



Mplify Standard
Mplify 173

CIM Notification Service
Business Requirements and Use Cases

October 2025

Disclaimer

© Mplify Alliance 2025. All Rights Reserved.

The information in this publication is freely available for reproduction and use by any recipient and is believed to be accurate as of its publication date. Such information is subject to change without notice and Mplify Alliance (Mplify) is not responsible for any errors. Mplify does not assume responsibility to update or correct any information in this publication. No representation or warranty, expressed or implied, is made by Mplify concerning the completeness, accuracy, or applicability of any information contained herein and no liability of any kind shall be assumed by Mplify as a result of reliance upon such information.

The information contained herein is intended to be used without modification by the recipient or user of this document. Mplify is not responsible or liable for any modifications to this document made by any other party.

The receipt or any use of this document or its contents does not in any way create, by implication or otherwise:

- a) any express or implied license or right to or under any patent, copyright, trademark or trade secret rights held or claimed by any Mplify member which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor
- b) any warranty or representation that any Mplify members will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor
- c) any form of relationship between any Mplify member and the recipient or user of this document.

Implementation or use of specific Mplify standards, specifications, or recommendations will be voluntary, and no Member shall be obliged to implement them by virtue of participation in Mplify Alliance. Mplify is a global alliance of network, cloud, cybersecurity, and enterprise organizations working together to accelerate the AI-powered digital economy through standardization, automation, certification, and collaboration. Mplify does not, expressly or otherwise, endorse or promote any specific products or services.

Table of Contents

1	List of Contributing Members	1
2	Abstract.....	1
3	Terminology and Acronyms.....	2
4	Scope.....	4
5	Compliance Levels	5
6	Introduction.....	6
7	CIM Notification Service Use Cases and Business Process Definitions	8
7.1	High-Level Use Cases	8
7.2	CIM Notification Service API Use Cases	9
7.2.1	Failure Notification Use Case.....	12
7.2.2	Service Impairment Notification Use Case.....	13
7.2.3	Maintenance Notification Use Case.....	15
7.2.4	Register for CIM Notifications Use Case	17
7.2.5	Send CIM Notification Use Case.....	18
8	Additional Trouble Ticketing Requirements	20
8.1	Trouble Ticketing Use Cases.....	20
8.2	Incident Type Values.....	21
8.3	Retrieve CIM Incident List.....	22
8.4	Register for Event Notifications	22
9	Incident Values and State Diagrams [Informative]	23
9.1	Incident Impact Values	23
9.2	Incident Process Flow.....	24
10	References.....	26
Appendix A	Acknowledgements	27

List of Figures

Figure 1 - LSO Reference Architecture Diagram	6
Figure 2 - CIM Notification Service API Use Cases	9
Figure 3 - Relevant Trouble Ticketing API - Incident Use Cases	10
Figure 4 - Incident Process Flow	24

List of Tables

Table 1 - Terminology	3
Table 2 - Abbreviations	3
Table 3 - CIM Notification Service API Use Cases	9
Table 4 - Relevant Trouble Ticketing API – Incident Use Cases	11
Table 5 - Failure Notification	12
Table 6 - Service Impairment Notification	13
Table 7 - Maintenance Notification	15
Table 8 - Register for CIM Notifications.....	17
Table 9 - Send CIM Notification	18
Table 10 - Additional Incident Type Values.....	21
Table 11 - Incident Impact Values.....	23
Table 12 - Incident State Values	24
Table 13 - Event Notification Type Values	25

1 List of Contributing Members

The following members of Mplify participated in the development of this document and have requested to be included in this list.

- Amartus
- Bloomberg
- Prodapt
- Sage Management

2 Abstract

This document identifies the common Use Cases and attributes needed to support the Circuit Impairment and Maintenance (CIM) Notification Service at the LSO Sonata/Cantata Interface Reference Point.

This document leverages the requirements defined in MEF 113 Trouble Ticketing Business Requirements and Use Cases [6] between business applications of a Buyer and a Seller at the LSO Sonata/Cantata Interface Reference Point, by providing the Buyer timely fault management and maintenance information to enable faster response to impairments and outages on the Seller's network. Information contained within this document will be utilized by both the Buyer and Seller.

3 Terminology and Acronyms

This section defines the terms used in this document. In many cases, the normative definitions to terms are found in other documents. In these cases, the third column is used to provide the reference that is controlling, in other Mplify or external documents.

In addition, terms defined in MEF 10.4 [3], MEF 50.1 [4], MEF 55.1.1 [5], and MEF 113 [6] are included in this document by reference and are not repeated in the table below.

Term	Definition	Reference
Circuit Impairment and Maintenance Notification Service	A standards based fault management and maintenance API service provided by a Seller to a Buyer that provides timely notifications of Failure Situations, Service Impairments and Planned Maintenance on the Seller's network.	This document
Incident	An entry within a Seller's tracking system created by the Seller, which contains information about a Situation in the Seller's network that has a possible negative impact on the operability of a Product for one or more Buyers. (Note: Incidents and Tickets are similar entries in a Seller's tracking system, with a key difference that an Incident is created by the Seller about a Situation that may impact one or more Buyers, whereas a Ticket is created by the Buyer about an Issue impacting normal operation of a Product.)	MEF 113 [6]
Issue	In the context of this document, denotes a problem with a Product as experienced by the Buyer that is not part of normal operation.	MEF 113 [6]
Notification	A message sent from the Seller to the Buyer to inform about an event that has occurred in regard to a specific instance of an Incident.	Adapted from MEF 113 [6]
Planned Maintenance	Any scheduled maintenance to be performed by the Seller that may impact a Product for the Buyer, which also includes the planned ending time and date.	This document
Product Identifier	A unique identifier provided by the Seller during activation to refer to the Product on which an Incident could have an impact on the normal operation for a Buyer. (Note: For circuit-based Mplify products, the Product Identifiers in Incidents and Tickets corresponds to the impacted circuit IDs.)	MEF 113 [6]

Term	Definition	Reference
Failure Situation	The Seller detects an occurrence of a Situation on a Product provided to the Buyer, where the Product is non-operational (for example, down, routing failures, severe packet drops, etc.).	This document
Service Impairment	The Seller detects an occurrence of a Situation on a Product provided to the Buyer, where the Product is not meeting the Product specifications or is not operational on an intermittent basis. This includes impairments due to traffic violating traffic profile thresholds (for example, excessive traffic drops due to policing) and/or traffic congestion exceeding thresholds.	This document
Situation	In the context of this document, denotes a problem that is not part of normal operation in the Seller's network.	MEF 113 [6]
Ticket	An entry within a Seller's tracking system created by the Buyer (or a third party on behalf of the Buyer), which contains information about an Issue impacting normal operation of a Product, along with support interventions made by technical support staff, or third parties.	MEF 113 [6]

Table 1 - Terminology

Abbreviations	Definition	Reference
CIM	Circuit Impairment and Maintenance	This document

Table 2 - Abbreviations

4 Scope

This document defines the process for CIM Notification Service between a Seller and Buyer. This document is limited to the business process requirements depicted as Use Cases and attribute definitions needed for the CIM Notification Service.

5 Compliance Levels

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 (RFC 2119, RFC 8174) when, and only when, they appear in all capitals, as shown here. All key words must be in bold text.

Items that are **REQUIRED** (contain the words **MUST** or **MUST NOT**) are labeled as [Rx] for required. Items that are **RECOMMENDED** (contain the words **SHOULD** or **SHOULD NOT**) are labeled as [Dx] for desirable. Items that are **OPTIONAL** (contain the words **MAY** or **OPTIONAL**) are labeled as [Ox] for optional.

6 Introduction

This document defines the business requirements and process-related guidelines for CIM Notification Service over the Sonata/Cantata Interface Reference Point. The Sonata/Cantata Interface Reference Point is defined in MEF 55.1 [5] as the Management Interface Reference Point supporting the management and operations interactions (e.g., ordering, billing, trouble ticketing, etc.) between two network providers (e.g., Service Provider Domain and Partner Domain) or between a Customer Domain and a Service Provider Domain. The scope of this document is limited to interactions between these parties; within this document, they are referred to as the “Buyer” and the “Seller”.

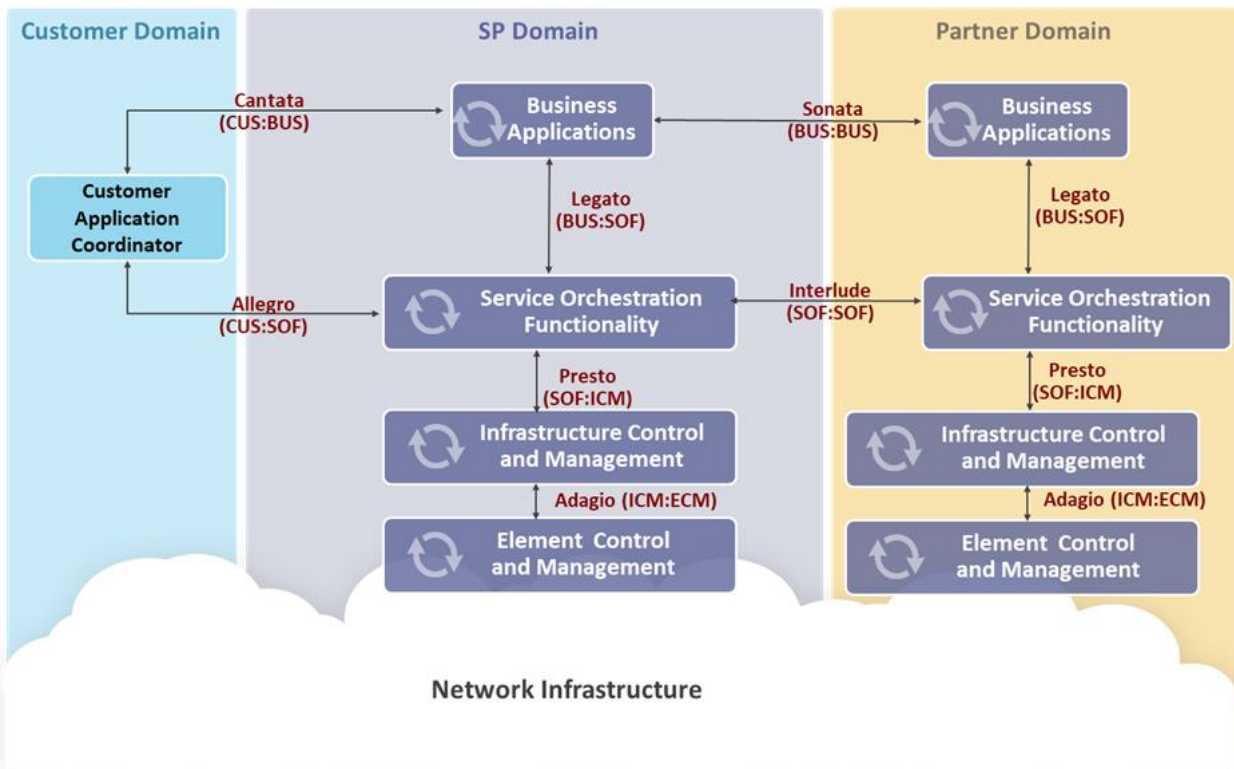


Figure 1 - LSO Reference Architecture Diagram

Figure 1 depicts the LSO Reference Architecture, per MEF 55.1 [5]. This document addresses the interactions between the business applications of the Buyer and Seller at the Sonata/Cantata Interface Reference Point required to support the CIM Notification Service.

Enterprises buying connectivity services from a retail service provider (Seller) are very dependent on the high availability of those connectivity services and their real-time performance, as any downtime or service interruption can result in lost productivity, loss revenue, and damage to the Buyer’s reputation. Changes in availability and performance are often unavoidable – e.g. because of scheduled maintenance or because of an internal failure within the Seller’s network or within the network of one of the downstream wholesale connectivity suppliers. Buyers therefore need to be able to respond quickly to outages and may need to reorganize their activities for any upcoming maintenance windows, so that they can minimize the impact on their operations. Advance, or at

least timely, and accurate information from the retail service provider Seller is critically important for the enterprise Buyer planning and operations.

The associated “patterns” to the interactivity between Buyer and Seller for the CIM Notification Service is based on the Seller sending CIM Notifications to the Buyer to provide timely information regarding Planned Maintenance, Failure Situations and Service Impairments in the Seller’s network impacting performance and/or availability, whenever the Seller creates, updates or closes an Incident.

Note: The Buyer at any time may retrieve a summary list of CIM related Incidents based on a specified filter criteria, or may retrieve detailed information about a single Incident to get the details and status of the Situation.

To fully define the business interactions associated with the CIM Notification Service, this document is focused on the following key areas:

- CIM Notification Service Use Cases and Business Requirements
- Relevant Trouble Ticketing - Incident Use Cases and Business Requirements
- Additional Trouble Ticketing - Incident Business Requirements

Incidents are used by the Seller to inform Buyers about Situations in the Seller’s network that have a possible impact on the operability of a Product for one or more Buyers. An Incident contains various attributes that includes a list of Product Identifiers, along with attributes such as Incident Impact, Incident Type, Incident State and others (see MEF 113 [6] Table 37 - Incident Attributes for details). For circuit-based Mplify products, the Product Identifiers is a list of impacted circuit IDs, since an Incident may apply to multiple circuits.

Note: A Buyer will only receive CIM Notifications for CIM related Incidents impacting Products they have Activated with the Seller. When a Buyer receives a CIM Notification they could, for example, use that Incident details to help plan around the Situation, or to create a new Ticket, or to defer creating new Tickets (e.g. wait for the Incident corresponding to a CIM Notification to be closed by the Seller) or update one or more existing Tickets whenever a CIM Notification is received.

7 CIM Notification Service Use Cases and Business Process Definitions

7.1 High-Level Use Cases

This section provides the set of Use Cases needed to support the CIM Notification Service API. These Use Cases are based on business process standards of interactivity between Buyers and Sellers of Products and are defined using the MEF 113 Trouble Ticketing Business Requirements and Use Cases [6] with an additional set of requirements and specific usage of attributes for the Use Case as defined in section 8.

Prior arrangements for Buyer authentication, security verification, and system interface requirements are not addressed within these use cases. The authentication, security profile, security approaches and security architecture based on OAuth2 and OIDC are defined in MEF 128.1 [7], and as such are not detailed in this specification.

All onboarding requirements must be defined and negotiated between the Buyer and Seller prior to applying the CIM Notification Service Use Cases defined in this section.

CIM Notification Service API Overview:

- The CIM Notification Service API supports registering and receiving CIM Notifications and retrieving Incident details between a Buyer and Seller as a result of a Situation for a Product provided by the Seller.
- The CIM Notification Service Use Cases and Requirements are not defined in regard to any particular Product specifications, and thus the Buyer will be able to register and receive CIM Notifications on any Activated Product supported by the Seller using the Use Cases defined in this document.

7.2 CIM Notification Service API Use Cases

This section defines the CIM Notification Service API use cases and interactions between the Buyer and Seller.

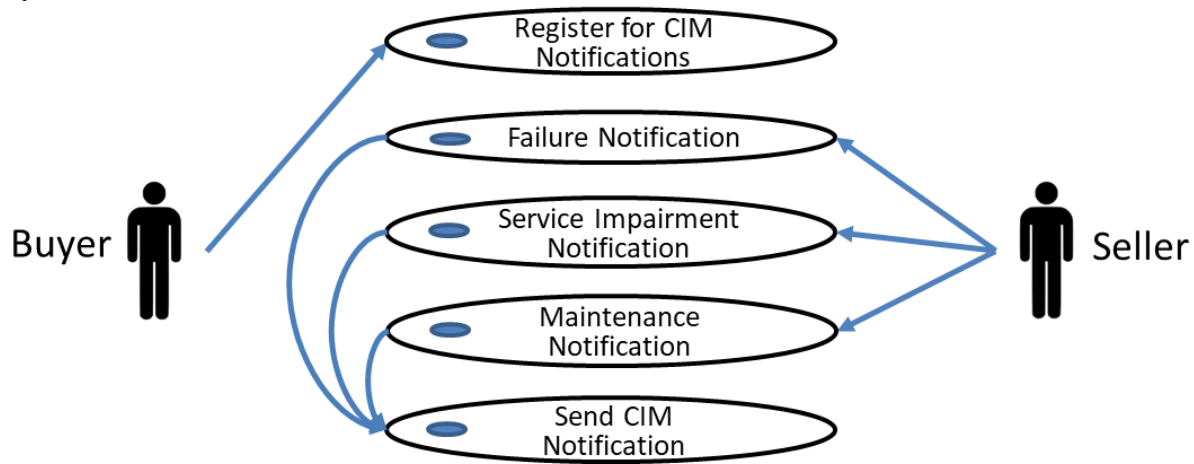


Figure 2 - CIM Notification Service API Use Cases

Use Case #	Use Case Name	Use Case Description
1	Failure Notification	The Seller notifies the Buyer when a Failure Situation occurs on a Product.
2	Service Impairment Notification	The Seller notifies the Buyer when a Service Impairment occur on a Product.
3	Maintenance Notification	The Seller notifies the Buyer about a Planned Maintenance that could impact the operation of a Product.
4	Register for CIM Notifications	The Buyer requests to subscribe to CIM Notifications from a Seller.
5	Send CIM Notification	The Seller sends a CIM Notification regarding an Incident to the Buyer.

Table 3 - CIM Notification Service API Use Cases

The figure and table below show the relevant MEF 113 Trouble Ticketing Incident Use Cases that are used to support the CIM Notification Service API Use Cases described above.

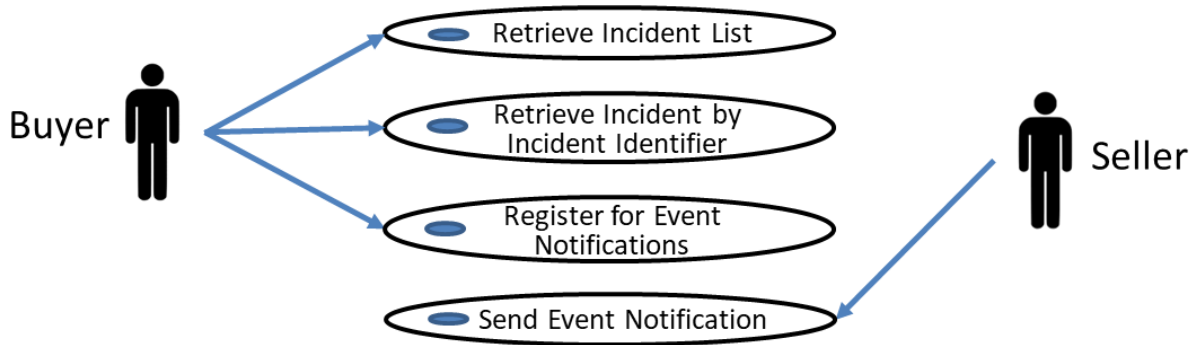


Figure 3 - Relevant Trouble Ticketing API - Incident Use Cases

Use Case #	Use Case Name	Use Case Description
MEF 113 [6] 15	Retrieve Incident List	The Buyer requests a list of Incidents from the Seller based on a set of specified filter criteria. The Seller returns a summarized list of Incidents. Only the following Incident Types are applicable for CIM: • CIM_FAILURE • CIM_POLICING • CIM_CONGESTION • CIM_PLANNED_MAINTENANCE
MEF 113 [6] 16	Retrieve Incident by Incident Identifier	The Buyer requests detailed information about a single Incident based on an Incident Identifier.
MEF 113 [6] 17	Register for Event Notifications	The Buyer requests to subscribe to Incident Notifications. Only the following Notification Type is applicable for CIM Notifications: • INCIDENT For the List of Event Notification Types, only a list of one or more of the following is applicable for CIM Notifications: • INCIDENT_CREATE • INCIDENT_UPDATE • INCIDENT_STATE_CHANGE

Use Case #	Use Case Name	Use Case Description
MEF 113 [6] 18	Send Event Notification	The Seller sends a notification regarding an Incident to the Buyer indicating that a specific event has occurred. Only the following Event Notification Types are applicable for CIM Notifications: • INCIDENT_CREATE • INCIDENT_UPDATE • INCIDENT_STATE_CHANGE

Table 4 - Relevant Trouble Ticketing API – Incident Use Cases

7.2.1 Failure Notification Use Case

The Failure Notification Use Case is detailed in this section.

Field	Description
Use Case Number	1
Use Case Name	Failure Notification
Description	Anytime the Seller detects an occurrence of a Failure Situation on a Product provided to the Buyer, the Seller will send a Failure Notification to the Buyer. The Incident details includes information about the nature of the Failure Situation and may include the expected closed date and time.
Actors	Buyer/Seller
Pre-Conditions	1. The Buyer has registered for CIM Notifications (as specified in section 7.2.4). 2. The Seller has detected a new Failure Situation on an Activated Product impacting the Buyer.
Process Steps	1. The Seller creates an Incident of Incident Type CIM_FAILURE and Incident Impact DOWN. 2. The Seller issues a Send CIM Notification for the Incident to the Buyer (as specified in section 7.2.5).
Post-Conditions	The Buyer has detailed information on the specific Failure Situation as described in the Incident, along with any IN_PROGRESS updates, including progress update notes, expected closed date/time and will be notified when the Incident is closed. 1. The Seller updates the Incident State to CLOSED. 2. The Seller issues a Send CIM Notification for the Incident to the Buyer (as specified in section 7.2.5). 3. The Buyer may respond appropriately based on the Failure Situation being closed.
Alternative Paths	None
Business Process	MEF 50.1 Problem-to-Resolution

Table 5 - Failure Notification

The following are additional Seller requirements for the Failure Notification Use Case.

- [R1]** The Seller **MUST** set the Incident Type to **CIM_FAILURE**.
- [R2]** The Seller **MUST** set the Incident Impact to **DOWN**.
- [R3]** The Seller **MUST** set the Incident Description with sufficient details about the nature of the Failure Situation.
- [D1]** When the Incident is created, the Seller **SHOULD** set the Incident Expected Closed Date to the estimated resolution date and time of the Failure Situation.

7.2.2 Service Impairment Notification Use Case

The Service Impairment Notification Use Case is detailed in this section.

Field	Description
Use Case Number	2
Use Case Name	Service Impairment Notification
Description	Anytime the Seller detects an occurrence of a Service Impairment on a Product provided to the Buyer, the Seller will send a Service Impairment Notification to the Buyer. The Incident details includes information about the nature of the Service Impairment and may include the expected closed date and time.
Actors	Buyer/Seller
Pre-Conditions	1. The Buyer has registered for CIM Notifications (as specified in section 7.2.4). 2. The Seller has detected a new Service Impairment on an Activated Product impacting the Buyer.
Process Steps	1. The Seller creates an Incident of Incident Type CIM_POLICING or CIM_CONGESTION. 2. The Seller sets the Incident Impact to DEGRADED or INTERMITTENT depending on the severity of the Service Impairment. 3. The Seller issues a Send CIM Notification for the Incident to the Buyer (as specified in section 7.2.5).
Post-Conditions	The Buyer has detailed information on the specific Service Impairment as described in the Incident, along with any IN_PROGRESS updates, including progress update notes, expected closed date/time and will be notified when the Incident is closed. 1. The Seller updates the Incident State to CLOSED. 2. The Seller issues a Send CIM Notification for the Incident to the Buyer (as specified in section 7.2.5). 3. The Buyer may respond appropriately based on the Situation being closed.
Alternative Paths	None
Business Process	MEF 50.1 Problem-to-Resolution

Table 6 - Service Impairment Notification

The following are additional Seller requirements for the attributes defined in Table 10 - Additional Incident Type Values and in MEF 113 [6] Table 37 - Incident Attributes for the Service Impairment Notification Use Case.

- [R4]** If the Service Impairment is due to traffic violating traffic profiles associated with the subscribed service, such as traffic drops due to policing, the Seller **MUST** set the Incident Type to **CIM_POLICING**.

- [R5] If the Service Impairment is due to traffic congestion, such as resulting in packet drops or traffic delays, the Seller **MUST** set the Incident Type to CIM_CONGESTION.
- [R6] The Seller **MUST** set the Incident Impact to DEGRADED or INTERMITTENT depending on the severity of the Service Impairment.
- [R7] The Seller **MUST** set the Incident Description with sufficient details about the nature of the Service Impairment.
- [D2] When the Incident is created, the Seller **SHOULD** set the Incident Expected Closed Date to the estimated resolution date and time of the Service Impairment.

Note: A Buyer receiving multiple Service Impairment Notifications over a specific duration for a Product may use that as a trigger for negotiating changes to the Product-Specific Attributes (for example, Bandwidth Capacity, Bandwidth Profile, Class of Service, etc.).

7.2.3 Maintenance Notification Use Case

The Maintenance Notification Use Case is detailed in this section.

Field	Description
Use Case Number	3
Use Case Name	Maintenance Notification
Description	The Seller notifies the Buyer about an upcoming Planned Maintenance that could impact the operation of a Product provided to the Buyer. The Incident details includes the Planned Maintenance start and ending dates and times, to help the Buyer plan around the maintenance.
Actors	Buyer/Seller
Pre-Conditions	1. The Buyer has registered for CIM Notifications (as specified in section 7.2.4). 2. The Seller has an upcoming Planned Maintenance that could impact the operation of an Activated Product for the Buyer.
Process Steps	1. The Seller creates an Incident of Incident Type CIM_PLANNED_MAINTENANCE. 2. The Seller issues a Send CIM Notification for the Incident to the Buyer (as specified in section 7.2.5).
Post-Conditions	The Buyer has detailed information on the upcoming Planned Maintenance window as detailed in the Incident identified by the Incident Identifier and will be notified when the maintenance is started. 1. When the maintenance is started, the Seller updates the Incident State to IN_PROGRESS. 2. The Seller issues a Send CIM Notification for the Incident Identifier to the Buyer (as specified in section 7.2.5). 3. The Buyer may respond appropriately based on the maintenance having started. The Buyer will be notified when the maintenance is completed. 4. When the maintenance is complete, the Seller updates the Incident State to CLOSED. 5. The Seller issues a Send CIM Notification for the Incident to the Buyer (as specified in section 7.2.5). 6. The Buyer may respond appropriately based on the maintenance having completed.
Alternative Paths	None
Business Process	MEF 50.1 Problem-to-Resolution

Table 7 - Maintenance Notification

The following are additional Seller requirements for the Maintenance Notification Use Case.

- [R8]** The Seller **MUST** set the Incident Type to CIM_PLANNED_MAINTENANCE.
- [R9]** The Seller **MUST** set the Situation Start Date to the Planned Maintenance start date and time.
- [R10]** The Seller **MUST** set the Incident Expected Closed Date to the Planned Maintenance ending date and time.

Note: The Seller Planned Maintenance notification should be sent days or weeks (depending on the Service Level Agreement) ahead of the activity.

7.2.4 Register for CIM Notifications Use Case

The Register for Event Notifications Use Case is detailed in this section.

Field	Description
Use Case Number	4
Use Case Name	Register for CIM Notifications
Description	The Buyer requests to subscribe to Incident Notifications.
Actors	Buyer/Seller
Pre-Conditions	None
Process Steps	1. The Buyer sends the Register for Event Notifications requests as defined in MEF 113 [6] section 8.18.1 to the Seller specifying where to send such notifications and which Event Notification Types to include in notifications. 2. The Seller receives this request, records which Event Notification Types to send, where to send such notifications for this Buyer, and returns an acknowledgement to the Buyer as defined in MEF 113 [6] section 8.18.2.
Post-Conditions	The Seller is aware of where to send Event Notifications.
Alternative Paths	The Seller returns an error message if an error is encountered while processing that prevents the Seller from completing the request.
Business Process	MEF 50.1 Problem-to-Resolution

Table 8 - Register for CIM Notifications

The following are additional Buyer requirements for the attributes defined in MEF 113 [6] Table 39 - Register for Event Notifications Attributes for the Register for Event Notification Use Case.

- [R11]** The Buyer **MUST** set the Notification Type to INCIDENT.
- [R12]** The Buyer **MUST** set the List of Event Notification Types to INCIDENT_CREATE, INCIDENT_UPDATE, INCIDENT_STATE_CHANGE.
- [R13]** If the Buyer wants to register for Incident Notifications, the Buyer **MUST** set the Action to START.
- [R14]** If Buyer wants to unregister for Incident Notifications, the Buyer **MUST** set the Action to STOP.

7.2.5 Send CIM Notification Use Case

The Send Event Notification Use Case is detailed in this section.

Field	Description
Use Case Number	5
Use Case Name	Send CIM Notification
Description	The Seller sends a notification regarding an Incident (e.g., a Situation in the Seller's network) to the Buyer indicating one of the following Event Notification Types has occurred: - INCIDENT_CREATE - INCIDENT_UPDATE - INCIDENT_STATE_CHANGE
Actors	Buyer/Seller
Pre-Conditions	- The Seller's system contains a CIM related Incident. - An Incident has gone through a qualifying Event Notification Type.
Process Steps	The Seller issues a Send Event Notification as specified in MEF 113 [6] section 8.19 to the location(s) registered by the Buyer.
Post-Conditions	The Buyer has received the appropriate Event Notification.
Alternative Paths	None
Business Process	MEF 50.1 Problem-to-Resolution

Table 9 - Send CIM Notification

The following are additional Seller requirements for the Send Event Notification Use Case.

[R15] The Seller **MUST** only send Event Notifications to a Buyer that has registered for CIM Notifications, if the Incident Type attribute is CIM_FAILURE, CIM_POLICING, CIM_CONGESTION or CIM_PLANNED_MAINTENANCE.

[R16] The Seller **MUST** include the following attributes:

- Incident Identifier
- Product Identifiers
- Incident Description
- Incident Severity
- Incident Priority
- Incident Impact
- Incident Type

- Incident Creation Date
- Situation Start Date
- Incident State
- Incident Contact

[R17] The Seller **MUST** include the following attributes, if they were set by the Seller:

- Incident Expected Closed Date
- Incident Notes
- Incident Attachments (as URL)
- Incident Technical Contact
- Incident Related Tickets And Incidents

[R18] The Seller **MUST** include the Incident Closed Date if the Incident State is CLOSED.

8 Additional Trouble Ticketing Requirements

This section lists the additional Trouble Ticketing Use Cases requirements needed to support the CIM Notification Service.

8.1 Trouble Ticketing Use Cases

The CIM Notification Service requires support of the Incident Use Cases, which are defined as optional in the MEF 113 Trouble Ticketing Business Requirements for an implementation to support. As such, a CIM Notification Service implementation requires that the following MEF 113 Trouble Ticketing Use Cases are mandatory for an implementation to support.

- [R19] An implementation of CIM Notification Service **MUST** support MEF 113 [6] Use Cases 15 and 16.
- [R20] A Seller implementation of CIM Notification Service **MUST** support MEF 113 [6] Use Cases 17 and 18 for Incident Notifications.
- [R21] A Seller implementation of CIM Notification Service **MUST** support MEF 113 [6] Use Case 17 and 18 for the following Event Notification Types:
 - INCIDENT_CREATE
 - INCIDENT_UPDATE
 - INCIDENT_STATE_CHANGE
- [D3] A Buyer implementation of CIM Notification Services **SHOULD** support MEF 113 [6] Use Cases 17 and 18 for Incident Notifications.

8.2 Incident Type Values

This section lists the additional Incident Type definitions defined in MEF 113 [6] Table 37 - Incident Attributes to support the CIM Notification Service.

Attributes	Description	Type	Comments
Incident Type	The presumed cause of the Incident as evaluated by the Seller.	One of: • CIM_FAILURE • CIM_POLICING • CIM_CONGESTION • CIM_PLANNED_MAINTENANCE	Set by the Seller CIM_FAILURE: Any Situation where the Product is non-operational, such as down, routing failures or severe packet drops. CIM_POLICING: Any Situation due to traffic violating traffic profiles associated with the subscribed service, such as traffic drops due to policing. CIM_CONGESTION: Any Situation due to traffic congestion, such as resulting in packet drops or traffic delays. CIM_PLANNED_MAINTENANCE: Any scheduled maintenance that may impact a Product for the Buyer.

Table 10 - Additional Incident Type Values

8.3 Retrieve CIM Incident List

A Buyer that has not enabled or does not support Register for Event Notifications (MEF 113 [6] Use Case 17) may poll to retrieve a summarized list of any new, open or recently closed Incidents by periodically submitting a Retrieve CIM Incident List request. The Buyer may then retrieve the full detailed information for a single Incident to get the details and status of the Situation by submitting a Retrieve Incident by Incident Identifier request (as specified in MEF 113 [6] section 8.17.1).

The following are additional requirements for MEF 113 [6] section 8.16.1 (Retrieve Incident List - Buyer Request) as to which attributes defined in MEF 113 [6] Table 37 - Incident Attributes may be used as filter criteria to support polling for the CIM Notification Service or to retrieve any set of specified filter criteria for CIM related Incidents.

- [D4] If the Buyer requests a list of new Incidents, the Buyer **SHOULD** include filter attribute of Incident Creation Date (range of dates) with a DateTime starting after the most recent Retrieve CIM Incident List poll request.
- [D5] If the Buyer requests a list of open Incidents, the Buyer **SHOULD** include filter attribute of Incident State with CREATED and IN_PROGRESS.
- [D6] If the Buyer requests a list of recently closed Incidents, the Buyer **SHOULD** include filter attributes of Incident State with CLOSED and Incident Closed Date (range of dates) with a DateTime starting after the most recent Retrieve CIM Incident List poll request.

The following are additional requirements for MEF 113 [6] section 8.16.2 (Retrieve Incident List - Seller Response) for each Incident that matches the Buyer's filter criteria.

- [R22] The Seller **MUST** only return Incidents for a Retrieve CIM Incident List response, if the Incident Type attribute is CIM_PLANNED_MAINTENANCE, CIM_FAILURE, CIM_POLICING, or CIM_CONGESTION.

8.4 Register for Event Notifications

The following are additional requirements for MEF 113 [6] Use Case 17 - Section 8.18 (Register for Event Notifications) to support the CIM Notification Service.

- [D7] The Buyer **SHOULD** register for all Event Notification Types for Resource Type INCIDENT.

9 Incident Values and State Diagrams [Informative]

The Incident Impact values, State Diagram and definitions of Event Notification Type values and Incident State values are defined in MEF 113 [6] and are included here for convenience.

9.1 Incident Impact Values

The definitions of the Incident Impact values are as follows:

Attributes	Description	Type	Comments
Incident Impact	The presumed impact on the Buyer for the referenced Product(s).	One of: • DEGRADED • INTERMITTENT • DOWN	Set by the Seller DEGRADED: When the Product is impacted and not meeting the Product specifications. INTERMITTENT: When the Product is not operational as intended on an intermittent basis. DOWN: When the Product is non-operational.

Table 11 - Incident Impact Values

9.2 Incident Process Flow

The Incident process flow is shown below. The diagram shows states that an Incident goes through in its lifecycle. The specific states and notifications are managed by the Seller.

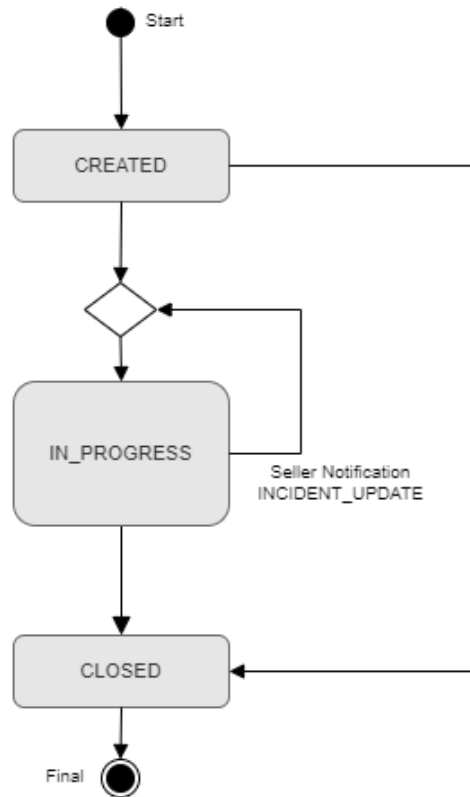


Figure 4 - Incident Process Flow

The definitions of the various Incident State values are as follows:

State	Description
CREATED	A new Incident has been created and allocated a unique Incident Identifier.
IN_PROGRESS	The Incident is in the process of being handled and investigated for resolution by the Seller.
CLOSED	The Situation described in the Incident has been resolved and normal operation has been restored on the Seller's network. This is a terminal state.

Table 12 - Incident State Values

The definitions of the various Event Notification Type values for an Incident are as follows:

Notification Type	Description
INCIDENT_CREATE	A new Incident was created by the Seller.
INCIDENT_UPDATE	An open Incident was updated by the Seller.
INCIDENT_STATE_CHANGE	An Incident State was changed by the Seller.

Table 13 - Event Notification Type Values

10 References

- [1] Internet Engineering Task Force RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, March 1997
- [2] Internet Engineering Task Force RFC 8174, *Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words*, May 2017
- [3] MEF 10.4, *Subscriber Ethernet Service Attributes*, December 2018
- [4] MEF 50.1, *MEF Services Lifecycle Process Flows*, August 2017
- [5] MEF 55.1.1, *LSO Reference Architecture and Framework*, October 2023
- [6] MEF 113, *Trouble Ticketing Business Requirements and Use Cases*, Oct 2022
- [7] MEF 128.1, *LSO API Security Profile*, April 2024

Appendix A Acknowledgements

The following individuals participated in the development of this document and have requested to be included in this list.

- Manfred **ARNDT**
- Wojciech **DZIUNIKOWSKI**
- Michał **ŁĄCZYŃSKI**
- Jeff **QUINN**
- Balamurugan **SUBBIAH**
- Boris **TRINAJSTIC**