Kommission für Jugendmedienschutz

die medienanstalten

Informationspapier

Übersicht über positiv bewertete Konzepte für geschlossene Benutzergruppen

Folgende Konzepte für Systeme bzw. für einzelne Module zur Sicherstellung einer geschlossenen Benutzergruppe im Sinne des § 4 Abs. 2 S. 2 JMStV (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 im Sinne des § 4 Abs. 2 S. 2 JMStV und technischen Mitteln im Sinne des § 5 Abs. 3 Nr. 1 JMStV zusammensetzen, 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.

1. Zentraler Kreditkartenausschuss (ZKA): „Debit-Chipkarte“
2. fun communications GmbH: „fun SmartPay AVS“
3. SCHUFA Holding AG: „Identitäts-Check mit Q-Bit“
4. Giesecke & Devrient GmbH: „Internet-Smartcard"
5. Informatikzentrum der Sparkassenorganisation GmbH (SIZ): „SIZCHIP AVS“
6. insic GmbH: „insic ident“
7. RISER ID Services GmbH: „ID Check“
8. Aristotle Inc.: „Aristotle Integrity/Instant Global ID and Age Verification (Integrity)“
9. edentiX GmbH: „Online Ausweischeck“
10. Web Shield Limited: „KYC Shield“
11. Cybits AG: „[verify-U] face-to-face”
12. identity Trust Management AG: „identity Age Check“
13. WebID Solutions GmbH : "WebID Identify & AgeCheck - Verfahren zur Identitätsprüfung und Altersverifikation"
14. Deutsche Post AG: „POSTIDENT durch Videochat“
15. IDnow GmbH: „IDnow Video-Ident”
16. arvato direct services: „arvato VideoIdentifizierung“
17. CheckTech Service GmbH: „CheckTech Service“

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)

➢ nach oben

fun communications GmbH: „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 enthalten Daten verifiziert werden.

(Entscheidung der KJM vom August 2005)

➢ nach oben

SCHUFA Holding AG: „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. Das Q-Bit-Modul ist positiv beauskunftet, solange die Übereinstimmung der abgefragten Daten bei 100% liegt.

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 Geldwäsche-Gesetzes 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)

➢ nach oben

Giesecke & Devrient GmbH: „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 hinzukommen, 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)

➢ nach oben

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)

➢ nach oben

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)

➢ nach oben

RISER ID Services GmbH: „ID Check“

Beim „ID Check“ der RISER ID Services GmbH handelt es sich um ein Modul (Teillösung) auf der Stufe der Identifizierung zur Altersprüfung für den wiederholten Nutzungsvorgang.

Basis für die Altersprüfung durch den „ID Check“ bildet eine bereits persönlich erfolgte Identifizierung in den Meldeämtern, indem auf die Melderegister der Kommunen zurückgegriffen wird. Damit ein Telemedienanbieter über den RISER ID Check die positive Auskunft „identifiziert“ aus dem Melderegister erhält, muss die betreffende Person über einen elektronischen Zugriff des ID Check-Systems auf das amtliche Melderegister eindeutig anhand ihres Namens, des Geburtsdatums sowie der Anschrift identifiziert werden. Die im Melderegister gespeicherten relevanten Personendaten basieren auf einer „face-to-face“-Identifizierung im Meldeamt mit amtlichen Ausweisdaten.

Bei Telemedien-Anbietern, die sich im Rahmen eines geeigneten Gesamtkonzepts zur Altersprüfung ihrer Nutzer des Identifizierungsmoduls „ID Check“ von RISER bedienen, muss der Anbieter anschließend zusätzlich sicherstellen, dass die Auslieferung von Zugangsdaten nur an diejenige Person erfolgt, die über den Datenabgleich als volljährig bestätigt wurde. Dies kann z.B. eigenhändig per Einschreiben an die durch den ID Check bestätigten Adressdaten geschehen oder durch eine ähnlich qualifizierte Alternative.

(Entscheidung der KJM vom Mai 2013)

➢ nach oben

Aristotle Inc.: „Aristotle Integrity/Instant Global ID and Age Verification (Integrity)“

Bei dem System „Aristotle Integrity/Instant Global ID and Age Verification (Integrity)“ handelt es sich um ein Modul (Teillösung) auf der Stufe der Identifizierung. Das Modul alleine reicht jedoch nicht aus, um eine geschlossene Benutzergruppe sicherzustellen, es muss im Rahmen eines geeigneten Gesamtkonzepts zur Anwendung kommen.

Der Identifizierungsvorgang, der auf einer „face-to-face-Kontrolle“ per Webcam basiert, erfolgt bei „Aristotle Integrity/Instant Global ID and Age Verification (Integrity)“ in mehreren Schritten. Nach der Eingabe der persönlichen Daten des Nutzers auf der Webseite des Inhalte-Anbieters werden diese durch den Webseitenbetreiber in verschlüsselter Form an Aristotle übermittelt. Dort erfolgt der Abgleich der Daten anhand von Bonitätsdatenbanken. Anschließend übermittelt der Nutzer eine Kopie seines Personalausweises.

Im letzten Schritt erfolgt der Datenabgleich mittels face-to-face-Kontrolle des Nutzers und seines Personalausweises in einer Videokonferenz mit einem

geschulten Mitarbeiter von Aristotle Inc. Die Videokonferenz endet mit der mündlichen Übermittlung eines Passwortes an den Nutzer, das auf der Webseite des Inhalte-Anbieters eingegeben wird. Dieses kann, nachdem Aristotle Inc. die Identität des Nutzers bestätigt hat, bei jedem weiteren Log-in Vorgang genutzt werden.

(Entscheidung der KJM vom Dezember 2014)

➢ nach oben

edentiX GmbH: „Online Ausweischeck“

Bei dem System „Online-Ausweischeck“ handelt es sich um ein Modul (Teillösung) auf der Stufe der Identifizierung. Das Modul alleine reicht jedoch nicht aus, um eine geschlossene Benutzergruppe sicherzustellen, es muss im Rahmen eines geeigneten Gesamtkonzepts zur Anwendung kommen.

Der Identifizierungsvorgang, der bei „Online-Ausweischeck“ auf einer „face-to-face-Kontrolle“ per Webcam basiert, erfolgt in mehreren Schritten. Zunächst muss sich der Nutzer über die Webseite des Inhalte-Anbieters registrieren, in die das System „Online-Ausweischeck“ eingebettet wird. Nach Erhalt einer Verifizierungs-TAN wird eine Video-Konferenz mit einem Mitarbeiter der edentiX GmbH durchgeführt. Nach Nennung der TAN und Zeigen des Personalausweises vor der Kamera werden die übermittelten Daten von geschulten edentiX-Mitarbeitern auf ihre Echtheit geprüft.

(Entscheidung der KJM vom Dezember 2014)

➢ nach oben

Web Shield Limited: „KYC Shield“

Bei dem System „KYC Shield“ handelt es sich um ein Modul (Teillösung) auf der Stufe der Identifizierung. Das Modul alleine reicht jedoch nicht aus, um eine geschlossene Benutzergruppe sicherzustellen, es muss im Rahmen eines geeigneten Gesamtkonzepts zur Anwendung kommen.

Der Identifizierungsvorgang, der bei „KYC Shield“ auf einer „face-to-face-Kontrolle“ per Webcam basiert, erfolgt in mehreren Schritten. Zunächst erfolgt die Identifizierung mittels der Eingabe der persönlichen Daten auf der Webseite des Inhalte-Anbieters, in die „KYC Shield“ eingebunden wird. Anschließend wird der Nutzer aufgefordert, ein Video seines Personalausweises zu übermitteln, in dem das Foto und das Hologramm klar

erkennbar sein müssen. Abschließend findet zum Datenabgleich eine Live-Videokonferenz zwischen dem Nutzer und Web Shield statt, bei der die übermittelten Daten durch zwei geschulte Mitarbeiter geprüft werden.

(Entscheidung der KJM vom Dezember 2014)

➢ nach oben

Cybits AG: „[verify-U] face-to-face"

Bei dem System „[verify-U] face-to-face" handelt es sich um ein Modul (Teillösung) für eine geschlossene Benutzergruppe auf der Stufe der Identifizierung. Das Modul alleine reicht jedoch nicht aus, um eine geschlossene Benutzergruppe sicherzustellen, es muss im Rahmen eines geeigneten Gesamtkonzepts zur Anwendung kommen.

Das Konzept beruht auf einem mehrstufigen Identifizierungsverfahren. Die Identifikation des Nutzers erfolgt dabei in einer Kombination aus der Eingabe seiner Daten auf der Webseite des Inhalte-Anbieters und der Feststellung seiner Identität durch einen Existenz-Check und einen elektronischen Ausweis-Check. Im Anschluss daran wird dann die Identität des Nutzers in einer Videokonferenz mit geschulten Mitarbeitern der Cybits AG verifiziert, bei der das Ausweisdokument und die Übereinstimmung der Daten geprüft werden. Nur wenn alle Schritte erfolgreich abgeschlossen wurden und keine Widersprüche auftreten, erlangt der Nutzer Zugang zum gewünschten Angebot.

(Entscheidung der KJM vom Januar 2015)

➢ nach oben

identity Trust Management AG: „identity Age Check"

Bei dem System „identity Age Check" der identity Trust Management AG handelt es sich um ein Modul (Teillösung) für eine geschlossene Benutzergruppe auf der Stufe der Identifizierung. Das Modul alleine reicht jedoch nicht aus, um eine geschlossene Benutzergruppe sicherzustellen, es muss im Rahmen eines geeigneten Gesamtkonzepts zur Anwendung kommen.

Das Konzept beruht auf einem mehrstufigen Identifizierungsverfahren. Die Identifikation des Nutzers erfolgt dabei in einer Kombination aus der Eingabe seiner Daten auf der Webseite des Inhalte-Anbieters und der Überprüfung

der eingegebenen Daten durch die identity Trust Management AG. Im Anschluss daran wird dann die Identität des Nutzers in einer Videokonferenz mit geschulten Mitarbeitern der identity Trust Management AG verifiziert, bei der das Ausweisdokument und die Übereinstimmung der Daten geprüft werden.

Darüber hinaus werden dem Nutzer Zugangsdaten übermittelt. Nur wenn alle Schritte erfolgreich abgeschlossen wurden und keine Widersprüche auftreten, erlangt der Nutzer Zugang zum gewünschten Angebot.

(Entscheidung der KJM vom April 2015)

➢ nach oben

WebID Solutions GmbH: „WebID Identify & AgeCheck - Verfahren zur Identitätsprüfung und Altersverifikation“

Bei dem System "WebID Identify & AgeCheck - Verfahren zur Identitätsprüfung und Altersverifikation" der WebID Solutions GmbH handelt es sich um ein Modul (Teillösung) für eine geschlossene Benutzergruppe auf der Stufe der Identifizierung. Das Modul alleine reicht jedoch nicht aus, um eine geschlossene Benutzergruppe sicherzustellen, es muss im Rahmen eines geeigneten Gesamtkonzepts zur Anwendung kommen.

Das Konzept beruht auf einem mehrstufigen Identifizierungsverfahren. Die Identifikation des Nutzers erfolgt dabei in einer Kombination aus der Eingabe seiner Daten auf der Webseite des Inhalte-Anbieters und der Überprüfung der eingegebenen Daten durch die WebID Solutions GmbH. Im Anschluss daran wird dann die Identität des Nutzers in einer Videokonferenz mit geschulten Mitarbeitern der WebID Solutions GmbH verifiziert, bei der das Ausweisdokument und die Übereinstimmung der Daten geprüft werden. Nur wenn alle Schritte erfolgreich abgeschlossen wurden und keine Widersprüche auftreten, erlangt der Nutzer Zugang zum gewünschten Angebot.

(Entscheidung der KJM vom April 2015)

➢ nach oben

Deutsche Post AG: „POSTIDENT durch Videochat“

Bei dem System „POSTIDENT durch Videochat“ handelt es sich um ein Modul (Teillösung) für eine geschlossene Benutzergruppe auf der Stufe der Identifi-

zierung. Das Modul alleine reicht jedoch nicht aus, um eine geschlossene Benutzergruppe sicherzustellen, es muss im Rahmen eines geeigneten Gesamtkonzepts zur Anwendung kommen.

Das Konzept beruht auf einem mehrstufigen Identifizierungsverfahren. Die Identifikation des Nutzers erfolgt dabei zunächst durch die Eingabe der Ausweisdaten im Identifizierungssystem. Im Anschluss daran wird die Identität des Nutzers in einer Videokonferenz mit geschulten Mitarbeitern der Deutschen Post AG verifiziert, bei der das Ausweisdokument und die Übereinstimmung der Daten geprüft werden. Schließlich wird dem Kunden eine TAN zugesandt, durch deren Eingabe die Identifizierung abgeschlossen wird. Nur wenn alle Schritte erfolgreich durchlaufen wurden und keine Widersprüche auftreten, erlangt der Nutzer Zugang zum gewünschten Angebot.

(Entscheidung der KJM vom Juni 2015)

➢ nach oben

IDnow GmbH: „IDnow Video-Ident"

Bei dem System „IDnow Video-Ident" handelt es sich um ein Modul (Teillösung) für eine geschlossene Benutzergruppe auf der Stufe der Identifizierung. Das Modul alleine reicht jedoch nicht aus, um eine geschlossene Benutzergruppe sicherzustellen, es muss im Rahmen eines geeigneten Gesamtkonzepts zur Anwendung kommen.

Das Konzept beruht auf einem mehrstufigen Identifizierungsverfahren. Die Identifikation des Nutzers erfolgt dabei zunächst durch die Übermittlung der Kundendaten durch den Inhalte-Anbieter. Im Anschluss daran wird die Identität des Nutzers in einer Videokonferenz mit geschulten Mitarbeitern der IDnow GmbH verifiziert, bei der das Ausweisdokument und die Übereinstimmung der Daten geprüft werden. Schließlich wird dem Kunden eine TAN zugesandt, durch deren Eingabe die Identifizierung abgeschlossen wird. Nur wenn alle Schritte erfolgreich durchlaufen wurden und keine Widersprüche auftreten, erlangt der Nutzer Zugang zum gewünschten Angebot.

IDnow bietet die Altersprüfung per Videochat ohne Anmeldung und externe Software sowohl für den Webbereich als auch für mobile Endgeräte.

(Entscheidung der KJM vom Juni 2015)

➢ nach oben

arvato direct services: „arvato VideoIdentifizierung“

Bei dem System „arvato VideoIdentifizierung“ handelt es sich um ein Modul (Teillösung) auf der Stufe der Identifizierung, das eine „face-to-face-Kontrolle“ per Webcam ermöglicht. Neben der bloßen Identifizierung via Webcam als initiale Altersprüfung werden für einen wiederholten Nutzungsvorgang zusätzliche Sicherungsmaßnahmen ergriffen, die eine ausreichende Verlässlichkeit gemäß den KJM-Eckwerten bieten. Das Konzept orientiert sich an den Vorgaben zur Geldwäschegesetz-konformen Identifikation und beruht auf einem mehrstufigen Identifizierungsverfahren. Die Identifikation des Nutzers erfolgt dabei in einer Kombination aus der Eingabe der persönlichen Daten des Nutzers auf der Webseite des Anbieters und der Übermittlung der Daten an das „arvato Online Legitimationscenter“. Im Anschluss daran wird die Identität des Nutzers in einer Videokonferenz mit geschulten Mitarbeitern des Unternehmens im Namen des jeweiligen Anbieters verifiziert. Die Überprüfung und Absicherung erfolgt mittels einer dem Kunden zugesandten TAN, nach deren Eingabe durch den Kunden der Agent die Daten des Nutzers aufrufen kann. Im Rahmen der Videositzung werden das Ausweisdokument und die Übereinstimmung der Daten geprüft. Nur wenn alle Schritte erfolgreich durchlaufen wurden und keine Widersprüche auftreten, erhält der Nutzer die Zugangsdaten zum gewünschten Angebot.

(Entscheidung der KJM vom Juli 2015)

➢ nach oben

CheckTech Service GmbH: „CheckTech Service“

Bei dem System "CheckTech Service" handelt es sich um ein Modul (Teillösung) auf der Stufe der Identifizierung, das eine "face-to-face-Kontrolle" per Webcam ermöglicht. Zunächst wird die zu prüfende Person durch geschulte Mitarbeiter der CheckTech Service GmbH im Videobild in Augenschein genommen. Danach wird der Nutzer aufgefordert, das jeweils zur Prüfung vorgesehene Dokument, den Personalausweis oder Reisepass, in die Kamera zu halten, damit der Prüfer feststellen kann, ob es für den jeweiligen Prüfvorgang zugelassen ist. Im nächsten Schritt wird überprüft, ob die vor der Kamera sitzende Person mit dem Ausweisdokument übereinstimmt. Nach Ab-

schluss des bisherigen Prüfverfahrens erfolgt die eigentliche Prüfung der Daten, bei der die Prüfer die Personendaten erfassen und kontrollieren und anhand des Geburtsdatums vom System automatisch die Volljährigkeit des Nutzers bestätigt wird. Im Anschluss daran wird dem Nutzer systemseitig eine individuelle Freischaltungs-TAN auf seine Mobilfunknummer zugeschickt, die er im System eingeben muss.

Die KJM kam nach Prüfung des Konzepts zu dem Ergebnis, dass es sich bei entsprechender Umsetzung als Teillösung auf der Stufe der Identifizierung im Sinne der KJM-Kriterien zur Sicherstellung einer geschlossenen Benutzergruppe eignet. Das Modul alleine reicht jedoch nicht aus, um eine geschlossene Benutzergruppe zu gewährleisten, es muss im Rahmen eines Gesamtkonzepts zur Anwendung kommen.

(Entscheidung der KJM vom März 2017)

➢ nach oben

Gesamtkonzepte

1. Coolspot AG: „X-Check“
2. Arcor Online GmbH: „Video on Demand“
3. T-Online International AG
4. Vodafone D2
5. Full Motion Entertainment GmbH: „Mirtoo AVS” (ehemals „Crow-lock”)
6. RST Datentechnik/F.I.S.: „AVSKey/AVSKeyfree“ plus „digipay“
7. HanseNet
8. Premiere AG: „Blue Movie“
9. Bernhard Menth Interkommunikation: „18ok“
10. Erotic media AG: für Mediendienst, der von Kabel Deutschland vermarktet wird
11. Cybits AG: „AVS ’[verify-U]-System II’“
12. S + M Schaltgeräte Service- und Vertriebsgesellschaft mbH: „m/gate“
13. Kabelnetzbetreiber ish NRW GmbH & Co KG und iesy Hessen GmbH & Co KG
14. Nordwest Lotto und Toto Hamburg – Staatliche Lotterie der Freien und Hansestadt Hamburg
15. media transfer AG: „mtG-AVS“
16. Staatlichen Lotterieverwaltung München: „SMS-PIN-Verfahren“
17. insic GmbH: „AVS InJuVerS“
18. Deutsche Telekom AG: „NetGate“
19. Vodafone D2: „Adultpark“
20. Cybits AG „[verify-U] III“
21. Giropay
22. SOFORT AG: „SOFORT Ident“
23. insic GmbH: „insic AVS InJuVers“
24. Deutsche Post AG: „POSTID“
25. Colbette II Ltd.: „AVS AgeID“
26. 1&1 De-Mail GmbH: „De-Mail“
27. AUTHADA GmbH: „AUTHADA QR“ und „AUTHADA ID“
28. WebID Solutions GmbH: „WebID DIMOCO MOBILE AVS“

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)

➢ nach oben

Arcor Online GmbH: „Video on Demand“

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)

➢ nach oben

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)

➢ nach oben

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)

➢ nach oben

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)

➢ nach oben

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)

➢ nach oben

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)

➢ nach oben

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)

➢ nach oben

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)

➢ nach oben

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 Bezahlfunktion integriert. Die Filmnutzung 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)

➢ nach oben

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; vgl. auch unten die Entscheidung der KJM vom Oktober 2012)

➢ nach oben

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-Post-Ident“) 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 angeforderte 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*)

➢ nach oben

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 Bezahlfunktion 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)

➢ nach oben

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 des 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 Lotterie- 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)

➢ nach oben

media transfer AG : „mtG-AVS“

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 Bezahlfunktion 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)

➢ nach oben

Staatlichen Lotterieverwaltung München: „SMS-PIN-Verfahren“

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-Annahmestelle 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)

➢ nach oben

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 Bezahlsysteme, 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)

➢ nach oben

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 zurückge-

griffen – 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. Einzelverbindungsnachweisen sowie das Ändern von Telefon-, Access- und Mobilfunktarifen.

(Entscheidung der KJM vom Dezember 2008)

➢ nach oben

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)

➢ nach oben

Cybits AG: „[verify-U] III“

Beim AVS-Konzept „[verify-U] III“ der Cybits AG handelt es sich um die Weiterentwicklung eines AVS, das schon 2006 von der KJM positiv bewertet wurde. Die ursprünglichen Identifizierungs- und Altersprüfvarianten über Postident und über den „Identitäts-Check mit Q-Bit“ der Schufa Holding AG in Verbindung mit der persönlichen Auslieferung von initialen Zugangsdaten (Autorisierungscode) per Einschreiben „eigenhändig“ bleiben erhalten.

Als neue Identifizierungsoption bietet „[verify-U] III“ an, beim Registrierungsprozess die Daten und das Alter des Nutzers über die eID-Funktion seines neuen Personalausweises (nPA) zu prüfen.

Zur Auslieferung des Autorisierungscodes sieht „[verify-U] III“ zusätzlich die Variante eines „Banklaufs“ vor: Mittels Gut- und Lastschrift wird ein zweiteiliger Autorisierungscode auf ein im Onlinebanking nutzbares Girokonto des Nutzers übermittelt. Um sicherzustellen, dass der Code über den Banklauf nur an die zuvor als volljährig identifizierte Person übermittelt wird, kommt neben Schufa-QBit im Vorfeld auch der Schufa KontonummernCheck zum Einsatz: Die Schufa bestätigt damit, dass zu der angefragten Person auch die angegebene Kontoverbindung gehört.

Alternativ kann eine Aktivierung des Nutzeraccounts über eine Variante des giropay-Verfahrens erfolgen: Der Nutzer loggt sich mit seinen Nutzerdaten über Online-Banking in sein Girokonto ein und gibt mittels gültiger TAN eine Transaktion frei. Bei erfolgreicher Transaktion bestätigt giropay umgehend die Überweisung. Anschließend erhält der als volljährig bestätigte Nutzer einen zeitlich begrenzten Aktivierungslink und kann im Registrierungsprozess von „[verify-U] III“ fortfahren.

Durch ein Zusammenspiel und Ineinandergreifen mehrerer Kontrollroutinen wird hinreichend sichergestellt, dass eine Aktivierung des Nutzeraccounts nur durch diejenige Person erfolgen kann, die zuvor als volljährig identifiziert

wurde. Der Nutzer muss sich vor jedem Zutritt zu einer geschlossenen Benutzergruppe mit seinen individuellen Zugangsdaten einloggen. Zudem ist eine Bindung des Nutzeraccounts an bestimmte im System registrierte Hardwarekomponenten erforderlich.

(Entscheidung der KJM vom Oktober 2012; vgl. hierzu auch oben Entscheidung der KJM vom August 2006)

➢ nach oben

Giropay

Für das AVS von giropay ist ein für das Online-Banking angemeldetes Girokonto des Nutzers bei einer Bank oder Sparkasse erforderlich, die am Online-Bezahlverfahren von giropay teilnimmt. Das Konzept sieht vor, dass entweder isoliert oder in Kombination mit einem Online-Bezahlvorgang an den Telemedien-Anbieter die Meldung weitergeleitet wird, ob der jeweilige Nutzer ausweislich der bei Kontoeröffnung erfolgten Identitätsprüfung volljährig ist. Bei der Begründung einer Geschäftsbeziehung mit einem kontoführenden Kreditinstitut müssen der Kunde sowie etwaige weitere Verfügungsberechtigte oder Bevollmächtigte von dem kontoführenden Kreditinstitut anhand gültiger amtlicher Ausweispapiere eindeutig und persönlich gemäß den Vorgaben des Geldwäschegesetzes (GwG) und der Abgabenordnung (AO) identifiziert werden.

Die Übermittlung des Altersmerkmals an den Telemedien-Anbieter erfolgt unmittelbar vor jedem Zugriff auf eine geschlossene Benutzergruppe unter Verwendung der technischen Infrastruktur des giropay-Systems zur Online-Überweisung, das im gesicherten Online-Banking der teilnehmenden Bank oder Sparkasse stattfindet. Der Nutzer muss seine persönlichen Zugangsdaten zum Online-Banking eingeben und die Transaktion des Altersmerkmals zusätzlich durch Eingabe einer zur einmaligen Verwendung generierten smartTAN / mobileTAN oder durch Einsatz seiner Signaturkarte autorisieren. Gibt es für ein Konto mehrere Verfügungsberechtigte, die nicht über eigene Zugangsdaten verfügen, so wird das Altersmerkmal des jüngsten Verfügungsberechtigten mitgeteilt.

Gibt giropay dem Anbieter die Rückmeldung „volljährig“, kann der betreffende Telemedien-Anbieter unmittelbar im Anschluss daran den Zugriff auf die geschlossene Benutzergruppe freigeben.

(Entscheidung der KJM vom Oktober 2012)

➢ nach oben

SOFORT AG: „SOFORT Ident“

Bei dem Gesamtkonzept „SOFORT Ident“ der SOFORT AG für eine geschlossene Benutzergruppe erfolgt die Identifizierung in zwei Varianten: erstens durch die Überprüfung von Kontaktdaten und Geburtsdatum via Online-Banking und einem anschließenden SCHUFA-IndentitätsCheck. Zum zweiten durch die Überprüfung der genannten Daten online mittels der eID-Funktion des neuen Personalausweises.

Die erste Variante mit Online-Banking-Login und anschließendem SCHUFA-IdentitätsCheck ist als Zugangsschlüssel für den wiederholten Nutzungsvorgang vorgesehen. Auf der Ebene der Identifizierung fragt die SOFORT AG zunächst Bankleitzahl und Online-Banking-Zugangsdaten (Benutzerkennung und PIN) des Nutzers ab und überprüft diese anhand eines Abgleichs der Online-Zugangsdaten mit einem tatsächlich bei der Bank hinterlegten Namen. Im nächsten Schritt wird eine SCHUFA-Q-Bit-Abfrage durchgeführt. Dabei wird die 100-prozentige Übereinstimmung von Name, Anschrift und Alter des Nutzers mit den bei der SCHUFA hinterlegten Daten geprüft.

Bei allen weiteren Login-Vorgängen ist nur noch ein vereinfachter Identifizierungsvorgang erforderlich: Durch Eingabe der Online-Banking-Nutzerdaten und ihrer darauf folgenden Überprüfung kann ein Nutzer mittels Hash-Wert eindeutig authentifiziert werden.

Bei der zweiten Variante der Altersverifikation mit dem „neuen“ Personalausweis werden Vor- und Nachname, Anschrift sowie das Geburtsdatum online via eID-Funktion geprüft.

Damit ist neben dem Besitz des neuen Personalausweises und eines dazugehörigen Lesegerätes auch ein spezielles Wissen (um den 6-stelligen Ausweis-PIN) für die Identifizierung vonnöten. Diese Variante ist nur für einen einmaligen Login-Vorgang vorgesehen.

(Entscheidung der KJM vom September 2013)

➢ nach oben

insic GmbH: „insic AVS InJuVers“

Bei dem System „insic AVS InJuVers“ handelt es sich um ein Konzept für ein AVS, das verschiedene Möglichkeiten der Identifizierung und der Authentifizierung bietet. Auf der Stufe der Identifizierung kann der Nutzer zunächst unter verschiedenen Varianten wählen. Zur Auswahl stehen u. a. der Schufa IdentitätsCheck Premium, das E-Postident-Verfahren oder eine kamerabasierte Identifizierung per Webcam. Die Authentifizierung kann entweder über ein Mobiltelefon mit einer SMS-basierten PIN/Tan oder über die Nutzung eines Browser-Plug-Ins zur Identifizierung des PC‘s erfolgen. Im Jahre 2008 hatte die KJM bereits das Konzept „AVS InJuVers“ der insic GmbH als Konzept zur Sicherstellung einer geschlossenen Benutzergruppe positiv bewertet, das vom Anbieter um verschiedene Funktionen erweitert wurde.

Die KJM kam nach Prüfung des Konzepts „insic AVS InJuVers“ zum Ergebnis, dass es sich bei entsprechender Umsetzung als AVS-Konzept im Sinne der KJM-Kriterien zur Sicherstellung einer geschlossenen Benutzergruppe eignet. Die Positivbewertung umfasst nicht die im Antrag dargestellten Verfahren zur Datenlöschung, da die KJM keine Zuständigkeit für Fragen des Datenschutzes besitzt.

(Entscheidung der KJM vom Oktober 2015)

➢ nach oben

Deutsche Post AG: „POSTID“

Bei dem System „POSTID“ handelt es sich um ein vollständiges Konzept für ein AVS, das verschiedene Möglichkeiten der Identifizierung bietet. Die Identifizierung erfolgt zunächst über die Angabe der persönlichen Daten sowie einer E-Mail-Adresse und einer Mobilfunknummer im POSTID Portal. Anschließend kann der Nutzer aus verschiedenen Identifizierungsverfahren

wählen. Zur Auswahl stehen POSTIDENT durch Videochat, durch Filiale oder durch neuen Personalausweis. Die Authentifizierung erfolgt ebenfalls über das POSTID Portal. Dort kann der Nutzer nach erfolgter Anmeldung die an den Anbieter zur Altersprüfung zu übermittelnden Daten mittels einer ihm zugesandten Mobile-TAN freigeben.

Die KJM kam nach Prüfung des Konzepts „POSTID“ zum Ergebnis, dass es sich bei entsprechender Umsetzung als vollständiges AVS-Konzept im Sinne der KJM-Kriterien zur Sicherstellung einer geschlossenen Benutzergruppe eignet. Die Positivbewertung umfasst auch die Positivbewertung als technisches Mittel.

(Entscheidung der KJM vom Dezember 2015)

➢ nach oben

Colbette II Ltd.: „AVS AgeID“

Bei dem System „AVS AgeID“ handelt es sich um ein vollständiges Konzept für ein AVS, das verschiedene Möglichkeiten der Identifizierung und der Authentifizierung bietet. Die Identifizierung kann der Nutzer entweder direkt über eine Registrierung auf der Website des Systems vornehmen oder durch eine Registrierung auf einer Internetplattform seiner Wahl, die Inhalte im Rahmen einer geschlossenen Benutzergruppe enthält, und auf der das System AgeID.com zum Einsatz kommt. Nach Erstellung des Nutzerkontos auf einer solchen Internetplattform wird der Nutzer aufgefordert, zur Website von AgeID.com zu wechseln, um sich dort zu identifizieren. Auf der Webseite muss er dann ebenfalls einen Nutzeraccount für das System AgeID.com erstellen, indem er seine persönlichen Daten eingibt. Die dort erstellten Zugangsdaten können dann im Rahmen eines Universal-Logins genutzt werden, indem das Nutzerkonto der Internetplattform mit dem Nutzerkonto von AgeID.com verknüpft wird. Nach erfolgter Registrierung hat der Nutzer die Auswahl zwischen zwei Identifizierungsoptionen, die beide bereits von der KJM als Teillösungen für ein AVS positiv bewertet wurden.

Die Authentifizierung erfolgt entweder mittels einer App, mittels einer SMS, die an ein zuvor bestimmtes Mobiltelefon geschickt wird, oder über den Internetbrowser des Nutzers, der mit AgeID.com verbunden ist. Im Rahmen der zuletzt genannten Möglichkeit wird der Computer bzw. Internetbrowser des Nutzers mittels eines komplexen Authentifizierungssystems mit dem Nutzerkonto auf AgeID.com verbunden. Ein Login ist im Anschluss daran nur mit dem jeweiligen Endgerät und dem jeweiligen Internetbrowser möglich.

Hat der Nutzer diese Möglichkeit gewählt, muss er zwar jedes Mal die Login-Daten von AgeID.com eingeben, die Authentifizierung erfolgt jedoch automatisch. Darüber hinaus besteht die Möglichkeit, die Authentifizierung per E-Mail via Pin-Code vorzunehmen. Sollte der Nutzer von verschiedenen Internetplattformen, die das System AgeID.com nutzen, wechseln, kann er unter Einsatz seiner Daten für den AgeID.com-Universal-Login direkt auf die Inhalte der jeweiligen Internetplattformen zugreifen. Solange der Seitenwechsel im Rahmen des gewährten Zeitfensters durchgeführt wird, ist keine erneute Authentifizierung nötig. Ist der Nutzer für einen Zeitraum von mindestens 15 Minuten inaktiv oder schließt der Nutzer die jeweilige Browser-Session, so ist eine erneute Authentifizierung des Nutzers gemäß der beschriebenen Methoden nötig.

(Entscheidung der KJM vom Juni 2016)

➢ nach oben

1&1 De-Mail GmbH: „De-Mail“

Bei dem System „De-Mail“ handelt es sich um ein vollständiges Konzept für ein AVS. Die Nutzung von „De-Mail“ als AVS erfolgt durch die Integration der Funktion „mit De-Mail anmelden“ in Telemedienangeboten, die eine geschlossene Benutzergruppe erfordern. Vor der eigentlichen Identifizierung beantragt der Nutzer sein De-Mail-Postfach durch Angabe seiner persönlichen Daten und seiner Ausweisdaten. Anschließend werden diese Daten im Rahmen einer persönlichen Überprüfung von Angesicht zu Angesicht durch einen zertifizierten Prüfer eines externen Datenverarbeitungsunternehmens entweder in einem Shop („Shop Ident“) oder an einem Ort seiner Wahl („Home Ident“) verifiziert. Waren die persönlichen Daten des Nutzers korrekt, erhält dieser von der 1&1 De-Mail GmbH seine individuellen Zugangsdaten und ein Freischalt-Passwort an die hinterlegte E-Mail-Adresse. Die Freischaltung des Kontos kann nur nach der Eingabe einer mTAN erfolgen, die dem Nutzer zuvor an die hinterlegte Mobilfunknummer geschickt wurde.

Die Authentifizierung erfolgt mittels der individuellen Zugangsdaten, sowie eines weiteren Sicherungsmittels. Dabei hat der Nutzer die Wahl zwischen einer mTAN oder dem neuen Personalausweis.

Die KJM kam nach Prüfung des Konzepts „De-Mail“ zum Ergebnis, dass es sich bei entsprechender Umsetzung als vollständiges AVS-Konzept im Sinne der KJM-Kriterien zur Sicherstellung einer geschlossenen Benutzergruppe eignet.

(Entscheidung der KJM vom Oktober 2016)

➢ nach oben

AUTHADA GmbH: „AUTHADA QR“ und „AUTHADA ID“

Bei dem System „AUTHADA QR“ und „AUTHADA ID“ handelt es sich um ein vollständiges Konzept für ein AVS. Die AUTHADA GmbH bietet zwei unterschiedliche Möglichkeiten der Identifizierung und Authentifizierung an:

Die AUTHADA QR-Browser-App-Lösung („AUTHADA QR“) kombiniert die Verwendung einer App und eines klassischen Webbrowsers. Befindet sich ein Endkunde auf einer Website, deren Anbieter das AVS verwendet, öffnet sich in dem Browser ein Formular und ein QR-Code, der vom User mittels der AUTHADA-App einzuscannen ist. Alternativ öffnet der Kunde die App des jeweiligen Inhalteanbieters, in welche die AUTHADA-Software integriert ist, und scannt den QR-Code im Browser. Dem Kunden wird sodann das vom Bundesverwaltungsamt ausgestellte AUTHADA CV-Berechtigungszertifikat angezeigt. Außerdem werden ihm die Daten angezeigt, die nach Eingabe seiner eID-PIN aus der eID-Karte ausgelesen und per NFC verschlüsselt an den Produktanbieter übermittelt werden. Abschließend wird dem Kunden in der App eine TAN angezeigt, die er in das Browserfenster eingeben muss.

Bei dem Konzept „AUTHADA ID“ hingegen erfolgt der Prozess ausschließlich über die App, die vom jeweiligen Inhalteanbieter zur Verfügung gestellt wird und in die das System der AUTHADA GmbH integriert ist. Wählt der Kunde in der App das Identifizierungsverfahren der AUTHADA GmbH, wird ihm das vom Bundesverwaltungsamt ausgestellte AUTHADA CV-Berechtigungszertifikat angezeigt und wie auch in der Lösung „AUTHADA QR“ die Daten aus der eID-Karte ausgelesen und an den Produktanbieter übermittelt.

Die KJM kam nach Prüfung des Konzepts zu dem Ergebnis, dass es sich bei entsprechender Umsetzung als vollständiges AVS-Konzept im Sinne der KJM-Kriterien zur Sicherstellung einer geschlossenen Benutzergruppe eignet. Der Inhalte-Anbieter hat in eigener Verantwortung zusätzliche Sicherungspflichten (wie z. B. Backdoorschutz, Time-Out nach bestimmter Idle-Time, zeitliche Begrenzung einer Sitzung) zu implementieren.

(Entscheidung der KJM vom Dezember 2017)

➢ nach oben

WebID Solutions GmbH: „WebID DIMOCO MOBILE AVS“

Möchte ein Endkunde online Inhalte erwerben, die für Erwachsene gekennzeichnet sind, erfolgt die Identifizierung in zwei Schritten. Zunächst wird der Kunde aufgefordert, seine Handynummer mittels eines SMS-TAN-Verfahrens zu verifizieren. Der eigentliche Identifikationsprozess erfolgt anschließend unter Verwendung des Systems „WebID Identify & Age Check – Verfahren zur Identitätsprüfung und Altersverifikation“ der WebID Solutions GmbH. Dieses System hat die KJM bereits im April 2015 als eine Teillösung für eine geschlossene Benutzergruppe auf der Stufe der Identifizierung positiv bewertet. Nach erfolgreicher Identifizierung wird der Endkunde zurück auf die eigentliche Website geleitet und erhält eine TAN per SMS, um den Kauf mit der Handynummer abschließen zu können.

Hat sich der Endkunde bereits registriert und identifiziert, kann er sich mittels des „WebID DIMOCO MOBILE AVS“ für wiederholte Nutzungsvorgänge authentifizieren. Dazu findet zunächst eine Überprüfung des Geburtsdatums des Kunden sowie – wieder mittels eines SMS-TAN-Verfahrens – seiner Handynummer statt. Stimmen Nummer und Geburtsdatum überein, erhält der Kunde erneut eine TAN per SMS, mit der er den Zahlungsvorgang abschließen kann.

Die KJM kam nach Prüfung des Konzepts zu dem Ergebnis, dass es sich bei entsprechender Umsetzung als vollständiges AVS-Konzept im Sinne der KJM-Kriterien zur Sicherstellung einer geschlossenen Benutzergruppe eignet. Der Inhalte-Anbieter hat in eigener Verantwortung zusätzliche Sicherungspflichten (wie z. B. Backdoorschutz, Time-Out nach bestimmter Idle-Time, zeitliche Begrenzung einer Sitzung) zu implementieren.

(Entscheidung der KJM vom Dezember 2017)

➢ nach oben