3GPP TSG SA WG3 Security – S3#29 **S3-030396**

15 - 18 July 2003

San Francisco, USA

Source: **Gemplus, Oberthur,**

Title: **Key distribution and billing in PayTV model**

Document for: **Discussion and decision**

Agenda Item: **T.B.D**

Abstract

This input paper aims at providing more information on the key distribution and the billing methods offered by PayTV model.

1. Introduction

At SA3#28 Berlin meeting, Gemplus and Oberthur presented the PayTV model as solution to address MBMS. This input paper provides more information on the key distribution and the billing offered by PayTV model.

2. Key distribution

The key distribution is based on ECM and EMM (Cf S3-030257 on PayTV model [1]).

- **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
- Keys update

The EMM is ciphered using a Management Key.

2.1. The Broadcast Key

The Broadcast Key is common to all subscribers of a given service of the Service Provider.

The Broadcast key is frequently changed by means of EMM (e.g. a Service Provider can send every month EMMs to update the Broadcast Key and the user's entitlements).

So, in case of a compromised Broadcast Key, EMM messages would be sent to all users to update the Broadcast Key.

2.2. The Management Key

EMMs are used to convey rights or keys to users, or to invalidate or delete rights or keys.

The EMM are encrypted with a Management Key belonging to the Service Provider. The EMM messages can only be read by the smart card, which stores the Management Key.

The Service Provider may associate one Management Key to a single user and/or a group of users. Groups of users may be easily handled by defining a key hierarchy for the Management Key.

It is also possible to have mechanisms on the smart card allowing the update/remove/add of a Service Provider's Management Key by means of a Master Key, which could belong to the Operator for example.

The key infrastructure may be very simple (one key for all subscribers) or very complex, with broadcast keys shared by all subscribers of a service offer and management keys either shared by all, by groups or individuals.

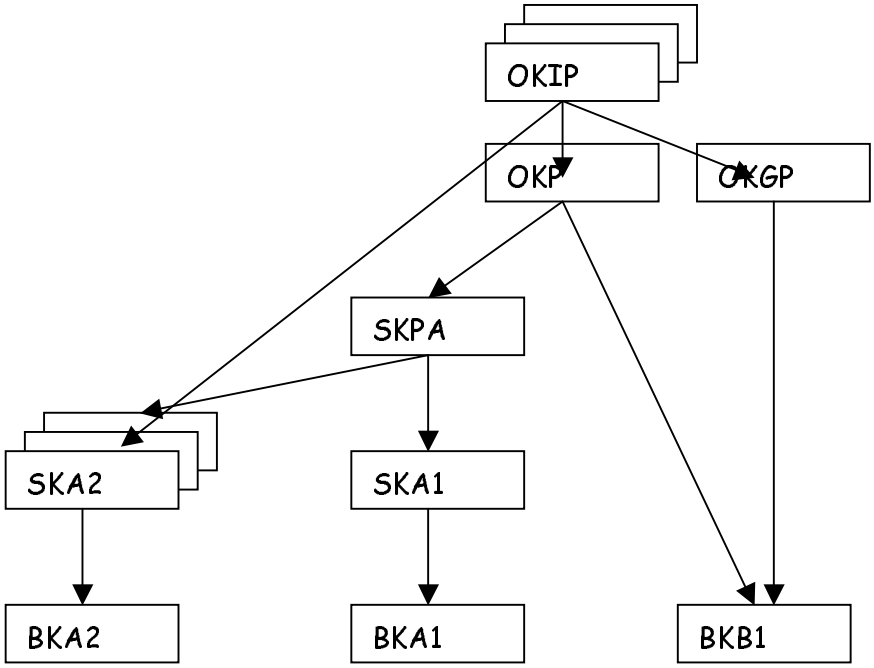
Example:
The following key infrastructure can be used with 3 services (A1, A2 and B1) offered by 2 service providers A and B on an operator OP:

Broadcast key for service A1: BKA1, same for all subscribers to the service
Broadcast key for service A2: BKA2, same for all subscribers to the service
Broadcast key for service B1: BKB1, same for all subscribers to the service

Service management key for service A1: SKA1, same for all subscribers to the service
Service management key for service A2: SKA2, different for each subscriber to the service
No service management key for service B1
Master service management key for service provider A: SKPA

Operator management key: OKP, same for all subscribers
Operator group management key: OKGP, same for a group of subscribers
Operator individual management key: OKIP, different for each subscriber

Following schematic shows which key may be used to upgrade/modify/invalidate which key and associated rights (represented by an arrow).



3. Security for payment

The smart card is also involved in the billing to prevent fraud. PayTV proposes different models for the billing, for example:

- The subscription: pre-payment for a given time period of viewing, a given programme or group of programmes.

- The Pay-Per-View: payment for a given programme or group of programmes. May be preordered (specific event, like a premium match) or chosen on impulse using a pre-paid or post-paid purse mechanism.

- The Pay-Per-Time: payment for a given programme depending on actual duration of usage.
  This model can be used for the benefit of the operator, independently of the service providers, to follow the consumption of bulk data (instead of time). Counters can be prepaid, with automatic reloading via connection to an accounting server, or postpaid with systematic interrogation of the cards.

The smart card is used to prevent a reset of the counting mechanism indicating the remaining credit.

Each Service Provider offers different kinds of billing methods. The billing methods are not standardized by DVB.

4. Standards

Digital PayTV systems are mostly based on the Digital Video Broadcasting (DVB) standard. The following chapters provide information on the scope of DVB standard.

4.1. PayTV and DVB.

DVB does not specify all the mechanisms involved in DVB-based services.

The Conditional Access in DVB [2]:
"The term "Conditional Access" is frequently used to describe systems that enable the control over the access to programmes, services etc.

- *Conditional Access (CA) systems consist of several blocks; among others, the mechanisms to scramble the programme or services*
- *The Subscriber Management System (SMS), in which all customer data are stored*
- *The Subscriber Authorization System (SAS), that encrypts and delivers those Codes Words which enable the descrambler to make the programme legible.*

It was one of the strategic decisions taken by the DVB Project that neither the SMS nor SAS should be standardized. The only part of a CA system which was developed jointly by members of DVB is the "Common Scrambling Algorithm"."

The structure/format of the EMM and ECM for transmission is standardized but not their content. The billing is also not specified by DVB.
This allows a Service Provider to choose the way to deal with the user's rights, the hierarchical key systems, the billing, etc.

ETSI DVB group has initiated standards effort to marry DVB broadcasting with the mobile cellular network.

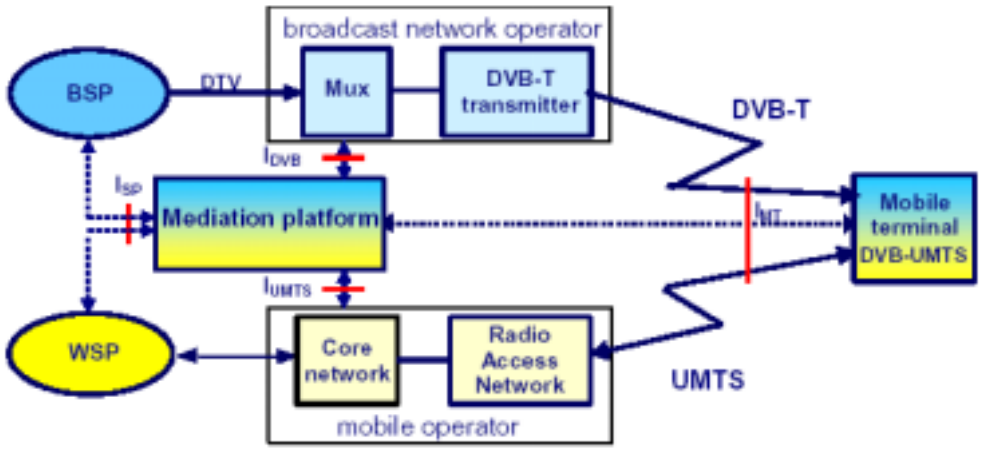
4.2. Convergence between ETSI DVB and 3GPP groups

PayTV model for MBMS would allow to have a common way to deal with content protection in DVB and 3GPP groups.

ETSI DVB-UMTS [3] and DVB-X [4] groups are working on methods to marry DVB broadcasting with the mobile cellular network.
DVB ad hoc group UMTS work is focused on the inter-working of DVB broadcast systems and services, with advanced generation (2.5G and 3G) mobile cellular networks. The group identifies co-operative services utilizing UMTS and DVB platforms to address consumer demands for more powerful interactive and personalized services.

An article [5] issued by the group in November 2002 presents their activity.
Extract from article [5]:

Generalised scenario for co-operative platforms:



A "Mediation Platform" function will exist between the two paths to allow sharing and re-directing of data. Content can be re-purposed and transferred between platforms (eg. DVB content delivered via UMTS), and opportunities for exciting new application exist."

This convergence between ETSI DVB and 3GPP groups was presented to SA1 in S1-030718 contribution [6].

5. Conclusion

The PayTV model offers simple mechanisms to manage the keys and to enforce the security policies. In particular, it allows easy update of the secret keys and addresses the problem of compromised keys.
Moreover, it allows the network operator to count the amount of data actually used independently of the accounting done for the service providers.
So, we propose to adopt the PayTV model as solution for MBMS.

6. References

[1] "PayTV model", Gemplus and Oberthur, 3GPP S3-030257, May 2003

[2] ETSI DVB, TR 101 200: "A Guideline for the Use of DVB Standards, ("Cookbook")"

[3] DVB ad hoc group UMTS,
Technical Module TM-UMTS: http://www.dvb.org/index.php?id=79
Commercial Module CM-UMTS: http://www.dvb.org/index.php?id=87

[4] DVB ad hoc group X,
Technical Module TM-X: http://www.dvb.org/index.php?id=72

[5] Professor David Crawford, Chairman, DVB ad hoc Group UMTS:
"'*UMTS' : DVB's Work on the Inter-working of Broadcast and Mobile Telecomms Networks*", Nov 2002.
http://www.dvb.org/documents/modules/TM-UMTS.DVB-Scene-0211.pdf

[6] "PayTV model", Gemplus and Oberthur, 3GPP S1-030718, July 2003