3GPP TSG SA WG3 Security — S3#30 S3-030590
6 –10 October 2003
Povoa de Varzim, Portugal

Source: **Nokia**

Title: **Use of shared keys in the TLS protocol: IETF status update**

Document for: **Information**

Agenda Item: **7.9 GAA and Support for subscriber certificates, 7.18 Presence**

1. INTRODUCTION

This contribution informs about the current state of “Use of Shared Keys in the TLS Protocol” IETF draft [[DRAFT]].

2. DISCUSSION

The draft describing the use of shared keys in the TLS protocol was introduced in the IETF tls working group last May. Currently, it is a working group draft and has been revised once. So far, no objections against the draft have been raised. There is already at least one reference implementation available [CRYPTLIB].

There is likely to be one more revision of the draft to describe how the TLS master secret is formed from the initial shared secret. Thereafter, the draft should be ready to proceed to last call.

3. CONCLUSION

The draft describing the use of shared keys in the TLS protocol has progressed well and appears to have no opposition. It has good prospects for becoming an RFC in the Release 6 time frame.

4. REFERENCES

[DRAFT] Gutmann, P., “Use of Shared Keys in the TLS Protocol”, Internet-Draft, June 2003. URL: http://www.ietf.org/internet-drafts/draft-ietf-tls-sharedkeys-01.txt

[CRYPTLIB] http://www.cs.auckland.ac.nz/~pgut001/cryptlib/.