

WLAN Smart Card Consortium

WLAN-SIM Specification Version 1.0

October 20th, 2003



**SUBJECT TO CHANGE
WITHOUT NOTICE**

1	Introduction	3
2	References	3
3	Terminology	4
4	Protocol Overview	4
5	Card Interface	6
5.1	WLAN-SIM Application Selection	6
5.2	WLAN-SIM PIN management	6
5.3	Get-Preferred-Identity	6
5.4	Select-Identity	7
5.5	Get-Random	8
5.6	Process-EAP	8
5.7	Get Profile Data	9
5.8	Get-Current-Version	10
6	Commands Summary	12

1 Introduction

This document specifies a smart card interface to provide authentication, session key distribution and identity management using the GSM Subscriber Identity Module (SIM) and the EAP-SIM authentication protocol [0].

The WLAN-SIM specification allows a developer to create an EAP-SIM handler that will interoperate with cards from many different manufacturers and issuers.

The WLAN-SIM specification provides the following functionality that supports EAP-SIM:

- generation of random material
- retrieval of network identities, (including IMSI and Pseudonyms)
- execution of EAP-SIM authentication/re-authentication

The WLAN-SIM specification also provides the following additional functionality:

- user authentication through WLAN-SIM PIN
- retrieval of network profile data elements
- retrieval of version data

The WLAN-SIM specification is the first of several specifications to be defined by the WLAN Smart Card Consortium as part of a major new initiative to enable world-wide access to Wireless LAN networks with smart card security, privacy, configuration, quality of service and related capabilities. Smart card applications adhering to the WLAN-SIM specification are intended to be complementary to applications adhering to the EAP-SMARTCARD draft specification [1].

2 References

- [0] IETF: draft-haverinen-pppext-eap-sim-11.txt: H. Haverinen & All, Nokia.
<http://www.ietf.org/internet-drafts/draft-haverinen-pppext-eap-sim-11.txt>
- [1] IETF: draft-urien-eap-smartcard-02.txt: P.Urien & All, ENST.
<http://www.ietf.org/internet-drafts/draft-urien-eap-smartcard-02.txt>
- [2] 3GPP TS 11.11: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".
<http://www.3gpp.org/ftp/Specs/html-info/1111.htm>
- [3] ETSI TS 102.221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 5)"
http://docbox.etsi.org/SCP/SCP/Specs/TS_102221/
- [4] GlobalPlatform Card Specification V2.1.1
<http://www.globalplatform.org/showpage.asp?code=cardspec>

3 Terminology

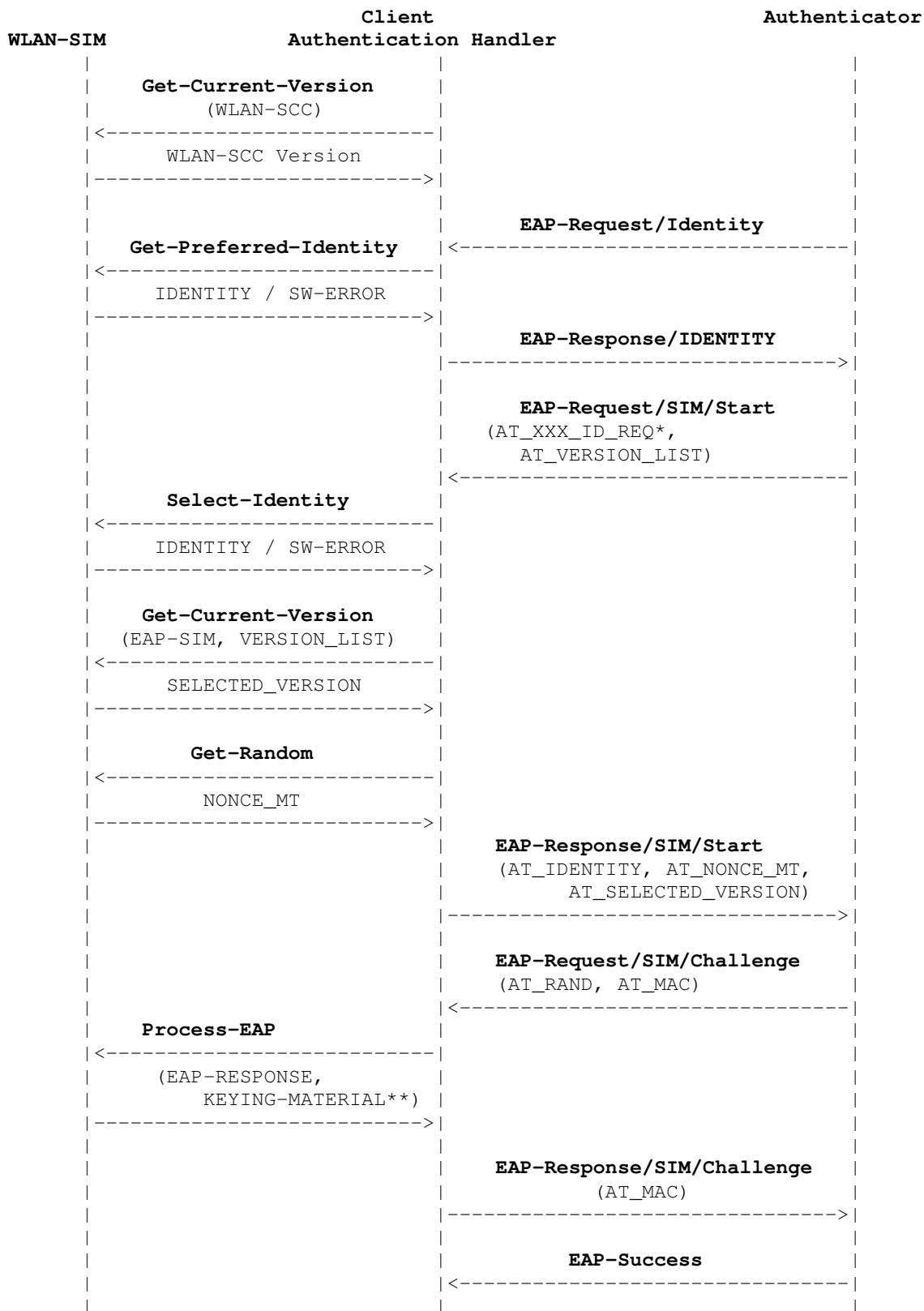
Acronym	Description
AID	Application Identifier
EAP	Extensible Authentication Protocol
GSM	Global System for Mobile Communication
MAC	Message Authentication Code
PIN	Personal Identification Number
RFU	Reserved for Future Use
SIM	Subscriber Identity Module
WLAN	Wireless LAN
WLAN SCC	Wireless LAN Smart Card Consortium

When words such as ‘MUST’, ‘SHOULD’ or ‘MAY’ are used in this document , their precise meaning is to be understood as described in the IETF RFC 2119.

All numbers are decimal by default. Hexadecimal numbers are represented between quotes such as ‘XY’.

4 Protocol Overview

This section describes the proposed implementation of the EAP-SIM protocol based on the WLAN-SIM smart card interface. The right section of the page refers to the EAP-SIM protocol exchange as described in [0]. The left section refers to the WLAN-SIM commands specified in this document.



This overview does not show all EAP-SIM command attributes. For a complete overview see [0]

*AT_ANY_ID_REQ, AT_PERMANENT_ID_REQ, AT_FULLAUTH_ID_REQ, see [0]

** master session key and extended master session key

5 Card Interface

5.1 WLAN-SIM Application Selection

The WLAN-SIM Smart Card Interface is implemented as a separate card application. Use of the WLAN-SIM Card interface requires selecting the application using the WLAN-SIM AID.

The WLAN-SIM Application selection MUST be handled within the established context such as SCP [3] or Global Platform [4].

WLAN-SIM AID structure

$$AID = RID \parallel PIX$$

RID 5 bytes, identifies the WLAN-SCC
PIX 11 bytes, identifies the application
RID '00 00 00 00 00' (TBD)
PIX '00 00 00 00 00 00 00 00 00 00 00' (TBD)

5.2 WLAN-SIM PIN management.

The WLAN-SIM Application MUST support the usage of a PIN within the established context such as SCP [3], or Global Platform [4].

5.3 Get-Preferred-Identity

This command is used by the Client Authentication Handler on reception of the EAP-Request Identity to determine the user identity string.

If the WLAN-SIM application is protected by PIN, this command MUST require PIN access rights to have been granted.

Command	CLA	INS	P1	P2	Lc	Le
GET PREFERRED IDENTITY	'Ax'	'16'	00	13	-	Le

Response parameters / Data

Byte(s)	Description	Length
1	IDENTITY TYPE	1
	WLAN -IDENTITY	X

IDENTITY TYPE indicates the type of identity returned:

'00': permanent identity,
 '01': pseudonym identity
 '02': re-authentication identity.

Returned Status Codes

SW1	SW2	DESCRIPTION
'67'	'00'	Incorrect parameter Le
'6B'	'00'	Incorrect parameter P1 or P2

'98'	'04'	Security status not satisfied (PIN _{WLAN})
'90'	'00'	Normal ending of the command.
'9F' or '6C'	'xx'	Normal ending of the command, 'xx' bytes available

5.4 Select-Identity

This command is used by the Client Authentication Handler on reception of the EAP-Request / SIM / Start. This command is used to select a user identity based using one of the identity attributes defined in the EAP-SIM specification [0].

If the WLAN-SIM application is protected by PIN, this command MUST require PIN access rights to have been granted.

This command is required prior to performing the PROCESS-EAP command.

Command	CLA	INS	P1	P2	Lc	Le
SELECT IDENTITY	'Ax'	'16'	00	<i>Identity Type</i>	–	<i>Le</i>

Identity-Type (corresponding EAP-SIM identity attribute).

- 0 the same identity as returned in the previous Get Preferred Identity command
- 13 any suitable identity chosen by the application (AT_ANY_ID_REQ)
- 10 the permanent identity (AT_PERMANENT_ID_REQ)
- 17 an identity suitable for full authentication (AT_FULLAUTH_ID_REQ)

Response parameters / Data

Byte(s)	Description	Length
1	<i>IDENTITY TYPE</i>	1
	<i>WLAN –IDENTITY</i>	X

IDENTITY TYPE indicates the type of identity returned:

- '00': permanent identity,
- '01': pseudonym identity
- '02': re-authentication identity.

Returned Status Codes

SW1	SW2	DESCRIPTION
'67'	'00'	Incorrect parameter Le
'6B'	'00'	Incorrect parameter P1 or P2
'98'	'21'	P2='00' and no previous Get Preferred Identity was issued
'98'	'04'	Security status not satisfied (PIN _{WLAN})
'90'	'00'	Normal ending of the command.
'9F' or '6C'	'xx'	Normal ending of the command, 'xx' bytes available

5.5 Get-Random

This command returns a 16 byte random number, which is used as the NONCE in the EAP-SIM protocol.

The card stores this value to use in a subsequent PROCESS-EAP command.

Command	CLA	INS	P1	P2	Lc	Le
GET RANDOM	'Ax'	'84'	'00'	'00'	-	'10'

Response parameters / Data

Byte(s)	Description	Length
1-16	NONCE	16

Returned Status Codes

SW1	SW2	DESCRIPTION
'67'	'00'	Incorrect parameter Lc
'6B'	'00'	Incorrect parameter P1 or P2
'90'	'00'	Normal ending of the command

5.6 Process-EAP

This command performs the client side cryptographic computations for the EAP-SIM protocol [0]. It supports both the authentication and re-authentication mechanisms as well as the pseudonym mechanism. The response data contains both the EAP response packet and the keying material, which can be used by the client authentication handler.

If the WLAN-SIM application is protected by PIN, this command MUST require PIN access rights to have been granted.

This command shall only be successfully executed if the SELECT IDENTITY command and the GET RANDOM command have been successfully executed.

This command supports large (>255 Byte) command data through chaining of commands.

The card verifies the MAC from the network and returns a MAC only if the network MAC is correct.

The optional AT-CHECKCODE attribute defined in [0] is not supported by the command in this version of the WLAN-SIM specification.

Command	CLA	INS	P1	P2	Lc	Le
PROCESS EAP	'Ax'	'80'	Reference Control	Authentication -Type	X	Y

Command parameters/data

Reference Control

Bit 8 = 0 more blocks follow
 Bit 8 = 1 last block

Authentication-Type

- '00' Full or Re-Authentication performed using identity returned by last SELECT IDENTITY command.
- '01' Full authentication using permanent identity (IMSI), irrespective of the identity returned by last SELECT IDENTITY command.

The command data is the EAP-request/SIM/Challenge or EAP-request/SIM/Re-authentication packet as received from the network. For detailed description, refer to [0] section 11.

Response parameters/data

The output is the EAP response packet plus the keying material (master session key and extended master session key).

Byte(s)	Description	Length
1-Z	EAP response packet	Z
Z+1 – Z+128	KEYING MATERIAL	128

Returned Status Codes

SW1	SW2	DESCRIPTION
'67'	'00'	Incorrect parameter Lc
'6B'	'00'	Incorrect parameter P1 or P2
'98'	'04'	Security status not satisfied (PIN _{WLAN})
'6A'	'80'	Parameter Error in Incoming Data Field
'98'	'23'	No GET VERSION (EAP-SIM Version previously issued (Full Auth))
'98'	'24'	Inconsistency between Selected ID and Authentication mode
'98'	'25'	Re-Auth without a previous successful Full Authentication
'98'	'20'	No GET RANDOM previously issued (Full Auth)
'98'	'21'	No SELECT IDENTITY previously issued
'98'	'22'	Invalid MAC
'90'	'00'	Concatenation in progress (P1 = "More blocks follow")
'9F' or '61'	'9C'	156 bytes available for GET RESPONSE (Full Authentication)
'9F' or '61'	'C4'	196 bytes available for GET RESPONSE (Re-Authentication)

5.7 Get Profile Data

This command allows for the retrieval of WLAN Profile Data Elements such as User Information, SSIDs, and Radio Channels.

This command can be executed at any time.

If the WLAN-SIM application is protected by PIN, this command MUST require PIN access rights to have been granted.

Command	CLA	INS	P1	P2	Lc	Le
GET PROFILE DATA	'Ax'	'1A'	<i>Profile Data</i>	<i>Element ID</i>	–	Y

Command parameters/data

Profile Data (P1)

0 to 127 Reserved for WLAN Profile Data Elements (TBD)

128 GetWebForm

If *Profile Data*=128 (GetWebForm)

Element ID (P2)

0 get first web form string (32 bytes ASCII)

1 get second web form string (32 bytes ASCII)

Returned Status Codes

SW1	SW2	DESCRIPTION
'67'	'00'	Incorrect parameter Le
'6B'	'00'	Incorrect parameter P1 or P2
'98'	'04'	Security status not satisfied (PIN _{WLAN})
'90'	'00'	Normal ending of the command.

5.8 Get-Current-Version

This command returns the version of the EAP protocol supported by the card, or the version of this specification that the card supports.

EAP protocol: WLAN-SIM cards supporting EAP-SIM version 1 will return '00 01'.

This specification: WLAN-SIM cards supporting WLAN-SIM version 1 will return '00 01'.

Command	CLA	INS	P1	P2	Lc	Le
GET CURRENT VERSION	'Ax'	'18'	'00'	<i>Version-Type</i>	XX	2

Command parameters / Data

Version-Type

0 EAP-SIM Version number (EAP-SIM)

1 WLAN SIM specification version number (WLAN-SCC)

In case P2='00', this command data (of which size is Lc bytes) is the data field from the AT_VERSION_LIST attribute, retrieved from the EAP-Request/SIM/Start packet received from the authenticator.

Response parameters/data

Byte(s)	Description	Length
1-2	<i>VERSION</i>	2

Returned Status Codes

<i>SW1</i>	<i>SW2</i>	<i>DESCRIPTION</i>
'67'	'00'	Incorrect parameter Le
'6B'	'00'	Incorrect parameter P1 or P2
'98'	'26'	P2='00' and Applet EAP-SIM Version is not found in Version List
'90'	'00'	Normal ending of the command.
'9F' or '6C'	'02'	Normal ending with EAP-SIM Version Number to be returned (P2='00')

6 Commands Summary

Command	CLA	INS
SELECT IDENTITY	'Ax'	'16'
GET PREFERRED IDENTITY	'Ax'	'16'
GET RANDOM	'Ax'	'84'
PROCESS EAP	'Ax'	'80'
GET PROFILE DATA	'Ax'	'1A'
GET CURRENT VERSION	'Ax'	'18'

The WLAN-SIM Application MAY also support other error codes specified in the established context [3] or [4]