

Technical Meeting DGTVi and ANIE – STB vendors

Cologno Monzese
17th of June 2005

Contents



1. Channels ordering

2. API for T-Government and Smart Card no CA

3. MHP Security

4. Hierarchical Modulation

5. Band III Signals (VHF)

Channels ordering: aims, requirements and options



- **Aims:**

- Arrange a system that permits channels ordering on the basis of a predetermined sequence. The specifications defined by DGTVi describe the STB behaviour and the characteristics of broadcasted signal, independently of the specific sequence of the services

- **Requirements:**

- The user can modify, whenever he/she wants, the proposed channels ordering
- The user's choice is dominant respect to eventual updating of channels ordering, either logic or manual.

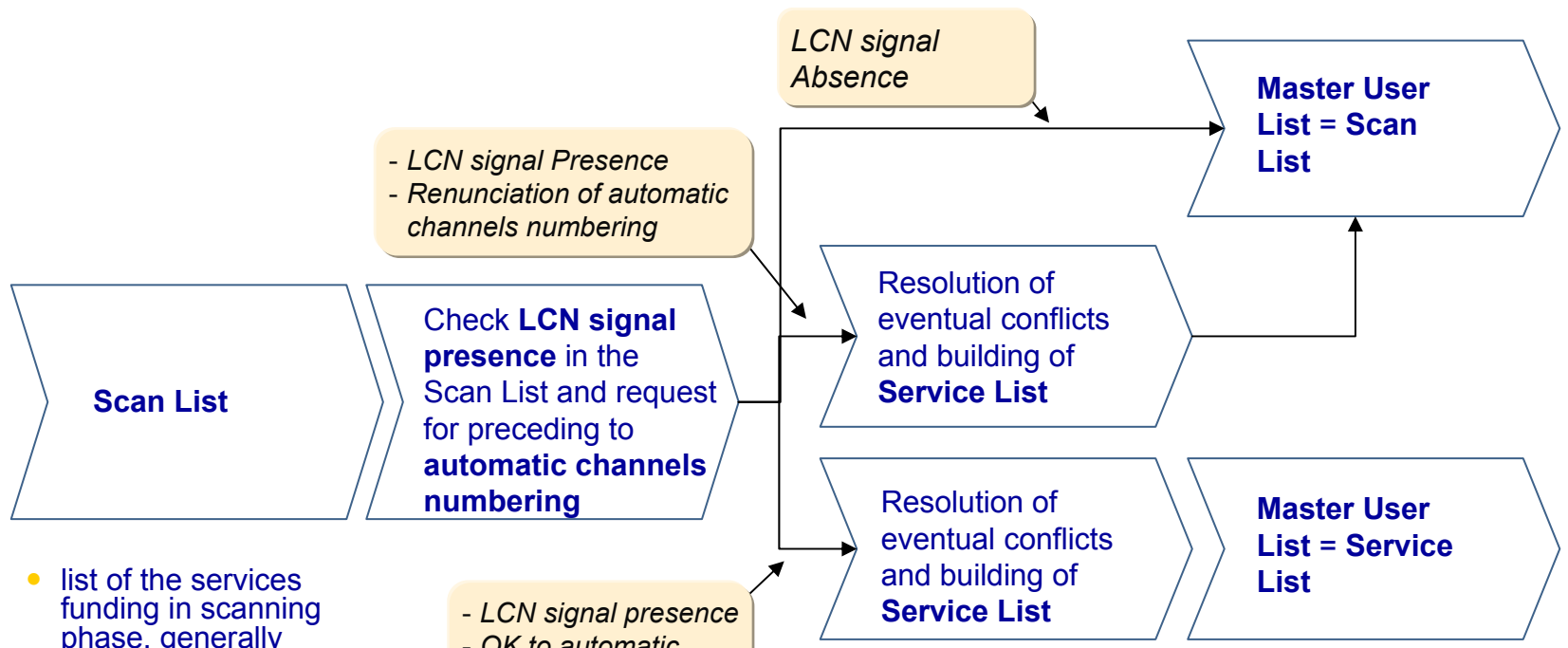
- **Options:**

- Every STB vendor can manage personalized services lists

Characteristics of Italian market

- The DGTVi proposal for automatic channels ordering is based on the Logical Channel Number (LCN) defined by EICTA specifications
- The characteristics of Italian market have required a particular examination in order to manage potential conflicts deriving from coexistence, in the same area, of locals TV signal from different areas or individual preferences of user in the positions allocation
- Consequently, two zone had been reserved to the services that are in conflict with each other and are not allocated:
 - *From 75 to 99 (Preferences Overflow)*
 - *From 850 to 999 (Main Overflow), if the first area is not sufficient*

Building Process of Master User List at the first installation phase



- list of the services funding in scanning phase, generally arranged on the basis of frequency, with eventual LCN associated

- Services List created and updated on the basis of LCN requests deriving from Scan List, after the resolution of eventual conflicts, automatic or manual

- Services list, at first identical to the Service List or to the Scan List, that register the manual modifications made by the user, marking them with the tag "user defined"

Contents



1. Channels ordering

**2. API for T-Government and Smart Card
no CA**

3. MHP Security

4. Hierarchical Modulation

5. Band III Signals (VHF)

Updating of STB specifications in order to manage the T-Government

- The opportunity to offer T-Government services (T-Gov) is essential for the DTT development in Italy
- In order to manage T-Gov services, the MHP standard must be consistent with two fundamental requirements: security and interactivity
- In particular, the MHP applications must be able to manage:
 - Interoperability with any kind of Smart Card corresponding to the standard ISO 7816
 - Sensitive data encrypted over interactive channel

T-Government services requirements

Requirements

- Access to information in the Smart Card
- Access to sensitive information on the Smart Card through a cryptographic system
- Authenticate the citizen (through STB) when he is connected to Back End infrastructure via interactive channel, using the Smart Card as access key
- Store on the Smart Card services / functionalities in order to save on air bandwidth

Examples

- Personal data
- Serial Number of Smart Card
- Sanitary data
- Personal Certificates
- Delivery of personalized and sensitive information by Institutions to the citizen
- Distribution services / functionalities of public interest

Necessary specifications in order to satisfy the T-Gov requirements

- The 1.0.x version of MHP standard, today on the market, haven't a sufficient API set to manage T-Gov applications with minimum required standard of security and interoperability
- a complete API set, adequate for that aims, is introduced on the recent version 1.1.2 of MHP standard
- In order to satisfy the minimum requirements of T-Gov applications (enter to information in the Smart Card), the DVB SATSA specification, present in this set, should be implemented:
 - *Generic Connection Framework*
 - *APDU*

Contents



1. Channels ordering
2. API for T-Government and Smart Card no CA
- 3. MHP Security**
4. Hierarchical Modulation
5. Band III Signals (VHF)

The MHP security model



- In order to protect the user and the system integrity, MHP had developed a security model based on Public Key Infrastructure (PKI), that guarantee the access to determined receiver facilities (return channel, tuner, smart card, semi-permanent memory) only to applications signed by recognized certificate
- The right support to MHP security model is required by ETSI certification for the branding and so it is in all receivers available on the market.
- At the moment, the checks foreseen by this model are disabled because of the absence of PKI

Guarantees given by the MHP security model

- The MHP security model doesn't guarantee that the application is free from faults and, if there were, it cannot impede the transmission
- Instead, an application consistent with MHP security model assure that:
 - *Who has signed the application he can be responsible of eventual damages caused*
 - *A potential Authority could verify and certify the applications before they were transmitted, so guaranteeing an extra level of stability to the system*
 - *DGTVi believes that the complete starting up of MHP security cannot be derogated in Italy*

Actions



- Defined policy for release and revocation of signature certificates
- Identification of a possible Certification Authority for releasing Root Certificates
- Identification of a possible Signing Authorities for the signatures of applications
- The associated assure the OTA updating on the STB for the Root Key installation and for the activation of MHP security checks

Contents



1. Channels ordering
2. API for T-Government and Smart Card no CA
3. MHP Security
- 4. Hierarchical Modulation**
5. Band III Signals (VHF)

Today scenario and possible evolution

- Today:
 - *Modulation: QPSK 16-QAM and 64-QAM constellation, on the basis of Determination AGCOM n. 216/00/Cons.*
 - *For Italian market, the present configuration of STB doesn't provide for adequate management of signals in hierarchic modulation*
- DGTVi specifications (D-Book 1.0) on hierarchic modulation:
 - *The receivers should be able to demodulate correctly the signal when there is a hierarchic modulation (in high and low priority)*
- Possible evolution:
 - *Several broadcaster are interested to adopt hierarchic modulation in order to transmit mixed DVB-T/DVB-H signals on the same Mux*

Requests for STB updating



- SW availability for qualify the hierarchic demodulation (in high and low priority) on all decoders models (old and new)
- Possibility for updating STB via OTA with the new SW version

Contents



1. Channels ordering
2. API for T-Government and Smart Card no CA
3. MHP Security
4. Hierarchical Modulation
- 5. Band III Signals (VHF)**

Today scenario and possible evolution

- Today:
 - Referring to band III VHF, the present configuration of DTT receivers guarantees a right decoding only for the signals with channelization (Italian) at 7 MHz
- DGTVi specifications (D-Book 1.0) on the band:
 - 7 MHz in III VHF band and 8 MHz in IV – V UHF band, consistent with National Plan for the Frequencies Assignment
 - The Plan provides for the possibility, in the future, to use a 8 MHz bandwidth also for the III VHF band
- Possible evolution:
 - Several broadcasters are interested to use channels both at 7 MHz and at 8 MHz on the III VHF band, choosing each time the appropriate bandwidth according to interference status of the given area

Information Request



1. Possibility to qualify the VHF reception both at 7MHz and at 8 MHz on every decoder model (old and new one)
2. Manage capacity, indifferently, a mixed VHF signals both at 7 MHz and at 8 MHz
3. Possibility to upgrade the installed base STB via OTA
4. Timetable for the realization

Provisional Working Plan 1/2

To discussion



Activities	Responsibility	2005				2006								
		May	June	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	
• LCN Project - Development and test software for the LCN management - Availability "off- the-shelf" of STB updated for manage LCN - Start of signal transmission with LCN		- STB Producers												
• T-Government Project - Development and test software for the management of SATSA modules - Availability "off- the-shelf" of STB updated for manage T-Government		- STB Producers												
• Security Project - Definition of policy for release and revocation of signature certificates - Identification of possible national Certification Authority - Root Key Implementation - Availability "off- the-shelf" of STB updated for manage Root Key		- STB Producers												

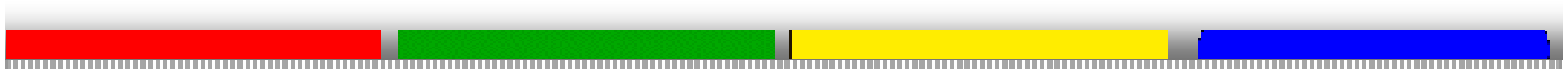
Provisional Working Plan 2/2

To discussion



Activities	Responsibilities	2005					2006						
		May	June	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr
<ul style="list-style-type: none"> • Hierarchic Modulation <ul style="list-style-type: none"> - Availability of SW to qualify the hierarchic demodulation for: <ul style="list-style-type: none"> . old models STB . new models STB 	- STB Producers												
	- STB Producers												
<ul style="list-style-type: none"> • Updating OTA for STB stock installed 													

ENCLOSED



Enclosed - Contents



- 1.Channels numbering**
- 2.API for T-Government and Smart Card no CA**

Details of building process of Service List and STB specifications

Process

- When there is LCN and when there aren't conflicts in positions allotment: Service List building
- When there is LCN with conflicts in positions allotment:
 - conflicts solution by the viewer and Service List building
 - if the user doesn't intervene, STB automatically chooses the first service on the list after a fixed interval and Service List building
- Collocation of the services in conflict not assigned on the first free position in the zone 75 -99 (Preferences Overflow), if available; instead, collocation of the services in conflict not assigned in the Main Overflow (850 – 999)

STB specifications

- Presentation Menu of the automatic channels numbering service and Service List recording
- Presentation Menu and management of services in conflict; Service List recording
- Time-out facility for automatic conflict solution on the basis of the first service of the services in conflict list; Service List recording
- Definition of two reserved zones for the allocation of services in conflict:
 - 75 – 99, Preferences Overflow
 - 850 – 999, Main Overflow

Master User List management

- Positions not assigned or assigned to “hidden” services are “holes” in the Master User List:
 - *They are “skipped” through zapping with P+/P-*
 - *Selecting them from the remote control it is tuned:*
 - ▶ *The “hidden” service, if it is, or*
 - ▶ *The first service really present in the following,*
- User can move, in every moment, any service in any position of Master User List:
 - *If the shift is to a free position, this is occupied and marked as “user defined” while the originating position is delivered*
 - *If the shift is to an occupied position, the services simply exchange their positions each other and the destination position is marked as “user defined”*
- Following the shifts, the Master User List doesn't correspond any more with the Service List or with the Scan List (in any case both must be store)

Service List updating

- If a new service, get in the manual or automatic update phase, is associated with:
 - *any LCN :*
 - ▶ *in the Service List, it is given the first free position in the zone Garbage*
 - *a LCN that corresponding to a free position and there aren't any requests for the same position*
 - ▶ *in the Service List it is given the required position*
 - *a LCN corresponding to a free position and there are other requests for the same position*
 - ▶ *the conflict is solved like in the first installation phase*
 - *a LCN corresponding to an occupied position from another service with the same LCN*
 - ▶ *the conflict is solved like in the first installation phase*

Master User List updating

- After the Service List updating, if user chose the automatic channels numbering in the first installation phase, the box updates the Master User List, copying the Service List, position by position, on the basis of following rules:
 - *The Master User List positions don't marked as "user defined", are occupied by the service corresponding to that position in the Service List*
 - *The Master User List positions marked as "user defined" aren't modified; every service that in the Service List occupies a position marked as "user defined", it is given the first free position in the Master User List:*
 - ▶ *range 75-99 or, if there is no more space in this zone, in Preferences Overflow zone, for the numbers below 99*
 - ▶ *In zone Main Overflow for all the numbers over 100*

Enclosed - Contents



1.Channels numbering

**2.API for T-Government and
Smart Card no CA**

Complete set API necessary to satisfy T-Gov requirements

	essential	optional
SATSA	<ul style="list-style-type: none">• SATSA Generic Connection Framework• SATSA-APDU Optional Package	<ul style="list-style-type: none">• SATSA-JCRMI• SATSA-PKI• SATSA-CRYPTO
PBP 1.1 + Optional Packages	<ul style="list-style-type: none">• PB 1.1• J2ME Security (JCE) Optional Package• J2ME Security (JSSE) Optional Package	
Client Authentication for TLS Session	<ul style="list-style-type: none">• Client authentication for TLS Session	
Algorithms	<ul style="list-style-type: none">• AES	
Cipher Suites	<ul style="list-style-type: none">• TLS_RSA_WITH_AES_128_CBC_SHA• TLS_RSA_WITH_AES_256_CBC_SHA	
DVB Extensions to Java PBP J2ME	<ul style="list-style-type: none">• Org.dvb.security• Org.dvb. Security.pkcs11• Org.dvb.security.provider• Org.dvb.auth.callback• Org.dvb.net.ssl	

T-Gov requirements and relative API 1/2

Requirements

- Access to information inside the Smart Card
-
- Access to sensitive information on the Smart Card through a cryptographic system

API

- SATSA Generic Connection Framework
 - SATSA-APDU Optional Package
 - SC Access Permission Request
-
- SATSA Generic Connection Framework
 - SATSA-APDU Optional Package
 - SC Access Permission Request
 - Org.dvb.auth.callback
 - Org.dvb.security (with all SPI classes)
 - Org.dvb.Security.pkcs11
 - Org.dvb.security.provider
 - *Except for methods:*
 - ▶ *getPersistentProviders()*
 - ▶ *RegisterProvider()*
 - ▶ *UnRegisterProvider()*

T-Gov requirements and relative API 2/2

Requirements

- Authenticate the citizen (through the STB) when he connects via return channel to a Back End infrastructure using the Smart Card as access key

-
- Store on the Smart Card services / functionalities in order to save on air bandwidth

API

- SATSA Generic Connection Framework
 - SATSA-APDU Optional Package
 - SC Access Permission Request
 - Org.dvb.auth.callback
 - Org.dvb.security (with all SPI classes)
 - Org.dvb.Security.pkcs11
 - Org.dvb.security.provider
 - *Except for methods:*
 - ▶ *getPersistentProviders()*
 - ▶ *RegisterProvider()*
 - ▶ *UnRegisterProvider()*
 - Org.dvb.net.SSL
 - J2ME Security (JCE) Optional Package
 - J2ME Security (JSSE) Optional Package
 - TLS Client Authentication
 - TLS_RSA_WITH_AES_128_CBC_SHA
 - TLS_RSA_WITH_AES_256_CBC_SHA
-
- SC Provider Permission Request
 - Org.dvb.security.provider (all methods)