3GPP TSG SA WG3 Security — SA3#37 **S3-050048**
February 21-25, 2005
Sophia Antipolis, France

Source: **BT Group**
Contact: **Colin Blanchard colin.blanchard@bt.com,**

Title: **Security extensions for IP Multimedia Sub-system - Issues identified and contributions presented at TISPAN**

Document for: **Discussion and decision**
Agenda Item: **6.1**

1. Introduction

This contribution is intended to provide 3GPP SA3 members with a summary of issues that have been identified with the 3GPP IMS 3GPP TS33.203 security specification to provide security for IMS use in fixed network as is being defined by ETSI TISPAN NGN and future 3G scenarios as defined by 3GPP. It gives a brief description of the issues identified so far, and where appropriate, links to contributions identifying the issue and the analysis of potential solutions on the 3GPP or ETSI web sites. The contribution is intended to compliment the 3GPP SA3 R7 work item on “Security extensions for IP Multimedia Sub-system” and to be used in agreeing the scope of this new work item. Please note that an ETSI account is required to download contributions from the ETSI web site.

2. Issues identified and contributions presented at TISPAN

1	**NA (P) T traversal in the customer environment** Three solutions have been proposed: 1. **IPsec/IKEv2:** Need to refresh NA(P)T binding frequently because the signalling is always encapsulated to UDP 2. **IPsec/SIP Digest AKA**: as specified by 3GPP in TS33.203 INA(P)T bindings and UDP encapsulation. Some specification is required for NA(P)T traversal which has already been proposed by BT in a previous contribution ([S3-040720]). 3. **TLS**: Removes the NAT traversal problems as works at the application layer TISPAN is not yet ready to make any decision related to preferred access security solution, and further work is required. The following contributions have been presented: 05TD161 “Feasibility of IPsec and TLS to provide SIP signalling security on the access in NGN/IMS” (Ericsson and Alcatel) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD161%20IMS_security_comparison.doc S3-040720 Proposal for an informative Annex to the 3GPP TS 33.203 on support of end user devices behind a NA(P)T firewall and protection of RTP media flows (BT Group) http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_35_Malta/Docs/ZIP/S3-040720.zip

2	**Soft ISIM** Concern that not all end user devices will be able to support a physical UICC. The following contributions have been presented: Feasibility study on (Universal) Subscriber Interface Module (U)SIM security reuse by peripheral devices on local interfaces (3GPP SA3) http://www.3gpp.org/ftp/Specs/html-info/33817.htm Use of ISIM and line and personal identifiers in NGN (Ericsson) http://portal.etsi.org/docbox/tispan/tispan/50-20041102-Sophia_4bis/04bTD109r1%20Use_of_USIL_in_NGN.doc 3GPP GAA usage in split terminal scenario (Nokia) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD175%203GPP_GAA_with_split_terminal.zip
3	**Multiple devices behind the end customer own Residential Gateway** Do we terminate the IPsec or TLS at the gateway resulting in one or maintain separate sessions to terminate in each device
4	**End customer is allowed to use a Residential Gateway in someone else home with their own “mobile” on the understanding that the homeowner will not be billed for the “call” and that the privacy and accuracy of their subsequent bill will be maintained.** This scenario suggests that security should be maintained through to the end user device.
5	**Use of WLAN “IP access security from TS33.234 as an equivalent of GPRS authentication an ciphering**. It has been suggested that all signaling and media could be tunneled through an independent IPSec tunnel terminating at a point before the P-CSCF. The following contributions have been presented: 3GPP/WLAN Interworking Architecture as Paradigm for NGN Access Independence. (Siemens) http://portal.etsi.org/docbox/tispan/tispan/50-20040913-Sophia_P4/04TD137%20Generic_access_in_NGN.zip International Roaming Access Protocols (IRAP) Program (Intel) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD171r2%20Roaming_Access_Testing_Considerations.zip

6	**Use of GAA/GBA** The load on the HSS to support the wider range of security features (particularly if media streams are protected) has been raised. The use of GAA/GBA as an intermediate stage has been suggested. The following contributions have been presented: 04bTD139 “Proposal for the use of standard key derivation function for media stream access security” (BT Group) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20041102-Sophia_4bis/04bTD139%20Standard_Key_Derivation.doc 05TD102 “Application layer secret key negotiations between the UE and the AS for IMS” (Huawei Technologies, Co., Ltd., China) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD102%20Application_layer_secret_key_negotiations_between_UE_%20and_AS_for_IMS.doc 3GPP GAA usage in split terminal scenario (Nokia) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD175%203GPP_GAA_with_split_terminal.zip
7	**Media protection** It has not been agreed that this is a requirement, but 5 contributions have been presented: 04bTD139 “Proposal for the use of standard key derivation function for media stream access security” (BT Group) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20041102-Sophia_4bis/04bTD139%20Standard_Key_Derivation.doc 05TD161 “Feasibility of IPsec and TLS to provide SIP signalling security on the access in NGN/IMS” (Ericsson and Alcatel) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD161%20IMS_security_comparison.doc 05TD101 “IMS application layer security requirements” (Huawei Technologies, Co., Ltd., China) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD101%20IMS_application_layer_security_requirements.doc 05TD102 “Application layer secret key negotiations between the UE and the AS for IMS” (Huawei Technologies, Co., Ltd., China) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD102%20Application_layer_secret_key_negotiations_between_UE_%20and_AS_for_IMS.doc 05TD103r1 “Application layer secret key negotiations between the UE and the AS for IMS” (Huawei Technologies, Co., Ltd., China) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD103r1%20An_End2End_Security_Solution_for_%20Media_%20Streams_Protection_within_IMS_framework.doc
8	**Unprotected messages** Some concern has been expressed that Initial registration message, and some error messages are always sent unprotected 05TD161 “Feasibility of IPsec and TLS to provide SIP signalling security on the access in NGN/IMS” (Ericsson and Alcatel} http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD161%20IMS_security_comparison.doc

9	**SIP transport using SCTP** The 3GPP IMS solution was designed to be compatible with SIP transported over UDP and for a possible extension to media, which is transported using UDP. However comments have been made that the constraints that dictate the use UDP for signaling transport do not apply in the fixed network and SCTP offers a number of advantages, but it is not clear if these advantages are relevant in the TISPAN NGN context. One claimed advantage is that it can be secure with both IPsec and TLS whereas UDP cannot be secure with TLS.
10	**Use of IKEV2** It has been noted by TISPAN WLAN IP Access uses IKEV2 in conjunction with AKA and address NAT but IMS security does not. Use of IKE is seen as one the solutions for NA (P) T traversal in the customer environment. The following contributions have been presented: 05TD161 “Feasibility of IPsec and TLS to provide SIP signalling security on the access in NGN/IMS” (Ericsson and Alcatel) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD161%20IMS_security_comparison.doc
11	**Use of TLS** Since SA3 took its decision to base IMS on IPSec in March 2002 various TLS has been proposed. The most significant being shared key TLS. Some TISPAN members are asking for the use of TLS to be reconsidered 05TD161 “Feasibility of IPsec and TLS to provide SIP signalling security on the access in NGN/IMS” (Ericsson and Alcatel) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD161%20IMS_security_comparison.doc
12	**Call set up performance** The impact will need to be understood for all mechanisms and combination of mechanisms. While this is obviously a concern for mobile networks as well, fixed network operators seem to have a greater concern over this.
13	**Multiplicity of IPSec/TCP connections at a node in the network** There is a concern that terminating large numbers of individual IPsec or TLS sessions within what could be a single logical node will create performance issues and there are various views on whether IPSec or TLS creates less of an issue. 05TD161 “Feasibility of IPsec and TLS to provide SIP signalling security on the access in NGN/IMS” (Ericsson and Alcatel) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD161%20IMS_security_comparison.doc
14	**Ease of deployment / management of authentication keying material** There appears to be a consensus that solutions that avoid the need for distribution of public key certificates to end users and the deployment of a global PKI are to be preferred. Hence SA3 use of 3GPP AKA and IPSec for IMS, but proponents of a TLS based solution suggest that shared key TLS or solution based on passwords at the user end would also meet this need. 05TD161 “Feasibility of IPsec and TLS to provide SIP signalling security on the access in NGN/IMS” (Ericsson and Alcatel) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD161%20IMS_security_comparison.doc

15	**Resilience and fallback options** Support for emergency calls, for example, when IMS and any associated access security is not available.
16	**Feasibility of the implementation in the CPE** There is a concern that IPSec and TLS implementations may not be available for the much wider range of CPE and even if there are, they may not be assessable by the IMS application (for example many TLS implementations are associated with Web browsers and IPsec with IKE for key management 3GPP TS33.203 does not use. The development of SA3's "security for early IMS" has also had an impact on TISPAN confidence in SA3 current solution. 05TD161 "Feasibility of IPsec and TLS to provide SIP signalling security on the access in NGN/IMS" (Ericsson and Alcatel) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD161%20IMS_security_comparison.doc
17	**Support for roaming** For IMS, 3GPP pass security information (quintuplets) between home and visited networks using MAP SS7 via a GRX type network. For WLAN interworking and UMA security information is passed between proxy radius servers using other protocols e.g. EAP via other Roaming network providers e.g. Wireless Broadband Alliance (WBA) networks. http://www.wirelessbroadbandalliance.com/ TISPAN require the ability to support both options. The following contributions have been presented: 3GPP/WLAN Interworking Architecture as Paradigm for NGN Access Independence (Siemens) http://portal.etsi.org/docbox/tispan/tispan/50-20040913-Sophia_P4/04TD137%20Generic_access_in_NGN.zip International Roaming Access Protocols (IRAP) Program (Intel) http://portal.etsi.org/docbox/TISPAN/TISPAN/50-20050117-Sophia_P5/05TD171r2%20Roaming_Access_Testing_Considerations.zip
18	**Definition of identifies for nodes** Many identities used in 3GPP specifications refer to 3GPP.org in the definition it is not clear if this is just stating a format or the node has to be part of the 3GPP.org domain.

3 Conclusions

When developing security extensions for IP Multimedia Sub-system, SA3 need to take the above issues into account even though not all issues may be require a change to TS33.203, when IMS is operated over the same operators GPRS network.