3GPP TSG SA WG3 (Security) meeting #30 **S3-030587**

7-10 October 2003

Povoa de Varzim, Portugal

Agenda Item: 7.5/7.6

Source: Ericsson, Vodafone

Title: Multiple PDP context security issue

Document for: Discussion/Decision

1. Background and introduction

In [S3-030087] Vodafone identified a security problem brought about due to the fact that a user can have multiple active GPRS PDP contexts to different APNs. The problem is that corporate customers want to be able to protect the security of their corporate networks by preventing their employees from having a GPRS connection to a public network (e.g the Internet) at the same time as they have a GPRS connection to the corporate network. To solve this problem it was proposed to develop a network-based feature to deny the establishment of new GPRS PDP contexts when there may be other context(s) active. [S3-030087] contains further details on the threat scenario and presented a brief rationale for standardising a network-based solution.

Some concerns have been raised that a terminal-based solution would be preferable to a network-based solution. In this contribution we argue that a network-based solution is complementary to a terminal-based solution and that the standardisation of a network-based solution would provide real benefits to operators.

2. Discussion

The main limitation of a GPRS network-based solution is that it cannot prevent a user connecting to a corporate network via GPRS whilst at the same time being connected to a public network via an alternative access network such as WLAN or the fixed Internet. A terminal-based solution can address this limitation and is also in line with recent developments in VPN and firewall technologies. However, a terminal-based solution also has its own limitations. In particular, terminal-based solutions rely on the security solution being installed, properly configured and enabled on any terminal that is used to access the corporate network.

From a mobile operator point of view, network-based security solutions have the advantage that they are easier to bundle into operator service offerings, potentially as an extension of existing service offerings. Agreements to enforce certain network-based security mechanisms are made between the operator and enterprises. These are then enforced on the end-users of the enterprise. Terminal-based security solutions are generally the responsibility of the enterprise and the end-user.

In summary we believe that a network-based solution is complementary to a terminal-based solution and that the standardisation of a network-based solution would provide real benefits to operators.

3. Conclusion

It is proposed that SA3 use this contribution as the basis for a reply LS to a recent LS received from SA2 [S2-033240].

4. References

[S3-030087] 3GPP Tdoc S3-030087: Security issue with multiple PDP contexts in GPRS, Vodafone, SA3#26, 25-28 February 2003, Sophia Antipolis, France.

[S2-033240] 3GPP Tdoc S2-033240: Reply LS on “Security issues regarding multiple PDP contexts in GPRS”.