3GPP TSG SA WG3 Security — S3#34 **S3-040467**
6 - 9 July 2004
Acapulco, Mexico

Source: **Gemplus**

Title: **WLAN: Justification for the introduction of a WLAN application**

Document for: **Discussion and decision**

Agenda Item:

Abstract

This contribution provides more justification for the introduction of WLAN application.

1. Introduction

At SA3#33 Beijing meeting Gemplus presented S3-040351 contribution on WLAN application. It was considered necessary to have more explanation of the justification for creating this functionality over the use of EAP-AKA with USIM. This contribution provides more justification for the introduction of this proposal.

2. Spreading of vulnerabilities between WLAN and GSM/GPRS domains

S3-040351 [1] proposed WLAN application as an alternative to the combination of countermeasures based on Special RAND and functional split of EAP-SIM/AKA, this proposal offers a higher security level to prevent attacks on vulnerabilities between WLAN and GSM/GPRS domains.

Special RAND
The Special RAND is a ME-based mechanism; the UICC is not involved in the decision to perform the authentication command according to the Special RAND value sent by the Home Network. The Special RAND mechanism assumes the use of a trusted device. So, in case of ME not implementing the Special RAND mechanism or a hacked ME then there is no separation of domains. The Home Network has no guarantee of the interpretation of the Special RAND by the ME since the HN has no information on the ME capability of the user's UE.
In case of usage of a WLAN application, the Home Network knows if a WLAN application is present on the user's UE since the HN knows the capabilities of the UICC. The Home Network controls the level of security associated to WLAN access request.

Moreover, SA3 have not yet selected Special RAND mechanism for A5/2 protection. So, the availability of special RAND mechanism is not guaranteed to prevent spreading of vulnerabilities between WLAN and GSM/GPRS domains.

Split UE
With WLAN application the session keys Kc, CK or IK are always protected whatever the type of split UE since these session keys never leave the UICC.

Independent key sets
The use of independent key sets for WLAN application guarantees the separation of GSM/GPRS, UMTS and WLAN domains.

The WLAN application offers higher security level than the EAP-SIM with SIM and also than EAP-AKA with USIM.

3. Justification for creating WLAN application over the use of EAP-AKA with USIM

WLAN application proposes additional features which improve the security level.

Control of the IMSI-based user identity
When the network does not recognize the temporary identifier used by the WLAN UE, the network requests the WLAN UE to sent the IMSI-based user identity.
A WLAN application allows controlling the sending of the IMSI-based user identity; it determines when to use temporary identifier (pseudonym) instead of the IMSI, e.g. the pseudonym should be used whenever it is available.
So, the Home Network controls the management of the IMSI sending since it is implemented on the UICC. Moreover, the Home Network has the possibility to change this management by means of OTA mechanism.

Storage of the new keying material
New keying material is derived during USIM-based WLAN Access Authentication.

New keying material
On EAP-AKA full authentication, a Master Key (MK) is derived from the UMTS AKA values (CK and IK keys) and the subscriber identity. The Master Key is fed into a Pseudo-Random number Function (PRF), which generates separate keys:

- The Transient EAP Keys (TEKs) for protecting EAP-AKA packets
  - **K_encr** (128 bits): Encryption key to be used with AT_ENCR_DATA attribute
    K_encr is involved in the ciphering of the user identity
  - **K_aut** (128 bits): Authentication key to be used with AT_MAC attribute
    K_aut is involved in MAC computations covering EAP messages
- Master Session Key (MSK) for link layer security
- Extended Master Session Key (EMSK) for other purposes

On fast re-authentication:

- The same TEKs shall be used for protecting EAP packets
- A new MSK and a new EMSK shall be derived from the original MK and new values exchanged in the fast re-authentication.

EAP-AKA with the USIM according to TS 33.234 [2]
The USIM sends RES, CK and IK to the device hosting the UICC, which computes the Master Key (MK) and derives the new keying material from MK.
Attacks on the device hosting the UICC can allow the retrieval of K_encr involved in the ciphering of the user identity and K_aut involved in MAC computations and checks covering EAP messages.

WLAN application:
The WLAN application computes the new keying material, it checks and computes MAC on EAP messages and deals with the ciphering of the user identity. The UICC does not reveal the Master Key (MK) and the Transient EAP Keys (K_encr and K_aut).

So, WLAN credentials for WLAN access authentication are not revealed in clear in unprotected environment, the WLAN application provides a higher security level than EAP-AKA with USIM.

4. EAP support in the UICC

ETSI SCP produced ETSI TS 102 310 "Extensible Authentication Protocol support in the UICC [3].

This specification enables the UICC to provide support of different EAP methods, ensuring interoperability between the UICC and any terminal, independently of their respective manufacturers. Examples of EAP methods are EAP-SIM, EAP-AKA, EAP-TLS.

So, the WLAN application could be based on "EAP support in the UICC" specification, 3GPP T3 group could specify the EAP-SIM/AKA methods involved in the 3GPP WLAN access authentication.

5. Conclusion

The use of a WLAN application offers a higher security level and the standardization of this application is not an issue.

We kindly recommend SA3 to adopt WLAN application and send LS to SA1 for consultation and to T3 to ask them to work on WLAN application.

6. References

[1] TD S3-040351, "WLAN application", Gemplus

[2] 3GPP TS 33.234, "Wireless Local Area Network (WLAN) Interworking security", Rel-6

[3] ETSI TS 102 310, "Extensible Authentication Protocol support in the UICC", Rel-6, v1.1.0 (2004-04)

3GPP TSG SA WG3 Security — S3#33 **S3-040351**
10 - 14 May 2004
Beijing, China

Source: **Gemplus**

Title: **WLAN application**

Document for: **Discussion and decision**

Agenda Item:

Abstract

This contribution proposes the use of a WLAN application to solve WLAN security issues.

1. Introduction

At SA3#31 and SA3#32 meetings some concern was expressed that the security breach in one domain could spill over into another domain. E.g. the A5/2 vulnerability can spread from the GSM network to the WLAN access network or end user devices can spread from the WLAN network to the GSM network. SA3#32 contributions discussed various countermeasures to prevent such security issues. This contribution proposes the use of a WLAN application as solution.

2. WLAN security

At SA3#32, the following contributions discussed countermeasures to prevent spreading of vulnerabilities between WLAN and GSM.

- **S3-040009** [1] proposes 4 countermeasures:
  - *Countermeasure 1*: Segregated HSS and UICC applications
  - *Countermeasure 2*: Key separation function in HSS
  - *Countermeasure 3*: the use of separate range of RAND for each access network type
    This countermeasure is associated with the assumption that "we have a device that can be trusted to interpret the information correctly i.e. a traditional GSM/GPRS 3G PS and CS mobile phone issued by the Home Network Operator".
  - *Countermeasure 4*: Appropriate functionality split of EAP-AKA and EAP-SIM over UE devices

- **S3-040100** [2] proposes to use Special RANDs to separate WLAN and GSM/GPRS domains

- **S3-040110** [3]

This contribution comments S3-040009 and S3-040100 and states that *"countermeasures 3 and 4 are not equivalent. It is not possible to substitute one for the other, and in order to achieve full protection, both have to be implemented"*.
The conclusion analyses EAP-SIM and EAP-AKA cases and concludes that:

- *The Special RAND mechanism is required to prevent a GSM security breach to affect the 3G-WLAN access*

- *When a split UE is used and the WLAN-TE is considered more vulnerable than the MT, then an appropriate functionality split of EAP-SIM and EAP-AKA shall be used such that MK or MSK, but not the GSM and UMTS session keys Kc, CK, IK are given to the WLAN-TE. This is to prevent false base station attacks on pre-Rel-6 mobiles and impersonation of EAP-SIM server.*

3. WLAN application

The use of a WLAN application was already proposed and discussed to solve the risks of using a legacy SIM card for WLAN interworking in case of EAP-SIM (Cf S3-020651 SA3#26 meeting). After that, vulnerabilities due to A5/2 attacks have been identified.

The use of an independent WLAN application allows separating GSM/GPRS and WLAN domains, the session keys Kc, CK and IK never leave the UICC. So, a WLAN application prevents all the security attacks identified in S3-030110 contribution [3], it is an alternative to the combination of countermeasures 3 and 4, which are based on Special RAND and functional split of EAP-SIM/AKA.

Special RAND

The Special RAND is a ME-based mechanism; the UICC is not involved in the decision to perform the authentication command according to the Special RAND value sent by the Home Network. The Special RAND mechanism assumes the use of a trusted device (cf assumption of countermeasure 3 [1]). So, in case of ME not implementing the Special RAND mechanism or a hacked ME then there is no separation of domains. The Home Network has no guarantee of the interpretation of the Special RAND by the ME since the HN has no information on the ME capability of the user's UE.
In case of usage of a WLAN application, the Home Network knows if a WLAN application is present on the user's UE since the HN knows the capabilities of the UICC. The Home Network controls the level of security associated to WLAN access request.

Split UE

With WLAN application the session keys Kc, CK or IK are always protected whatever the type of split UE since these session keys never leave the UICC.

Sharing security functions and data with USIM

The WLAN application may share security functions and data with the USIM, different options of sharing could be proposed. Options have already been specified for ISIM in TS 33.203 [4].
These options of sharing allow dealing with different business models. E.g. of business models [1]

- The WLAN access network operator and GPRS operator are separate companies
- 3G WLAN interworking is used to ensure that the users use their subscription (and USIM) to get access also over WLAN, in this way bind users to one operator.

So, the WLAN application offers a higher level of security to prevent attacks. An open issue could be the availability of the WLAN application. This point is developed in the following section.

4. Standardization of WLAN application

The WLAN Smart Card Consortium (WSCC) specified WLAN SIM application and ETSI SCP proposes EAP support on UICC. The WLAN-SIM application is in line with the initiative support of EAP for Smart Cards currently in progress in ETSI SCP.

WLAN-SIM

The WLAN Smart Card Consortium took on the work of specifying an interoperable solution to integrate a smart card in the EAP framework used for authentication. While their goal is to run EAP

inside the card, they felt the need to satisfy an intermediate requirement of mobile network operators currently deploying I-WLAN on GSM. Therefore they specified the WLAN-SIM.

Features of the WLAN SIM:

- Shall be compatible with EAP-SIM
- Shall protect the A3A8 algorithm by executing the EAP-SIM specific cryptographic calculations in the UICC
- Does not expose SIM specific data (IMSI, ADN, PLMN…) to malicious programs in the WLAN terminal
- Shall determine when to use Pseudonym instead of IMSI
- Shall derive and store EAP authentication key and WPA-Session key in UICC: protection of the WLAN session against hijacking.
- Shall be independent from SIM, to possibly separate the I-WLAN subscription credentials from GSM and GPRS
- Shall allow re-use of the credentials from the SIM on the same UICC
- Shall be optional
- Shall be standard
- Shall not have a big impact on terminal software

Advantages of the WLAN SIM:

- Already specified and agreed by a large number of industry players
- Can be adopted by 3GPP in Rel-6 timeframe
- Can be developed on existing UICC
- Does not need to modify the SIM (specs are frozen)
- Compatible with the EAP support in UICC initiative currently in progress in SCP, as every EAP method can be implemented as an independent application. EAP support in UICC naturally integrates the WLAN-SIM in the overall.

So, the standardization of a WLAN application is possible in Rel-6 timeframe.

5. Conclusion

The use of a WLAN application offers a higher security level to prevent attacks on vulnerability spreading between WLAN and GSM/GPRS domains. The standardization of a WLAN application is not an issue.

We kindly recommend SA3 to adopt WLAN solution and send a LS to T3 to ask them to work on WLAN application.

6. References

[1] TD S3-040009, “Protecting GSM/GPRS networks from attacks form compromised from compromised WLAN networks when interworking”, BT Group

[2] TD S3-040100, “Using special RAN to separate WLAN and GSM/GPRS”, Nokia.

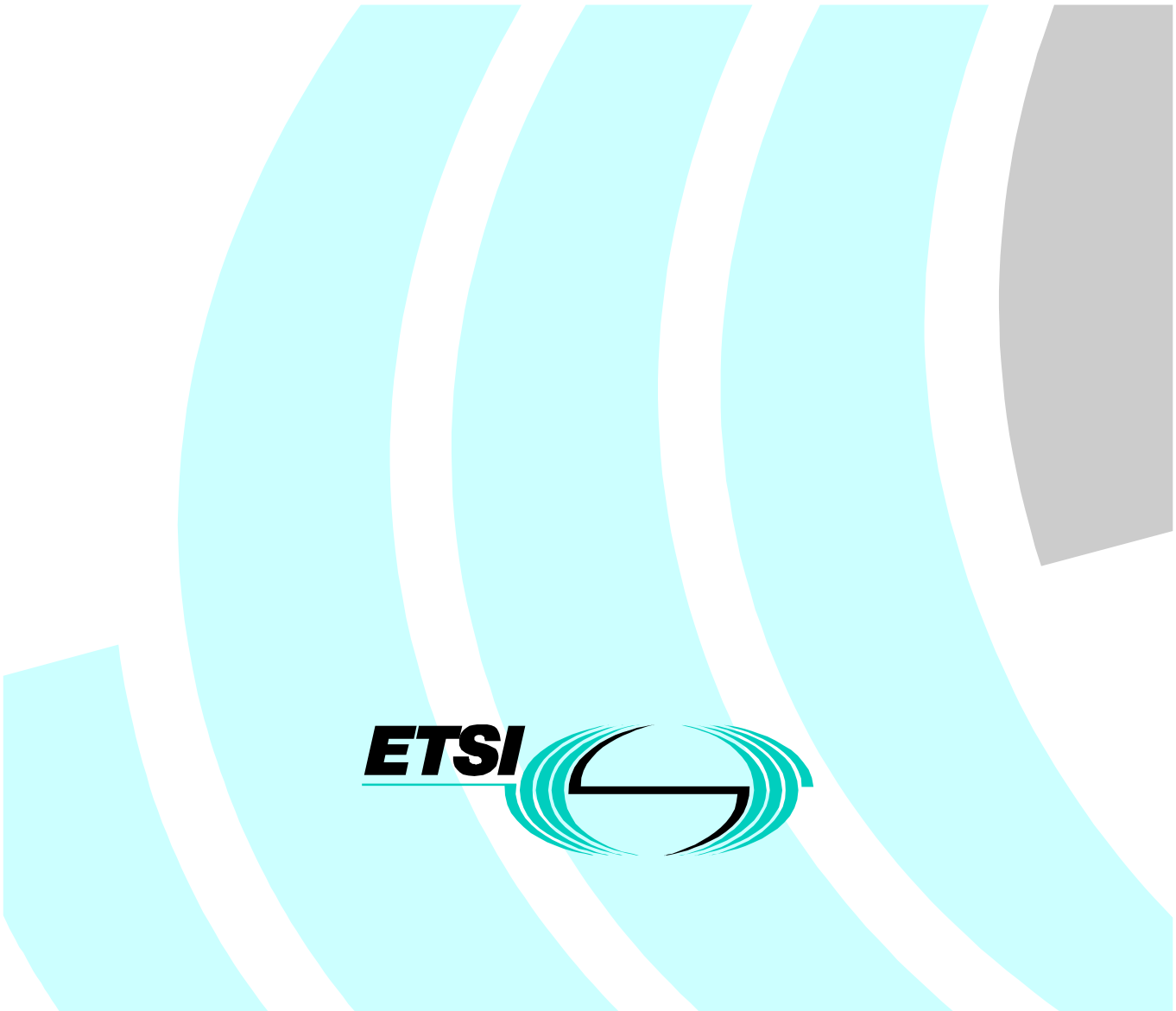
[3] TD S3-040110, “Comments on S3-040009 and S3-040100 on countermeasures for separation of domains”, Siemens.

[4] TD 33.234, “Wireless Local Area Network (WLAN) interworking security” v6.0.0

ETSI TS 102 310 V 1.1.0 (2004-04)

Technical Specification

Smart Cards;
Extensible Authentication Protocol support in the UICC;
(Release 6)



Reference

Keywords
EAP, UICC

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by the ETSI Project Smart Card Platform (SCP).

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

Version x.y.z

where:

x indicates the release (3 indicates Release 1999 and 4 indicates the subsequent release (called "Release 4").

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 specification.

1 Scope

The present document defines additional features that shall be provided by the UICC to support EAP authentication capabilities.

The goal of these new features is to adapt the UICC to provide support of different EAP methods, ensuring interoperability between the UICC and any terminal independently of their respective manufacturers.

The present document defines:

- The architectural framework
- The additional commands required;

2 References

The following documents contain provisions that, 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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] Extensible Authentication Protocol (EAP) (IETF <draft-ietf-eap-rfc2284bis-06.txt>)

[2] IETF RFC 2284 "PPP Extensible Authentication Protocol (EAP) (http://www.ietf.org/rfc/rfc2284.txt)

[3] EAP-support in smartcards (http://www.ietf.org/internet-drafts/draft-urien-eap-smartcard-03.txt)

[4] ETSI TS 102 221 "Smart cards; UICC-Terminal interface; Physical and logical characteristics

[5] draft-arkko-pppext-eap-aka-11, "EAP AKA Authentication". http://www.ietf.org/internet-drafts/draft-arkko-pppext-eap-aka-11.txt

[6] draft-haverinen-pppext-eap-sim-12, "EAP SIM Authentication".http://www.ietf.org/internet-drafts/draft-haverinen-pppext-eap-sim-12.txt

[7] IETF RFC 2284 "PPP EAP TLS Authentication Protocol"

[8] 3GPP TS 51.011: "Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface".

[9] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.

3 Definitions and Acronyms

3.1 Definitions

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

Authenticator: The end of the EAP link initiating EAP authentication

Peer or Supplicant: The end of the EAP Link that responds to the authenticator.

3.2 Acronyms

4 Introduction

The Extensible Authentication Protocol (EAP) [1] is a general authentication framework, which supports multiple authentication methods. EAP typically may run directly over data link layers such as PPP or IEEE 802.

As described in EAP [1], EAP implementations consist of three main components:

-A **lower layer** that is responsible for transmitting and receiving EAP frames between the peer and the authenticator. (EAP has been run over a variety of lower layers including PPP; wired IEEE 802 LANs [IEEE-802.1X]; IEEE 802.11 wireless LANs [IEEE-802.11]; UDP (L2TP [RFC2661] and ISAKMP [PIC]); and TCP [PIC]).

-An **EAP layer** that receives and transmits EAP packets via the lower layer, implements duplicate detection and retransmission, and delivers and receives EAP messages to and from EAP methods.

-EAP methods that implement the authentication algorithms and receive/transmit EAP messages via the EAP layer.

The UICC offers suitable possibilities for the implementation of some of these EAP methods in the peer side, since it provides the required protection of credentials and authentication algorithms. This is even more important when the following conditions apply:

-The authentication methods require the usage of credentials that are stored in the UICC.

-For security reasons, these credentials shall not be revealed in clear in an unprotected peer environment (e.g. a laptop or mobile terminal).

The IETF draft "EAP support in smartcards" [3] specifies some principles on how it is possible to carry out a particular EAP method inside a smart card.

The present document defines how these principles shall be implemented in the UICC in order to enable that UICC applications may support one or more of these EAP methods.

Examples of EAP methods that can be implemented in the UICC are EAP SIM [6], EAP AKA [5] and EAP TLS [7].

Note: This document refers to the EAP-bis draft [1], which is intended to make obsolete the RFC 2284 [2] once approved. However, all statements contained in this document may be also applied for devices compliant with RFC 2284 [2].

5 Architecture

5.1 Architectural Principles

The following architectural principles are applied:

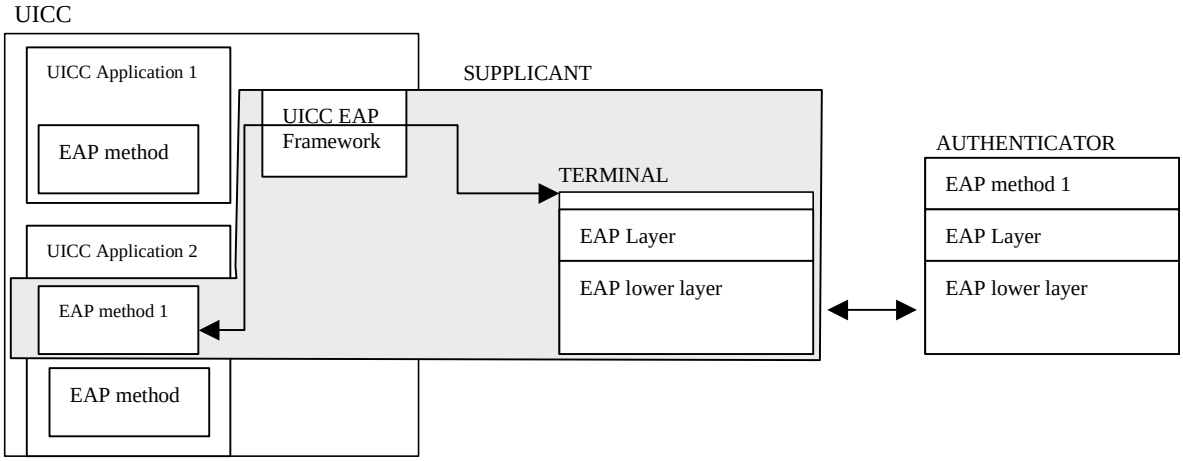
-The authenticator is able to perform an EAP authentication process (using an specific EAP method) with a UICC application implementing this method. That means that the authentication is performed end-to-end between the authenticator and the UICC application.

-The peer is composed of several components:

-**The UICC EAP Framework** provides information to the terminal about the existing UICC applications that provide UICC EAP clients.

-A **UICC application** provides one or more UICC EAP clients.

-A UICC EAP client implements one specific EAP method.



-

Figure 1: EAP architecture when supplicant is split between a UICC and a terminal.

5.2 EAP clients discovery

When a UICC application implements one or more EAP clients, its corresponding record in EF_{DIR} shall contain the following EAP related Data Objects.

-Application EAP support types list: Defining the EAP methods supported by the corresponding UICC application

-Application EAP Dedicated File list: Defining the list of Dedicated Files associated to a particular supported EAP method. Each of this DF are hereafter referred as DF_{EAP}

-Application EAP Label: Defining a user readable label defining the EAP clients

Table 1: Coding of EAP related DOs

Length	Description	Status
1	Discretionary template tag = '73'	M
1	Length of the discretionary template	M
1	Application Type Tag = ‘80’ Editor’ s Note: To be Reserved in 102.221	M
1	Application Type length	M
1	Application Type Value (EAP=’81’) Editor’ s Note: To be Reserved in 102.221	M
1	Application specific data content tag (=”A0”) Editor’ s Note: To be Reserved in 102.221	M
1	Application specific data content length	M
1	Application EAP supported types list tag = '01'	M
1	Length of the Application EAP supported types list	M
A	Application EAP supported types list	M
1	Application EAP Dedicated file list tag = '02'	M
1	Length of Application EAP Dedicated file list	M
B	Application EAP Dedicated File list	M
1	Application EAP Label tag = '03'	M
1	Length of the Application EAP Label	M
C	Application EAP Label	M

Coding:

-Application EAP support types list:

Contain a list of supported EAP type (as defined in [1]) each of them coded in one byte.

Example: An UICC application supporting EAP-SIM and EAP-TLS provides the following "Application EAP supported types list":

' 120D'corresponding to EAP-SIM (Type=18) and EAP-TLS (Type=13)

-Application EAP Dedicated Files list:

Contain a list of file identifiers of each DF_{EAP} associated to a particular supported EAP type. Each of them coded in two bytes.

Example: Using the previous example, A DF '6D34' for EAP-SIM and the same for EAP-TLS will result in the following EAP Dedicated Files list:

'6D346D34'

-Application EAP label:

The application label is a DO that contains a string of bytes provided by the application provider to be shown to the user for information.

5.3 EAP-capable-application selection

The terminal shall use the information in EF_{DIR} file if available to present the list of EAP-capable applications to the user or to any application that may request an EAP authentication.

The terminal shall then select the corresponding EAP-capable-application to start an EAP authentication. Once selected, all EAP-Client state machines of the application are reset.

5.4 Key derivation

It is possible for many EAP methods to derive key material after successful authentications. These keys may be used for subsequent processes (e.g. for WEP encryption in 802.11).

Keys derived from an authentication shall be retrieved by the terminal by inspecting the mandatory file $EF_{EAPKEYS}$

5.5 Authentication Status

The terminal may retrieve the authentication status of the EAP client in the selected UICC application by inspecting the mandatory file $EF_{EAPSTATUS}$

6 EAP related Commands

The following sections specify the additional commands needed to implement the EAP framework in the UICC. These commands are described in [3]

6.1 EAP Authenticate

6.1.1 Command description

The function is used to transfer the EAP packets from the terminal to the selected UICC EAP client (i.e. EAP client in the selected UICC application that corresponds to the given EAP type)

The UICC EAP client shall provide a response EAP packet (as defined in [1]) or a warning status word according to the authentication method being used.

The UICC EAP client shall maintain the state machine of the authentication process as described for the particular EAP method used.

The function is related to a particular UICC application supporting EAP and shall not be executable unless this application has been selected and activated, and the current directory is a DF_{EAP} related to a specific EAP method.

Each UICC application implementing a UICC EAP client may require different security conditions to execute this command (e.g. user PIN verification).

The format of the EAP packet is defined by the application implementing the EAP client and shall respect the conventions corresponding for the EAP method.

The following EAP packets are allowed input packets for this command: EAP packets with code field equal to 1 “Request”, 3 “Success” or 4 “Failure” and EAP packets with code equal to 2 “Response” for EAP type 1 “Identity” (Code and type values as defined in [1]).

> Note: EAP Response Identity packet may be delivered to the UICC application when the identity is managed outside the UICC application and the method itself need to have access to the chosen identity.

The command may contain specific EAP method related data as an additional input parameter (e.g. gmt_unix_time for EAP-TLS implementations as defined in [7]).

Input:

- EAP Packet
- EAP type
- EAP method related data

Output

- Either none (i.e. if authentication successful: EAP success packet received)

or

- EAP Response Packet
- EAP method related data

6.1.1.2 Command parameters and data

Code	Value
CLA	As specified in ETSI SCP 102 221 [4]
INS	'88'
P1	EAP type (coded as defined in EAP related Data Objects)
P2	See table 9.1
Lc	Length of subsequent EAP command data
Data	See below
Le	Length of the response data

NOTE: Parameter P1 indicates the targeted EAP client in the selected application.

Table 6.1: Coding of P2

b8	b7	b6	b5	b4	b3	b2	B1	Meaning
1	-	-	-	-	-	-	-	Specific reference data (DF $_{EAP}$ application dependent KEY)
-	X	X	-	-	-	-	-	'00' (other values are RFU)
-	-	-	X	X	X	X	X	Reference data number ('01' to '1F')

Command data:

Byte(s)	Description	Length
1 - Lc	EAP command data (see table 6.2)	Lc

Table 6.2: Coding of EAP command data

Byte(s)	Description	Status	Length
1-J	EAP packet (coded as defined for the method of EAP used as defined in [1])	M	J bytes
J+1-J+K+1	EAP method related data (must be specified by each application specific document defining a particular EAP method implementation)	O	K bytes

Note: The length of an EAP packet is contained within the packet and can therefore be retrieved from it.

Response data :

Byte(s)	Description	Length
1 - Le	EAP ~~Packet (see note)~~Response data	Le
~~NOTE: EAP packet coded as defined for the method of EAP used as defined in [1]~~		

Table 6.3: Coding of EAP Response data

Byte(s)	Description	Status	Length
1-L	EAP packet	M	L bytes
L+1-L+N+1	EAP method related data (must be specified by each application specific document defining a particular EAP method implementation)	O	N bytes

Note: The length of an EAP packet is contained within the packet and can therefore be retrieved from it.

6.2 Specific status conditions returned

This clause specifies the coding of the specific status words SW1 and SW2.

6.2.1 Status words

The following table shows the meaning of possible status conditions returned.

Table 6.2: Status byte coding - warnings

SW1	SW2	Description
'62'	'00'	- No information given, state of non volatile memory unchanged (EAP Packet silently ignored)

Table 6.3: Status byte coding - application errors

SW1	SW2	Description
‘98’	‘62’	- Authentication error (EAP Failure Packet received)

7 EAP Files

This clause describes the files present in an application supporting an EAP type. The following files are situated under the corresponding DF_{EAP} of a particular UICC application:

7.1 $EF_{EAPKEYS}$ (EAP derived keys)

This EF contains the key material derived after a successful EAP authentication.

Structure of $EF_{EAPKEYS}$

Identifier: '4F01'	Structure: transparent	Conditional (see Note)
File size: n	Update activity: high	
Access Conditions: READ PIN UPDATE ADM/NEVER DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1	1st Key Tag	O	1 bytes
2	1st Key Length	O	1 bytes
3-L1+3	1st Key Value	O	L1 bytes
	...		
	Kst Key Tag	O	1 bytes
	Kst Key Length	O	1 bytes
	Kst Key Value	O	LK bytes

Note: The presence of this file depends on the supported EAP methods.

- Key Tag

  Contents:

  -Identifier of the derived key

  Coding:

  Editors Note: key tags reserved are FFS.

- Key Length

  Contents:

  -Length of the derived key

- Key Value

  Contents:

  -Derived key

7.2 $EF_{EAPSTATUS}$ (EAP Authentication STATUS)

This EF contains the authentication status corresponding to each of the EAP clients supported by the application.

Structure of $EF_{EAPSTATUS}$

Identifier: '4F02'	Structure: transparent	Mandatory
File size: n	Update activity: high	
Access Conditions: READ PIN UPDATE ADM/NEVER DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1	EAP type	M	1 bytes
2	Authentication Status	M	1 bytes
	...		
K	EAP type (K supported type)	O	1 bytes
K+1	Authentication Status	O	1 bytes

- EAP Type

Contents:
-Type of EAP supported by the application

Coding:
-As defined for EAP related DOs

- Authentication Status

Contents:
-Status of the corresponding EAP authentication

Coding:

-Authentication Status coded in one byte as below:

Value	Meaning
'00'	No authentication started
'01'	Authenticating
'02'	Authenticated
'03'	Held (Authentication failure)

7.3 EF_{PUId} (Permanent User Identity)

This EF contains the permanent user identity. Permanent User identity may be used as the username part of the Network Access Identifier (NAI)

This File is not mandatory if the Permanent user identity is derived by other means. (e.g. as defined in EAP SIM [6] or EAP-AKA [5]).

Structure of EF_{PUid}

Identifier: '4F03'		Structure: transparent		Optional
File size: n (where n ≥10 bytes)		Update activity: low		
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM				
Bytes	Description		M/O	Length
1 to n	Permanent user identity		M	n bytes

Permanent user identity

Contents:

-user identity to be used as the username part of the NAI

Coding:

-Binary. Unused bytes shall be set to 'FF' and shall not be considered as a part of the value.

7.4 EF_{PS} (Pseudonym)

This EF contains a temporary user identifiers (pseudonym) for subscriber identification. Pseudonyms may be provided as part of a previous authentication sequence. This may be used as the username part of the Network Access Identifier (NAI).

This File is not mandatory if pseudonyms are not managed by the application or they are derived by other means.

Structure of EF_{PsL}

Identifier: '4F04'	Structure: transparent	Optional
File size: n	Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to n	Pseudonym	M	n bytes

- Pseudonym.

Contents:

-Pseudonym to be used as the username part of the NAI

Coding:

-Binary Unused bytes shall be set to ‘FF’ and shall not be considered as a part of the value.

Annex A History (Informative)

Change History

This annex lists all change requests approved for the present document by ETSI SCP.

SCP#	SCP tdoc	WG tdoc	VERS	CR	RV	PH	CAT	SUBJECT	Resulting Version

Document History

Document history		
V1.0.0	February 2004	For information
V1.1.0	April 2004	For approval.