3GPP TSG SA WG3 Security — S3#28 **S3-030257**
06 - 09 May 2003
Berlin, Germany

Source: **Gemplus, Oberthur**

Title: **PayTV model**

Document for: **Discussion and approval**

Agenda Item:

Abstract

This input paper aims at proposing PayTV model as solution for MBMS data protection.

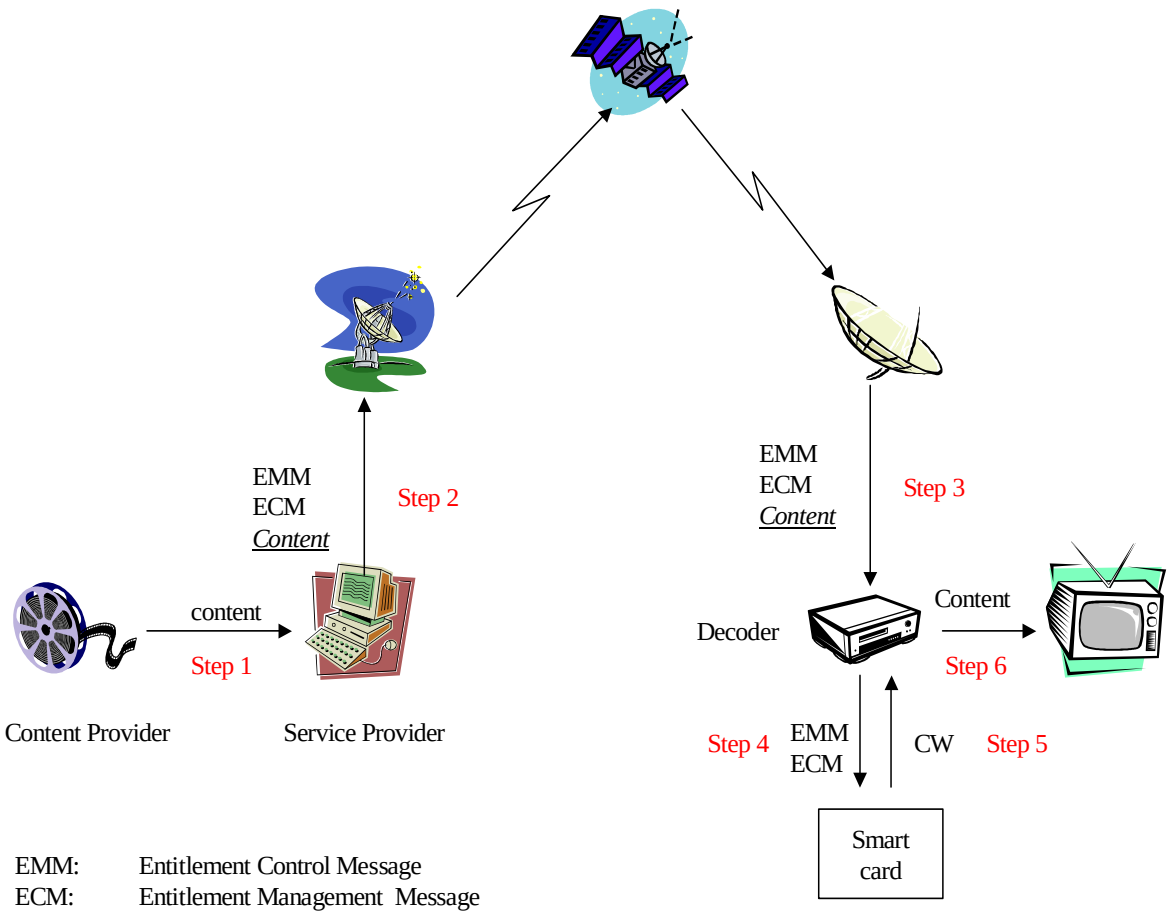
1. Introduction

3GPP is currently working on MBMS and there are some proposals for MBMS data protection. At Sophia-Antipolis SA3#27 meeting, Gemplus and Oberthur briefly presented an overview of a model PayTV-based that could be adapted for MBMS traffic. This input paper provides a more detailed presentation of this model and will propose it as solution for MBMS data protection.

2. PayTV model description

The PayTV model is a full broadcast model where the data only flow from the Service Provider to the users. All users receive all data transmitted, but according to his associated access conditions, a particular user is allowed or not to have access to the content. This is performed by means of a conditional access system residing in a smart card inserted in the decoder. Actual descrambling of the content (i.e. deciphering of the video stream) is done in the decoder.

2.1. Overview



2.2. Actors

- Content Provider

Owns the content to be broadcasted

- Service Provider

Owns:

- Broadcast key **BK**
- Database containing the list of subscribers with following information:
  - Subscriber ID
  - List of rights

- Decoder

- Smart Card

Owns

- Database containing the list of user subscriptions with following information:
  - Service Provider Broadcast Key: BK
  - List of rights

2.3. Elements of PayTV

- **ECM** (Entitlement Control Message)

Consists of**:**

- Control Word **CW** (which is the content encryption key)
- Content_Id
- Description of the rights required to access content

ECM is ciphered using the Broadcast Key

- **EMM** (Entitlement Management Message)

Consists of:

- Subscriber_Id
- Rights update

- ***Content*** (in steps 2 and 3)

Consists of:

- ECM_id
- Content_id
- Content (sent Step 1) ciphered using Control Word **CW**

2.4. Actions performed by the actors

Control Messaging

- Service Provider actions:
  - On sending content, the Service Provider defines the types of rights needed to access the content.
  - He prepares the ECM (ciphered with the BK) according to the profile and generates a control word CW (i.e. the content encryption key).
  - He sends the ECM and starts streaming the content ciphered with CW (Steps 2 and 3).

Decoder / smart card actions:

- On reception of an ECM (Step 4), the smart card deciphers the ECM (using the Broadcast Key) and checks the required rights relatively to the list of rights stored in the card.
- If the rights are OK, the card returns the CW to the decoder (Step 5) who uses it to decipher the received content.

Management Messaging

- When subscriber rights have to be updated EMM is sent to the user smart card. It is ciphered with the Broadcast Key BK and contains the updating information (new rights, loss of rights, increase purse…) and the Subscriber_Id.
- The Subscriber_Id is ciphered with an encryption key that might be different from the BK and user related. Moreover, the Subscriber_Id may be repeated in the clear to allow the decoder to filter EMMs destined to the smart card currently inserted (see DVB standards for data format).

2.5. Developpements

ECM in its simplest expression is just an ID and a date. This allows the card to check if the basic right “view until date” is OK.
This can be upgraded by profiling the content by category and level. Category can be a type of subscription, appartenance to apackage, typology of the content… Level can reffer to a notion of price or age or security clearance. The card is then in charge of matching the profile of the content with the rights stored in the card and make a decision on wether or not to allow the decryption of the content. DVB standardises the format of the messages between card and decoder.

EMMs are completely independent of the ECM system. They can be handled using a global key for the system, but this is very dangerous since this key allows the update of any card in the system. It is usually prefered to have one key associated to each card, and the EMMs are then secured using this particular key. In an online system, other methods are possible, like initiating a secure channel and transfering the EMMs via this channel.
Management keys of a higher level are usually also comprised in the system, allowing updates of the EMM keys, the ECM key, defining new categories, activting anti-piracy counter-measures…

Groups of users may be handled simply by defining a key hierarchy for EMM keys or simply adding group keys to the already existing subscriber’s EMM key.

3. Advantages of PayTV model for MBMS data protection

- PayTV area has long history of tackling issues of security in broadcast systems.

- The key used to decrypt CW (the content encryption key) is stored in the UICC. This feature is really necessary since in MBMS a potential attacker is the subscriber/user.

- This PayTV model has the advantage of being independent of the bearer.

- The access conditions management is performed in the smart card, so it reduces the amount of work for the network (computations and traffic).

- This PayTV model addresses multicast and broadcast in the same way, since PayTV always links the content to the conditional access. Some content may be tagged free but is still handled with condition access.
  However, it is possible with PayTV model to optimise the network resources in case of MBMS multicast, since there is a joining phase (MBMS multicast activation) when the user indicates to the network he is willing to receive Multicast mode data of a specific service

- Group of subscribers may be easily handled with PayTV model.

- The secret and algorithm used for PayTV model could be different from the 3G AKA. An attack performed on MBMS content protection would not affect 3G AKA. In the worst case, a change of smart cards is still possible without compromising all the system.

- The Service Provider could have feedback on the use of MBMS data by the subscriber. This uplink could be established by means of SIMToolkit.

- ETSI Digital Video Broadcast group has initiated standard efforts to marry the cell phone network infrastructure with terrestrial digital TV broadcasting. The mobile device could be able to receive signals from cellular networks (GPRS/UMTS) as well as DVB-T and DVB-X broadcast transmissions.
  In this context, the use of PayTV model for MBMS data protection would allow to have a common way to deal with content protection.

4. Conclusion

The PayTV model is a solution that addresses MBMS issue by providing content protection and keying distribution. We propose to incorporate PayTV model to TS 33.246.