Verschlüsselung und Adressierung in Kabelnetzen

– Ein Beitrag zur Klarstellung der Begriffe –

TKLM-Dokument Nr. 02/2004 V 0.1 vom 26. April 2004

1. Ausgangslage

Beim GSDZ-Workshop „Set-Top-Boxen“ am 5. Februar 2004 wurden wiederholt die Begriffe „Verschlüsselung“ und „Adressierung“ in einen Zusammenhang gebracht, der fachlich nicht gegeben ist und deshalb eher Verwirrung stiftete.
Nachfolgend werden beide Begriffe erläutert und die Unterschiede verdeutlicht.

2. Verschlüsselung
Überblick die Verschlüsselung

Nach einem grundsätzlichen Überblick über den Zweck von Systemen zur Verschlüsselung werden die in digitalen Kabelnetzen wesentlichen Gründe für den Einsatz von Verschlüsselung dargelegt. In der Fachsprache gelten für die Verschlüsselung für Fernsehangebote die eigentlich richtigeren Bezeichnungen „Conditional Access“ und die Abkürzung „CA“. Das kann mit „Zugriff unter Bedingungen“ oder „Bedingter Zugriff“ übersetzt werden. Das CA-System erlaubt den „bedingten Zugriff“ auf Fernsehangebote. Es ist vornehmlich dafür gedacht, über einen längeren Zeitraum (mehrere Minuten und länger) laufende Fernsehangebote nur den Teilnehmern zugänglich zu machen, die dafür berechtigt sind. Auch sind die CA-Systeme so ausgelegt, dass jeweils eine größere Zahl von Kunden berechtigt ist, die jeweiligen Angebote zu nutzen. CA-Systeme sind für Point-to-Multipoint-Kommunikation gedacht, sie sind nicht dafür konzipiert, die Kommunikation zwischen Einzelnen zu schützen. (Ob die heutigen CA-Systeme die Last eines ein echtes Video-on Demand-Fernsehens verarbeiten können, wurde noch nirgends getestet; man darf aber getrost bezweifeln, dass die CA-Systeme mit dem dabei entstehenden Verkehrsaufkommen zurecht kommen.)

2.2 CA-Systeme zum Schutz von Pay-Angeboten

Verschlüsselung steht für ein technisches System, mit dem der Zugriff auf Programme und/oder Dienste nur besonders Autorisierten möglich ist. Die Verschlüsselung dient hier dazu, den Zugang zu einzelnen Programmen zu steuern. Oft handelt es sich dabei um Pay-Programme oder Pay-Dienste, bei denen der Zugriff durch einen kostenrelevanten Vertrag mit dem Anbieter/den Anbietern ermöglicht wird. Die Bezahlung des vereinbarten Betrags ist somit eine für den Zugriff zu erfüllende Bedingung. Typische Pay-Angebote umfassen eine Vielzahl von Paketen, die der Kunde in unterschiedlichen Kombinationen bestellen kann, und die für ihn individuell freigegeben werden. Wer mehr Pakete abonniert, muss auch mehr bezahlen. Das Extremum ist Video on Demand, wo ein bestimmter Film für einen einzelnen Kunden freigeschaltet wird und vom Kunden bezahlt werden muss. Die Verschlüsselung dient dazu, dass nur der Kunde, der für das Angebot bezahlt, dieses auch nutzen kann.

2.3 Grundverschlüsselung

Aus Sicht des Kunden etwas anders gelagert ist die sog. „Grundverschlüsselung“. Hier werden *alle* Angebote verschlüsselt, auch das Grundangebot mit den Programmen, die üblicherweise als kostenfrei oder „Free-to-air“ bezeichnet werden. Hier dient die Verschlüsselung dazu, den Zugang zum gesamten Netz zu steuern.
Der Kunde erhält bei Abschluss eines Vertrages mit dem Netzbetreiber eine Smart-Card. Außerdem muss seine Set-Top-Box in der Lage sein, das vom Netzbetreiber verwendete CA-System zu „verstehen“. Sogenannte „Free-to-air-Boxen“ oder „Zapping-Boxen“ enthalten keinerlei CA-Kompenten und sich daher für den Empfang jedweder verschlüsselter Programme ungeeignet. Hinter der beabsichtigten Einführung einer Grundverschlüsselung in Kabelnetzen steht zunächst die Absicht „Schwarzseher“ auszuschließen. Es kommt immer wieder vor, dass Hausbewohner ein „coaxiales Verlängerungskabel“ an die Kabeldose ihres Nachbarn anschließen und sich so unrechtmäßigen Zugang zum Kabel verschaffen. Die Kabelnetzbetreiber behaupten, dass etwa 10 % der tatsächlichen Nutzer des Kabels keinen Vertrag haben und die von ihnen in Anspruch genommene Dienstleistung nicht bezahlen. Bei etwa 17 Mio. zahlenden Kabelkunden in Deutschland errechnet sich daraus ein jährlicher Verlust in der Größenordnung von 250 Mio. €. Wenn alle Programme grundverschlüsselt sind, so benötigt ein Kabelhaushalt für jedes angeschlossene Fernsehgerät eine eigene Karte. Das „Umstecken“ einer Karte in das jeweils benutzte Gerät ist zwar grundsätzlich möglich, stößt aber in der Praxis auf vielerlei Schwierigkeiten und wird in der Realität keine Bedeutung gewinnen.
Die Grundverschlüsselung bringt über das Verhindern von Schwarzsehern hinaus aber noch einen weiteren Vorteil für die Kabelnetzbetreiber: Sind es die Kunden einmal gewöhnt, dass sie für den Fernsehempfang eine Smart-Card besitzen müssen, so lassen sich Pay-Angebote viel leichter vermarkten. Der Schritt zu er CA-fähigen Set-Top-Box ist bereits getan. Für den Empfang von Pay-Angeboten sind keinerlei Änderungen am Empfangssystem des Kunden mehr nötig. Der Nutzer kann damit unkompliziert auf Pay-Angebote zugreifen. Genau dies aber wollen die heutigen Free-to-air-Anbieter verhindern. Sie haben keinerlei Interesse daran, dass der Markt durch zusätzliche Angebote – und seien es Pay-Angebote – erweitert wird. Das ist ein wesentlicher Grund, warum sich die öffentlich-rechtlichen und auch die großen privaten Fernsehanbieter gegen die Grundverschlüsselung aussprechen.

2.4 Verschlüsselung zum Schutz von Individualkommunikation

Der Schutz der Point-to-Point-Verbindungen vor unberechtigtem Mithören ein weiterer Grund dafür, in digitalen Kabelnetzen eine Verschlüsselungstechnologie einzusetzen. Das Kabel ist ein sogenanntes „Shared medium“. Das bedeutet, dass alle an einem Strang des Kabels hängenden Teilnehmer sämtliche dort vorbeilaufenden Informationen im Grunde genommen mithören können. Sofern es sich bei diesen Informationen um Fernsehprogramme handelt, kann der rechtmäßige Zugriff durch die bereits zuvor geschilderten Methoden des Conditional Access sichergestellt werden. Im digitalen Kabel soll jedoch zukünftig nicht nur Fernsehen übertragen werden sondern auch Telefonie und schnelles Internet. Damit Telefonie und Internet nur von dazu Berechtigten gehört und genutzt werden können, ist neben anderen technischen Maßnahmen auf eine Verschlüsselung des Datenverkehrs zwischen Kabelkopfstation und dem berechtigten Nutzer erforderlich. Auch diese Art der Verschlüsselung wird im Englischen mit „encryption“ bezeichnet und hat nichts mit dem CA-System von DVB zu tun.

3. Das Konzept von CA-Systemen für DVB

Das Konzept der Verschlüsselung von Fernsehsignalen erfordert Maßnahmen auf der Sende- und Empfangsseite. Zuerst wird die Reihenfolge der Bits des DVB-Transportstroms gemäß einem europäisch standardisierten, jedoch vertraulichen Algorithmus verändert. Für die Maßnahme gilt die Bezeichnung Verwürfelung [scrambling]. Diesem Signal werden nun elektronische Schlüsselworte hinzugefügt, die eine beliebige Struktur aufweisen können. Dieser Vorgang ist aus technischer Sicht die eigentliche Verschlüsselung [encryption].
Das mit den Schlüsselworten ergänzte verwürfelte Signal wird nun übertragen. Bedingt durch die Verwürfelung kann es auf der Empfangsseite ohne zusätzliche Maßnahmen nicht genutzt werden. Es besteht nämlich der Bedarf, die Verwürfelung wieder rückgängig zu machen, was mit Hilfe einer als Entwürfeler [descrambler] bezeichneten technischen Funktionseinheit erfolgen kann. Um diese in Betrieb setzen zu können, sind einerseits die Schlüsselworte erforderlich, aber auch die Daten auf einer dem Nutzer bei Vertragsabschluss ausgehändigten SmartCard, bei der es sich um eine auch von anderen Anwendungen (z. B. EC-Karte) her bekannte intelligente Chipkarte handelt. Diese Kombination führt zur Entschlüsselung [decryption], wobei nach dem Entwürfeler wieder der ursprüngliche DVB-Transportstrom zur Verfügung steht.
Für die Realisierung eines CA-Systems ist auf der Empfangsseite auf jeden Fall ein CAM [conditional access module] erforderlich. Diese technische Funktionseinheit kann entweder im Endgerät (z. B. Set-Top-Box) integriert sein, was als „embedded CA“ bezeichnet wird, oder über die standardisierte Schnittstelle CI [common interface] in das Endgerät eingesteckt werden.
In den beiden aufgezeigten Fällen benötigt der Nutzer die bereits erwähnte SmartCard. Sie wird in den Kartenleser des CAMs eingesteckt.
Es gibt unterschiedliche CA-Systeme, bedingt durch die Verwendung verschiedener Strukturen für die Schlüsselworte. Die Kennzeichnung der CA-Systeme erfolgt durch Kunstworte wie „Betacrypt, „Nagravision“ und andere.
CA regelt den Zugriff auf Programme und Dienste. Dies wird nicht nur von den relevanten DVB-Standards unterstützt, sondern hat sich auch in der Praxis bestens bewährt. Dabei spielt es keine Rolle, ob es sich um Angebote von Bouquets, einzelnen Kanälen, VoD [video on demand] oder NVoD [near video on demand] handelt. Falls der Vertrag seitens des Teilnehmers nicht erfüllt wird, ist im Bedarfsfall eine Sperrung der SmartCard durch Sperrung der Schlüsselworte möglich.
Eine CA-SmartCard ist weder personenbezogenen noch gerätebezogen. Jeder der die SmartCard zur Verfügung hat, kann mit einem entsprechenden Endgerät die
abonnierten Programme/Dienste empfangen, soweit es an das Netz angeschlossen ist, in dem die gewünschten Programme/Dienste verbreitet werden. Allerdings hat jede SmartCard eine eindeutige Nummer. Diese Nummer wird benötigt, um bestimmte Karten für bestimmte Angebote freizuschalten. Im Subscriber Management System (SMS) wird die Verknüpfung zwischen dem Namen des Abonnenten und der Nummer seiner SmartCard hergestellt. Wenn der Kunde ein Paket oder einen Film bestellt hat, werden über das SMS Schlüsselworte in den Datenstrom des Kabelnetzes eingefügt. Diese Steuerbefehle gelten nur für die SmartCard des bestellenden Kunden, dies wird durch die eindeutige Nummer gewährleistet. Die Schlüsselworte erlauben es der Kabelbox, in der die SmartCard des Kunden steckt, das bestellte Angebot zu entschlüsseln. Die Nummer ist auch erforderlich, um verloren gegangene, missbräuchlich verwendete oder kopierte Karten zu sperren.
Bei dem bisherigen Konzept wird davon ausgegangen, dass für den Empfang von Pay-Programmen/Pay-Diensten für jedes Endgerät eine SmartCard erforderlich ist, wenn Programme/Dienste gleichzeitig empfangen werden sollen. Es ist aber auch grundsätz-

lich möglich, die Freischaltung am Wohnungsübergabepunkt (WÜP) oder sogar am Hausübergabepunkte (HÜP) durchzuführen. Dies ist besonders dann von Interesse, wenn Programme/Dienste über unterschiedliche CA-Systeme empfangen werden sollen.
CA-Systeme haben sich optimal bewährt und stellen für den Zugriff auf Pay-Programme/Pay-Dienste eine praxisorientierte Lösung dar.

4. Adressierung

Eine Adresse ist die eindeutige Beschreibung eines Ziels, wie von der klassischen Post Jedem bekannt.. Die Adresse eines Geräts in einem Rechnernetz wird in aller Regel dadurch gewonnen, dass die Seriennummer des Geräts mit weiteren Parametern verknüpft wird. Sie ist somit eindeutig und nur schwer zu fälschen oder von unberechtigten Dritten in Erfahrung zu bringen.
In der Praxis wird meist die auf dem Internet-Protokoll (IP) basierende Adressierung angestrebt, weil dann auf bereits bekannte Verfahren zurückgegriffen werden kann. Grundsätzlich sind aber beliebige Systeme möglich.
Wie bei jedem Rechnernetz benötigt auch bei DVB jedes Endgerät, das für Point-to-Point-Kommunikation genutzt werden soll, eine Adresse. Dies erscheint allerdings nur vertretbar, wenn gezielt ein bestimmtes Endgerät erreicht werden soll. Ein Beispiel wären Anwendungen mit Interaktivität über den Rückkanal (also nicht lokale Interaktivität). Derartige Anwendungen sind in Deutschland noch kaum am Markt. Deshalb verwenden die in Deutschland bislang verwendeten Set-Top-Boxen auch nur ein CA-System und keine Adressierung. Eine Adressierung wird dann unumgänglich, wenn das „Triple-Play“ zum Zuge kommt oder wo über das Fernsehgerät eine bidirektionale individuelle Kommunikationsbeziehung aufgebaut wird. Wird am Fernsehgerät nur ein Artikel zum Bestellen ausgewählt, die Bestellung selbst aber über den Rückkanal eines Festnetz- oder Mobilfunktelefons abgewickelt, so ist auch hier keine Adressierung der STB oder des Fernsehgeräts nötig.
Für die Fernsehverbreitung in Kabelnetzen ist also Adressierung nicht erforderlich, da für Pay-Angebote ein CA-System völlig ausreicht. Die vollständige Abwicklung des Betriebs über Adressierung würde außerdem dem Kabelnetzbetreiber eine unangemessene Kontrolle der Nutzer ermöglichen.
Die Adressierung stellt auch keine sachlich gebotene Lösung dar, um die Zahlung der Entgelte für den Kabelanschluss sicherzustellen. Dafür bietet sich in Netzen mit Baumstruktur ein CA-System an. Alternativ kommt der Einsatz von Sternnetzen für die Verteilung der Programme/Dienste in Betracht. Ein typisches Beispiel hiefür ist die Programmverbreitung über xDSL-Netze.

5. Fazit

Verschlüsselung (CA) ist eine auf Programme/Dienste bezogene Maßnahme zum Schutz der finanziellen Interessen von Netzbetreiber und Inhalteanbieter. Adressierung ist eine auf das physikalische Kabelnetz bezogene Maßnahme, die zum Schutz der bidirektionalen Kommunikation vor unerwünschtem Mithören oder Missbrauch des Netzes erforderlich ist.
CA-Module können beim Endgerät, Wohnungsübergabepunkt (WÜP) oder Hausübergabepunkt (HÜP) eingesetzt werden. Adressierung ist dagegen bei jedem Endgerät erforderlich.
Verschlüsselung (CA) und Adressierung stellen völlig unterschiedliche Funktionalitäten dar. Es besteht auch keine Abhängigkeit voneinander. In der Praxis müssen allerdings auch adressierte Informationen verschlüsselt werden, damit die übertragenen Informa-

tionen ausschließlich vom Adressaten genutzt werden können. (Vergleich mit der Briefpost: Auch ein adressierter Umschlag sollte undurchsichtig sein.)
Für die GSDZ sind Verschlüsselung (CA) und Adressierung auch deshalb von besonderem Interesse, weil durch beide Formen Zugangskontrolle ausgeübt wird.

Düsseldorf/Stuttgart, 26. April 2004

LfM / U. Freyer
LFK / W. Berner