

Übersicht über positiv bewertete Konzepte für geschlossene Benutzergruppen

(September 2003 bis Januar 2010)

Folgende Konzepte für Systeme bzw. für einzelne Module zur Sicherstellung einer geschlossenen Benutzergruppe (AV-Systeme) hat die Kommission für Jugendmedienschutz bisher positiv bewertet. Die Bewertungen der KJM stehen unter dem Vorbehalt einer entsprechenden Umsetzung im Regelbetrieb.

Darüber hinaus hat die KJM einige übergreifende Jugendschutzkonzepte, die sich jeweils aus Bausteinen mit AV-Systemen und technischen Mitteln zusammen setzen, positiv bewertet. Vgl. hierzu die gesonderte Übersicht über positiv bewertete übergreifende Jugendschutzkonzepte.

Die Übersicht ist nach den Kategorien Module und Gesamtkonzepte geordnet und innerhalb der Kategorien chronologisch nach Datum der Entscheidung durch die KJM.

Module

Die KJM bewertet auch Teillösungen für geschlossene Benutzergruppen positiv. Dies ermöglicht den Anbietern eine leichtere Umsetzung von geschlossenen Benutzergruppen in der Praxis. So besteht für Anbieter die Möglichkeit, diese Teillösungen in Eigenverantwortung in unterschiedliche Altersverifikationssysteme einzubauen und zu Gesamtlösungen geschlossener Benutzergruppen zu kombinieren, die dann den Anforderungen des Jugendmedienschutz-Staatsvertrags (JMStV) und der KJM entsprechen. Damit kann eine größere Vielfalt von gesetzeskonformen Lösungen entstehen. Derartige Module reichen allein aber nicht aus, sondern müssen vom Inhalte-Anbieter im Rahmen eines geeigneten Gesamtkonzepts eingesetzt werden.

Zentraler Kreditkartenausschuss (ZKA): Debit-Chipkarte:

Bei der vom Zentralen Kreditausschuss (ZKA) entwickelten Debit-Chipkarte handelt es sich um ein Modul für eine geschlossene Benutzergruppe. Die Karte alleine reicht nicht aus, um eine geschlossene Benutzergruppe sicherzustellen, sie muss im Rahmen eines geeigneten Gesamtkonzepts zur Anwendung kommen.

Die Debit-Chipkarte wird von deutschen Kreditinstituten seit 1996 unter anderem mit der Funktion „GeldKarte“ eingesetzt. Die aktuelle Version, die seit einiger Zeit durch Banken und Sparkassen im Rahmen des turnusmäßigen Austausches an deren Kunden ausgegeben wird, bietet weitere Funktionen außerhalb des bargeldlosen Zahlungsverkehrs. Dazu gehört ein „Jugendschutzmerkmal“, das in Kooperation mit dem Bundesverband Deutscher Tabakwaren-Großhändler und Automatenaufsteller (BDTA) entwickelt wurde, um der Verpflichtung zur Altersverifikation an Zigarettenautomaten nachzukommen. Die gleiche Lösung kann im Internet im Rahmen der Herstellung geschlossener Benutzergruppen eingesetzt werden.

(Entscheidung der KJM vom November 2003)

fun communications GmbH mit dem Modul „fun SmartPay AVS“:

Bei „Fun SmartPay AVS“ von fun communications handelt es sich ebenfalls um ein Modul für eine geschlossene Benutzergruppe. Das Modul alleine reicht nicht aus, um eine geschlossene Benutzergruppe sicherzustellen, es muss im Rahmen eines geeigneten Gesamtkonzepts zur Anwendung kommen. Das Modul „Fun SmartPay AVS“ basiert auf einer bereits erfolgten Face-to-Face-Kontrolle bei der Eröffnung eines Bankkontos. „Fun SmartPay AVS“ wertet das Jugendschutzmerkmal der o.g. GeldKarte der deutschen Kreditwirtschaft aus. Die ec-, Bank- und Sparkassen-Karten sind in der aktuellen Version mit Chips (GeldKarte) ausgestattet, die den Bankkunden durch ein Altersmerkmal zur Nutzung verschiedener Funktionen autorisieren. Die Authentifizierung des Nutzers einer geschlossenen Benutzergruppe im Internet erfolgt über einen Chipkartenleser am Computer, über den die auf dem Chip der ec-Karte enthaltenen Daten verifiziert werden.

(Entscheidung der KJM vom August 2005)

SCHUFA Holding AG mit dem Modul „Identitäts-Check mit Q-Bit“:

Auch beim „Identitäts-Check mit Q-Bit“ der Schufa handelt es sich um ein Modul für eine geschlossene Benutzergruppe. Das Modul alleine reicht nicht aus, um eine geschlossene Benutzergruppe sicherzustellen, es muss im Rahmen eines geeigneten Gesamtkonzepts zur Anwendung kommen.

Beim Modul „Identitäts-Check mit Q-Bit“ wird zum Abgleich von User-Daten auf eine bereits erfolgte Face-to-Face-Kontrolle zurückgegriffen. Zum Abgleich werden nur Daten von Kreditinstituten genutzt, die die Volljährigkeitsprüfung gemäß den Vorgaben des Geldwäschegesetzes durchführen. Bei AV-Systemen, die sich der SCHUFA-Abfrage bedienen, muss zusätzlich sicher gestellt sein, dass die Auslieferung der Zugangsdaten eigenhändig per Einschreiben oder durch eine ähnlich qualifizierte Alternative erfolgt.

(Entscheidung der KJM vom September 2005)

Giesecke & Devrient GmbH: Modul „Internet-Smartcard“:

Die Internet-Smartcard von Giesecke & Devrient stellt ein Modul für die Authentifizierung dar. Nach der Identifizierung wird dem Nutzer persönlich ein spezielles Hardware-Token übergeben: seine persönliche, auslesesichere und kopiergeschützte Internet-Smartcard. Sie wird über den USB-Anschluss in den Computer eingesteckt und gewährleistet eine gegenseitige Authentisierung ihres Inhabers und des genutzten Portals mittels sicherer Signaturen. Damit kann leicht bedienbar der Zugang zu der geschlossenen Benutzergruppe hergestellt werden. Seine Internet-Smartcard muss der Nutzer bei jeder Nutzung zur Authentifizierung in den Computer einstecken und die dazugehörige Adult-PIN eingeben. Die Smartcard allein reicht für eine geschlossene Benutzergruppe nicht aus, sondern muss vom verantwortlichen Anbieter in ein geeignetes Gesamtkonzept eingebaut werden. Neben einem ausreichenden Identifizierungsverfahren müssen hier außerdem Maßnahmen hinzu kommen, die das Risiko der Weitergabe der Zugangsdaten an unberechtigte Personen wirksam reduzieren. Ein Beispiel für einen geeigneten Gesamtansatz ist das Konzept von Lotto Hamburg (s.u.).

(Entscheidung der KJM vom November 2007 und vom August 2008)

Informatikzentrum der Sparkassenorganisation GmbH (SIZ): „SIZCHIP AVS“:

SIZ stellt seine Software-Plattform „SIZCHIP AVS“ als Modul bzw. Baustein AVS-Betreibern oder Inhalteanbietern zur Verfügung. SIZ liefert die Altersinformationen aus der geprüften ZKA-Chipkarte und ermöglicht ihnen damit, sichere Altersprüfungen vorzunehmen. Dabei wird das auf der Debit-Chipkarte (u. a. ec-Karte) des Nutzers gespeicherte Jugendschutzmerkmal ausgewertet und der Zugang zu Inhalten in der geschlossenen Benutzergruppe des Anbieters nur dann freigegeben, wenn der Nutzer volljährig ist.

(Entscheidung der KJM vom März 2008)

insic GmbH: „insic ident“:

Beim Verfahren „insic ident“ handelt es sich um ein Modul für die Identifizierung. Die Identifizierung sowie eine Volljährigkeitsprüfung sind in drei Schritten vorgesehen: Nach der Registrierung werden die Daten und die Volljährigkeit des Nutzers mit Hilfe des Verfahrens „Ident-Check mit Q-Bit“ der Schufa überprüft. Als letzter und wesentlicher Schritt ist die Überprüfung der Identität und Volljährigkeit des Nutzers im Rahmen einer Face-to-Face-Kontrolle unter Einbeziehung von amtlichen Ausweisdaten an einer Verkaufsstelle mit persönlicher Aushändigung eines Aktivierungscodes vorgesehen.

(Entscheidung der KJM vom April 2008)

Gesamtkonzepte:

Coolspot AG: „X-Check“:

In einer Variante erfolgt die Identifizierung des Kunden entweder mittels des Post-Ident-Verfahrens oder mittels des positiv bewerteten Moduls „Identitäts-Check mit Q-Bit“ der Schufa. Das Schufa-Modul gewährleistet dabei eine verlässliche Identifizierung von Erwachsenen, indem auf bereits erfolgte Face-to-Face-Kontrollen von Kreditinstituten zurückgegriffen wird. Die Zugangsdaten für die geschlossene Benutzergruppe werden nur den zuvor als volljährig identifizierten Nutzern persönlich zugestellt. Für die Authentifizierung benötigt der Kunde neben einer eigenen Software eine Hardware-Komponente (USB-Stick) sowie eine PIN-Nummer: Bei jedem Durchschreiten des X-Check-Tores muss sich der Nutzer mit dem persönlichen Passwort und seinem personalisierten „Personal ID Chip“ authentifizieren.

In einer weiteren Variante bei Coolspot wird für die Altersprüfung das positiv bewertete Modul „fun Smart Pay AVS“ der fun communications GmbH genutzt. „Fun SmartPay AVS“ greift auf eine bereits erfolgte Identifizierung bei der Eröffnung eines Bankkontos zurück und nutzt für die Authentifizierung das Jugendschutzmerkmal der Geldkarte der deutschen Kreditwirtschaft. Dazu benötigt der Nutzer einen Chipkartenleser an seinem Computer. Bei jedem Durchschreiten des X-Check-Tores wird das Jugendschutzmerkmal der ZKA-Chipkarte überprüft.

(Entscheidung der KJM vom September 2003 in der Fassung der Entscheidung vom Oktober 2005)

Arcor Online GmbH:

Beim Konzept „Video on Demand“ von Arcor erfolgt die Identifizierung mittels des Post-Ident-Verfahrens. Die Authentifizierung bei jedem Nutzungsvorgang erfolgt mittels eines zweistufigen Zugangskonzepts, das den Zugriff auf den Erwachsenenbereich mit zusätzlichen Hürden versieht.

Von einer Hardwarekomponente kann nur deshalb abgesehen werden, weil die Zugangsdaten nicht nur mit unkalkulierbar hohen finanziellen, sondern zusätzlich mit großen persönlichen Risiken für den autorisierten Nutzer verknüpft sind. Durch das von der geschlossenen Benutzergruppe unabhängige Kunden-Lieferantenverhältnis besteht bei Weitergabe der Zugangsdaten ein erhebliches Risiko der Übernahme oder Manipulation der virtuellen Identität des Kunden. Auch ein unautorisierter Nutzer kann Verträge kündigen oder neue abschließen, er kann im Namen des Kunden agieren, kann E-Mails abrufen oder versenden, den Mail-Verkehr verfolgen oder in fremden Namen Übergriffe tätigen. Das System von Arcor ist nur als Zugangsschutz für eigene Inhalte und nicht bei Inhalten Dritter ausreichend.
(Entscheidung der KJM vom November 2003)

T-Online International AG:

Beim Konzept von T-Online erfolgt die Identifizierung mittels des Post-Ident-Verfahrens. Bei der Authentifizierung bei jedem Nutzungsvorgang wird der Zugriff auf den Bereich der Inhalte, vor denen entsprechend § 4 Abs. 2 Kinder und Jugendliche geschützt werden müssen, über ein doppeltes Login abgesichert.

Von einer Hardwarekomponente kann nur deshalb abgesehen werden, weil die Zugangsdaten nicht nur mit unkalkulierbar hohen finanziellen, sondern zusätzlich mit großen persönlichen Risiken für den autorisierten Nutzer verknüpft sind. Durch das von der geschlossenen Benutzergruppe unabhängige Kunden-Lieferantenverhältnis besteht bei Weitergabe der Zugangsdaten ein erhebliches Risiko der Übernahme oder Manipulation der virtuellen Identität des Kunden. Auch ein unautorisierter Nutzer kann Verträge kündigen oder neue abschließen, er kann im Namen des Kunden agieren, kann E-Mails abrufen oder versenden, den Mail-Verkehr verfolgen oder in fremden Namen Übergriffe tätigen. Das System von T-Online ist nur als Zugangsschutz für eigene Inhalte und nicht bei Inhalten Dritter ausreichend.

(Entscheidung der KJM vom November 2003)

Vodafone D2:

Das Konzept von Vodafone D2 sieht die Volljährigkeitsprüfung des Kunden durch den persönlichen Kontakt bei Vertragsabschluss in einem Vodafone D2-Shop bzw. einem angeschlossenen Partnergeschäft vor. Für die Authentifizierung bei jedem Nutzungsvorgang kommt eine individualisierte Adult-PIN unter Einbeziehung einer Hardware-Komponente (SIM-Karte) zum Einsatz. Auf ein darüber hinausgehendes Schutzniveau kann verzichtet werden, weil Vodafone das AVS nicht als Dienstleistung für Dritte anbietet.

(Entscheidung der KJM vom Dezember 2003 in der Fassung der Entscheidung vom Juli 2005)

Full Motion Entertainment GmbH: Mirtoo AVS (ehemals Crowlock):

Die Identifizierung der Kunden erfolgt durch das Post-Ident-Verfahren. Die Authentifizierung bei jedem Nutzungsvorgang erfolgt mittels eines Challenge-Response-Verfahrens mit Hardwareschlüssel in Form einer VideoDVD und einer PIN. Hardwareschlüssel und PIN werden dem Kunden persönlich, per Post-Ident-Verfahren, zugestellt.

(Entscheidung der KJM vom Mai 2004)

RST Datentechnik/F.I.S.: AVSKey/AVSKeyfree plus digipay:

Bei AVSKey/AVSKeyfree plus digipay ist die Identifizierung der Kunden mittels Post-Ident-Verfahren vorgesehen. Für die Authentifizierung bei jedem Nutzungsvorgang werden eine individualisierte und kopiergeschützte CD-ROM und eine Adult-PIN eingesetzt. Durch das zusätzliche Payment-Modul „digipay“ wird die Gefahr der Weitergabe der Zugangsdaten minimiert.

(Entscheidung der KJM vom September 2004)

HanseNet:

Für die Identifizierung wird das oben genannte positiv bewertete Modul „Identitäts-Check mit Q-Bit“ der Schufa genutzt. Das Schufa-Modul gewährleistet dabei eine verlässliche Identifizierung von Erwachsenen, indem auf bereits erfolgte Face-to-Face-Kontrollen von Kreditinstituten zurückgegriffen und Zugangsdaten für die geschlossene Benutzergruppe nur den zuvor als volljährig identifizierten Nutzern persönlich zugestellt werden. Für die Authentifizierung bei jedem Nutzungsvorgang der Video-on-Demand-Angebote wird eine personalisierte Smartcard verwendet, die nur im eigenen Netz nutzbar und an den Anschluss des identifizierten Kunden gebunden ist.

(Entscheidung der KJM vom Oktober 2005)

Premiere AG: Blue Movie:

Die Identifizierung der Kunden wird entweder durch das positiv bewertete Schufa-Modul „Identitäts-Check mit Q-Bit“ oder vor Ort im Handel durch geschultes und ausgebildetes Personal durchgeführt. Das Schufa-Modul gewährleistet dabei eine verlässliche Identifizierung von Erwachsenen, indem auf bereits erfolgte Face-to-Face-Kontrollen von Kreditinstituten zurückgegriffen und die Zugangsdaten für die geschlossene Benutzergruppe nur den zuvor als volljährig identifizierten Nutzern persönlich zugestellt werden. Die Authentifizierung bei jedem Nutzungsvorgang erfolgt über eine personalisierte Smartcard. Der „Blue Movie“-Kunde muss bei jeder Filmbestellung seinen persönlichen Adult-PIN angeben. Um die Gefahr der Weitergabe von Zugangsdaten weiter zu reduzieren, sind Bezahlfunktionen integriert.

(Entscheidung der KJM vom Dezember 2003 in der Fassung der Entscheidung vom Oktober 2005)

Bernhard Menth Interkommunikation: „18ok“:

Die zumindest einmalige Identifizierung des Nutzers erfolgt durch das Post-Ident-Verfahren. Zur Authentifizierung des identifizierten Nutzers bei jedem Nutzungsvorgang wird als technische Maßnahme eine Hardwarekomponente in Form eines persönlichen USB-Sticks verwendet, zu dem ein individueller Zugangs-PIN ausgegeben wird. Um die Weitergabe der Zugangsdaten zusätzlich zu erschweren, kommt in der Sphäre des Benutzers noch ein Kostenrisiko dazu.

(Entscheidung der KJM vom Dezember 2005)

Erotic media AG: für Mediendienst, der von Kabel Deutschland vermarktet wird:

Nutzer, die auf das Pay-per-View-Angebot zugreifen möchten, müssen zuerst ihre Volljährigkeit persönlich nachweisen, in dem sie sich über das Post-Ident-Verfahren identifizieren. Danach bekommen sie ihren individuellen Zugangsschlüssel, die „Erotik-PIN“, persönlich zugestellt. Um zu gewährleisten, dass die Filme in der geschlossenen Benutzergruppe nur für die identifizierten Erwachsenen zugänglich sind, müssen sich diese zu Beginn jeder Nutzung authentifizieren. Dafür muss die Erotik-PIN (Adult-Passwort) sowie die Nummer der personalisierten Smart-Card eingegeben werden. In Zugangsdaten und Smart-Card ist auch eine Bezahlungsfunktion integriert. Die Filmmutzung ist zeitlich begrenzt. Durch diese Kombination verschiedener Schutzmaßnahmen wird das Risiko der Weitergabe von Zugangsdaten und Smart Card an unautorisierte Dritte reduziert.

(Entscheidung der KJM vom Juni 2006)

Cybits AG: „AVS '[verify-U]-System II'“:

Mit diesem AV-System wird die Möglichkeit zur Einrichtung geschlossener Benutzergruppen an mehreren Endgeräten vorgesehen: gegenwärtig sowohl bei PCs als auch bei Mobilfunkgeräten und Settopboxen. Die Identifizierung erfolgt über den "Identitäts-Check mit Q-Bit" der Schufa Holding AG. Als alternative Identifizierungsvariante ist außerdem das Post-Ident-Verfahren vorgesehen. Um zu gewährleisten, dass der Zugang zur geschlossenen Benutzergruppe nur für die zuvor identifizierten Erwachsenen zugänglich ist, müssen sich diese zu Beginn jeder Nutzung authentifizieren. Hierfür muss jeder Nutzer seinen Zugang mit dem persönlich zugestellten Alters-PIN (Adult-PIN) auf der Verify-U-Internetseite aktivieren und sein Endgerät beim System anmelden. Zusätzlich ist im Fall der Weitergabe der Zugangsberechtigung ein Kostenrisiko gegeben.

(Entscheidung der KJM vom August 2006)

S + M Schaltgeräte Service- und Vertriebsgesellschaft mbH: „m/gate“:

Die S+M GmbH setzt bei ihrem AV-System „m/gate“ das Mobiltelefon als Hardwarekomponente ein. Für die Identifizierung der erwachsenen Nutzer ist neben verschiedenen Varianten des Post-Ident-Verfahrens („m/gate-PostIdent“) die Identifizierung über den Geldautomaten sowie über Online-Banking („m/gate-Bank“), in Verbindung mit Übersendung einer gesonderten Jugendschutz-PIN per Übergabe-Einschreiben, vorgesehen. Um zu gewährleisten, dass nur identifizierte User Zugang zu der geschlossenen Benutzergruppe erhalten, müssen sich diese zu Beginn jeder Nutzung eines für S+M freigeschalteten Internetangebots authentifizieren. Dafür muss der Nutzer mit seinem registrierten Mobiltelefon die auf der Website an-

geforderte und zugeordnete Rufnummer wählen. Der Nutzer wird mit einem Voice-Recorder verbunden, der ihn um Mitteilung seiner individuellen, per Übergabe-Einschreiben zugestellten Jugendschutz-PIN bittet. Der Nutzer gibt nach Wahl der angezeigten Telefonnummer die Jugendschutz-PIN ein. Nach Überprüfung aller Daten wird das kostenpflichtige Angebot freigeschaltet. Die Nutzung ist dabei auf eine IP-Adresse begrenzt. Das Konzept umfasst ausreichende Schutzmaßnahmen, die die Multiplikation der Zugangsdaten erschweren und das Risiko der Weitergabe dieser Zugangsdaten reduzieren.

Das System der S + M GmbH soll neben dem Internet auch an Verkaufsautomaten wie z.B. Zigarettenautomaten eingesetzt werden.

(Entscheidung der KJM vom Oktober 2006)

Kabelnetzbetreiber ish NRW GmbH & Co KG und iesy Hessen GmbH & Co KG:

Das Konzept von ish und iesy ist für den Einsatz bei deren geplantem Pay-per-View-Angebot vorgesehen. Bei dem Angebot können Erwachsene pornografische Filme mittels kostenpflichtigen Einzelabrufs bestellen. Der Mediendienst kann nur mit kabeltauglichem Digital Receiver und Smart-Card empfangen werden.

Nutzer, die auf das Angebot zugreifen möchten, müssen zuerst ihre Volljährigkeit persönlich nachweisen. Dafür ist die Identifizierung über das Express-Ident-Verfahren der Deutschen Post Express GmbH (DHL) oder gegenüber Handelspartnern oder technischen Service-Mitarbeitern der Kabelnetzbetreiber vorgesehen. Der individuelle Zugangsschlüssel zur geschlossenen Benutzergruppe, das „Adult-Passwort“, wird den Nutzern zusammen mit der Smart-Card und den allgemeinen Zugangsdaten persönlich übergeben.

Um zu gewährleisten, dass die Filme in der geschlossenen Benutzergruppe nur identifizierten Erwachsenen zugänglich sind, müssen sich diese zu Beginn jeder Nutzung authentifizieren, indem sie ihr individuell zugeteiltes Adult-Passwort eingeben. Nur bei Übereinstimmung des Adult-Passwortes mit der personalisierten Smart-Card und – bei der Bestellung per SMS – der zuvor registrierten Mobilfunknummer des Nutzers erfolgt die Freischaltung des bestellten Films. Außerdem ist in den Zugangsdaten und der Smart-Card eine Bezahlungsfunktion integriert. Durch die Kombination dieser verschiedenen Schutzmaßnahmen wird das Risiko der Weitergabe von Zugangsdaten und Smart Card an unautorisierte Dritte reduziert.

(Entscheidung der KJM vom November 2006)

Nordwest Lotto und Toto Hamburg – Staatliche Lotterie der Freien und Hansestadt Hamburg:

Beim Konzept von LOTTO Hamburg erfolgt die Identifizierung der Internet-Nutzer über das „Lotto-Ident-Verfahren“: Die Volljährigkeit des Kunden wird in einer Lotto-Annahmestelle persönlich und mit Abgleich von Personalausweis oder Reisepass überprüft. Für die Authentifizierung ist eines der o.g. Module – die Internet-Smartcard der Giesecke und Devrient GmbH - vorgesehen: Nach erfolgreicher Identifizierung erhält der Kunde vor Ort ein spezielles Hardware-Token: seine persönliche, auslesesichere und kopiergeschützte Internet-Smartcard. Sie wird über den USB-Anschluss in den Computer eingesteckt und gewährleistet eine gegenseitige Authentisierung ihres Inhabers und des genutzten Portals mittels sicherer Signaturen. Damit kann leicht bedienbar der Zugang zu der geschlossenen Benutzergruppe hergestellt werden. Seine Smartcard muss der Nutzer bei jedem Lotteriede-

bzw. Wettspiel zur Authentifizierung in den Computer einstecken und die dazugehörige Adult-PIN eingeben. Das grundsätzliche Risiko, dass ein Nutzer seine Smartcard und Zugangsdaten an unberechtigte Dritte weitergibt, wird dadurch reduziert, dass dem berechtigten Nutzer dabei Kosten entstehen können. Der Nutzer ist auch der Eigentümer des Bankkontos, von dem aus die Spieltransaktionen bezahlt werden.

(Entscheidung der KJM vom Juli 2007)

„mtG-AVS“ der media transfer AG:

Das Konzept „mtG-AVS“ der media transfer AG (mtG) beinhaltet zwei Authentifizierungsvarianten: Die erste Variante arbeitet mit einer Bindung an ein Endgerät (PC), bei der zweiten Variante wird ein USB-Token zur Authentifizierung eingesetzt. Die Identifizierung erfolgt in beiden Fällen durch das Modul „Identitäts-Check mit Q-Bit“ der Schufa Holding AG, die Zugangsdaten werden per Einschreiben eigenhändig ausgeliefert.

In beiden Varianten wird das Risiko der Weitergabe an unautorisierte Personen dadurch reduziert, dass mit der Authentifizierung eine Bezahlungsfunktion verbunden ist. Der Zugriff auf Inhalte, die nur Erwachsenen zugänglich gemacht werden dürfen, ist kostenpflichtig und wird dem Account des Kunden belastet.

(Entscheidung der KJM vom Dezember 2007)

„SMS-PIN-Verfahren“ der Staatlichen Lotterieverwaltung München:

Das Konzept zum „SMS-PIN-Verfahren“ von Lotto Bayern sieht die Identifizierung der Internet-Nutzer über das Lotto-Ident-Verfahren oder Post-Ident-Verfahren vor: Die Volljährigkeit des Kunden wird dabei persönlich und mit Abgleich von Personalausweis oder Reisepass überprüft, z.B. in einer Lotto-Aannahmestelle oder bei der Post. Bei jedem Online-Spiel am PC ist eine Authentifizierung des Kunden erforderlich. Hierfür hat der Kunde das „SMS-PIN-Verfahren“ zu durchlaufen: Der Server generiert dabei als Zugangspasswort für die geschlossene Benutzergruppe per Zufall eine begrenzt gültige PIN. Der Kunde muss von seinem bei der Registrierung angegebenen Handy eine SMS mit dieser PIN an Lotto Bayern senden. Die empfangene SMS kann von Lotto Bayern über die Handynummer des Absenders eindeutig dem Kunden zugeordnet werden, der diese Handynummer bei der Identifizierung angegeben hat. Da dem berechtigten Nutzer bei Weitergabe seiner Zugangsdaten erhebliche Kosten entstehen können und gleichzeitig mögliche Gewinne immer nur auf sein Konto fließen, ist die Wahrscheinlichkeit für einen Missbrauch der Zugangsdaten gering.

(Entscheidung der KJM vom Januar 2008)

insic GmbH: „AVS InJuVerS“:

Das Konzept „AVS InJuVerS“ der insic GmbH soll insbesondere bei staatlichen Lottogesellschaften und gewerblichen Spielvermittlern eingesetzt werden und sieht die Identifizierung der Internetnutzer über das Post-Ident-Verfahren oder über das Verfahren „Schufa Ident-Check mit Q-Bit“ vor. Nach der Anmeldung auf einer Registrierungsseite findet bei jedem Nutzungsvorgang im Internet sowie bei jeder Transaktion, z.B. einer Bezahlung oder Spielschein-Abgabe, eine Authentifizierung des Kunden statt. Bei der Authentifizierung

kommen verschiedene Endgeräte zum Einsatz: Mobilfunkgerät, PC oder Set-Top-Box. Das insic-AVS ist gleichzeitig ein Bezahl-System bzw. steuert angeschlossene Bezahlssysteme, so dass mit den Zugangsdaten in angeschlossenen Shops und Diensten (Lotto) bezahlt werden kann. Dabei besteht ein Kostenrisiko von mehreren 1000 Euro, die von unberechtigten Personen vom hinterlegten Konto des berechtigten Nutzers abgebucht werden können.

(Entscheidung der KJM vom April 2008)

Deutsche Telekom AG: „NetGate“:

„NetGate“ baut auf bereits von der KJM positiv bewerteten AVS-Konzepten der T-Online International AG auf und enthält zusätzliche Möglichkeiten der Identifizierung und Authentifizierung für einen künftigen Einsatz im gesamten Konzern der Deutschen Telekom AG. Auch für Kooperationspartner soll „NetGate“ als Altersverifikationsdienst eingesetzt werden. Die Identifizierung ist entweder mittels Post-Ident-Verfahren, persönlich im Telekom-Shop oder über entsprechend geschulte Vertriebspartner vorgesehen. Alternativ ist auch eine Identifizierung über das von der KJM positiv bewertete Modul „Identitäts-Check mit Q-Bit“ der Schufa oder über Personendaten möglich, die bei Abschluss eines T-Mobile-Vertrags erfasst wurden. In den letzten beiden Varianten wird auf eine bereits erfolgte Face-to-Face-Kontrolle zurückgegriffen – ergänzt durch eine Auslieferung der Zugangsdaten per eigenhändigem Einschreiben. Auch für die Authentifizierung gibt es verschiedene Varianten. Es kommen verschiedene Endgeräte zum Einsatz – PC, Set-Top-Box und Mobilfunkgerät – und damit verschiedene Verfahren mit Hardwarebindung. Zudem ist in jedem Fall die Eingabe einer speziellen, individuellen Erwachsenen-PIN erforderlich. Hinzu kommen Maßnahmen in der Sphäre des Benutzers, die das Risiko der Weitergabe der Zugangsdaten und deren unautorisierte Nutzung durch Dritte reduzieren: Finanzielle Risiken sowie weitere persönliche Risiken, wie die Übernahme der virtuellen Identität des autorisierten Nutzers, das Einsehen von Rechnungsdaten und ggf. Einzelverbindungsdaten sowie das Ändern von Telefon-, Access- und Mobilfunktarifen.

(Entscheidung der KJM vom Dezember 2008)

Vodafone D2: „Adultpark“

Das Konzept des „Adultpark“ baut auf einem im September 2003 von der KJM positiv bewerteten Altersverifikationskonzept der Arcor AG & Co. KG zur Sicherstellung einer geschlossenen Benutzergruppe für Video-on-Demand-Angebote im Internet auf. Mit der zum Dezember 2009 vollzogenen vollständigen Verschmelzung von Arcor auf Vodafone werden im Internet die Video-on-Demand-Angebote beider Unternehmen unter dem Dach von Vodafone zusammengeführt. Die bereits im Post-Ident-Verfahren als volljährig identifizierten Video-on-Demand-Kunden von Arcor können nun auch auf die Angebote im „Adultpark“ von Vodafone zugreifen, ohne sich nochmals persönlich identifizieren zu müssen. Eine Anmeldung zur geschlossenen Benutzergruppe des „Adultpark“ ist künftig aber auch für Erwachsene möglich, die weder Arcor-Kunde waren noch über einen Vodafone-Mobilfunkvertrag verfügen. Für diese Nutzer sieht das Konzept ebenfalls eine persönliche Identifizierung über Post-Ident vor. Für die Authentifizierung bei jedem Nutzungsvorgang des Web-Angebots muss der Nutzer jeweils Benutzername und Passwort sowie zusätzlich einen

speziellen, individuellen „ab 18-PIN“ eingeben. Damit soll sichergestellt werden, dass nur identifizierte und altersgeprüfte Personen Zugriff auf die geschlossene Benutzergruppe des „Adultpark“ erhalten.

(Entscheidung der KJM vom Dezember 2009)