3GPP TSG SA WG3 Security — S3#24   **S3-020376**

9 - 12 July, 2002

Helsinki, Finland

Source:	**Nokia**
Title:	**Protect port number to be assigned by UE in re-registration**
Agenda item:	**7.1, IMS**
Document for:	**DISCUSSION/APPROVAL**

CHANGE REQUEST

⌘	**33.203** CR **CRNum** ⌘**rev** **-** ⌘	Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐   ME **X** Radio Access Network ☐   Core Network **X**

Title:	⌘	Protect port number to be assigned by UE in re-registration
Source:	⌘	Nokia
Work item code:	⌘	IMS-ASEC ***Date:*** ⌘ 4 July 2002
Category:	⌘	**F** ***Release:*** ⌘ Rel-5

Use one of the following categories:	*Use one of the following releases:*
F *(correction)*	*2* *(GSM Phase 2)*
A *(corresponds to a correction in an earlier release)*	*R96* *(Release 1996)*
B *(addition of feature),*	*R97* *(Release 1997)*
C *(functional modification of feature)*	*R98* *(Release 1998)*
D *(editorial modification)*	*R99* *(Release 1999)*
Detailed explanations of the above categories can	*Rel-4* *(Release 4)*
be found in 3GPP TR 21.900.	*Rel-5* *(Release 5)*
	Rel-6 *(Release 6)*

Reason for change:	⌘	The current specification specifies the procedure when UE is challenged and new SA is to be established, but not UE's behavior if UE is not be challenged and no new SA is going to be established.
Summary of change:	⌘	To clarify UE's behavior during re-registraiton that new port number must be assigned by UE and communicated to the P-CSCF, preparing a new SA is to be established.
Consequences if not approved:	⌘	Implementation may assume no port number to be assigned if no new SA is to be established.

Clauses affected:	⌘	

		Y	
Other specs affected:	⌘	**X**	TS 24.228, 24.229 ⌘

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

   3)   With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

7.1   Security association parameters

The security association set-up procedure is necessary in order to decide what security services to apply and when the security services start. In the IMS authentication of users is performed during registration as specified in clause 6.1. Subsequent signaling communications in this session will be integrity protected based on the keys derived during the authentication process.

1.1 7.1   Security association parameters

For protecting IMS signaling between the UE and the P-CSCF it is necessary to agree on shared keys that are provided by IMS AKA, and a set of parameters specific to a protection method. The security mode setup (cf. clause 7.2) is used to negotiate the SA parameters required for IPsec ESP with authentication, but without confidentiality.
The SA parameters that shall be negotiated between UE and P-CSCF in the security mode set-up procedure, are:
- **Integrity algorithm**

NOTE 1: What is called "authentication algorithm" in [13] is called "integrity algorithm" in this specification in order to be in line with the terminology used in other 3GPP specifications and, in particular, to avoid confusion with the authentication algorithms used in the AKA protocol.

The integrity algorithm is either HMAC-MD5-96 [15] or HMAC-SHA-1-96 [16].

NOTE 2: This, in particular, excludes the use of the NULL integrity algorithm.

Both integrity algorithms shall be supported by both, the UE and the P-CSCF as mandated by [13]. In the unlikely event that one of the integrity algorithm is compromised during the lifetime of this specification, this algorithm shall no longer be supported.

NOTE 3: If only one of the two integrity algorithms is compromised then it suffices for the IMS to remain secure that the algorithm is no longer supported by any P-CSCF. The security mode set-up procedure (cf. clause 7.2) will then ensure that the other integrity algorithm is selected.

- **SPI (Security Parameter Index)**

The SPI is allocated locally for inbound SAs. The triple (SPI, destination IP address, security protocol) uniquely identifies an SA at the IP layer. The most significant bit of any SPI allocated by the P-CSCF shall be "0" and the most significant bit of any SPI allocated by the UE shall be "1".

NOTE 4:   This allocation of SPIs ensures that protected messages in the uplink always differ from protected messages in the downlink in, at least, the SPI field. This thwarts reflection attacks. When several applications use IPsec on the same physical interface the SIP application should be allocated a separate range of SPIs.

The following SA parameters are not negotiated:
-   Life type: the life type is always seconds;

-   SA duration: the SA duration has a fixed length of $2^{32}-1$;

NOTE 5:   The SA duration is a network layer concept. From a practical point of view, the value chosen for "SA duration" does not impose any limit on the lifetime of an SA at the network layer. The SA lifetime is controlled by the SIP application as specified in clause 7.4.

-   Mode: transport mode;

-   Key length: the length of the integrity key IK_{ESP} depends on the integrity algorithm. It is 128 bits for HMAC-MD5-96 and 160 bits for HMAC-SHA-1-96.

Selectors:
The security associations (SA) have to be bound to specific parameters (selectors) of the SIP flows between UE and P-CSCF, i.e. source and destination IP addresses, transport protocol, and source and destination ports.
-   IP addresses are bound to a pair of SAs, as in clause 6.3, as follows:

    -   inbound SA at the P-CSCF:
        The source and destination IP addresses associated with the SA are identical to those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.

    -   outbound SA at the P-CSCF:
        the source IP address bound to the outbound SA equals the destination IP address bound to the inbound SA;
        the destination IP address bound to the outbound SA equals the source IP address bound to the inbound SA.

NOTE 6:   This implies that the source and destination IP addresses in the header of the IP packet in which the protected SIP REGISTER message was received by the P-CSCF need to be the same as those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.

-   The transport protocol is either TCP or UDP.

-   Ports:

    1.   The P-CSCF receives messages protected with ESP from any UE on one fixed port (the"protected port") different from the standard SIP port 5060. The number of the protected port is communicated to the UE during the security mode set-up procedure, cf. clause 7.2. No unprotected messages shall be sent to or received on this port. From a security point of view, the P-CSCF may receive unprotected messages from any UE on any port which is different from the protected port.

NOTE 7:   The protected port is fixed for a particular P-CSCF, but may be different for different P-CSCFs.

    2.   For protected or unprotected outbound messages from the P-CSCF (inbound for the UE) any port number may be used at the P-CSCF from a security point of view.

    3.   For each security association, the UE assigns a port to send or receive protected messages to and from the P-CSCF ("protected port"). No unprotected messages shall be sent to or received on this port. The UE may use different protected port numbers for TCP and UDP. The numbers of these ports are communicated to the P-CSCF during the security mode set-up procedure, cf. clause 7.2. When the UE sends a re-REGISTER request, it shall always pick up a new port number and send it to the network. If the UE is not challenged by the network, the port number shall be obsolete. Annex H of this specification gives detail how the port number is populated in SIP message. From a security point of view, the UE may send or receive unprotected messages to or from the P-CSCF on any ports which are not protected ports.

Editor's note: The condition that the UE sends and receives protected messages on the same port is not necessary from a security point of view. These ports could be made different, at the expense of one more parameter to be negotiated in the security mode set-up procedure, but they have to be fixed in the registration procedure.

4. The P-CSCF is allowed to receive only REGISTER messages on unprotected ports. All other messages not arriving on the protected port shall be discarded by the P-CSCF.

5. The UE is allowed to receive only the following messages on an unprotected port:

   - responses to unprotected REGISTER messages;

   - error messages.

   All other messages not arriving on a protected port shall be discarded by the UE.