



Curso Multimedia Home Platform 1.1.2

MHP NON-CA SMARTCARD. SATSA

Recomendación en España

Problemática de Versiones (1.1.2 & 1.1.3)

API org.dvb.smartcard. Establecimiento de Conexión

Curso Multimedia Home Platform 1.1.2

Copyright 2008 © Enrique Pérez Gil

Licensed under the ***Creative Commons Attribution-Non-Commercial-No Derivative Works 3.0 Unported License***. You may not use this file except in compliance with the License. You may obtain a copy of the License at:

<http://creativecommons.org/licenses/by-nc-nd/3.0/legalcode>

This is a human-readable summary of the License applied:

(<http://creativecommons.org/licenses/by-nc-nd/3.0/>)

You are free to Share, to copy, distribute and transmit the work **Under the following conditions:**

- **Attribution.** You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).
- **Noncommercial.** You may not use this work for commercial purposes.
- **No Derivative Works.** You may not alter, transform, or build upon this work.

For any reuse or distribution, you must make clear to others the license terms of this work. Any of the above conditions can be waived if you get permission from the copyright holder. Nothing in this license impairs or restricts the author's moral rights.

Recomendación Española

- Hoy en día la versión MHP 1.1.3 incluye un nuevo API para acceder a smartcards que además es el recomendado por la norma española: *Guía de Implementación de la TDT en España Versión 1.0.6* (

Punto 2.7 refs/GT7_SG2_Implementacion_TDT_España.pdf

- http://www.televisiandigital.es/NR/rdonlyres/E2CD7E0A-C971-4F5F-A6FE-31DADF9FC560/0/GT7_SG2_Implementacion_TDT_Espa%C3%B1a.pdf
- Veamos el detalle de los dos puntos del documento en los que se indican las recomendaciones

Recomendación Española

- *2.7 Guía de Implementación de la TDT en España Versión 1.0.6*

2.7 API de tarjetas inteligentes

En el supuesto de que sea necesario el uso de API de tarjetas inteligentes, éste deberá seguir las siguientes recomendaciones:

- * MHP 1.1.3 define el entorno para las operaciones con tarjetas inteligentes sin relación con el acceso condicional (acceso a los datos de la tarjeta inteligente, *TLS client authentication* con una tarjeta inteligente para servicios de *T-gov*, *TBank*, etc.). Non-CA smart card API (SATSA-APDU) no se prevé que vaya a sufrir modificaciones, por lo que se recomienda usar sólo esta API en los primeros servicios que utilicen tarjetas inteligentes.
- * Si un receptor dispone de lector de tarjetas inteligentes (es decir, la propiedad de sistema `mhp.smartcard.reader` devuelve "SUPPORTED"), debe cumplir con los mecanismos y APIs definidos en MHP 1.1.3 al respecto. Entre otros:
 - 11.8.2 APIs for return channel security
 - 11.8.5 Cryptographic API
 - 11.8.6 DVB Extensions for Cryptography
 - 11.9.4 Non-CA smart card API
 - **Annex AM: Smart card reader API**

Recomendación Española

- 2.8 Guía de Implementación de la TDT en España Versión 1.0.6

2.8 Providers

Para simplificar y favorecer el uso de tarjetas inteligentes criptográficas (como el DNI Electrónico español) MHP 1.1.3 estandariza la señalización, instalación y el ciclo de vida de los Providers.

Los receptores que soporten aplicaciones con uso de tarjetas inteligentes criptográficas deben seguir las siguientes especificaciones de MHP 1.1.3:

- 9.11 Providers
- 10.15 Signalling for providers
- Annex AJ: Cryptographic service provider installation
- Annex AN: Provider APIs

No es obligatorio pero si altamente recomendable incluir el soporte para Stored Services que permita el almacenamiento de un único Provider que pueda ser utilizado por las distintas aplicaciones emitidas.

Problemática de Versiones

- Curiosamente la normativa española se queda en mhp 1.0.x pero en relación a Smartcard aplicamos la especificada en la última versión del profile 1.1.x.
- En los meses de Abril/mayo de 2008 mhp publicó la última revisión de mhp 1.1.2 la cual incluye el documento de erratas sobre la 1.1.2 y alguna modificación como la referida a los requerimientos respecto a SMARTCARD.

Ved <http://www.mhp.org/mhpgem11.htm>

Problemática de Versiones

- Veamos el contenido de las especificaciones respecto a SMARTCARD en las distintas versiones MHP

- **MHP 1.1.2 A0068r1**

11.9.4 Non-CA smart card API

The non-conditional access API for smart cards is the "SATSA-APDU" optional package defined by SATSA [106] and the class `javax.microedition.apdu.APDUPermission` defined in clause B.1.2.1 of that document.

The present document does not require support for U(SAT).

- **MHP 1.1.3 A0068r3 / MHP 1.1.2 ETSI TS 102 812 V1.3.1**

- Las diferencias entre la última versión de 1.1.2 y 1.1.3 son mínimas, pero importantes respecto a 1.1.2 A068r1.



Problemática de Versiones

- MHP 1.1.3 A0068r3 / MHP 1.1.2 ETSI TS 102 812 V1.3.1

11.9.4 Non-CA smart card API

The API for access to non-conditional smart cards shall be comprised of the following:

- the "SATSA-APDU" optional package defined by SATSA [106]
- the class `javax.microedition.apdu.APDUPermission` defined in clause B.1.2.1 of that document.
- **the `org.dvb.smartcard` package defined in Annex AM "(normative): Smart card reader API" on page 1151.**

NOTE 1: For MHP terminals without a non-CA smart card reader, the failure mode is defined by SATSA [106]. The present document does not require support for U(SAT).

NOTE 2: SATSA's Generic Connection Framework calls for opening a Connection to a Java Application, identified by an ID (the AID). At the time of this writing, many of the smart cards of interest are standards based but are not Java cards. Although an Application ID could be set on these cards, it is not mandatory and rarely available.

NOTE 3: Any method call of the form `Connector.open("apdu...;target=a0.00...")` issued against such cards returns a `ConnectionNotFoundException`. This is because the card has neither an AID set nor is a Java Card with such application listening.

NOTE 4: Any method call of the form `Connector.open("apdu...;target=SAT")` may also fail as this is normally used on (U)SIM as defined per SIM Application Toolkit mode.

In order to open the `APDUConnection` with this kind of smartcards, the method `openDefaultConnection()` in `org.dvb.smartcard.SmartCardReader` must be used.

In these `APDUConnection` instances, the Application Selection (SELECT FILE by DF NAME) and MANAGE CHANNEL commands are allowed.

NOTE 5: To open the `APDUConnection` when the smart card contains AID or it is a (U)SIM, the GCF method can still be used. In this case, Application Selection (SELECT FILE by DF NAME) and MANAGE CHANNEL commands are not allowed.

Problemática de Versiones

- Con respecto a lo indicado en el punto 2.7 referido
 - La última revisión de MHP 1.1.2 satisface la recomendación española.
 - **El paquete org.dvb.smartcard está incluido en los últimos stubs publicados por MHP.**
 - Además dicho paquete es soportado por el STB Strong 5510.

Problemática de Versiones

- En el punto 2.8 de la *Guía de Implementación de la TDT en España Versión 1.0.6* se indica lo siguiente:

2.8 Providers

Para simplificar y favorecer el uso de tarjetas inteligentes criptográficas (como el DNI Electrónico español) MHP 1.1.3 estandariza la señalización, instalación y el ciclo de vida de los Providers.

Los receptores que soporten aplicaciones con uso de tarjetas inteligentes criptográficas deben seguir las siguientes especificaciones de MHP 1.1.3:

- 9.11 Providers
- 10.15 Signalling for providers
- Annex AJ: Cryptographic service provider installation
- Annex AN: Provider APIs

No es obligatorio pero si altamente recomendable incluir el soporte para Stored Services que permita el almacenamiento de un único Provider que pueda ser utilizado por las distintas aplicaciones emitidas.

Problemática de Versiones

- Con respecto a lo indicado en el punto 2.8 referido

Las diferencias entre la última versión MHP 1.1.2 y MHP 1.1.3 consisten en:

Annex AJ

En MHP 1.1.3 desaparece la clase ProviderPermission del paquete org.dvb.security.provider

Annex AN

Nuevo paquete org.dvb.spi.selection (7 clases)

Nuevo paquete org.dvb.spi.util (1 clase)

Paquete org.dvb.spi: Actualización en 4 de las 6 clases. Todas salvo:

XletBoundProvider

SystemBoundProvider

- En cuanto a estos paquetes por tanto, la norma MHP 1.1.2 no cumple la recomendación española

API org.dvb.smartcard

- Vamos a ver en las siguientes Slides el API incluido en el paquete org.dvb.smartcard. No vamos a entrar en los protocolos posteriores de comunicación.

SmartCardReaderManager API

- Factoría que ofrece los objetos SmartCardReader.
 - public static SmartCardReaderManager **getInstance()**
 - Nos devuelve la Factory mediante un Singleton (as usual)
 - public int **getNumber()**
 - Nos dice el número de Smartcard readers disponibles
 - public SmartCardReader[] **getSmartCardReaders()**
 - Nos devuelve el número de SmartcardReaders disponibles. Array de 0 si no hay.

API org.dvb.smartcard

SmartCardReader API. El Dispositivo

- public int **getSlotId()**
 - Devuelve el ID con el que se identifica el Slot del SmartCardReader
- public int **getStatus()**
 - Nos devuelve el Estado en que se encuentra. Los valores están definidos en SmartCardReaderEvent. Lo vemos a continuación.
- public boolean **isSmartCardInserted()**
 - ¿ está tu smartcard insertada ?
- public void **addSmartCardReaderListener**(SmartCardReaderListener listener)
 - Queremos se notificados de cambios en la situación del Smartcard. Mediante SmartCardReaderListener
- public void **removeSmartCardReaderListener**(SmartCardReaderListener listener)
 - De-suscripción.
- public APDUConnection **openDefaultConnection()**
 - Abre la Conexión

API org.dvb.smartcard

SmartCardReaderListener API. Nos permite conocer la situación de la Conexión con la tarjeta

```
public interface SmartCardReaderListener {  
    public void smartCardReaderEventReceived(SmartCardReaderEvent event);  
}
```

```
public class SmartCardReaderEvent extends EventObject {  
    public static int SMART_CARD_IN = 0;  
        SmartCard OK. se ha obtenido un ATR correctamente. (APDUConnection)  
  
    public static int SMART_CARD_OUT = 1;  
        no hay tarjeta insertada  
  
    public static int SMART_CARD_MUTED = 2;  
        La tarjeta no devuelve un ATR. No hay comunicación eléctrica con la tarjeta.  
  
    public static int SMART_CARD_ERROR = 3;  
        Hay Tarjeta, hay comunicación eléctrica pero no devuelve un ATR.  
  
    public int getType()  
        El tipo de Evento  
}
```

API `javax.microedition.apdu`. `APDUConnection`

- El objeto que vamos a usar para comunicarnos con la tarjeta. No vamos a entrar en el protocolo APDU.

```
public interface APDUConnection extends javax.microedition.io.Connection {
```

```
    public byte[] exchangeAPDU(byte[] commandAPDU) throws java.io.IOException;
```

- Permite el intercambio de comandos APDU

```
    public byte[] getATR();
```

- Devuelve la respuesta de la tarjeta a una operación de Reset de la tarjeta(ATR)

Operaciones relacionadas con la gestión del PIN. Ved el API

```
    public byte[] enterPin(int pinID) throws java.io.IOException;  
    public byte[] changePin(int pinID) throws java.io.IOException;  
    public byte[] disablePin(int pinID) throws java.io.IOException;  
    public byte[] enablePin(int pinID) throws java.io.IOException;  
    public byte[] unblockPin(int blockedPinID, int unblockingPinID);
```

```
}
```

Establecimiento de conexión APDU

- Vemos a continuación los dos métodos utilizados en sendas versiones de MHP para abrir una conexión

```
try {
```

```
    // PARA MHP 1.1.2
```

```
    ac = org.dvb.smartcard.SmartCardReaderManager.getInstance().getSmartCardReaders()[0].openDefaultConnection();
```

```
    // PARA MHP 1.1.3
```

```
    ac = org.dvb.smartcard.SmartCardReaderManager.getInstance().getSmartCardReaders()[0].openRawConnection();
```

```
} catch (RuntimeException e) {
```

```
    e.printStackTrace();
```

```
}
```

Ejercicios Bloque SATSA-1

ISO/IEC 13818-1	Part 1. Elementary Streams transport definition
ISO/IEC 13818-6	Part 6. Extensions for DSM-CC. Digital Storage Media Command and Control
ETSI EN 300 468	Digital Video Broadcasting (DVB);Specification for Service Information (SI) in DVB systems
ETSI EN 301 192	DVB specification for data broadcasting
ETSI TR 101 202	Implementation Guidelines for Data broadcasting
ETSI TR 101 162	Digital broadcasting systems for television, sound and data services; Allocation of Service Information (SI) codes for Digital Video Broadcasting (DVB) systems
ETSI TR 102 154	Implementation guidelines for the use of MPEG-2 Systems, Video and Audio in Contribution and Primary Dist
ETSI TR 101 211	Guidelines on implementation and usage of Service Information (SI)
ETSI TR 101 200	Digital Video Broadcasting (DVB); A guideline for the use of DVB specifications and standards
DAVIC	Digital Audio Visual Council. davic 1.4.1
HAVI	Specification of the Home Audio/Video Interoperability (HAVi) Architecture
Interactivetvweb	http://www.interactivetvweb.org/
Wikipedia DSMCC	http://en.wikipedia.org/wiki/DSM-CC
MHP 1.1.2	Multimedia Home Platform, A068r1 & tam668r23_11xdraft_20061115
MHP 1.1.3	Multimedia Home Platform, A068r3
CDC 1.1	Connected Device Configuration (CDC) 1.1 (JSR=218).
PBP 1.1	Personal Basis Profile 1.1 (JSR 217)
MHP.org	www.mhp.org
INTRO MHP 1.1.3	tam1032r1-mhp-iptv-presentation