Multiple Conditional Access Systems

Michael Adams
Sr. Project Engineer, Advanced Engineering
Time Warner Cable

Tony Wasilewski
Chief Scientist, Software Systems
Scientific Atlanta

Abstract

There are a number of well-developed standards currently being used to deliver digital video over cable systems in the area of modulation, forward error correction, transport and compression. However, encryption and conditional access systems are typically, by their very nature, highly proprietary systems. This presents a road-block to the support of multi-vendor set-tops in cable systems. One possible solution is the adoption of a common, standard, service encryptor at the lowest level combined with multiple conditional access systems that provide key distribution and control functions.
This paper will describe the technical challenges in building multiple-conditional access systems and argue that, in practice, other standards are required to support cost effective deployment of multi-vendor set-tops.

Introduction

Conditional Access (CA) systems, by their very nature, tend to be proprietary. However, Cable Operators would like to have the choice of set-top terminals from many different suppliers. One approach would be to settle on a single system design and have all manufacturers license that one system. This would have negative implications for all parties concerned, however, because there is little incentive for feature innovations from the alternate suppliers, since they are locked into a sub-licensed design.

The digital age offers the promise of supporting a highly standard, multi-vendor environment. This includes the possibility of having more than one conditional access system at work within the same network simultaneously. Because the industry has focused on and agreed upon the use of standards such as MPEG-2 and DAVIC[1], it is now feasible to finalize agreements that permit complete interworking of products from different suppliers while still reaping the benefits of digital compression.

The MPEG-2 systems layer[2] provides various hooks to support the co-existence of multiple CA systems within the same digital channel. This allows decoders, using different CA systems, to gain access to the same services with no need to simulcast the MPEG-2 payload.

So that the MPEG-2 payload need only be sent once, it must be encrypted with a standard 'service' encryptor. The multiple CA systems then effectively provide different key and entitlement delivery systems. Because only the CA key and entitlement delivery information needs to be simulcast, this adds relatively little overhead. We will show that, in practice, this is less than 1% per CA system.

Definition Of Terms

The following terms will be used in this paper:

- **Conditional Access (CA)** System - the software and other components necessary to provide for selective access or denial of specific services in a network. The CA system is used to establish the means by which subscription or other payments may be collected from users of a network for use of a service. A conditional access system includes mechanisms for payload encryption, secure key delivery, addressed messaging, secure entitlement delivery and appropriate links to administrative gateways or billing systems.
- **Key Delivery** - the mechanism by which various keys are delivered to the set-top terminal in a secure manner (so that the service cannot be pirated).
- **Key Hierarchy** - a key hierarchy is usually defined in a broadcast security system. At the

lowest level is the Control Word which is the key used with the Service Encryptor.

- **Service Encryptor** - the encryption algorithm performed on the MPEG-2 payload bytes. Note that the MPEG-2 transport system and adaptation headers are always sent in the clear.
- **Control Word (CW)** - the key used with the service encryptor to provide confidentiality of the delivered services. It is changed at a rapid rate to increase the security of the content.

First we will describe an example of a single CA system before turning to multi-CA systems

An Example System

Traditionally, CA systems for broadband networks have been intended to protect primarily against signal theft for the benefit of the network operator. With the advent and migration to digital compression and two-way services, security issues have greatly expanded and so has the list of beneficiary parties. For example, content owners, service providers, billing providers, and end users now all have security concerns in addition to network operators. In addition to signal security, examples of these emerging concerns include:

- sensitive or private data accessed and transmitted in cable modem applications
- authenticating service providers in a multi-provider network
- multiple entitlement agents ("gatekeepers") in one decoder
- authenticating messages in forward and reverse directions
- protecting software and application downloading to Home Communication Terminals (HCT's), including virus protection
- two-way services
- shopping services and E-commerce, E-cash
- subscriber identification and digital signature
- subscriber privacy, for example, credit card numbers.

Scientific-Atlanta's PowerKEY System is the broadband industry's first CA system to support both public key and secret key cryptography. PowerKEY's use of public key (RSA) cryptography allows it to address the issues discussed above in a unique way that traditional secret key-only CA systems cannot match.

The requirements of a robust CA system are met by the following PowerKEY system components:

- Stream Encryption & ECM Streamer Module
- Control Suite
- Transaction Encryption Device (TED)
- Service Decryptor Module
- Security Manager
- Home Communication Terminal (HCT) Secure Element

Figure 1 depicts the configuration of these components within a typical system and the interfaces that must be established with other components and subsystems for delivering secure digital services. In this figure, the HCT receives signals from a Broadcast Center - the dotted lines indicate that the transmission could be either over-the-air or on a wired network. An "out-of-band" data path can be activated, which could be, for example, a QPSK or telephone transmission. This path can be used for impulse pay-per-view returns or with a suitable form of modulation, highly interactive services. The LAN Interconnect Device would typically be an IP router.

EMMs may be sent on this "out-of-band" path. In fact, since PowerKEY EMMs may be encapsulated within IP packets, they can be selectively routed to specific Broadcast Centers. This not only conserves EMM broadcast bandwidth, but considerably complicates the business of the "clone pirate", since there may be many broadcast centers. The "pirate" must maintain legitimate HCTs in each of these broadcast centers to enable clone reception.

PowerKEY System Interfaces for Digital Services

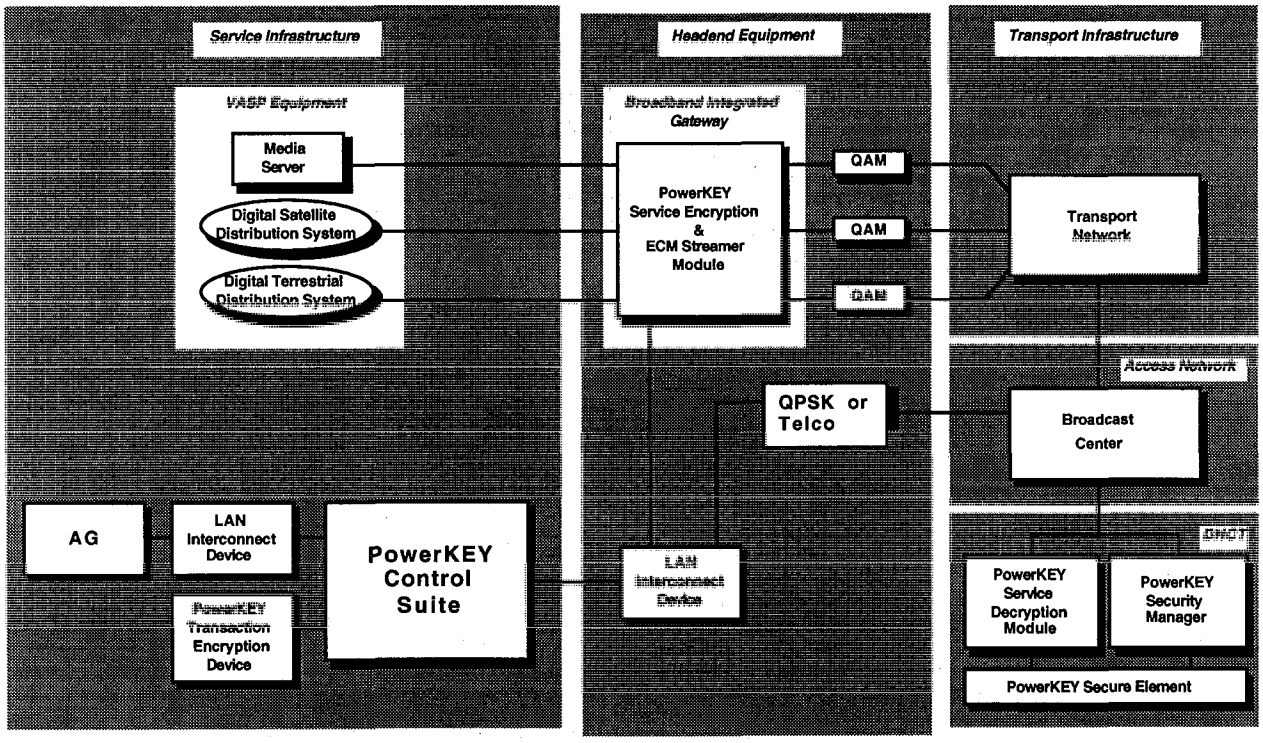

Figure 1. PowerKEY System Interfaces

The PowerKEY CA system employs a multi-level key hierarchy. Control words are fast-changing keys used to encrypt the services (video, audio, data). Mid-level keys called multi-session keys are used to protect the control words so that they can not be discovered in transmission, except by authorized units. The multi-session keys are sent to individual decoders using messages (EMMs) that are encrypted with the RSA public key algorithm. These EMMs are also digitally signed by an Entitlement Authority.

The CableLabs Agreement

In October 1996[3] some major elements of an interoperable digital cable systems specifications were agreed by CableLabs and its members:

- The agreement was based on existing standards (DES encryption, MPEG-2 systems layer).
- The agreement was deliberately defined to be the minimum intersection of multiple CA systems:
  1. The adoption of a standard service encryption algorithm based on DES standards[4,5].
  2. A common control word generation method.
  3. Use of existing features in the MPEG-2 systems layer to allow multiple CA systems to co-exist within a single digital channel.

This agreement represents the final and the most difficult step in long history of standardization. Because the CA system is typically the most feature-rich it significantly differentiates one vendor's product from another. By separating the CA system into two parts (the service encryptor and other components), each vendor is still able to innovate and add features to its CA system without introducing incompatibilities at the service encryptor level.

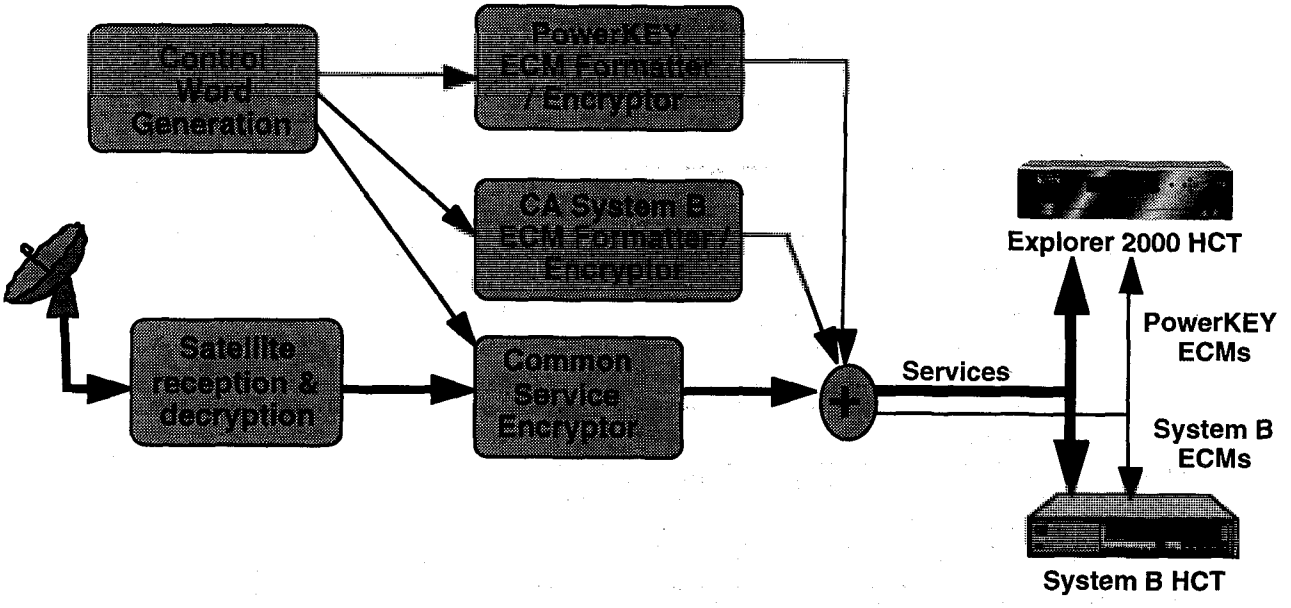

Figure 2. A Dual-CA System

Figure 2 illustrates an example multiple conditional access system. A common control word is used with a common service encryptor to encrypt the MPEG-2 payload. Each of the two conditional access systems independently deliver the control word to the two vendor's Home Communications Terminal (HCT). Each HCT receives and operates only on the ECM stream that it 'understands'.

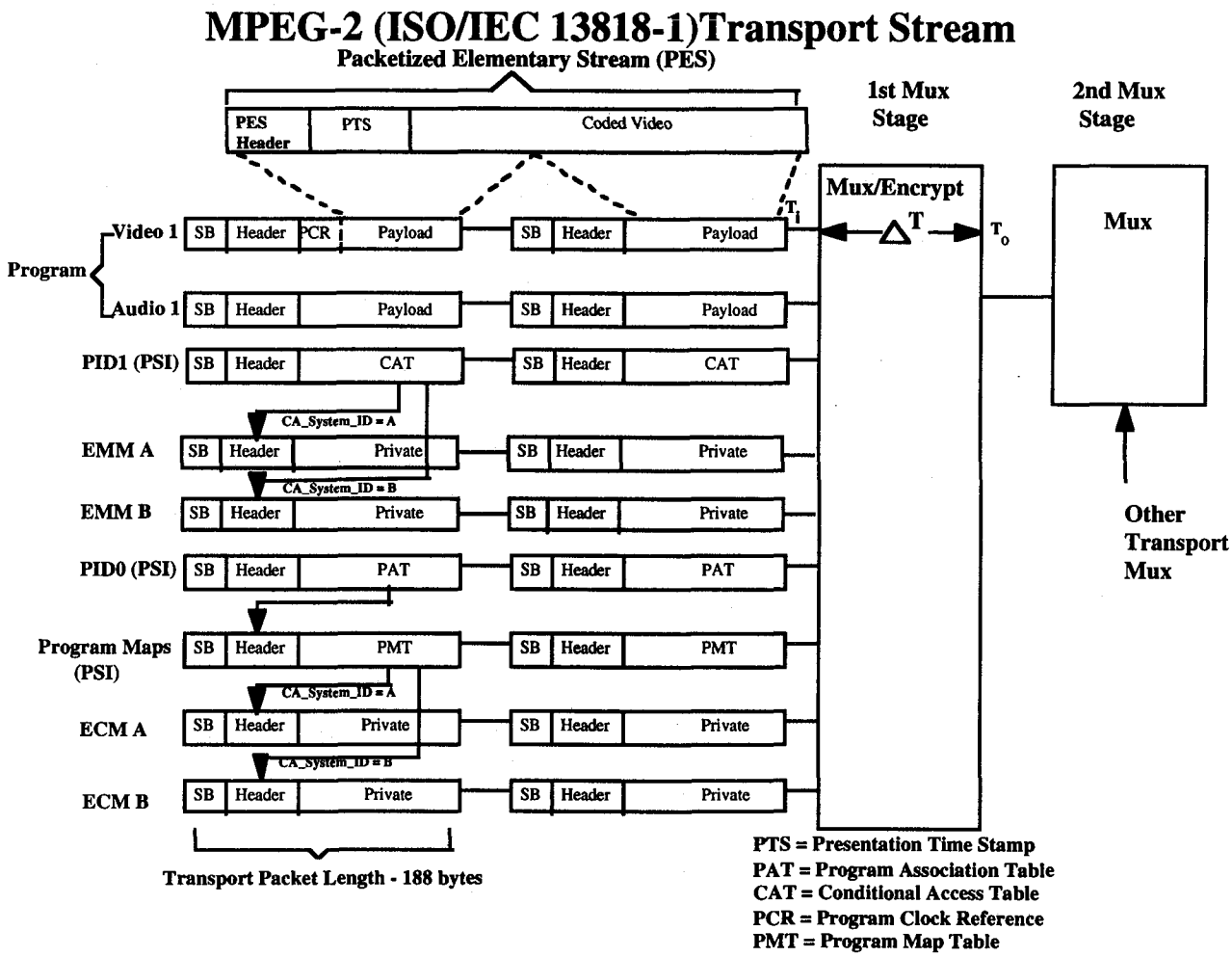

Figure 3. MPEG-2 Systems Layer

Figure 3 illustrates how the MPEG systems layer supports multiple conditional access systems.

- The Conditional Access Table (CAT) provides pointers to multiple Entitlement Management Message (EMM) streams.
- The Program Map Table (PMT) provides descriptors to multiple Entitlement Control Message (ECM) streams.

Increased Overhead of Dual-CA System

What is the overhead of operating a dual-CA system? If we assume 100 Kbps for the additional ECM stream this amounts to less than 0.4% of the digital channel. Taking an estimate of 100 Kbps for the additional EMMs < 0.4% this also amounts to less than 0.4% of the digital channel. (Note that in a cable system EMMs are typically delivered in an out-of-band, QPSK channel.) Therefore the total overhead is less than 0.8%.

In any case, it is the exception rather than the rule, that both CA systems would be active in a single system at the same time. The benefits of a multiple CA strategy of second sourcing, CA system evolution and CA replacement are more important than placing two set-tops, which require different CA systems, side-by-side in the a cable system.

Future Work

Much work still remains to be done to develop multiple conditional access systems:

1. CA system interworking - there are many problems to solve:

- Program schedules and program guide information need to be synchronized. Program guide information must be delivered in a form that all HCTs can access.
- Billing interfaces must become more standard so that the two conditional access systems can be supported by a single billing system.

2. Security Extensions - a standard API is needed to support secure applications, for example, secure WEB transactions, electronic commerce, games, etc.

Summary

The framework to implement multi-CA systems within was initially established by the MPEG-2 systems layer and has been further defined within the CableLabs agreement. However, there is still much work that remains to be done.

There is only a minimal and reasonable overhead to operate a dual-CA system. This represents less than 1% in a cable system.

The conditional access system significantly differentiates one vendor's product from another. By separating the CA system into two parts, each vendor is still able to innovate and add features to its CA system without introducing incompatibilities at the service encryptor level. Therefore, multiple conditional access allows interworking without reducing CA to the lowest-common denominator.

REFERENCES

[1] Digital Audio Visual Council (1996), DAVIC 1.1 Specification Part 8: Lower Layer Protocols and Physical Interfaces (draft as of September, 1996).
[2] ISO/IEC 13818-1 (1994), Information Technology — Generic Coding of Moving Pictures and Associated Audio: Systems.
[3] "Cable Industry Agrees on Key Elements of Digital Systems Specification", CableLabs Press Release, October 3, 1996.
[4] Data Encryption Standard (DES), NIST FIPS PUB 46-2, January 1988.
[5] DES Modes of Operation, NIST FIPS PUB 81, December 1980.