3GPP TSG SA WG3 Security — S3#32 **S3-040113**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda Item:	3GPP-WLAN UE split
Source:	Nokia
Title:	Response on S3-040049
Document for:	Discussion/Decision

This is a response contribution to previously submitted Tdoc S3-040049:"A man-in-the-middle attack using Bluetooth in a WLAN interworking environnment", by Eric Gauthier, Orange.

Clarifications to misunderstanding of BT

The Tdoc S3-040049 raised a relevant issue. It is true that in some cases only the master contributes to the randomness of the encryption key. However, it is not the case in the scenario described in the contribution S3-040049, since it is based on wrong assumptions about how authentication works and how the encryption key is derived in Bluetooth.
Below find the correct facts, see Bluetooth Specification v1.2 Vol 2, Core System Package, Part H, Section 5, page 774:

(1) The authentication verifier is not required to be the master. The application indicates which device has to be authenticated. Some applications only require a one-way authentication. However, some peer-to-peer communications should use a mutual authentication in which each device is subsequently the challenger (verifier) in two authentication procedures. The Link Manager shall process authentication preferences from the application to determine in which direction(s) the authentication(s) takes place.

(2) The ACO (Authentication Ciphering Offset) value from the last successful authentication is retained.

In particular, it follows from (2) that the sentence "It appears however that Bluetooth does not use RAND2 in the computation of ACO" (section 3 of S3-040049) is incorrect. This misunderstanding may have been caused by the fact that in broadcast encryption, the ACO value for encryption key derivation is replaced by a value derived from the Bluetooth address of the master. But in point-to-point encryption the ACO that is used for encryption key derivation does not depend on the roles of the devices.

Moreover, from the fact (1) it follows that the application can decide in which order the authentication is performed.

Another misunderstanding is that devices can switch roles independently of any control by the application. It can be required in this specific application that the laptop is the master device, if so wanted.

Conclusion

We conclude that there are several ways how the application is able to ensure that both the Laptop and the Phone contribute to the randomness of the Bluetooth encryption key, so that it cannot be replayed by any of the parties. In particular:

- The Bluetooth specifications allow the application to have control on the modes of authentication and key generation that are used;
- To utilize any existing suitable modes in Bluetooth specifications that enable both parties to contribute to the randomness of the encryption key.