

Technical Specification Group Services and System Aspects
Meeting #19, Birmingham, UK, 17-20 March 2003

TSGS#19(03)0103

Source: SA WG3
Title: 1 CR to 33.203: Add protected port into Via header (Rel-5)
Document for: Approval
Agenda Item: 7.3.3

The following CR was approved by SA WG3 meeting #27 and is hereby presented to TSG SA#19 for approval.

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-030103	33.203	038	-	Rel-5	Add protected port into Via header	F	5.4.0	IMS-ASEC	S3-030158

CHANGE REQUEST

⌘ **33.203 CR 038** ⌘ rev - ⌘ Current version: **5.4.0** ⌘

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 Radio Access Network Core Network

Title:	⌘ Add protected port into Via header		
Source:	⌘ SA WG3		
Work item code:	⌘ IMS-ASEC	Date:	⌘ 26/02/2003
Category:	⌘ F	Release:	⌘ Rel-5
	Use <u>one</u> 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 <u>one</u> 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) Rel-6 (Release 6)

Reason for change:	⌘ UE must insert the protected port number for the P-CSCF to respond according to SIP RFC3261 . Furthermore, this has to be mandatory in IMS where different SAs are applied to the same UE-P-CSCF using different ports, since the recipient must pick up the proper port i.e. proper SA when responding.
Summary of change:	⌘ Add protected port into Via header. The contact address is updated to the 'address pair' of the UE during the registration procedure.
Consequences if not approved:	⌘ If no port is specified in the requests, the server would send a response to the default port for that transport that is specified as unprotected port in this specification. In the SA handing scenario, the response may be sent using the old SA, which should not be used anymore.

Clauses affected:	⌘ 7.1						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
Other comments:	⌘						

7.1 Security association parameters

***** <text skipped> *****

- 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. [For every protected request towards UE, the P-CSCF shall insert the protected port into Via header.](#) No unprotected messages shall be sent ~~to~~-from 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: 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 local 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 shall use a single protected port number for both TCP and UDP connections. The port number is 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 the protected ports.
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. [For every protected request, the UE shall insert the protected port of the corresponding SA into Via header.](#) 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.

The following rules apply:

1. For each SA which has been established and has not expired, the SIP application at the P-CSCF stores at least the following data: (UE_IP_address, UE_protected_port, SPI, IMPI, IMPU1, ... , IMPUn, lifetime) in an "SA_table".

NOTE: The SPI is only required when initiating and deleting SAs in the P-CSCF. The SPI is not exchanged between IPsec and the SIP layer for incoming or outgoing SIP messages.

2. The SIP application at the P-CSCF shall check upon receipt of a protected REGISTER message that the [pair](#) (source IP address, [source port](#)) in the packet headers coincides with the UE's [address pair](#) (IP address, [source port](#)) inserted in the Via header of the protected REGISTER message. If the Via header does not explicitly contain the UE's ~~IP~~-address [pair](#), but rather a symbolic name then the P-CSCF shall first resolve the symbolic name by suitable means to obtain an ~~IP~~-address [pair](#).