Die kommende Generation Conditional Access – Integration von Sicherheitsaspekten aus Rundfunk und Kommunikation

Dr. Dirk Jaeger, Institut für Nachrichtentechnik, EuroCableLabs, Braunschweig, Deutschland
Stuart Savage, EuroCableLabs, Brüssel, Belgien
Bart Brusse, ConTeSt consultancy, Gorssel, Niederlande
Christoph Schaaf, Kabel Deutschland GmbH, Unterföhring, Deutschland

Kurzfassung

Vor über 10 Jahren wurde digitales Kabelfernsehen in verschiedenen Ländern Europas eingeführt. Es wurde 1995 auf der IFA erstmals in Deutschland demonstriert. Die Systeme, die heute zur Übertragung von Rundfunksignalen eingesetzt werden, wurden zu Beginn der 90er Jahre in der Anfangsphase des DVB-Projekts entwickelt. Dies gilt gleichermaßen für die heute verwendete Sicherheits-, bzw. Conditional-Access-(CA-) Architektur. Mit Blick auf die technologische Weiterentwicklung, die Sicherheitssysteme in den letzten 12 Jahren erfahren haben, erscheint dieser Zeitraum wie eine Ewigkeit. Die Systemsicherheit der neuesten Versionen DVB-kompatibler CA-Systeme hat sich durch die Einführung von zusätzlichen Features und Leistungsmerkmalen im Vergleich zu den ursprünglichen Versionen substanziell verbessert. Allerdings wurden gleichzeitig die ursprünglich sehr wichtige Interoperabilität zwischen CA-Systemen verschiedener Hersteller und die Austauschbarkeit der Systeme stetig reduziert, was dazu führte, dass heute ein Wechsel des CA-Systems für einen Plattformbetreiber nur noch sehr eingeschränkt möglich, bzw. nur unter hohen Risiken und Kosten durchzuführen ist. Diese Situation ist für Kabelnetzbetreiber in Europa untragbar, weshalb sie Maßnahmen ergriffen haben, die Sicherheitsarchitektur des DVB-CA-Systems an die Anforderungen der Zukunft anzupassen. Neben den Problemen der fehlenden Interoperabilität bestand ein weiterer wesentlicher Grund für die Überarbeitung der gesamten Architektur in der Tatsache, dass sich insbesondere Kabelnetze seit einigen Jahren von unidirektionalen Rundfunkinfrastrukturen in bidirektionale Kommunikationsnetzwerke umwandeln. Parallel zu dieser technischen Konvergenz von Rundfunk- und Telekommunikationsnetzinfrastrukturen beginnt sich auf der Ebene der Dienste eine Integration zu entwickeln. Es erscheint konsequent, die in Kabelnetzen eingesetzten unterschiedlichen Sicherheitssysteme (wie CA, SSL/TLS oder BPI) ebenfalls zu integrieren.

1 Einleitung

Conditional-Access-(CA-)Systeme, die heute im digitalen Fernsehen angewendet werden, wurden in den frühen 90er Jahren des vorigen Jahrhunderts definiert und entwickelt. Ihre Architektur wurde für einen Einsatz in unidirektionalen Übertragungsnetzen konzipiert. Eine Anwendung in konvergenten Infrastrukturen und Kommunikationsnetzwerken stand damals nicht zur Disposition. Die technischen Möglichkeiten der CA-Systeme unterstützten daher die geschäftlichen Anforderungen für Vertikalmärkte mit programm-orientierten Dienstkonzepten. Sie wurden nicht entwickelt, um die Verteilung von individuell zu vermarktenden Inhalten und Diensten per integriertes bidirektionales Telekommunikationsnetz zu ermöglichen.

Während der letzten Jahre hat sich die Situation bezüglich der Vermarktung von traditionellen Fernsehinhalten dramatisch geändert. Neben den neuen Audio- und Video-Formaten gibt es heute eine Vielzahl von neuen technischen Übertragungs- und Vermarktungsmodellen. Inhalte werden nicht mehr per se von einem Programmanbieter vertrieben (z.B. Video on Demand); es entstehen vielmehr Märkte, bei denen die Dienste über private Verbindungen (z.B. Peer-to-Peer-Dienste) und in zunehmendem Maße über hochratige, bidirektionale Kommunikationssysteme (z.B. DOCSIS oder DSL) verteilt werden. Anbieter können ihre Dienste flexibel entweder traditionell per DVB-Transportströmen oder eingebettet in IP-Pakete transportieren lassen.

Diese technische Entwicklung ermöglichte die Einführung neuer Fernsehdienste, wodurch neue Geschäftsmodelle entstanden, die sich aus den traditionell horizontalen Geschäftsmodellen (z.B. der öffentlich-rechtlichen Rundfunkanstalten) und den vertikalen Geschäftsmodellen (z.B. der Pay-TV-Anbieter) verbinden. Zukünftig werden für die Konsumenten mehr und mehr Möglichkeiten entstehen, immer öfter zwischen traditionellem Fernsehen oder modernen Fernsehdiensten auszuwählen. Mit Hinblick auf diesen Wanderungsprozess erscheint es notwendig, die traditionelle CA-Architektur weiter zu entwickeln, damit sie den Sicherheitsanforderungen der Hersteller und der Plattformbetreiber in den kommenden Jahren

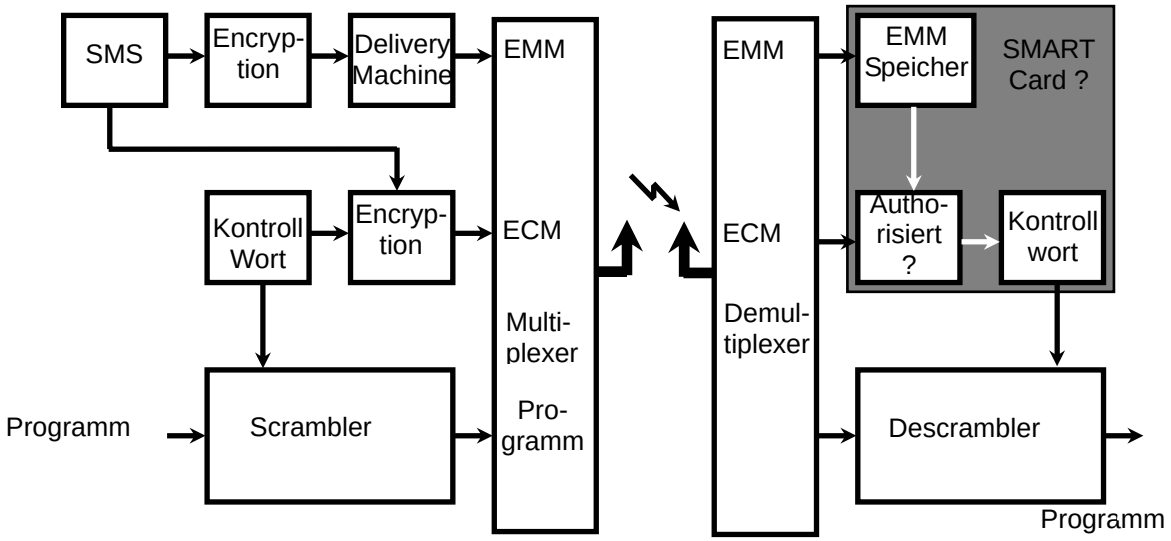

Bild 1: Blockschaltbild eines CA-Systems nach DVB (Quelle: [1])

erfüllen wird. Dabei stellt sich die Frage, ob letztendlich auch im Bereich der Sicherheitssysteme ein Konvergenzprozess zwischen den unterschiedlichen Sicherheitssystemen aus Rundfunk und Internet stattfinden wird oder ob es neue Konzepte geben wird, die den zukünftigen Marktanforderungen besser entsprechen werden.
Nach einem Überblick über die zur Übertragung von Fernsehsignalen verwendeten Sicherheitssysteme werden die Gründe und die laufenden Arbeiten für die Weiterentwicklung des CA-Systems erläutert

2 Überblick über Sicherheitsmechanismen

Obwohl heutzutage im Fall der digitalen Kabelnetze Europas der Prozess der Diensteintegration bereits begonnen hat und die Konvergenz der Übertragungssysteme stattfindet, gibt es noch keine integrierte Sicherheitslösung. Vielmehr werden individuelle Systeme zum Schutz der Dienste und privaten Daten eingesetzt, wie

- Conditional-Access-Systeme
- Internet-Sicherheitssysteme
- Datensicherheitssysteme

In den nächsten Absätzen werden kurz die wesentlichen Merkmale dieser Systeme vorgestellt.

2.1 Conditional-Access-Syssteme

Seit längerer Zeit werden in analogen sowie in digitalen Kabelnetzen CA-Systeme benutzt, um zu garantieren, dass nur die für einen speziellen Dienst registrierten und autorisierten Kunden diesen Dienst auch konsumieren können. Es findet durch das CA-System eine Freischaltung einzelner Kunden oder von Kundengruppen statt. Die CA-Systeme wurden im Wesentlichen für den Betrieb von unidirektional übertragenen Diensten entwickelt. Die heute üblicherweise verwendeten digitalen Systeme verwenden eine intelligente Komponente innerhalb des digitalen Empfängers, in der Regel ist dies eine Smartcard. Die SmartCard wird vom Plattformbetreiber so konfiguriert, dass sie den Freischaltungsprozess auszuführen kann. Die hierfür notwendigen Informationen werden per Transportstrom unidirektional, also wie ein gewöhnliches Rundfunksignal übertragen. Dieses Sicherheitskonzept baut auf 3 wichtige Elemente auf, die in jedem heute eingesetzten CA-System enthalten sind: (1) Verwürfelung der zu schützenden Daten, (2) Konfiguration einer Smartcard und (3) Kombination von Zugangsrechten eines Kunden mit dienstspezifischen Entschlüsselungsinformationen. In **Bild 1** wird das Blockschaltbild eines DVB-CA-Systems vorgestellt. Es zeigt die drei Elemente in Form der Datenverwürfelung durch den Scrambler, die Einheit zur Generation der EMMs für die Konfiguration der SmartCard und Erstellung von Zugangsrechten der Kunden (ECMs) durch den Kontrollwort-Generator mit nachfolgender Encryption. Die einzelnen Einheiten werden in den nachfolgenden Abschnitten näher erläutert.

2.1.1 Verwürfelung der Daten

In Europa wird für die Verwürfelung von digitalen Fernsehinhalten, entsprechend den Festlegungen der Universal Service Directive der Europäischen Kommission [2], in CA-Systemen allgemein der so genannte DVB Common Scrambling Algorithm (DVB-CSA) eingesetzt. Im Bild 1 befindet sich der CSA in dem Block mit der Bezeichnung Scrambler. Im Gegensatz zu den meisten anderen Verschlüsselungssystemen, bei denen häufig nur ein einziger Schlüssel permanent verwendet wird, wird der für ein empfängerseitiges Entwürfeln erforderliche Schlüssel beim

digitalen Fernsehen laufend geändert bzw. aktualisiert. Die ständige Veränderung des Schlüssels mit anschließender Verteilung ist aufwändig und kann, je nach Konfiguration des Systems, einen nennenswerten Teil der Kapazität des Übertragungskanals beanspruchen. Die hierfür erforderliche Datenrate liegt nicht selten bei einem Wert von 1 MBit/s pro Übertragungskanal oder sogar noch darüber. Aus diesen Gründen wurden Effizienzuntersuchungen gestartet, die sich mit der Frage auseinandersetzen, ob zukünftig bei einigen Diensten, z.B. beim Verteilen von geschützten Inhalten an kleinere Kundengruppen (wie bei Video-on-Demand), die relativ aufwändige Art der Verschlüsselung aus der Rundfunkwelt durch einen bidirektionalen Sicherheitsmechanismus ersetzt oder ergänzt werden sollte.

2.1.2 Konfiguration einer Smartcard

Für das Freischalten eines Dienstes wird in der Regel eine Smartcard eingesetzt. Diese wird vom Endnutzer in den Empfänger gesteckt und vom Kabelnetzbetreiber oder von einem anderen Dienstanbieter durch so genannte Entitlement Management Messages (EMMs) so konfiguriert, dass sie den Zugriff auf die vom Kunden abonnierten Inhalte und Dienste ermöglicht. Das Blockschaltbild des Algorithmus ist in Bild 1 zu sehen. Er besteht senderseitig aus den drei Einheiten SMS (Subscriber Management System, Encryption (Verschlüsselung) und Delivery Machine. Weil aber der CA-Mechanismus ursprünglich für Rundfunkdienste entwickelt wurde, müssen alle individuellen EMMs für alle Smartcards in regelmäßigen Abständen zum Kunden übertragen werden. In der Praxis geschieht dies etwa alle 15 bis 30 Minuten. Obwohl technisch nicht notwendig, werden die EMMs in der Praxis quasi in jeden Transportstrom eingespeist. Falls dies nicht geschehen würde, würde ein Kunde nach einem zwischenzeitlichen Umschalten auf einen Kanal ohne EMM-Informationen und Rücksprung auf Transportsrom mit verwürfeltem Dienst nicht sofort eine Zugriffsberechtigung haben, wenn er während des Updates der EMM auf einem anderen Kanal verweilte. Unter Umständen ist es sinnvoll, den durch eine Smartcard frei geschalteten Empfänger nicht komplett auszuschalten, so dass dieser auch im inaktiven Zustand weiterhin EMMs empfangen kann. Entsprechende Anforderungen lassen sich allerdings nur schwer mit den Zielen vereinbaren, die sich die Europäische Kommission gesetzt hat, um die Energieverbrauch von digitalen Fernsehempfängern zu verringern. [3].

2.1.3 Kombinieren von Zugangrechten und Enschlüsselungsinformationen

Der letzte Schritt in einem CA-Prozess beruht darauf, dass neben den verschlüsselten Inhalten und den entsprechenden EMMs auch spezifische Entitlement Control Messages (ECMs) generiert und zu den Kunden übertragen werden. Wurde eine Smartcard, wie im letzten Unterabschnitt erläutert, durch die EMMs autorisiert, so erfolgt per ECM die empfängerseitige Generierung des Kontrollwortes zur Entschlüsselung der Daten im Descrambler (vergleiche Bild 1).

2.2 Sicherheitssysteme für das Internet

Im Internet werden Protokolle wie SSL (Secure Sockets Layer) und dessen Nachfolger TLS (Transport Layer Security) angewendet, um Daten und Inhalte vor unautorisiertem Zugriff zu schützen. Die Protokolle erfüllen also ähnliche Funktionen wie das CA-System bei Rundfunkanwendungen. Durch die verschlüsselte Übertragung von Signalisierungsinformationen sollen sie darüber hinaus eine vertrauenswürdige Kommunikation ermöglichen. So bieten SSL und TLS dem Endnutzer eine gewisse Sicherheit bezüglich der Authentizität des Servers bzw. des Anbieters der Inhalte sowie bezüglich der Integrität und der Geheimhaltung der übertragenen Daten.
In modernen Kommunikationssystemen wird TLS häufig in Kombination mit einer Public Key Infrastructure (PKI) angewendet, die für die sichere Verteilung der für die Verschlüsselung und Entschlüsselung der Daten notwendigen Informationen sorgt. So kann zwischen dem Anbieter und dem Endnutzer ein zweiseitig gesicherter Kommunikationsprozess etabliert werden.
Der wesentliche Unterschied zwischen TLS/PKI-basierten Sicherheitssystemen und CA in Rundfunksystemen bleibt, dass - neben einer Reihe von technischen Differenzen - im ersten Fall der Anbieter der Inhalte den Kunden nicht unbedingt kennt, während er im zweiten Fall den Endkunden (durch die Anwendung einer Smartcard) identifizieren kann.

2.3 Baseline Privacy Interface (BPI)

In den Kabelkommunikationssystemen (DOCSIS/-EuroDOCSIS) wird noch ein zusätzliches Sicherheitssystem angewendet, um die Daten auch auf der Medium Access Control (MAC)-Ebene zu schützen. Diese Maßnahme ist dem Charakter der Kabelnetze als ‚shared medium' geschuldet, bei dem jegliche Kommunikation von allen angeschlossenen Stationen empfangen werden kann. Das Baseline Privacy Interface (in dessen neuester Version BPI+ [4]) sorgt dafür, dass nur autorisierte Endgeräte Informationen austauschen können. Unbeteiligte Endgeräte sind dagegen nicht in der Lage, die Daten zu entschlüsseln. BPI stellt dazu im Prinzip eine verschlüsselte Punkt-zu-Punkt-Verbindung her, über das die gesamte Kommunikation zwischen Endgerät und Kopfstelle stattfindet. Das

Konzept ist also unmittelbar mit dem Netzwerk verknüpft und ersetzt daher auch nicht die Systeme, die sich auf die Verschlüsselung der Inhalte konzentrieren.

2.4 Neue Sicherheitskonzepte

Zusätzlich zu den Sicherheitssystemen, die momentan schon in Rundfunk, Internet und Kabelnetzen genutzt werden, sind auch einige neue Konzepte in der Entwicklung, hauptsächlich zum Zweck, Lösungen bereitzustellen, die die Anforderungen der konvergierenden Technologien (wie Kabelnetze und Hausnetze) und der entsprechenden Geschäftsmodelle (z.B. Koexistenz von horizontalen und vertikalen Märkten im selben Netz) gewährleisten. Neben den nicht standardisierten DRM-(Digital Rights Management-) Systemen (z.B. von Microsoft) sind dies u.a. die Verfahren von DVB (CPCM - Content Protection & Copy Management) und von den US-amerikanischen CableLabs (DCAS - Downloadable CA System).

2.4.1 DVB CPCM

Das CPCM-Konzept von DVB fokussiert sich auf die Sicherheit der Inhalte innerhalb eines persönlichen Umfelds, z.B. innerhalb eines privaten Hausnetzes. Das System sorgt dafür, dass Inhalte genutzt (d.h. sicher gespeichert, kopiert, konsumiert und weitergeleitet) werden können, gemäß den Rechten, die der Kunde sich in Zusammenhang mit den Inhalten gekauft hat. Das CPCM-Konzept wird innerhalb der DVB-Aktivitäten stark von den großen amerikanischen Filmstudios und deren Verband der MPAA (Motion Picture Association of Amerika) unterstützt, so dass es durchaus eine reelle Chance für eine kommerzielle Einführung des Systems gibt. Eine hierfür hilfreiche Eigenschaft von CPCM ist es, das System mit traditionellen (proprietären) DRM- oder CA-Systemen über offenen Schnittstellen zu integrieren.

2.4.2 DCAS

In den Vereinigten Staaten von Amerika hat sich während der letzten Jahre der Druck der Regulierungsbehörde auf die Kabelnetzbetreiber verstärkt, mehr Wettbewerb in den Kabelmärken für CE-Hersteller zuzulassen. Dies hat dazu geführt, dass von der amerikanischen Kabelindustrie eine ausreichend sichere Methode entwickelt wurde, ein beliebiges CA-System, bzw. einen so genannten CA-Client per Software-Download auf ein Endgerät herunterzuladen und zu installieren. Dieses Konzept erlaubt nicht nur mehr Wettbewerb im Endgeräte- und CA-Anbieter-Markt, sondern es bietet auch einen besseren Schutz gegen Piraterie, weil beispielsweise ein gehackter Algorithmus relativ einfach und unmittelbar durch einen neueren und ggf. sichereren Algorithmus ersetzt werden kann. Außerdem erhält der Plattformbetreiber die Möglichkeit, sein CA-System komplett gegen ein moderneres und leistungsfähigeres System auszutauschen.

3 Conditional Access – die Idee und was daraus geworden ist

CA als Sicherheitskonzept ist wesentlich älter als (kommerzielles) digitales Fernsehen oder Internet. Es wurde für analoges Bezahlfernsehen entwickelt und in der ersten Hälfte der 80er Jahre in verschiedenen Märkten Europas eingeführt. In den meisten Fällen waren die Systeme jedoch aus Gründen der Systemsicherheit vollständig auf proprietäre Technologie aufgebaut. Integriert z.B. in einem Fernsehempfänger waren die Systeme nur schwer austauschbar. Als Mitte der 90er Jahre das DVB-CSA definiert und die auf Smartcard- und EMM/ECM-Technologien basierte Architektur entwickelt wurde, stellten sehr viele Anbieter von Bezahlfernsehdiensten ihre Technik auf diese damals neue DVB-Technik um und machten somit Gebrauch von der ganz wesentlich verbesserten Interoperabilität und von der Möglichkeit der Austauschbarkeit zwischen den unterschiedlichen CA-Systemen. Obwohl sich dadurch gute Voraussetzungen für die Einführung eines horizontalen Marktes für Premium Dienste ergaben, entwickelte sich dieser horizontale Markt nicht. Die für diese Entwicklung verantwortlichen Gründe liegen unter anderem in den relativ hohen Kosten für das Common Interface (CI) und für die externen CA-Module, die für die Errichtung einer den horizontalen Markt unterstützenden Technikplattform notwendig waren.

3.1 Die Situation von heute

In den über 12 Jahren, in denen die von DVB definierte CA-Architektur im Markt etabliert ist, haben sich praktisch in allen europäischen Ländern, und auch in Deutschland, kleinere oder größere Pay-TV-Märkte entwickelt. Die unterschiedlichen Anbieter innerhalb eines Marktes bedienen sich meist verschiedener CA-Systeme von häufig unterschiedlichen CA-Anbietern, um – wenigstens für eine bestimmte Anzahl von Jahren – die getätigte Anschubfinanzierung der neuen Dienste, die in der Regel in Form von Subventionierungen der Endgeräte stattfindet, gegen potentielle Konkurrenz schützen zu können. So entstand in Europa ein Markt, in dem 5 CA-Anbieter (NDS, Conax, Viaccess, Nagravision und Irdeto) verblieben sind. Ihre Systeme basieren auf der DVB-Architektur, jedoch ist keines mit irgendeinem anderen der 5 Systeme kompatibel, geschweige denn interoperabel. Aus Sicht des Endkunden ist die Situation

mit den 5 zueinander inkompatiblen Lösungen oftmals sehr unbefriedigend, da der Kunde bei Empfang verschiedener Dienste in der Regel auch mehrere Empfangsgeräte mit unterschiedlichen CA-Decodern benötigt.

3.2 Die Anforderungen von heute

Die meisten heute am Markt etablierten CA-Systeme bieten sehr ähnliche Leistungsmerkmale, obwohl diese auf sehr unterschiedliche Art und auf verschiedenem Sicherheitsniveau implementiert sind. Alle Systeme haben als selbes Ziel, mediale Inhalte so abzusichern, dass diese nur für autorisierte Kunden zugänglich sind. Dabei soll es sehr flexibel möglich sein, einzelne Applikationen für Kundengruppen oder sogar für individuelle Kunden separat freizuschalten, und dies innerhalb sehr kurzer Zeiträume. Wichtig ist außerdem, dass CA-Systeme für alle Geschäftsmodelle eingesetzt werden können, und dass sie den Empfang von anderen, nicht durch CA geschützten Diensten nicht blockieren oder deren Konsum beeinträchtigen. Außerdem müssen CA-Systeme kostengünstig implementierbar sein. Eine weitere sehr wichtige Anforderung besteht in der einfachen Möglichkeit, die Systeme zu aktualisieren oder sogar komplett auszutauschen. Eine problemlose Aktualisierung ist wichtig, um schnell und sicher auf die Einführung neuer Dienste reagieren zu können oder stets die höchst mögliche Sicherheitsstufe implementiert zu haben, während die Austauschbarkeit u.a. Konkurrenz zwischen den CA-Herstellern fördert.

3.3 Die Probleme von heute

Wie bereits erläutert, war in den Anfangsjahren des digitalen Fernsehens die Austauschbarkeit der unterschiedlichen CA-Systeme gut gewährleistet. Die verfügbaren Smartcard-Technologien erfüllten die Sicherheitsanforderungen der Plattformbetreiber. Mit zunehmendem kommerziellem Erfolg von Pay TV, z.B. in Frankreich, Spanien und Großbritannien, steigerte sich auch die Hacker-Aktivität und damit der Druck auf die Plattformbetreiber und die CA-Hersteller, die Sicherheit der Systeme zu erhöhen und mögliche Schwachstellen abzustellen. Die sich in den darauf folgenden Jahren der Internet-Revolution etablierenden Internet-Foren verstärkten diesen Druck zusätzlich und ermöglichten es, dass sich neben Pay TV und CA auch die Aktivitäten der Piraten zu einem Millionengeschäft entwickelten.
Um die Sicherheit ihrer Systeme trotz verstärkter Hacker-Aktivitäten gewährleistet zu wissen, mussten die meisten CA-Lieferanten ihre kommerziell eingesetzten Systeme regelmäßig durch zusätzliche Sicherheitsmaßnahmen aktualisieren. Die zu diesem Zweck entwickelten Sicherheitstechniken wurden nicht durch DVB spezifiziert, sondern von den CA-Herstellern individuell entwickelt. Sie basieren demnach nicht auf einen Standard sondern sind hochgradig proprietär. Besonders dramatisch an dieser Entwicklung war, dass diese anbieterspezifischen Techniken zum Teil direkt in die Integrierten Schaltkreise der Digitalempfänger integriert wurden, um z.B. ein Pairing zwischen dem Decoder-Gerät und der Smartcard zu bewirken. Die Sicherheit der CA-Systeme konnte dadurch zwar erhöht werden, jedoch wurde die Interoperabilität, im Sinne einer Austauschbarkeit von CA-Systemen, quasi unmöglich gemacht und nur noch durch den Einsatz eines sehr hohen technischen und finanziellen Aufwands ermöglicht. Die proprietären Systemkomponenten verursachen eine Bindung an einen CA-Anbieter, die einen gewünschten Wettbewerb zwischen den CA-Systemen verhindert.
Im Zuge der Entwicklung der heutigen digitalen Rundfunkplattformen zeigte sich, dass CA-Systeme aus rein kommerziellen Gründen immer öfter ausgetauscht werden müssen. Dies ist z.B. im Fall einer Aquisition eines CA-Anbieters durch einen anderen CA-Anbieter notwendig oder im Fall der Übernahmen eines Kabelnetzes durch einen anderen Betreiber, wenn dieser die unterschiedlichen technischen Systeme zwecks Effizienzsteigerung harmonisieren muss. Außerdem werden CA-Wechsel notwendig, wenn das eingesetzte System stark kompromittiert ist. Die erwähnten zusätzlichen Sicherheitsmaßnahmen der CA-Lieferanten machen in der Regel den Austausch eines CA-Systems ohne gleichzeitigen Austausch der bestehenden Empfängerpopulation nicht mehr möglich. Ein Austausch der Empfänger jedoch ist für einen Plattformbetreiber oft wirtschaftlich nicht darstellbar.
Neue Sicherheits- und Funktionalitätsanforderungen an die CA-Systme bewirken ihre kontinuierliche und marktorientierte Modernisierung durch die CA-Hersteller. Bei diesen Entwicklungsarbeiten spielen allerdings die aktuellen, kurzfristig zu behebenden Probleme eine weitaus größere Rolle als die Notwendigkeit, eine strategisch orientierte Anpassung an die Anforderungen für die nahe Zukunft durchzuführen. Zudem riskieren die etablierten Marktteilnehmer bei einer Neuorientierung des Marktes einen Verlust des im ursprünglichen Markt erworbenen Status. Diese Tatsachen gelten gleichermaßen für den CA-Markt. Deshalb ist das Bestreben von einigen Marktteilnehmern nicht sonderlich groß, zu einem interoperablen System zurückzukehren.
Großen Handlungsbedarf sehen dagegen die Kabelnetzbetreiber durch die Tatsache gegeben, dass die CA-Systeme noch immer stark rundfunkorientiert sind und z.B. keine Möglichkeiten bieten, den bidirektionalen Charakter der Kabelnetze zum Zwecke der Effizienzsteigerung zu nutzen. Zudem ist es fraglich, ob es anhand der heutigen CA-Architektur überhaupt möglich ist, die Inhalte der neuen, auf interakti-

vem Fernsehen basierenden Dienste (z.B. Video on Demand) ausreichend zu schützen und zugleich die für diese Dienste charakteristischen Funktionalitätsmerkmale in Anspruch zu nehmen. In DSL-Netzen beispielsweise wird in der Regel heute kein CA eingesetzt. DRM-Systeme übernehmen hier Teilfunktionen des CA wie die Freischaltung der Kunden.

4 Anforderungen an die nächste Generation CA-Systeme

Der primären Aufgabe eines CA-Systems nachkommend, Inhalte und Dienste gegen unerlaubten Zugriff zu schützen und dadurch Diebstahl zu vermeiden, stehen als oberste Anforderung für eine Weiterentwicklung die Sicherheitsaspekte. CA-Hersteller gleichsam wie die Betreiber von CA-Plattformen haben dies in den verschiedenen Arbeitsgremien immer wieder bestätigt. Trotzdem müssen die Betreiber der CA-Plattformen dafür sorgen, dass weitere Anforderungen bei der Entwicklung neuer Techniken beachtet werden. Bei diesen Anforderungen geht es darum, die zukünftigen CA-Syteme mit Schnittstellen zu versehen, die eine spätere Integration in den operationellen Betrieb z.B. der Kabelplattformen auf möglichst einfache und effiziente Weise erlauben. Im Fall eines Kabelnetzes betrifft dieser Integrationsprozess hauptsächlich das vollständige Einbinden des CA-Systems in das technische Übertragungssystem (Play-out, Empfänger, etc.), die Anbindung an das Netzmanagement und die Integration in das Back-Office-System, wie OSS (Operational Support System) und CSS (Customer Support System). Weitere wichtige Anforderungen bestehen in der Interoperabilität und der Austauschbarkeit der technischen Systeme bzw. einzelner Module sowie in einer hohen Kosteneffizienz.
Erfahrungen der letzten Jahre zeigen, dass die Anforderungen bezüglich Interoperabilität und Austauschbarkeit einerseits und Kosteneffizienz andererseits stark miteinander verbunden sind und sich gegenseitig bedingen, weshalb diese Anforderungen auch, neben denen der Sicherheitsaspekte, bei der Entwicklung der nächsten Generation CA-Systeme eine bedeutende Rolle spielen.

4.1 Interoperabilität und Sicherheit

Die in den letzten 10 Jahren gemachten Erfahrungen beim Betrieb von CA-Systemen lehren, dass eine praktisch kontinuierliche Verbesserung der Sicherheitsaspekte der kommerziell eingesetzten CA-Systeme nicht umgangen werden kann, um Diebstahl oder andere Schäden durch Hacker und Piraten zu minimieren. Zudem hat sich herausgestellt, dass durchaus die Notwendigkeit besteht, die Sicherheitssysteme komplett auszutauschen. Durch einen Austausch des CA-Systems können Sicherheitsrisiken weiter minimiert werden. Es können neue Funktionalitäten implementiert und die Kosteneffizienz der gesamten Infrastruktur optimiert werden.
Beobachtungen zeigen, dass der Grad der Interoperabilität zwischen CA-Systemen während der letzten 5 bis 10 Jahre kontinuierlich abgenommen hat. Wie bereits erwähnt, ist die Verwendung von proprietärer Technologie dabei von entscheidender Bedeutung. Das Gleichgewicht zwischen Sicherheit und Interoperabilität spiel besonders für den Dienstanbieter eine wichtige Rolle. Es ist notwendig, um einerseits die Einnahmen sicherzustellen und andererseits genügend Flexibilität zu haben, um auf die Entwicklungen am Markt reagieren zu können. Weil die Interoperabilität steigenden Sicherheitsanforderungen weichen musste, verschlechterte sich die Gesamtwettbewerbsposition der Plattformbetreiber zunehmend. Unter anderem soll genau dieses Phänomen in der nächsten Generation CA-Systeme vermieden werden. Um in der Zukunft eine marktgerechte Alternative bereitzustellen, soll die nächste Generation CA-Systeme auf einer Architektur beruhen, die auf State-of-the-Art-Sicherheitstechniken aufgebaut ist und es zudem ermöglicht, z.B. durch das Herunterladen neuer Software auf die eingesetzten Decoder-Plattformen, das alte CA-System komplett oder in Teilen auszutauschen, ohne dass dadurch der Betrieb gestört oder die Sicherheitsaspekte negativ beeinträchtigt werden.

4.2 Von der Rundfunkinfrastruktur zum Telekommunikationsnetz

Die Infrastrukturen der europäischen Kabelnetzbetreiber haben sich schon während der letzten Jahre von traditionell rundfunkorientierten Verteilstrukturen in bidirektionale Telekommunikationsnetze gewandelt. Diese modernen Breitbandnetze unterstützen sowohl die Übertragung einer Vielzahl von analogen und digitalen Fernsehsignalen als auch das Bereitstellen von High-speed-Internet- und Telefondiensten. Werden diese Dienste heute allgemein als einzelne Komponenten eines Dienstkatalogs angeboten, so hat bereits die Integration der Komponenten zu einem individuellen Multimediadienst begonnen. Diese Entwicklung wird sich fortsetzen; traditionelle und neue Applikationen werden sich vermischen und neue Dienstkonzepte entstehen lassen. Für Kabelnetzbetreiber hat diese Entwicklung ganz erheblichen Einfluss auf die Festlegung der Anforderungen.

4.2.1 Optimierung der Netzwerkauslastung

Die im Bereich der Dienstintegration erkennbare Tendenz stellt konkrete Anforderungen an die nächste Generation CA-Systeme. Erstens müssen Wege ge-

funden werden, den bidirektionalen Charakter der modernen Breitbandnetze besser auszunutzen. Es wurde bereits erwähnt, dass momentan ein nennenswerter Teil der Downstream-Kapazität in Kabelnetzen dazu verwendet wird, regelmäßig CA Informationen (z.B. EMMs) auszusenden, weil es bei einem Rundfunksystem keine Möglichkeit gibt zu erkennen, ob der Kunde, bzw. die Smartcard des Kunden, die für die Freischaltung notwendigen Informationen auch tatsächlich erhalten hat. Dies wäre bei der Nutzung eines Rückkanals nicht notwendig. Der Empfänger könnte den Erhalt der Information quittieren, und die zyklische Aussendung könnte bis auf weiteres ausgesetzt werden. Diese Funktionalität wird von der heutigen DVB-CA-Architektur nicht berücksichtigt. Eine entsprechende Erweiterung der CA-Architektur ist somit aus erläuterten Gründen notwendig.

4.2.2 Neue Dienste & Anforderungen

Zukünftig werden Inhalte in zunehmendem Maße nicht nur in bestimmten Marktsegmenten vermarktet werden, sondern plattformübergreifend, ggf. sowohl über Rundfunknetze als auch IP-basiert übertragen. Beispielsweise können die heute traditionell ausgestrahlten Rundfunkprogramme durch interaktive Anwendungen begleitet werden. Die Möglichkeit, rechtlich erworbene Applikationen z.B. in einer Heimnetz-Umgebung möglicherweise per CPCM- oder DRM-Verfahren zu managen, stellt zusätzliche Anforderungen an das CA-System. Die Minimalanforderung besteht darin, dass das CA-System die Möglichkeiten des CPCM-/DRM-Systems nicht einschränken oder gar verhindern darf. Weitere Möglichkeiten der Abstimmung zwischen CA- und CPCM-/DRM-Verfahren sind denkbar. Bei all diesen neuen Möglichkeiten ist die Sicherstellung der Interoperabilität zwischen CA-Systemen umso erforderlicher. Hinzu kommt die Tatsache, dass zukünftig nicht mehr alle Inhalte von professionellen Betreibern angeboten werden. Dienste, die per Peer-to-Peer-Verbindung ausgetauscht werden, können ebenfalls schutzwürdig sein, so dass die nächste Generation CA-Systeme auch entsprechenden Anforderungen gerecht werden muss. Weitere Konstellationen sind denkbar und dürfen nicht vom zukünftigen Sicherheitsmechanismus ausgeschlossen werden.

5 Laufende Arbeiten

Ziel der Kabelnetzbetreiber ist es, die oben erläuterten Anforderungen möglichst zeitnah in die existierenden CA-Systeme zu integrieren und für den kommerziellen Einsatz nutzbar zu machen. Aus diesem Grund wurden laufende Arbeiten in DVB unterstützt und, soweit die Notwendigkeit bestand, neue Arbeiten initiiert und aktiv vorangetrieben. Gleichzeit wurde eine Arbeitsgruppe innerhalb von EuroCableLabs ins Leben gerufen mit der Aufgabe, die DVB-Arbeiten aktiv vorzubereiten und voranzutreiben. Im Folgenden werden die Aktivitäten der DVB Commercial und Technical Modules sowie die Arbeiten von EuroCableLabs vorgestellt.

5.1 DVB Commercial Module

Mitte 2005 signalisierten einige DVB-Mitglieder die Notwendigkeit, den damals bereits 12 Jahre bestehenden DVB Common Scrambling Algorithmus (DVB-CSA) zu aktualisieren. Als Hauptproblem wurde die sich stetig und rasant entwickelnde Rechenleistung von handelsüblichen PCs angeführt. Diese Entwicklung kann möglicherweise dazu führen, dass in naher Zukunft per CSA verwürfelte Signale nach nur kurzer Rechenzeit entwürfelt werden können. Der CA-Algorithmus wäre in diesem Fall grundlegend geknackt und entsprechend geschützte Programme könnten praktisch frei und ohne Autorisierung dekodiert werden. Um dieser Situation zuvorzukommen, wurde in DVB beschlossen, die kommerziellen Anforderungen für CSA neu zu definieren und eine neue Version des DVB-CSA, Version 3, zu entwickeln.
Hauptsächlich durch die Eingaben der Kabelnetzbetreiber wurden die Arbeiten in einem zweiten Schritt auf Untersuchungen der gesamten DVB-CA-Architektur ausgeweitet. Wegen des hohen Stellenwertes, die diese Arbeiten für die Kabelnetzbetreiber besitzen, hat sich EuroCableLabs verstärkt engagiert und besetzt mit dem Sekretär der Arbeitsgruppe und weiteren verantwortlichen Positionen Schlüsselfunktionen für die zukünftige Entwicklung.
Wichtige Voraussetzungen für alle sicherheitsrelevanten Arbeiten innerhalb von DVB bestehen darin, ihre Ergebnisse in eine umfassende Sicherheitsarchitektur zu integrieren, die auch als „Harmonized Security Framework“ bezeichnet wird.
Erster konkreter Schritt für die Entwicklung des CA-Systems der nächsten Generation war die Durchführung einer Study Mission, die eine generelle Notwendigkeit dieser Technologie feststellen sollte. Aus 11 eingereichten Beiträgen wurden 8 Fälle konstruiert, von denen wiederum 5 die für einen Start der Arbeiten durch DVB genügend breite Unterstützung von DVB-Mitgliedern bekamen:

1. Interoperabilität und Austauschbarkeit (z.B. durch Herunterladen des CA-Systems, Beispiel DCAS)
2. Alternative für das Common Interface (CI)
3. Verhinderung der Möglichkeit des Austauschens von Kontrollwörtern zwischen Endnutzern (z.B. per Internet)
4. Rückkanalfähigkeit der Netze
5. Erweiterung der CA-Architektur für den PC

Die Punkte 1. und 2. wurden mit höchster Priorität bereits in das Arbeitsprogramm von DVB aufgenommen. Punkt 3 wurde als Teilaspekt in die Arbeiten der Austauschbarkeit (Punkt 1) aufgenommen. Auch zu Punkt 4 betreffend der Rückkanalfähigkeit insbesondere von Fernsehkabelnetzen wurden bereits spezifische Arbeiten gestartet. Die zurzeit durchgeführten Arbeiten beinhalten die Erstellung von Nutzeranforderungen für die nachfolgend zu entwickelnde Technik. Dies gilt für die Punkte 1. bis 4. Punkt 5 wird derzeit nicht bearbeitet.

5.2 DVB Technical Module

Die dritte Version des DVB Common Scrambling Algorithmus - es ist die zweite für den kommerziellen Einsatz in Fernsehempfängern vorgesehene Version - wurde in 2006 von einer innerhalb des Technical Modules erstellten Arbeitsgruppe bestehend aus Cryptology-Experten entwickelt. Das Ergebnis wird zurzeit durch ein unabhängiges Expertenteam sicherheitstechnisch überprüft.

5.3 EuroCableLabs

Im Rahmen der Arbeiten der EuroCableLabs werden die Anforderungen der Kabelnetzbetreiber zusammengetragen und in die Aktivitäten des DVB Commercial Modules eingespeist. Die Vorstellungen der einzelnen Netzbetreiber zu den zukünftigen Sicherheitsmechanismen harmonisieren generell, gehen jedoch im Detail auseinander und beinhalten z.T. unterschiedliche Migrationsszenarien bezüglich eingesetzter Technologien und Zeiträume. Diese unterschiedlichen Ansichten entstehen aufgrund der Vielzahl der derzeit in Europa betriebenen CA-Systeme/-Versionen und Netzarchitekturen. Eine Konsensbildung der involvierten Betreiber konnte jedoch bisher immer herbeigeführt werden.
Eine weitere Aufgabe von EuroCableLabs besteht darin, eine enge Zusammenarbeit mit der Industrie (z.B. die Gerätehersteller und die CA-Lieferanten) zu initiieren. Es sollen kurz- und mittelfristige Möglichkeiten analysiert werden, wie die Migration des heutigen CA-Systems in ein System der nächsten Generation effizient und den Anforderungen der Kabelindustrie entsprechend durchgeführt werden kann.

6 Ausblick

Die Modernisierung des CA-Systems durch die Entwicklung des neuen CSA durch DVB ist für viele Anwender dieser Technik ausreichend. Kabelnetzbetreiber unterstützen die von DVB durchgeführten Arbeiten, benötigen jedoch für die zukünftige Nutzung von CA-Systemen weitere Maßnahmen. Dies liegt insbesondere an der konvergenten Netzstruktur, die aus den herkömmlichen Rundfunkverteilnetzen und den modernen Kommunikationsstrukturen entstehen und die sich hervorragend zur Übertragung von integrierten Multimediadiensten anbieten. Um diese modernen Dienste mit hoher Sicherheit gegen unbefugten Zugriff effizient über die neue Infrastruktur übertragen zu können, muss ein modernes Sicherheitssystem entwickelt werden. Aufgrund der weiten Verbreitung des DVB-CA-Systems der heutigen Generation und der Tatsache, dass auch zukünftig noch Rundfunkdienste über einfache Verteilnetze übertragen werden müssen, ist es aus Sicht der Kabelnetzbetreiber wünschenswert, das CA-System von heute den Anforderungen entsprechend anzupassen und weiter zu entwickeln. Zu diesem Zweck werden innerhalb der EuroCableLabs Anforderungen erstellt und diese in die entsprechenden DVB-Gremien eingespeist. Zudem diskutieren die Kabelnetzbetreiber im Rahmen der von EuroCableLabs koordinierten Arbeiten die Anforderungen mit anderen Industriefirmen und versuchen, Migrationstrategien in Richtung auf die zu entwickelnde, neue Generation CA-System vorzubereiten. Dabei ist das Interesse aller beteiligten Firmen zu berücksichtigen. Die Arbeiten und Prozesse, die zusammen mit den Partnern aus den andern Industriezweigen begonnen wurden, werden in den nächsten 12 bis 18 Monaten voraussichtlich konkrete Ergebnisse liefern. Die Lieferanten der Sicherheitssysteme werden anschließend die Entwicklung der nächsten Systemgeneration beginnen können. Ziel wird es sein, die erforderliche Interoperabilität und die funktionellen und sicherheitstechnischen Anforderungen der nächsten 5-10 Jahre zu gewährleisten.

7. Literatur

[1] U. Reimers: Digitale Fernsehtechnik - Datenkompression und Übertragung für DVB, 2. Auflage, Springer Verlag Berlin Heidelberg New York, 1997

[2] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), Official Journal of the European Commission, 24.4.2002

[3] EU Stand-by Initiative.
http://energyefficiency.jrc.cec.eu.int/

[4] DOCSIS 1.1 Baseline Privacy Plus Interface Specification. CM-SP-BPI+-I12-050812, 12. August 2005, www.cablemodem.com/specifications