3GPP TSG SA WG3 Security — SA3#35 **S3-040760**
October 5-8, 2004
St Paul's Bay, Malta

Source: **Axalto, Gemplus**

Title: **3GPP UE function split for a 3GPP WLAN user equipment**

Document for: **Discussion and decision**

Agenda Item:

1. Introduction

SA3 identified 3 alternatives to proceed their work on 3GPP UE function split for a 3GPP WLAN user equipment and decided during SA3#32 to drop alternative 1, where all functions of the EAP peer are executed on the TE, with the exception of the GSM/UMTS cryptographic algorithms on the SIM/USIM. To achieve its purposes, alternative 1 uses the SIM Access Profile (SAP) developed in BLUETOOTH SIG forum. The security risks, and threats of this alternative were already assessed by SA3, which concluded that alternative 1 is unacceptable and consequently shall be dropped.

Furthermore, alternative 2 was chosen as the working assumption for WLAN UE functional split (see S3-040197). However, if SA3 confirms the need to WLAN UE split interworking for release 6, basic precautions need to be taken to ensure the feasibility of alternative 2. In this paper, we propose a technically feasible solution to implement WLAN UE functional split as described in alternative 2.

2. Alternative 1 was dropped by SA3

TS 33.234 shall be updated to reflect SA3 decision to drop alternative 1. Indeed, the following quote from TS 33.234 allows a WLAN Terminal Equipment to perform all functions of the EAP peer on the TE, with the exception of the GSM/UMTS cryptographic algorithms (i.e. alternative 1):

> *For SIM access via a Bluetooth link, the SIM Access Profile developed in BLUETOOTH SIG forum may be used. See [22].*

In fact, the Bluetooth SIM Access Profile makes the SIM accessible by the TE (e.g. PCs, PDAs), exposing the SRES and Kc cryptographic parameters. Exposure of these parameters to open mobile platforms like PCs and PDAs is a serious problem that can lead to fraud. Furthermore, this may compromise the security of the whole system, spreading the GSM vulnerabilities from the GSM network to the WLAN network. For those reasons, SA3 decided to drop the so-called alternative 1 solution for WLAN authentication using EAP-SIM protocol (see S3-040197).

Furthermore, there are discrepancies in TS 33.234 between section 6.7 and 4.2.4.3. In fact, the section 6.7 states that EAP termination shall be in the MT, while section 4.2.4.3 authorize the use of the Bluetooth SAP without any restriction and consequently authorize the implementation of the so-called alternative 1 of the WLAN UE functionality split.

However, it would be possible to use the SAP for implementing alternative 2 if the termination of EAP is in the UICC. This is achievable in the release 6 timeframe, as T3 has only to reference ETSI TS 102.310 in the USIM specification. Besides some restriction on SAP must be added to avoid any misinterpretation of the specification.

Finally, we would like to stress the fact that this solution will function only with Bluetooth. Therefore, in the present document we present another generic solution, which works on all local bearers, and which is achievable in the release 6 timeframe.

3. Alternative 2 as currently defined

We acknowledge the benefits of accessing the USIM capabilities directly by a Laptop PC to authenticate a WLAN session. Unfortunately alternative 2, as presently defined in TS 33.234 is not technically feasible in release 6 since the required standardized API between the TE and the ME is currently not defined. Some SA3 delegates proposed to ask Bluetooth SIG to define a new suitable profile, to have such API specified. But this is not an acceptable solution, as 33.234 will be soon frozen. During SA3#34, it was clarified (see SA3#34 report) that Bluetooth SIG needs a couple of years to come up with a new suitable Access Profile. Since this API will not be available on time, proprietary solution will be developed compromising interoperability. Furthermore this solution will only function for Bluetooth, and is not reusable by other widely deployed local links such as USB, IrDA, and serial interfaces. Finally, we would like to stress the fact that a frozen specification must not reference a not stabilized and published specification, because related features may evolve and consequently existing implementations risk to become out of the standard.

Additionally, SA3 acknowledged that alternative 2, where EAP is handled by the USIM, provides security improvements compared to all other alternatives and can enhance user identity privacy.

Finally, we would like to note that it is strange to require a ME without any WLAN interface (likely a low-end terminal) to support an EAP client for the WLAN functional split (necessarily including e.g. hashing functions, pseudo-random number generators, EAP packet handling and logic, etc). Besides the proposed solution (see section 4) can function with MEs supporting a subset of UICC AT commands defined in TS 27.007 [1]. Furthermore those AT commands may be useful (i.e. already implemented) for other applications.

4. Feasible alternative 2 solution for release 6

On the other hand, alternative 2, where the termination of EAP is in the UICC, is feasible using the AT commands defined in TS 27.007 [1] and EAP support in UICC as defined in TS 102.310 [2]. The new *UICC +CRLA and +CGLA* AT commands were created to allow communication with a UICC application (e.g. USIM) through the ME. A TE can use those commands to exchange EAP packets with the USIM, and to get MSK and EMSK keys.
First, this solution is technically feasible as the API is already standardized in release 6 in TS 27.007 [1]. Second, the usage of those commands can be restricted to commands defined in ETSI TS 102.310 [2] to avoid falling back to alternative 1, which was rejected by SA3. The usage of AT commands restricted to a set of APDU guarantees interoperability and provide an API that is usable for all local links (not only Bluetooth).

Presently this is the only already standardized way to support the alternative 2 of the functional split in release 6. However, some requirements and restrictions shall be added to the Bluetooth security mechanism to provide the necessary security level for reuse.

5. Proposed solution benefits

It is certainly worth reminding that interestingly the usage of EAP support in UICC has the following benefits:

- The computation of EAP-AKA and EAP-SIM master keys will be performed by the UICC and securely stored along with user identities on the card. This will strengthen the user and network security, as critical cryptographic parameters (e.g. Kc, SRES, MK, counter …) will never leave the secure smart card environment. Additionally, re-authentication information cannot be replayed, as they don't leave the card. This will protect the WLAN session against hijacking and will result in much less frequent full authentication, preventing high network load especially when the number of connected users is high.
- This solution offers a higher security level to prevent attacks identified in S3-040110 contribution. Moreover security domains are implicitly segregated through the usage of different APDU commands (see S3-040009): one for WLAN authentication and one for UTRAN/GERAN authentication, preventing the spreading of vulnerabilities between WLAN and UTRAN/GERAN.
- The executing of the EAP-SIM specific cryptographic calculations in the UICC protects the A3/A8 algorithm. Additionally, we ensure that the mutual authentication is performed between the user (i.e. smart card) and the network.
- The proposed EAP functional spilt prevents false base station attacks and impersonation of EAP-SIM server (see S3-040110).
- Only temporary keys are transmitted over the local link (we would like to remind that EAP packets are already transmitted in clear on the WLAN radio interface,) and consequently the security of the local link (e.g. Bluetooth) only impacts the user security and does not impact the security of the network. However, additional recommendation and requirement to enforce the local link security are necessary to enforce user security.
- Easy to implement on the ME, and the TE. Enhance interoperability since the required API is well specified and can be used by different type of local links.
- Can be adopted by 3GPP in Rel-6 timeframe (API and EAP support in UICC are standardized).

6. Conclusion

- The usage of SIM Access Profile, as currently specified by TS 33.234, may result in undesired implementations, compromising the security of the whole system and spreading the threats between WLAN and GSM/GPRS domains. An attached CR is presented in S3-040xxx [7], which includes some specific requirements for the SIM Access Profile usage in WLAN UE functional split.

- The usage of EAP authentication capabilities of a UICC offers higher security and improves interoperability. Moreover, this is the only implementable solution in Rel-6 timeframe as ETSI SCP has completed the standardization of the EAP support in UICC and as T2 completed the standardization of UICC AT commands. We kindly recommend SA3 to adopt this solution as a new functional split scenario. An attached CR is presented in S3-040xxx [8].

7. References

[1] 3GPP TS 27 007, “AT command set for User Equipment (UE)”, Rel-6, v6.6.0

[2] ETSI TS 102 310, “Extensible Authentication Protocol support in the UICC”, Rel-6, v6.0.0

[3] 3GPP TS 33.234 V6.2.0 “Wireless Local Area Network (WLAN) Interworking Security”.

[4] S3-040009, " Protecting GSM/GPRS networks from attacks from compromised WLAN networks when interworking"

[5] S3-040110, "Comments on S3-040009 and S3-040100 on measures for separation of domains"

[6] S3-040197, " Further Liaison on Termination of EAP authentication over Bluetooth for 3GPP UE function split"

[7] TD S3-040xxx, “CR: Alignment of TS 33.234 with SA3 decisions on WLAN UE function split”, Axalto, SA3#35

[8] TD S3-040xxx, “CR: Correction of WLAN UE function split”, Axalto, SA3#35