3GPP TSG-SA WG3 Meeting #33 **TD S3-040382**
Beijing, China, May 10-14, 2004

Title: **Reply LS on Security of the Management Plane**

Response to: TD S3-040214(S5-046209) LS from SA5: LS on Security of the Management Plane.
Release:
Work Item:

Source: TSG-SA WG3
To: SA5, ITU-T SG4
Cc:

Contact Person:
Name: Huang Yingxin
Tel. Number: +86 10 82882752
E-mail Address: huangyx@huawei.com

Attachments: **Comments on the ITU COM4-D 127-E Study Group 4 "Baseline of Security Requirements for the Management Plane"**

---

1. Overall Description:

SA3 would like to thank SA5 for the LS: Security of the Management Plane.

LS (from SA WG5) on Security of the Management Plane and LS response (from SA WG5) to ITU-T SG 4 regarding Security of the Management Plane were introduced at SA3#33 meeting. Delegates were asked to consider the ITU-T document in order to provide any further Security-related comments to SA WG5. It was decided to collect comments off-line.

The attachment is comments on ITU-T Security of the Management Plane collected over e-mail.

2. Actions:

Actions to ITU-T SG4:

ITU-T SG4 are kindly asked to consider the attached comments in progressing the work on Security of the Management Plane.

Actions to SA5, ITU-T SG4 :

SA3 would ask to be kept informed with any decision on security protocols and algorithms in this work item.

3. Date of Next TSG-SA WG3 Meetings:

.

S3#34	06-09 July 2004	Acapulco, Mexico
S3#35	5-8 October 2004	Malta
S3#36	23-26 November 2004	Shenzhen, China
S3#37	February 2005	Australia (TBC)

5/20/2004

TITLE:

Comments on the ITU COM4-D 127-E Study Group 4 "Baseline of Security Requirements for the Management Plane"

SOURCES:

Lucent Technologies Inc.
Michael Marcovici - 3GPP SA 3
marcovici@lucent.com

ABSTRACT:

This contribution includes Lucent's comments on the ITU-T SG4 Management Plane Security Recommendations, Reference COM4-LS 27Rev2-E.

General Comments:

We feel that a more streamlined *Scope* section may be more beneficial to the reader. The *Scope* section shall clearly identify the goal of the document, as well as clearly differentiate among the different security planes, e.g., user plane, signaling plane, bearer plane.

The vast majority of the recommendations throughout this document imply that each security recommendation equally applies to all NE/MS in a network (e.g., "EACH NE/MS …") . We consider that some security requirements cannot always be applied to each NE/MS network entity, therefore the use of "Shall" is not appropriate.

To better evaluate potential threats and specify methods to protect against those threats, it may be preferable to associate the threats described with a specific security plane (e.g., physical plane, user plane, management plane, etc.).

Specific Comments:

Section 6.1.5 - key management M-7 , O-1,	Includes the following statement: "the NE/MS supplier shall provide secure key generation, distribution ... *as defined in X.500 and X.509*." This sentence implies a mandatory use of a PKI certificate management system. But we will like to highlight that without a PKI, a centralized key distribution center that could manage the keys would also be sufficient. This comment is also valid for other instances where PKI is implied to be the only mechanism that can be used (e.g., O-1). Change M-7 to: REC-7: An NE/MS may provide capabilities for secure key generation, distribution, storage and replacement/recovery" (Note that M-9 recommends that X.509 may be used to support Rec-7 above)
Section 6.2.2 M-19	Change to: REC-19: "Passwords should be user changeable at the user's discretion, following a configurable minimum interval since the last change. **The configurable minimum interval should be set by the SYSTEM SECURITY ADMINISTRATOR.** The default should be one day."
Section 6.3.2 M-32	Change to: REC-32: "The system age threshold for login passwords should be configurable by the SYSTEM SECURITY ADMINISTRATOR or by the APPLICATION SECURITY ADMINISTRATOR if the functionality is also built into the application. The default should be 90 days. **At the expiration of the age threshold the login password for an affected application should be reset to an original default state defined in REC-31. All password change privileges should be revoked for all users except for the SYSTEM SECURITY ADMINISTRATOR or the APPLICATION SECURITY ADMINISTRATOR."**
M-33	Change to: REC-33 "The system inactivity timer value should be configurable by the SYSTEM SECURITY ADMINISTRATOR or by the APPLICATION SECURITY ADMINISTRATOR if the functionality is also built into the application. The default should be 60 minutes. **When the system inactivity timer is enabled, an access to the system for a given user ID shall be prevented and the login process for this user should be disabled.**
M-35	Change to: REC-35: "Each NE/MS should be able to log any action that changes the security attributes and services, access controls, or other configuration parameters of the devices; **each login attempt and its result that caused invocation of the system inactivity timer defined in M-33 (REC-33)."**
M-54	Define "lockout".
M-57	Add to current recommendation: **"To re-enable a DISABLED login ID at least one of the following should be used:** ... "

M-64	Changed to: REC-64: "All software delivered to a service provider or other customer should include, **when appropriate,** cryptographic AUTHENTICATION and integrity protection mechanisms such as digital signatures or symmetric message AUTHENTICATION ~~as specified in clause 6.1~~ . For software distribution, typically digital signatures, rather than symmetric message authentication codes, are included for receivers to verify authenticity. It is generally much too difficult for a software provider to share a secret with all of her customers)."
M-65	The recommendation is too restrictive; other security methods may apply as well, and this fact should be reflected in the REC-65
M-66	This is not a security requirement. Thus, it should be deleted from the document.