3GPP TSG SA WG3 Security **S3z020017**

January 31 – February 1, 2002

Antwerp, Belgium

Agenda Item: TBD

Source: Ericsson

Title: Requirements on SA_ID

Document for: Discussion and decision

1. Scope and objectives

This contribution address the issues related to the identifier of the Security Association established between the UE and the P-CSCF. It is currently not clarified in the TS 33.203 specification, how the SA_ID shall be used and what entity that shall handle the allocation of the SA_ID, in the case when SIP level protection is used between the UE and the P-CSCF.

A number of reasonable requirements on the SA_ID are listed in this paper, which should be considered in the discussion regarding the SA_ID.

It is also proposed that an LS is sent from SA3 to CN1 asking what information at SIP level that encompasses the SA_ID.

2 Requirements on SA_ID

In TS33.203 it is currently required that an SA_ID shall be used between the UE and the P-CSCF for identifying the algorithms and keys to be used. The Security Association between the UE and the P-CSCF is a fundamental element for SIP level integrity protection, as well as IPSec of course. It specifies what keys, algorithms etc that shall be used. According to Annex D the SPI shall be used for IPSec one in each direction. Currently it has not been specified what requirements or how the SA_ID should look like for SIP-level protection.

2.1. Visibility

For IPSec the SA is one way or simplex between the nodes. Furthermore the SA in IPSec is security protocol specific and hence there will be a SA for each protocol (AH or ESP). In general, the SPI identifies the SA from other SAs to the same IP address and using the same security protocol and it is 32-bit long. The SPI is sent in every packet in clear between the nodes and the destination can use this value to fetch the correct SA. SPIs must be unique in the destination address, and consequently the receiver must issue its own SPIs. The SPI is re-used once the SA expires but it is guaranteed that the mapping <SPI, destination address, security protocol identifier> is one to one. In multihoming, also the source address is used to identify the SA.

Following the IPSec model it can be concluded that the SA_ID shall be sent in clear in each SIP message in both directions between the UE and the P-CSCF.

The most promising SIP layer solution for confidentiality protection is currently S/MIME with CMS. If SIP message is encrypted using S/MIME, the key identifier will be transferred in the CMS packet in clear. CMS does not set any special requirements for the identifiers of previously distributed symmetric keys. For example, the identifiers used in HTTP Digest could be used.

2.2. Uniqueness

It is clear that the P-CSCF is aware of the IP-address of the UE after the UE has registered. Assuming e.g. a terminating INVITE towards the UE which passes through the P-CSCF there is information at SIP level such that the P-CSCF is

able to uniquely identify the UAS i.e. the UE. Hence this means that this piece of information shall have a one to one mapping to the SA_ID. Let us assume that this information is collected in the term Info. In theory Info could equal SA_ID but let us assume they are different but by knowing Info also the SA_ID is known. This is also valid for the IPSec alternative for IMS i.e. knowing Info at SIP level means that also the SPI is uniquely identified since no other information is available in the P-CSCF in this terminating scenario. Hence it follows that the SA_ID needs to be resolved at SIP level.

SIP layer protection will probably use HTTP Digest for integrity protection. The “integrity key” (i.e. the password) is identified by the client (i.e. the end-user) based on the information in the HTTP Digest challenge in *realm* parameter. The server or the proxy identifies the “integrity keys” based on the information in the HTTP Digest response in the *username* parameter. If HTTP Digest is used for integrity protection, the use of previous parameters for SA identification should be considered in order to guarantee the flexible development of the IMS security architecture. Furthermore, the solution for integrity protection should not prevent the use of HTTP Digest in the future; e.g. it must be possible to use HTTP Digest for authentication with application servers. In general, SA_ID needs to be unique but it is different for both directions in HTTP Digest.

IMS does not necessarily need unique SA_IDs for both directions. For example, IPSec utilises a security policy, which is consulted for both inbound and outbound processing of the IP-packets. A separate Security Policy database can be kept for inbound and outbound traffic. Hence it is possible to have different policies for incoming and outgoing IP-packets. For IMS this flexibility does not seem to add any value since the trust model adopted for IMS assumes that the UE or the ISIM trusts the HSS and the HSS or the HN trusts the P-CSCF. Hence once the UE has authenticated the challenge and the S-CSCF has authenticated the IMPI the UE and the P-CSCF will have a relation during the time the user is registered. Then there is no need to protect or to have different policies for inbound or outbound SIP-traffic between the UE and the P-CSCF.

2.3. Change of SAs

HTTP Digest does not identify different versions of integrity keys, and the concept of SA_ID is rather static. HTTP Digest is only using the keys that are valid “now”. This sets some additional requirements for key update. When an authenticated re-registration takes place there will be two SAs available: the old SA (i.e. SA1) and the new SA (i.e. SA2). During the authenticated re-registration SM6 will reach the UE, which includes the challenge and the UE can check the authenticity of the message. The UE shall now in SM7 use the new SA i.e. SA2 and send the RES towards the S-CSCF. Upon receiving this message the P-CSCF expects that the UE shall use SA2 if no time-out has been reached. In this scenario the old SA i.e. SA1 is deleted in the UE and the P-CSCF. If an expected message does not arrive before time-out the old SA i.e. SA1 is used. Hence the SA_ID can be re-used and the P-CSCF and the UE keeps track on the old and the new SA, which is a deterministic procedure.

2.4. Encoding

The encoding of the SA_ID needs to be defined. The information (or collection of information, i.e. Info) P-CSCF is using to route terminating SIP messages to the correct UE could be used as SA Identifier. The IMPI could for example be used as the SA_ID. This would ensure a static and unique SA_ID in the UE and the P-CSCF. Another possibility could be the use of the information in the Contact Header, which is available at SIP level. Not all of the potential possibilities are included here instead it is proposed that an LS is sent from SA3 to CN1 asking for guidance about what could encompass a suitable SA_ID at SIP level.

4 Conclusions

- It is proposed that SA3 adopts the following requirements on the SA_ID which is used in conjunction with HTTP Digest.

    1. The SA_ID shall be resolved at SIP level.

    2. The SA_ID shall be shared by the UE and the P-CSCF. It may be different or the same for both direction.

    3. The SA_ID value shall be unique in the UE and the P-CSCF in order to be able to distinguish between different UE’s in the P-CSCF.

4. The SA_ID shall be a static identifier associated with security data as security keys and algorithms, negotiated between the network and the UE. The UE and the P-CSCF shall keep track on the old and the new SA and apply them whenever no time-out is reached. If a time-out is reached the old SA shall be utilised.

5. The SA_ID identifying the SA with the security keys, that is currently used to protect a SIP signalling message, shall be included as part of the SIP message. The SA_ID has to be sent in clear between the UE and the P-CSCF.

6. The SA_ID has to be included in all SIP signalling messages that are protected between the UE and the P-CSCF.

- SA3 is encouraged to send an LS to CN1 in order to find out a suitable SA_ID at SIP level