3GPP TSG SA WG3 Security – S3#25 **S3-020517**

8 - 11 October 2002

Munich, Germany

Source: **GEMPLUS Card International**

Title: **Use of smart cards in WLAN interworking**

Document for: **Discussion**

Agenda Item: **7.9**

Abstract

This input paper aims at proposing a pertinent way of defining a 3GPP system- WLAN interworking in secure manner with the help of smart cards.

1. Reasons to use smart cards in WLAN

The WLAN security requirements deal with subscriber's credentials storage, authentication, key management, confidentiality and data integrity.

On the market today, there are several solutions to provide security, and more particularly authentication, confidentiality and data integrity. In this section we will discuss the use of software only solutions.

Several attempts have been made to secure data in computer platforms such as PC, MAC or PDA. All implementations on such devices leave potential risks such as the possibility to load Trojan horses, worms or virus. Software applications lack the protective mechanisms often found in dedicated hardware devices (e.g., tamper resistance and physical encapsulation of critical circuitry). Reverse engineering techniques, such as extracting program code and disassembly/debugging methods, are simplified greatly in a software environment, allowing a token's secret components such as cryptographic algorithms, private keys, and other assumed secure information to be recovered.

Software tokens provide convenience because they operate on a platform that the user already has access to. They do no require owning an application-specific piece of hardware and do not add another piece of equipment that could be lost or stolen. Software tokens allow the execution of an application that previously ran on a secure device to be embodied on an insecure platform, causing a weak link in the security chain because in software environment the application inherits the same level of security as the operating system it is running on. The availability of free and commercial decompilers for software token environments such as Windows, Palm OS and Java, makes the software reverse engineering task a more likely one than hardware counterparts.

The main advantage of smart cards is that they are tamper resistant devices that allow to store and process information needed for user identification and authentication. Hardware and software countermeasures are built into smart cards to protect them against invasive and non-invasive attacks, among which fault attacks, power attacks, buffer overflows, malicious code attacks, and ultimately cryptanalysis.

So, the smart card shall be used to fulfil WLAN security requirements.

2. SIM in WLAN

Using a SIM or USIM for access credential storage and authentication of a subscriber in a WLAN interworking scenario with telephony system has a lot of advantages due to its being tamper resistant, independent of the hardware and related to a very large distributed subscriber base, allowing continuity of services and roaming.
However, the use of current SIM in WLAN has to be carefully studied. In the context of the EAP SIM protocol, the following risks have been identified.

2.1. Identified risks

There are some risks due to the use of a standard SIM in the EAP SIM protocol described in Internet Draft draft-haverinen-ppext-eapsim-v04.

This authentication mechanism is based on client software receiving a challenge from the network, submitting it to the SIM and sending the result back to the network. In this case, the possibilities to hack have changed. The system is doubly open. Firstly, the Internet is infected by lots of Trojan horses and other malicious programs and secondly, by suppressing the wires, there is no physical barrier anymore for a hacker to interfere with the SIM.

- Possible attack on the secret key Ki

The authentication agent needs as a first step to fetch the appropriate triplets from the SIM using the RAND received from the AAA server. The authentication agent executes the Run GSM Authentication APDU command. This APDU command is run as many times as the system requires.
It is obvious to imagine that a non-authorized agent running in the mobile client can process an appropriate number of times the APDU command Run GSM Authentication to retrieve authentication triplets (RAND, SRES, Kc).
If the algorithm used to execute the APDU command Run GSM Algorithm authentication is COMP128**-1**, then the Berkeley attack discovered in 1998, based on the knowledge of a concomitant amount of the triplets (RAND, SRES, Kc) can be performed to discover the key Ki.

- Possible spying on, or attack on the SIM data

The standard SIM states that the user pin-code (CHV1) needs to be presented before RUN GSM ALGORITHM command can be executed. Therefore, in order to authenticate to WLAN, using a standard SIM, the user will have to type his CHV.
This CHV gives access to most of the data in the SIM, abbreviated dialling numbers, short messages, network settings, IMSI and other. Therefore, a malicious program in the supplicant can read this data and either upload it to a cracker server or modify the contents for some criminal reasons.

Some risks have been identified but improvements exist to fix those threats.

2.2. Improvements

Taking into account the today's GSM architecture and the identified risks, the following SIM improvements are proposed:

- Use of stronger algorithm

The COMP128 was improved, new versions exist (COMP128-2,3) or other proprietary algorithms.

- The SIM has to perform authentication computations

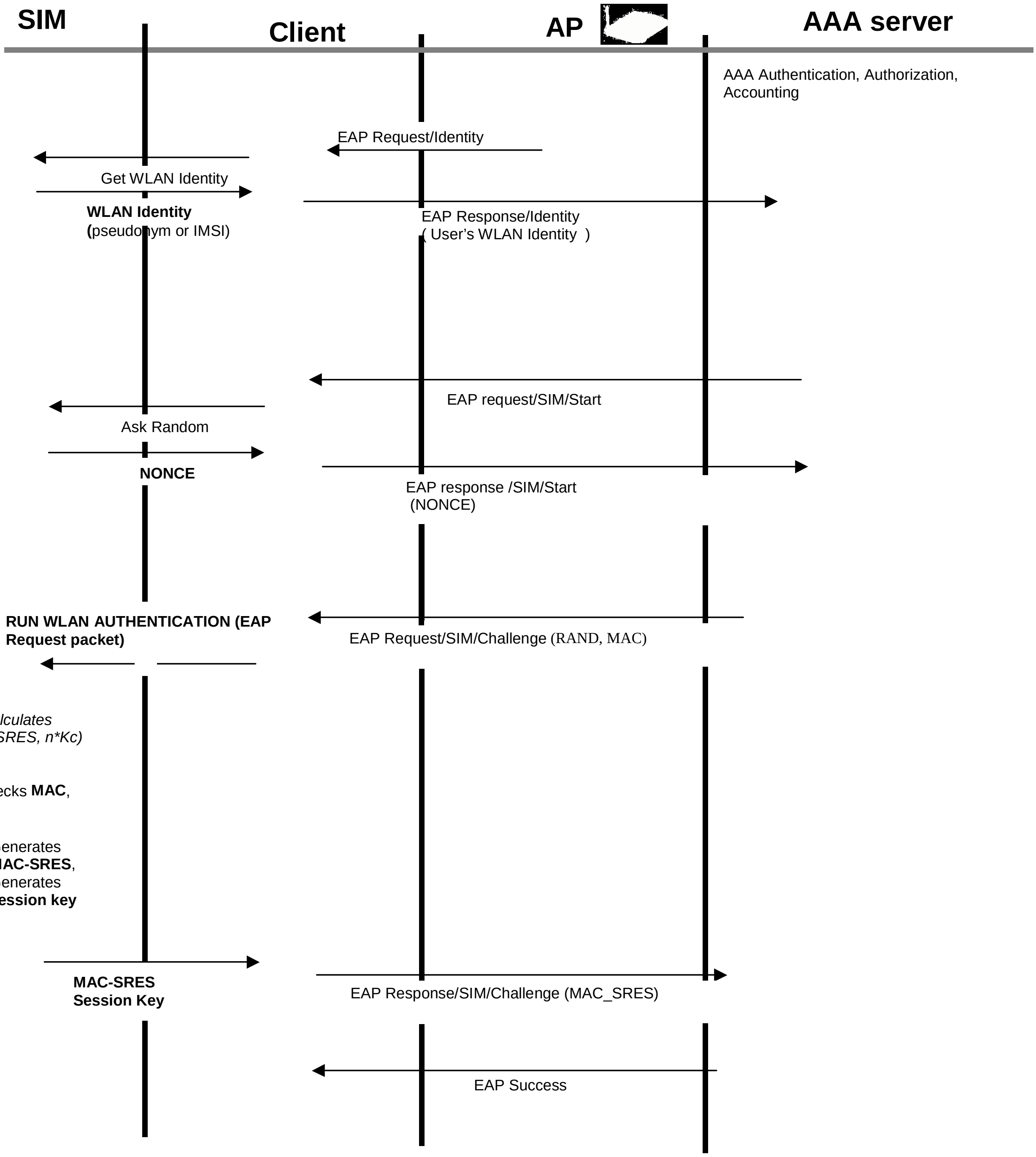
The SIM shall run the GSM algorithm, verify MAC, derive MAC_SRES and compute session key.
In this way, the triplets (RAND, SRES, Kc) are no longer available in the authentication agent.

- To protect WLAN data by logically different PIN

This PIN prevents access to GSM data as GSM CHV1 is not presented.

Those improvements are possible by modifying the current EAP SIM protocol and the SIM. New supplementary commands have to be added to control use of IMSI and GSM algorithm. A new file structure is also necessary to create a dedicated file for WLAN data, DF_{WLAN}, protected by a dedicated PIN.

Proposal for the EAP SIM protocol:



Conclusion:

Those SIM improvements are solution to fix problems in a today's GSM architecture.

3. WLAN specific UICC application

For interworking purposes between 3GPP systems and WLAN networks, the use of standard USIM is often mentioned as the solution to authenticate a user for WLAN access.
However, USIM data and commands are defined for UTRAN access and WLAN having its own specific protocols, environment and business model, the definition of a WLAN independent application in the UICC is a better approach for tackling this issue.

3.1. Reasons for a WLAN specific application on UICC

- Independency of access credentials

Access credentials can be shared with USIM, but could also be specific to WLAN. It should be a 3GPP system's operator decision to either allow the same credentials to grant access via UTRAN as via WLAN, or to differentiate the access rights. This can only be possible if an application is used on UICC, independent of USIM (but possibly sharing data and algorithms with USIM)

- Specificity of WLAN authentication algorithms

It is important to build the interworking architecture upon the existing WLAN standards, while UMTS AKA shall be reused for compatibility with 3GPP.
Authentication algorithms or procedures are WLAN specific: WLAN authentication is based on EAP and confidentiality is defined in e.g. IEEE 802.11i, based on the derivation of temporary session keys from a Master Secret obtained within the EAP process.
Should standard USIM commands be used? In this case, the supplicant software will have to process the UMTS authentication vectors to obtain WLAN specific authentication vectors. But, the environment of WLAN is doubly open. Firstly, the Internet is infected by lots of Trojan horses and other malicious programs and secondly, by suppressing the wires, there is no physical barrier anymore for a hacker to interfere with the software in a terminal. Network operators have no or little influence on the PC environment and its protection, in contrary to UICC.
Therefore, if UICC only executed UMTS AKA, leaving the rest of the authentication to the supplicant software, the security of the system could be jeopardized.
Thus a specific authentication function shall be implemented on the UICC, to execute the whole EAP based authentication and calculation of the temporary session keys in this tamper resistant device; UICC can use UMTS AKA internally, but a specific algorithm can also be used.

- Protection of USIM data

USIM data shall be protected if needed, against eavesdropping from malicious programs in the client.
As mentioned above, the environment of WLAN terminals is prone to introduce malicious programs, able to download to a distant server information from phonebook, network –e.g. IMSI-, or other sensible data, if USIM was to be activated in a WLAN terminal.
When a specific WLAN application is used for interworking scenarios and not USIM, it is possible to protect USIM data from the outside world, simply, because only the data needed in the WLAN situation can be filtered through this independent application, USIM itself remaining off-line.

3.2. Architecture of WLAN specific UICC application

A WLAN specific UICC application, called WSIM in the remainder of this document, is an application on UICC, independent of other applications residing on UICC. Therefore it can be combined with USIM and ISIM for a complete subscription to 3G services or it can be a stand-alone application, in case a WLAN subscriber is not access allowed on UTRAN.

The three figures below give some possible implementations:

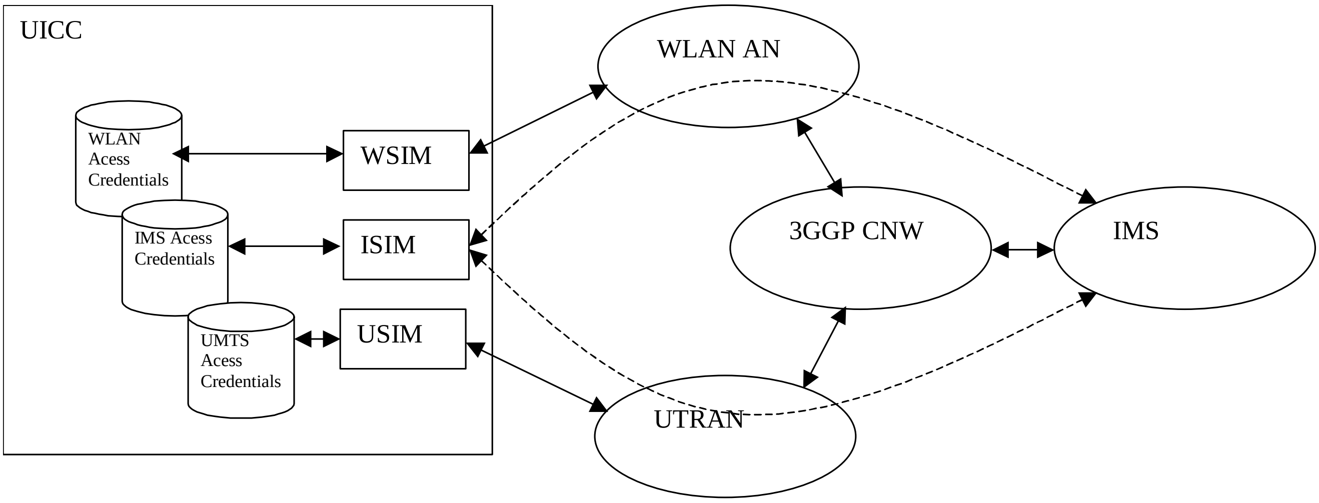


Figure 1: UICC allowing access to WLAN AN, UTRAN and IMS, with access credentials that are specific to WSIM, USIM and ISIM.

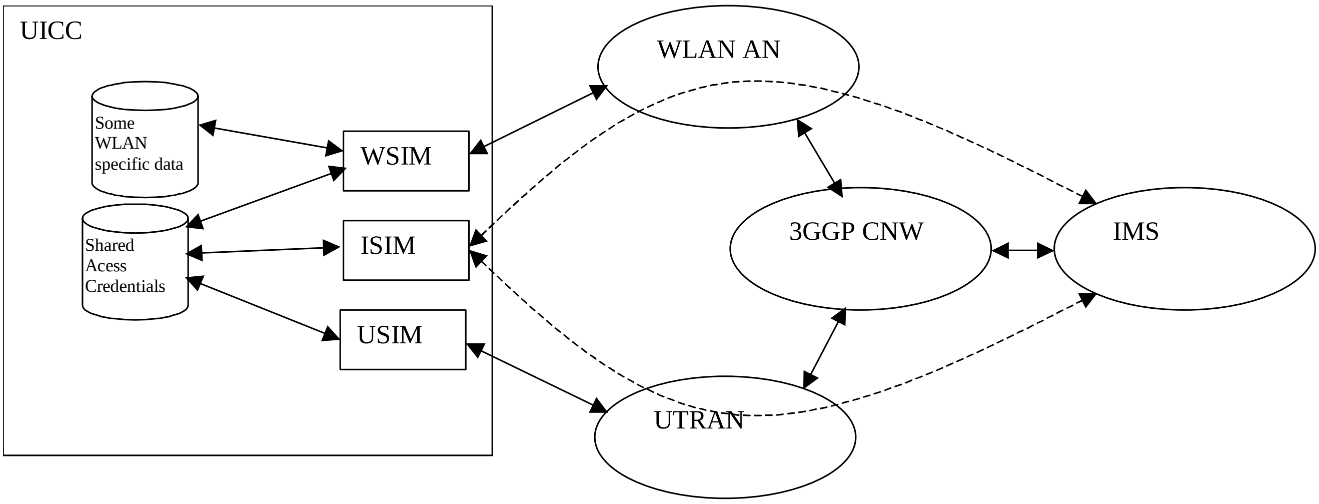


Figure 2: UICC allowing access to WLAN AN, UTRAN and IMS, with some access credentials shared between WSIM, USIM and ISIM.

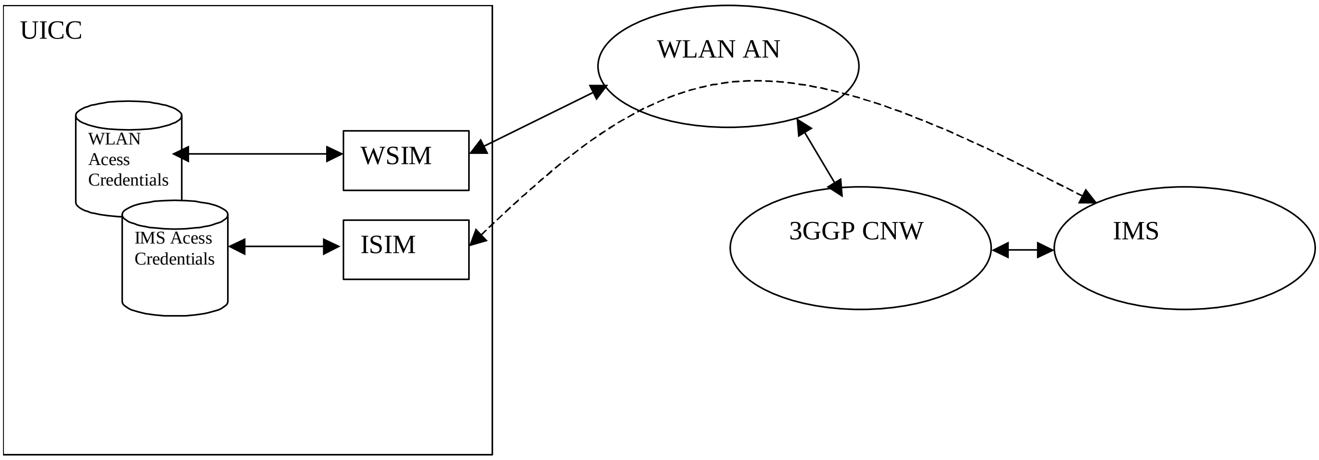


Figure 3: UICC allowing access to WLAN AN and IMS, with access credentials that are specific to WSIM and ISIM.

3.3. Commands and data of WSIM

Commands and data are identified for this WLAN specific application.

- Network Access Identifier

The NAI is used in WLAN AAA protocols to identify a client. The NAI can either be derived from the IMSI, in which case this data element is shared with the USIM, but it can also be defined specifically for WLAN access, in which case this data element should be stored independently in WSIM

- Identity protection

Unlike IMSI, which in UMTS can practically only be discovered when eavesdropping radio transmissions, the NAI of the client can be spied easily when the client is connected to the Internet. Therefore a method should be defined hiding the real NAI as much as possible from the outside world, by using some sort of temporary NAI.
A special command shall be defined allowing the supplicant software to obtain this temporary NAI, under control of WSIM, denying any access to the real NAI.

- WLAN authentication algorithm

A command, with input and output parameters based on e.g. EAP, IEEE 802.1x, TKIP or the like, will be needed to execute a WLAN specific authentication procedure as complete and secure as possible. This command can reuse UMTS AKA, possibly with extensions to generate e.g. WLAN specific session keys, and can use USIM related data elements, in order to allow the integration with the existing HLR/AUC.

- Backward compatibility

The reality of the market being that WLAN networks are being deployed in a world that mainly still uses SIM in GSM networks, the above mentioned data elements and command interfaces should be defined in such a way that they can be implemented on legacy SIM. Thus, the same level of security can be obtained with a WLAN interworking with GSM as well as with a 3GPP system, without modifying the role of the supplicant software, and thus restricting the related software modifications of devices in the field, if ever the network was upgraded from GSM to 3GPP.

4. Conclusion

This paper presents the advantages of using smart cards in WLAN interworking, the smart cards features allow to fulfil security requirements.
In the context of SIM in WLAN, some improvements of the current SIM and the EAP SIM protocol are needed to reinforce the security.
This paper also defines a WLAN specific UICC application. The advantages of this new application (called WSIM) are the support of legacy WLAN standards, protection of USIM data, potential independency of the WLAN system and possibility of backward compatibility with GSM.