**3GPP TSG SA WG3 Security — S3#33** **S3-040250**
**10 - 14 May 2004**
**Beijing, China**

---

**3GPP TSG-SA5 (Telecom Management)** **S5-046378**
**Meeting #37bis, Sophia Antipolis, FRANCE, 29 Mar - 2 Apr 2004**

| | |
|---|---|
| **Title:** | **LS response to ITU-T SG 4 regarding Security of the Management Plane** |
| **Response to:** | **ITU-T SG4 LS27-SG4-rev2 / S5-042107** |
| **Release:** | **Release 6** |
| **Work Item:** | **OAM-NIM (Security Management)** |
| **Source:** | **3GPP SA5** |
| **To:** | **ITU-T SG4** |
| **Cc:** | **3GPP SA3, 3GPP2 TSG-S WG5** |
| **Cc:** | **ITU-T/3GPP Co-ordinator, Stephen HAYES, TSG CN Chair (stephen.hayes@ericsson.com)** |

**Contact Person:**
**Name:** **Yangli**
**Tel. Number:** **+86 21 68644808-24040**
**E-mail Address:** **afi@huawei.com**

**Attachments:** None but see the URL below.

---

## 1. Overall Description:

3GPP SA5 has a work task to address security management aspects of the Itf-N within the current Release 6 work plan. SA5 agreed that it would be very beneficial to refer to an international recommendation from within 3GPP specifications in order that compliance might be made to a single security management standard which addresses the security requirements from many countries within a single standard body such as the ITU-T.

To achieve this aim, which will considerably ease the compliance and design issues for any vendor supplying equipment to many international markets, it is necessary to be able to uniquely identify sets of requirements which are directly associated with the problem domain a particular network operator encounters performing the activity of running a network. As it is not expected that a network operator will encounter ALL security threats within his network, it must be easy for an operator to identify particular threats and comply with associated counter measures in a manner that a "pick and mix" set of threats and requirements associated with the counter measures for the threats may be achieved.

SA5 appreciates that there may be plans within the ITU-T to restructure the current draft which may not be available until 2005 which is after the SA5 Release 6 cut-off date. SA5 intends to document its security requirements for Release 6 within the current security management IRP work which is planned to consist of the following specifications:

- 32.371: Security Management IRP: Concept and Requirements (the current agreed draft may be found at the following URL: http://www.3gpp.org/ftp/Specs/html-info/32371.htm )
- 32.372: Security Management IRP: Information Service (protocol-neutral)
- 32.37x: Security Management IRP: x Solution Set (protocol-specific, e.g. x=3 for CORBA, x=4 for CMIP)

NOTE: For an understanding of the IRP concept, see the 3GPP TS 32.150 sent to you via a separate liaison or available at http://www.3gpp.org/ftp/Specs/html-info/32150.htm

**The SA5 specifications related to the SG4 activity will be provided to SG4 for its review and use in its Recommendation and it is our intention to reference the ITU-T Recommendation when it is available. SA5 believes that there are the following key differences between the ITU-T requirements and those SA5 has identified in 32.371 above:**

- The ITU-T draft cites in its Summary"...It focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the network infrastructure". The 3GPP SA5 security requirement focuses only on the IRPAgent (i.e., the ITU-T MS) and not NE(s). This is an important difference since the number of NE(s) is much larger than the number of IRPAgents in 3G networks and therefore, security solutions for them can be different.
- ITU-T draft Summary cites "…specifies baseline security requirements for cryptographic algorithms, authentication, administration, management of NE/MS, management communications, and NE/MS development and delivery." 3GPP SA5 security requirement and solutions currently do not focus on the standardization of security aspects relating to security "administration", security "management of NE" and "NE/MS development and delivery".
- The ITU-T draft discusses the security issues related to user-login, user account etc. 3GPP SA5 security requirement does not concern itself with user (e.g., operator John and Mary) login and user account management. 3GPP SA5 security authentication and access control are related to IRPManager (e.g., a large computer system/system process that can handle multiple users.)

**SA5 additionally offers the following more specific comments on the current security draft**

1. Note that it should be possible to balance the costs of implementing a particular security counter measure with the probability of the threat and the possible damage. Therefore the extensive usage of the word "Shall"in the security draft should be avoided, because it would imply that all requirements have to be satisfied.
   It may also be possible for new threats to be identified, and so any counter measure should allow a vendor to implement something which is an improvement on current knowledge as technology advances.
2. The current document refers to other ITU-T specifications; it would be useful to determine and state how these specifications are to be used to address how ambiguity and conflicts are resolved.
3. There are security issues, which are specific to mobile networks. E.g. specification of security gateways, the relationship between these issues regarding 3GPP architecture and the ITU-T specifications need to be handled. E.g. not all Network Elements should have a mandatory requirement for including security measures. This is related to the vulnerability and potential threats.
   - Many of the requirements seem applicable to EM/NM servers rather than real-time embedded systems. Careful consideration should be given to how applicable many of the requirements are to real time embedded systems and what special requirements these systems have. An indication of which requirements are applicable to which type of system could be considered.
4. We have some concerns with the current document structure. In its current form there is a mix of requirements, potential threats, counter measures and implementation directives / statements. We would prefer an alternate approach to the requirements in recommendation structure. This is based on the observation that the current structure goes straight into detailed implementation section 6. We would propose the structure should comprise several related parts. This is in order to identify sets of security vulnerability (e.g. physical access, internet access, file transfer etc) and for each vulnerability identify a set of potential security threats including the possible damage. Then for each and every identified security threat there is a corresponding set of requirements to overcome, or mitigate that particular threat.
   - Scope includes a brief overview of architecture and security issues. This could be put later in the document and expanded and aligned with other security documents, for example M.3016 terminology.
   - Section 4, terms defined in this document, includes both well know terms defined in other standards (e.g. access control) and definitions of a subjective nature such as roles (e.g. application administrator). In most cases the definition of roles includes a list of functions for that role, which SA5 would like to see discussed and defined in a separate section dedicated to this topic.
   - Annex I covers a wide range of topics in a fairly high level way. These seem more appropriate for inclusion in quality standards and building security guidelines. It would seem more appropriate to have a separate document that mandates security quality plans, or to update existing standards to include security related issues.

5. Section 6 introduces 6 principles of OAM&P (mechanisms) without explaining how they counter the threat and which threats they counter. This should be defined here or reference made to standards that define the connection.

6. Some of the requirements are not precise. For example M-1, which is "For all symmetric encryption applications, algorithms with strengths similar to AES or TDEA shall be used." SA5 would prefer to see these requirements defined quantitavely not qualitatively, e.g. "it should take x years for an attacker to break …" Once the requirements have been defined in absolute terms another section or perhaps an annex could define how these requirements can be met with existing technology and processing power. This approach would help to "future proof" the document and make the requirements clearer.

    - Section 6 includes a general overview of specific security methods used to implement the mechanisms, e.g. types of asymmetric encryption algorithms. Again SA5 would prefer to see the requirements separated from how they can be implemented and constraints to meet the requirements.

    - There is some duplication in the requirements, for example section 6.4.1 (login process) duplicates much of 6.2 (authentication)

    - A lot of the requirements giving default parameters for login to a system have underlying requirements. SA5 would like to see these identified. These need to be identified (e.g. that attacks such as dictionary attacks should be made infeasible, that old unused user accounts should not remain active on a system) and the recommended (or mandated) default parameters defined in a separate section or annex.

7. The current document refers to many federal standards (FIPS). We question whether this is appropriate for an international standard e.g. try and refer to equivalents international specifications. (e.g. ITU-T or ISO specifications).

## 2. Actions:

**To ITU-T SG4**

**ACTIONS:** SA5 asks ITU-T SG4 to:

- Take these comments into account in progressing the draft ITU-T Recommendation
- Keep SA5 informed as to the progress of this work

## 3. Date of Next SA5 Meetings:

| | | | |
|---|---|---|---|
| 3GPPSA5#38 | 10 - 14 May 2004 | Beijing | CN |
| 3GPPSA5#38-bis | 28 Jun - 2 Jul 2004 | Sophia Antipolis | FR |