3GPP TSG SA WG3 Security — S3#22bis IMS ad hoc **S3z020056**

Ft. Lauderdale, USA

8 April, 2002

Source: **Siemens**

Title: **Allocation of port numbers for protected and unprotected messages in SIP integrity using IPsec ESP**

Document for: **Discussion**

Agenda Item: **7.2**

Abstract

The P-CSCF distinguishes protected and unprotected messages by means of different ports. It is said in TS 33.203 v510 that the port for protected messages is fixed while the port for unprotected error messages is determined in the security mode set-up procedure. It is proposed in this contribution to do this allocation of ports the other way round. The reason is simplicity, not security. It is also suggested to discuss the best way to allocate the port number for protected messages with CN1.
A pseudo-CR implementing the proposed change is included in section 2 of this contribution.

---

1. Problem description and rationale for proposed change

In general, when SIP integrity using IPsec ESP is applied, the SIP messages received in unprotected or incorrectly protected IP packets are discarded by the IP layer and do not reach the SIP layer. However, certain unprotected messages need to be received by the P-CSCF to be forwarded to the S-CSCF. These are (cf. TS 33.203 v510, Annex D.1):

- initial REGISTER message;
- REGISTER message with network authentication failure indication;
- REGISTER message with synchronization failure indication.

Therefore, it is necessary to ensure that these messages are not discarded at the IP layer. This is done by sending them to a fixed port for unprotected messages at the P-CSCF, as specified in TS 33.203 v510, Annex D.

The UE finds the IP address and port of the P-CSCF in the P-CSCF discovery procedure. The UE sends initial REGISTER messages to this IP address and port, hence the IP layer at the P-CSCF must accept unprotected packets over this port. It now seems the most natural way to also send the two error messages (network authentication failure indication, synchronization failure indication) to this same port, and use a different fixed port for protected packets. This was not recognised in TS 33.203 v510.

The number of the fixed port for protected packets could be determined in two ways:
1) 3GPP fixes a system-wide port number for SIP messages protected with IPsec ESP.
This solution has the potential disadvantage that interaction with the IETF may be required for the allocation of this port number. (This may need further discussion.) The solution could, however, simplify implementation.
2) the port number for protected packets is fixed by the P-CSCF and communicated to the UE in the security mode set-up procedure by using the *info* field of message SM6. This has the advantage that interaction with

the IETF is not needed. Note also that every P-CSCF could use a port number different from that of other P-CSCFs. The disadvantage is that the *info* field needs to be used.

It is proposed that the second alternative is chosen as the timeliness of the specification is the overriding concern, and the disadvantage seems to be comparatively small. However, this is not a security matter and should also be discussed with CN1.

2. Pseudo CR to TS 33.203 v510 to implement the changes proposed in section 1

This contribution includes only a pseudo-CR because formal CRs should be based on a new version of TS 33.203 without annexes, reflecting the decision on the SIP integrity mechanism.

It is proposed that the ad hoc meeting endorses this pseudo-CR.

Annex D (informative): Set-up procedures for IPSec based solution

[Editors Note: If the IPSec solution is finally chosen the chapters below shall be moved into the main body of this TS in the corresponding sections.]

This section is based on section 7 and provides additional specification for the support of IPsec ESP.

D.1 Security association parameters

The SA parameters, identifiers and attributes that shall be negotiated between UE and P-CSCF, are

- ESP transform identifier
- Authentication (integrity) algorithm
- SPI

Further parameters:

- Life type: the life type is always seconds
- SA duration: the SA duration has a fixed length of 2^{32}-1.
- Key length: the length of encryption and authentication (integrity) keys is 128 bits.

Selectors:

The security associations (SA) have to be bound to specific parameters (selectors) of the SIP flows between UE and P-CSCF, i.e. IP addresses and ports. Both sides have to use the same policy here, but since the required selectors will be known from the SIP messages, there is no need to negotiate them, with the exception of a fixed port for protected SIP messages at the P-CSCF which shall be established in the security mode set-up procedure. However, it is critical to keep the source IP address and source port number, the selector pair unique in P-CSCF. The P-CSCF must reject any REGISTER message sent from a valid SA's selector pair corresponding to a different IMPI than the one that is bound to this selector pair. ~~The only parameter that shall be negotiated, is a fixed port for specific unprotected SIP messages at the P-CSCF~~:

1. For ~~the~~ inbound ~~SA~~ protected messages at the P-CSCF (outbound for the UE) the P-CSCF shall use a fixed port. This fixed port shall be established in the security mode set-up procedure (cf. D.2). ~~This may be port 5060 as the standard SIP port, or any other fixed port where the server accepts SIP messages from the UE.~~ In addition, ~~another~~ a different port for specific unprotected SIP messages from the UE to the server is fixed. This shall be the port at the P-CSCF to which the UE sends initial REGISTER messages.
   For the outbound SA at the P-CSCF (inbound for the UE) ANY port number shall be allowed at the P-CSCF.

2. On the UE side, the SIP UAs shall use the same port for both sending and receiving SIP signalling to the P-CSCF.

3. If there are multiple SIP UAs belonging to different ISIMs in one UE they shall use different SAs and bind them to different ports on the UE side.

4. The UE may send only the following messages to the fixed port for unprotected messages:

   - initial REGISTER message;

   - REGISTER message with network authentication failure indication;

   - REGISTER message with synchronization failure indication.

   All other messages incoming on this port must be discarded by the SIP application on the P-CSCF.

[Editors' note:It is ffs whether case 3 can actually occur.]

For each incoming message the SIP application must verify that the correct inbound SA associated with the public ID (IMPU) given in the SIP message has been used. This shall be done by verifying that the correct source IP address and source port bound to the public ID (IMPU) of the SIP message have been used for sending the message.

D.2 Security mode setup for IPsec ESP

This section describes how the security mode setup described in chapter 7 shall be used for negotiating ESP as protection mechanism and setting up the parameters required by ESP.

D.2.1 General procedures specific to the ESP protection mechanism

The integrity and encryption mechanisms both have the value "esp". The fields SA_ID_U and SA_ID_P carry the SPI values to be exchanged, to identify the ESP SAs.

The P-CSCF shall ~~use an unprotected port to be able to receive specific unprotected~~fix a port for receiving protected messages. This ~~unprotected~~ port ~~has to be~~shall be communicated to the UE, by using the *info* field of message SM6. This port may be different for different P-CSCFs.~~This unprotected port is required, when an IPsec SA is already in place at the P-CSCF, but the UE due to any reason is not able to use this SA. In this case, the UE shall send error messages or a new REGISTER message in the clear to the P-CSCF port received in the *info* field within SM6. Otherwise at the P-CSCF side, ESP would simply drop all IP packets from the UE that fail the integrity check.~~

~~*The error messages that shall be sent in the clear from the UE to the P-CSCF are these for network authentication failures (sections 7.3.1.2) and synchronization failures (section 7.3.1.*~~