3GPP TSG SA WG3 Security — SA3#26 **S3-020695**
19- 22 November 2002, Oxford, UK

3GPP TS 33.234 V0.~~2~~3.0 (2002-11)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Service and System Aspects;
3G Security;
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

The present document studies 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] 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, "PPP Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-~~04~~06, ~~June~~ November 2002, "EAP AKA Authentication".

[5] draft-haverinen-pppext-eap-sim-~~05~~07, ~~June~~ November 2002, "EAP SIM Authentication".

~~[5] IEEE P802.1X/D11, March 2001, "Standards for Local Area and Metropolitan Area Networks: Standard for Port Based Network Access Control".~~

[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 TR 21.905: "Vocabulary for 3GPP Specifications"

[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)", September 2001

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

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

3 Definitions, symbols and abbreviations

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.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

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

4 Security Requirements for the 3GPP-WLAN Interworking

[Editor's note: This section shall have a description of the overall architecture for the ~~WLAN~~ 3G-WLAN interworking system ~~and explaining text on the trust relations, possible threats~~ and a list of the identified security requirements]

4.1 Security architecture and Roles

[Editor's note: This architecture is copied from SA2's TS 23.xxx v0.1.0 for the first draft of this TS, and shall be updated in later versions according to the work done in SA3]

4.1.1 Reference Model

The home network is responsible for access control. The Wx interface is intra-operator. The 3GPP network interfaces to other 3GPP networks, WLANs, and intermediate networks via the Wr interface.

The 3GPP proxy AAA relays access control signalling to the home 3GPP AAA server.

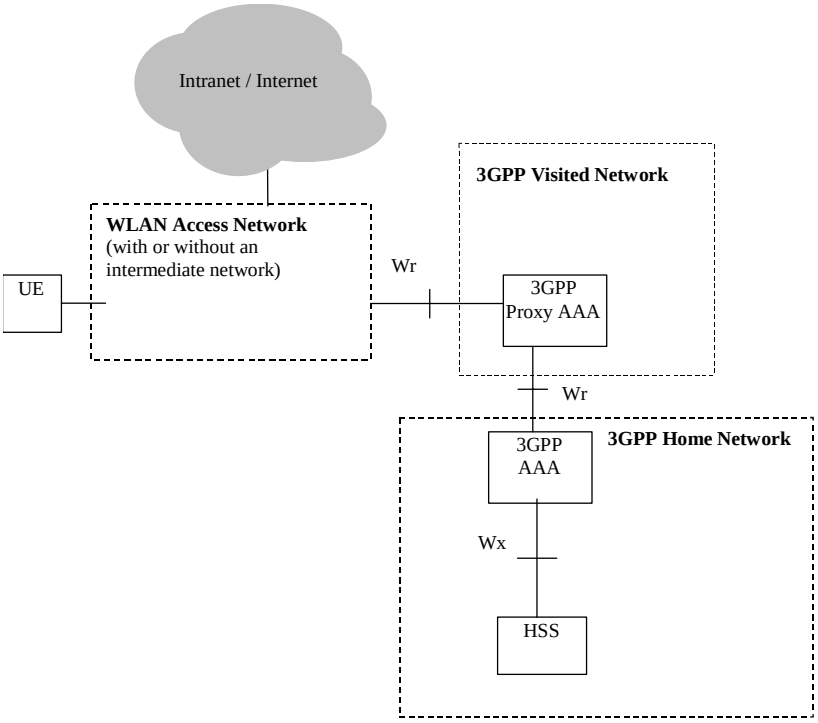


Figure 4.1 Access Control Reference Model

4.1.2 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** (~~potentially~~ equipped with (U)ICC card) utilised by a 3GPP subscriber to access the WLAN interworking service. The WLAN-UE may be capable of WLAN access only, or it may be capable of both WLAN and 3GPP System access. Some WLAN-UE may be capable of simultaneous access to both WLAN and 3GPP systems. The WLAN-UE may include terminal types whose configuration (e.g. interface to a UICC), operation and software environment are not under the exclusive control of the 3GPP system operator. For instance, the WLAN-UE may be a laptop computer or PDA with a WLAN card, UICC card reader and suitable software applications, or the UICC may reside in the 3GPP ME and be accessed through Bluetooth, IR or serial cable interface. 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 and subscriber profile (including subscriber's authorisation 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.

  - registers its (the 3GPP AAA server) address or name with the HLR/HSS for each authenticated and authorised 3GPP subscriber.

  - may act also as a AAA proxy (see above).

4.2 Security Requirements

~~*[Editor's note: These requirements are copied from TS 23.xxx v0.1.0 for the first version of this TR, and shall be reviewed and updated according to the input from the preceding sections]*~~

4.2.1 General

~~- Legacy WLAN terminals should be supported.~~

~~- Minimal impact on the user equipment, i.e. client software.~~

~~- The need for operators to administer and maintain end user SW should be minimized~~

~~- Existing UICC cards should be supported.~~

~~- Changes in the HSS/HLR/AuC should be minimized.~~

- The security data, i.e. long-term keys, which are stored on the UICCcard must not be sent from the card itself. Instead the interface to the UICC card should be of type challenge-response, i.e. a challenge is sent to the UICC card and a response is received in return.
- The subscriber should have at least the same security level for WLAN access as for his current cellular access subscription (i.e. GSM or UMTS)
- Mutual Authentication shall be supported for GSM and UMTS subscribers
- The selected Authentication solution should also allow for Authorisation

~~- Methods for key distribution to the WLAN access NW shall be supported~~

- For UMTS subscribers, the selected WLAN authentication mechanisms for 3GPP interworking shall provide at least the same security as 3GPP System authentication procedure. For GSM subscribers, the selected WLAN authentication mechanisms for 3GPP interworking shall provide at least the same security as the GSM system authentication procedure
- Subsequent WLAN re-authentication shall not compromise the requirement for 3GPP/GSM System equivalent security
- Selected WLAN Authentication mechanisms for 3GPP interworking shall support agreement of session keying material.
- Selected WLAN key agreement and key distribution mechanism shall be secure against man in the middle attacks. In other words, a man in the middle shall not be able to learn the session key material.
- The WLAN technology specific connection between the ~~WLAN~~ WLAN-UE and WLAN AN shall be able to utilise the generated keying material for protecting the integrity of an authenticated connection
- It shall be possible to store all long-term security credentials used for subscriber and network authentication in a tamper resistant memory such as the UICC card.

4.2.2 User identity privacy

- Any secret keys used in WLAN AAA servers for the generation of pseudonyms should be infeasible to recover (even for an attacker that has available a number of matching permanent identities and pseudonyms).
- Given a pseudonym (or even a number of correlated pseudonyms), it should be infeasible for an attacker to recover the corresponding permanent identity.
- It should be infeasible for an attacker to determine whether or not two pseudonyms correspond to the same permanent identity.
- It should be infeasible for an attacker to generate a valid pseudonym (irrespective of the underlying permanent identity).

- It should be infeasible for an attacker to generate a valid pseudonym corresponding to a given permanent identity.

4.2.3 WLAN-UE Functional Split

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 carrying security-relevant information must be adequately protected against eavesdropping and undetected modification. This protection may be provided by physical or cryptographic means.
- The endpoints of a local interface must be authenticated and authorised. The authorisation may be implicit in the security set-up.
- The involved devices must be adequately protected against attacks on stored security-relevant information

5 Security features

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

5.1 Authentication of the subscriber and the network and Key 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 Authentication

WLAN Authentication signalling is executed between ~~WLAN~~ 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 signalling over the WLAN Radio interface

WLAN authentication signalling is carried between ~~WLAN~~ 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 multivendor 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 authentication signalling between the WLAN access network and the 3GPP network

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 or RADIUS protocols.

5.1.4 User Identity Privacy

User identity privacy (Anonimity) 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 use the received identifier at the next authentication. Pseudonyms are not stored in any node in the network. 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 a number of "active" pseudonyms.

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.]

5.2 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~~(hop-by-hop or end-to-end) and protection at different layers]

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]

5.4 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

[Editor's note: This section shall deal with the network capability to terminate ongoing subscriber activitiesin the WLAN access when this is required due to e.g. end of subscription, expiration of charging account, detection of fraudulent activities, etc.]

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 Authentication

USIM based authentication is a proven solution that satisfies the authentication requirements from section 4.2. However, requiring USIM based authentication does not automatically mean that the USIM needs to be included in the WLAN card, for example the WLAN device can be linked with a WLAN-UE supporting a USIM via, for example Bluetooth, Irda, USB or serial cable.

6.1.1.1 EAP/AKA Procedure

USIM based authentication may be based on existing AKA method. In the case of WLAN-3GPP system interworking, this method should be supported by a generic authentication mechanism (independently of the underlying WLAN standard), e.g. EAP. EAP/AKA authentication mechanism is described in Internet Draft draft-arkko-pppext-eap-aka (ref. [4]). The following procedure is based on EAP/AKA authentication mechanism:

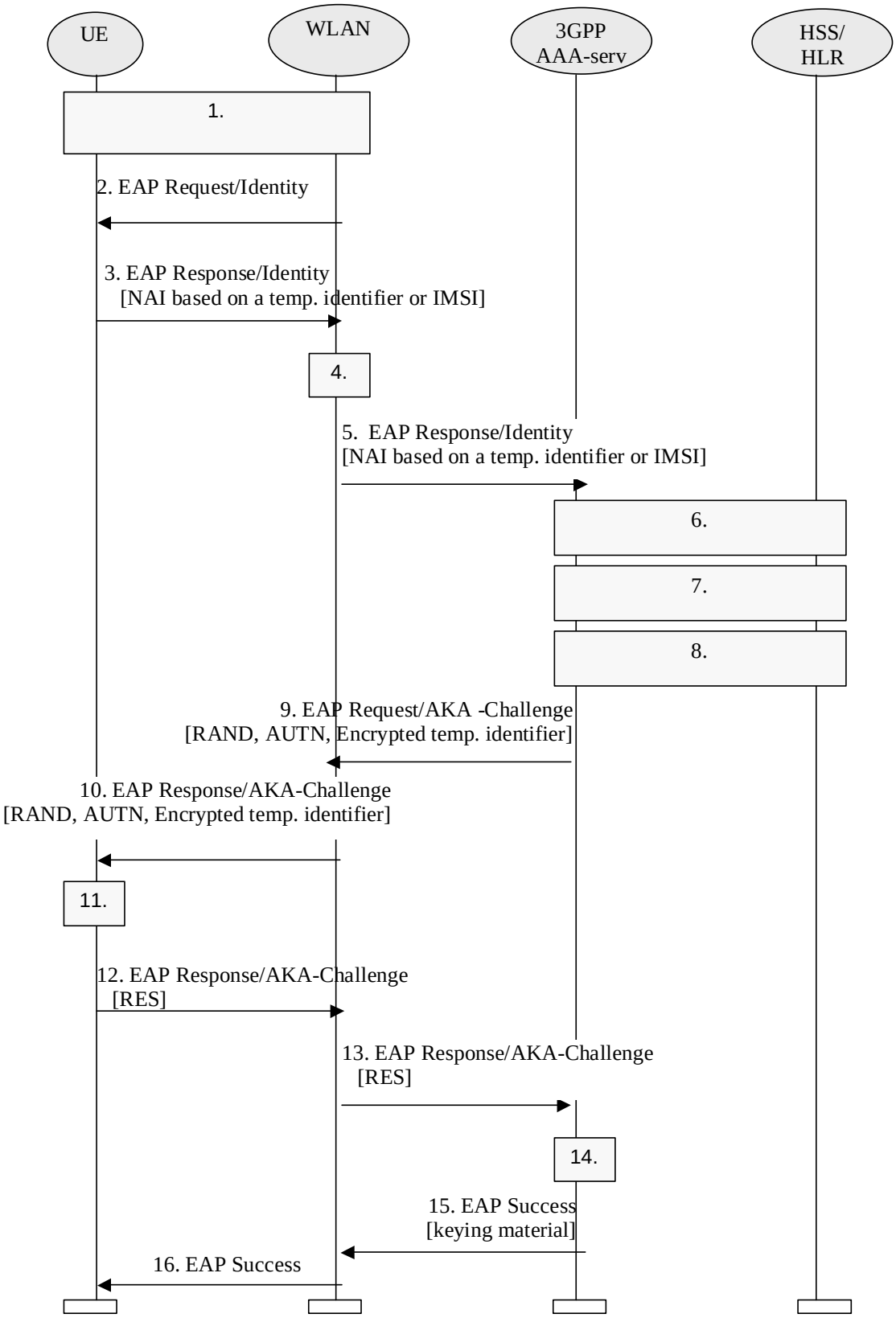


Figure 7.1 Authentication based on EAP AKA scheme

1. After WLAN connection establishment, Extensible Authentication Protocol is started with a Wireless LAN technology specific procedure (out of scope for 3GPP).

2. The WLAN 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 starts EAP AKA authentication procedure by sending an EAP Response/Identity message. The WLAN-UE sends its identity complying to 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 draft (draft-arkko-pppext-eap-aka-03.txt).

4. The 3GPP AAA Server is chosen based on the NAI.

Note : diameter/radius proxy chaining and/or diameter referral can 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 checks that it has an authentication vector available (RAND, AUTN, XRES, IK, CK) for the subscriber from previous authentication. If not, a set of authentication quintuplets is retrieved from HSS/HLR. A mapping from the temporary identifier to the IMSI may be required.

7. 3GPP 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 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. The extra keying material is required in order to pass the encrypted and integrity protected temporary identifier to the WLAN-UE. The keying material may also be used for WLAN technology specific confidentiality or integrity protection.

A new pseudonym is chosen and encrypted.

9. 3GPP AAA Server sends RAND, AUTN, and encrypted temporary identifier to WLAN in EAP Request/AKA-Challenge message.

10. The WLAN 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 (not shown in this example). If AUTN is correct, the USIM computes RES, IK and CK.

~~UE~~WLAN-UE derives required additional keying material from IK and CK. ~~UE~~WLAN-UE decrypts pseudonym and saves it to be used on next authentication.

12. ~~UE~~WLAN-UE sends EAP Response/AKA-Challenge containing calculated RES to WLAN

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

14. 3GPP AAA Server compares XRES and the received RES.

15. If the comparison in step 14 is successful, then 3GPP AAA Server sends the EAP Success message to WLAN. The 3GPP AAA Server includes the derived keying material in the message. WLAN stores the keying material to be used in communication with the authenticated ~~UE~~WLAN-UE.

16. WLAN informs the ~~UE~~WLAN-UE about the successful authentication with the EAP Success message. Now the EAP AKA exchange has been successfully completed, and the ~~UE~~WLAN-UE and the WLAN share session key material.

Note 1: The 3GPP AAA Server that is referred to in this diagram is the one that actually realises the authentication. If AAA Proxies are used between the WLAN Access Network and the AAA Server, they are not referred to in this diagram.

Note 2: Temporary identifier generation and storage is FFS.

6.1.2 GSM SIM based authentication

GSM SIM based authentication is useful for GSM subscribers that do not have a UICC card with a USIM application. SIM based authentication, with enhancements for network authentication, satisfies the authentication requirements from section 4.2.

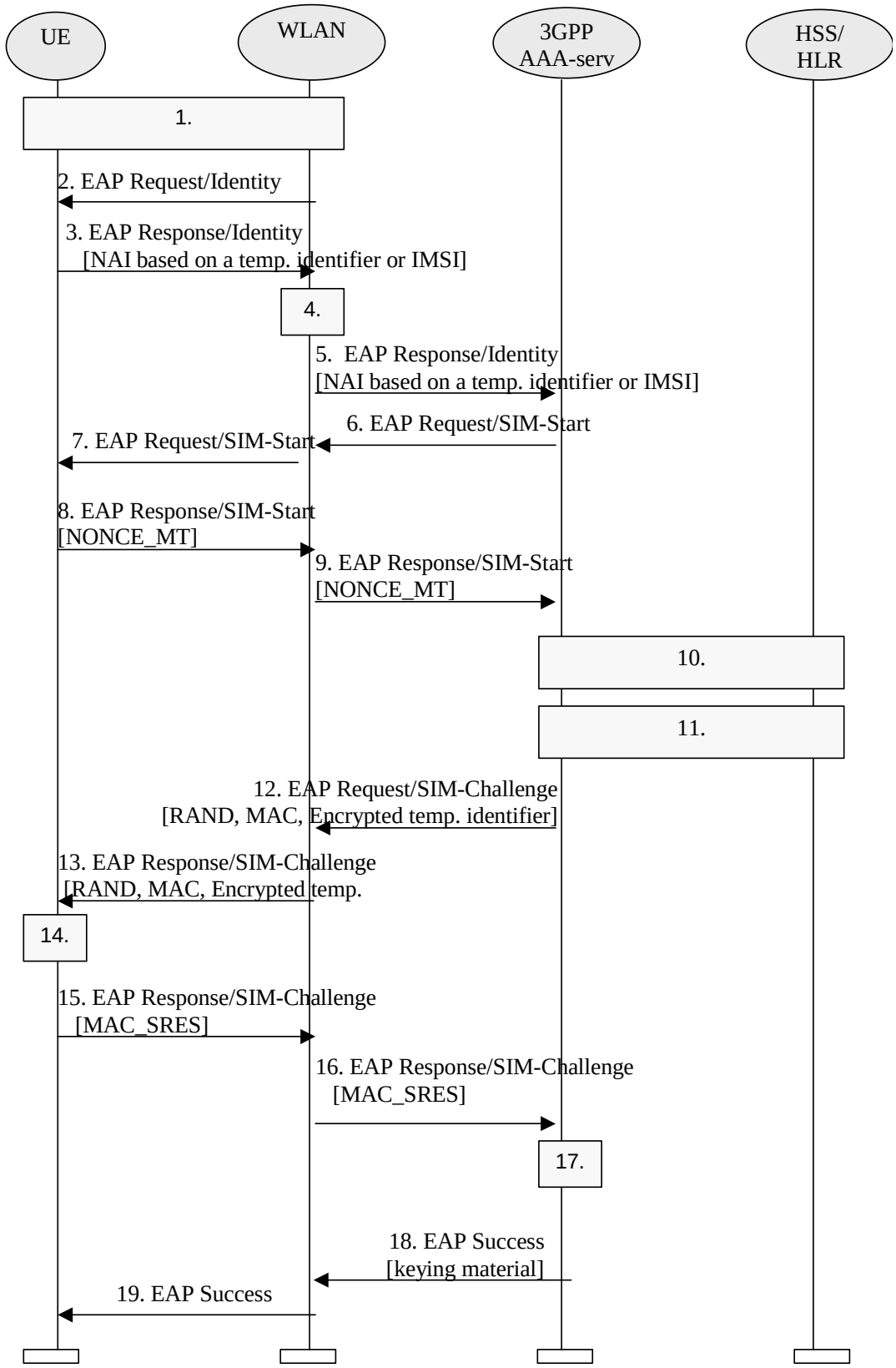
However, requiring SIM based authentication does not automatically mean that the SIM needs to be included in the WLAN card, for example the WLAN device can be linked with a UE supporting a SIM via, for example Bluetooth, Irda, USB or serial cable.

6.1.2.1 EAP SIM procedure

SIM based authentication shall be based on existing GSM AKA method but shall include enhancements for network authentication. In the case of WLAN-3GPP system interworking, this method should be supported by a generic authentication mechanism (independently of the underlying WLAN standard), e.g. EAP.

EAP SIM authentication mechanism is described in Internet Draft draft-haverinen-pppext-eapsim (ref. [5])

The following procedure is based on EAP SIM authentication mechanism:



7.2 Authentication based on EAP SIM scheme

1. After WLAN connection establishment, Extensible Authentication Protocol is started with a Wireless LAN technology specific procedure (out of scope for 3GPP).

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

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

3. The ~~UE~~WLAN-UE starts EAP SIM authentication procedure by sending an EAP Response/Identity message. The ~~UE~~WLAN-UE sends its identity complying to Network Access Identifier (NAI) format specified in RFC 2486. NAI contains either a temporary identifier (pseudonym) allocated to ~~UE~~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 (draft-haverinen-pppext-eap-sim-04.txt).

4. The 3GPP AAA Server is chosen based on the NAI.

Note : diameter/radius proxy chaining and/or diameter referral can 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 guesses, based on the NAI, that the subscriber is a GSM user; hence it sends the EAP Request/SIM-Start packet to WLAN.

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

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

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

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

10. 3GPP AAA Server checks that it has N (usually two or three) available authentication triplets (RAND, SRES, Kc) for the subscriber from previous authentication. Several triplets are required in order to generate longer session keys. If N triplets are not available, a set of authentication triplets 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. 3GPP 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. The extra keying material is required in order to calculate a network authentication value and to pass the encrypted and integrity protected temporary identifier to the ~~UE~~WLAN-UE. The keying material may also be used for WLAN technology specific confidentiality or integrity protection.

A message authentication code (MAC) is calculated over the RAND challenges using a newly derived key. This MAC is used as a network authentication value.

A new temporary identifier is chosen and encrypted.

3GPP AAA Server sends RAND, MAC, and encrypted temporary identifier to WLAN in EAP Request/SIM-Challenge message.

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

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

This computing gives N SRES and Kc values.

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

The ~~UE~~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 ~~UE~~WLAN-UE cancels the authentication (not shown in this example). The ~~UE~~WLAN-UE continues the authentication exchange only if the MAC is correct.

~~UE~~WLAN-UE decrypts pseudonym and saves it to be used on next authentication.

~~UE~~WLAN-UE calculates a combined response value MAC_SRES from the N SRES responses.

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

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

17. 3GPP AAA Server compares its copy of the MAC_SRES with the received MAC_SRES.

18. If the comparison in step 17 is successful, then 3GPP AAA Server sends the EAP Success message to WLAN. The 3GPP AAA Server includes the derived keying material in the message. WLAN stores the keying material to be used in communication with the authenticated ~~UE~~WLAN-UE.

19. WLAN informs the ~~UE~~WLAN-UE about the successful authentication with the EAP Success message. Now the EAP SIM exchange has been successfully completed, and the ~~UE~~WLAN-UE and the WLAN share session key material.

Note 1: The 3GPP AAA Server that is referred to in this diagram is the one that actually realises the authentication. If AAA Proxies are used between the WLAN Access Network and the AAA Server, they are not referred to in this diagram.

Note 2: Temporary identifier generation and storage is FFS.

Note 3 : the derivation of the value of N is for further study

6.2 Confidentiality mechanisms

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

6.3 Integrity mechanisms

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

6.4 Temporary identity management

6.4.1 Pseudonym Generation

Pseudonyms 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)

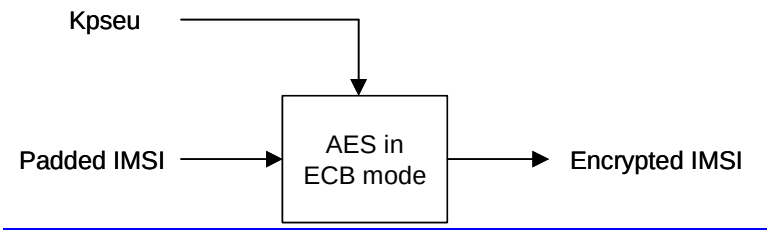
   Compressed IMSI = 0xF2 0x14 0x07 0x01 0x23 0x45 0x67 0x89

   Observe that, at reception of a pseudonym, 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*.

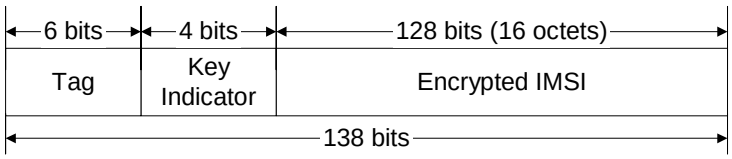
A 128-bit secret key, Kpseu, is used for the encryption. The same secret key must be configured at all the WLAN AAA servers in the operator network so that any WLAN AAA server can obtain the permanent identity from a pseudonym generated at any other WLAN AAA server (see section 6.4.2).

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



The *Pseudonym 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, then the permanent user identity must be requested from the WLAN client. As the procedure to request the permanent user identity is different in EAP-SIM and EAP-AKA, the *Pseudonym Tag* must be different for EAP-SIM pseudonyms and for EAP-AKA pseudonyms, so that the AAA can determine which procedure to follow.

The last step in the generation of the pseudonym 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 is 23 characters, and no padding is necessary. Observe that the length of the *Pseudonym 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 for EAP-SIM or a pseudonym for EAP-AKA without performing any reverse transformation (i.e. without translating any printable character into the corresponding 6 bits).

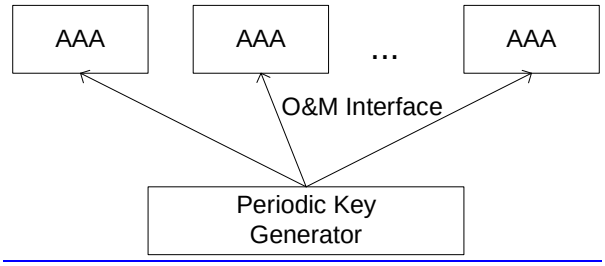
6.4.2 Key Management

A 128-bit encryption key shall be used for the generation of pseudonyms 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, but the AAA servers must keep a number of suspended (old) keys for the interpretation of received pseudonyms 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 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, it can use the corresponding key for obtaining the *Padded IMSI* (and thence the Username).

If a pseudonym 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 could eventually be removed from all the WLAN AAA servers. If the user initiates an authentication attempt after that time using that old pseudonym, the receiving AAA server will not be able to recognise the pseudonym as a valid one, and it will request the permanent user identity from the WLAN client. 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 (out of the scope of this proposal).

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.

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~~802.11i~~]. It has been decided to use IEEE 802.1X as the authentication framework ref. [~~802.1X~~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.

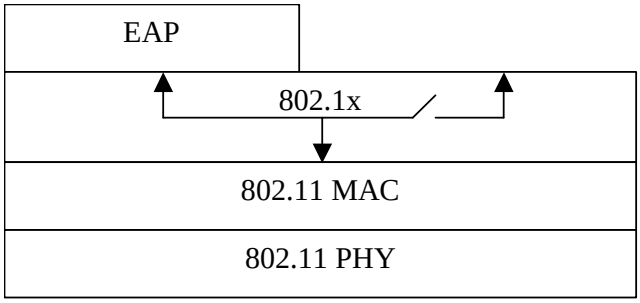


Figure 1 IEEE 802.1X in part of protocol stack in Access Point or mobile station. EAP messages are always accepted while other packets are filtered based on authentication status.

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 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.

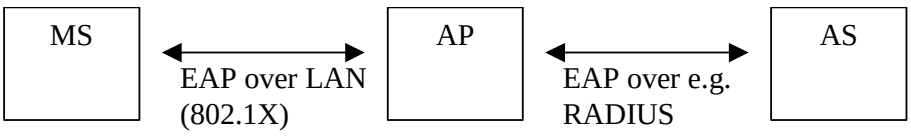


Figure 2 Example of end-to-end authentication using EAP.

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 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)

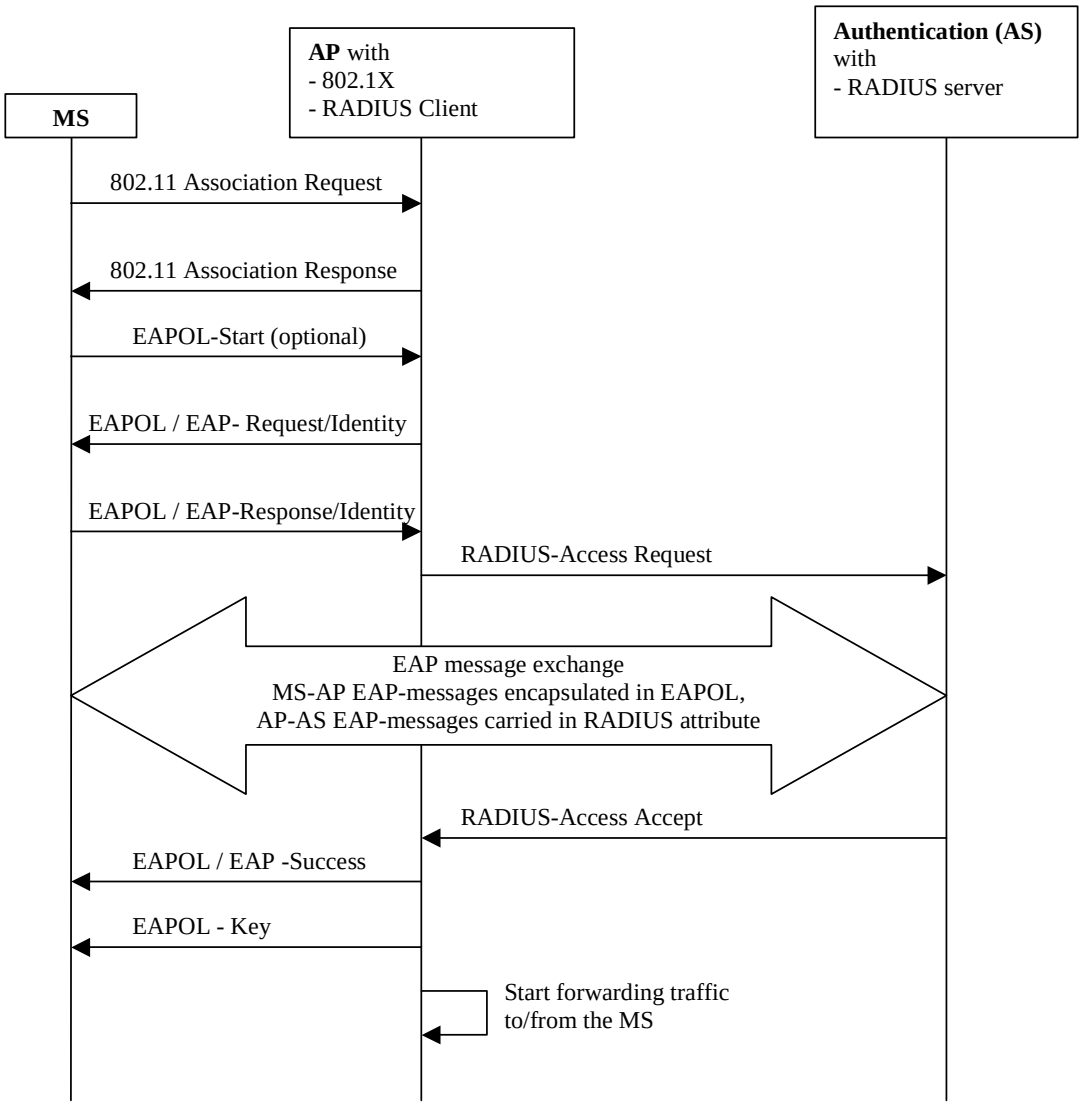


Figure 3 General EAP authentication with 802.11i and RADIUS as AAA protocol.

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.

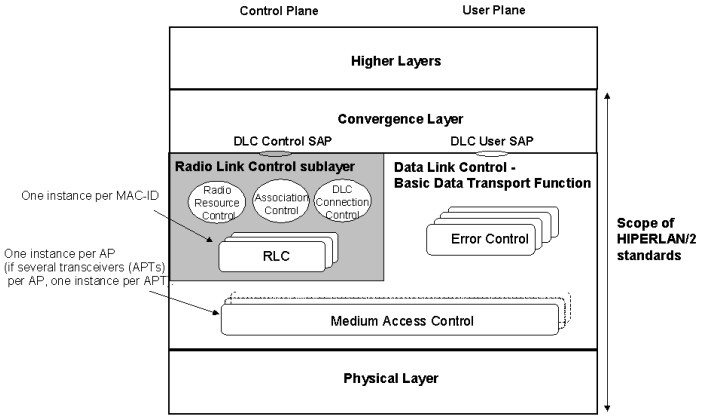


Figure 4: Protocol stack in the AP/CC

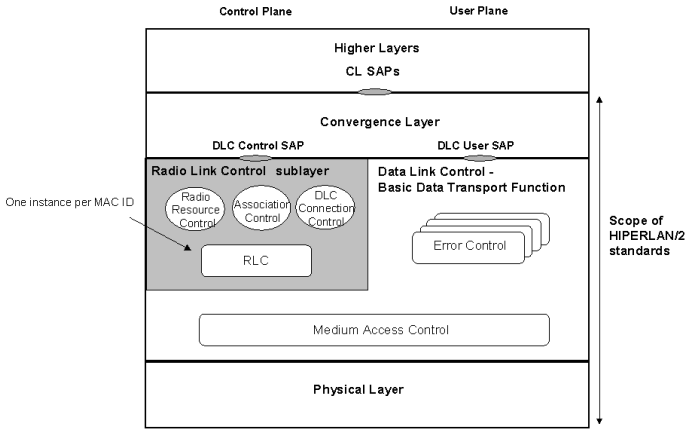


Figure 5: Protocol stack in the MT

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.

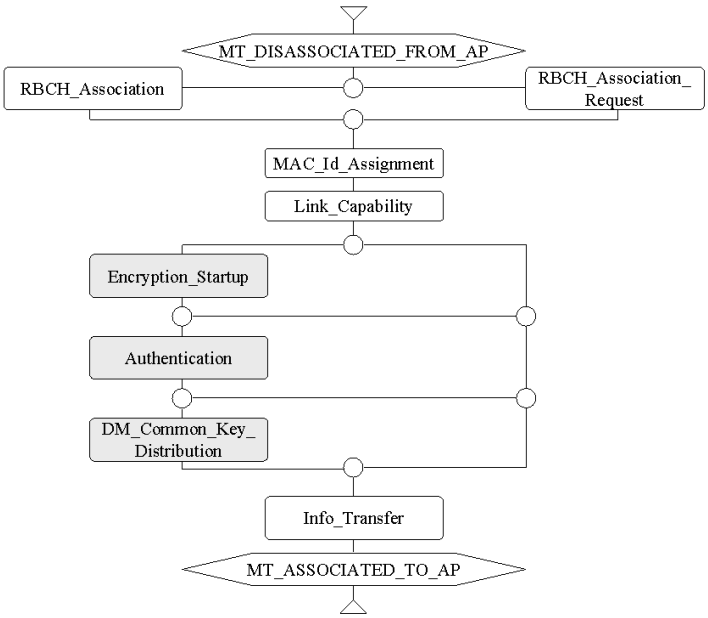


Figure 6: The Association Control Function

A.2.1.1 Confidentiality protection

Confidentiality protection is provided for user data and part of RLC signaling. 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.

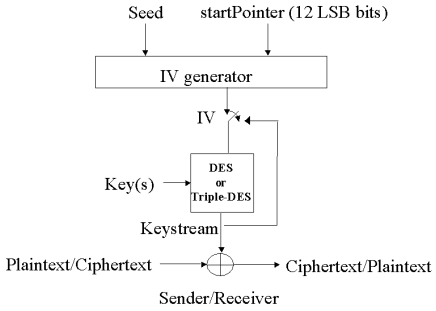


Figure 7: The encryption/decryption function

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

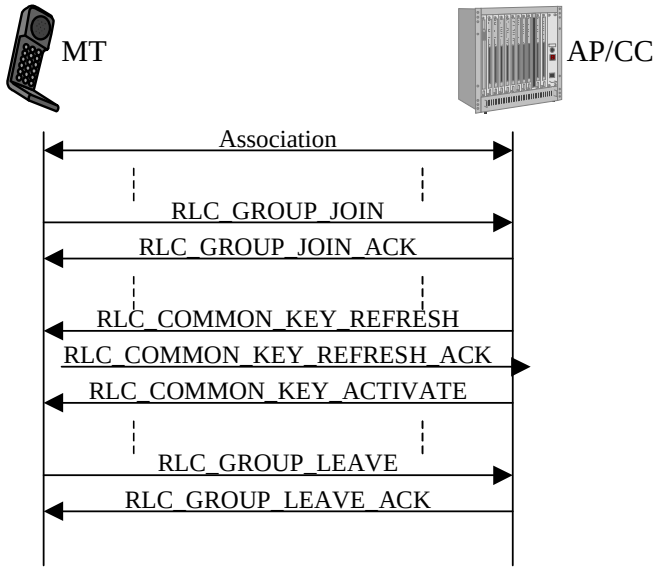


Figure 8: A Multicast example.

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.

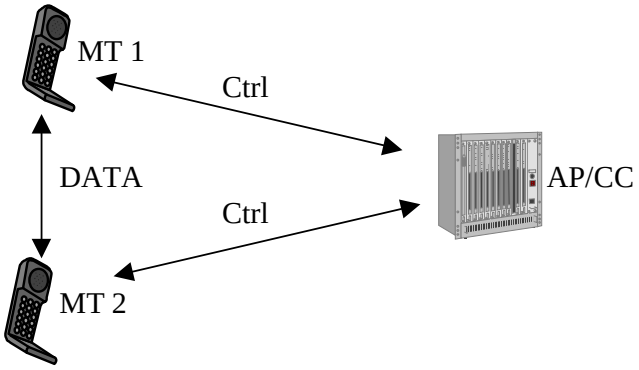


Figure 9: The data and control flow in a direct link scenario.

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.

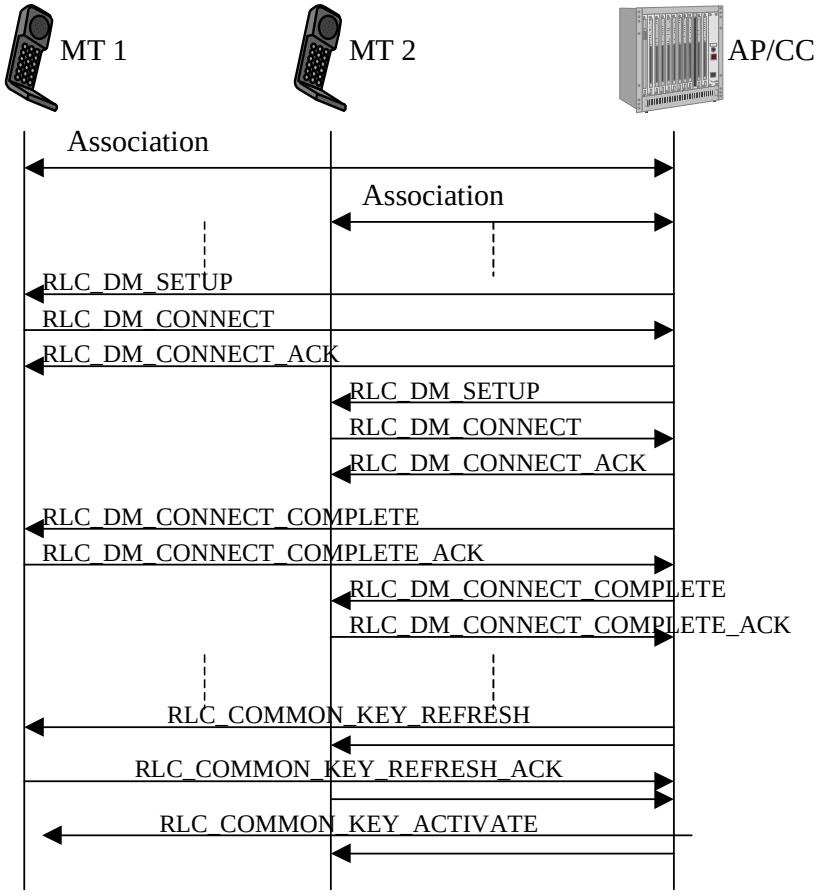


Figure 10: AP/CC Initiated DiL setup with key refresh.

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

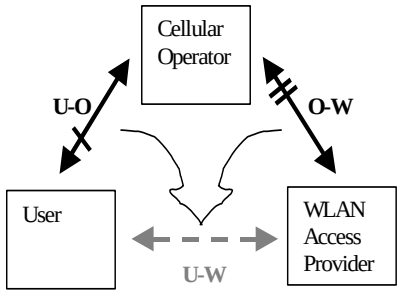


Figure 1 Trust model

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 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 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.

[Editor's note: It is probable that the cellular operators will provide the WLAN access in the future, and that small WLAN-only operators will be few or non-existent. It is, however, not impossible that there will be important WLAN-only operators on the market. These could team up with one or more cellular operators. The trust relations that are induced by access through such an operator are the same as the ones considered in the case of roaming between two cellular operators.]

Annex C (informative): Analysis of Threats

[Editor's note: In this section potential threats shall be identified and suitable countermeasures will be proposed]

Annex D (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