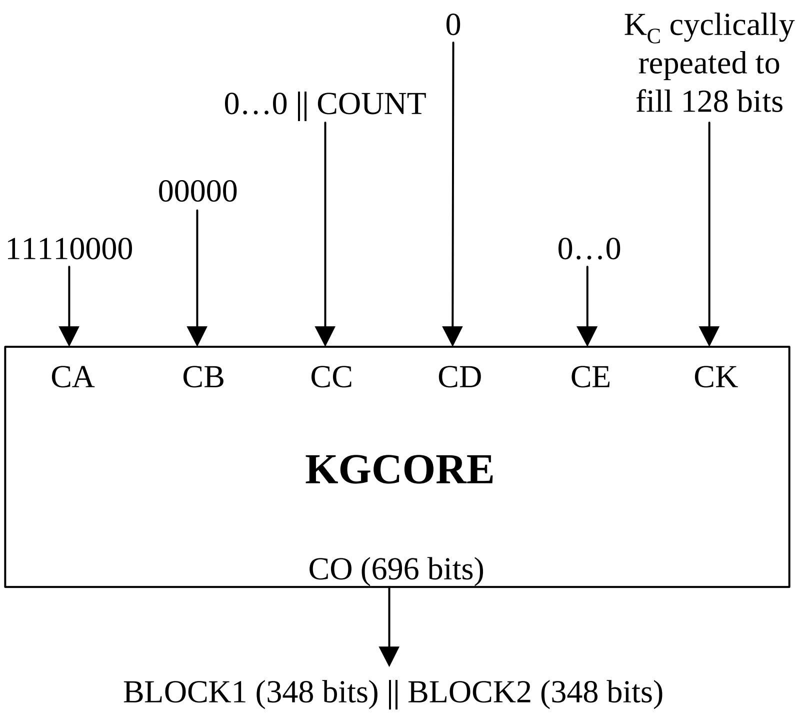


Figure 3: ECSD**A5/4** Keystream Generator Function

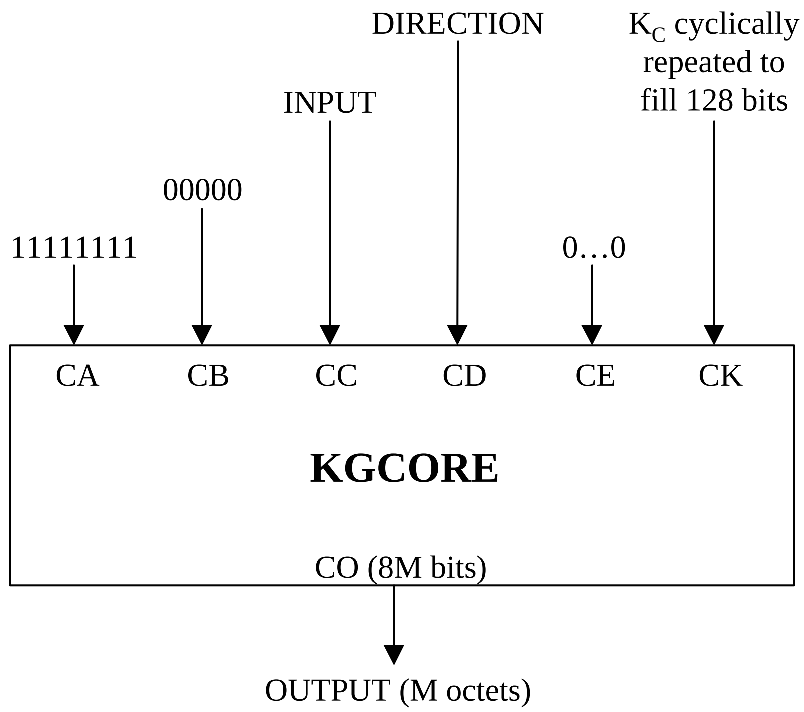


Figure 4: **GEA4** Keystream Generator Function

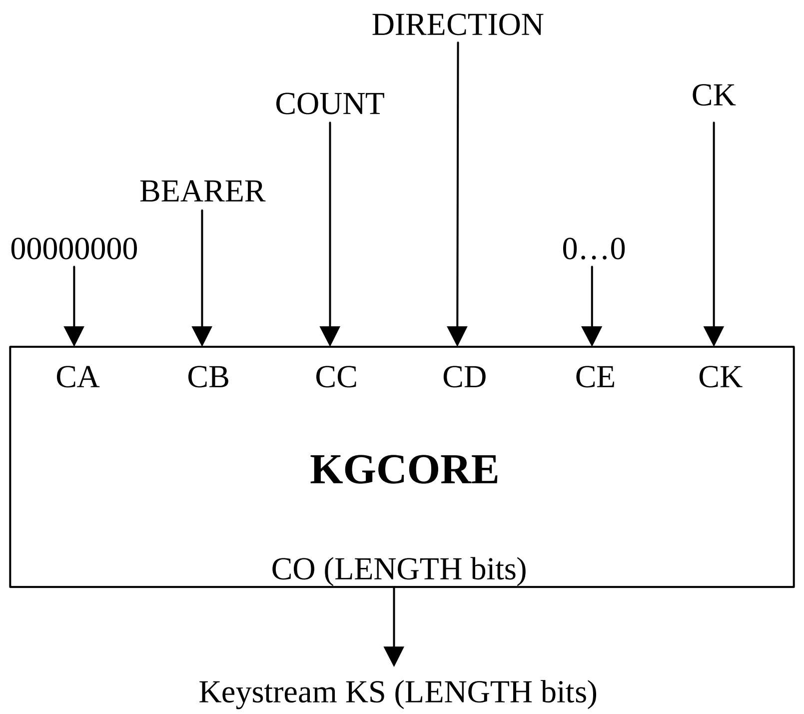


Figure 5: 3GPP *f*8 Keystream Generator Function

	GSM **A5/4**	ECSD **A5/4**	**GEA4**	***f*8**
CA	**0 0 0 0 1 1 1 1**	**1 1 1 1 0 0 0 0**	**1 1 1 1 1 1 1 1**	**0 0 0 0 0 0 0 0**
CB	**0 0 0 0 0**	**0 0 0 0 0**	**0 0 0 0 0**	**BEARER**
CC	**0...0‖COUNT**	**0...0‖COUNT**	**INPUT**	**COUNT**
CD	**0**	**0**	**DIRECTION**	**DIRECTION**
CE	**0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0**			
CK	$\mathbf{K_C}$ 128 bits			**CK**
CO	**BLOCK1‖BLOCK2**	**BLOCK1‖BLOCK2**	**OUTPUT**	**KS**

Table B.1: GSM **A5/4**, ECSD **A5/4**, **GEA4** and ***f*8** in terms of **KGCORE**

Note: The values for A5/4 are the same as for A5/3

The values for ECSD A5/4 are the same as for ECSD A5/3

The values for GEA4 are the same as for GEA3

ANNEX C (informative) Simulation program listings

For coding example of the algorithms see annex C in 55.216 [1]:

Specification of the **A5/3** Encryption Algorithms for GSM and ECSD, and the **GEA3** Encryption Algorithm for GPRS; Document 1: **A5/3** and **GEA3** Specifications.

ANNEX D (informative)
Test data

Test data for the algorithms are to be found in:

Specification of the **A5/3** Encryption Algorithms for GSM and ECSD, and the **GEA3**Encryption Algorithm for GPRS; Document 2: Implementors' Test Data. [2]

Specification of the **A5/3** Encryption Algorithms for GSM and ECSD, and the **GEA3** Encryption Algorithm for GPRS; Document 3: Design Conformance Test Data. [3]

Both documents contain examples where KLEN is set to be 128 bits.

~~6 Security mechanisms~~

~~[Editor's note: This section shall describe the security mechanisms that are provided inter domain, intra domain and to the WLAN-UE.]~~

~~6.1 Authentication and key agreement~~

~~[Editor's note: This section shall describe in detail how the authentication is performed and how the keys are derived and delivered to the different nodes.]~~

~~[Editor's note: The content of this section is directly copied from TS 23.xxx v0.1.0 and shall be reviewed by SA3]~~

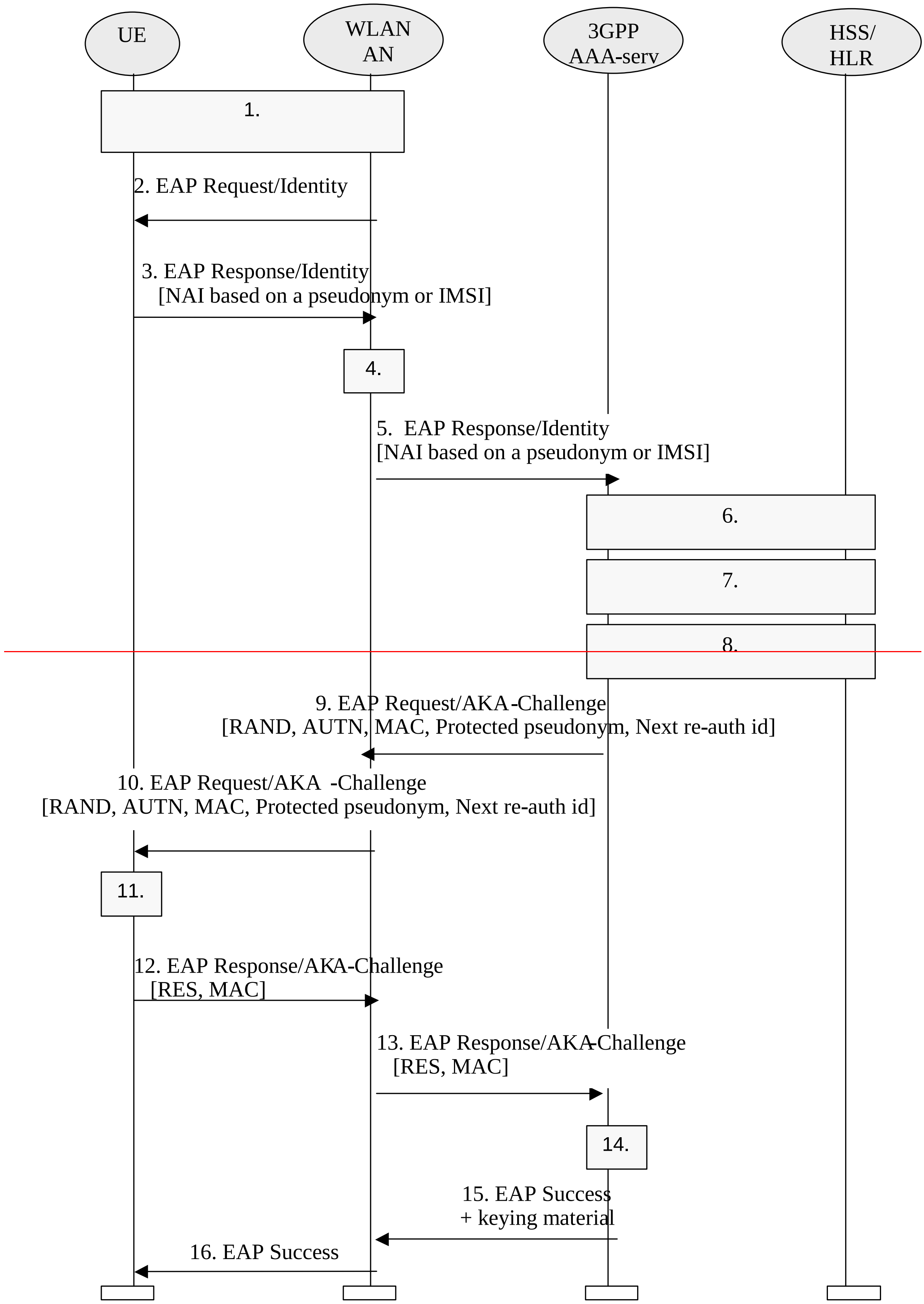
~~6.1.1 USIM-based WLAN Access Authentication~~

~~USIM based authentication is a proven solution that satisfies the authentication requirements from section 4.2. This form of authentication shall be based on EAP-AKA (ref. [4]), as described in section 6.1.1.1.~~

~~[Editor's note: also see section 4.2.4 on WLAN-UE Functional Split]~~

~~6.1.1.1 EAP/AKA Procedure~~

~~The EAP-AKA authentication mechanism is specified in ref. [4]. The present section describes how this mechanism is used in the WLAN-3GPP interworking scenario.~~



~~Figure 7.1: Authentication based on EAP AKA scheme~~

~~1. A connection is established between the WLAN-UE and the WLAN-AN, using a Wireless LAN technology specific procedure (out of scope for this specification).~~

~~2. The WLAN-AN sends an EAP Request/Identity to the WLAN-UE.~~

~~EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.~~

~~3. The WLAN-UE sends an EAP Response/Identity message. The WLAN-UE sends its identity complying with Network Access Identifier (NAI) format specified in RFC 2486. NAI contains either a temporary identifier (pseudonym) allocated to WLAN-UE in previous authentication or, in the case of first authentication, the IMSI.~~

~~NOTE: Generating an identity conforming to NAI format from IMSI is defined in EAP/AKA [4]~~

~~4. The message is routed towards the proper 3GPP AAA Server based on the realm part of the NAI. The routing path may include one or several AAA proxies (not shown in the figure).~~

~~NOTE: Diameter referral can also be applied to find the AAA server.~~

~~5. The 3GPP AAA server receives the EAP Response/Identity packet that contains the subscriber identity.~~

~~6. 3GPP AAA Server identifies the subscriber as a candidate for authentication with EAP-AKA, based on the received identity. The 3GPP AAA Server then checks that it has an unused authentication vector available for that subscriber . If not, a set of new authentication vectors is retrieved from HSS/HLR. A mapping from the temporary identifier to the IMSI may be required.~~

~~NOTE: It could also be the case that the 3GPP AAA Server first obtains an unused authentication vector for the subscriber and, based on the type of authenticator vector received (i.e. if a UMTS authentication vector is received), it regards the subscriber as a candidate for authentication with EAP-AKA.~~

~~7. 3GPP AAA server checks that it has the WLAN access profile of the subscriber available. If not, the profile is retrieved from HSS. 3GPP AAA Server verifies that the subscriber is authorized to use the WLAN service.~~

~~Although this step is presented after step 6 in this example, it could be performed at some other point, however before step 14. (This will be specified as part of the Wx interface.)~~

~~8. New keying material is derived from IK and CK., cf. [4]. This keying material is required by EAP-AKA, and some extra keying material may also be generated for WLAN technology specific confidentiality and/or integrity protection.~~

~~A new pseudonym mat be chosen and protected (i.e. encrypted and integrity protected) using EAP-AKA generated keying material..~~

~~9. 3GPP AAA Server sends RAND, AUTN, a message authentication code (MAC) and two user identities (if they are generated): protected pseudonym and/or re-authentication id to WLAN-AN in EAP Request/AKA-Challenge message. The sending of the re-authentication id depends on 3GPP operator's policies on whether to allow re-authentication processes or not. It implies that, at any time, the AAA server decides (based on policies set by the operator) to include the re-authentication id or not, thus allowing or disallowing the triggering of the re-authentication process.~~

~~10. The WLAN-AN sends the EAP Request/AKA-Challenge message to the WLAN-UE.~~

~~11. WLAN-UE runs UMTS algorithm on the USIM. The USIM verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the terminal rejects the authentication (not shown in this example). If the sequence number is out of synch, terminal initiates a synchronization procedure, c.f. [4]. If AUTN is correct, the USIM computes RES, IK and CK.~~

~~Using IK and CK the WLAN-UE checks the received MAC and derives required additional keying material~~

~~If a protected pseudonym was received, then the WLAN-UE stores the pseudonym for future authentications.~~

~~12. WLAN-UE sends EAP Response/AKA-Challenge containing calculated RES and a new MAC value to WLAN-AN~~

~~13. WLAN-AN sends the EAP Response/AKA-Challenge packet to 3GPP AAA Server~~

~~14. 3GPP AAA Server checks the received MAC and compares XRES to the received RES.~~

~~15. If all checks in step 14 are successful, then 3GPP AAA Server sends the EAP Success message to WLAN-AN. If some extra keying material was generated for WLAN technology specific confidentiality and/or integrity protection then the 3GPP AAA Server includes this keying material in the underlying AAA protocol message (i.e. not at EAP level). The WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.~~

~~16. WLAN-AN informs the WLAN-UE about the successful authentication with the EAP Success message. Now the EAP AKA exchange has been successfully completed, and the WLAN-UE and the WLAN-AN share keying material derived during that exchange.~~

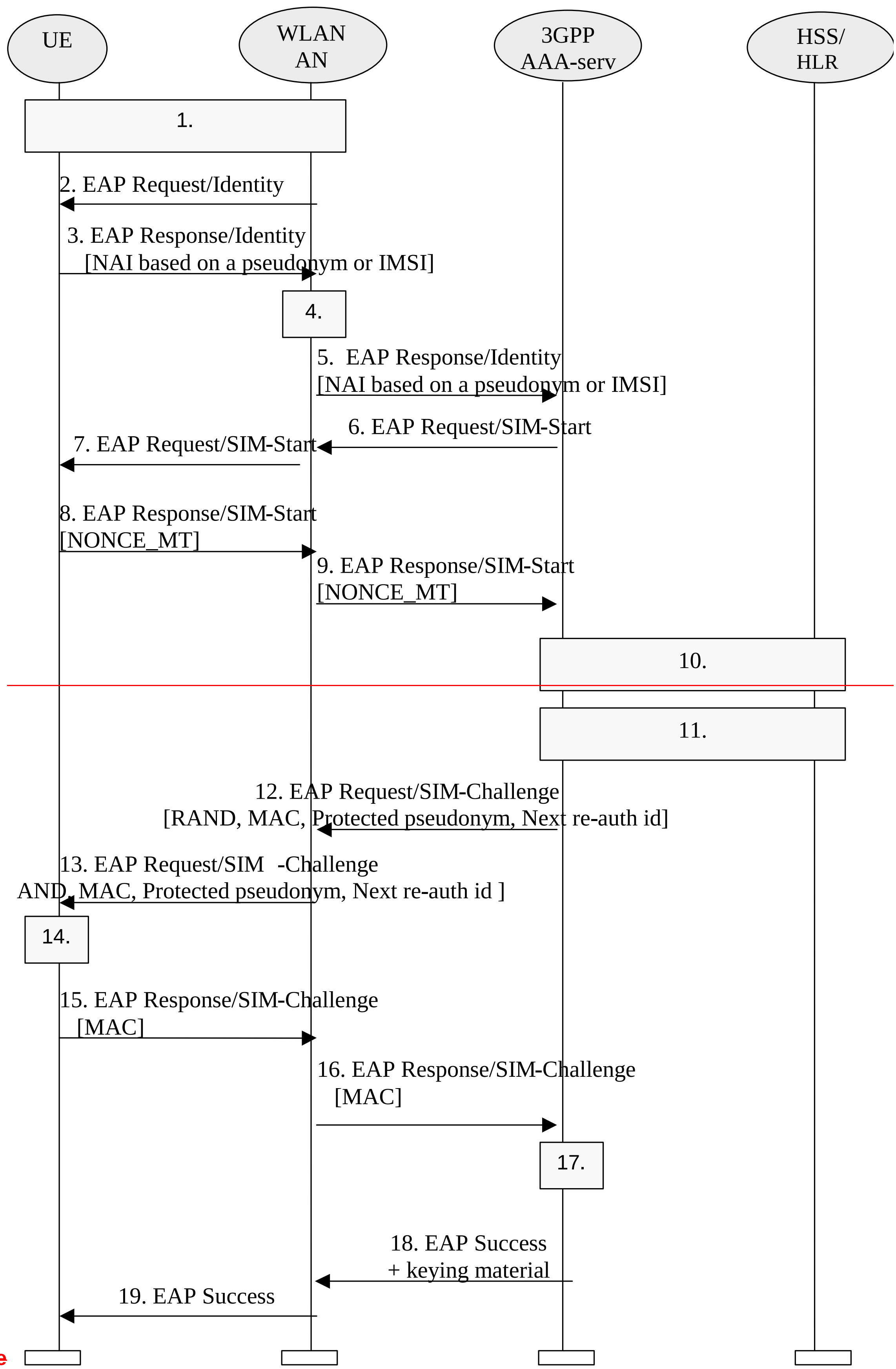
~~6.1.2 GSM SIM based WLAN Access authentication~~

~~SIM based authentication is useful for GSM subscribers that do not have a UICC with a USIM application. This form of authentication shall be based on EAP-SIM (ref. [5]), as described in section 6.1.2.1. This authentication method satisfies the authentication requirements from section 4.2., without the need for a UICC with a USIM application~~

~~[Editor's note: also see section 4.2.4 on WLAN UE split]~~

~~6.1.2.1 EAP SIM procedure~~

~~The EAP-SIM authentication mechanism is specified in ref. [5]. The present section describes how this mechanism is used in the WLAN-3GPP interworking scenario.~~



~~scheme~~

~~7.2: Authentication based on EAP SIM scheme~~

~~1. A connection is established between the WLAN-UE and the WLAN-AN, using a Wireless LAN technology specific procedure (out of scope for this specification).~~

~~2. The WLA-AN sends an EAP Request/Identity to the WLAN-UE.~~

~~EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.~~

~~3. The WLAN-UE sends an EAP Response/Identity message. The WLAN-UE sends its identity complying with the Network Access Identifier (NAI) format specified in RFC 2486. NAI contains either a temporary identifier (pseudonym) allocated to WLAN-UE in previous authentication or, in the case of first authentication, the IMSI.~~

~~NOTE: Generating an identity conforming to NAI format from IMSI is defined in EAP/SIM.~~

~~4. The message is routed towards the proper 3GPP AAA Server based on the realm part of the NAI. The routing path may include one or several AAA proxies (not shown in the figure).~~

~~NOTE: Diameter referral can also be applied to find the AAA server.~~

~~5. The 3GPP AAA server receives the EAP Response/Identity packet that contains the subscriber identity.~~

~~6. The 3GPP AAA Server, identifies the subscriber as a candidate for authentication with EAP-SIM, based on the received identity, , and then it sends the EAP Request/SIM-Start packet to WLAN-AN.~~

~~NOTE: It could also be the case that the 3GPP AAA Server first obtains an authentication vector for the subscriber and, based on the type of authenticator vector received (i.e. if a GSM authentication vector is received), it regards the subscriber as a candidate for authentication with EAP-SIM.~~

~~7. WLAN-AN sends the EAP Request/SIM-Start packet to WLAN-UE~~

~~8. The WLAN-UE chooses a fresh random number NONCE_MT. The random number is used in network authentication.~~

~~The WLAN-UE sends the EAP Response/SIM-Start packet, containing NONCE_MT, to WLAN-AN.~~

~~9. WLAN-AN sends the EAP Response/SIM-Start packet to 3GPP AAA Server~~

~~10. The AAA server checks that it has available N unused authentication vectors for the subscriber. Several GSM authentication vectors are required in order to generate keying material with effective length equivalent to EAP-AKA.. If N authentication vectors are not available, a set of authentication t vectors is retrieved from HSS/HLR. A mapping from the temporary identifier to the IMSI may be required.~~

~~Although this step is presented after step 9 in this examples, it could be performed at some other point, for example after step 5, however before step 12. (This will be specified as part of the Wx interface.)~~

~~11. The AAA server checks that it has the WLAN access profile of the subscriber available. If not, the profile is retrieved from HSS/HLR. 3GPP AAA Server verifies that the subscriber is authorized to use the WLAN service.~~

~~Although this step is presented after step 10 in this example, it could performed at some other point, however before step 18. (This will be the specified as part of the Wx interface).~~

~~12. New keying material is derived from NONCE_MT and N Kc keys. This keying material is required by EAP-SIM, and some extra keying material may also be generated for WLAN technology specific confidentiality and/or integrity protection.~~

~~A new pseudonym and/or a re-authentication identity may be chosen and protected (i.e. encrypted and integrity protected) using EAP-SIM generated keying material.~~

~~A message authentication code (MAC) is calculated over the EAP message using an EAP-SIM derived key. This MAC is used as a network authentication value.~~

~~3GPP AAA Server sends RAND, MAC, protected pseudonym and re-authentication identity (the two latter in case they were generated) to WLAN-AN in EAP Request/SIM-Challenge message. The sending of the re-authentication id depends on 3GPP operator's policies on whether to allow re-authentication processes or not. It implies that, at any time, the AAA server decides (based on policies set by the operator) to include the re-authentication id or not, thus allowing or disallowing the triggering of the re-authentication process.~~

~~13. The WLAN sends the EAP Request/SIM-Challenge message to the WLAN-UE.~~

~~14. WLAN-UE runs N times the GSM A3/A8 algorithms in the SIM, once for each received RAND.~~

~~- This computing gives N SRES and Kc values.~~

~~- The WLAN-UE derives additional keying material from N Kc keys and NONCE_MT.~~

~~- The WLAN-UE calculates its copy of the network authentication MAC and checks that it is equal with the received MAC. If the MAC is incorrect, the network authentication has failed and the WLAN-UE cancels the authentication (not shown in this example). The WLAN-UE continues the authentication exchange only if the MAC is correct.~~

~~- WLAN-UE calculates a new MAC covering the EAP message concatenated to the N SRES responses.~~

~~- If a protected pseudonym was received, then the WLAN-UE stores the pseudonym for future authentications.~~

~~15. WLAN-UE sends EAP Response/SIM-Challenge containing calculated MAC to WLAN-AN.~~

~~16. WLAN-AN sends the EAP Response/SIM-Challenge packet to 3GPP AAA Server.~~

~~17. 3GPP AAA Server compares its copy of the response MAC with the received MAC.~~

~~18. If the comparison in step 17 is successful, then 3GPP AAA Server sends the EAP Success message to WLAN-AN. If some extra keying material was generated for WLAN technology specific confidentiality and/or integrity protection, then the 3GPP AAA Server includes this derived keying material in the underlying AAA protocol message. (i.e. not at EAP level). The WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.~~

~~19. WLAN-AN informs the WLAN-UE about the successful authentication with the EAP Success message. Now the EAP SIM exchange has been successfully completed, and the WLAN-UE and the WLAN_AN may share keying material derived during that exchange.~~

~~NOTE: The derivation of the value of N is for further study.~~

~~6.1.3 EAP support in Smart Cards~~

~~[Editors note LS (S3-030187/ S1-030546) from SA1 has stated that "There are requests from operators for a secure SIM based WLAN authentication solution". SA3 has SA1 in an LS (S3-030306) if this request is confirmed. The input paper to SA3 on this can be found at:~~

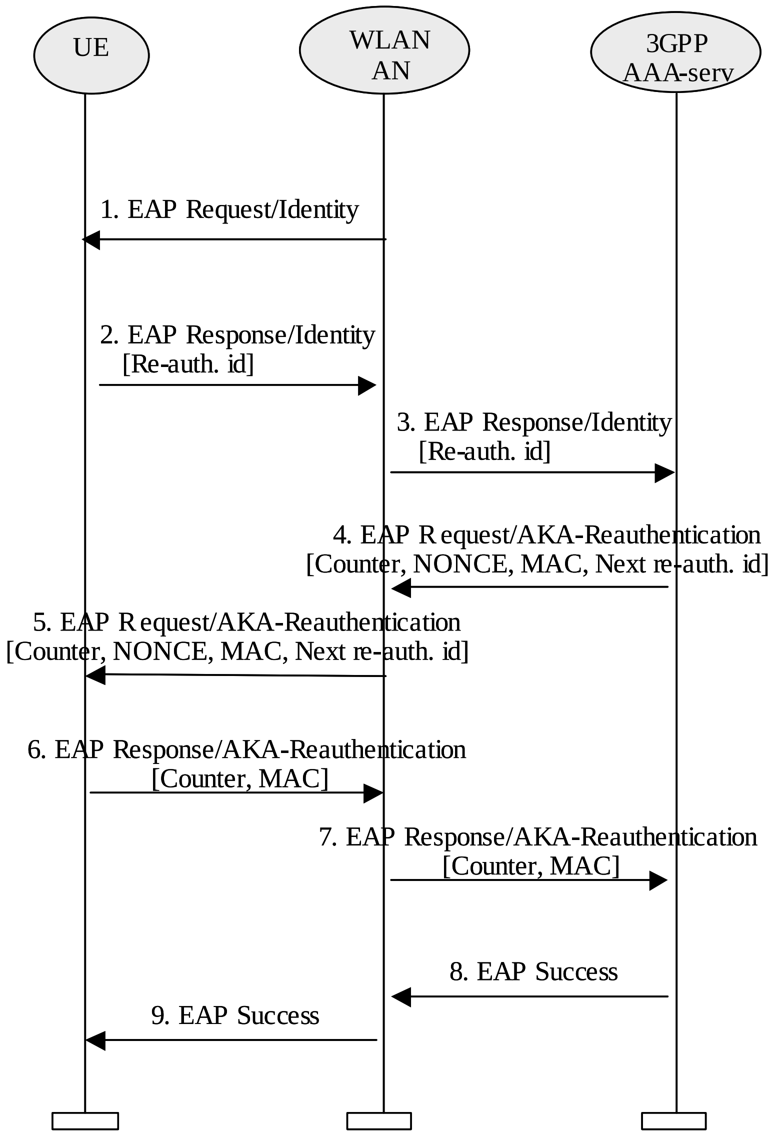
~~http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_28_Berlin/Docs/ZIP/S3-030198.zip]~~

~~6.1.4 Re-authentication mechanisms in WLAN Access~~

~~When authentication processes have to be performed frequently, it can lead to a high network load specially when the number of connected users is high. Then it is more efficient to perform re-authentications. Thus the re-authentication process allows the WLAN-AN to authenticate a certain user in a lighter process than a full authentication, thanks to the re-use of the keys derived on the previous full authentication.~~

~~6.1.4.1.EAP/AKA procedure~~

~~The implementation of EAP/AKA must include the re-authentication mechanism described in this chapter, although its use is optional and depends on operator's policies. The complete procedure is defined in ref [4]. In this section it is described how the process works for WLAN-3GPP interworking.~~



~~Figure 7.3 : EAP AKA Re-authentication~~

~~1.WLAN-AN sends an EAP Request/Identity to the WLAN-UE~~

~~2.WLAN-UE replies with an EAP Response/Identity containing a re-authentication identity (this identity was previously delivered by AAA server in a full authentication procedure). The WLAN-UE can take the decision of not performing a re-authentication but a full authentication. In that case, it will include a pseudonym in the message to the WLAN AN and a normal authentication process will take place.~~

~~3.The WLAN-AN forwards the EAP Response/Identity to the AAA server.~~

~~4.The AAA server initiates the Counter (which was initialized to one in the full authentication process) and sends it in the EAP Request message, together with the NONCE, the MAC (calculated over the NONCE) and a re-authentication id for a next re-authentication. If the AAA server is not able to deliver a re-authentication identity, next time the WLAN-UE will force a full-authentication (to avoid the use of the re-authentication identity more than once).~~

~~5.The WLAN-AN forwards the EAP Request message to the WLAN-UE~~

~~6.The WLAN-UE verifies that the Counter value is fresh and the MAC is correct, and it sends the EAP Response message with the same Counter value (it is up to the AAA server to step it up) and a calculated MAC.~~

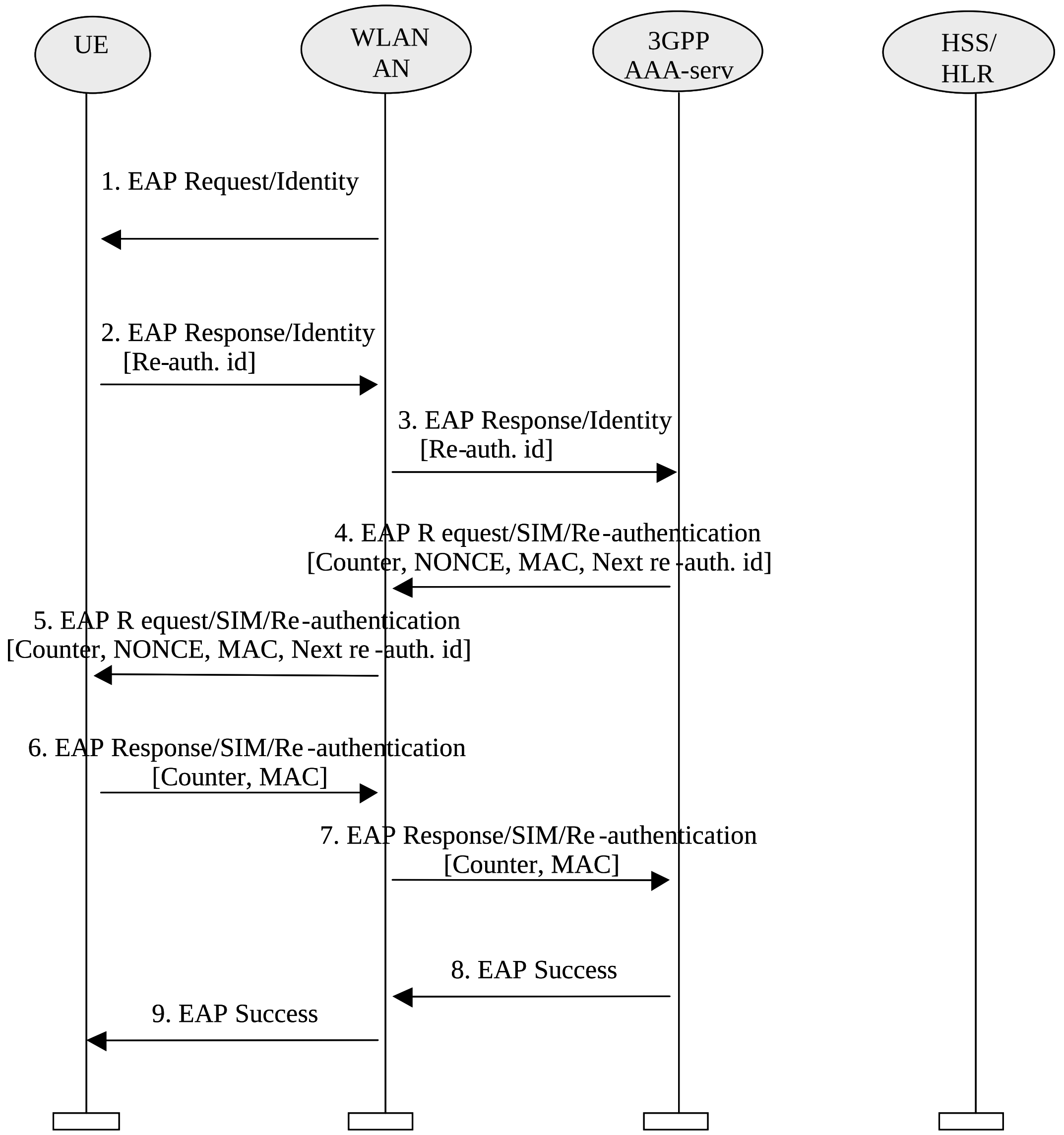
~~7.The WLAN-AN forwards the response to the AAA server~~

~~8.The AAA server verifies that the Counter value is the same as it sent, and the MAC is correct, and sends an EAP Success message~~

~~9.The EAP Success message is forwarded to the WLAN-UE.~~

~~6.1.4.2.EAP/SIM procedure~~

~~The implementation of EAP/SIM must include the re-authentication mechanism described in this chapter, although its use is optional and depends on operator's policies. The complete procedure is defined in ref [4]. In this section it is described how the process works for WLAN-3GPP interworking.~~



~~Figure 7.4 : EAP SIM Re-authentication~~

~~1.WLAN-AN sends an EAP Request/Identity to the WLAN-UE~~

~~2.WLAN-UE replies with an EAP Response/Identity containing a re-authentication identity (this identity was previously delivered by AAA server in a full authentication procedure). The WLAN-UE can take the decision of not performing a re-authentication but a full authentication. In that case, it will include a pseudonym in the message to the WLAN AN and a normal authentication process will take place.~~

~~3.The WLAN-AN forwards the EAP Response/Identity to the AAA server.~~

~~4.The AAA server initiates the Counter (which was initialized to one in the full authentication process) and sends it in the EAP Request message, together with the NONCE, the MAC (calculated over the NONCE) and a re-authentication id for a next re-authentication. If the AAA server is not able to deliver a re-authentication identity, next time the WLAN-UE will force a full authentication (to avoid the use of the re-authentication identity more than once).~~

~~5.The WLAN-AN forwards the EAP Request message to the WLAN-UE~~

~~6.The WLAN-UE verifies that the Counter value is fresh and the MAC is correct, and it sends the EAP Response message with the same Counter value (it is up to the AAA server to step it up) and a calculated MAC.~~

~~7.The WLAN-AN forwards the response to the AAA server~~

~~8.The AAA server verifies that the Counter value is the same as it sent, and the MAC is correct, and sends an EAP Success message~~

~~9.The EAP Success message is forwarded to the WLAN-UE.~~

~~6.1.5 Mechanisms for the set up of UE-initiated tunnels (Scenario 3)~~

~~The WLAN UE and the PDG use IKEv2, as specified in [ikev2], in order to establish IPsec security associations.~~

~~Public key signature based authentication with certificates, as specified in [ikev2], is used to authenticate the PDG.~~

~~Editor's note: It is for further study whether Public Key signatures for PDG authentication are needed.~~

~~EAP-AKA within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN UEs, which contain a USIM.~~

~~EAP-SIM within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN UEs, which contain a SIM and no USIM.~~

~~A profile for IKEv2 is defined in section 6.5.~~

~~Editor's note: the discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing in SA3. The text in this section reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in Annex X. They may replace the current working assumption in this section if problems with the working assumption arise. Otherwise, Annex X will be removed before the TS is submitted for approval. The aove points on the use of IKEv2 are dependent on the analysis of the open issues on legacy VPN clients and key management, in particular, the use of EAP-AKA and EAP-SIM will be studied.~~

~~6.2 Confidentiality mechanisms~~

~~[Editor's note: This section shall deal with cipher algorithms]~~

~~6.2.1 Confidentiality mechanisms in scenario 2~~

~~*Text to be added*~~

~~6.2.2 Confidentiality mechanisms in scenario 3~~

~~The confidentiality of IP packets sent through a tunnel between the UE and the PDG, if required, shall be protected by IPsec ESP [rfc2406]. A profile for IPsec ESP is defined in section 6.6.~~

~~6.3 Integrity mechanisms~~

~~[Editor's note: This section shall deal with integrity algorithms]~~

~~6.3.1 Integrity mechanisms in scenario 2~~

~~*Text to be added*~~

~~6.3.2 Integrity mechanisms in scenario 3~~

~~The integrity of IP packets sent through a tunnel between the UE and the PDG shall be protected by IPsec ESP [rfc2406]. A profile for IPsec ESP is defined in section 6.6.~~

~~6.4 Temporary identity management~~

~~6.4.1 Pseudonym Temporary Identity Generation~~

~~Temporary Identities (Pseudonyms or re-authentication identities) are generated as some form of encrypted IMSI. Advanced Encryption Standard (AES) (see ref. [17]) in Electronic Codebook (ECB) mode of operation with 128-bit keys is used for this purpose.~~

~~In order to encrypt with AES in ECB mode, it is necessary that the length of the clear text is a multiple of 16 octets. This clear text is formed as follows:~~

1. ~~A *Compressed IMSI* is created utilising 4 bits to represent each digit of the IMSI. According to ref. [18], the length of the IMSI is not more than 15 digits (numerical characters, 0 through 9). The length of the *Compressed IMSI* shall be 64 bits (8 octets), and the most significant bits will be padded by setting all the bits to 1.~~

   ~~E.g.: IMSI = 214070123456789 (MCC = 214 ; MNC = 07 ; MSIN = 0123456789)~~

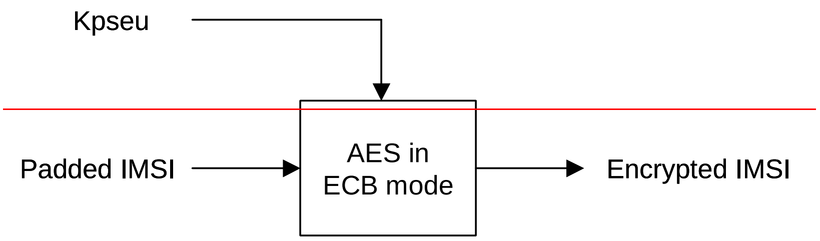
   ~~Compressed IMSI = 0xF2 0x14 0x07 0x01 0x23 0x45 0x67 0x89~~

   ~~Observe that, at reception of a temporary identitypseudonym, it is easy to remove the padding of the *Compressed IMSI* as none of the IMSI digits will be represented with 4 bits set to 1. Moreover, a sanity check should be done at reception of a pseudonym, by checking that the padding, the MCC and the MNC are correct, and that all characters are digits.~~

2. ~~A *Padded IMSI* is created by concatenating an 8-octet random number to the *Compressed IMSI.*~~

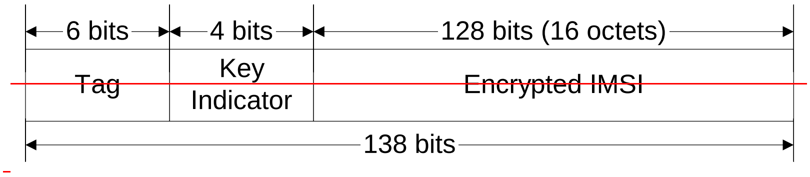
~~A 128-bit secret key, Kpseu, is used for the encryption. The same secret key must be configured at all the WLAN AAA servers in the operator network so that any WLAN AAA server can obtain the permanent identity from atemporary identity pseudonym generated at any other WLAN AAA server (see section 6.4.2).~~

~~The figure below summarises how the *Encrypted IMSI* is obtained.~~



Once the *Encrypted IMSI* has been generated, the following fields are concatenated:

- *Encrypted IMSI*, so that a AAA server can later obtain the IMSI from the temporary identitypseudonym.
- *Key Indicator*, so that the AAA server that receives the temporary identitypseudonym can locate the appropriate key to de-encrypt the Encrypted IMSI. (See section 6.4.2.)
- *Pseudonym Temporary identity Tag*, used to mark the identity as temporary a pseudonym or re-authentication identity. The tag should be different for pseudonyms generated for EAP-SIM and for EAP-AKA.



The *Pseudonym* Temporary Identity *Tag* is necessary so that when a WLAN AAA receives a user identity it can determine whether to process it as a permanent or a temporary user identity. Moreover, according to EAP-SIM/AKA specifications, when the Authenticator node (i.e. the AAA server) receives a temporary user identity from which a permanent user identity cannot be successfully obtained which does not recognize, then the permanent user identity must be requested from the WLAN client(if the process was full authentication) or a full authentication identity (if the process was re-authentication) shall be requested from the WLAN client. As the procedure to request the permanent user identity is different in EAP-SIM and EAP-AKA, the *PseudonymTemporary Identity Tag* must be different for EAP-SIM pseudonyms or re-authentication identities) and for EAP-AKA pseudonyms or re-authentication identities, so that the AAA can determine which procedure to follow.

The last step in the generation of the pseudonym temporary identities consists on converting the concatenation above to a printable string using the BASE64 method described in section 4.3.2.4 of ref. [16]. With this mechanism, each 6-bit group is used as an index into an array of 64 printable characters. As the length of the concatenation is 138 bits, the length of the resulting pseudonym temporary identity is 23 characters, and no padding is necessary. Observe that the length of the *Pseudonym* Temporary identity *Tag* has been chosen to be 6 bits, so that it directly translates into one printable character after applying the transformation. Therefore, at reception of a user identity, the AAA server can recognise that it is a pseudonym temporary identity for EAP-SIM or a pseudonym temporary identity for EAP-AKA without performing any reverse transformation (i.e. without translating any printable character into the corresponding 6 bits).

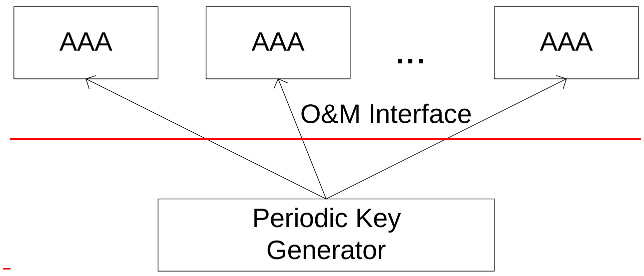
6.4.2 Key Management

A 128-bit encryption key shall be used for the generation of pseudonyms temporary identities for a given period of time determined by the operator. Once that time has expired, a new key shall be configured at all the WLAN AAA servers. The old key shall not be used any longer for the generation of pseudonyms temporary identities, but the AAA servers must keep a number of suspended (old) keys for the interpretation of received pseudonyms temporary identities that were generated with those old keys. The number of suspended keys kept in the AAA servers (up to 16) should be set by the operator, but it must be at least one, in order to avoid that a just-generated pseudonym temporary identity becomes invalid immediately due to the expiration of the key.

~~Each key must have associated a Key Indicator value. This value is included in the pseudonym (see *Key Indicator* field in section 6.4.1), so that when a WLAN AAA receives the pseudonym temporary identity, it can use the corresponding key for obtaining the *Padded IMSI* (and thence the Username).~~

~~If a pseudonym temporary identity is sent to a WLAN client but then the user does not initiate new authentication attempts for a long period of time, the key used for the generation of that pseudonym temporary identity could eventually be removed from all the WLAN AAA servers. If the user initiates an authentication attempt after that time using that old pseudonym temporary identity, the receiving AAA server will not be able to recognise the pseudonym temporary identity as a valid one, and it will request the permanent user identity from the WLAN client(if the process was re-authentication, the AAA server will request first a pseudonym, and if it is not recognized, the permanent user identity). Hence, in order to achieve that permanent user identities are used as little as possible, it is recommended that the encryption key is not renewed very often.~~

~~The configuration of the keys could be done via O&M, as shown in the figure below.~~



~~Handling of these secret keys, including generation, distribution and storage, should be done in a secure way.~~

~~6.4.3 Impact on Permanent User Identities~~

~~User identities (permanent or temporary) are sent with the form of a NAI, according to the EAP-SIM/AKA specifications, and the maximum length of a NAI that we can expect to be handled correctly by standard equipment is 72 octets (see ref. [14]). Moreover, this NAI will be transported inside the User-Name attribute of a RADIUS Access-Request, with standard length up to 63 octets (see ref. [15]). Therefore, it can be assumed that the maximum length of a WLAN user identity should be 63 octets (i.e. 63 characters).~~

~~Since the length of the pseudonym proposed in section 6.4.1 is 23 characters, the length of the realm part of any WLAN permanent user identity must always be 40 characters or less. This applies regardless of whether the length of the username part of the permanent user identity is less than 23 characters. (Note that a WLAN temporary user identity is formed as a NAI with the pseudonym as the username part and the same realm part as the permanent user identity.)~~

~~Moreover, the WLAN permanent user identities should not begin with the character resulting of the printable encoding transformation (see section 6.4.1) of the *Pseudonym Tag* used for EAP-SIM and EAP-AKA pseudonyms. This is needed so that at reception of a WLAN user identity, the AAA server can determine whether it is a permanent or a temporary user identity.~~

~~6.4.4 Acknowledged Limitations~~

~~This mechanism does not prevent forging of pseudonyms generated with keys that are no longer maintained in the AAA servers. That is, an attacker may form a pseudonym by concatenating the desired *Pseudonym Tag* and 132 bits of random information, and then applying the printable encoding transformation (see section 6.4.1). At reception of such pseudonym in a AAA server, the following cases are possible:~~

- ~~The *Key Indicator* may not correspond to any key (active or suspended) maintained at the AAA server.~~
- ~~If the *Key Indicator* corresponds to any of the keys maintained at the AAA server, then that key is used for the de-encryption of the *Encrypted IMSI*, but the sanity check over the padding, the MCC and the MNC would show that the IMSI is not correct.~~

~~In any case, the AAA server must interpret that the received pseudonym was generated with a key that is no longer available, and therefore it must request the permanent user identity to the WLAN client.~~

~~This could be exploited to perform DoS attacks by initiating a large amount of authentication attempts presenting different forged temporary identities. Nonetheless, the consequences of this attack should not be worse than the already possible attack of initiating a large amount of authentication attempts presenting different forged permanent identities.~~

~~6.4.5 UE behaviour on receiving requests to send the IMSI-based user identity~~

~~When the 3GPP AAA server does not recognize a temporary identifier used by the UE, the 3GPP AAA server requests the UE to send the IMSI-based user identity. The UE can operate according to one of the following three alternatives.~~

1. ~~Ignore the Request: This alternative may result in deadlock situations that prevent the UE from connecting to a valid network. If this alternative is implemented, then there must be a separate mechanism available for the user to override the policy (for example to delete the stored temporary identifier, which would result in using the IMSI-based identity upon the next connection).~~
2. ~~Prompt the User: In this alternative, the UE prompts the user during the EAP authentication whether to send the IMSI-based identity to the network. If the user denies sending the IMSI, then the authentication exchange is cancelled.~~
3. ~~Always Send the IMSI-Based Identity: In alternative #3, the UE always sends the IMSI-based identity when requested.~~

~~The decision is UE specific and outside the scope of this specification.~~

~~6.5 Profile of IKEv2~~

~~IKEv2, as specified in [ikev2], contains a number of options which are not all needed for the purposes of this specification. IKEv2ESP is therefore profiled in this section. When IKEv2 is used in the context of this specification the profile specified in this section shall be supported.~~

~~Editor's note: an example of a profile of IKE, which may be useful to study when writing this section, can be found in TS 33.210, section 5.4.~~

~~6.6 Profile of IPsec ESP~~

~~IPsec ESP, as specified in [rfc2406], contains a number of options which are not all needed for the purposes of this specification. IPsec ESP is therefore profiled in this section. When IPsec ESP is used in the context of this specification the profile specified in this section shall be supported.~~

~~Editor's note: an example of a profile of IPsec ESP, which may be useful to study when writing this section, can be found in TS 33.210, section 5.3.~~

~~Annex A (informative): Review of the security of existing WLAN-related technologies~~

~~A.1 IEEE~~

~~A.1.1 IEEE 802 Project~~

~~IEEE Project 802 develops LAN and MAN standards, mainly for the lowest 2 layers of the OSI Reference Model. IEEE 802.11 is the Wireless LAN Working Group (WG) within Project 802. The existing 802.11 standard with amendments are:~~

- ~~802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.~~
- ~~802.11a High-speed Physical Layer in the 5 GHz Band.~~
- ~~802.11b Higher-Speed Physical Layer Extension in the 2.4 GHz Band.~~
- ~~802.11d Specification for operation in additional regulatory domains.~~

~~Currently there are a number of Task Groups (TG) in the 802.11 WG that each work on new amendments to the standard:~~

- ~~802.11e Medium Access Control (MAC) Enhancements for Quality of Service (QoS).~~
- ~~802.11f Inter Access Point Protocol (IAPP). (A recommended practice, not a standard).~~
- ~~802.11g Higher-Speed Physical Layer Extension in the 2.4 GHz Band.~~
- ~~802.11h Spectrum and Power Management extensions in the 5 GHz band in Europe.~~
- ~~802.11i Specification for Enhanced Security.~~

~~Membership in IEEE 802.11 is individual (i.e. not based on company) and anyone that has been present at a certain number of meetings becomes member in the WG. Membership is required in order to get voting rights and all members have one vote (again, votes are not company based).~~

~~A.1.2 Authentication~~

~~Legacy 802.11 authentication~~

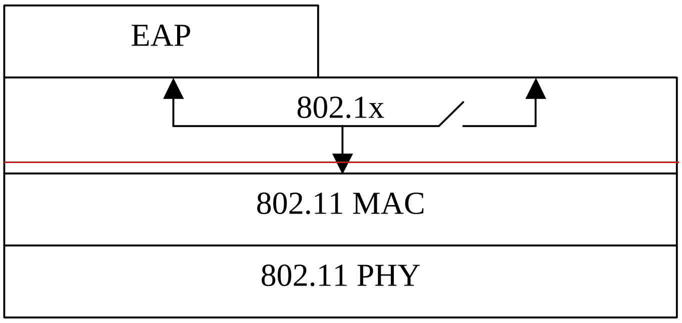
~~The 802.11-1999 authentication mechanism works at the data link layer (MAC layer). Two authentication methods exist, open system authentication and shared key authentication. Open system authentication is in principle a null authentication scheme and accepts anyone that requests authentication.~~

~~Shared key authentication is a challenge-response authentication based on a shared secret. The mobile station sends an Authentication request to the Access Point (AP). The Access Point sends a chosen plaintext string to the station and the station responds with the WEP-encrypted string. (See below for more details on WEP). If the string is correctly encrypted the AP sends an Authentication message to the station to indicate that the authentication was successful. The standard allows for up to four keys in a cell but in practice all communication parties in the cell share the same secret. Note that the authentication is not mutual, only the mobile terminals are authenticated. Shared key authentication is very weak. An attacker that listens to a successful authentication exchange will have all elements that are needed to successfully perform an authentication of his/her own, even if the shared key is unknown. Today shared key authentication is not considered useful.~~

~~**IEEE 802.1X and EAP**~~

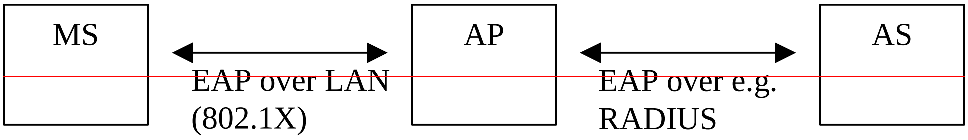
~~The 802.11i Task Group (TGi) within IEEE is working on enhancements to the 802.11 security ref. [6]. It has been decided to use IEEE 802.1X as the authentication framework ref. [19]. IEEE 802.1X in turn uses the Extensible Authentication Protocol (EAP) that allows for end-to-end mutual authentication between a Mobile Station and an Authentication Server (see ref. [3]). Thus, even though 802.11i still performs access control on layer 2, the authentication message exchange is not restricted to the MAC layer but uses other IEEE standard as well as IETF standards.~~

~~IEEE 802.1X is a standard for port-based access control. IEEE 802.1X can be described to lie between the MAC layer and higher layers and takes care of filtering of frames to/from non-authenticated stations. Before authentication is completed only EAP-traffic is allowed to pass. This allows an authentication exchange to cross the Access Point before general data is allowed to pass. When the 802.1X entity in the Access Point (AP) is informed that a mobile station has successfully authenticated, the AP starts to forward data packets to/from that station.~~



~~**Figure A.1: IEEE 802.1X in part of protocol stack in Access Point or mobile station. EAP messages are always accepted while other packets are filtered based on authentication status**~~

~~EAP allows for end-to-end authentication between a Mobile Station and an Authentication Server (AS). EAP is a generic protocol that allows different authentication mechanisms (called EAP methods) to be transported. EAP has a general part that describes the general packet format and header content. Each EAP method then has a more specific description for how the actual authentication mechanism is carried by the EAP packets. The EAP packets can then be transported over different protocols. In 802.1X a special frame format called EAP over LAN (EAPOL) is defined for sending EAP messages over 802 links. This allows EAP messages to be sent over the LAN before higher layer protocols, e.g. IP, have been initiated. Between the Access Point (AP) and the AS, EAP messages are typically encapsulated in an AAA protocol, e.g. in RADIUS or DIAMETER (see figure A.2). It is out of the scope of 802.11i to specify a certain AAA protocol. IEEE 802.11i can in principle also be used without AAA protocol if the EAP method is implemented in the AP.~~



~~**Figure A.2: Example of end-to-end authentication using EAP**~~

~~Examples of EAP methods (RFCs or Internet Drafts) are:~~

- ~~EAP-SIM for SIM-based authentication. (Internet Draft) (ref. [5]);~~
- ~~EAP-AKA for SIM and USIM-based authentication (Internet Draft) (ref. [4]);~~
- ~~EAP-TLS for certificate-based authentication (RFC) [EAP-TLS] (ref. [7]).~~

~~The actual EAP authentication takes place between the MS and the AS and is in principle transparent to the AP. The AP only has to forward EAP messages: EAPOL-encapsulated on the wireless side and e.g. RADIUS-encapsulated on the wired side. If authentication is successful, the AS sends a RADIUS-Access Accept message to the AP (in the case RADIUS is used as AAA protocol). The AP then knows that the MS has been authenticated and can start forwarding traffic to/from the MS. After reception of the Access-Accept message from the AS, the AP sends an EAP-Success message to the MS (see figure A.3).~~

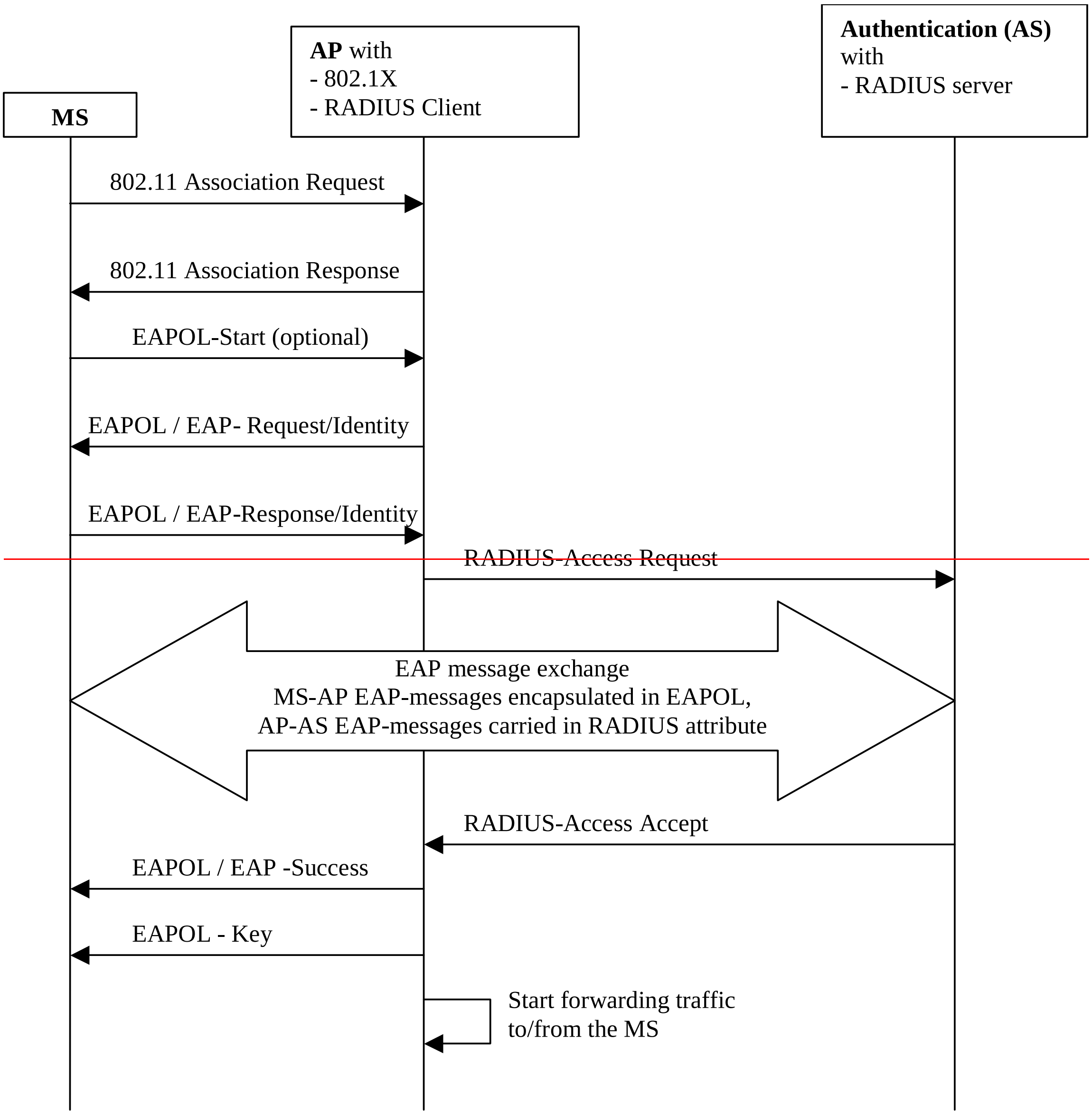
~~**Key management**~~

~~To use an EAP method with 802.11i it is required that a 256-bit master key is established as part of the authentication process. Many EAP methods generate key material as part of the authentication (e.g. EAP-SIM, EAP-AKA, EAP-TLS) but the exact way in which the master key is generated depends on the EAP method and is outside the scope of 802.11i. After the EAP authentication is finished, both the MS and the AS will know the master key. If RADIUS is used, the AS then sends the master key to the AP as an attribute in the RADIUS-Access Accept message. The MS and AP use the master key to derive session keys for encryption and integrity protection, as specified in 802.11i. This provides unique unicast keys for each MS-AP association.~~

~~The broadcast/multicast key in a cell is generated by the AP and sent in an EAPOL-Key message (defined in 802.1X) to each station. To protect the broadcast/multicast key the EAPOL packet is encrypted with TKIP or AES (see below) using the unicast key. The AP can in principle update the broadcast/multicast key any time, e.g. when a MS leaves the cell.~~

~~It shall also be possible to use a pre-shared key instead of the EAP master key material.~~

~~**Message exchange (example with RADIUS)**~~



~~**Figure A.3: General EAP authentication with 802.11i and RADIUS as AAA protocol**~~

~~A.1.3 Encryption and integrity protection~~

~~The air-link protection in IEEE 802.11 occurs in the MAC layer. This means that all layer-2 data frames, including LAN broadcasts, are protected. The 802.11-1999 standard specifies the Wired Equivalent Privacy (WEP) for encryption and integrity protection. The 802.11i task group is specifying two new encryption/integrity-protection protocols, the Temporal Key Integrity Protocol (TKIP) and the Wireless Robust Authenticated Protocol (WRAP). The 802.1X/EAP authentication mechanism can in principle be used with any of the three encryption protocols but configuration can restrict the number of allowed encryption protocols in a cell.~~

~~In order to be backwards compatible, an 802.11i-capable cell could support several encryption protocols simultaneously. For example, to support legacy stations a manually configured shared WEP key may need to be used for those stations. This key will then also be used as broadcast/multicast key for 802.11i-capable stations that instead use unique pair-wise keys for unicast traffic.~~

~~WEP~~

~~The IEEE 802.11-1999 Standard specified the Wireless Equivalent Privacy (WEP). WEP uses RC4 with a 40-bit key and 24-bit initialisation vector (IV) for encryption. RC4 is a stream cipher where a seed is used as input to the RC4 PRNG which produces an output bit string that is XOR:ed with the plaintext to produce the ciphertext. For WEP the seed to the RC4 PRNG is the key concatenated with the IV. The key is shared between the communicating parties and the IV is transmitted in clear text in each packet. Message integrity is provided using a CRC checksum that is added to the payload and then encrypted together with the rest of the payload. WEP does not protect against replay.~~

~~Since the publication of the standard, several shortcomings of WEP have been discovered. Attacks to retrieve the WEP key and to modify the payload have been described. One weakness is the seed derivation. With RC4 it is important that each packet has a different RC4 seed. The RC4 seed in 802.11-1999 is constructed by concatenating the IV and the 40-bit key but the standard did not contain specifications to ensure uniqueness of <key,IV> pairs.~~

~~Today, WEP is not considered useful.~~

~~TKIP~~

~~The Temporal Key Integrity Protocol (TKIP) is a new protocol that will fix the known problems with WEP. TKIP uses the same ciphering kernel as WEP (RC4) but adds a number of functions:~~

- ~~128-bit encryption key.~~
- ~~48-bit Initialisation Vector.~~
- ~~New Message Integrity Code (MIC).~~
- ~~Initialisation Vector (IV) sequencing rules.~~
- ~~Per-packet key mixing algorithm that provides a RC4 seed for each packet.~~
- ~~Active countermeasures.~~

~~The purpose of TKIP is to provide a fix for WEP for existing 802.11b products. It is believed that essentially all existing 802.11b products can be software-upgraded with TKIP (all major 802.11 vendors participate in the 802.11i standardisation).~~

~~The TKIP MIC was designed with the constraint that it must run on existing 802.11 hardware. It does not offer very strong protection but was considered the best that could be achieved with the majority of legacy hardware. It is based on an algorithm called Michael that is a 64-bit MIC with 20-bit design strength. Details can be found in ref. [6].~~

~~The IV sequence is implemented as a monotonically incrementing counter that is unique for each key. This makes sure that each packet is encrypted with a unique <key,IV> pair, i.e. that an IV is not reused for the same key. The receiver shall also use the sequence counter to detect replay attacks. Since frames may arrive out of order due to traffic-class priority values, a replay window (16 packets) has to be used.~~

~~A number of "weak" RC4 keys have been identified for which knowledge of a few number of RC4 seed bits makes it possible to determine the initial RC4 output bits to a non-negligible probability. This makes it easier to cryptanalyze data encrypted under these keys. The per-packet mixing function is designed to defeat weak-key attacks. In WEP, the IV and the key are concatenated and then used as seed to RC4. In TKIP, the cryptographic per-packet mixing function combines the key and the IV into a seed for RC4.~~

~~Because the TKIP MIC is relatively weak, TKIP uses countermeasures to compensate for this. If the receiver detects a MIC failure, the current encryption and integrity protection keys shall not be used again. To allow a follow-up by a system administrator the event shall be logged. The rate of MIC failure must also be kept below one per minute, which means that new keys shall not be generated if the last key update due to a MIC failure occurred less than a minute ago. In order to minimize the risk of false alarms, the MIC shall be verified after the CRC, IV and other checks have been performed.~~

~~TKIP is an interim solution to support 802.11i on legacy hardware. It is not considered as secure as the AES solution (WRAP) but very much better than WEP.~~

~~WRAP (AES)~~

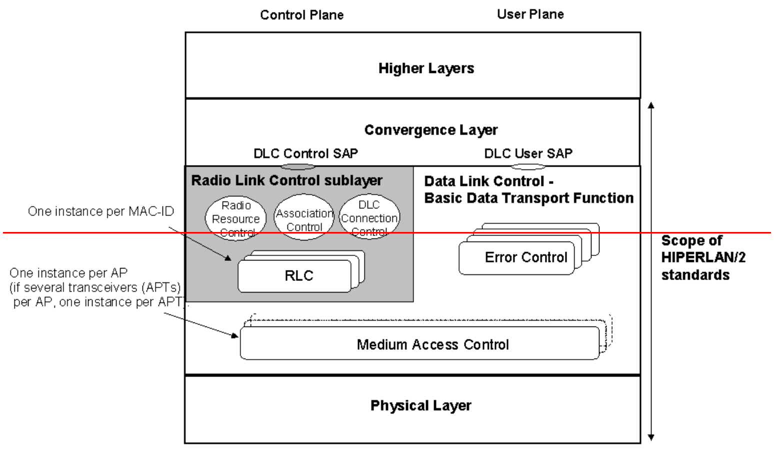
~~The Wireless Robust Authenticated Protocol (WRAP) is the long-term solution and is based on the Advanced Encryption Standard (AES). AES is a block cipher that can be used in different modes of operation. In 802.11i, two modes have been discussed: Offset Codebook (OCB) and Counter-mode with CBC-MAC (CCM). These two modes use AES differently to provide encryption and message integrity. OCB is a mode that provides both encryption and integrity in one run. CCM uses the Counter-mode for encryption and CBC-MAC for integrity. It is currently undecided if both or only one of the modes will be included in the final 802.11i spec. Both modes have been submitted to NIST as proposed block cipher modes.~~

~~The AES implementation requires hardware support and the majority of legacy 802.11b products will thus not be able to run WRAP.~~

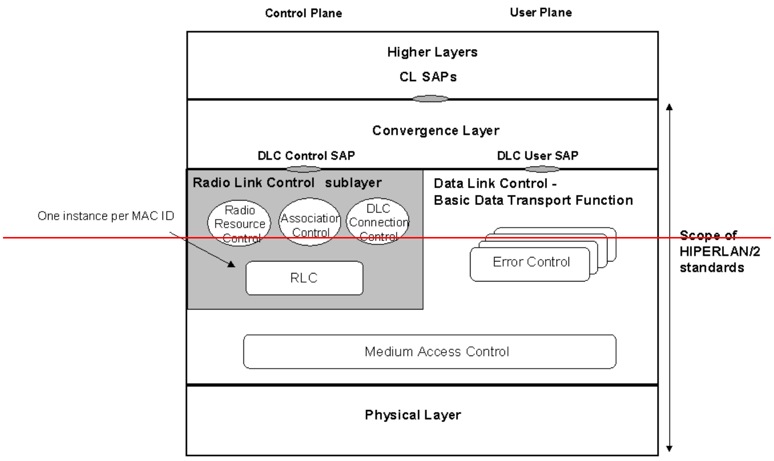
~~A.2 ETSI/BRAN~~

~~A.2.1 HIPERLAN/2 Security architecture~~

~~The BRAN Hiperlan/2 (references [9], [10], [11] and [12]) protocol stack consists of a physical layer at the bottom, a DLC layer in the middle, which includes the RLC sub-layer and the convergence layer(s) at the top. The RLC sub-layer is responsible for Radio Resource Control, Association Control and Data Link Control Connection Control. The DLC take cares of error control. Between the RLC and the DLC is the Medium Access Control located per instance of AP, cf. the two figures below.~~



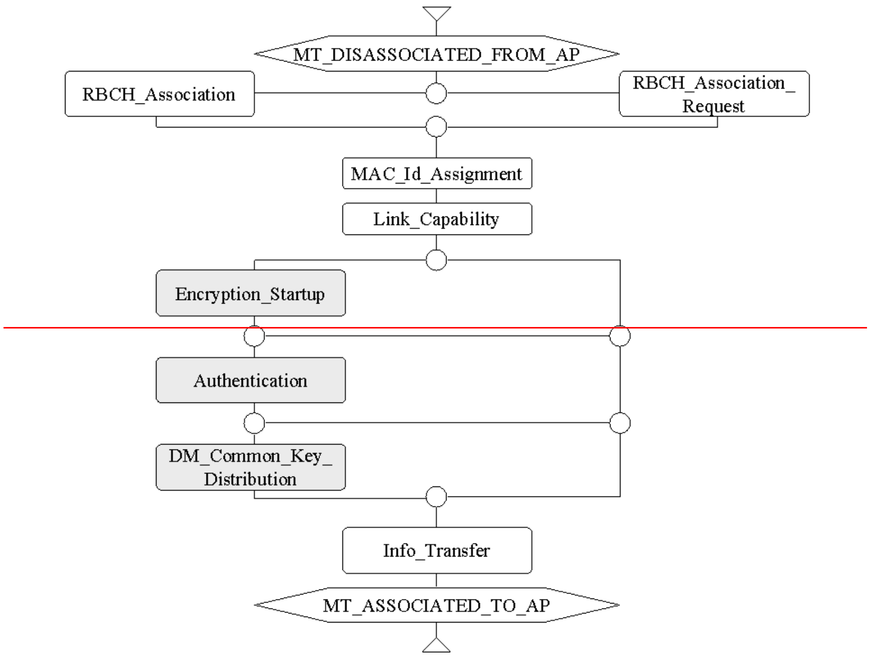
~~Figure A.4: Protocol stack in the AP/CC~~



~~**Figure A.5: Protocol stack in the MT**~~

~~An AP is a device responsible for the centralized control of the resources in a radio cell and is in the most cases connected to a fixed network. A CC is a device that that provides with the same functionality as an AP but is not necessarily connected to a fixed network. The term CC is normally used when the central controller and the MT functionality is located in single device.~~

~~The Association Control Function performs 1) encryption startup, 2) authentication and 3) DM Common Key Distribution (OMT/OAP) in that order, see figure below.~~



~~**Figure A.6: The Association Control Function**~~

~~A.2.1.1 Confidentiality protection~~

~~Confidentiality protection is provided for user data and part of RLC signalling. The protection can be provided between:~~

~~1 MT and AP/CC;~~

~~2 MT and MT (note that the AP has to be trusted).~~

~~The following algorithms are defined for confidentiality protection:~~

~~1 No-encryption;~~

~~2 DES, Data Encryption Standard;~~

~~3 Triple-DES (Optional).~~

~~A.2.1.2 Authentication~~

~~The authentication mechanism provides mutual authentication between the MT and the AP. If the authentication of the MT is successful then access to the connected fixed network is granted. It is the policy of the operator that decides whether authentication of the MT is necessary or not for access.~~

~~The authentication of the AP allows the MT to cancel an access attempt if the AP can not be proven to be authentic. The mechanism allows the MT to detect false AP. The authentication protocol is a challenge-response protocol.~~

~~Three protocols are defined, based on:~~

1. ~~Pre-shared keys~~
   - ~~A pre-shared key shall be at least 128 bits;~~
2. ~~RSA signatures~~
   - ~~Three lengths are supported: 512, 768 and 1024 bits (OAP/OMT);~~
3. ~~No Authentication.~~

~~How the keys for the authentication is generated, configured, stored and fetched is out of the scope of the Hiperlan/2 standard.~~

~~Each MT will be assigned an authentication key identifier (AKI). The AKI will be sent to the AP with which the MT has a Security Association. There are six different types that can be used:~~

1. ~~48-bit IEEE address;~~
2. ~~64-bit extended IEEE address;~~
3. ~~A NAI, Network Access Identifier;~~
4. ~~Distinguished name;~~
5. ~~Compressed type which is used when an available AKI is to long to be carried in the RLC messages;~~
6. ~~Generic type, which is a non-structured octet string.~~

~~A.2.1.3 Integrity protection~~

~~No integrity mechanism is defined for HIPERLAN/2.~~

~~A.2.2 Security mechanisms~~

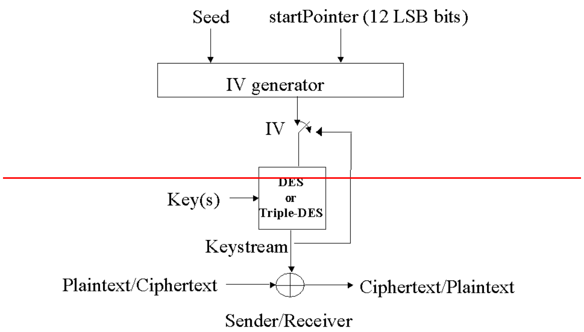
~~A.2.2.1 Confidentiality~~

~~Confidentiality protection can be used for Unicast, Multicast and Broadcast scenarios. In order to have Multicast and/or Broadcast confidentiality protection a Unicast encryption has to be established first. The Unicast encryption is optional to use.~~

~~The algorithms defined for confidentiality protection are:~~

- ~~DES which is mandatory to implement for AP/CC and MT;~~
- ~~Triple-DES (EDE mode) which is optional to implement for AP/CC and MT.~~

~~It is possible to provide confidentiality protection for the User Data Channel, User Multicast Channel, User Broadcast Channel, the Dedicated Control Channel and all LCH PDUs except the downlink RLC Broadcast Channel since it has to reach all MT's. The encryption/decryption mechanism is visualized in the figure below.~~



~~Figure A.7: The encryption/decryption function~~

~~Unicast~~

~~A Unicast security association is defined between a MT and an AP.~~

~~Calculate a Session Secret Key (SSK)~~

~~During an Encryption Startup both the MT and the AP calculate a public Diffie-Hellman value and send it to the other party.~~

~~This material is used at both sides to calculate an SSK.~~

~~Assume that the MT sends gx mod n and the AP sends gy mod n where~~

~~g=2 the generator of the group~~

~~n=2768-2704-1+264 *{ [2638pi] + 149686 }, First Oakley Group 1 (768 bit prime)~~

~~The AP and the MT now have a shared secret: gxy mod n, which is the basis for calculating the Session Secret Key.~~

~~DES~~

~~DES is mandatory to implement.~~

~~SSK is defined as the most significant 8 octets defined from KeyMat where:~~

1. ~~KeyMat=HMAC-MD5(gxy mod n, 0x00)~~
2. ~~KeyMat=HMAC-MD5(gxy mod n, 0x01)~~
3. ~~KeyMat=HMAC-MD5(gxy mod n, 0x02)~~
4. ~~etc.~~

~~This process ends when the SSK is found to be a non-weak and a non-semi-weak DES key.~~

~~Triple-DES~~

~~Triple-DES is optional to implement.~~

~~SSK is for this case defined as three keys k1, k2 and k3 where k1 is taken from KeyMat=K1|K2 as the most significant 8 octets, k2 as the next 8 octets and k3 as the following 8 octets where:~~

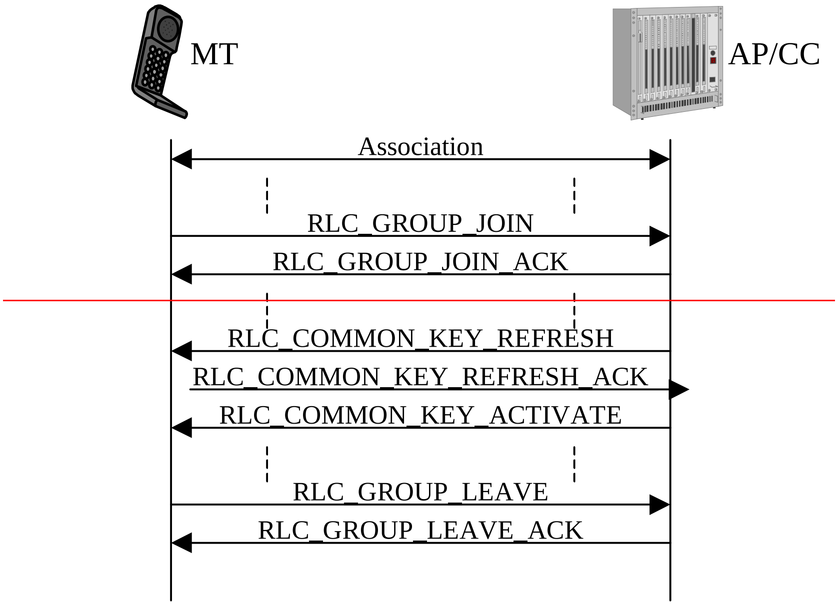
1. ~~K1= HMAC-MD5(gxy mod n, 0x00) & K2= HMAC-MD5(gxy mod n, K1|0x00)~~
2. ~~K1= HMAC-MD5(gxy mod n, 0x01) & K2= HMAC-MD5(gxy mod n, K1|0x01)~~

3. ~~K1= HMAC-MD5(gxy mod n, 0x02) & K2= HMAC-MD5(gxy mod n, K1|0x02)~~

4. ~~etc.~~

~~Until all three keys k1, k2 and k3 are unequal and that all of them are non-weak and non-semi-weak DES keys.~~

~~Multicast and Broadcast~~



~~Figure A.8: A Multicast example~~

~~To join a broadcast or multicast group, the MT must first be associated with an AP/CC. There are two ways of implementing multicast:~~

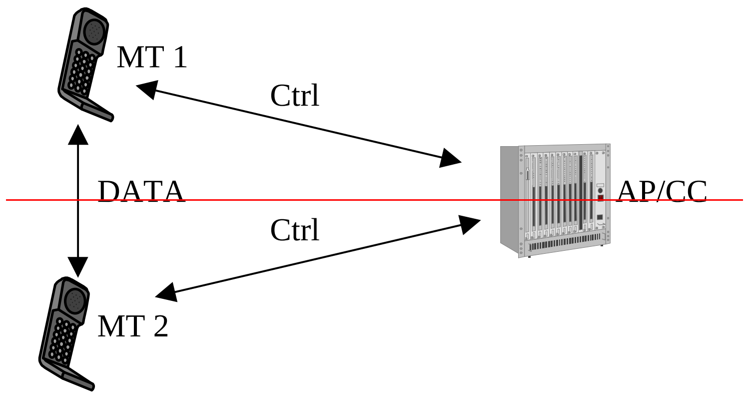
- ~~Using multicast MAC ID and transmitting the information once to the multicast group over the air;~~
- ~~Using n times unicast, i.e. transmitting the information individually to each member of the group.~~

~~The figure above describes a scenario where the MT joins a multicast group. The MT begins with sending a join-message, to indicate what group(s) it would like to join. In this message it also specifies what encryption algorithms it supports or would like to use. The AP/CC response consists of an acknowledgment, which includes the encryption algorithm and encryption key to be used for the group(s). The AP/CC is responsible for handling the key refresh. When a MT wishes to leave a group it sends a group-leave request to the AP/CC, which the AP/CC must acknowledge.~~

~~For the broadcast scenario, similar join and leave procedures apply for the MT, as in the multicast case. Instead of sending an RLC_GROUP_JOIN request the MT sends an RLC_CL_BROADCAST_JOIN request.~~

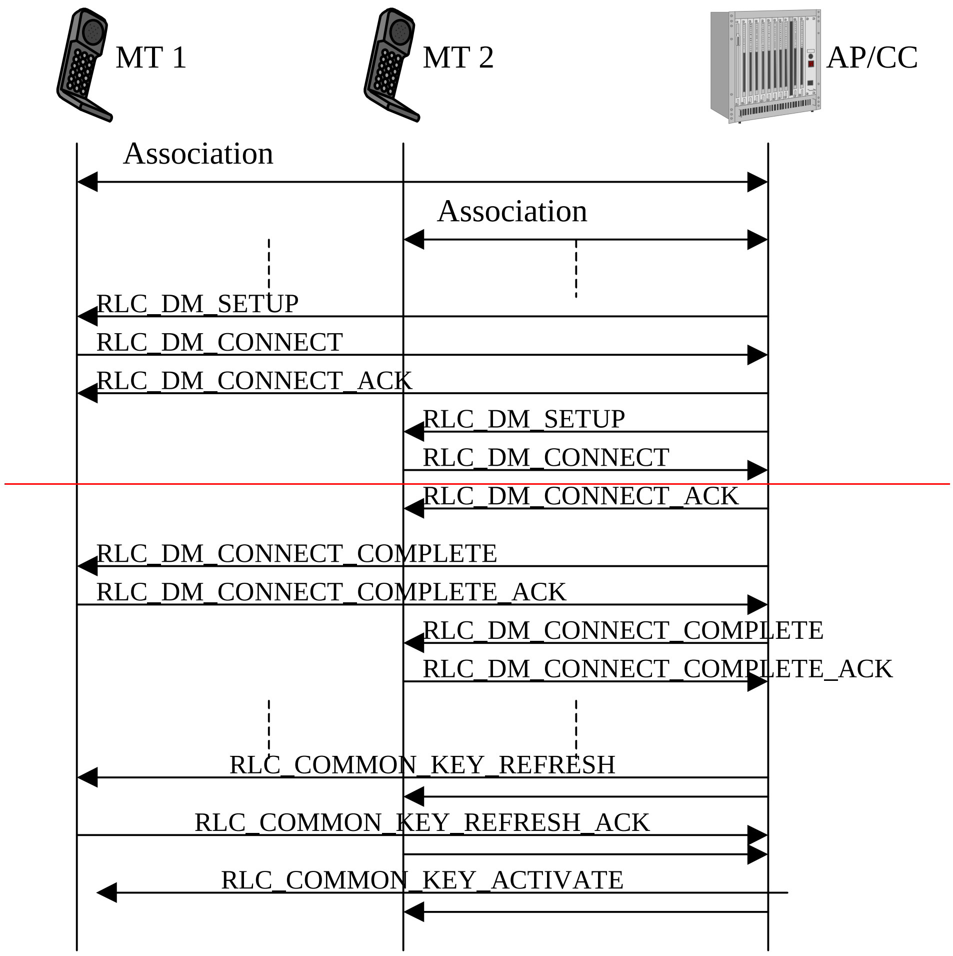
~~Direct Link Scenario~~

~~In a direct link connection, two mobile terminals set up a direct communication channel between themselves. The data will be sent directly between the terminal, while the AP/CC still handles the control functions (see figure below). Note that when direct link is not used between two parties, all traffic must go via the AP/CC. Therefore, the direct link is a feature that helps to off-load the AP/CC, so not all traffic have to be routed through it.~~



~~**Figure A.9: The data and control flow in a direct link scenario**~~

~~The figure above describes a small scenario where the AP/CC initiates a Direct Link Setup. Both terminals must be associated with the AP/CC before this can be done. The AP/CC initiates by sending the RLC_DM_SETUP message, which include information about the peer's MAC id, common attributes etc. The AP/CC is responsible for distributing a common encryption key to the terminals and also for handling (when needed) the key refresh. To synchronize the two terminals, the AP/CC sends the RLC_DM_CONNECT_COMPLETE message.~~



~~**Figure A.10: AP/CC Initiated DiL setup with key refresh**~~

~~A.2.2.2 Authentication~~

~~When encryption has been activated the mechanism for mutual authentication can start. Authentication with a pre-shared key is mandatory to implement and RSA based signatures are optional to implement. There are six different key identifiers and one of them is mandatory to be implement but since all of them are optional it is a choice to choose one of them. The MT fetches the authentication key of the AP based on identities that are sent over the broadcast channels.~~

~~The MT sends a RLC_AUTHENTICATION including the type of the AKI. Upon receiving this message the AP sends a challenge to the MT. The MT calculates the response and creates a challenge to the AP. The MT sends a RLC_AUTHENTICATION_AP to the AP including the response and the challenge. The AP checks the response and it is equals the expected response the AP sends a RLC_AUTHENTICATION_ACK including the response based on the challenge sent by the MT. The MT checks the response if it is a valid one i.e. if the AP is authentic.~~

~~Since the Diffie-Hellman exchange is vulnerable to a man-in-the-middle attack this mutual authentication mechanism prevents this attack. Furthermore the proposed and selected encryption and authentication alternative is checked to prevent an attack aiming for a lower security level than requested.~~

~~The challenge response protocol is based on a good random number generator but there is no random generator specified in the standards so it is implementation specific.~~

~~Pre-shared key~~

~~The keys have to be distributed to the MTs and the APs in a secure manner. It is suggested in the standard to use this key management to business and residential environment for scalability reasons.~~

~~The responses are calculated as:~~

~~Response=HMAC-MD5(Preshared Key, AuthenticationString)~~

~~AuthenticationString = challenge [| mt_dh | ap_dh |] auth_encryption_list | auth_encr_selected~~

~~The AuthenticationString shall include the received challenge, the proposed encryption and authentication algorithms proposed by the MT and the selected encryption and authentication algorithms selected by the AP. If encryption is chosen, i.e. Encryption Startup proceeded the Authentication, then the received Diffie-Hellman public value and the sent Diffie-Hellman public value shall also be included in the AuthenticationString. The challenge is 128 bit long and the Diffie-Hellman public value is 768 bit long. The length of the pre-shared keys shall be at least 128 bit long.~~

~~RSA-based~~

~~It is suggested in the standard that a public-key certificate signed by a trusted party is an efficient way to implement this system. A PKI, Public Key Infrastructure, is needed to issue, verify and revoke public-key certificates. The signature and the verification shall be calculated by using PKCS#1 and the MD5 hash algorithm. The response is calculated as:~~

~~Response=RSASSA_PKCS_V1_5_SIGN(Private Key, AuthenticationString)~~

~~The AuthenticationString is specified in the same way as for the pre-shared key case. There are three public key lengths specified: 512, 768 and 1024 bits.~~

~~A.3 IETF~~

~~A.3.1 Key Generation and EAP Methods~~

~~Reference [27] discusses the security aspects of EAP methods generating keys, distributing them to access points via AAA protocols such as Diameter EAP [23], and using them in establishing link-layer security~~

~~A.3.12 Co-Existence of RADIUS and Diameter~~

~~While Diameter does not share a common protocol data unit (PDU) with RADIUS [15], considerable effort has been expended in enabling backward compatibility with RADIUS, so that the two protocols may be deployed in the same network. Initially, it is expected that Diameter will be deployed within new network~~

~~devices, as well as within gateways enabling communication between legacy RADIUS devices and servers. This capability, described in [23], enables Diameter support to be added to legacy networks, by addition of a gateway or proxy speaking both RADIUS [EAP [15,26]] and Diameter EAP [23,24].~~

~~RADIUS is currently widely used protocol in WLAN environments. At the same time RADIUS is missing several features, such as server initiated messages and may not operate with the highest possible security turned on. Diameter is a better protocol, but it is not very widely deployed yet. Therefore, gradual migration from RADIUS to Diameter seems to be one potential way to go further.~~

~~It seems reasonable to start from an initial model of the AAA network where most or all of the access points implement only RADIUS, and a core which uses Diameter but is capable of talking to the RADIUS-only capable access points. This would mean that leaf AAA proxies should support both RADIUS and Diameter. As Diameter-capable access points are inserted to the network, they can be taken into use immediately. An advantage of placing the RADIUS/Diameter-capable nodes on the leafs of the network is that it becomes easier to take advantage of the features found in Diameter. For instance, even accounting may be more reliable if only the first hop is run in RADIUS but the traversal of the access provider, roaming consortium, and home operator proxies is done via DIAMETER.~~

~~The actual translation gateway must be able to run both RADIUS and Diameter protocols. The [24] extension defines a framework for the protocol conversion, where the RADIUS attribute space is included into Diameter, which eliminates the need to perform many attribute translations. However, some explicit translations between RADIUS and Diameter attributes must be made, like translating vendor specific and accounting information.~~

~~Some Diameter related messages cannot be translated during the communication with RADIUS client, such as messages initiated by Diameter server. Interoperability between RADIUS and DIAMETER in the presence of some of the non-standard RADIUS extensions has not been specified.~~

~~The gateway needs to add RADIUS application layer security mechanisms towards RADIUS, and IPsec or TLS towards Diameter. Given the use of the hop-by-hop security mechanisms, this translation can be performed without the knowledge of the original sender of the message. RADIUS requires pre-shared keys, while Diameter can take advantage of either IKE or TLS.~~

~~In addition, the translation gateway must secure attribute data towards the home server using Diameter CMS techniques (when the RFC is published). That is, end-to-end security mechanisms can be employed between the translation proxy and the home server, but not between the RADIUS-only access point and the translation proxy.~~

~~Diameter – RADIUS compatibility mode should support both protocols along with the necessary translation mechanisms in order to enable the use of RADIUS-only access points. Such translation should occur as near the leaves of the network as possible. As not all functions can be translated in full, some loss of functionality occurs for those devices, which use RADIUS.~~

~~It is possible to use IPSec in those cases where RADIUS is used, as currently required in RFC 2869bis. This may help to eliminate some of the vulnerabilities of RADIUS. In addition, 3GPP may adopt the use of RFC 2869bis and corresponding Diameter counterpart as the standard for running EAP over AAA protocols.~~

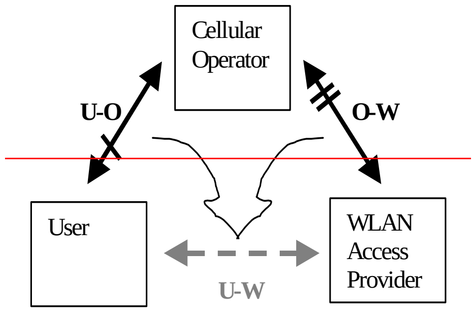
~~A.4 Bluetooth~~

~~Annex B (informative):~~
~~Trust Model~~

~~B.1 Trust model entities~~

~~Although any real implementation of a trusted access solution will depend on the exact system architecture, for the high-level concepts presented in this contribution we restrict attention to the three key players: the user/customer, the cellular operator, and the WLAN access provider.~~

~~Figure B.1 shows a simplified system model showing only the three roles and their trust relationships.~~



~~Figure B.1: Trust model~~

~~The cellular operator offers GSM/GPRS/UMTS services. Architecture-wise, the "cellular operator" box represents the complete cellular network (including radio access network, core network, service network), and also extends to partners in a roaming consortium.~~

~~The WLAN access provider offers public Wireless LAN access as a service. The "WLAN Access Provider" box in the figure groups the WLAN access network and its possible supporting nodes. The WLAN access provider may be "part of" (owned by) the cellular operator or a cellular roaming partner, or it could be a WLAN-only access provider or Wireless ISP.~~

~~The user in this model is assumed to be a subscriber/customer of the cellular operator who wishes to use both the traditional cellular services and the complementary (but not complimentary) WLAN access, when available. As such, the user is assumed to operate equipment capable of both GPRS/UMTS and WLAN access. This could be some combination of a phone (handset or PC-card) and a laptop / PDA, or possibly a combined WLAN/GPRS terminal. The collection of a user's devices acting on behalf of the user will often be called a client.~~

~~Legally, the user-operator trust relation, labelled "U-O" in figure B.1, is based on the service agreement between these two parties. From a technological perspective, this trust is embodied in a shared secret stored securely both on the user's (U)SIM and at the operator's Authentication Centre, and allows for an authenticated secure connection between the user's terminal and the cellular network.~~

~~If the cellular operator and the WLAN access provider are part of the same legal entity their trust relation is self-evident, and results in an intra-domain security solution. In the more general case, the operator-WLAN trust, labelled O-W in figure B.1, is based on roaming agreements or other partnerships (such as a Single Sign-On federation). Physically, this trust can translate to a security solution for roaming, AAA, trusted or semi-trusted servers in the context of WAP, or SMS-gateway access.~~

~~B.2 Trust relations~~

~~To design or evaluate a security solution, the trust relations between the participants must be identified. In a public WLAN access scenario, we have one or more operators and (possibly independent) access providers, and several subscribers.~~

~~The subscribers cannot trust each other. Someone else accessing the network from the same WLAN access network as the user, may be trying to perform DoS attacks targeted at the user, or eavesdrop on his traffic, steal his credentials to gain access at a later time, etc.~~

~~An operator cannot trust any mobile terminal that tries to connect to the network. Before authentication, the mobile station could belong to anyone, with or without a subscription. Even after a mobile station has been authenticated, the device may act maliciously. The user himself may be performing fiendish activities, or someone else may have hijacked his session.~~

~~The operators and/or access providers may choose to trust each other. Such trust relations normally rely on (legally binding) roaming agreements. If such an agreement is in place, a user may use another operator's access network, and will be authenticated by the "home operator". Depending on which solution is chosen, the user may have to put trust in other, visited operators, as well as in his home operator.~~

~~The cellular operators may provide the WLAN access in the future In addition, there also will be important WLAN-only operators on the market.. The level of trust of communication between the WLAN and the 3GPP system may be considered to have three levels –~~

~~1) The WLAN may be completely untrusted by the UE and the 3GPP system.~~

~~2) The WLAN contains elements that may be trusted by the UE and the 3GPP system. For example, the WLAN may include trusted servers that look after aspects of security and authentication interworking with the 3GPP systems (e.g. 802.1x, 802.11i). However, other elements of the network may be untrusted.~~

~~3) All of the elements of the WLAN may be fully trusted by the UE and the 3GPP system.~~

	~~LOW TRUST~~	~~HIGH TRUST~~
~~Access to services provided by the WLAN Access Provider~~	~~Charging based on usage or authorisation level.maybe risky for the Cellular Operator, the accounting information may be not reliable.~~ ~~Cellular Operator cannot grant user data protection.~~	~~Cellular Operator controls sessions, charging, authorisation, etc., based on information received from the WLAN Access Provider Network, and actions performed at said network.~~ ~~The WLAN Access Provider is trusted to grant adequate protection of user data.~~
~~Access to services provided by the Cellular Operator~~	~~Charging, authorisation enforcement, control of sessions, etc. must be performed at the Cellular Operator Network, counting on user data received via tunnels.~~ ~~The tunnelling mechanism must be able to provide data origin authentication and integrity protection at least.~~ ~~The tunnelling mechanism may have as end point either the HPLMN or the VPLMN, depending on some aspects e.g. the need to access services in the VPLMN~~	~~Charging, authorisation enforcement, control of sessions, etc. can be performed with participation of both networks.~~ ~~It may be unnecessary that the tunnelling mechanism implements any protection mechanism, if there is protection of user data in the WLAN AP and there is some security mechanism between the WLAN AP and the Cellular Operator.~~

~~Annex C (informative): Analysis of Threats~~

~~C.1 Security for Public WLAN Access~~

~~These questions related to security in the 3GPP-WLAN architecture must be addressed:~~

- ~~What needs to be protected? I.e., what are the assets, and to whom are they valuable?~~
- ~~What trust relations can be assumed? I.e., who can trust whom, and to what degree? The Trust Model is described in Annex B.~~
- ~~What are possible attacks against the assets, how can they be performed, and what is done to detect/prevent them?~~

~~In section 3 the relevant assents and threats to those assets are identified. section 4 contains examples of possible attacks. Countermeasures are not discussed in this contribution but the threats and specific attacks should be taken into consideration when defining security mechanisms for 3GPP-WLAN interworking.~~

~~C.2 Assets and Threats~~

~~This section describes different types of assets that are valuable to the parties involved. Threats to these assets are also identified.~~

~~C.2.1 3GPP Operator's Assets~~

~~C.2.1.1 Access to WLAN Services~~

~~The WLAN Services is what the 3GPP Network Operator is offering to its WLAN customers. The 3GPP Network Operator expects some benefit in return for providing this asset.~~

~~The following threats are relevant for this asset:~~

- ~~An attacker bypasses the access control and authorisation mechanisms in order to get the WLAN services for free.~~
- ~~An attacker impersonates a legitimate WLAN user. This way the attacker has free access to WLAN services and the victim gets charged for the attacker's usage of the services.~~
- ~~The attacker is a legitimate WLAN user in the sense that he has a customer relationship with the operator (i.e. a WLAN user account), but he bypasses the authorisation mechanism to get services he has not paid for.~~
- ~~The attacker interferes with the charging mechanism for the WLAN services, rending a legitimate user's bills incorrect.~~
- ~~The attacker is a legitimate WLAN user and he gets to interfere with the charging mechanism, e.g. to reduce the own bill.~~
- ~~The attacker is a legitimate prepaid user that avoids disconnection when the prepaid account expires.~~
- ~~The attacker prevents WLAN users from accessing to WLAN services (DoS).~~
- ~~The attacker prevents WLAN users from accessing to the operator's WLAN services, and sets up rogue "services" (e.g. propaganda) instead.~~

C.2.1.2 Non-WLAN Assets

Other 3GPP operator assets may not be offered over WLAN access networks. Such assets are e.g. access to GSM/UMTS CS services, access to GPRS services, etc. There is a threat that an attacker takes advantage of the WLAN access to perform attacks (e.g. impersonation, DoS, MitM, etc.) against these assets whenever the WLAN access is not properly secured and isolated.

C.2.2 WLAN User's Assets

Since the user's subscription can be considered as an asset for the 3GPP Network Operator, the assets of the user can be considered, to some extent, as 3GPP Operator's assets too. That is, if the user perceives that the utilisation of WLAN services poses a threat to his/her assets, it is likely that the user will avoid using those services, or that the price the user is willing to pay for the services will diminish. Moreover, users might claim liability of the 3GPP Network Operator for the damage caused to their assets.

C.2.2.1 Access to WLAN Services

From the WLAN user's standpoint, this is the asset the user expects to obtain. The user is willing to pay a price to get this asset.

The following threats should be considered:

- The WLAN user gets impersonated by an attacker, which obtains access to WLAN services at the user's expense. Moreover, the attacker can utilise the WLAN services of the victim to perform deceitful activities.
- An attacker gets to make the user charged for services that the victim has not requested.
- The WLAN user cannot get WLAN services due to a DoS attack against the network, or to a targeted DoS attack against that specific user.
- The WLAN user cannot access to the operator's WLAN services, and gets rogue "services" (e.g. propaganda) set up by an attacker instead.

Note that there is some overlapping between these threats and those relevant for this asset from the 3GPP Network Operator's standpoint. For instance, a DoS attack is a problem for the user in the sense that he/she cannot get the WLAN services. It is also a problem for the Operator because it cannot charge the users for the services while they are unavailable (unless they are charged as a flat rate) and the Operator's image gets damaged. Similar arguments can be used for the rest of the overlaps.

C.2.2.2 User Data and Privacy

The user expects that the data he sends/receives while accessing to WLAN services, and personal information (such as identity, which services he/she uses or where he/she is located at a given time) is kept away from unauthorised parties.

The following threats are relevant:

- An attacker obtains the information that the user sends/receives while accessing to WLAN services. This includes user credentials transferred during the authentication phase, as well as any other data (e.g. documents) exchanged once the user has gained access to the WLAN services. The attacker might know or not who the user is.
- An attacker manipulates or substitutes the information that the user sends/receives while accessing to WLAN services. The attacker might know or not who the user is.
- An attacker analyses the information sent/received by users (even if it is mostly concealed) in order to derive some personal information about the users (such as which services they are using or where they are located at a given time).
- An attacker obtains information about the user (permanent identity etc.) and traces where and when the user has been accessing WLAN services.

~~C.2.3 WLAN Access Network Provider's Assets~~

~~In principle, the WLAN Access Network is outside the scope of 3GPP-WLAN interworking standardisation. Nevertheless, it is important to consider the "Access to WLAN Services" asset of the WLAN Access Network provider, since it can be regarded as a part of the "Access to WLAN Services" asset of the 3GPP Operator. In fact, many threats against the 3GPP Operator's assets can be realised by attacking the WLAN AN. Therefore, it is important that 3GPP-WLAN interworking sets security requirements on the WLAN AN and/or chooses a security solution that is robust to different levels of WLAN AN security.~~

~~The same threats as for the "Access to WLAN Services" asset of the 3GPP Operator are valid here.~~

~~C.3 Attacks~~

~~This section is an attempt to give a concrete form to the threats of the previous section, and to identify several attacks that are applicable in a typical WLAN-3GPP interworking scenario. A single attack can be used to realise one or possibly several of the threats described in the Sec. 3, depending on the intent of the attacker. An attacker setting up a rouge AP may e.g. attempt to get free access, modify a legitimate user's traffic or do a Denial of Service attack. Most of the attacks are performed by an attacker in the WLAN AN but may have implications on the 3GPP operator's assets. Attacks can also be performed remotely over the Internet. For certain types of attacks, the perpetrator does not need to "be a part" of the network. Examples are some types of layer 2 attacks and certain DoS attacks, e.g. setting up a radio jammer in a hotspot. Other attacks require that the attacker has access to the WLAN AN or the Internet. It should be noted that an easy way of getting access to the WLAN AN is to simply become a legitimate subscriber.~~

~~The attacks are classified according to where the attack is performed/launched:~~

- ~~victim's WLAN UE;~~
- ~~attacker's WLAN UE and/or AP;~~
- ~~WLAN Access Network infrastructure;~~
- ~~other device on the Internet.~~

~~The attacks mentioned are by no means the only ones possible. Moreover, the actual possibility to carry out an attack may depend on the WLAN technology and the level of WLAN specific protection used.~~

~~Even though some attacks can be easily prevented no effort is made in this section to describe countermeasures.~~

~~C.3.1 Attacks at the Victim's WLAN UE~~

~~Open platform terminals may be infected by viruses, Trojan horses or other malicious software. The software operates without the knowledge of the user on his terminal, and can be used for different types of attacks:~~

- ~~If the user has credentials stored on a smart card connected to his terminal, a Trojan residing in the terminal can make fake requests to the smart card and send challenge-response results to another MS. For example, the owner of the latter MS could then get access with the stolen credentials.~~
~~Note that this attack is performed inside the terminal, and it is independent of the external link between the terminal and the smart card reader, which can be secured or assumed to be physically secure.~~
- ~~Trojans may perform all the usual activities: monitor the user's keyboard or sensitive data, and forward the information to another machine.~~
- ~~Malicious software can be used to perform Distributed DoS (DDoS) attacks. That is, several instantiations of the software (residing on different hosts) synchronise and start a DoS attack simultaneously against a target.~~
- ~~Malicious software could be trying to connect to different WLANs, just to annoy the user.~~

~~Alternatively, the (U)SIM in the cellular phone can be used remotely from the WLAN client through a serial, infrared, or Bluetooth connection; in order to use the phone as a smart card reader. As the terminal must access the (U)SIM in the phone, the link in between must be secure. Both cable and IR can be assumed physically secure, and Bluetooth will depend highly on the current Bluetooth security mechanism.~~

~~C.3.2 Attacks from an Attacker's WLAN UE and/or AP~~

~~Several types of attacks are possible if the attacker has access to a laptop with WLAN interfaces and/or an Access Point. Denial of Service (DoS) attacks are easy to launch, e.g. by setting up a radio jammer at the hot spot. For some WLAN technologies, the layer 2 control signalling is not integrity protected opening up for DoS attacks by e.g. disassociating legitimate users.~~

~~Unless protected, an attacker can easily eavesdrop on the traffic between a user and an AP. The only equipment needed to do this is a laptop with a WLAN interface.~~

~~In a rogue AP / rogue network attack, the attacker e.g. employs an AP (masqueraded as a legitimate AP in a given hotspot) connected to a WLAN UE. Based on signal strength, an unsuspecting WLAN UE may connect to the rogue AP. This type of attack can be used to realise several different threats. The attacker could possibly modify the user's traffic or divert the traffic to a network other than the WLAN AN the user intended to use. The attacker could e.g. also fake a network or a commercial site to get access to e.g. credit card information. The attacker can also act as a Min in the Middle during the authentication procedure and cause the MAC/IP address-pair of the attacking WLAN UE to be bound to the credentials of the legitimate user. As a consequence, the attacker gains access to anything the legitimate user would, while the legitimate user is denied access.~~

~~An important class of IP-network attacks relevant in connection with rogue AP / networks are "service spoofing" attacks, where the attacker impersonates one or several services/servers in the network, e.g., a DNS server or a DHCP server. These attacks could be performed e.g. by setting up a rouge AP. Another set of attacks uses fake configuration/control messages (such as ARP or ICMP messages) to redirect a user's traffic. ARP spoofing could also be used to redirect the AP's traffic, e.g. AAA messages generated by the AP. Note that the above include only the best-known and most serious attacks. Given the rich (and always expanding) set of protocols run over IP, all possible attacks could not be accounted for.~~

~~Another way to interfere or possibly gain access for an attacker is to simply eavesdrop on the traffic around an AP. Depending on WLAN technology and the level of protection, the MAC and IP addresses may be sent in the clear (they are not encrypted) and the attacker can record these. When the attacker knows the MAC/IP address-pair of a user currently connected, he can set his own addresses to the same values.~~

~~C.3.3 Attacks at the WLAN AN Infrastructure~~

~~Attacks can be performed at the WLAN AN infrastructure, e.g. Access Points (AP), the LAN connecting the APs, Ethernet switches etc. To perform any type of attacks "inside" the WLAN AN, the attacker needs access to the network in some way. For ordinary wired networks, an attacker needs to somehow hook up to the wires to get access. The WLAN AN is partially a wired network, and an attacker may hook up to that part of the network. In public spaces the APs and corresponding wired connections may be physically accessible by attackers. Simply connecting a laptop to the wired LAN "behind" the APs may give the attacker free access to WLAN services as well as access to other user's data and signalling traffic.~~

~~Depending on where charging data is collected, an attacker with access to the wired LAN of the WLAN AN can also interfere with the charging functions. If the volume based charging model is applied, an attacker could e.g. inject packets with any chosen source or destination MAC and IP addresses, just to increase a user's bill.~~

~~C.3.4 Attacks Performed by Other Devices on the Internet~~

~~Several attacks can be performed from devices connected to the Internet.~~

~~If the volume based charging model is applied, an attacker could flood a user with garbage packets, just to increase the user's bill. This is e.g. effective if the attacker resides somewhere on the Internet with a flat rate charging model, or if the attacker has infected other users' machines with "bot"-software. (Bot is short for robot, and refers to software that "lives on its own"). The bot could for instance listen for connections on a certain port, and when receiving a command from the attacker on that port, it starts flooding a given IP address with packets. Various distributed denial of service (DDoS) tools using such bots are known and available in the hacker world.~~

~~C.3.5 Implications of the A5/2 Attack for 3GPP WLAN Access~~

~~This annex provides an analysis of the implications of the A5/2 attack on 3GPP WLAN access, and provides recommendations on how to mitigate the impacts of the attack to 3GPP WLAN access~~

~~Barkan et.al. [28] presented a real-time attack on A5/2 algorithm in [Bar03]. The attack breaks the A5/2 algorithm. In the man-in-the middle version of the attack, the terminal is forced to use A5/2, while the attacker can use A5/1 against the network. The keys that are used for A5/2 algorithm can be used also with A5/1 cipher. Unfortunately, the vulnerability spreads also to A5/3 and GEA algorithms. The main reasons to the A5/2 flaws are: weak cipher, no bidding down protection and usage of same keys for different algorithms. The attack affects SIM usage. This analysis reflects the impacts from WLAN access point of view. The implications can be analyzed as follows:~~

~~Scenario:~~	~~Implication:~~
~~1. SIM shared between WLAN device and GSM device~~	~~A5/2 should not be allowed in the terminal, OR~~ ~~Some key separation countermeasures should be used in the terminal, OR~~ ~~A5/2 vulnerability may reveal Kc and this may allow WLAN terminal impersonation towards 3G network~~

~~Based on the analysis, it may make sense to avoid the use of the A5/2 algorithm in the terminal and/or provide some countermeasures against the attack. If A5/2 is used and there is an attack against it, Kc may be revealed. This implies that the A5/2 vulnerability can spread from the GSM network to the WLAN network. This, in turn, implies that the revealed Kc may be used to impersonate a terminal in the WLAN-3G network towards the network. Similarly an attack using A5/2 can destroy the confidentiality of the WLAN radio access, as the Kc:s used can be retrieved via A5/2 attacks.~~

~~It should be noted that the threats applies to EAP-SIM, as specified in 33.234. EAP-SIM can be attacked whenever a few valid GSM triplets have been retrieved.~~

~~It should also be noted that in order to alleviate the security problem with the A5/2 attack new terminals are required cf. the discussion on the Special RAND or that a USIM is used instead of a SIM. The exact terminal and network requirements on how to alleviate the A5/2 issues are currently studied in 3GPP and it is proposed that those requirements shall also apply to WLAN and 3G interworking for consistency reasons. So, for example, if the special RAND mechanism is adopted then special RANDs should be sent to WLAN AAA servers to prohibit the use of all A5 and GEA algorithms. When the GSM device implements the special RAND mechanism, this will protect against a man-in-the-middle exploiting a weakness in any GSM algorithm in order to masquerade as a WLAN client or eavesdrop the WLAN communications.~~

~~Annex D (informative): Management of sequence numbers~~

~~The example sequence number management schemes in [21] Informative Annex C can be used to ensure that the authentication failure rate due to synchronization failures to kept sufficiently low when the same sequence number mechanism and data is used for authentication in the PS/CS domains, in IMS and WLAN. This can be done by enhancing the method for the allocation of index values in the AuC so that authentication vectors distributed to different service domains shall always have different index values (i.e. separate ranges of index values are reserved for PS, CS ,IMS operation and WLAN access). The AuC is required to obtain information about which type of service node has requested the authentication vectors. Reallocation of array elements to the IMS domain can be done in the AuC with no changes required to already deployed USIMs.~~

~~As the possibility for out of order use of authentication vectors within the WLAN service domain may be quite low, the number of existing array elements that need to be reallocated to the WLAN domain could be quite small. This means that the ability to support out of order authentication vectors within the PS, CS and IMS domains would not be significantly affected.~~

~~Sequence number management is operator specific and for some proprietary schemes over the air updating of the UICC may be needed.~~

~~Annex E: Alternative Mechanisms for the set up of UE-initiated tunnels (Scenario 3)~~

~~Editor's note: the discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing. The text in section 6.1.5 reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in this Annex X. They may be replace the current working assumption in section 6.1.5 of the main body if problems with the working assumptions arise. Otherwise, this annex will be removed before the TS is submitted for approval.~~

~~Annex E1: IKE with subscriber certificates~~

~~The UE and the PDG use IKE, as specified in [rfc2409], in order to establish IPsec security associations.~~

~~Public key signature based authentication with certificates, as specified in [rfc2409], is used in order to authenticate the PDG and the UE.~~

~~A profile for IKE is defined in section 6.5.~~

~~Annex E2: IKEv2 with subscriber certificates~~

~~The UE and the PDG use IKEv2, as specified in [ikev2], in order to establish IPsec security associations.~~

~~Public key signature based authentication with certificates, as specified in [ikev2], is used in order to authenticate the PDG and the UE.~~

~~A profile for IKEv2 is defined in section 6.5.~~

~~Annex EF (informative):~~ ~~Change history~~

~~Change history~~							
~~Date~~	~~TSG #~~	~~TSG Doc.~~	~~CR~~	~~Rev~~	~~Subject/Comment~~	~~Old~~	~~New~~
~~2002-07~~					~~First draft created by the editor~~		~~0.1.0~~
~~2002-11~~					~~Updated after SA3#25~~	~~0.1.0~~	~~0.2.0~~
~~2002-11~~					~~Updated after SA3#26~~	~~0.2.0~~	~~0.3.0~~
~~2003-03~~					~~Updates after SA3#27~~	~~0.3.0~~	~~0.4.0~~
~~2003-06~~					~~Updates after SA3#28~~	~~0.4.0~~	~~0.5.0~~
~~2003-09~~					~~Updates after SA3#29~~	~~0.5.0~~	~~0.6.0~~
~~2003-11~~					~~Updates after SA3#30~~	~~0.6.0~~	~~0.7.0~~
~~2003-12~~					~~Updates after SA3#31~~	~~0.7.0~~	~~0.8.0~~