3GPP TSG WG SA3 –Security SA3#16 **S3-000769**
28-30 November, 2000
Sophia Antipolis, France

Title: **Security aspects of UE conformance testing**

Source: **TSG SA WG3**

To: **TSG T WG1**

Copy: **TSG CN WG1, TSG RAN WG2**

Contact Person:

Name: Peter Howard

peter.howard@vf.vodafone.co.uk

S3 would like to highlight some concerns regarding the absence of some security features in the definition of the 3G terminal test environments in 3G TS 34.108.

Integrity protection

Integrity protection seems to be missing entirely from 3G TS 34.108. This is a major concern for two reasons:

- It is important that terminals check the integrity of down-link RRC signalling messages in the proper way. For example, where integrity protection is expected, terminals must reject messages that have a missing or incorrect message authentication code and messages that have been replayed.
- It is also important that terminals apply integrity protection to up-link RRC signalling messages in the proper way. For example, where integrity protection is expected by the RNC, signalling messages will be rejected if the integrity check in the RNC is not successful. This will lead to interoperability problems since the application of integrity protection is mandatory.

Network authentication failure

Although a test authentication algorithm is defined, authentication failure cases are not covered. Terminal behaviour on network authentication failure (temporal cell barring and cell reselection) must be properly implemented, otherwise it could lead to the terminal being denied service from a legitimate cell. Furthermore, the resynchronisation procedure must be implemented properly, otherwise out-of-order authentication vectors might also lead to the terminal being denied service from a legitimate cell.

Security indicators

There is currently no mention of the security indicators that may be supported by 3G terminals. It may be useful to include the cipher indicator and the 2G/3G security context indicator to allow terminals which implement these features to be properly tested. S3 currently have an ongoing work item to look at the visibility and configurability of security in R99 and beyond. Any further clarifications to the specifications on the visibility and configurability of security will be communicated to T1. An extract from the current version of 33.102 is provided below.

Conclusion

3G introduces new security features which are not present in GSM. Some of these features introduce new requirements on terminal testing which should be addressed in the UE conformance specifications. S3 would like to highlight the above deficiencies in the current Release 99 UE conformance specifications and kindly ask T1 to ensure that the necessary CRs to 34.108 are approved. It is expected that further liaison with S3, N1 (with respect to authentication) and R2 (with respect to integrity) might be necessary in order to complete this task.

Extract 33.102:

5.5.1 Visibility

Although in general the security features should be transparent to the user, for certain events and according to the user's concern, greater user visibility of the operation of security features should be provided. This yields to a number of features that inform the user of security-related events, such as:

- indication of access network encryption: the property that the user is informed whether the confidentiality of user data is protected on the radio access link, in particular when non-ciphered calls are set-up;
- indication of the level of security: the property that the user is informed on the level of security that is provided by the visited network, in particular when a user is handed over or roams into a network with lower security level (3G → 2G).