



Система кодирования цифрового телевидения СТІ

Высокая защищенность CTI CAS

High-Security CTI CAS



High security CA system

- No broken record
- Multi-layers encryption keys
- Master-slave card
- Support short message payment
- Pre-encryption function, support applications such as VOD, PVR, Time-shift TV, etc
- Support high secure chipset solution
- Against CW sharing
- Device-card pairing
- Support payment modes such as PPV, IPPV, IPPV-T

Skyworth 创维

COSHIP 同洲

MOTOROLA

Haier

WELLAV 伟乐科技

KONKA 康佳

CHANGHONG 长虹

DAYANG

inspur 浪潮

SMIT

Hisense 海信

YINHE

DTT 大唐电信

新大陆通信
Newland CS&T

SHENZHOUS 神州电子

JIUZHOU 九州

ZORAN

PBI

SEEPA 金亚科技

BAUSTEM

DareGlobal 大业科技

Blossoms

TYWALKER

GranVision

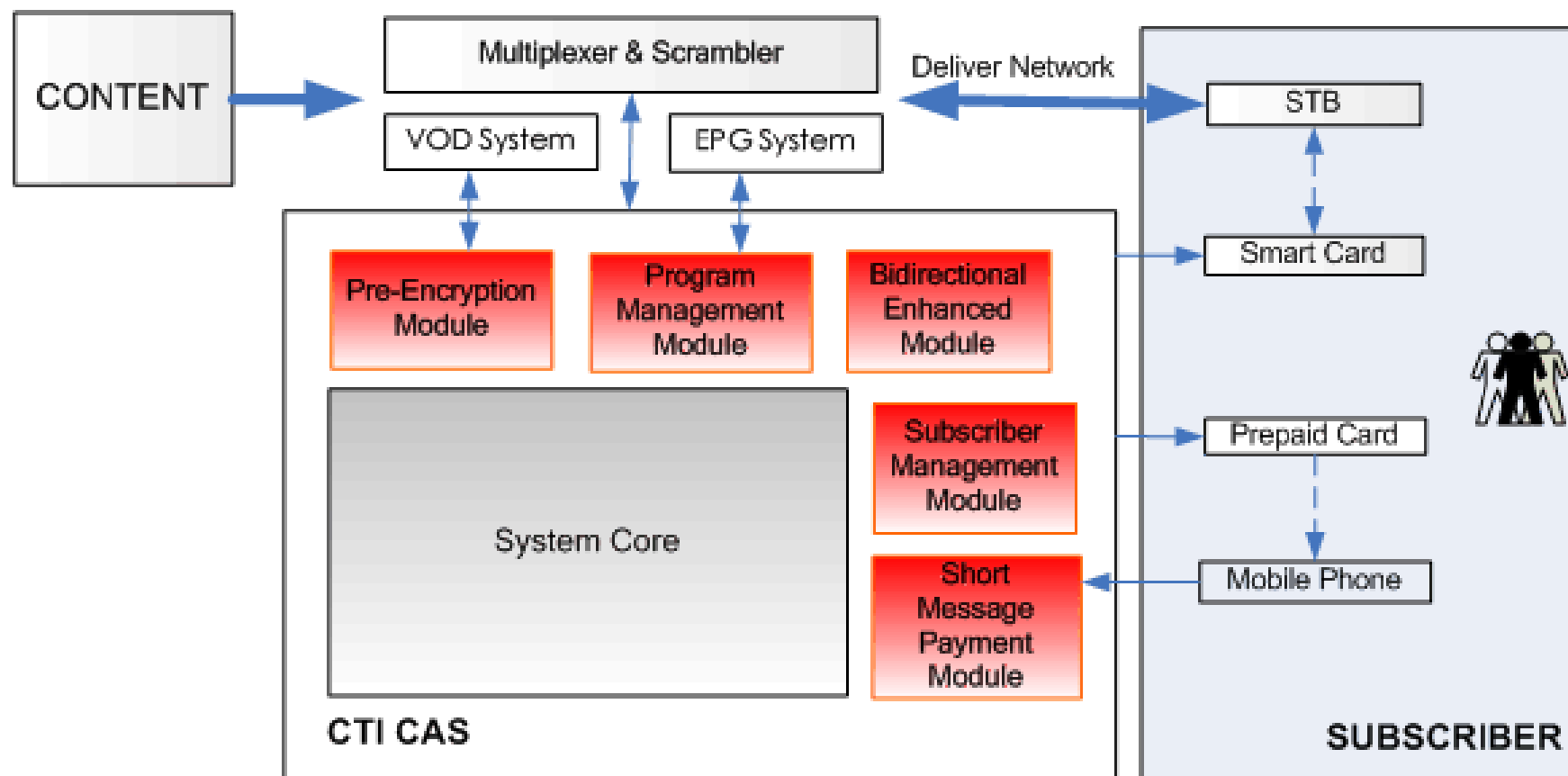
清华同方
THUNGA TONGFANG



СТI-CAS: история развития

- Первая DVB система кодирования, появившаяся в 2000 г.
- Установлена на более чем 210 головных станций в 70 различных странах мира
- Независимый алгоритм разработан собственными сотрудниками компании
- Отсутствие свидетельств взлома на протяжении всей истории
- Отмечена серебряным призом Национального Китайского Бюро Науки и Технологии

СИСТЕМА КОДИРОВАНИЯ СТ



ЭЛЕМЕНТЫ СИСТЕМЫ КОДИРОВАНИЯ СТІ

- Базис:
 - Ядро системы кодирования (CAS)
- Опциональные элементы:
 - Система управления абонентами (SMS)
 - Система управления программами (PMS)
 - Система оплаты доступа через СМС (TVM)
 - Система предварительного кодирования (PRCA)
 - Система двустороннего взаимодействия (BCA)

СТІ-CAS:

Сертификат Национального Финансового Комитета

商用密码产品生产定点单位证书

(国密局产字 SSC497 号)

北京算通科技发展有限公司:

兹批准你单位为商用密码产品生产定点单位。

生产范围：经国家密码管理机构批准的商用密码产品的开发、生产。

本证书有效期 3 年，自 2008 年 10 月 31 日至 2011 年 10 月 31 日。

特发此证。

国家密码管理局

2008 年 10 月 31 日



Сертификат SARFT, подтверждающий высшую степень надежности (Класс А)

 编号: C024
No.

国家广播电影电视总局
数字电视广播条件接收系统入网测评
认证证书
Certificate of Approval for Digital TV
Broadcasting Conditional Access System
(正 本)

下述CAS符合数字电视广播条件接收系统入网相关技术要求, 经审核, 特发此证。
This is to certify that the following CAS is in compliance with the corresponding technical requirements for network access of digital TV broadcasting CAS.

申请单位: 北京算通科技发展有限公司
Applicant

系统版本号: CTL_CAS条件接收系统 V2.55
Version of System

证书等级: A
Class of Certificate

发证日期: 2007-5-24
Date of Issue

有效期至: 2010-5-23
Date of Expiry


(The Official Seal of the State Administration of Radio, Film and Television)

<http://www.chinasarft.gov.cn>

СТИ-CAS. Принципы разработки:

- Открытая система
- Интегрированная система
- Защищенная система
- Надежная система
- Легкая в использовании система
- Расширяемая система

STI-CAS. Принцип совместимости

Совместимость:

- Соответствует международным стандартам, обладает собственным “system ID”, зарегистрирована в “Консорциуме DVB”
- Полностью соответствует стандарту EN 103 197 Simulcrypt
- Интегрирована со многими системами учета абонентской платы, мультиплексорами, скремблерами и абонентскими приставками

Системы кодирования Simulcrypt



Интегрированные с СТТ Системы Учета Абонентов



Интегрированные скремблеры



Сертификаты интегрированных скремблеров



Scientific Atlanta

美国科学亚特兰大公司北京办事处
北京市建国门北大街8号华润大厦2308A室 邮编: 100005
Scientific-Atlanta Inc. Beijing Representative Office.
Room2308A, China Resource Building 电话 Tel: (8610) 8519 2028
8, Jianguomenbei Avenue, 传真 Fax: (8610) 8519 2038
Beijing, 100005, China

Certificate

To whom it may concern

This is to certify the integration of CTI's CA System and SCIENTIFIC ATLANTA'S D9600 SERIES Scrambler. The ECMG integration is well done and the result of interoperability is satisfied by both parties.

D9600 SERIES+SCRAMBLER

SOFTWARE V02.01.40

CTI_CAS Version

ECMG: CTI_CAS ECMG 2.541 Version
EMMG: CTI_EMMG 2.5.2 Version

DVB Simucrypt Protocol

Version 2.0

Scientific-Atlanta Inc.

Zhou Hongyi

2005-6-3

Beijing Communicate Technology Inc.
CAS Product Manager

C. Jie

2005-6-3

Notice: The information in this facsimile is intended only for the use of the individual(s) to whom it is addressed. If you are not the intended recipient (or the person responsible to deliver it to the intended recipient), you are hereby notified that any use, disclosure or copying of this communication is strictly prohibited. If you have received this facsimile in error, please notify us immediately by telephone and return the received pages to us at the address above via U.S. Postal Service. We will reimburse you for any expenses you may incur in doing so.



COMMUNICATE TECHNOLOGIES INC.

Scrambler Certificate

This is to certify that

RGB Networks, Inc.

BNP 3xr

Has been tested by Communicate Technologies Inc. and found to be compatible with Communicate CTI CAS v3.0

Following features has been certificated:

- ECMG Connection
- EMMG Connection
- Smart Card Registration, Resume and Stop
- Authorization and cancellation
- Send Mail (OSD)

Mr. Pengfei Gao
Chairman & CTO
Communicate Technologies Inc.

Pengfei Gao
Signature
Date 23/06/10

Ramin Farassat
Vice President of Marketing & Business Development
RGB Networks, Inc.

Ramin Farassat
Signature
Date 28/06/10

Сертификаты операторов

farncombe
TECHNOLOGIES LTD



Security Review of Beijing Communicate Technologies Inc CA System

Version of Full report edited for
Home Box Office Central Europe (HBO CE)

Author: Ian Whitworth

J-M Racine

Version: 1.0

Date: 24th August 2007

telephone
+44 1256 844161

facsimile
+44 1256 844162

e-mail
farncombe@ft.co.uk

www
ft.co.uk

Farncombe Technology (2006) Ltd
ViewPoint
Basing View
Basingstoke
RG21 4RG
UK

Registered in England No. 05997790

Certification

This is to certify that we Family Entertainment Group Co., Ltd are using
COMPUNICATE Conditional Access System in our digital TV project and
the subscriber quantity is 64,500, moreover that CAS has been found to be
high in security and the has never been broken by now.

Certified true and correct.


Win Khine
Director
Family Entertainment Group Co., Ltd

Date: 25, Nov; 2009

No. 34/B, New University Avenue Road, Bahan Township, Yangon, Myanmar.
Ph : +95-1- 558874, 559847, 548430, 541420. Email: family-ent@myanmar.com.mm

Интегрированные абонентские приставки



Без смарт-карт



**С использованием
смарт-кард**



CI модуль + цифровой телевизор

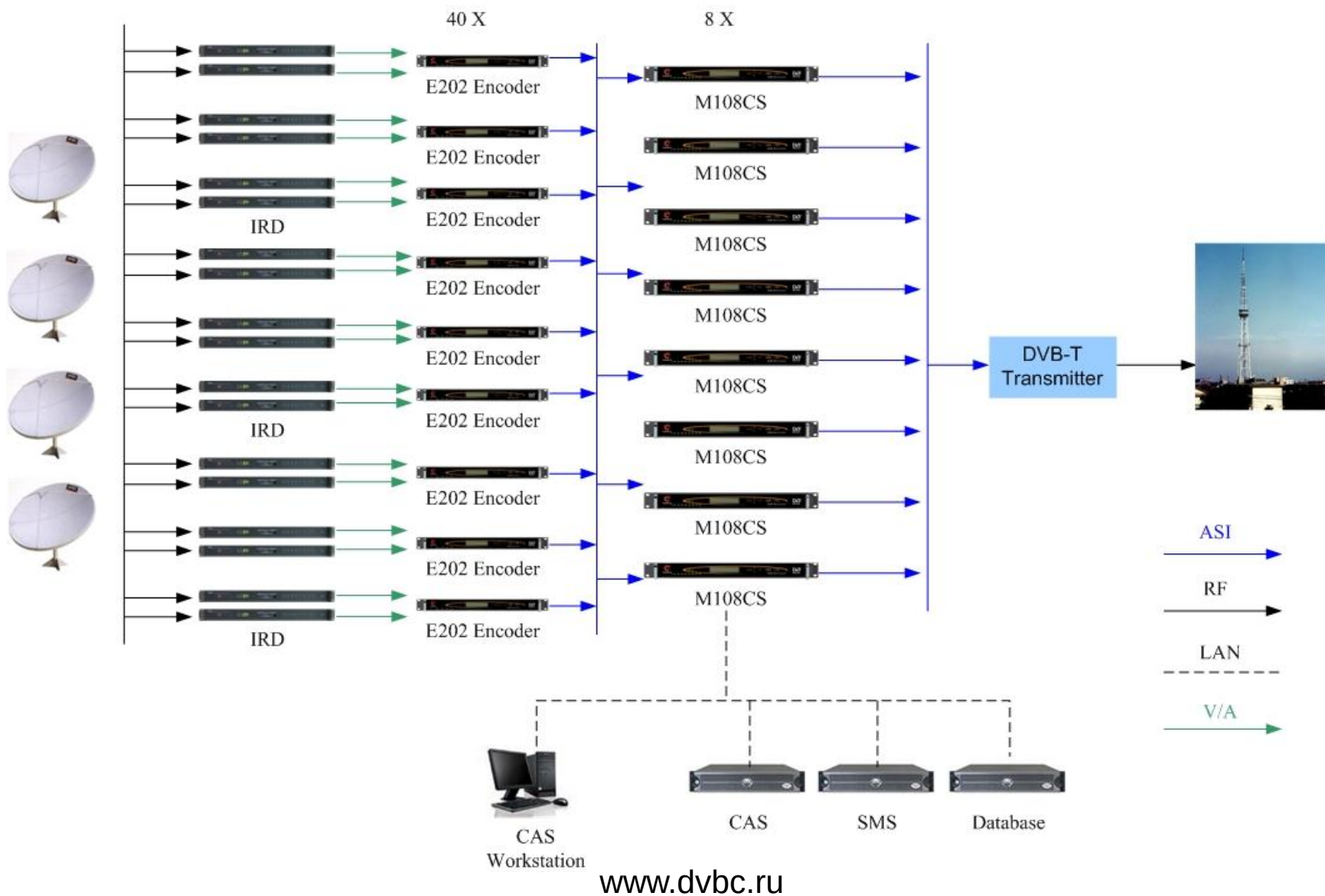
- Skyworth
- WELLAV
- Dehoo
- Coship
- Hisense
- Xoceco
- SMIT
- OKI
- Conexant system
- DAYANG
- TVwalker
- Biaoqi
- China integrated circuit
- CHANGHONG
- BVcom media
- DTC industrial
- Zoran
- Mingxing Technology
- Jingwei Baian
- Tetong
- Tsinghuatv
- Zdtong
- Inspur
- DMT
- Daya
- NEXS (Korea)
- Gospel
- Hangwang
- Baustem
- SDG Information
- PBI
- Haier
- Ascom Media
- Dongtai
- Beiguang Media
- Dahua Tech.
- Yinhe
- Malta
- Image Silicon
- Jiuzhou Tech
- Golden Net
- Net
- Unitend
- Global Tech
- Guangdong BBK
- Teer
- Intercross(Russia)
- Vityaz(Belarus)
- Geeya
- Yingji
- Biecc
- Blossoms
- Unitend
- Tsinghua Tongfang Legend Silicon
- Hisense
- TCL
- Haier
- Cycle Century
- Konka
- Newland
- Zhida
- Wanxiang Digital
- Motorola

Реализованные проекты

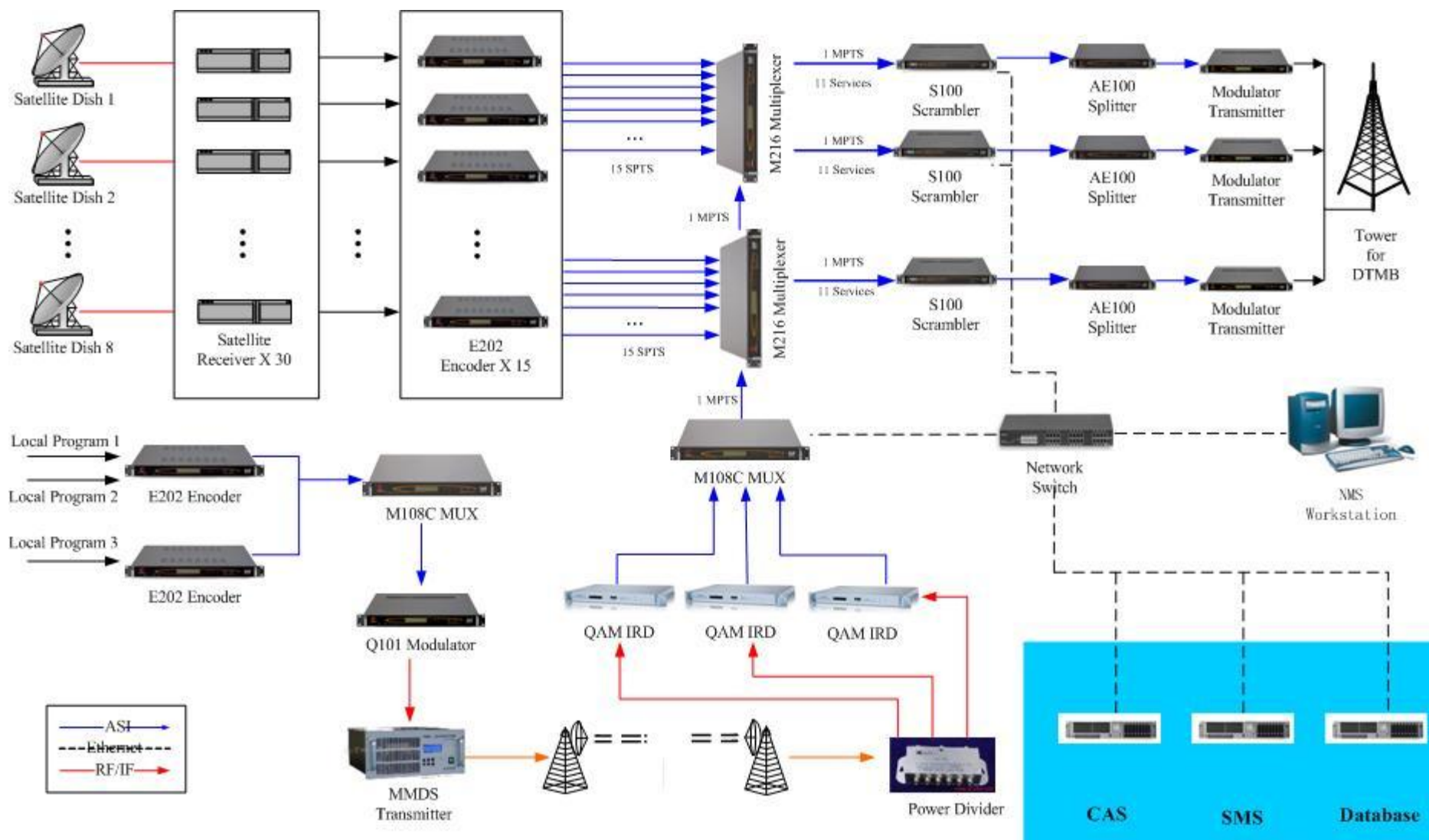
Telmex, Колумбия DVBC-S



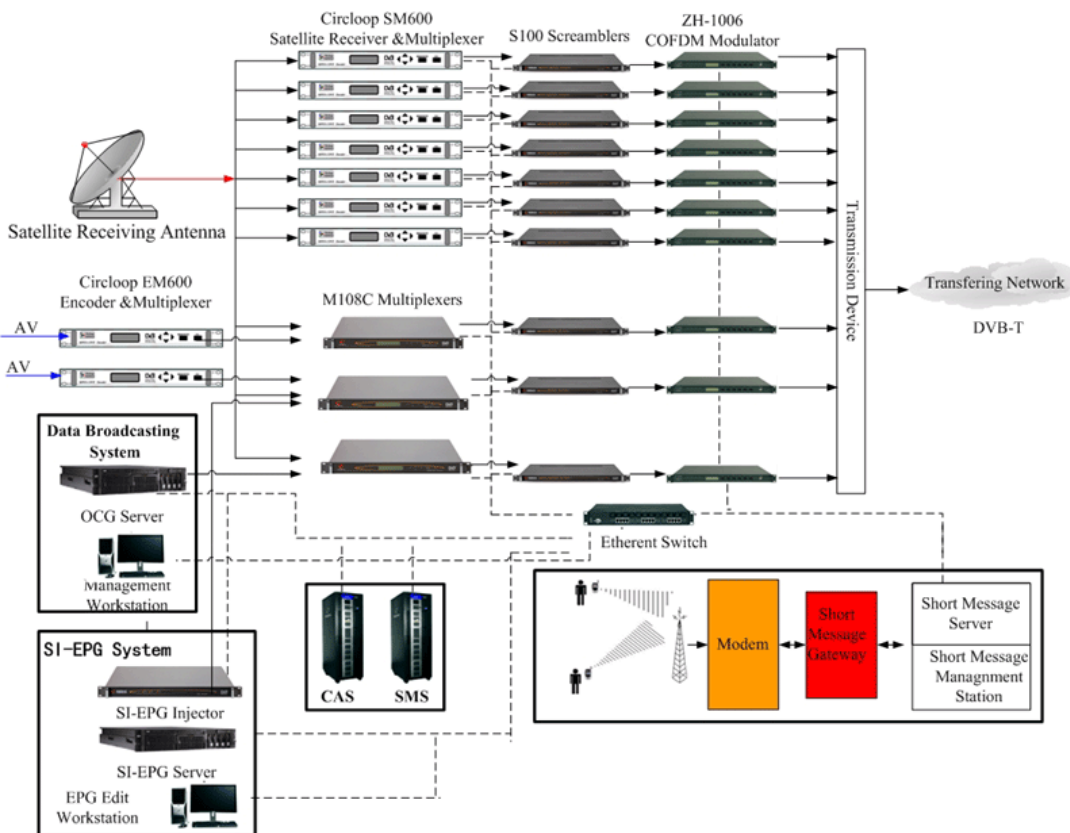
MNBC, Монголия DVB-T



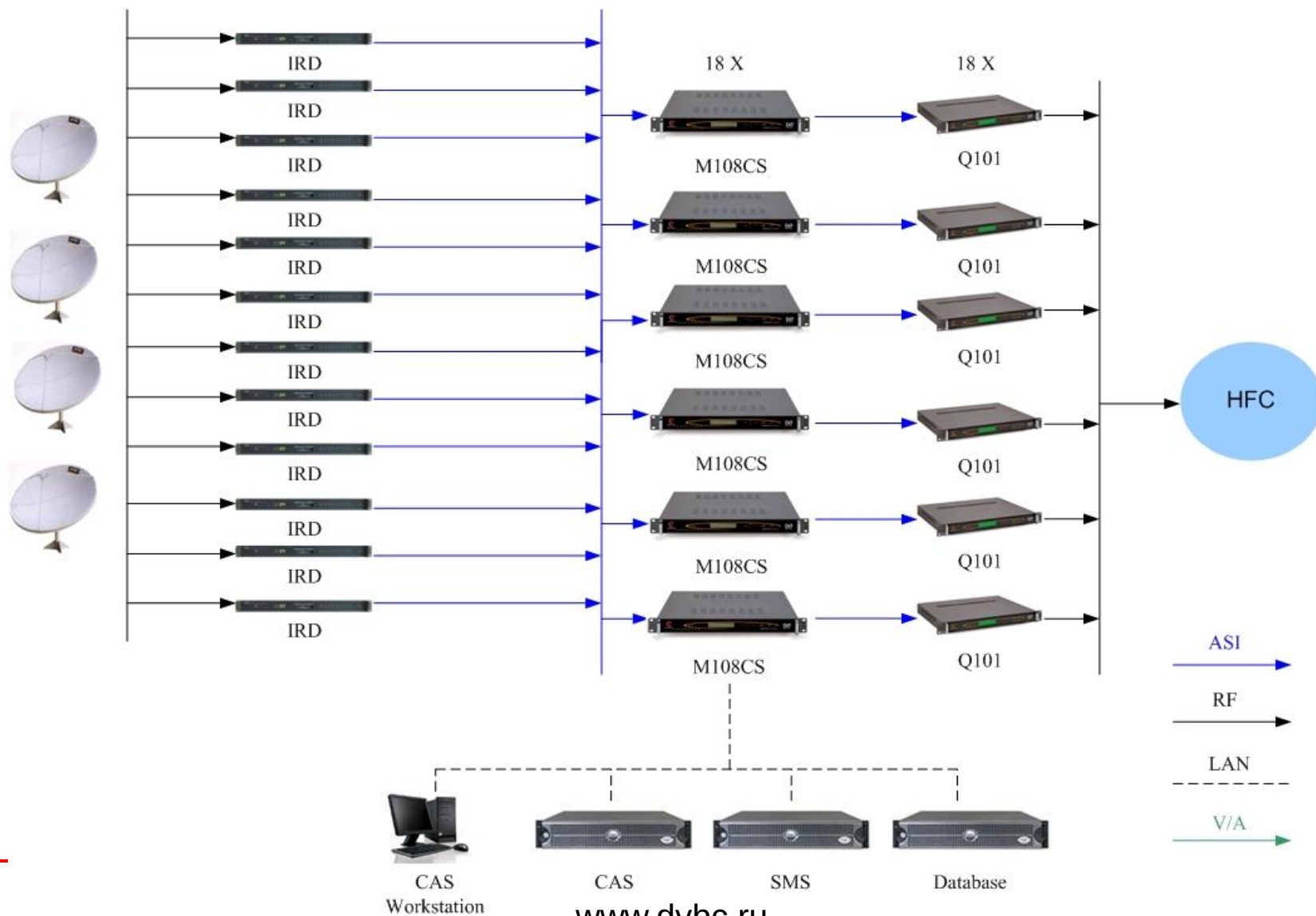
National TV Station, Јаoc, DTMB



EasyTV, Танзания, DVB-T

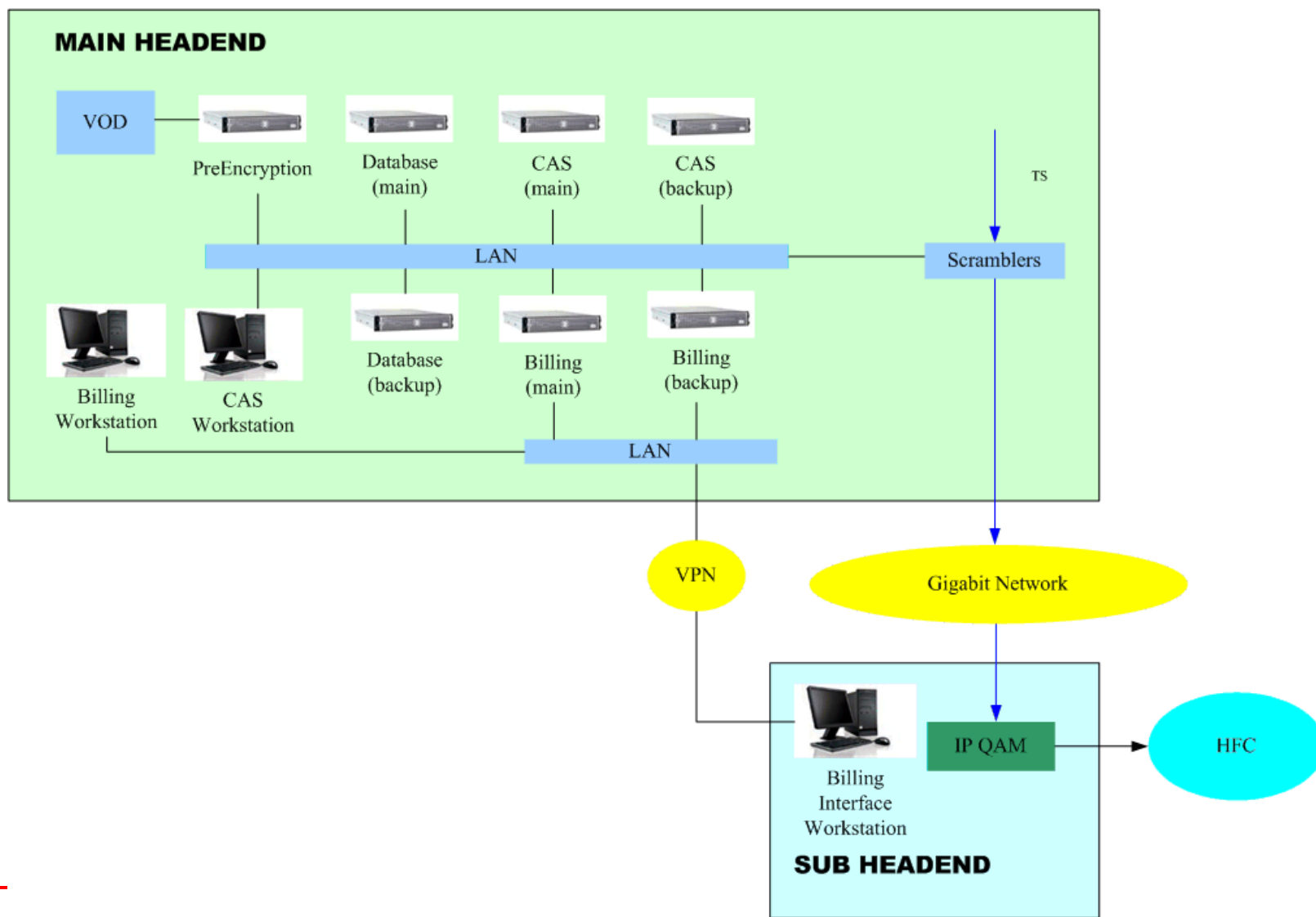


Sheriff TV, Молдова, DVB-C

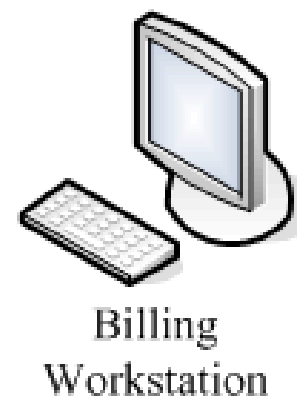
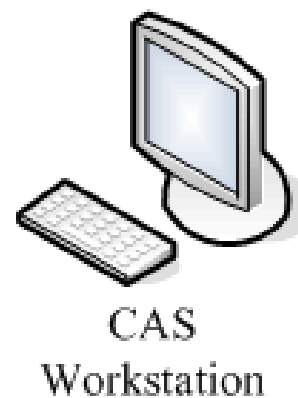
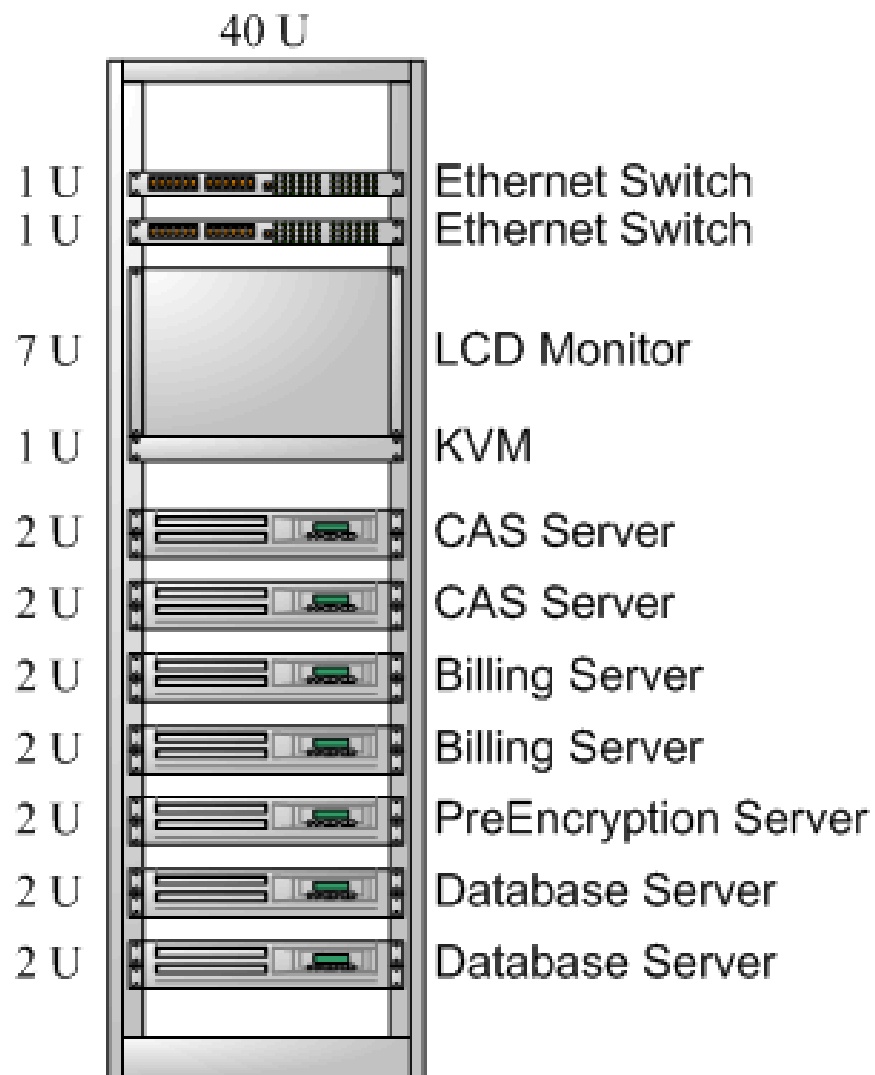


Система кодирования

Структурная схема системы кодирования

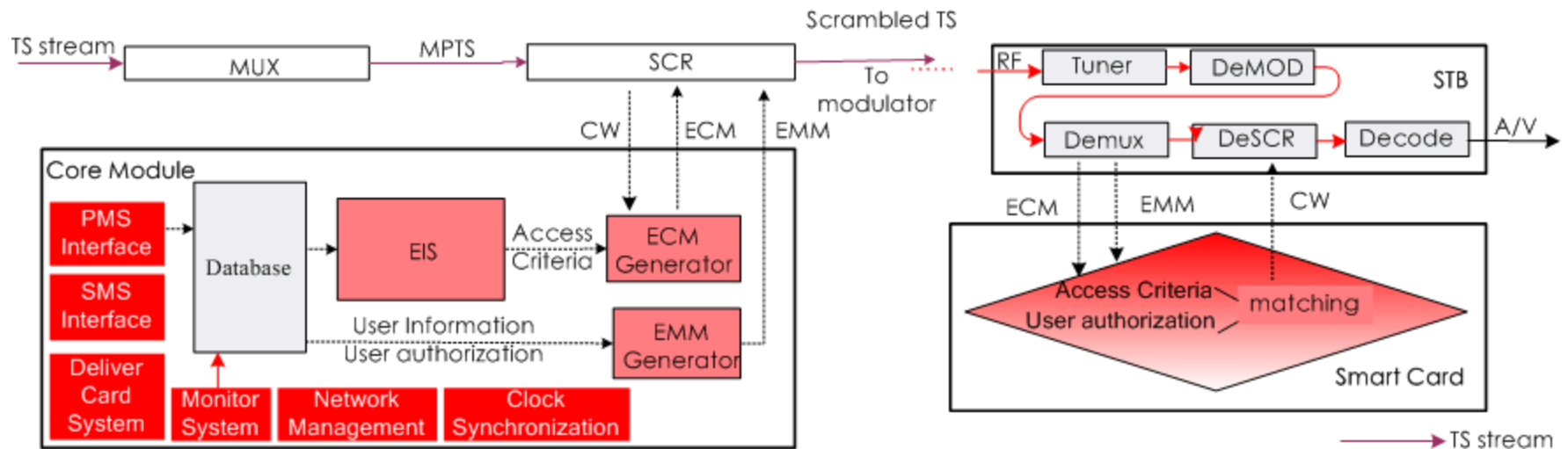


Расположение оборудования в стойке



Ядро системы кодирования

Архитектура системного ядра



ECM: Entitlement Control Message
(encrypted CW, Access Criteria, etc)

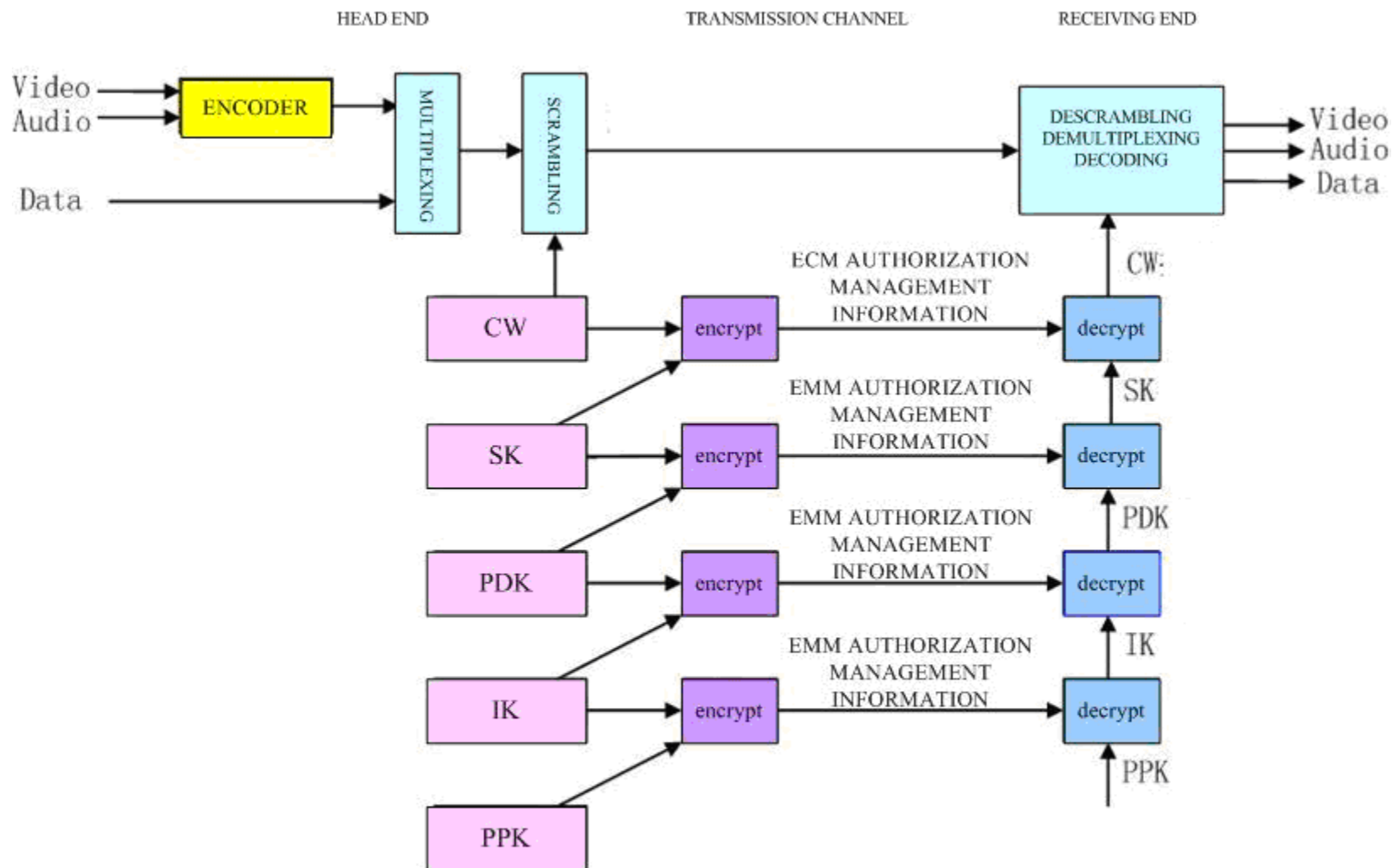
EMM: Entitlement Management Message
(User authorization, control order, encrypted key, etc)

EIS: Event Information Scheduler

CTI-CAS. Основы защиты доступа

- Реализация common encryption алгоритма, система многоуровневого ключа кодирования
- Обновление контрольного слова каждые 5-10 секунд
- Постоянный контроль периода авторизации для предотвращения доступа к просмотру после окончания периода доступа
- Независимо разработанная COS смарт-карта, защищенная от пиратского копирования
- Система безопасной авторизации. Система CTI CAS ни разу не взламывалась за всю свою историю существования
- Алгоритм замещения кодирования. Улучшенная системная безопасность
- Поддержка функций временного прекращения авторизации и удаления из системы любой смарт-карты

Многоуровневые ключи кодирования



Период обновления каждого из ключей

Ключ	Рекомендуемое обновление	Минимальное обновление
CW	5~10 секунд	5 секунд
SK	1 месяц	1 час
PDK	3 месяца	1 час
IK	1 год	1 час
PPK	Статический	Статический

СТI-CAS – СМАРТ-КАРТЫ

Технология защиты смарт-карт:

- Независимо разработанная COS смарт-карта
- Использование CMOS чипа с высокой степенью защищенности
- Использование общего алгоритма и специального кодирующего алгоритма для обеспечения безопасности передачи данных (3DES,CES,AES,IDEA)
- Кодовые приложения и алгоритм загрузки
- Защищенный чипсет



EAL 5+ Сертификаты смарт-карт



BSI-DSZ-CC-0340-2005
Infineon Smart Card IC (Security Controller)
SLE66C168PE/m1530-a25,
SLE66C84PE/m1538-a25,
SLE66C44PE/m1539-a25 and
SLE66C24PE/m1563-a25
with specific IC Dedicated Software
from
Infineon Technologies AG



The IT products identified in this certificate have been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0 extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999) and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

PP Conformance: Protection Profile BSI-PP-0002-2001
Functionality: BSI-PP-0002-2001 conformant plus product specific extensions
Common Criteria Part 2 extended
Assurance Package: Common Criteria Part 3 conformant
EAL5 augmented by:
ALC_DVS.2 (Life cycle support - Sufficiency of security measures),
AVA_MSU.3 (Vulnerability assessment - Analysis and testing for insecure states),
AVA_VLA.4 (Vulnerability assessment - Highly resistant)

This certificate applies only to the specific version and release of the products in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 30. September 2005

The President of the Federal Office
for Information Security



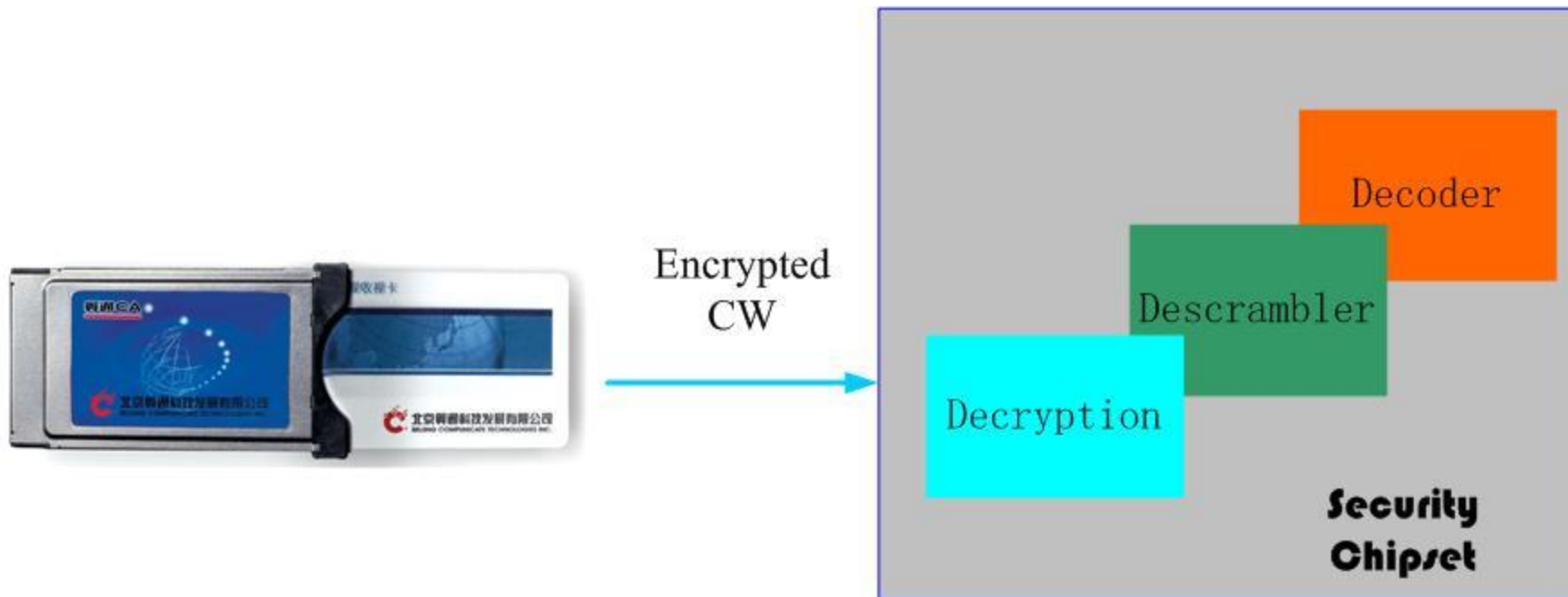
Dr. Helmbrecht

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 · D-53175 Bonn · Postfach 20 03 63 · D-53133 Bonn
Phone: +49 228 9592-0 · Fax: +49 228 9592-455 · Infoline: +49 228 9592-111



Защищенный чипсет



Партнеры-производители защищенных чипсетов

- **Чипсет:**
 - ST
 - Broadcom
 - Ali (в разработке)
 - Haier (в разработке)
- **Абонентские приставки:**
 - Skyworth
 - Motorola
 - Coship
 - Huawei (в разработке)
 - New Land (в разработке)

Сертификаты на производимые чипсеты



北京算通科技发展股份有限公司
BEIJING COMMUNICATE TECHNOLOGIES INC.

No.901-905, Office Building B Maples International Center, No.32 Xizhimen North Street, Haidian District,
Beijing 100082 P.R.C

Communicate Technologies Inc.

Chip Security Certificate

This is to certify that

STMicroelectronics

STi5197

Has been tested by **Communicate Technologies Inc.** and found to be compatible with
Communicate's **CTI CAS v3.0**

Following features have been certified,

- Secure Control Words
- jTag protection
- Secure boot

Mr. Pengfei Gao
Chairman & CTO
Communicate Technologies Inc.

Signature:

Date: 2010.3.30

Mr. YU Lee
Vice President of Greater China & South
Asia Region
General Manager of Digital Consumer
Segment STMicroelectronics

Signature:

Date: 2010.04.12



COMMUNICATE TECHNOLOGIES INC.

Certificate of Approval for CA
is hereby Granted to

Shenzhen Skyworth Digital Technology Co., Ltd

STB Model: C7000NX
Chip Model: STI5197BFBC
V3.20 Version

Sign:

Date: 2010-7-30

No. : 2010073032001



COMMUNICATE

CTI-CAS – системные характеристики

- Максимальное количество абонентов – 3 миллиона
- Количество кодируемых телеканалов - $8 \times 256 = 2048$; классификаций - 256; тематических групп - 256
- Поддержка до 4 различных регионов обслуживания
- Максимальное количество программ-провайдеров: 8
- Скорость передачи:
 - EMM 100-1500 пакетов/сек (полоса 0.15-2.2Mbps),
 - ECM 2-5 пакета/секунда/канал
- Один ECMG и EMMG поддерживается в 20 TS

STI-CAS – главная и зависимые карты

- Одна главная карта поддерживает несколько зависимых карт
- Авторизация зависимой карты через приставку с главной картой
- Срок работы зависимой карты определяется оператором
- Данная функция должна поддерживаться приставкой

CTI-CAS – главная и зависимые карты



Master card STB

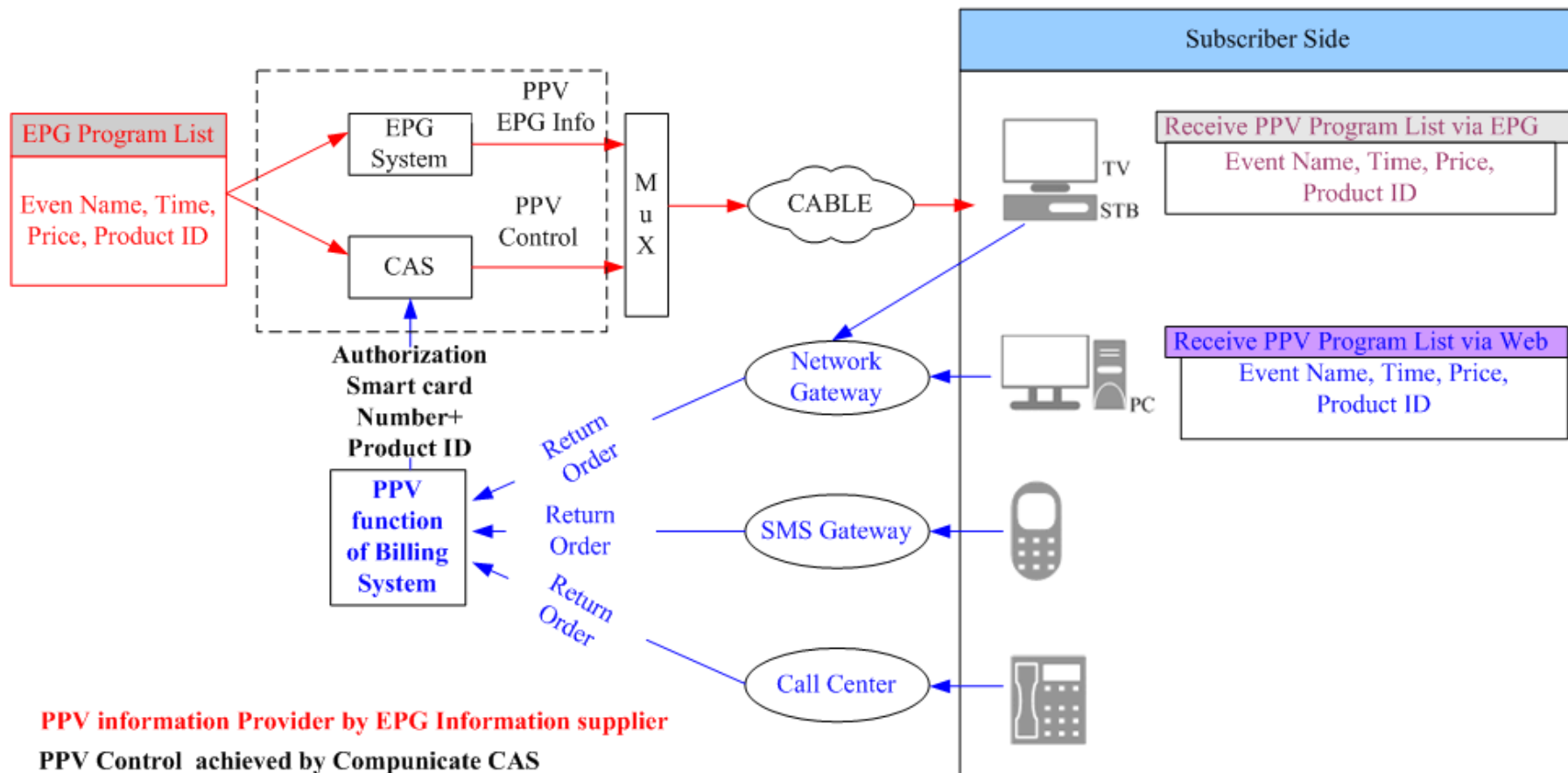


Subsidiary card STB

← Getting authorization →

Интеграция PPV с системой EPG

CTI-CAS PPV Working flow



PPV information Provider by EPG Information supplier

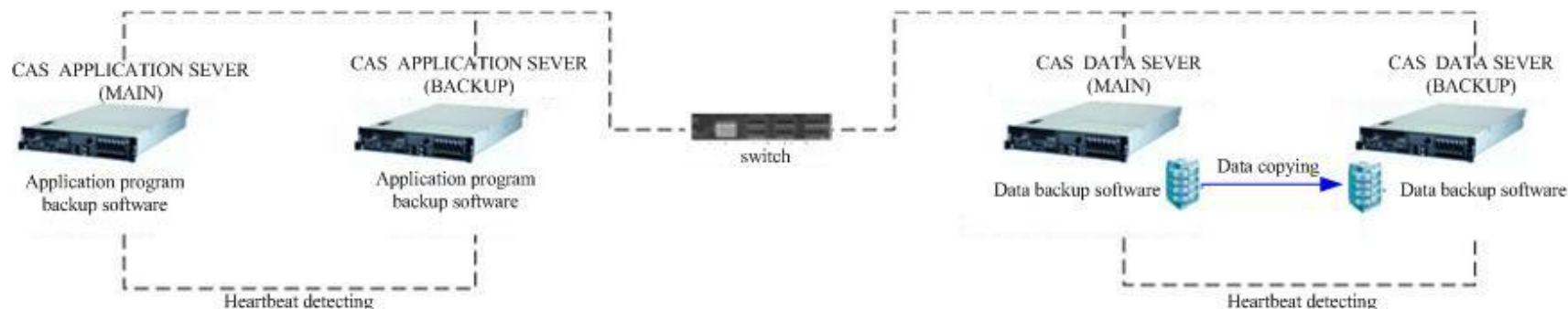
PPV Control achieved by Communicate CAS

STB should display EPG with PPV information

Suggest Billing System Provider to develop Blue parts with Telmex

СТІ-CAS. Архитектура резервирования

- Поддержка главного и резервного сервера
- Программное обеспечение, поддерживающее резервирование



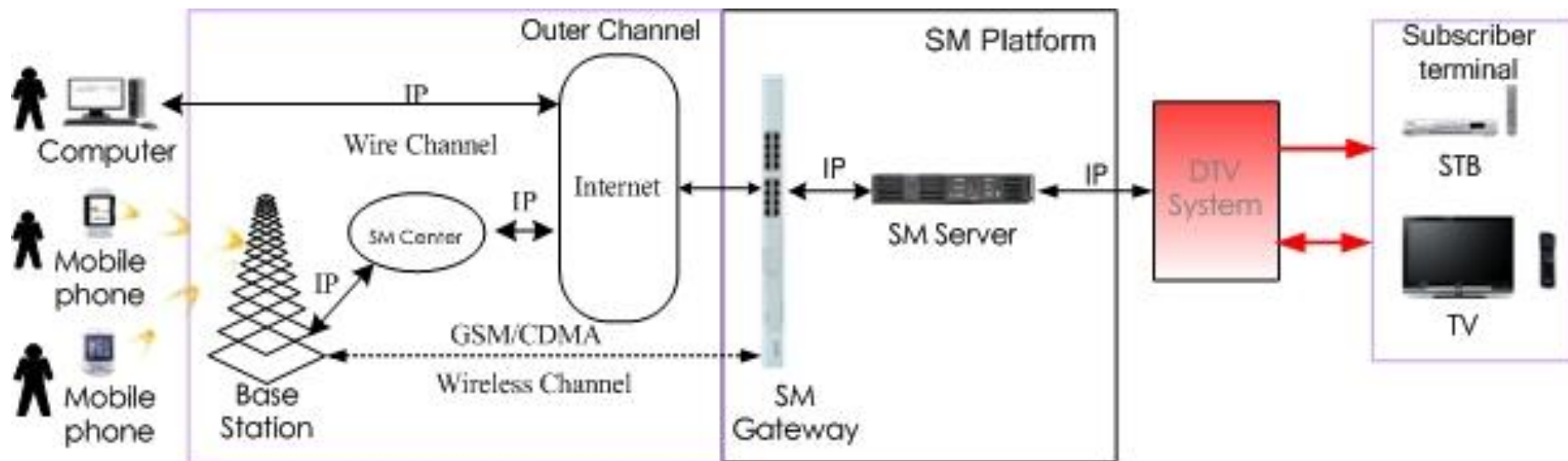
TVM – платформа СМС

Оплата доступа через СМС

- Организация СМС-центра оператора
- Взаимодействие ядра системы кодирования и СМС
- Списание средств
- Запрос баланса
- Заказ программ



TV платформа СМС



TVM платформа СМС

- Модульный дизайн
- Поддержка систем кодирования, в том числе двусторонних
- Гибкая и надежная система выставления счетов
- TVM поддерживает функцию «Сохранить все сообщения» и базу данных
- Абонентам доступны функции запроса выставления счетов, списывания средств, покупки пакетов программ через отправку СМС

IPRV-T и карты предоплаты



map | job | home

HOME Program Program

operator manager

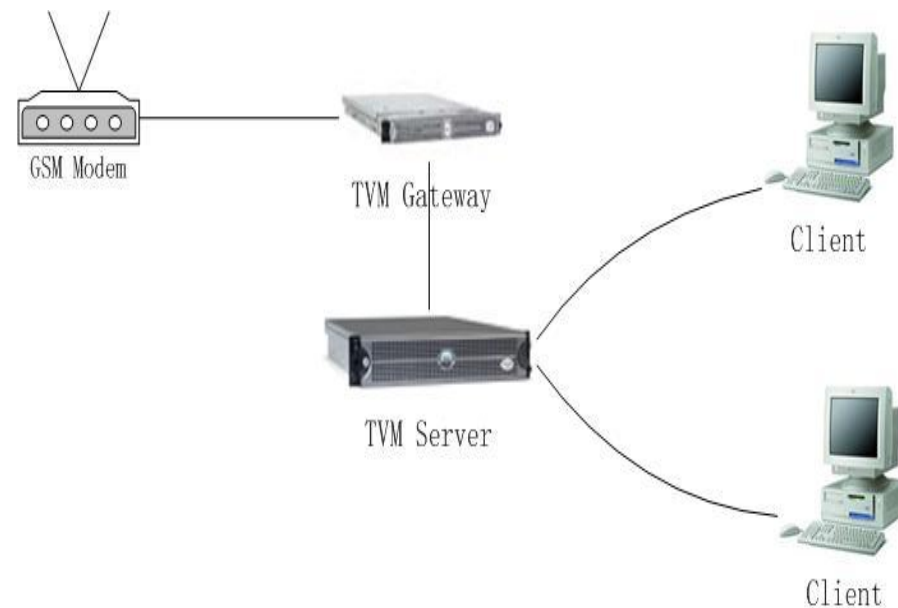
Function	Format in mobile message
Need Help	HLP#
Complain	CPL#
Open Account	OPE#
Query Balance	BAL#[smartcard number]#[password]
Charge Money	CHA#[smartcard number]#[password]
Purchase Product	PUR#[smartcard number]#[password]#[product number]
Cancel Product	CAN#[smartcard number]#[password]#[product number]
Transfer	TRA#[smartcard number]#[password]#[amount]
Change Password	PWD#[smartcard number]#[old password]#[new password]

all the features of
IC card

\$99

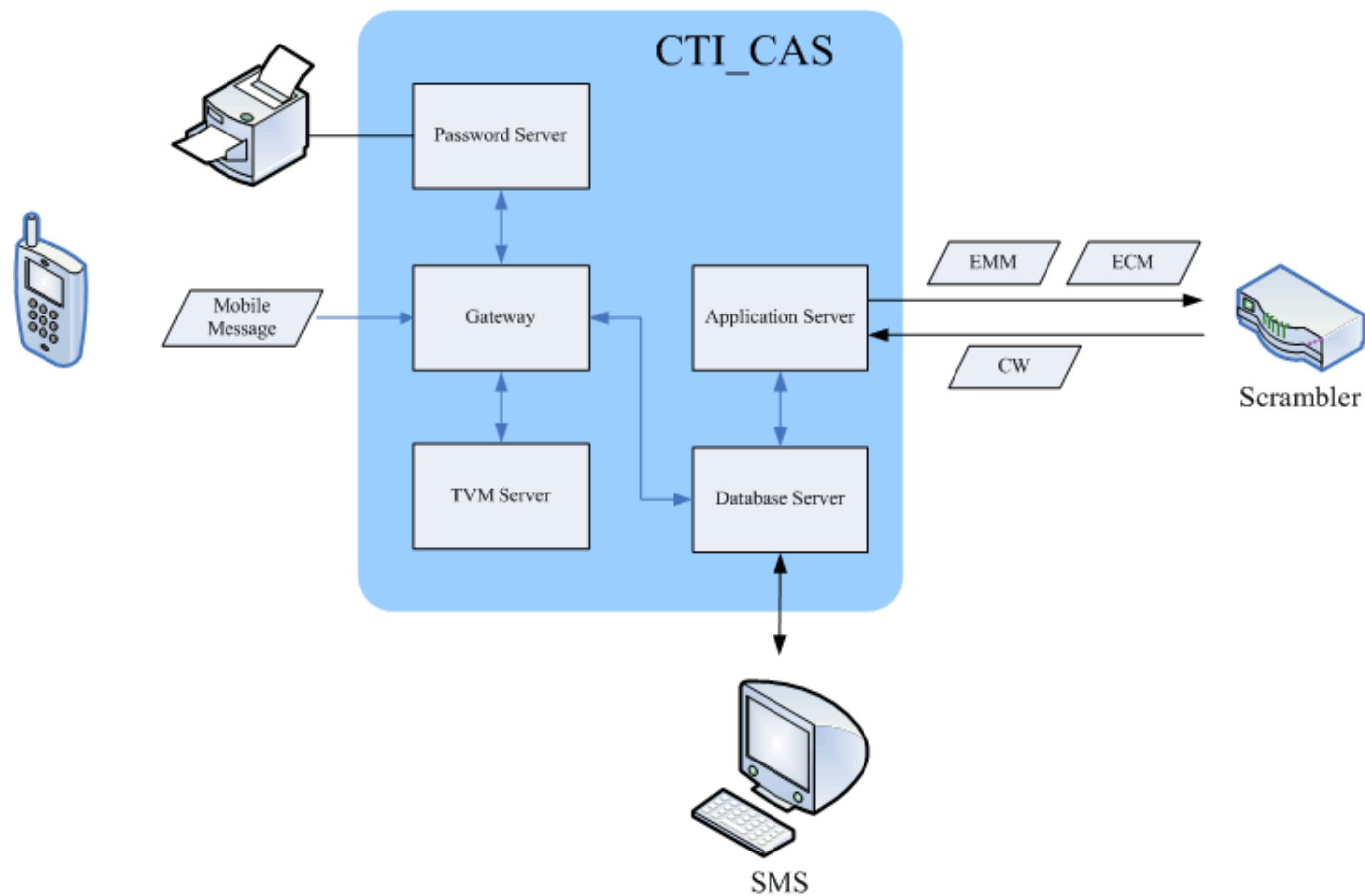
TEL: + 0086

More 



TV Message System Structure

Система кодирования, TVM и СМС

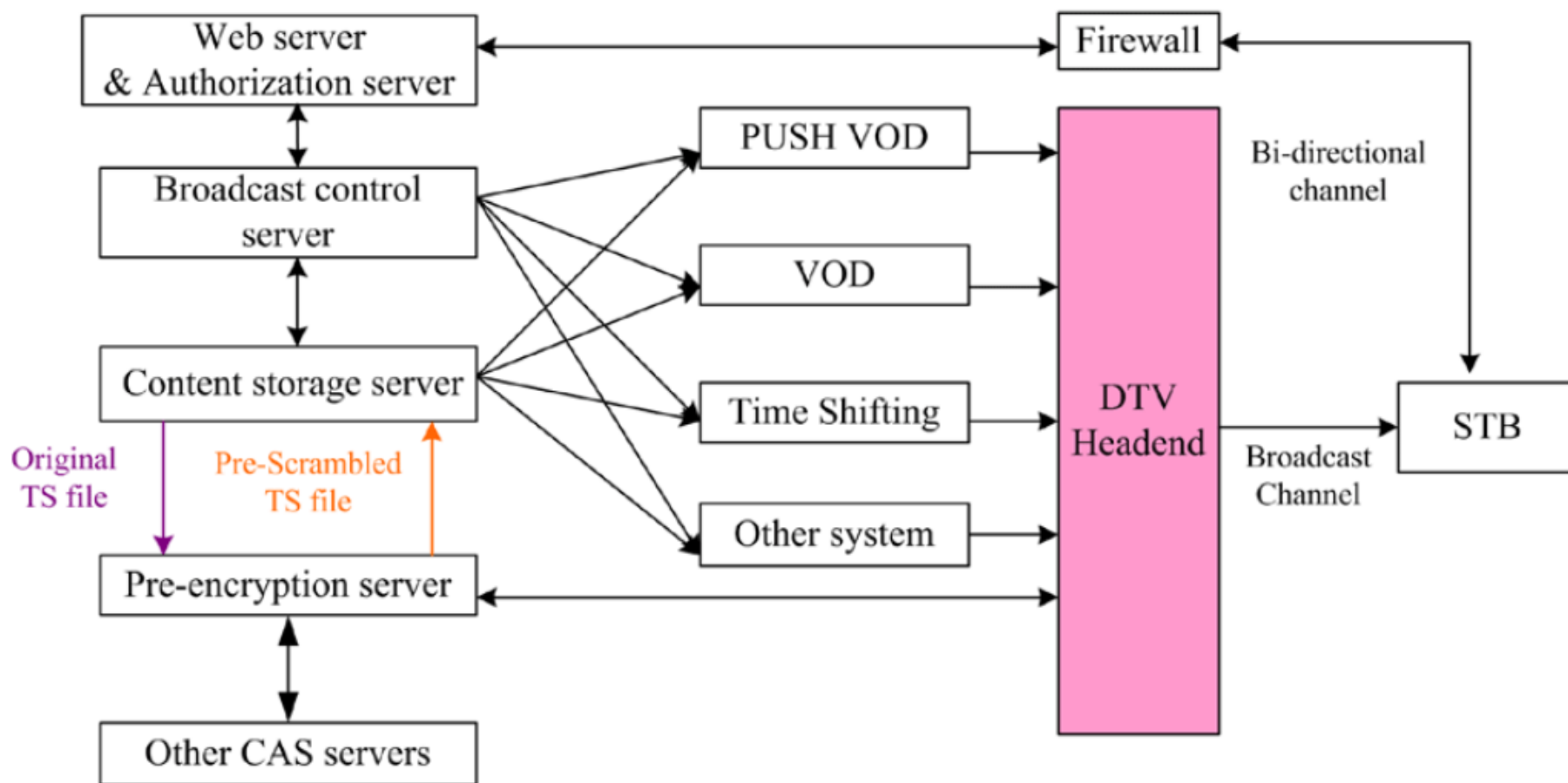


Алгоритм предварительного кодирования

Функциональные особенности

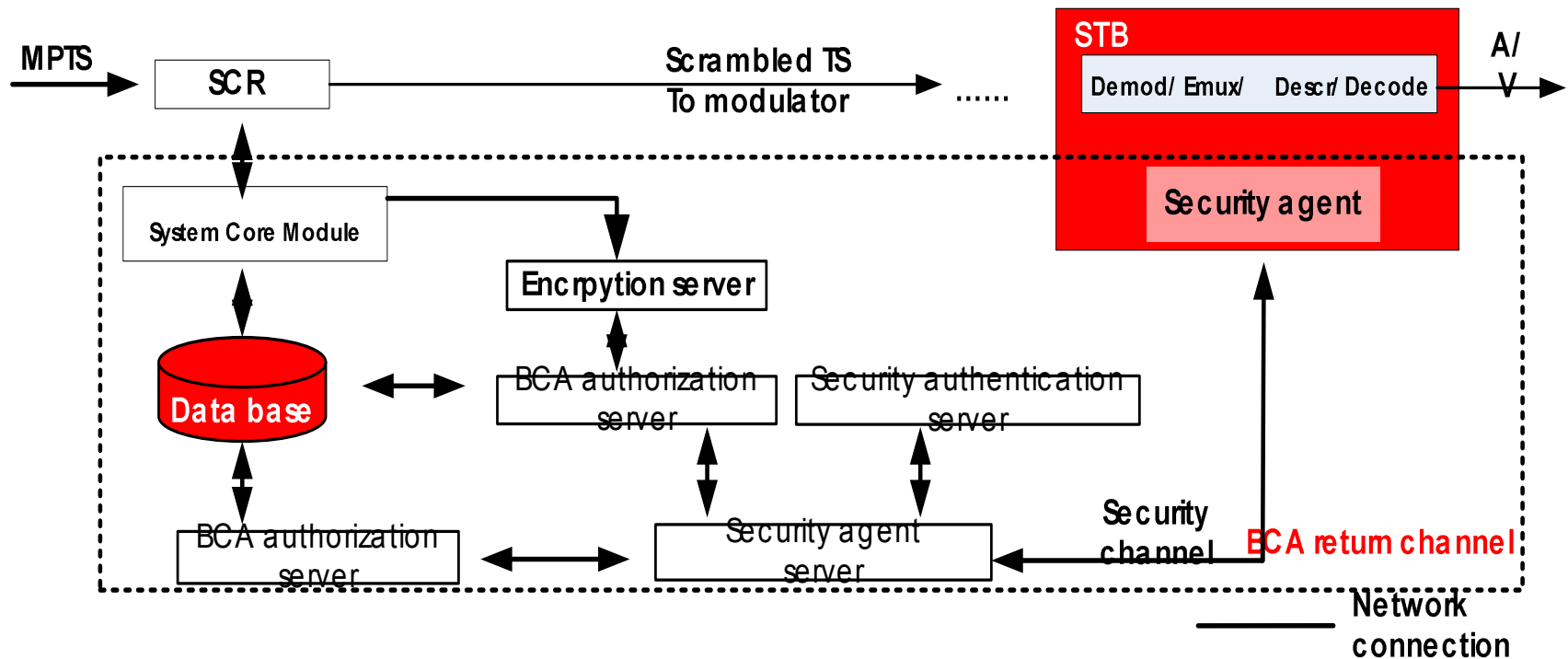
- Кодированная программа сохраняется на носителе информации
- Поддержка VOD, PUSH VOD, PVR приложений
- TS файл не может быть декодирован offline:
 - ECM расположен в самом TS файле
 - EMM передается в режиме онлайн

Структура системы предварительного кодирования



Двусторонняя система условного доступа (BCA)

BCA



Функциональные особенности:

- Авторизация пользователей, различные виды аутентификации статусов, более высокий уровень защиты контента
- Передача данных интерактивных сервисов
- Расширенные возможности сбора статистических данных об абонентах, в том числе рейтинга телепрограмм

- Широкие возможности интерактивной связи с абонентами
- Регистрация, вход/выход абонента из системы через абонентский терминал
- Получение рейтингов и статистических данных
- Резервирование программ PPV и многое другое