

WLAN-SIM Specification Version 0.1

Draft for public comment

July 15, 2003



WLAN Smart Card Consortium

Table of Contents

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	6
5.5	Get-Random	7
5.6	Process-EAP	7
5.7	Get Profile Data	8
5.8	Get-Current-Version	9
6	Commands Summary	10

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

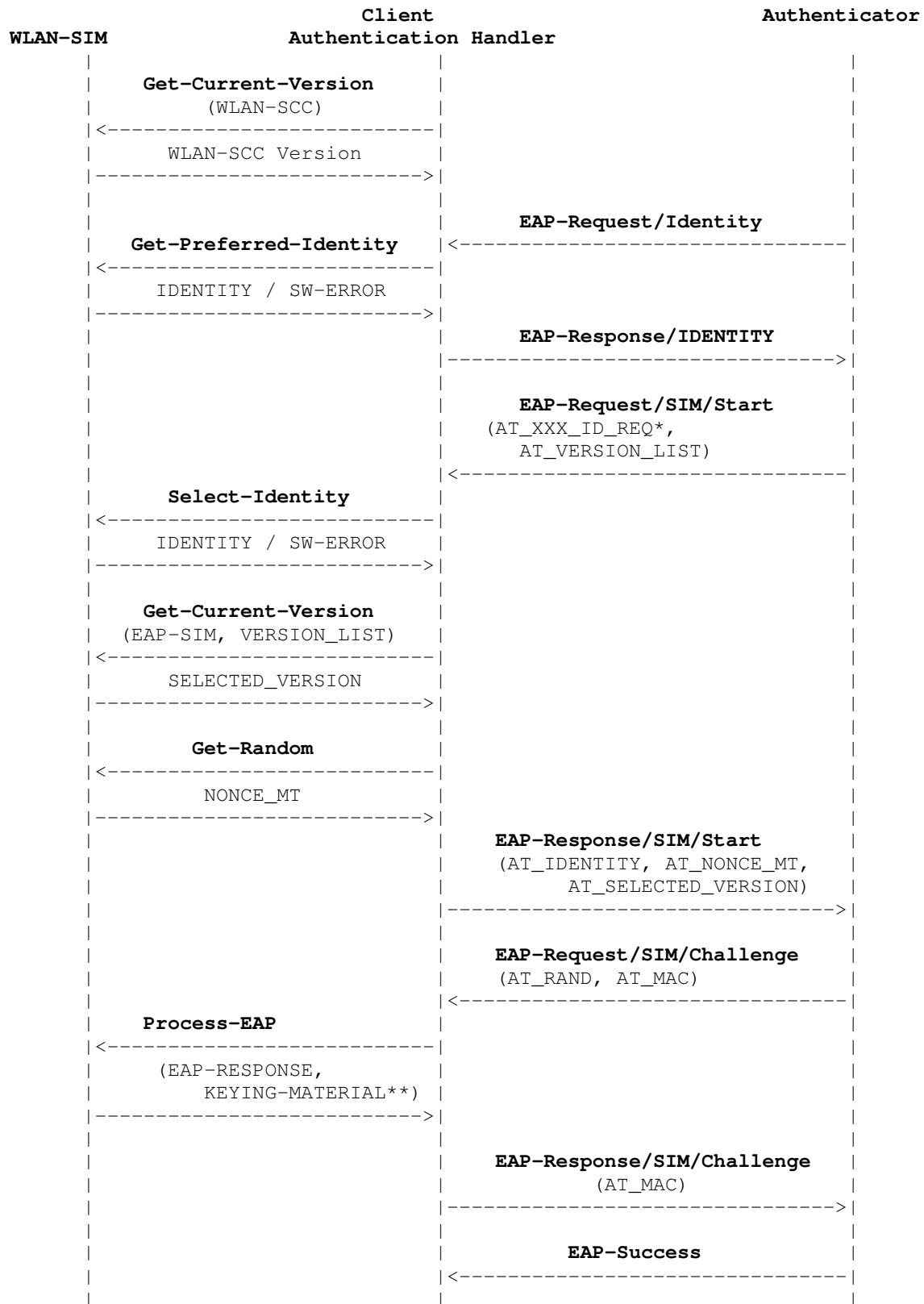
- [0] draft-haverinen-pppext-eap-sim-11.txt: H. Haverinen & All, Nokia.
- [1] draft-urien-eap-smartcard-02.txt: P.Urien & All, ENST.
- [2] 3GPP TS 11.11: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".
- [3] 3GPP TS 102.221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 5)"
- [4] Global Platform card specification V2.1.1 (March 2003)

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

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 should be handled within the established context such as SCP [3] or Global Platform [4].

WLAN-SIM AID structure

$$AID = RID | PIX$$

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 may be protected by a PIN.

The WLAN-SIM Application PIN presentation and Management should be handled 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.

This command may 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
	WLAN -IDENTITY	X

Returned Status Codes

9000 normal ending of command
 6B00 incorrect parameter P1 or P2
 9804 access conditions not fulfilled

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].

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).

- 00 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 - X	<i>WLAN –IDENTITY</i>	<i>X</i>

Returned Status Codes

- 9000 normal ending of command
- 6B00 incorrect parameter P1 or P2
- 9804 access conditions not fulfilled

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	<i>NONCE</i>	16

Returned Status Codes

- 9000 normal ending of 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. The response data contains both the EAP response packet and the keying material, which can be used by the client authentication handler.

This command may update the pseudonym and/or the re-authentication ID of the user, which can be read using the SELECT IDENTITY command.

This command may 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'	<i>Reference Control</i>	<i>Authentication -Type</i>	<i>X</i>	<i>Y</i>

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	<i>Z</i>
Z+1 – Z+128	KEYING MATERIAL	128

Returned Status Codes

- 9000 normal completion
- 6B00 incorrect parameter P1 or P2
- 9804 access conditions not fulfilled
- 9820 no previous GET RANDOM performed
- 9821 no previous SELECT IDENTITY performed
- 9822 authentication failed, network MAC was incorrect

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.

This command may 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

9000 normal completion
6B00 incorrect parameter P1 or P2
9804 access conditions not fulfilled

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 '0001'.

This specification: WLAN-SIM cards supporting WLAN-SIM version 1 will return '0001'.

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

9000 normal completion
6B00 incorrect parameter P2
9804 access conditions not fulfilled

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'