3GPP TSG SA WG3 Security — S3#23 **S3-020270**
14 - 17 May 2002
Victoria, Canada

CR-Form-v4

CHANGE REQUEST

⌘ **33.203** **CR** ⌘ ev **-** ⌘ Current version: **5.1.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	IP address as SA selector
Source:	⌘	Nokia
Work item code:	⌘	***Date:*** ⌘
Category:	⌘	**C**

Release: ⌘ REL-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	Adding Security negotiation into SA setup procedure.
Summary of change:	⌘	**Adding Security negotiation for IPsec into SA setup procedure.**
Consequences if not approved:	⌘	The SA establishment is rely on the missing function. Without Security negotiation, it may not be able to establish~~setup~~ IPsec SA.

Clauses affected:	⌘	
Other specs affected:	⌘	**X** 24.228 **X** 24.229
Other comments:	⌘	

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[2] 3GPP TS 22.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Requirements for the IP Multimedia Core Network".

[3] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem".

[4] 3GPP TS 21.133: "3rd Generation Partnership Project; T Technical Specification Group Services and System Aspects; Security Threats and Requirements ".

[5] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

[6] IETF RFC 3261 "SIP: Session Initiation Protocol".

[7] 3GPP TS 21.905: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Vocabulary for 3GPP specifications".

[8] 3GPP TS 24.229: "3rd Generation Partnership Project: Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on SIP and SDP".

[9] 3GPP TS 23.002: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, Network Architecture".

[10] 3GPP TS 23.060: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, General Packet Radio Service (GPRS); Service Description".

[11] 3GPP TS 24.228: "3rd Generation Partnership Project: Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP".

[12] IETF RFC 2617 (1999) "HTTP Authentication: Basic and Digest Access Authentication".

[13] IETF RFC 2407 (1998) “The Internet IP Security Domain of Interpretation for ISAKMP”

7 Security association set-up procedure

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

7.1 Security association parameters

For protecting IMS signaling between the UE and the P-CSCF it is necessary to agree on shared keys provided by IMS AKA, on certain protection methods (e.g. an integrity protection method) and a set of parameters specific to a protection method, e.g. the cryptographic algorithm to be used. The parameters negotiated are typically part of the security association to be used for a protection method.

The security mode setup shall support the negotiation of different protection mechanisms. It shall be able to negotiate or exchange the SA parameters required for these different protection mechanisms. Although the supported protection mechanisms could be quite different, there is a common set of parameters that ~~have to~~can be negotiated for each of

them. . ~~This~~ The set of attributes, algorithms and parameters for establishing IPsec SA~~includes~~are grouped together and a method how to achieve this is given in Annex D.1.~~:~~

~~- Authentication (integrity) algorithm, and optionally encryption algorithm;~~

~~- SA_ID that is used to uniquely identify the SA at the receiving side;~~

~~- Key length: the length of encryption and authentication (integrity) keys is 128 bits.~~

~~The UE and P-CSCF both have static lists of security mechanisms and parameters they support. The lists do not and cannot change based on input from the other side. There may, however, be several lists for each node.~~

Parameters specifically related to certain protection methods are kept in the annexes describing the protection methods.

The SA between the UE and the P-CSCF will have a limited lifetime. The lifetime timer shall be the same as the registration timer, which is defined per contact address. When the UE registers the registration timer will be negotiated between the UE, the P-CSCF and the S-CSCF. The S-CSCF will be able to accept, decrease or increase the proposed expiration time from the UE and the final value is sent in the response to the UE. The expiry time in the UE will be shorter than the expiry time in the S-CSCF, such that the UE is able to re-register. For each new successful authentication the SA shall be updated. The S-CSCF shall align the expiration of subsequent registrations with any existing registration timer. The SA is deleted if the registration timers expire~~s~~ in the P-CSCF or in the S-CSCF.

[Editors Note: The support of different mechanisms is FFS.]

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 to be predefined

To establish IPsec SA under same policy in the UE and P-CSCF, ~~The~~ an essential range of SA parameters, identifiers and attributes ~~that shall be negotiated between UE and P-CSCF~~, are grouped together under SA suite definition. SA Suite is predefined for flexible SA establishment and shall be proposed during the security negotiation procedure. It contains information:

- IPsec Situation Definition
- ESP transform identifier
- ~~-~~Authentication (integrity) algorithm
- SA Life type: measured by time or by data amount
- SA duration: the SA duration has a fixed length.
- Key length: the length of encryption and authentication (integrity) keys.

There are two suites defined for Release 5 usage. The naming scheme is align with [13].

Suite 1:

a) Situation definition

Situation=SIT_INTEGRITY

b) IPsec protocol

Protocol id=PROTO_IPSEC_ESP

ESP Transform Identifiers= ESP_NULL

c) SA attributes

SA Life Type=seconds

SA Life Duration=2^{32}-1

Authentication Algorithm= HMAC_MD5

Encapsulation Mode=Transport

key lengths=128 bits

Suite 2:

a) Situation definition

Situation=SIT_INTEGRITY

b) IPsec protocol

Protocol id=PROTO_IPSEC_ESP

ESP Transform Identifiers= ESP_NULL

c) SA attributes

SA Life Type=seconds

SA Life Duration=2^{32}-1

Authentication Algorithm= HMAC_SHA

Encapsulation Mode=Transport

key lengths=128 bits

Note: The HMAC-SHA-1-96 requires 160 bits key length, which shall be converted from 128 bits session key.

The other ephemeral parameters associated with each particular SA connection, such as SA_ID and port numbers shall be negotiated separately during security negotiation procedure.

~~- 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. 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 at the P-CSCF (outbound for the UE) the P-CSCF shall use a fixed port. 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 port for specific unprotected SIP messages from the UE to the server is fixed.
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.~~