TLN WRO Specification type Document

< Requirement specification for AO STB Conditional Access ***(CAS)*** subsystem to enable usage of TLN ROTV >

Document Housekeeping

Document Category and type

CAT	TYPE	DOC ID	Comment
iDTV	SPEC	TLN-WRO-TA-I-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	05.11.2012	Director TLN Wholesale	Draft	TLN WRO Engineering

Document Maturity State

EDITION	DATE	APPRAISAL AUTHORITY	STATUS	ORIGINATOR
0.5	05.11.2012	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

Table of Figures

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:

A. Appendix A, <APP-I-C-PDAA-A> contains :
    1) Appendix A1 – <CPPS - Telenet CAS XML API v3 doc >

The appendix(es) referred to in this section List of Appendixes, contain(s) detailed technical information which is only relevant when a Beneficiary enters in a concrete implementation project to become Beneficiary of the Telenet Reference Offer and/or Annex.

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:
Reference 1: TLN WRO CAT: Interactive Digital TV: TLN-WRO-TA-I-C-PAAB
Reference 2: TLN WRO CAT: Interactive Digital TV: TLN-WRO-TA-I-S-PDAA

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 major building blocks of the Conditional Access Subsystem (CAS) an AO STB must have in order to be able to successfully interoperate with the TLN ROTV. Each required building block is briefly described explaining it´s expected functional behavior.

This document has a corresponding certification document with reference: TLN-WRO-TA-I-C-PAAB which is used to test AO WO equipment compliance against this specification.

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

AO: Alternative Operator
API: Application Programming Interface
BSS: Business Support System
CA: Conditional Access
CAS: Conditional Access System
CPE: Customer Promises Equipment
CPPS: CAS Proxy Provisioning System
CRM: Customer Relationship Management
ECM: Entitlement Control Message
EMM: Entitlement Management Message
ETSI: European Telecommunications Standards Institute
IPSEC: Internet Protocol Security
OSS: Operation Support Systems
PKI: Public Key Infrastructure
SAS: Subscriber Authorization System
SC: Smartcard
SDI: Serial Digital Interface
SMS: Subscriber Management System
STB: Set top box
VHE: Video Head end

3 AO STB Conditional Access*(CA)* subsystem Functional Description

(1) Following figure shows the structure of TLN/AO CA subsystem. A typical CA process consists of four key elements: the broadcast multiplexing equipment (in the VHE), the AO 3rd party CA system (in the 3rd party location), the STB, and the STB security module. The broadcast multiplexing equipment (located in the TLN VHE) generates the encrypted program streams (using encryption keys provided by the 3rd party CA system (located in 3rd party site) that are transmitted to the customer STB. The STB filters out the signals requested by the customer and pass them to the STB security module. The security module then authorizes these programs for decryption if the customer has a subscription for the requested program. The programs are then decrypted in real time and sent back to the STB for display.

(2) Only one distinct 3rd party CA system can be present that operates on behalf of all different AO´s together.

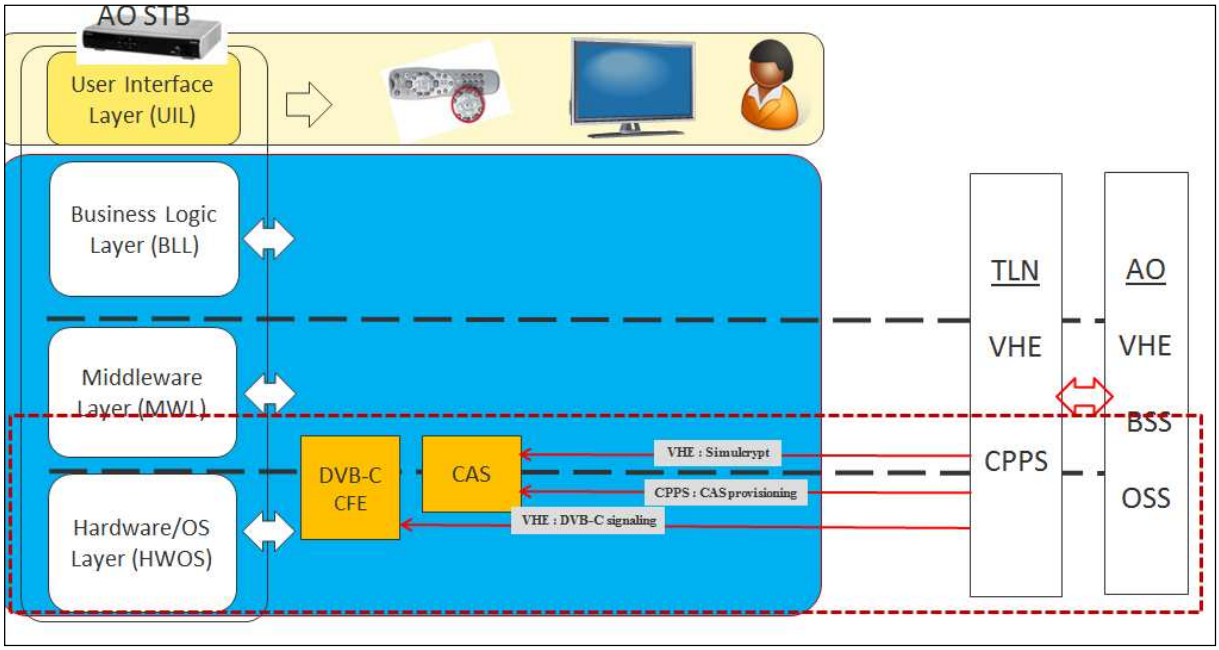

Figure 3-1

4 AO STB Conditional Access *(CA)* subsystem Functional Requirements

4.1 General

(3) The primary purpose of a CA system for digital broadcasting is to determine which individual receivers/set-top decoders shall be able to decode and deliver particular program services / individual programs, to the viewers. Both smartcard-less and smartcard based solutions can be used for the CA system. Typically a DVB-C based CA system enables “simul-crypt”, which allows several (but limited in total number) CA systems to be present in parallel. The TLN wholesale offer will use this “simul-crypt” technique to enable the offer to AO´s.

4.2 3rd party CA system to TLN VHE interface

4.2.1 General

(4) TLN offers a DVB-C based interface that allows the single 3rd party CA system that is operated by the 3rd party on behalf of all AO´s together to inject it´s conditional access signaling at TLN Head-end level where it will be merged with the signaling of existing TLN CA systems.

4.2.2 DVB-C Normative References

(5) AO STB´s must be compatible with below specified ETSI standards.

(6) Normative reference is a term covering separate documents referenced within the standard and means that, unless otherwise stated, the most recent versions of the separate documents should be referenced.

- [1] ETSI TS 101 197 (V1.2.1): "Digital Video Broadcasting (DVB); DVB SimulCrypt; Head-end architecture and synchronization".
- [2] ETSI TS 103 197 (V1.4.1): "Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt".
- [3] ETSI EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".
- [4] ISO/IEC 13818-2: "Information technology; Generic coding of moving pictures and associated audio information: Video".
- [5] ISO/IEC 13818-3: "Information technology; Generic coding of moving pictures and associated audio information - Part 3: Audio".

4.2.3 TLN DVB-C SimulCrypt specifications

(7) Telenet completely adheres to the latest DVB SimulCrypt specifications and as such no further specific requirements are applicable in this domain.

(8) Telenet currently deploys card based and card-less (software based) CA systems concurrently in SimulCrypt mode. For the card-less CA, specific signaling and data streams are broadcasted on the Telenet DVB-C network. Next to the regular CA descriptors in the CAT and PMT tables for EMM and ECM declaration, and the ECM and EMM streams itself, the

card-less CA also uses private data streams to distribute the security modules and other data to the different STB models.

(9) Obviously the CA client software on the STB of the AO needs to ignore this card-less CA specific signaling and data streams. It must filter out the CA data targeted for the AO client. Verification of this functionality will be part of the certification process for the introduction of the AO CA System and STB on the Telenet network.

(10) During certification, it will also be verified that the introduction of the AO CA system and its dedicated signaling and data streams does not adversely affect the already deployed Telenet STB ´s.

4.2.4 CA system signalling connection

(11) The AO 3rd party CA System is connected from its location at the 3rd party CA operator premises with a secure encrypted IP connection that will carry the EMM/ECM messages generated by the AO 3rd party CA servers towards the TLN VHE where they will be merged and "simul-crypted" and injected in the digital transport streams by the TLN statistical multiplexers

(12) The AO SMS is the subsystem of the 3rd party CA system that manages the subscriber's information and generates the required entitlement management messages (EMM) based upon the provisioning information it receives from the TLN – CPPS.AO. An EMM provides general information about the subscriber and the status of the subscription. The EMM is sent with the ECM. The ECM is a data unit that contains the key for decrypting the transmitted programs.

(13) SimulCrypt allows multiple STB´s, each using a different CA system, to operate in parallel within the same DVB-C transmission system and to authorize and decode the programs for display. The different ECMs and EMMs required by each CA system are transmitted simultaneously. Each STB recognizes and uses the appropriate ECM and EMM needed for authorization.

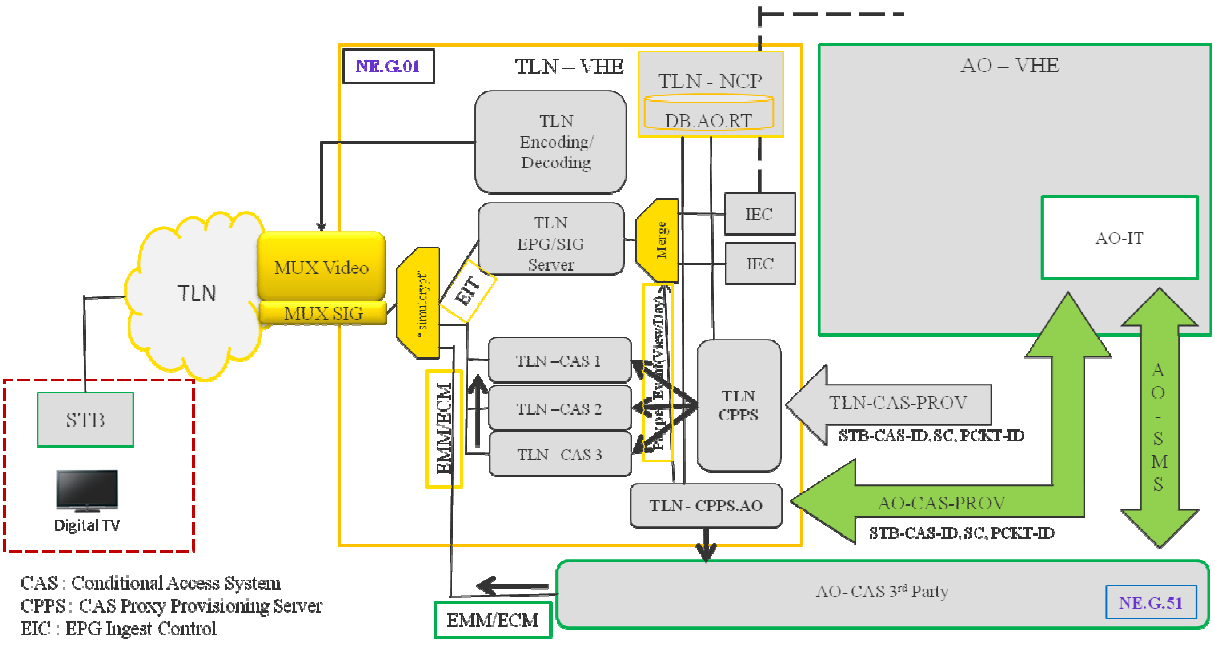

Figure 4-1

4.2.5 3rd party CA system explicit operational requirements

(14) For security reasons it is important to include at least the following operational functions in the CA system:

-Disable/enable decoder
-Disable/enable card
-Disable/enable program service
-Send message to decoder
-Send message to decoder for individual program service
-Show customer's ID card

4.3 CA Provisioning

4.3.1 General

(15) The CA system Proxy Provisioning Server (CPPS) is the TLN API server that is used for all CA system provisioning currently in use in the TLN network.

4.3.2 CA Provisioning

(16) A CA system is typically provisioned from a CRM system. The CRM system holds the customer accounts and also stores the services the customer has subscribed to (e.g. the customer subscription towards premium pay TV packages). As such the AO CRM system will have to fulfill this role towards the 3rd party CA system. The AO CRM system will typically upon creation of a new customer or addition of new or extra services to an existing customer send updates to a multi-CA "technical" provisioning system which will on its turn translate this information in the specific messages required by the different CA systems in use and will eventually also update other network elements with this provisioning information. In important step in this provisioning flow is the "so called" "pairing" of an STB with a smartcard. In this way a STB gets "personalized" and linked to a given customer and given smartcard.

4.3.3 TLN CPPS to 3rd party CA system

(17) The AO´s IT systems will use the TLN CPPS API (exposed as XML over HTTP) to send customer subscription information on (i)DTV services towards the TLN CPPS dedicated for AO operation. The CPPS will translate this in the messages required by the 3rd party CA system (just like it does for the TLN own CA systems) and will at the same time update the necessary information in the relevant TLN network element and databases to ensure correct operation of AO STB´s in the overall set-up.

(18) The main API messages and their purpose are explained on a conceptual level here below. Full details of the API can be found in Appendix A1: CPPS - Telenet CAS XML API v3.

(19) As can be deducted from the figure below the main CPPS API messages allow the AO CRM system to perform following actions :

- Activate STB : allows to provision a new STB on the CA system, link it with the SC and activate the combination so that the 3rd party AO CA system will start to generate the required ECM/EMM messages for this combination
- Add Package : allows to provision a new service package that will entitle the customer owning an earlier activated STB/SC combination to the reception of the TV channels (or other services) inside the package
- Remove Package : Remove earlier granted entitlements from an STB/SC combination
- De-activate STB : Remove an STB/SC combination from the CA system

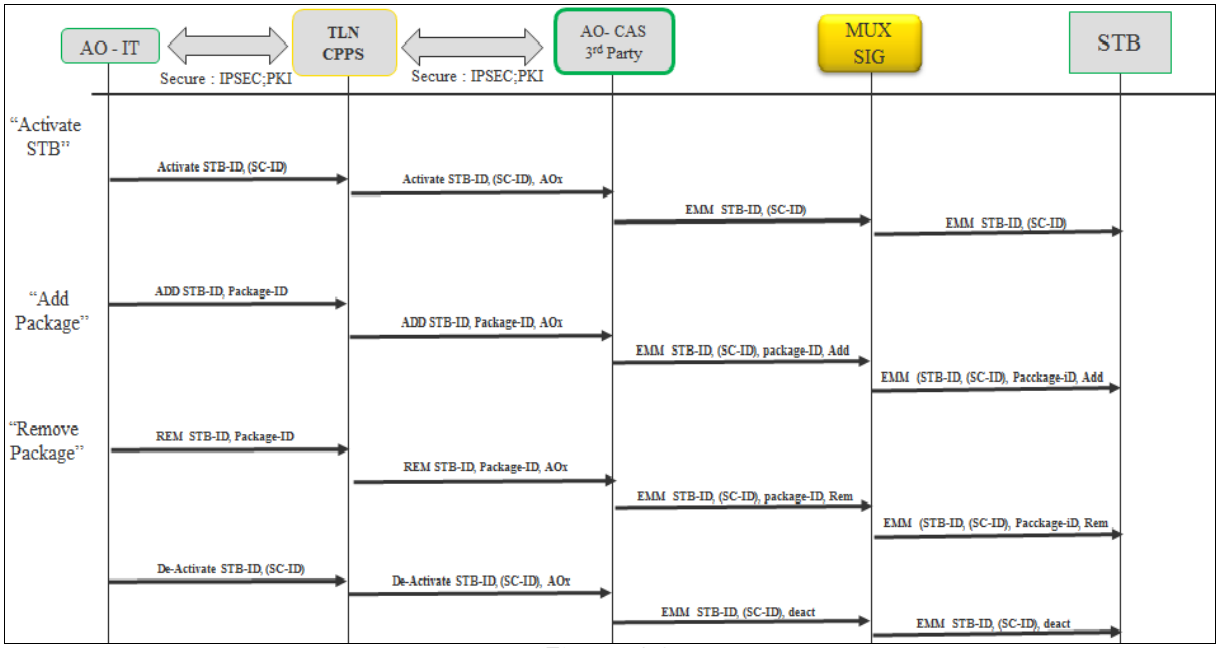

Figure 4-2

4.3.4 CA Provisioning connection

(20) The TLN CPPS is an API which is exposed as XML over http and located between the AO-CAS 3rd Party and AO-IT systems. A Secure connection (IPSEC, PKI) is used to transport the provisioning messages between the AO IT CRM systems and the CPPS.

4.4 CA Restrictions

4.4.1 One-way STB

(21) Depending on the capabilities of the 3rd party CA system, jointly chosen by the different AO´s, limitations will apply to the use of the CA system on non-interactive STB`s (not having an IP return path). As those limitations have an impact on the overall security (e.g. if a given CA supplier does not guarantee the security of its technology for one-way STB`s the whole set-up becomes insecure), TLN will strictly impose and follow-up with the AO`s and 3rd party CA provider that all relevant CA system supplier guidelines are strictly followed.

4.4.2 CA system Migration

(22) Migration from one CA system to another one is a complex, costly and time consuming process. Hence AO`s should provide all possible measures to avoid the need for migrations.

4.4.3 CA connection to IP Return path

(23) For most home STB installations, a return path is available between the set-top decoder and the network. This return path will allow the security modules in the STB to contact the back-end CA Subscriber Management System. For example, the operator may want the customer's STB to contact the SMS to perform certain security operations. This process could be initiated by commands sent over-air or (less likely) the SMS could initiate an inbound connection to the customer's STB and interrogate it directly.

(24) There are a number of reasons for using a return path:

a) *Enhanced security;*
The return path establishes a one-to-one link between the operator and each STB.
b) *Transmission of entitlement messages;*
For large shared networks, the capacity for transmission of entitlement messages may be in adequate and additional capacity may be achieved by using the return path connection.
c) *Upgrade of security protocols;*
The return path provides an extra facility which allows in case of emergency to upgrade the security algorithms.

(25) If the selected CA system is a software based CA system, the return path will have to be used to connect the STBs of the AO with the CA servers for authentication and for entitlement updates.

(26) TLN may in the future make the use of the STB return path for CA operations mandatory if network capacity constraints or security requirements would impose this.

4.5 TLN CA Operational procedures

(27) For security reasons it is important to include at least the following functions in a CA system:

-Disable/enable decoder
-Disable/enable card
-Disable/enable program service
-Send message to decoder
-Send message to decoder for individual program service
-Show customer's ID card

(28) Telenet regularly performs maintenance work on its multiplexors and CA systems. This can cause temporary loss of connectivity between multiplexors and the CA system. Completely in accordance with the SimulCrypt standard, the Multiplexors will go in crypto period extension, meaning that the scrambling is static (with the same key) and the ECMs are also static.

(29) Depending on the CA of the AO, this can have an impact on e.g. the provisioning of new customers. AO STB and systems should be able to handle those operational aspects.

4.6 AO Device Management by TLN Requirements

(30)The applicable requirements are described in TLN-WRO-TA-I-S-PDAA.

5 AO STB general - Non Functional Requirements

(31)The applicable requirements are described in TLN-WRO-TA-I-S-PDAA.