3GPP TSG SA WG3 Security — S3#17 **S3-010033**

27 February - 02 March, 2001

Gothenburg, Sweden

TSG-SA WG 1 (Services) meeting #11 **TSG S1 (01) 0261**
Capetown, SA 6th to 9th February 2001 **Agenda Item:**

Source: **TSG-SA WG1**

To: **TSG-SA WG3**

Title: **Requirement for End-to-End Encryption of IP Multimedia Subsystem Controlled Voice over IP Calls**

Contact: DeWayne Sennett, AWS.

S1 has discussed the document S1(01)0185 and this is attached to this Liaison Statement. The document proposes the introduction of end to end encryption for voice calls supported by the IP Multimedia Subsystem.

S1 believes these matters should be dealt with by S3.

If S3 confirm that a suitable mechanism can be standardised within R5 then S1 have agreed to add the requirements for this to TS22.228 – Service requirements for the IP Multimedia Core Network Subsystem (Stage 1) at S1#11.

TSG-SA WG 1 (Services) meeting #11 TSG S1 (01) 0185
Capetown, SA 6th to 9th February 2001 **Agenda Item: 7.1**

Source: **AT&T Wireless Services**

Title: **Requirement for End-to-End Encryption of IP Multimedia Subsystem Controlled Voice over IP Calls**

Agenda item: **7.1**

Document for: **Discussion and Acceptance**

AT&T Wireless Services proposes that the capability for the end-to-end encryption of the subscriber's voice calls over IP that are controlled by the IP Multimedia Subsystem should be supported in Release 5. The end points for the encryption of these voice over IP calls could either be the IMS capable mobile devices, the radio air interface, and/or the gateways that provide the interconnectivity with other networks (e.g., PSTN).

AT&T Wireless Services believes that this end-to-end encryption is required for the following reasons:

1. Increased Security for Subscriber Voice Calls

Encryption could be provided on either an end-to-end basis or on a link-by-link basis. Encryption on an end-to-end basis provides a greater level of security than encryption on a link-by-link basis since the voice call can be subject to eavesdropping at the end of each link.

2. Not Dependent on Encryption Capabilities of Serving Network

Since encryption is provided on an end-to-end basis, no capabilities are required in the serving network to provide the encryption.

3. Improved Performance & Reduced Delay Times

No intermediate decryption and re-encryption is required. This will perform the performance of the network elements and will reduce the delay times associated with this voice call.

Key Management and Lawful Surveillance

The IP Multimedia Subsystem would be responsible for the key management procedures required to support the end-to-end encryption of voice calls controlled by the IP Multimedia Subsystem.

Consequently, the IP Multimedia Subsystem would have the key information required to potentially support lawful surveillance requirements for these types of calls.

Recommendation

It is proposed that S1 accept the principle of the proposed requirement for the capability for the end-to-end encryption of the subscriber's voice calls over IP that are controlled by the IP Multimedia Subsystem should be supported in Release 5. If this proposal is accepted, CRs will be created for the specific changes to 22.228.

End-to-end encryption for other types of multimedia services is for future study.

TSG-SA WG 1 (Services) meeting #11 **TSG S1 (01) 0185**
Capetown, SA 6th to 9th February 2001 **Agenda Item: 7.1**

Source:	**AT&T Wireless Services**
Title:	**Requirement for End-to-End Encryption of IP Multimedia Subsystem Controlled Voice over IP Calls**
Agenda item:	**7.1**
Document for:	**Discussion and Acceptance**

AT&T Wireless Services proposes that the capability for the end-to-end encryption of the subscriber's voice calls over IP that are controlled by the IP Multimedia Subsystem should be supported in Release 5. The end points for the encryption of these voice over IP calls could either be the IMS capable mobile devices, the radio air interface, and/or the gateways that provide the interconnectivity with other networks (e.g., PSTN).

AT&T Wireless Services believes that this end-to-end encryption is required for the following reasons:

1. Increased Security for Subscriber Voice Calls

Encryption could be provided on either an end-to-end basis or on a link-by-link basis. Encryption on an end-to-end basis provides a greater level of security than encryption on a link-by-link basis since the voice call can be subject to eavesdropping at the end of each link.

2. Not Dependent on Encryption Capabilities of Serving Network

Since encryption is provided on an end-to-end basis, no capabilities are required in the serving network to provide the encryption.

3. Improved Performance & Reduced Delay Times

No intermediate decryption and re-encryption is required. This will perform the performance of the network elements and will reduce the delay times associated with this voice call.

Key Management and Lawful Surveillance

The IP Multimedia Subsystem would be responsible for the key management procedures required to support the end-to-end encryption of voice calls controlled by the IP Multimedia Subsystem.

Consequently, the IP Multimedia Subsystem would have the key information required to potentially support lawful surveillance requirements for these types of calls.

Recommendation

It is proposed that S1 accept the principle of the proposed requirement for the capability for the end-to-end encryption of the subscriber's voice calls over IP that are controlled by the IP Multimedia Subsystem should be supported in Release 5. If this proposal is accepted, CRs will be created for the specific changes to 22.228.

End-to-end encryption for other types of multimedia services is for future study.