Source: **WG SA5 (Telecom Management)**

Title: **3 CRs to 32.101 v.3.0.0 (3G Telecom Management principles and high level requirements)**

Document for: **Approval**

Agenda Item: **5.5.3**

Ty	Number	Title	WG	editor	version
TS	32.101	3G Telecom Management principles and high level requirements	S5	Michael Truss	3.0.0

TSG Meet-ing	TSG WG doc number	Spec	CR	Ph	Vers Old	Vers New	Subject	TSG WG meeting	WG status	Workitem
SP-07	S5-000153	32.101	001	R99	3.0.0	3.1.0	Clarify use of X.25 as a Network Layer Protocol	S5-10	Agreed	Telecom Management Principles & Requirements (PR)
SP-07	S5-000156	32.101	002	R99	3.0.0	3.1.0	Correction of IRP-related terminology	S5-10	Agreed	PR
SP-07	S5-000157	32.101	003	R99	3.0.0	3.1.0	Clarification of Software Management	S5-10	Agreed	PR

CHANGE REQUEST	*Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.*

32.101 CR **Xxx**   Current Version: **3.0.0**

GSM (AA.BB) or 3G (AA.BBB) specification number ↑   ↑ *CR number as allocated by MCC support team*

For submission to:	**SA#7**	for approval	**X**	strategic	**X**	*(for SMG use only)*
list approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 1.1 for 3GPP and SMG   The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CRF-11.rtf

Proposed change affects: (U)SIM ☐   ME ☐   UTRAN **X**   Core Network **X**
(at least one should be marked with an X)

Source:	SA5		**Date:**	01.03.00

Subject: 32.101 CR to Clarify use of X.25 as a Management Network Layer Protocol

Work item: Principles & Requirements

Category: F Correction   **X**   **Release:**   Phase 2   ☐
(only one category shall be marked with an X)
    A Corresponds to a correction in an earlier release   ☐   Release 96   ☐
    B Addition of feature   ☐   Release 97   ☐
    C Functional modification of feature   ☐   Release 98   ☐
    D Editorial modification   ☐   Release 99   **X**

(releases phase2, 96, 97 and 98 apply only to GSM specifications)

Reason for change: This CR proposes that a clarification be added to Annex A of 32.101 stating that IP is the recommended Networking Protocol.

Clauses affected: Annex A

Other specs affected:

Other 3G core specifications	☐	→ List of CRs:	
Other GSM core specifications	☐	→ List of CRs:	
MS test specifications	☐	→ List of CRs:	
BSS test specifications	☐	→ List of CRs:	
O&M specifications	☐	→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

Annex B (normative):
UMTS Management Network Layer Protocols

The valid Network Layer Protocols for the Management of UMTS are:

- IP

- X.25

Note: IP is the recommended Networking Protocol.

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

32.101	**CR**	**xxx**	Current Version:	**3.0.0**

GSM (AA.BB) or 3G (AA.BBB) specification number ↑   *↑ CR number as allocated by MCC support team*

For submission to:	**SA#7**	for approval	**X**	strategic		*(for SMG*
list expected approval meeting # here ↑		for information		non-strategic		*use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG   *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM ☐   ME ☐   UTRAN / Radio **X**   Core Network **X**
(at least one should be marked with an X)

Source:	SA5		**Date:**	2000-03-01

Subject:	Correction of IRP-related terminology

Work item:	Principles and High-level Requirements

Category:	F	Correction	**X**	**Release:**	Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
(only one category	B	Addition of feature			Release 97	
shall be marked	C	Functional modification of feature			Release 98	
with an X)	D	Editorial modification			Release 99	**X**
					Release 00	

Reason for change:	The purpose of the proposed changes is to improve one of the IRP-related terms in this TS: It is proposed to change the name "Resource Model" to "Network Resource Model" (in this and all TSs using IRP terminology). The reason for this is that the former name is very generic and can be interpreted as "any kind of model", while the proposed new name more clearly indicates that it is a model for the managed network resources.

Clauses affected:	3.1, 3.3, 5.6

Other specs affected:	Other 3G core specifications		→ List of CRs:	
	Other GSM core specifications		→ List of CRs:	
	MS test specifications		→ List of CRs:	
	BSS test specifications		→ List of CRs:	
	O&M specifications	**X**	→ List of CRs:	32.102 CR xxx

Other comments:	

help.doc

<--------- double-click here for help and instructions on how to create a CR.

3.1　Definitions

For the purposes of the present document, the following definitions apply:

Operations System (OS): This abbreviation indicates a generic management system, independent of its location level within the management hierarchy.

Element Manager (EM): Provides a package of end-user functions for management of a set of closely related types of network elements. These functions can be divided into two main categories:

Element Management Functions: for management of network elements on an individual basis. These are basically the same functions as supported by the corresponding local terminals.

Sub-Network Management Functions: that are related to a network model for a set of network elements constituting a clearly defined sub-network, which may include relations between the network elements. This model enables additional functions on the sub-network level (typically in the areas of network topology presentation, alarm correlation, service impact analysis and circuit provisioning).

Enterprise Systems: those Information Systems that are used in the telecommunication organisation but are not directly or essentially related to the telecommunications aspects (Call Centre's, Fraud Detection and Prevention Systems, Invoicing etc).

IRP Information Model: An IRP Information Model consists of an IRP Information Service and a **Network** Resource Model (see below for definitions of IRP Information Service and **Network** Resource Model).

IRP Information Service: An IRP Information Service describes the information flow and support objects for a certain functional area, e.g. the alarm information service in the fault management area. As an example of support objects, for the Alarm IRP there is the alarm record and alarm list.

IRP Solution Set: An IRP Solution Set is a mapping of the IRP Information Service to one of several technologies (CORBA/IDL, SNMP/SMI, CMIP/GDMO, etc.). An IRP Information Service can be mapped to several different IRP Solution Sets. Different technology selections may be done for different IRPs.

Management Infrastructure: The collection of systems (computers and telecommunications) a UMTS Organisation has in order to manage UMTS.

Network Element (NE): a discrete telecommunications entity which can be managed over a specific interface e.g. the RNC.

Network Manager (NM): Provides a package of end-user functions with the responsibility for the management of a network, mainly as supported by the EM(s) but it may also involve direct access to the network elements. All communication with the network is based on open and well standardized interfaces supporting management of multi-vendor and multi-technology network elements.

Network Resource Model (NRM): A protocol independent model describing managed objects representing network resources, e.g. an RNC or NodeB.

UMTS Organisation: A legal entity that is involved in the provisioning of UMTS.

3.3　Abbreviations

For the purposes of the present document, the following abbreviations apply:

CEIR	Common Equipment Identification Register
CPE	Customer Premises Equipment
IRP	Integration Reference Point
MMI	Man-Machine Interface
NRM	Network Resource Model
QoS	Quality of Service
SLA	Service Level Agreement

TM	Telecom Management
TMF	TeleManagement Forum
TMN	Telecommunications Management Network
TOM	Telecom Operations Map
UMTS	Universal Mobile Telecommunication System
VHE	Virtual Home Environment

5.6 Logical Level

This level covers the mutual and conceptual knowledge of entities being connected by a given interface.

For type 1b interfaces (such as Itf-N in figure 1.1 above) interactions at this level are fully standardised by 3GPP in terms of protocol independent **Network** Resource Models (static information definition) and IRP Information Services (information flows) where available. These protocol independent **Network** Resource Models and IRP Information Services are hereafter referred to as IRP Information Models (Integration Reference Point Information Models).

For type 1a interfaces (such as Itf-B and Itf-R in figure 1.1 above) interactions at this level are not standardised in terms of information models or flows, though functional aspects will be specified.

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

32.101	CR	**xxx**	Current Version:	3.0.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑   ↑ *CR number as allocated by MCC support team*

For submission to: **SA#7**   for approval **X**   strategic ☐   *(for SMG*
list expected approval meeting # here ↑   for information ☐   non-strategic ☐   *use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG   The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM ☐   ME ☐   UTRAN / Radio **X**   Core Network **X**
(at least one should be marked with an X)

Source:	SA5		**Date:**	2000-02-24

Subject: Clarification of Software Management

Work item: Principles and High-level Requirements

Category: F Correction
          A Corresponds to a correction in an earlier release
(only one category   B Addition of feature
shall be marked   C Functional modification of feature   **X**
with an X)   D Editorial modification

Release: Phase 2 ☐
          Release 96 ☐
          Release 97 ☐
          Release 98 ☐
          Release 99 **X**
          Release 00 ☐

Reason for change: The purpose of the proposed changes is to add explanatory material and to make Section 8.7 (Software Management) more generally applicable. Section 8.7 provides a useful presentation of software management processes. However, the section presents two software management scenarios and gives the impression that this is the only permissible solution, whereas we can foresee that within the framework of 3G there will be certain useful variants of the processes illustrated. We propose that the processes presented must be seen and labelled as <u>examples</u>, and that some more explanatory text should be added to explain this and software management in general.

Clauses affected: 8.7

Other specs affected:
Other 3G core specifications	☐	→ List of CRs:	
Other GSM core specifications	☐	→ List of CRs:	
MS test specifications	☐	→ List of CRs:	
BSS test specifications	☐	→ List of CRs:	
O&M specifications	☐	→ List of CRs:	

Other comments: There are several figures of varying styles and formalisms (e.g., Figs. 5, 7, 8, 9, 11, 12). It would help the reader if these were brought in line with each other, standardizing on a single diagram type.

help.doc

<--------- double-click here for help and instructions on how to create a CR.

8.7   Software Management

This subclause describes the software management process for third generation networks. Two main scenarios are considered:

- Main SW Management Process : It covers requesting, acceptance, installation, monitoring, documenting, data base updating and feedback to the vendor for managing software. The sub-processes are valid for complete software releases and software patches for fault correction of the network elements and even element managers.

- Software Fault Management: Its emphasis is on network monitoring and handling faults which are caused by software malfunctions.

8.7.1   Main Software Management Process

The main focus is the management of new software releases and correction patches. Importance is placed integrating new software into a network with out causing unnecessary service disruptions and maintaining high levels of quality for the network. ~~The Software Installation process is illustrated in Fig. A.~~ The main steps in the software management process are:

- Delivery of software from the vendor.

- ~~Delivery~~ Delivery of the software to local storage in the network elements and/or element managers.

- Validation of the software to ensure that the SW is not corrupt.

- Activation of the software to an executable state.

- ~~Validation~~ Validation of the software to ensure that ~~it runs~~ it runs ~~properly~~ correctly.

- Acceptance or rejection of the software, depending on the outcome of the ~~tests~~ validation. (A rejection of the software implies a reversion to a previous software version).

Figure 11 shows an example of how these steps may be realized in terms of activities involving the processes defined in the Telecom Operations Map. However, alternative sequences may exist. For example, increased automation may cause step 3 to be omitted. Instead, a vendor certification activity could be run for a series of software releases or patches.

~~<With the above text, it is proposed to remove the points 1-9 below.>~~

The following list is an explanation to the steps in figure 11.

1) Based on inputs ~~for~~ from customer care interactions and marketing research, a network operator will establish new feature requirements. These requirements are sent to the vendor in the form of a feature request.

2) The vendor ~~deliveries~~ a new software release/correction with the corresponding documentation and installation procedure to the network operator. It should be noted that when a network operator utilises equipment ~~for~~ from more than one vendor, this process ~~must~~ run~~s~~ as multiple parallel processes.

3) A service quality management department of the network operator receives and reviews the software. Upon approving the software for installation, the software is sent to the network provisioning department.

4) Installation Task

   a) The software is installed in the appropriate network elements and/or element managers by network provisioning.

   b) Installation information is sent to the network maintenance and restoration department to inform them of pending changes in the network.

   c) Installation information is sent to the customer care centre to inform them of pending changes in the network.

5) Installation Test and Validation

a) Once the software has been installed, network provisioning ~~must (should)~~ perform<u>s</u> test<u>s</u> to check and ensure that the new software is working properly.

b) In addition to the checks that are performed by network provisioning, network maintenance and restoration could also detect malfunctions with-in and outside the updated network element.

c) Should network maintenance and restoration detect a problem with-in the updated network element, then ~~the~~ network provisioning is informed to decide on further actions.

6) Successful Installation Result

a) Upon successful installation of the software, the service quality management department~~s~~ is informed.

b) A report is sent to network maintenance and restoration to inform them that the software will remain implemented in the network. At this point the documentation library and software data base ~~must be~~<u>is</u> updated.

c) The network data management department is informed over the changes in the network.

7) Negative Installation Result

a) If the installation fails, network provisioning ~~must~~ perform<u>s</u> a "fallback", i.e. remove the new software and insure that the network element is running properly on the old software.

b) A report containing the negative results and finding<u>s</u> will be sent to ~~the~~ service quality management and at the same time to ~~the~~ network maintenance and restoration.

8) Once the installation procedure has been ended, the network maintenance and restoration department ~~must~~ closely monitor<u>s</u> the affected network element to ensure proper performance.

9) Service quality management will send feedback to the vendor as to the positive or negative results of the installation.
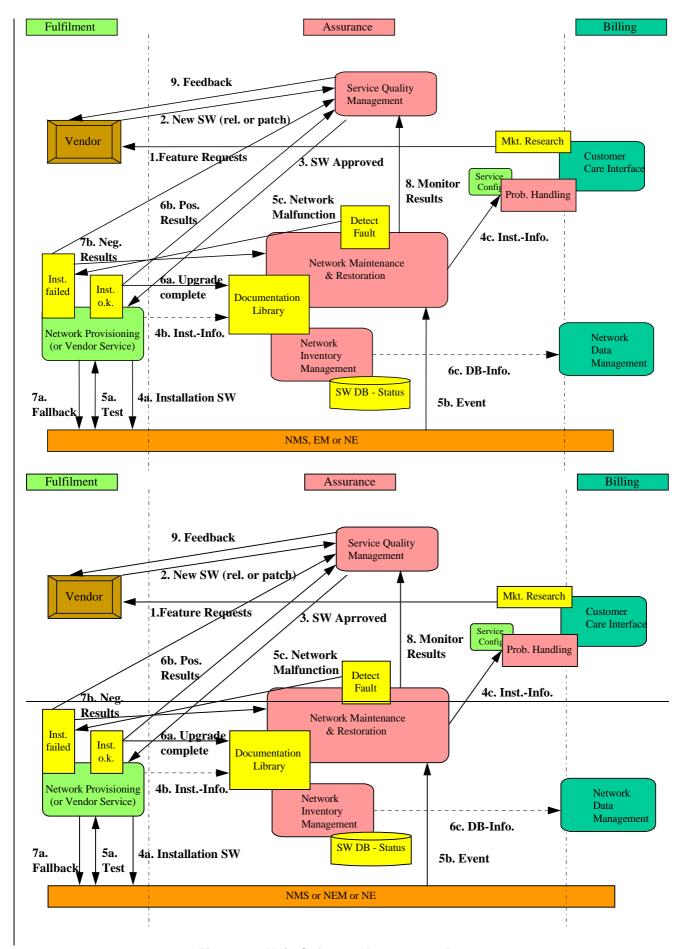
| Fulfilment | Assurance | Billing |

9. Feedback

Service Quality Management

2. New SW (rel. or patch)

Vendor

Mkt. Research

Customer Care Interface

1.Feature Requests

3. SW Approved

Service Config

Prob. Handling

8. Monitor Results

6b. Pos. Results

5c. Network Malfunction

Detect Fault

4c. Inst.-Info.

7b. Neg. Results

Network Maintenance & Restoration

Inst. failed

Inst. o.k.

6a. Upgrade complete

Documentation Library

Network Provisioning (or Vendor Service)

4b. Inst.-Info.

Network Inventory Management

Network Data Management

SW DB - Status

6c. DB-Info.

7a. Fallback

5a. Test

4a. Installation SW

5b. Event

NMS, EM or NE

| Fulfilment | Assurance | Billing |

9. Feedback

Service Quality Management

2. New SW (rel. or patch)

Vendor

Mkt. Research

Customer Care Interface

1.Feature Requests

3. SW Aprroved

Service Config

Prob. Handling

8. Monitor Results

6b. Pos. Results

5c. Network Malfunction

Detect Fault

4c. Inst.-Info.

7b. Neg. Results

Network Maintenance & Restoration

Inst. failed

Inst. o.k.

6a. Upgrade complete

Documentation Library

Network Provisioning (or Vendor Service)

4b. Inst.-Info.

Network Inventory Management

Network Data Management

SW DB - Status

6c. DB-Info.

7a. Fallback

5a. Test

4a. Installation SW

5b. Event

NMS or NEM or NE

Figure 11: Main Software Management Process

~~<In TOM, it says explicitly that it is the Network Inventory Management process that is responsible for software upgrades. Why is this performed by Network Provisioning in Figure 11 (and Figure 12)?>~~

~~<The Customer Care Interface in Figures 11 and 12 is not a TOM process. Can it be replaced by the Customer QoS Management process?>~~

~~<The arrows marked 6a and 6b in Figure 11 seem to be swapped with respect to the text in Section 8.7.1.>~~

8.7.2   Software Fault Management.

Software fault management involves the following steps:

- Detection of SW malfunctions in the network.

- Problem resolution. The origin of the malfunction is determined and corrective action is decided. The corrective action can be one of the following:

  - Reversion to an earlier software version. This can imply both load and activation of the earlier software.

  - Load and activation of correction software, according to 8.7.1.

  - Re-activation of current software.

Figure 12 shows an example of how these steps may be realized in terms of activities involving the processes defined in the Telecom Operations Map.

~~<With the above text, it is proposed to remove the points 1-9 below.>~~

The following list is an explanation to the steps in figure 12.

1) The network maintenance and restoration department detects an event or an alarm/fault from the network element.

2) Problem solving and informing customer care

   a) The alarm is forwarded to the service problem resolution department for corrective actions and it is determined that the problem is caused by a software defect.

   b) In parallel the Customer Care Centre is informed, if the malfunction of the network may have impact on customers.

3) The service problem resolution department informs problem handling and subsequently the customer care centre over service impairments with-in the network.

4) Problem handling reports to the service quality management department. The service disturbance is described with-in the report.

5) Service quality management checks the current software level of the affected network element with the network inventory management department.

6) If major network disturbances still appear the Service Quality management decides to fallback to a stable SW version (maybe some time after a new SW installation) and requests Network Provisioning.

7) a+b) :Network Provisioning performs the fallback and informs Network Maintenance and Inventory.

8) Service quality management sends a request for a software correction to the vendor.

9) The vendor sends a new software release or correction to the network operator. The rest of the procedure can be followed in the main software management process.
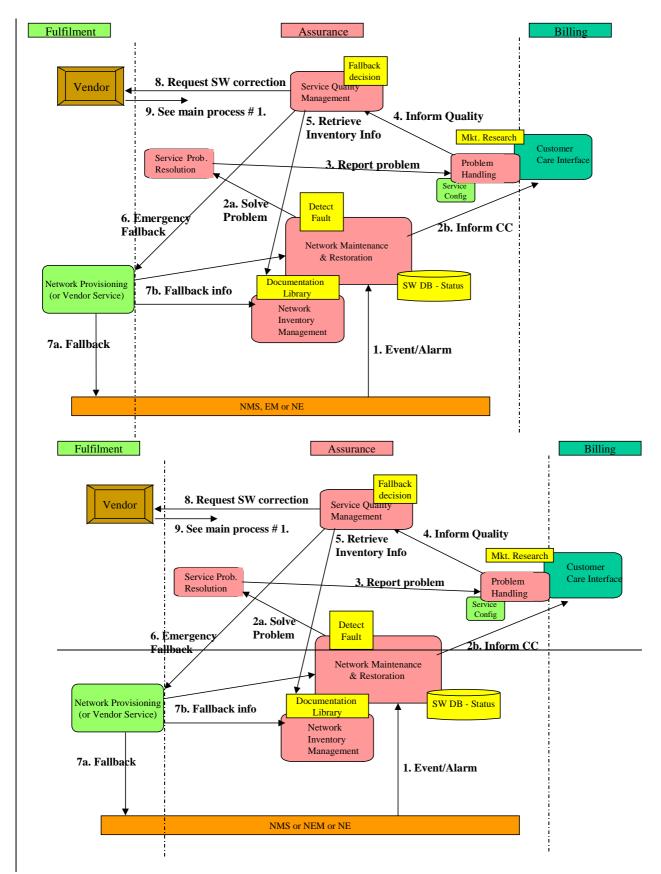
Figure 12: Software Fault Management