

# DAVIC Information Day, January 12th, 1999

---

- ◆ **Security specifications**
  - ◆ **Published in DAVIC 1.2**
  - ◆ **Provided security tools for DAVIC 1.0**
  - ◆ **Extensions published in DAVIC 1.4 (for DAVIC 1.4°)**

Vincent Lenoir, CCETT

# Introduction to Security (1)

---

- ◆ **Definition of a single security system for DAVIC is a very difficult task**
- ◆ **Security requirements depend on :**
  - ↔ the application
  - ↔ the characteristics of the access network
  - ↔ the nature and value of content
  - ↔ the business model which governs the system

# Introduction to Security (2)

---

- ◆ Implementation of security hardware and software is subject to strict Governmental regulations
- ◆ Failure modes are different for security and other systems : there is no “secure” algorithm, we only know broken algorithm
- ◆ Decreasing cost of computational power makes any given algorithm more vulnerable to attack over time

# Consequences for the DAVIC security system

---

- ◆ Flexibility is needed in the choice of security mechanisms
- ◆ One tool - One solution is not applicable for security
- ◆ Multiple algorithms must be coexist for the same tool
- ◆ Negotiation mechanisms are needed
- ◆ Compromised algorithms need to be replaced

# DAVIC Security specifications

---

- ◆ **S1 flow : scrambling, key distribution**
- ◆ **S2 flow : authentication, key exchange, confidentiality, integrity, secure download, parental control**
- ◆ **S3 flow : confidentiality, integrity**
- ◆ **Two conditional access interfaces for the STU : CA0 & CA1**

# S1 security specifications

- ◆ **Scrambling**
  - ◆ Shall be done at MPEG 2 TS packet layer
  - ◆ Shall be applied only to packet payload
  - ◆ TS packets shall be scrambled independently of each other
- ◆ **Control Words synchronisation indicated in the TSC field (Even/Odd control word), DVB specifications**
- ◆ **Scrambling algorithm**
  - ◆ may be negotiated in the S2 flow for retrieval profile
  - ◆ may be indicated in a PMT Scrambling Descriptor for broadcast profile
- ◆ **Conditional access system is proprietary**

# S2/S3 security specifications (1)

- ◆ S2/S3 authentication
  - ◆ based on the 3 way authentication mechanism described in ITU-T X.509
  - ◆ certificates according to ITU-T X.509
  - ◆ provides one or two key pairs (that can be used for signature, key exchange, confidentiality at S2/S3 flow)
  - ◆ carried in DSM-CC U-U messages for S2 flow (not specified for S3 flow)
- ◆ S2/S3 confidentiality and integrity
  - ◆ done at IP level
  - ◆ based on Internet RFC 1825 (IPv6)

# S2/S3 security specifications (2)

- ◆ S2 signature done at application layer
- ◆ DSM-CC commands for S1 security management
  - ◆ used for retrieval profile
  - ◆ allows to distribute and renew Control Words in S2 flow
  - ◆ allows to negotiate the scrambling algorithm
  - ◆ Control words are used to scramble the S1 flow
- ◆ Secure downloading
  - ◆ completes DAVIC downloading specifications
  - ◆ provides the integrity, the source and the freshness of the downloaded data and software

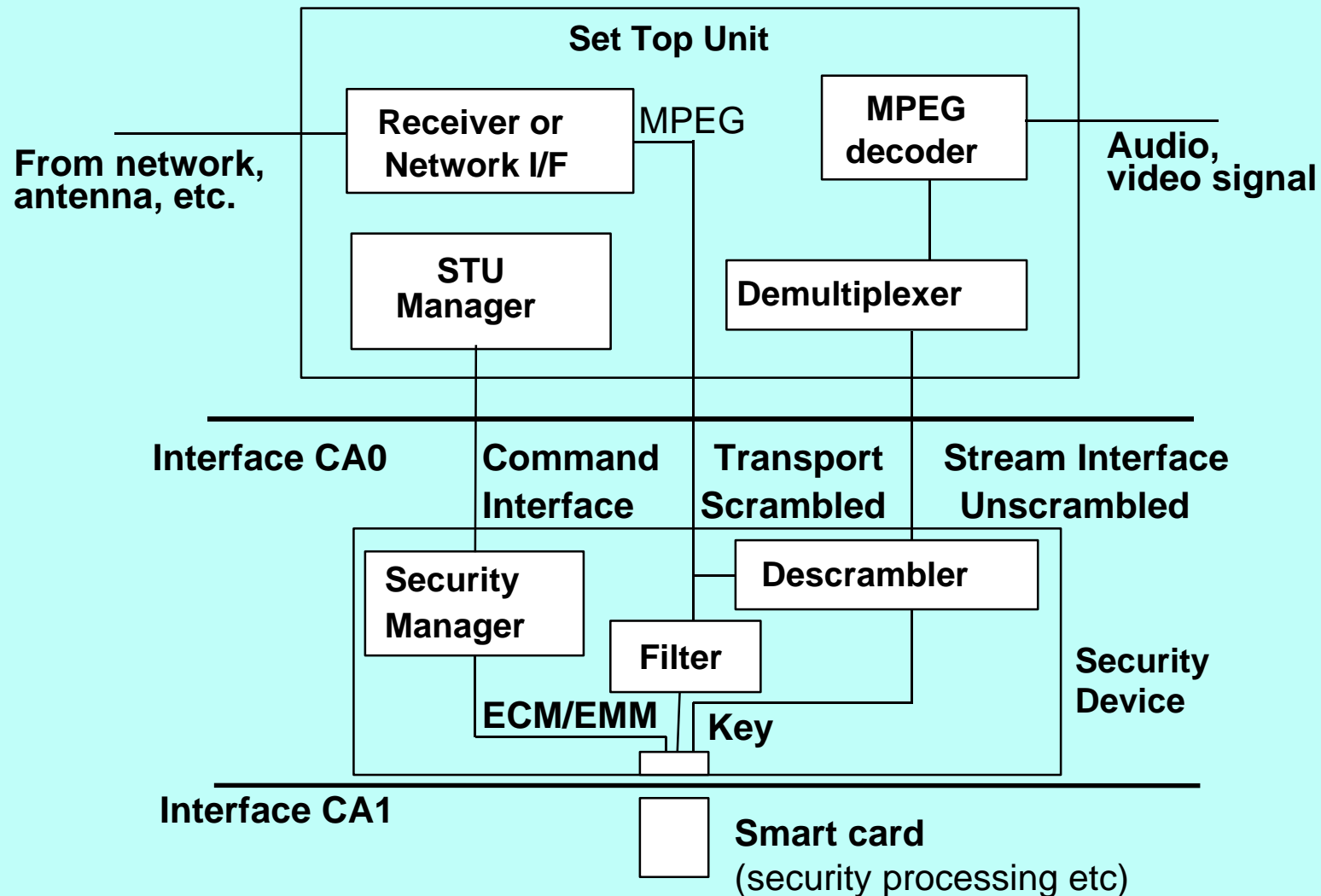
# Parental control

---

---

- ◆ Specified for broadcast profile
  - ◆ not used for retrieval profile
  - ◆ content rating according to DVB-SI in the S1 flow

# Security interfaces in the STU



# CA0 Interface

- ◆ **PC Card based**
- ◆ **All security elements in the detachable module**
  - ◆ MPEG2 stream descrambling
  - ◆ conditional access
  - ◆ S2/S3 security
- ◆ **Based on DVB Common interface (EN 50221)**
- ◆ **Additional functions and resources specified for DAVIC**
  - ◆ TCP/IP communications
  - ◆ HTML MMI display
  - ◆ Authentication
  - ◆ IP security

# CA1 interface

- ◆ **Smart card based**
- ◆ **MPEG2 stream descrambling, CA message filtering and system control on the STU**
- ◆ **All other security functions on the detachable module**
- ◆ **CA1 specification**
  - ◆ ISO 7816 Part 1 to 6 based and prEN726-3
  - ◆ Basic specifications for subscription
  - ◆ Completely new application protocol (compatible with no existing smart card)
- ◆ **CA message format according to DVB (ETR 289)**
- ◆ **Filtering of CA messages specified**

# DAVIC 1.4 CA1 extensions

---

- ◆ **Protection of Control Words on CA1 interface**
- ◆ **Authentication of CA1 by STU**
- ◆ **Impulse pay-per-view support**
- ◆ **Transparent mode support in S2 flow : allows to use existing smart with DAVIC**

# **JAVA Security API (DAVIC 1.4)**

---

- ◆ **Access to CA0 module**
- ◆ **Access to CA1 module**
- ◆ **Message passing for CA dependant application**
- ◆ **Ability for applications to implement MMI dialogue with CA0/CA1**
- ◆ **Explicit descrambling for data services**