Network Resource Assurance - DDP BA

TMF518_NRA

Version 1.2

September, 2011

Notice

No recipient of this document and code shall in any way interpret this material as representing a position or agreement of TM Forum or its members. This material is draft working material of TM Forum and is provided solely for comments and evaluation. It is not “Forum Approved” and is solely circulated for the purposes of assisting TM Forum in the preparation of final material in furtherance of the aims and mission of TM Forum.

Although it is copyrighted material of TM Forum:

- Members of TM Forum are only granted the limited copyright waiver to distribute this material within their companies and may not make paper or electronic copies for distribution outside of their companies.
- Non-members of the TM Forum are not permitted to make copies (paper or electronic) of this draft material other than for their internal use for the sole purpose of making comments thereon directly to TM Forum.
- If this material forms part of a supply of information in support of an Industry Group Liaison relationship, the document may only be used as part of the work identified in the Liaison and may not be used or further distributed for any other purposes

Any use of this material by the recipient, other than as set forth specifically herein, is at its own risk, and under no circumstances will TM Forum be liable for direct or indirect damages or any costs or losses resulting from the use of this material by the recipient.

This material is governed, and all recipients shall be bound, by all of the terms and conditions of the Intellectual Property Rights Policy of the TM Forum (http://www.tmforum.org/Bylaws/1094/home.html) and may involve a claim of patent rights by one or more TM Forum members or by non-members of TM Forum.

Direct inquiries to the TM Forum office:

240 Headquarters Plaza,
East Tower – 10th Floor,
Morristown, NJ 07960 USA
Tel No. +1 973 944 5100
Fax No. +1 973 944 5110
TM Forum Web Page: www.tmforum.org

Table of Contents

List of Requirements

List of Use Cases

Not Applicable.

List of Figures

List of Tables

Executive Summary

This document is the Business Agreement (BA) part of the Network Resource Assurance (NRA) Document Delivery Package (DDP). This BA addresses the Data Model (DM) aspects of resource assurance and as such it defines all resource related managed entities visible across the Interface that are used in support of resource assurance.

See Section 1 for additional introductory material related to this document.

1 Introduction

1.1 DDP Structure

In order to allow for more efficient release delivery, the previous monolithic BA, IA and SS documents have been partitioned into smaller self-contained (though not independent) units called Document Delivery Packages (DDPs).

This is similar to the 3GPP concept of Integration Reference Point (IRP). The basic idea is that the Interface, which is specified by the entire document set (of a release), is partitioned into DDPs where each DDP specifies “a certain aspect” of the Interface, which needs to be very clearly scoped.

There are three kinds of DDPs:

- the FrameWork DDP (FMW) – this DDP contains the generic artifacts that are applicable to all the other DDPs.
- Data Model DDP (DM-DDP) – a DDP that concerns a data model (entities, data structures, attributes, state, but no operations)
- Operation Model DDP (OM-DDP) – a DDP that concerns a computational model (operations, notifications, transactions) for a given functional area (such as resource inventory management)

The unified deliverables structure for any given MTOSI / MTNM product release is as follows:

- Product Release Notes:
  - a scope specification for the type and extent of the delivered product,
  - the partitioning of the release into DDPs (i.e., definitions of various aspects of the release),
  - and an overview of the release’s (delta) deliverables;
- For each DDP:
  - Business Agreements (BAs): a business view specification
  - Information Agreements (IAs): a system view specification
  - Interface Implementation Specifications (ISSs): implementation and deployment view specification per supported enabling technology (mapping of the IA to either CORBA (IDL, services usage) or XML (WSDL, XSD, bindings…)
  - Supporting Documentation: normative and informative supporting documents.
- Reference Implementation (optional) of core IIS fragments for selected interfaces and enabling technologies.

1.2 Document Structure

This document is divided into the following sections:

Section 1 is this introduction.

Section 2 defines the business problem and project scope.

Section 0 has the requirements and associated descriptive text.

Section 4 contains the use cases.

Section 5 has traceability matrices between the use cases and associated requirements, and vice versa.

Section 6 provides a summary and list of open issues to be considered in later versions of this document.

Section 7 lists references and states IPR claims, if any.

Section 8 provides administrative details such as author contact information, document history and acknowledgements.

1.3 Terminology Used In This Document

Refer to the SD0-1 supporting document.

2 Business Problem Description, Project Scope

2.1 Project Scope

The TM Forum Integration Program is responsible for all of the interface and business services work within the TM Forum. In some cases, interface work is delegated to other teams but the final verification for technical uniformity and integrity is the responsibility of the TM Forum Integration Program.

Initially, the TM Forum Integration Program was formed to coordinate the various existing TM Forum interfaces activities (as shown in **Figure 2-1**). In particular, the responsibility for maintaining MTOSI and MTNM is now covered by the MTOSI-MTNM Users Group which is a team within the TM Forum Integration Program. The long term plan (which is already well under progress) is to migration the various input work to a single harmonized suite of interfaces.

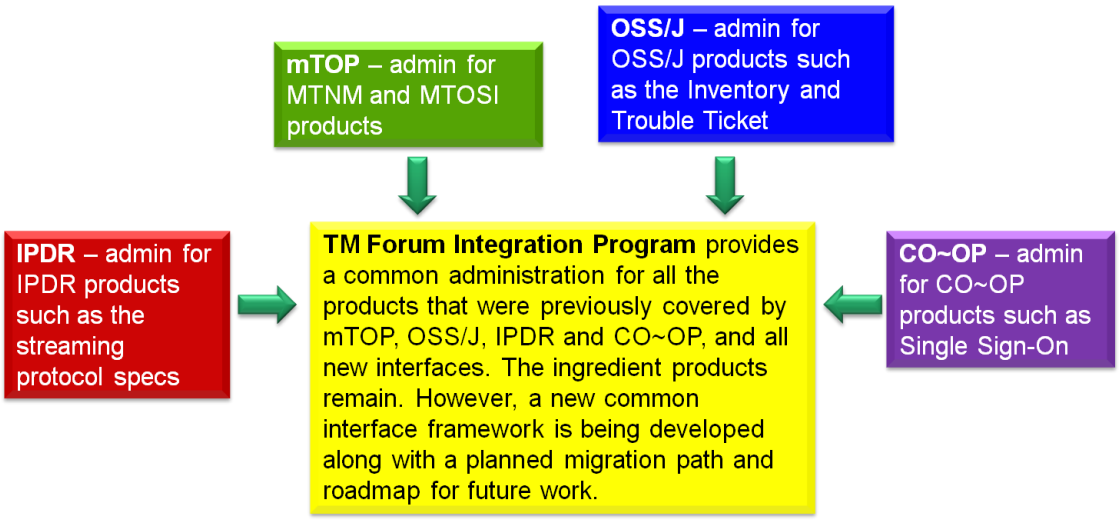

Figure 2-1**. Inputs to the TM Forum Integration Program**

Figure 2-2 provides a summary of the team within the TM Forum Integration Program as well as a few teams outside of the program but which also do some interface work. In terms of MTOSI and MTNM, the main input for updates come from the Resource and Service Management Team.

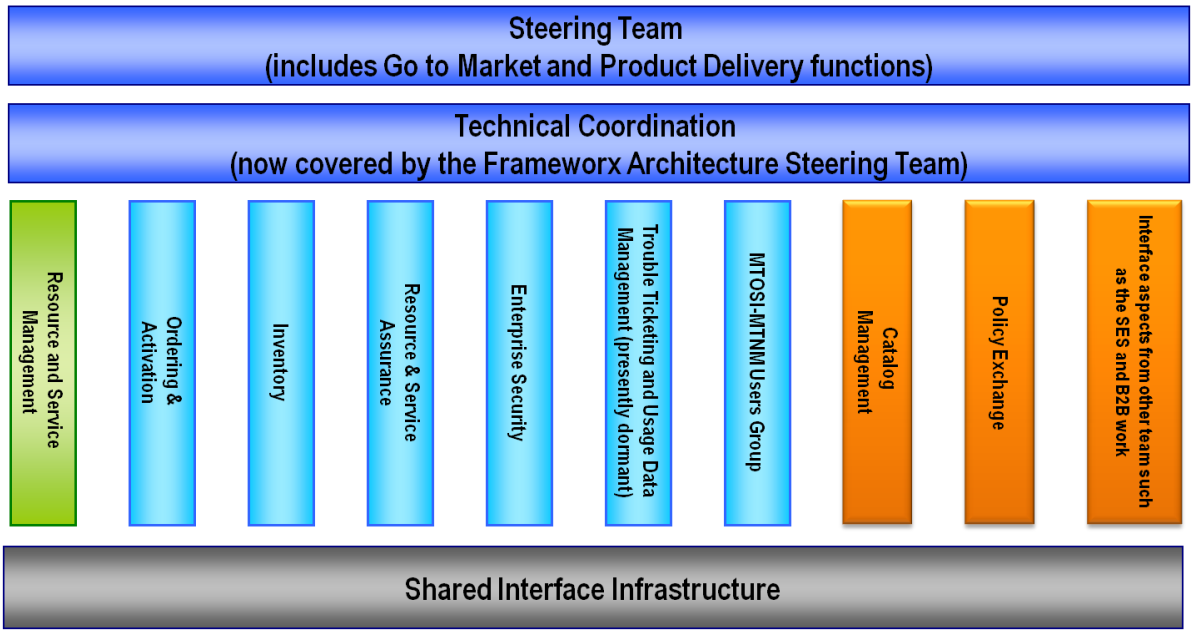

Figure 2-2**. TM Forum Integration Program**

2.2 Benefits

MTOSI and MTNM provide a set of Interface specifications that allow for resource and service management (with only MTOSI covering service management, but with MTOSI and MTNM both covering resource management, using very much the same information model).

These specifications are intended to lower design, implementation, Verification Validation & Testing (VVT), and maintenance costs for management interfaces. These Interfaces are intended for use by service providers, suppliers of equipment and OSS suppliers. The intention is to also encourage system integrator usage of management systems that make use of the Interfaces.

In particular, the followed approach tends to minimize the cost of integration, provide access to all necessary information and control, and support all vendor/operator differentiation. The intent of the interface is to provide compatibility among different version, for a detailed description see SD2-6_VersioningAndExtensibility.

2.2.1 Service Provider Benefits

The service provider benefits are as follows:

- One stop shopping concerning feature requests for much of the TM Forum contract specification work is part of the defined Change Control Group (CCG) process that TM Forum makes available in order to control the interface.
- The technical deliverables are also of high value to the service provider. The Interface specifications allow for an open, multi-supplier environment, shorten delivery times and lower integration costs.
- The MTOSI and MTNM products provide an integrated, multi-technology interface with support for most key layer 1 and layer 2 transport technologies. This is in contrast to earlier approaches where

each technology-specific forum provided a single-technology management interface. The service provider was faced with having to use many different, uncoordinated management interfaces.

- These products are not bound to any one middleware, transport or computing language. So, the service provider will be able to evolve to new technologies as they arise.

2.2.2 Supplier Benefits

The supplier benefits are as follows:

- Fewer Adapters leads to Lower Costs – in as much as MTOSI and MTNM gain market penetration (and there has already been significant market acceptance of these interfaces), the supplier is faced with the need to build fewer adapters between their products and the products of their partners. A supplier can also directly see cost savings in the use of the Interfaces among its own products (as the need for an open interface arises).
- Lower Middleware Transitions Costs – the Interfaces are defined to be middleware and transport independent. So, the supplier can migrate from one middleware or transport technology to another without changing the supporting business logic in the code.
- Increase Usage by System Integrators (SIs) – a supplier's support of their own "open" interfaces goes only so far to encourage SIs. Clearly, an SI would like to make use of supplier products (both equipment and OSS suppliers) that make use of well supported standard interfaces rather than supplier specific interfaces. The latter case forces the SI into a situation characterized by many pair-wise negotiations between various suppliers.
- Lower Training Cost – in as much as a supplier re-uses the Interfaces for multiple products and for multiple customers, the various training costs are lower because the designers, system engineers, developers and testers are using the same Interfaces over and over again.

3 Business Processes

3.1 Category I: Static and Structural Requirements

3.1.1 Alarm Severity Assignment Profile (ASAP)

R_TMF518_NRA_I_0001	The ***Alarm Severity Assignment Profile (ASAP)*** object shall represent a set of severities that can be assigned to specific alarm probable causes. An ***ASAP*** is contained within an OS.
Source	TMF 513, Version 3.0, Requirement I 080

R_TMF518_NRA_I_0002	An ***ASAP*** object shall have, in addition to the attributes identified in requirement R_TMF518_NRB_I_0001, the following attributes: • ***fixed*** - this attribute shall indicate whether the ***ASAP*** is modifiable by an OS. If not, the ***ASAP*** can be neither modified nor deleted by an OS, but only assigned/de-assigned. • ***alarm severity assignment list*** - this attribute shall represent a list of Alarm Severity Assignments (ASA).
Source	TMF 513, Version 3.0, Requirement I 081

3.1.1.1 Alarm Severity Assignment (ASA)

R_TMF518_NRA_I_0003	The ***Alarm Severity Assignment (ASA)*** object shall represent the specific severities for the various service affecting conditions that are to be assigned to a specific alarm probable cause. An ***ASA*** has the following attributes: • ***probable cause*** - this attribute shall represent the name of a specific probable cause to which the severities are to be assigned. Refer to SD1-33. • ***probable cause qualifier*** - this attribute shall represent the probable cause qualifier and shall be present if the probable cause attribute is not sufficient to uniquely

	identify an alarm. OPTIONAL • ***native probable cause*** - this attribute shall represent the native probable cause. OPTIONAL • ***service affecting severity*** - this attribute shall represent the value to be assigned in the case where the reportable alarm is service affecting. • ***non-service affecting severity*** - this attribute shall represent the severity value to be assigned in the case where the reportable alarm is non-service affecting. • ***service independent severity*** - this attribute shall represent the severity value to be assigned in the case where the reportable alarm is service independent. This severity value may also be assigned in the case where the reporting OS is unable to determine whether the alarm is service affecting or not.
Source	TMF 513, Version 3.0, Requirement I 082

3.1.2 Performance Monitoring Point (PMP)

R_TMF518_NRA_I_0004	The ***Performance Monitoring Point (PMP)*** object shall represent an access point at which performance monitoring and threshold supervision are provided for a set of PM parameters. It is contained in a Termination Point (TP). All ***PMP***s contained in a TP constitute the PM capabilities of the containing TP.
Source	TMF 513, Version 3.0, Requirement I 084

R_TMF518_NRA_I_0005	A ***PMP*** object shall have, in addition to the attributes identified in requirement R_TMF518_NRB_I_0001, the following attributes: • ***layerRate*** - this attribute shall represent the layer rate of the ***PMP***. The layer specified must be supported by the containing TP. Refer to requirement R_TMF518_NRB_I_0003. • ***location*** - this attribute shall represent the location of the performance monitoring measurement. • ***granularity*** - this attribute shall represent the time granularity of the ***PMP***, either 15 minutes or 24 hours. This attribute is not applicable for instantaneous measurements (i.e. gauge type measurements). • ***supervision state*** - this attribute shall represent whether threshold supervision is enabled or disabled. • ***monitoring state*** - this attribute shall represent

	whether performance monitoring is enabled or disabled. • ***pm parameter list*** - this attribute shall represent a list of the names of the PM parameters associated with the ***PMP***. Refer to SD1-28 for the list of currently defined performance parameters. • ***pm threshold list*** – this attribute shall represent a list of the names of the thresholds associated with each PM parameter. Refer to R_TMF518_NRA_I_0006.
Source	TMF 513, Version 3.0, Requirement I 085

3.1.2.1 PM Threshold

R_TMF518_NRA_I_0006	The ***PM Threshold*** object shall represent the specific severities for the various service affecting conditions that are to be assigned to a specific alarm probable cause • ***threshold type*** - this attribute shall represent the type of the PM threshold, (shall indicate the level at which the threshold is triggered or cleared). • ***trigger*** - this attribute shall indicate whether the PM threshold shall trigger a “raise” or a “clear” Threshold Crossing Alert. • ***value*** - this attribute shall represent the value for the PM threshold parameter. • ***measurement units*** - this attribute shall represent the unit of measurement for the PM threshold parameter.
Source	TMF 513, Version 3.0, Requirement I 099

3.1.3 Equipment Protection Group (EPG)

R_TMF518_NRA_I_0007	The ***Equipment Protection Group (EPG)*** object shall represent Equipment protection.
Source	TMF 513, Version 3.0, Requirement I 072

R_TMF518_NRA_I_0008	An ***EPG*** object shall have, in addition to the attributes identified in requirement R_TMF518_NRB_I_0001, the following attributes: • ***protection type*** - this attribute shall represent the type of the ***EPG*** (e.g. M:N). • ***protection scheme state*** -this attribute shall indicate the current state of the protection scheme (i.e. whether it is active or locked).

	• ***reversion mode*** - this attribute shall indicate whether the protection scheme is revertive or not. • ***protected equipment list*** - these attribute shall represent a list of the protected Equipment instances. • ***protecting equipment list*** - this attribute shall represent a list of the protecting Equipment instances. • ***pg parameter list*** - this attribute shall represent the ***EPG*** specific parameters. For example SwitchMode, SwitchPosition, wait to restore time, etc. • ***alarm severity assignment profile*** - this attribute shall represent the name of the Alarm Severity Assignment Profile (ASAP) that has been assigned to the ***EPG***.
Source	TMF 513, Version 3.0, Requirement I 073

3.1.4 Protection Group

R_TMF518_NRA_I_0009	The ***Protection Group (PG)*** object shall represent trail protection schemes.
Source	TMF 513, Version 3.0, Requirement I 034

R_TMF518_NRA_I_0010	A ***PG*** object shall have, in addition to the attributes identified in requirement R_TMF518_NRB_I_0001, the following attributes: • ***type*** - this attribute shall represent the type of the ***PG***. • ***protection scheme state*** - this attribute shall indicate the current state of the protection scheme (i.e. whether it is active or locked). • ***reversion mode*** - this attribute shall indicate whether the protection scheme is revertive or not. • ***layer rate*** - refer to requirement R_TMF518_NRB_I_0003. • ***protection related PTP list*** - this attribute shall represent a list of the Physical Termination Points (PTP) related by the ***PG***. • ***pg parameter list*** - this attribute shall represent the ***PG*** specific parameters (e.g. switch mode, switch position, wait to restore time, etc.). • ***aps protocol type*** - this attribute shall indicate the type of APS protocol supported by the ***PG***. • ***alarm severity assignment profile*** - this attribute shall represent the name of the Alarm Severity Assignment Profile (ASAP) that has been assigned to the ***PG***.

Source	TMF 513, Version 3.0, Requirement I 066

3.1.5 Threshold Crossing Alert (TCA) Parameter Profile

R_TMF518_NRA_I_0011	A ***Threshold Crossing Alert (TCA) Parameter Profile*** object shall represent for a specific layer rate a set of Threshold Crossing Alert (TCA) Parameters associated with a set of Termination Point (TP)s.
Source	TMF 513, Version 3.0, Requirement I 067

R_TMF518_NRA_I_0012	A ***TCA Parameter Profile*** object shall have, in addition to the attributes identified in requirement R_TMF518_NRB_I_0001 , the following attributes: • ***layer rate*** - this attribute shall represent the layer to which the PM threshold values apply. (Refer to R_TMF518_NRB_I_0003). • ***associated TP list*** - this attribute shall represent a list of the Termination Points (TP) that are associated with the ***TCA Parameter Profile***. • ***tca parameter list*** - this attribute shall represent a list of Threshold Crossing Alert (TCA) Parameters.
Source	TMF 513, Version 3.0, Requirement I 087

3.1.6 Threshold Crossing Alert (TCA) Parameters

R_TMF518_NRA_I_0013	A ***Threshold Crossing Alert (TCA) Parameter*** object shall represent the the TCA parameters contained with a Threshold Crossing Alert (TCA) Parameter Profile.
Source	TMF 513, Version 3.0, Requirement I 088

R_TMF518_NRA_I_0014	A ***TCA Parameter*** object shall have the following attributes: • ***name*** - this attribute shall represent the name of the TCA parameter. Refer to SD1-28 for the currently defined ***TCA parameter*** names. • ***granularity*** - this attribute shall represent the time granularity of the ***TCA parameter***, either 15 minutes or 24 hours. This attribute is not applicable for instantaneous measurements (i.e. gauge type measurements). • ***location*** - this attribute shall represent the location of

	the ***TCA parameter*** relative to the signal flow. • ***threshold type*** - this attribute shall represent the type of the ***TCA parameter***, (shall indicate the level at which the threshold is triggered or cleared). Refer to SD1-37 for more details of the threshold type. • ***trigger*** - this attribute shall indicate whether the threshold type shall trigger a "raise" or a "clear" TCA. • ***value*** - this attribute shall represent the value for the ***TCA parameter***. • ***measurement units*** - this attribute shall represent the unit of measurement for the ***TCA parameter***.
Source	TMF 513, Version 3.0, Requirement I 035

3.1.7 Notifications

Table 3-1 identifies the different specific event types that have been defined for this Interface.

Table 3-1: Event Notification Types

	Event
1	Threshold Crossing Alert (TCA) Notification
2	Alarm Notification
3	Performance Monitoring Point (PMP) State Change Notification
4	Protection Switch Notification
5	Equipment Protection Switch

3.1.7.1 Access Identifier (AID)

There are certain alarm conditions that an OS may wish to report for which there is no explicit object modeled across the Interface (i.e. there is no specific object type defined). Under these conditions the OS shall use the "AID" object type.

R_TMF518_NRA_I_0015	The Interface shall allow an OS to generate alarms against objects that are not explicitly modeled in the Interface by using the "AID" objectType. The OS that generates the alarm shall ensure that all such entities have a unique value for the AID within the containing Network Element (NE).
Source	TMF513, Version 3.0, Requirement I.057

3.1.7.2 Threshold Crossing Alert (TCA) Notification

R_TMF518_NRA_I_0016	A ***Threshold Crossing Alert (TCA)*** notification is an event used across the Interface to indicate that a performance

	monitoring parameter threshold has been crossed. A ***TCA*** notification shall have in addition to the attributes identified in R_TMF518_FMW_I_0011 the following attributes: • ***edge point related*** - this attribute shall indicate whether the event is related to a Termination Point (TP) at the edge of a subnetwork. (Refer to R_TMF518_NRF_I_0008) • ***alias name list*** – this attribute shall represent a list of zero or more alias names for the object whose threshold has been crossed. The native EMS name is an example of one such alias. • ***clearable*** – refer to R_TMF518_NRA_I_0019. • ***perceived severity*** – this attribute shall indicate (when the ***TCA*** is reported as an alarm) whether it is a raise (value shall be INDETERMINATE) or a clear (value shall be CLEARED) alarm. • ***layer rate*** – this attribute shall indicate the layer at which the threshold was crossed. Refer to R_TMF518_NRB_I_0003. • ***granularity*** – this attribute shall represent the time granularity of the ***TCA***, either 15 minutes or 24 hours. This attribute is not applicable for instantaneous measurements (i.e. gauge type measurements). • ***parameter name*** – refer to R_TMF518_NRA_I_0014. • ***parameter location*** - refer to R_TMF518_NRA_I_0014. • ***threshold type*** – refer to R_TMF518_NRA_I_0014. • ***value*** - refer to R_TMF518_NRA_I_0014. • ***measurement units*** - refer to R_TMF518_NRA_I_0014. • ***acknowledgement*** –refer to R_TMF518_NRA_I_0025.
Source	TMF513 Version 3.0, Requirement I.047

3.1.7.3 Alarm Notification

R_TMF518_NRA_I_0017	An ***Alarm Notification*** is an event used across the Interface to indicate that a fault condition has occurred. An Alarm Notification shall have in addition to the attributes identified in R_TMF518_FMW_I_0011 the following attributes: • ***edge point related*** - this attribute shall indicate whether the event is related to a Termination Point (TP) at the edge of a subnetwork. (Refer to R_TMF518_NRF_I_0008)

	• ***clearable*** – refer to R_TMF518_NRA_I_0019 • ***layer rate*** – this is the layer rate at which the alarm occurred. • ***probable cause*** – refer to R_TMF518_NRA_I_0020. • ***perceived severity*** – refer to R_TMF518_NRA_I_0021. • ***service affecting*** – refer to R_TMF518_NRA_I_0022. • ***probable cause qualifier*** – refer to R_TMF518_NRA_I_0018. OPTIONAL • ***affected PTP list*** – this attribute shall in the case of equipment related alarms represent the names of the affected Physical Termination Point (PTP) implemented by the alarmed equipment. OPTIONAL. • ***additional text*** – see R_TMF518_NRA_I_0024. OPTIONAL. • ***alias name list*** - this attribute shall represent a list of zero or more alias names for the object whose threshold has been crossed. The native EMS name is an example of one such alias OPTIONAL. • ***native probable cause*** – this attribute shall represent the value of the probable cause shown on the user interface of the OS sending the alarm. OPTIONAL. • ***acknowledgement*** – see R_TMF518_NRA_I_0025. • ***root cause alarm indication*** – this attribute shall indicate whether the alarm is a raw (un-correlated) alarm or a root cause alarm indication. • ***x.733 event type*** – this attribute shall represent the classification of the alarm in terms of the categories specified in ITU-T X.733. This is consistent with the ITU-T X.733 definition. OPTIONAL. • ***x.733 specific problems*** – this attribute shall represent a clarification of the Probable Cause of the alarm. This is similar to Probable Cause Qualifier, but this attribute is designed to be human readable and compatible with ITU usage. This is consistent with the ITU-T X.733 definition. OPTIONAL • ***x.733 backed-up status*** – this attribute shall represent whether or not the object emitting the alarm has been backed-up, and services provided to the user have, therefore, not been disrupted. This is consistent with the ITU-T X.733 definition OPTIONAL • ***x.733 back-up object*** – this attribute shall represent the object that is providing back-up services for the object to which the alarm notification pertains. This attribute shall be present when the ***x.733 backed-up***

	status attribute is present and indicates that the object has been backed up. This is consistent with the ITU-T X.733 definition. OPTIONAL. • ***x.733 trend indication*** – this attribute shall represent the current severity trend of the object it indicates that there are one or more alarms ("outstanding alarms") which have not been cleared, and pertain to the same object as that to which this alarm ("current alarm") pertains. This is consistent with the ITU-T X.733 definition. OPTIONAL • ***x.733 correlated notification list*** – this attribute shall represent a list of notification identifiers and, if necessary, their associated object names. This list is defined to be the set of all notifications to which this notification is considered to be correlated. The source object name shall be present if the correlated event report is from an object other than the one in which the ***correlated notification list*** attribute is present. Otherwise it shall be empty. This is consistent with the ITU-T X.733 definition. OPTIONAL. • ***x.733 monitored attribute list*** – this attribute shall represent the one or more attributes of the managed object and their corresponding values at the time of the alarm. This is consistent with the ITU-T X.733 definition. OPTIONAL. • ***x.733 proposed repair action list*** – this attribute shall represent one or more possible solutions (such as switch in standby equipment, retry, replace media, etc.). This is consistent with the ITU-T X.733 definition. OPTIONAL. • ***x.733 additional information*** – this attribute shall represent a set of additional information in an alarm notification. The same information can be directly encoded as separate parameters of the notification. However, this parameter is retained for consistency with ITU-T X.733. OPTIONAL.
Source	TMF513 Version 3.0, Requirement I.048

R_TMF518_NRA_I_0018	The ***probable cause qualifier*** attribute, when present, identifies further refinements to the ***probable cause*** attibute of the alarm, so as to correlate the "raise" and "clear" notifications of the same fault condition in case of ambiguity (i.e., when several different fault conditions give rise to the same values). This parameter gives more detail about the alarm, e.g., it may further qualify the source. Refer to R_TMF518_NRA_I_0023.
Source	TMF513 Version 3.0, Requirement I.049

R_TMF518_NRA_I_0019	An indication is required as to whether an alarm raise event will

	have an associated alarm clear event. If an alarm clear event is generated then the alarm is defined to be ***clearable***. The same distinction is used in the Threshold Crossing Alert (TCA) Notification.
Source	TMF513 Version 3.0, Requirement I.050

R_TMF518_NRA_I_0020	The ***probable cause*** attribute shall allow the reporting OS to indicate the likely cause of the alarm. Refer to SD1-33 for the currently specified probable cause names.
Source	TMF513 Version 3.0, Requirement I.051

R_TMF518_NRA_I_0021	The ***perceived severity*** attribute has the following values: • critical • major • minor • warning • cleared • indeterminate
Source	TMF513 Version 3.0, Requirement I.052

R_TMF518_NRA_I_0022	The ***service affecting*** attribute shall provide the alarm generating OS' determination of whether or not the condition affects service. The possible values for this attribute are: • service affecting • not service affecting • unknown as to whether it is service affecting.
Source	TMF513 Version 3.0, Requirement I.053

R_TMF518_NRA_I_0023	An instance of an alarm shall be uniquely identifiable if: • the ***object name***, ***layer*** and ***probable cause*** attribute values can uniquely correlate clears with raises. In this case, the ***probable cause qualifier*** is left empty (default value). • the ***object name***, ***layer*** and ***probable cause*** attribute values are not sufficient to uniquely correlate clears with raises. In this case, the ***probable cause qualifier*** attribute needs to be populated. It contains information such that any clear of that alarm can be correlated to the raise. This means that if the alarm is raised, cleared, raised again,

	and cleared again, if the original clear and second alarm were missed, the second clear would clear the first alarm.
Source	TMF513 Version 3.0, Requirement I.054

R_TMF518_NRA_I_0024	The optional ***additional text*** attribute shall allow a free form text description to be reported.
Source	TMF513 Version 3.0, Requirement I.056

R_TMF518_NRA_I_0025	The ***acknowledgement*** attribute shall have the following possible values: • Not applicable – this indicates that the reporting OS (i.e., the OS that generated the alarm or TCA) does not support acknowledgement for this event or does not support acknowledgement at all. • Acknowledged – this indicates that the alarm has been acknowledged in the reporting OS. All alarm fields other thanOS time and acknowledge indication shall remain similar to the original alarm notification. (The OS time is always provided as the time that the alarm acknowledgement notification has been reported by the reporting OS.) • Unacknowledged – this indicates that the alarm has not been acknowledged by the reporting OS, or in the event that the alarm has been previously acknowledged and then unacknowledged. All alarm fields other than osTime shall remain in that case similar to the original alarm notification. (The osTime is always provided as the time that the alarm acknowledgement notification has been reported by the reporting OS.)
Source	TMF513 Version 3.0, Requirement I.071

3.1.7.4 Performance Monitoring Point (PMP) State Change Notification

R_TMF518_NRA_I_0026	A ***Performance Monitoring Point (PMP)*** State Change Notification is a special type of State Change Notification event used across the Interface to indicate the following: • PM data has been cleared • PM data collection has been disabled or enabled • TCA generation has been enabled or disabled. This notification is used to report only one type of change at a time. The reporting OS shall not use both this notification and individual PMP state change notifications to report the same event.

	This notification and an attribute value change notification on a PMP may be used interchangeably by the reporting OS on individual PMPs and at other times on a list of PMPs. A PMP State Change Notification shall have in addition to the attributes identified in R_TMF518_FMW_I_0010 the following attributes: • ***pmp name list*** – this attribute shall represent a list of the PMP name(s) for which a state attribute has changed its value. • ***attribute value list*** – this attribute shall represent a list of the state attribute name(s) that have changed their value along with their new values. • ***OS time*** – this attribute shall represent the time at which the event occurred at the reporting OS. Note: Assumes that the ***source time*** attribute is the time at which the event occurred in the NE.
Source	TMF513 Version 3.0, Requirement I.083

3.1.7.5 Protection Switch Notification

R_TMF518_NRA_I_0027	A ***Protection Switch Notification*** is an event used across the Interface to indicate that a protection switch has occurred. A ***Protection Switch Notification*** shall have in addition to the attributes identified in R_TMF518_FMW_I_0010 the following attributes: • ***protection type*** – this attribute shall represent the type of the protection for which the switch has occurred. • ***switch reason*** – this attribute shall represent the reason for the switch. • ***layer rate*** – this attribute shall represent the layer at which the switch has occurred. • ***protection group*** – this attribute shall represent the name of the Protection Group (PG) in the case of a trail switch. Not used if the protection type is Subnetwork Connection Protection (SNCP). • ***protected TP*** – this attribute shall represent the name of the Termination Point (TP) being protected. • ***switch away from TP*** – this attribute shall represent the name of the TP being switched away from. • ***switch to TP*** – this attribute shall represent the name of the TP that is switched to. • ***OS time*** – this attribute shall represent the time at which the event occurred at the OS.

Source	Amended from TMF513 v3.0, Requirement I.046

3.1.7.6 Equipment Protection Switch

R_TMF518_NRA_I_0028	An ***Equipment Protection Switch Notification*** is an event used across the Interface to indicate that an equipment protection switch has occurred. An ***Equipment Protection Switch Notification*** shall have in addition to the attributes identified in R_TMF518_FMW_I_0010 the following attributes: • ***protection type*** – this attribute shall represent the type of the protection for which the switch has occurred. • ***switch reason*** – this attribute shall represent the reason for the switch. • ***equipment protection group*** – this attribute shall represent the name of the Equipment Protection Group (EPG). • ***protected equipment*** – this attribute shall represent the name of the Equipment being protected. • ***switch away from equipment*** – this attribute shall represent the name of the Equipment being switched away from. • ***switch to equipment*** – this attribute shall represent the name of the Equipment that is switched to. • ***OS time*** – this attribute shall represent the time at which the event occurred at the OS.
Source	Amended from TMF513 v3.0, Requirement I.074

3.2 Category II: Normal Sequences, Dynamic Requirements

Not Applicable.

3.3 Category III: Abnormal or Exception Conditions, Dynamic Requirements

Not Applicable.

3.4 Category IV: Expectations and Non-Functional Requirements

Not Applicable.

3.5 Category V: System Administration Requirements

Not Applicable.

4 Use Cases

Not Applicable.

5 Traceability Matrices

Not Applicable.

6 Future Directions

None identified at this time.

7 References

7.1 References

[1] TMF513, Multi-Technology Network Management (MTNM) Business Agreement, Version 3.1, March 2007

[2] TMF518_FMW, Framework DDP-BA

[3] SD1-28, Performance Parameters

[4] SD1-33, Specification of Probable Cause Strings

[5] SD1-37, PM Threshold Types

[6] SD0-1, Dictionary

7.2 IPR Releases and Patent Disclosure

There are no known IPR claims on the material in this document. As per the TM Forum bylaws, any TM Forum member company that has IPR claims on this or any TM Forum specification needs to make the claims known to the TM Forum membership immediately.

8 Administrative Appendix

This Appendix provides additional background material about the TM Forum and this document.

8.1 About this document

This document has been generated from the SD0-3_Template_BA.dot Word template.

8.2 Use and Extension of a TM Forum Business Agreement

This document defines the business problem and requirement model for resource assurance. The Business Agreement is used to gain consensus on the business requirements for exchanging information among processes and systems in order to solve a specific business problem. The Business Agreement should feed the development of Information Agreement(s), which is a technology-neutral model of one or more interfaces. While the Business Agreement contains sufficient information to be a "stand alone" document, it is better read together with the Information Agreement document TMF612_NRA when the Information Agreement is available. Reviewing the two documents together helps in gaining a full understanding of how the technology neutral information model solution is defined for this requirement model. An initial Business Agreement may only deal with a subset of the requirements. It is acceptable for subsequent issues of the document to add additional requirements not addressed by earlier releases of the BA. Business Agreements are the basis for requirement traceability for information models.

- It is expected that this document will be used:
- As the foundation for a TM Forum Information Agreement(s)
- To facilitate requirement agreement between Service Providers and vendors
- As input to a service Provider's Request for Information / Request for Proposal (RFI/RFP—RFX)
- As input for vendors developing COTS products
- As a source of requirements for other bodies working in this area

8.3 Document History

Version	Date Modified	Description of changes
1.0	September 2007	This is the first version of the document and as such, there are no changes to report.
1.1	May 2008	Updated based on review and consolidation comments for the preparation of the MTOSI 2.0 release.

1.2	September 2011	Updated sections 1.1 and 2. Replaced mTOP by MTNM / MTOSI everywhere in the document.

8.4 Company Contact Details

Document Contact
Keith Dorking
Ciena Corporation
Email: kdorking@ciena.com
Phone: +1 678 867 5007