3GPP TSG SA WG3 Security#30 **S3-030550**
6 – 10 October, 2003
Povoa do Varzim, Portugal

Agenda Item: **7.10 (WLAN)**

Source: **Siemens**

Title: **Evaluation of alternatives for secure set-up of UE initiated tunnels**

Document for: **Discussion and decision**

1. Introduction

So far, 3GPP SA3 has addressed only the security of scenario 2 for 3G-WLAN interworking. Scenario 2 is about network access over WLAN, using the 3G authentication infrastructure. The results of SA3's work are contained in draft TS 33.234. But other 3GPP working groups, in particular SA2, have progressed work on scenario 3 for 3G-WLAN interworking. Scenario 3 is about the access of 3G subscribers to MNO-provided services (e.g. IMS) using WLAN access. 3GPP SA2 took some important decisions at their last meeting, which are contained their draft TS 23.234 v200. Although the last SA plenary did not put TS 23.234 under change control they agreed that the material in draft TS 23.234 v200 should be taken as working assumption.

It is now the time for SA3 to start their security work relating to scenario 3. This contribution is intended to state the problem to be solved by SA3, and evaluate potential solutions.

In particular, SA2 took the following decisions:

- A UE-initiated tunnel from the UE to a suitable network-endpoint is required for scenario 3;
- This network endpoint is the Packet Data Gateway (PDG). This is the so-called end-to-end tunnelling solution.

The debate in SA2 and in SA mainly centred on the alternatives "end-to-end tunnelling solution " vs. "tunnel switching solution". In the latter, the network endpoint of the tunnel would be the WAG. Although we assume in this contribution that the endpoint is the PDG, in accordance with SA2's, and SA's, current working assumption, the contents of this contribution are largely independent of the particular tunnelling solution.

The PDG may reside in the home or in the visited network. It can be expected, however, that the PDG will reside in the home network in the initial phases of deployment.

The precise nature of the tunnel (IP in IP only, or layer 2 tunneling) will be decided as part of the stage 3 work. It is argued below, however, that this has no influence on the security work.

2. SA2 requirements and consequences for security

TS 23.234 v200 (= SP-030391) contains the following requirements:

Section 4:

"For scenario 3, access to External IP Networks should, as far as possible, be technically independent of WLAN Access Authentication and Authorisation. However, Access to External IP Networks from 3GPP

WLAN interworking systems shall be possible only if WLAN Access Authentication/Authorisation has been completed first.

Note: The independence requirement does not preclude the possibility that the procedure for access to external IP network may rely on information derived in the procedure for WLAN Access Authorization."

Section 5.6:

- "The Service authorisation procedure should, as far as possible, be independent from WLAN access authentication and authorisation."
- "Service authorization information shall be protected"

Section 5.7:

- "Minimal requirements to the underlying IP connectivity network, i.e. WLAN UE initiated tunnelling and tunnel establishment signalling can be deployed on top of generic IP connectivity networks"
- "Minimal impacts to the WLAN"
- "Establishment of trusted relationships (e.g. mutual authentication for both tunnel end-points) shall be possible."
- "Set up secure tunnels between WLAN UE and remote tunnel endpoint. Especially support encryption and integrity protection during tunnel establishment and while transporting user data packets, if enabled."

The following can be concluded from the above requirements:

A security mechanism is required to provide confidentiality and integrity protection for IP packets. This mechanism is to be general enough to work without additional assumptions on the particular IP connectivity network or underlying link layers. The only such mechanism standardised and widely used today is IPsec ESP (RFC2406). Please note that IPsec ESP can be used, no matter whether a layer 3 tunnel (IP in IP) or a layer 2 tunnel will be used.

Proposed Working Assumption 1: use IPsec ESP to protect the tunnels between UE and PDG required by scenario 3.

This immediately leads to the following task to be solved by SA3:

Proposed Task 1 for SA3: define a profile of IPsec ESP for use with scenario 3.

An example of a profile for IPsec ESP elaborated by SA3 in a different context is given in section 5.3 of TS 33.210 (NDS/IP).

Furthermore, providing the working assumption to use IPsec ESP is accepted, it is also required to standardise a method to establish security associations. This leads to the second task to be solved by SA3:

Proposed Task 2 for SA3: standardise the set-up of security associations for IPsec ESP between UE and PDG.

As a matter of course, the set-up of security associations will **have** to include "mutual authentication for both tunnel end-points " (not only making it possible), thus satisfying one of SA2's requirement, cited above.

Independence of access to External IP Networks, service authorisation and WLAN AAA: the statements by SA2 seem a bit vague here. But the principle expressed here, also adhered to by SA3 for other work items in an analogous fashion, seems to be, that the security for the IP tunnel in scenario 3 is to be independent of the link layer security in scenario 2. I.e., in principle the security specified for scenario 3 could also be used for other link layer, e.g. GERAN or UTRAN, where currently no protection

of user data is available beyond the SGSN or RNC respectively. The use of this independence principle (also used for IMS security) seems a prudent approach, as it makes the 3GPP security specifications more modular, and hence, provides a greater potential for re-use in different system configurations. We therefore propose this as a working assumption for SA3:

Proposed Working Assumption 2: the security mechanisms used in context with the IP tunnel in scenario 3 are to be independent of the link layer security in scenario 2.

The remaining part of the document deals with the proposed task 2, as it is considered the main problem to be solved.

3. Methods to establish IPsec security associations

Various methods are available as drafts or standards or as proprietary solutions in products. The conclusion of this section is to only take IKE and IKEv2 into account for further study in SA3. For these two protocols, the credentials required for mutual authentication of the two peers are also discussed.

3.1 Internet Key Exchange (IKE)

IKE is specified in RFC2409. It has been available in products for quite some time, e.g. as part of VPN gateways and VPN clients. An issue may be its complexity, which may cause difficulties for mobile terminals with low computational and storage capacity.

IKE has two phases. For the mutual authentication of IKE peers in IKE phase 1, the following options are possible:

- Both peers use pre-shared keys;
- Both peers use certificates.

The fact, that IKE knows four different certificate-based methods, and that the certificates are on digital signature keys, or encryption keys, need not interest us for our purposes here.

3.2 Internet Key Exchange (IKEv2)

This is ongoing work at the IETF. The current draft is draft-ietf-ipsec-ikev2-10. The work was motivated by the need to reduce the complexity of IKE while maintaining and even enhancing its valuable features. The work is considered quite mature, and a completion can be expected soon, although it appears difficult to give precise dates. But this situation is no different from the intended use of other Internet drafts for 3GPP Release 6 specifications (e.g. EAP-AKA, http digest akav2).

For the mutual authentication of IKEv2 peers, as for IKE, the following options are possible:

- Both peers use pre-shared keys;
- Both peers use certificates.

IKEv2 also allows the option that one peer uses certificates, while the other uses a secret key. But this seems to make little sense, except with the following new feature of IKEv2 (cf. draft-ietf-ipsec-ikev2-10, section 2.16), which is not present in IKE:

- the initiator (e.g. UE) is authenticated by means of EAP (e.g. EAP/SIM or EAP/AKA) and the responder (e.g. PDG) uses certificates.

This feature may prove quite interesting for 3GPP scenario 3, as it would allow the UE to be authenticated by means of EAP/SIM or EAP/AKA, the protocols which are also used for scenario 2. The 3GPP AAA infrastructure and the interface of the AAA server to the HSS could also be re-used. And yet, the

requirement that the security for scenarios 2 and 3 be independent would be fulfilled. In a way, this situation is analogous to IMS security: IMS AKA, and ISIM, are functionally identical to UMTS AKA and USIM, but are different instances of these functions, and IMS security is no doubt independent of UMTS network access security.

It should also be mentioned that IKEv2 provides a number of other enhancements over IKE. They include the protected exchange of configuration data from the PDG to the UE in an extensible manner, and enhanced NAT traversal capabilities. 3GPP IMS security

TS 33.203 defines a method to establish IPsec ESP security associations, using http digest aka (RFC3310), sip-sec-agree (RFC3329), and transport in appropriate SIP headers. But while http digest aka may be re-usable in the setting of 3G WLAN interworking scenario 3, the other elements seem bound to a SIP environment, and it is difficult to see how the security solution for the IMS could be applied here.

3.3 Other methods

There are a number of other methods to set up security associations. None of them seem particular suitable. We mention the following for completeness:

KINK (RFC3129):

KINK is a protocol to facilitate centralised key management for IPsec security associations, as an alternative to IKE. Participating systems will use the Kerberos architecture as defined in RFC 1510 (and its successors) for key management. KINK is claimed to be a streamlined, fast, easily managed, and cryptographically sound protocol that does not require public key operations, and is compatible with existing and future Kerberos infrastructures.

As Kerberos is not used anywhere in a 3G environment, KINK seems not useful for our purposes.

Proprietary methods:

Some vendors defined their own methods, e.g. XAUTH by Cisco. XAUTH is mentioned here, as it is used in some WLAN hotspots today. However, it seems not appropriate for a 3G specification to make reference to, and rely upon, vendor-proprietary methods.

3.4 Conclusion of section 3

Proposed Working Assumption 3: SA3 will concentrate their further study on IKE and IKEv2.

4. Methods to establish credentials

4.1 Shared keys

4.1.1 Manual establishment

Manual establishment of shared keys is known to be cumbersome and difficult to manage for large numbers of users. It may only be considered an option in the very initial phases of deployment. It would also imply that the PDG as the network-side endpoint of the IPsec tunnel would have to hold a large number of permanent user secrets, thus becoming a new sort of 3G authentication centre. This seems undesirable.

4.1.2 3GPP Generic Bootstrapping Architecture (GBA)

It was agreed by those present at the SA3 ad hoc meeting in September 2003, that the security for new Release 6 feature should make use of a GBA as far as possible, in order to avoid a proliferation of security methods, in particular in the terminal. But it was also acknowledged that the GBA could probably not be applied to 3G-WLAN interworking scenario 2 (network access using EAP-AKA and EAP-SIM).

The GBA is yet to be defined. The main agreement reached so far is that it is to be based on the architecture described in section 4 of the draft TS 33.109 ("Bootstrapping of application security using AKA and support for subscriber certificates"). The main elements of the architecture are depicted in figure 1 below. Figure 1 is taken from figure 1 in TS 33.109. This architecture could be mapped to 3G-WLAN interworking scenario 3 as follows:

The GBA would be used to supply the UE and the PDG (as the network-side endpoint of the IPsec tunnel) with a shared key. So, the PDG would assume the role of a NAF (Network application function). The BSF (Bootstrapping server function) would be an element shared with other applications, and would not be specific to 3G WLAN interworking. The shared key established through the GBA could then be used for mutual authentication in IKE or IKEv2, as described in section 3.1 and 3.2.

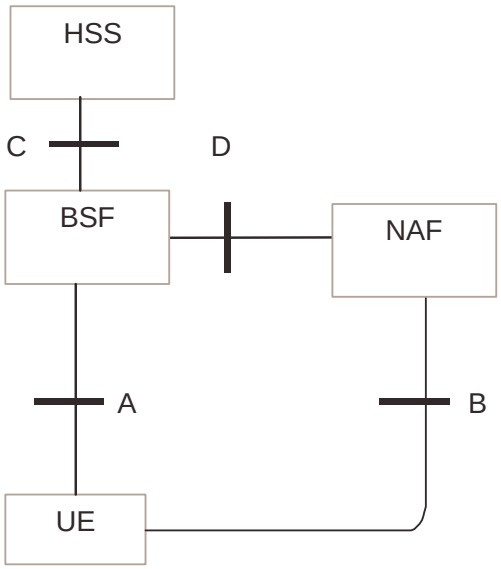

Figure 1: Simple network model for bootstrapping

However, there seem to be a number of problems with using the GBA for 3G-WLAN interworking scenario 3, quite apart from the fact that important details of the GBA specification are still missing.

- It is not clear what should serve as protocol B. In TS 33.109, or the GBA, protocol B is meant to be using the shared key established by the GBA. Then protocol B would have to be IKE, or IKEv2. But the architecture in TS 33.109 requires of protocol B that a transaction identifier can be carried in the first message sent from the UE to the NAF = PDG. The transaction identifier is needed by the NAF so that the NAF can retrieve the shared key from the BSF via protocol D. However, there seems to be no field in IKE or IKEv2 which would allow to carry such a transaction identifier. And, perhaps more importantly, even if there was, this would be a non-standard use of IKE and IKEv2, not compatible with any standards-compliant implementations. So, an additional protocol would be required to inform the NAF = PDG of the transaction identifier agreed between UE and BSF. This additional protocol would have to be added to the current architecture of TS 33.109.

- The PDG, as far as its function to terminate the IPsec tunnel on the network side goes, can be considered as a VPN gateway. This VPN gateway would require 3GPP-specific enhancements to dynamically acquire pre-shared keys, using protocols B and D. It would also require interaction between these 3GPP-specific enhancements and the IKE, or IKEv2, implementation to allow the resulting key to be written into a key store for pre-shared keys, from which IKE, or IKEv2, could retrieve it at the start of a run of IKE, or IKEv2. This would certainly prevent the re-use of VPN gateways, just conforming to existing, or upcoming IETF standards.

4.1.3 Derivation from EAP-AKA / EAP-SIM link layer keys

After network access over WLAN (scenario 2) shared keys are available at the UE and the 3GPP AAA server from a run of EAP-AKA or EAP-SIM. These keys could be used as a basis to derive further keys. There is ongoing work at the IETF on "EAP Key Derivation for Multiple Applications" (cf. draft-salowey-eap-key-deriv-01), which could prove potentially useful for establishing a shared key for IKE, or IKEv2, in scenario 3. But there are a number of difficulties with this approach as well:

- It is unclear at the moment how fast this work can be completed as the EAP working group is currently busy to solve more elementary issues related to the EAP keying framework.

But the next issue seems more important. It is quite similar to that noted for the use of the GBA in section 4.1.2:

- The PDG, as VPN gateway, would require 3GPP-specific enhancements to dynamically acquire pre-shared keys, using protocols between the PDG and the 3GPP AAA server yet to be specified. It would also require interaction between these 3GPP-specific enhancements and the IKE, or IKEv2, implementation to allow the resulting key to be written into a key store for pre-shared keys, from which IKE, or IKEv2, could retrieve it at the start of a run of IKE, or IKEv2. This would certainly prevent the re-use of VPN gateways, just conforming to existing, or upcoming IETF standards.

And, finally:

- This approach would tightly couple the security for scenarios 2 and 3, contradicting the proposed working assumption 2 in section 2.

4.1.4 EAP-based authentication of the initiator in IKEv2

When this option is used then shared keys are required for the authentication of the IKEv2 initiator, i.e. the UE. (For server certificates cf. section 4.2.) It would be natural to assume that the protocols used should include EAP-AKA. It needs to be discussed further whether the use of EAP-SIM, i.e. SIM-based access, should also be allowed. But this is an operator decision and depends on the security level an operator wants to achieve when allowing access to services. This solution has the following advantages:

- The existing 3G authentication infrastructure is used for UE authentication.
- No 3GPP-specific extensions to an IETF standard are necessary.
- A 3GPP AAA server to handle the EAP protocols is already available for the purposes of scenario 2.
- The required protocols are already implemented in the UE for scenario 2.
- The security for scenario 3 is independent of the security of scenario 2 in the sense that the former can be realised without the latter, and that different instances of the same protocol are used. But if both are in place then there is considerable synergy.

The drawback is that

- IKEv2 may be expected to be finalised in the Release 6 timeframe, but it is uncertain when it will appear in products, e.g. for VPN gateways.

4.1.5 EAP-based authentication using PANA

Currently, it is not possible to use EAP over IP in general. But there is related ongoing work in the PANA WG at the IETF, cf. draft-ietf-pana-pana-01. If an EAP exchange can be done over IP then EAP-AKA and EAP-SIM can be run between the UE and the 3GPP AAA server. The PDG would play the role of a PANA Authentication Agent, terminating the PANA protocol from the UE, playing the role of PANA Authentication Client. The resulting shared key could then be made be used by the UE and the PDG as a shared key in IKE or IKEv2.

- as for the solutions in subsections 4.1.2 and 4.1.3, the IKE implementation in the PDG would need to be enhanced to allow the shared key resulting from the EAP protocol run to be imported.
- With the solution in subsection 4.1.4 it shares the advantage that it uses the authentication servers and protocols already available for scenario 2.
- The completion date of the PANA work at the IETF is open at the moment. The work seems less mature than the IKEv2 work.

4.2 Certificates

4.2.1 Server certificates

The infrastructure and management for server certificates (in IKE or IKEv2) is considered relatively easy to achieve, in comparison to client (subscriber) certificates. The main reason is that the number of servers is smaller than the number of clients by several orders of magnitude, and that it is more economical for an operator to make changes in servers than it is to interact with and manage subscribers.

Server certificates have been in use for a long time with SSL/TLS. From this use of server certificates, it is also well known that careless handling of root certificates may lead to security gaps, so a certain care and effort is needed here.

It should also be taken into account that, in general, a PDG may reside in the visited network. Then the server certificates have to be understood by UEs across network boundaries, i.e. an inter-operator PKI is required. This would slow down the process of installing such a PKI. But, on the other hand, it may be expected that PDGs will reside in the home network in the early phases of deployment.

4.2.2 Client (subscriber) certificates

To supply all UEs with certificates so that the UE can authenticate to the PDG (the IKE or IKEv2 peer) is likely to be a big effort. One drawback for an operator is that a large number of potential users have to be equipped with certificates, while the number of users actually using the certificates for service access in scenario 3 may be much smaller. This would imply that the operator has to realise a big investment, with the return coming only from that smaller number of users. The effort to install certificates on UICCs would be bigger than on MEs.

As for server certificates, it must also be taken into account that, in the general case, an inter-operator PKI is required.

Methods of establishing certificates in clients:

Manual establishment
This could take the form of establishing certificates on the UE e.g. in an operator’s shop. This is relatively expensive and time consuming.

Certificates pre-installed on terminals

This seems only possible when UEs are sold through operators. It is unclear how to handle UEs sold through other channels.

3GPP support for subscriber certificates (cf. draft TS 33.109)

The completion of this work is planned for Release 6. The question for 3GPP SA3 to answer is the dependency on the completion and implementation of this specification is to be made a pre-requisite for 3G WLAN interworking scenario 3.

OMA wireless PKI

It is not clear how widespread implementations of the relevant OMA specs will be, and whether they will be ready for use with Release 6 equipment.

Storing certificates and private keys

SA3 has to answer the question where certificates and private keys should be stored. Ideally, they should be stored on the UICC (and private keys should perhaps even be generated there), but this would imply that 3G WLAN interworking scenario 3 would require Release 6 UICCs and would not work with UICCs of earlier releases.

5. Conclusions

5.1 Proposed working assumptions for SA3

Proposed Working Assumption 1: use IPsec ESP to protect the tunnels between UE and PDG required by scenario 3.

Proposed Working Assumption 2: the security mechanisms used in context with the IP tunnel in scenario 3 are to be independent of the link layer security in scenario 2.

Proposed Working Assumption 3: SA3 will concentrate their further study on IKE and IKEv2.

SA3 is asked to endorse these working assumptions.

5.2 Proposed tasks for SA3

It is proposed in this contribution that SA3 has to solve the following tasks relating to the security of scenario 3:

Proposed Task 1 for SA3: define a profile of IPsec ESP for use with scenario 3.

Proposed Task 2 for SA3: standardise the set-up of security associations for IPsec ESP between UE and PDG.

SA3 is asked to endorse this task description.

5.3 Summary relating to IKE

- IKE is well established in products.
- If shared keys are used then, because manual key handling at the PDG is considered infeasible (cf. section 4.1.1), 3GPP-specific interfaces to IKE would have to be defined to dynamically manage shared keys in the PDG.

- These key management procedures for shared keys are not yet mature in 3GPP (cf. section 4.1.2) and IETF (cf. section 4.1.3) respectively.
- If certificates are used then, in particular, subscriber certificates have to be implemented. This may constitute a considerable effort on the part of the operator, and may require Release 6 UICCs, depending on the requirements.
- If certificates are used then no changes or additions to IKE-compliant equipment are required.

5.4 Summary relating to IKEv2

- IKEv2 is not established in products yet.
- But the IKEv2 specification is likely to be completed by the IETF within the Release 6 timeframe. This has usually been considered sufficient so that an IETF specification can be included in a 3GPP Release 6 specification.
- When both IKEv2 peers use shared secrets, or both IKEv2 peers use certificates, then the same comments apply as for IKE.
- When the IKEv2 initiator is authenticated using EAP-AKA or EAP-SIM then no changes or additions to IKEv2-compliant equipment would be necessary, and the security infrastructure used for 3G WLAN interworking scenario 2 could be re-used for scenario 3. The provision of server certificates in this solution would be considered easier to solve than that of subscriber certificates.
- IKEv2 is less complex than IKE.

5.5 Conclusions

- From the above summary, it appears that, from a technical point of view, IKEv2 with EAP-based authentication of the UE is the preferable solution.
- It remains to be decided by SA3, however, whether IKE should be preferred because of existing product implementations.
- If IKE was preferred for this reason then this seems to contradict 3GPP-specific additions to IKE implementations for key management as this would also mean the development of new products. However, the effort to get such additions in place is certainly a factor to be considered further.
- A decision for IKE as available today would mean the introduction of subscriber certificates. SA3 (especially operators) need to decide whether the deployment of subscriber certificates for the purposes of scenario 3 is considered feasible and desirable.
- As usual, several options in the standard should be avoided.