3GPP TSG SA WG3 Security — S3#16 **S3-000695**

28-30 November, 2000

Sophia Antipolis, France

Source: **Vodafone**

Title: **Security aspects of UE conformance**

Document for: **Decision**

Agenda Item:

Vodafone have recently studied 3G TS 34.108 (Common Test Environments for UE Conformance Testing) and would like to highlight some concerns regarding the absence of some security features in the definition of the 3G terminal test environments.

Integrity protection

Integrity protection seems to be missing entirely. 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 are required to be supported by 3G terminals. It may be useful to include the cipher indicator and the 2G/3G security context indicator in the UE conformance specifications.

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. It is therefore proposed that S3 highlight the deficiencies in the current UE conformance specifications in a liaison statement to T1 to ensure that the necessary CRs are produced by T1. It is suggested that the liaison statement is copied to N1 and R2.