

# **TLN WRO Specification type Document**

< TLN Device management server interface  
specification for management of AO CPE by AO >



## Document Housekeeping

### Document Category and type

CAT	TYPE	DOC ID	Comment
General	SPEC	TLN-WRO-TA-G-S-PAAB	Specification type documents (-SPEC) are documents specifying logical / physical interfaces / protocols, etc..., to which AO equipment/systems need to comply

### Document Authorization

EDITION	DATE	APPRAISAL AUTHORITY	STATUS	ORIGINATOR
0.5	21.05.2012	Director TLN Wholesale	Draft	TLN WRO Engineering

### Document Maturity State

EDITION	DATE	APPRAISAL AUTHORITY	STATUS	ORIGINATOR
0.5	21.05.2012	Director TLN Wholesale	Draft(DR)	TLN WRO Engineering
0.9	xx.xx.2012	Director TLN Wholesale	Final Submit(FS)	TLN WRO Engineering
1.0	xx.xx.2012	Director TLN Wholesale	Approval(AP)	TLN WRO Engineering

### Document Effective Date

This document has come into effect as of xx/xx/2012 and remains valid until a valid subsequent Telenet Wholesale Reference offer, substituting this document is published.

### Legal Disclaimer

"This document constitutes an integral part of the Telenet Reference Offer for Basic TV / IDTV / BB and should be fully complied with by the Beneficiary at all times. Non compliance, incomplete or deviating application of this document by the Beneficiary, or his authorized agent, results in the suspension and ultimately termination of the Contract between Telenet and the Beneficiary.

At any time this document is susceptible to change by Telenet, Regulator's decision or by decision of a relevant judicial authority. Changes to this document will, depending on the circumstances for change, be appropriately notified to the Beneficiary and published on the Telenet website.

Telenet has appealed the CRC decisions of the VRM, BIPT and CSA of 1 July 2011 concerning the market analysis of the broadcasting market in Belgium and it consequently reserves all its rights in relation to this document."

## Table of Contents

1	Abstract .....	5
2	Glossary and Abbreviations .....	6
3	TLN AO Device management Server (TADMS) Functional Description .....	7
4	TLN AO Device management Server (TADMS) Functional Requirements .....	8
4.1	TADMS BUILDING BLOCKS .....	8
4.1.1	<i>General</i> .....	8
4.1.2	<i>TADMS API</i> .....	8
4.1.3	<i>TADMS security module</i> .....	8
4.1.4	<i>TADMS policy enforcement module</i> .....	9
4.1.5	<i>TADMS device access module</i> .....	9
4.2	TADMS API FORMAL DEFINITION .....	9
4.3	TADMS SECURITY MODULE DETAILED DEFINITION .....	9
4.4	TADMS POLICY ENFORCEMENT MODULE DETAILED DEFINITION .....	9
4.5	TADMS DEVICE ACCESS MODULE DETAILED DEFINITION .....	10
5	“In band” management access to AO devices .....	10
6	Remote management protocol choices .....	10

## Table of Figures

Figuur 3-1 .....	7
Figure 4-1 .....	8

## **List of Appendixes**

This document may refer to further detailed documents that are added in Appendixes to this document.

A reference to an appendix is in this document highlighted with grey background.

The list with appendixes of this document:

None.

## **List of References**

This document may refer to external documents or information sources.

A reference to an external document or information source is in this document highlighted with grey background.

The list of referred external documents or information sources in this document:

None.

## **Restricted information**

This document may contain sections that are not public information and that can be made available only to parties that have executed specific NDA`s.

Information that is subject to NDA is marked in this document as follows:

NDA  
NDA

The information in this text box is available only under NDA

Before conversion to PDF format for publication of the document, the information will be made unreadable by converting the background of the text box to black.

# 1 Abstract

This document describes the API definition of the TLN management server for AO CPE equipment that will enable operational management by the AO of the CPE equipment deployed with its customers. In addition it will provide the AO with a basic read-only access on the status of some essential TLN network elements and servers that are involved in providing the service to the AO customers.

The feasibility of the technical designs and methods described in this document are subject to verification by a Proof of Concept (POC) test organized by Telenet and may be changed or updated depending on the outcome of this POC.

## 2 Glossary and Abbreviations

API: Application Program Interface

CMTS: Cable Modem Termination System

CPE: Customer Premises Equipment

Docsis: Data Over Cable Service Interface Specification

HFC: Hybrid Fiber Coax

MAC: Media Access Control

OAM: Operations Administrations and Management

SNMP: Simple Network Management Protocol

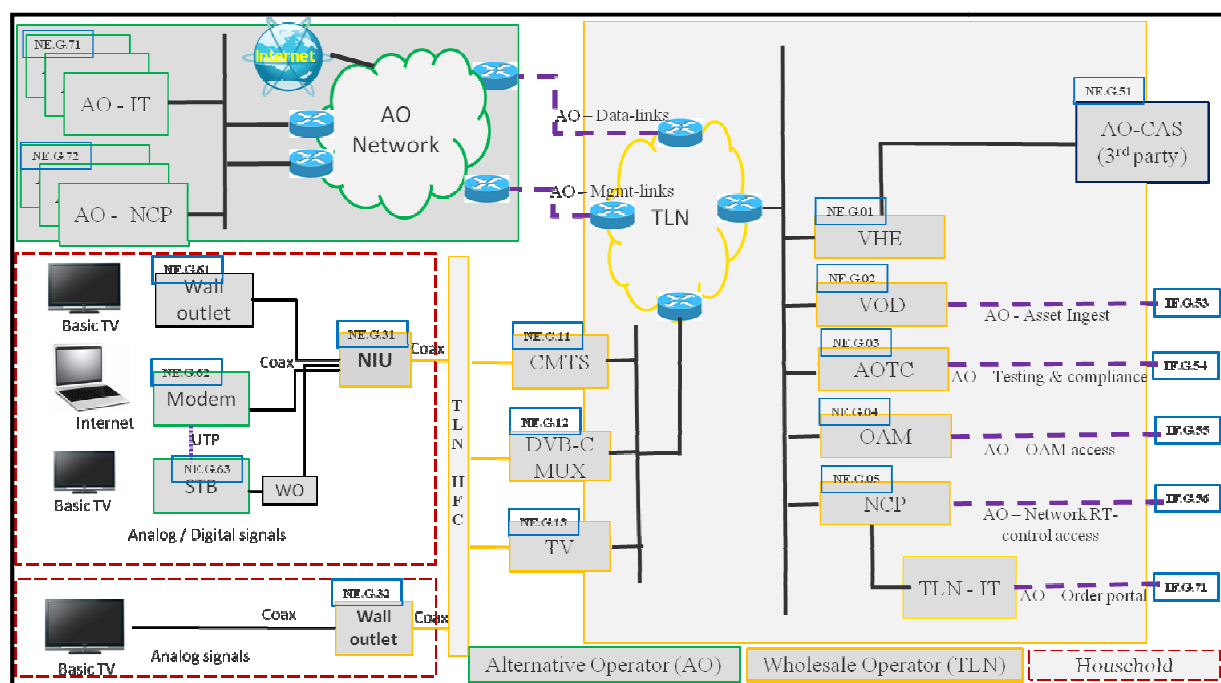
TADMS: Telenet AO Device management Server

VPN: Virtual Private Network

WIFI: Wireless Fidelity

### 3 TLN AO Device management Server (TADMS) Functional Description

- (1) Overall management access by AO to its devices is provided by an API based management proxy server provided by TLN. The possibilities and restrictions of this API based management proxy server are described in this document. The concept of proxy management is provided as direct access by AO on the AO CPE device would impose unmanageable security risks on the TLN network as the devices are accessing a shared MAC layer.
- (2) Device management as described here in section 3 and 4 relates to management of the “modem” or “Docsis” component of the AO CPE device that provides the connectivity and transport service on the Docsis layer towards the TLN CMTS over the TLN HFC network.
- (3) Besides API based proxy management, TLN will consider under certain circumstances, and after review that by granting this no security risks will be present, direct “in band” management access by AO to its devices for the “non Docsis” or “non-modem” part of the AO CPE. With “non Docsis” or “non-modem” part is meant e.g. a WIFI module or integrated IP router module that might be present in the AO CPE. This part is described in section 5.
- (4) Via the API it will provide the AO also with a basic read-only access on the status of some essential TLN network elements and servers that are involved in providing the service to the AO customers. This will allow the AO to have a view on non individual customer specific problems that might affect the service to its customers
- (5) The TADMS server is part of the OAM subsystem as shown in the general architecture picture below and can be reached over the AO - OAM Access interface.



Figuur 3-1

## 4 TLN AO Device management Server (TADMS) Functional Requirements

### 4.1 TADMS building blocks

#### 4.1.1 General

- (6) The TADMS (see figure below) consists of 4 major building blocks which are each briefly described on a functional level in the remainder of this section.

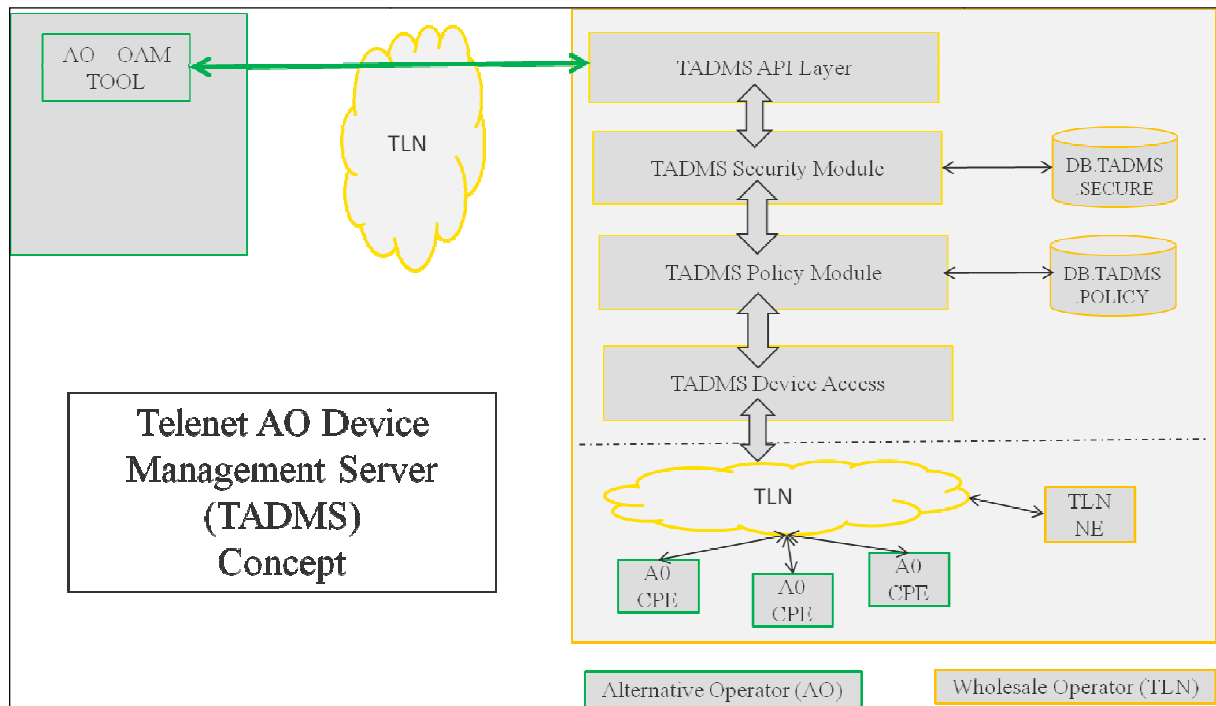


Figure 4-1

#### 4.1.2 TADMS API

- (7) The API provides remote Machine to Machine access for OAM tools build by the AO's.

#### 4.1.3 TADMS security module

- (8) The security module ensures that only authorized access will be allowed. As such it will verify the authenticity of incoming API requests from the AO environment, to ensure they present the correct credentials, use the pre-agreed secure IP VPN communication paths, etc... This module will also authenticate the AO and dynamically enforce a VPN view ensuring that a given AO has only access to its own devices and interfaces.
- (9) The security module will also log all transactions made via the API, in order to be able to provide audit and log trails in case of eventual disputes.



#### **4.1.4 TADMS policy enforcement module**

- (10) The policy enforcement module will define the “rule sets” that will determine which “management” actions are allowed and which are forbidden.
- (11) As a first general rule TLN will allow all “Read-Only” operations on AO devices by the AO without any functional restrictions, however the policy module might put limitations on the number of management transactions per time-unit that the AO systems may launch as excessive rates might cause congestion impact on Telenet network elements and hence impact on other customers
- (12) As a second general rule TLN will allow also change operations on AO devices by the AO in an “as broad as possible” way by offering the possibility for the AO to add a configuration file under the control of Telenet so that the AO has optimal commercial freedom in implementing its services, however a well defined list of exceptions will apply.
- (13) This list of exceptions will contain mainly those operations that by changing the configuration of the AO CPE might also compromise the overall network security. For example : the AO will not be allowed to dynamically change the base modem configuration file containing the Docsis layer parameters as one insecure modem can affect others because an HFC network is a shared medium.

#### **4.1.5 TADMS device access module**

- (14) The device access module is responsible for passing the “management” action received via the API request towards the device and returning the device response.

### **4.2 TADMS API formal definition**

- (15) The formal API definition is pending further study. Telenet is currently conducting a number of studies and tests in order to optimize the quality of its wholesale reference offer.

### **4.3 TADMS security module detailed definition**

- (16) The formal security definition is pending further study. Telenet is conducting a number of tests in the framework of the overall Proof of Concept (POC) set-up it is building and testing in order to optimize the quality of its wholesale reference offer.

### **4.4 TADMS policy enforcement module detailed definition**

- (17) The formal policy enforcement definition is pending further study. Telenet is conducting a number of tests in the framework of the overall Proof of Concept (POC) set-up it is building and testing in order to optimize the quality of its wholesale reference offer.

## 4.5 TADMS device access module detailed definition

- (18)The formal device access definition is pending further study. Telenet is conducting a number of tests in the framework of the overall Proof of Concept (POC) set-up it is building and testing in order to optimize the quality of its wholesale reference offer.

## 5 “In band” management access to AO devices

- (19)Besides API based proxy management, TLN will consider under certain circumstances, and after review that by granting this no security risks will be present, direct “in band” management access by AO to its devices for the “non Docsis” or “non-modem” part of the AO CPE. With “non Docsis” or “non-modem” part is meant e.g. a WIFI module or integrated IP router module that might be present in the AO CPE.
- (20)The decision to allow or not this direct “in band” management access on this parts of the CPE and the precise means it will be provided is pending further study. Telenet is conducting a number of tests in the framework of the overall Proof of Concept (POC) set-up it is building and testing in order to optimize the quality of its wholesale reference offer.

## 6 Remote management protocol choices

- (21)At this stage TLN is evaluating the use of TR069 as main remote management protocol for AO CPE devices versus the use of SNMP. The pro’s and con’s of both mechanisms are being evaluated in a wholesale context.
- (22)The decision which protocol to choose is pending further study. Telenet is conducting a number of tests in the framework of the overall Proof of Concept (POC) set-up it is building and testing in order to optimize the quality of its wholesale reference offer.