Stellungnahme

zum Entwurf einer EU-Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

18.04.2013

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.700 Unternehmen, davon über 1.100 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

Hintergrund und Zusammenfassung

Das Internet und elektronische Prozesse werden für Konsumenten, Bürger, Unternehmen und staatliche Stellen immer wichtiger. Abläufe werden zunehmend aus Komfort- und Effizienzgründen durch Web-Technologien realisiert und in das Internet verlagert. Insbesondere rechtsverbindliche Vorgänge benötigen dabei sichere digitale Identitäten, da die Gefahr des Identitätsmissbrauchs und des Diebstahls persönlicher Daten bereits heute Realität ist. Sicherheitsexperten sind sich einig, dass in absehbarer Zeit der Zugangsschutz eines Nutzerprofils durch Nutzername und Passwort nicht mehr ausreicht. Technische Lösungen, bspw. durch die Nutzung eines zusätzlichen Sicherheitstokens, z.B. eine Smartcard, ein mobiles Endgerät oder moderne Ausweisdokumente mit Chip stehen bereits zur Verfügung und werden sukzessive im Markt etabliert. Europaweite Standards sollten zukünftig auch grenzüberschreitende Prozesse mit einem angemessenen Sicherheitsniveau ermöglichen.

Daher begrüßt BITKOM begrüßt grundsätzlich die mit dem Verordnungsentwurf zum Ausdruck gebrachte Absicht, die EU-weiten Nutzungsmöglichkeiten elektronischer Identitäten zu fördern.

Das Ziel eines einheitlichen Niveaus einer rechtssicheren und datenschutzkonformen elektronischen Kommunikation wird unterstützt. Erfolgreich werden diese Bemühungen nur sein, wenn Rechtssicherheit gewährleistet und somit Vertrauen in eine datenschutzkonforme Umsetzung bei Wirtschaft und Bürgern geschaffen wird.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Nils Hullen
Leiter Büro Brüssel
Tel. +32.2.609 53 21
Fax. +32.2.609 53 39
n.hullen@bitkom.org

Michael Barth
Bereichsleiter Verteidigung
und Öffentliche Sicherheit
Tel. +49.30.27576-102
Fax.+49.30.27576-409
m.barth@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

1. Der vorliegende Verordnungsentwurf (VO-E) stellt für verschiedene Wirtschaftsbereiche eine Gefährdung bereits getätigter und zukünftiger Investitionen dar.

Bereits heute ist absehbar, dass Cybercrime-Vorfälle wie insbesondere Identitätsdiebstahl und -missbrauch weiter zunehmen werden. In Deutschland ist von 2010 nach 2011 eine Steigerung von 16 Prozent bei den Cyberkriminalitätsfälle zu verzeichnen. Weltweit wurden im Jahr 2011 allein in den bekannt gewordenen Fällen rund 200 Mio. digitale Identitäten gestohlen. Experten gehen von ungleich höheren Zahlen durch ein großes Dunkelfeld aus.

In mehr als 20 Staaten in Europa sind derzeit elektronische Identifizierungssysteme in der Anwendung. Diese Systeme decken elektronische Dienste überwiegend im öffentlichen Bereich ab, lassen aber auch teilweise privatwirtschaftliche Anwendungen (für Banken, Handel, Versicherungen) zu. In 15 europäischen Staaten (Belgien, Deutschland, Estland, Finnland, Irland, Italien, Lettland, Norwegen, Monaco, Österreich, Portugal, Schweden, Schweiz, Spanien, Tschechische Republik) wird aus Sicherheitsgründen eine Zwei-Faktor-Authentisierung verwendet.

Staaten, die sich bereits früh mit ihren Wirtschaftsunternehmen, Ministerien und Behörden den Herausforderungen sicherer, digitaler Identitäten gestellt, ein rechtliches Rahmenwerk erstellt und entsprechende Lösungen konzipiert und eingeführt haben, werden durch den vorliegenden Verordnungsentwurf veranlasst, neu zu planen, um künftig mit verschiedenen Identifizierungs- und Sicherheitsniveaus der Mitgliedstaaten in den darauf aufsetzenden Geschäftsprozessen in Behörden und der Industrie umgehen zu können.
Eine angemessene Sicherheit sollte hier wesentliches Ziel sein. Sicherheitsmechanismen wie „Benutzername/Passwort“ sollten wie in der Einleitung des Verordnungsentwurfes erwähnt, gerade für kritische Prozesse wie die Identifizierung nicht verwendet werden. Die im EU-Projekt STORK erarbeiteten „authentication level“ können hier eine Brücke bereitstellen möglichst schnell unionsweit nur noch höhere Level zu verwenden. Der Entwurf berücksichtigt dies nur unzureichend.

2. Der Verordnungsentwurf behindert wichtige Innovationen und Investitionen durch fehlende Planungssicherheit.

Der Markt für Endgeräte sowie Angebote und Anwendungen für das mobile Internet wird sich massiv weiterentwickeln. Innovationen im Bereich von mobilen Lösungen treiben auch den Bedarf an notwendigen, innovativen Sicherheitsfunktionen und -verfahren. Eine EU Verordnung darf Innovationen in diese wichtigen Sicherheitsfunktionen nicht behindern.

Derzeit behält sich die EU-Kommission in ihrem Vorschlag zu den meisten Themen Gestaltungsfreiheit in Form „delegierter Rechtsakte“ vor. Weiterhin sind einige Artikel des Vorschlages derzeit nicht präzise formuliert und eröffnen Interpretationsspielräume.
Die daraus resultierende Unsicherheit führt zu Investitionspausen bis das rechtliche Umfeld hinreichend geklärt ist.

Neben den oben angeführten Mitgliedsstaaten, haben weitere EU-Mitgliedsstaaten und/oder Beitrittskandidaten nationale eID Programme angekündigt. Dies sind beispielsweise Polen, Ungarn, Slowenien, Rumänien, Kroatien, Norwegen und Frankreich. Obwohl sich - wie bereits dargestellt - die Bedrohungslage verschärft und damit der Bedarf nach sichereren Lösungen zum Schutz digitaler Identitäten steigt, steht zu befürchten, dass diese Programme nun durch die Planungsunsicherheiten im Rahmen des EU Verordnungsentwurfes ausgesetzt oder verschoben werden. Es ist hier dringend geboten, Klarheit in den einzelnen Aspekten, wie angemessene Sicherheitsstandards für Vertrauensdienste-Anbieter, für Behörden und für die Industrie zu schaffen.

In dem EU Verordnungsentwurf sind einheitliche angemessene Sicherheitsstandards z. B. für Vertrauensdienste-Anbieter und Identifizierungsdienste nicht hinreichend geregelt. Vielmehr sollen diese durch die Kommission mittels Durchführungsrechtsakten nachträglich festgelegt werden. (z. B. Art 15, Abs 6, Art. 17, Abs. 5, Art. 19, Abs. 5, Art 38). Des Weiteren sind weder der Zeitplan, noch die Inhalte derzeit abschätzbar. Da der Verordnungsentwurf bisher auch keinen inhaltlichen Rahmen für diese Durchführungsrechtsakte setzt.

Für die Trust-Services-Provider- und für die Identitäten-Provider-Industrie erzeugt diese Vorgehensweise große wirtschaftliche Unsicherheiten, da notwendige Geschäftsplanungen nicht durchgeführt werden können. Die gleiche Unsicherheit trifft auch die Anwender, also Behörden, Industrie und Bürger.
Im Detail hat dies zur Konsequenz: Jede nachträgliche Festlegung zu technischen Anforderungen und Normen an Vertrauensdienste-Anbieter, jede nachträgliche Festlegung von Prüfungsform und –verfahren von noch festzulegenden Aufsichtsstellen können Zusatz-Investitionen in Einrichtungen, in Personen, in Prozesse und in Dokumentationen erforderlich machen, die nicht unmittelbar an den Nutzer von elektronischen Diensten weitergereicht werden können. Weder notwendige Maßnahmen noch mögliche Umsetzungstermine lassen sich aus dem vorliegenden EU Verordnungsentwurf ableiten. Daher wird empfohlen, die Artikel 16, 17 und 19 deutlich zu präzisieren.
Die in dem Verordnungsentwurf angestrebte gegenseitige Anerkennung und Interoperabilität von Sicherheitsverfahren zwischen den Entitäten verschiedener Staaten, in denen auch jetzt schon heterogene Lösungen im Betrieb sind, dürften ohne ein gemeinsames Rahmenwerk und standardisierte Normen zu Security kaum zu erreichen sein. Um z. B. jede Form eines Zugangsprozesses bedienen zu können, müsste eine Behörde oder ein Unternehmen eine Vielzahl von Zugangsverfahren vorhalten, die Auswirkungen der verschiedenen Sicherheitsniveaus in die folgenden Geschäftsprozesse einarbeiten und entsprechende Kosten für Implementierung und Betrieb tragen. Die in der Verordnung geplanten Durchführungsakte müssen deshalb zumindest auf bestehende (offene und proprietäre) Standards und erprobte Lösungen, die in angemessenes Sicherheitsniveau bieten, aufsetzen, um den Marktzugang und die Wettbewerbsfähigkeit der Unternehmen nicht zu behindern.

Der EU Verordnungsentwurf legt für Vertrauensdienste-Anbieter weder Mindestversicherungssummen noch Haftungsobergrenzen fest. Dies sollte sowohl zum Schutz von Verbrauchern als auch zum Schutz von Anbietern erfolgen.

Die Rolle von sognannten 'beauftragten Dritten', die im Auftrag von Vertrauensdienste-Anbietern Aufgaben übernehmen, ist nicht umfassend geregelt. Dies sollte in der EU Verordnung präzisiert werden. Auch für beauftrage Dritte sollten Haftungsobergrenzen gelten.

Verschiedene Mitgliedsstaaten betreiben bereits Identifikationssysteme, die auf völlig unterschiedlichen Philosophien basieren. Diese elektronischen Identifikationssysteme haben alle unterschiedliche Sicherheitsmechanismen für die Identifikation und Authentisierung (gegenseitige Authentisierung, Zugangsmechanismen, Verschlüsselung etc.) und enthalten unterschiedliche Datensätze bzw. –formate des Nutzers. Somit sind allerdings ***erhebliche Vorinvestitionen*** angezeigt, die zunächst in keiner Wirtschaftlichkeitsbetrachtung bewertet werden können. In Staaten mit hohen EU-Ausländerzahlen, wie Deutschland werden somit 27 oder mehr zu unterstützende elektronische Identifikationssysteme von Vertrauensdienste-Anbieter zu berücksichtigen sein.
Der Verordnungsentwurf zeigt hier keinen Weg auf, obwohl in EU-Projekten wie ICT LSP STORK, mit Beteiligung der meisten EU-Staaten, bereits Lösungen für diese Problematik entwickelt wurden.

3. Im Verordnungsentwurf werden bewährte, bestehende Standards sowie die Formulierung eines notwendigen angemessenen Sicherheitsniveaus nicht berücksichtigt.

Die EU-Mitglieder benötigen in der Tat eine EU-weite technische Verifikationsmöglichkeit ihrer eID- und eSignatur-Werkzeuge, welche lediglich durch die gegenseitige rechtliche Anerkennung heterogener IT-Systeme nicht zu erreichen ist. Eine gegenseitige Anerkennung ohne definierte und vergleichbare Sicherheitsniveaus fördert aus betriebswirtschaftlichen Gründen die Tendenz zum kleinsten gemeinsamen Nenner, was die so wichtige Innovationskraft bei dem Thema nachhaltig hemmt.

Angemessene Sicherheitsanforderungen werden im aktuellen Entwurf bisher nicht berücksichtigt. Dies sollte aus zwei Gründen verbessert werden: erstens ist eine vergleichbare, wirtschaftliche Bewertung von Identitätssystemen ohne feste Sicherheitsparameter nicht möglich. Zweitens stellt das Fehlen von angemessenen Sicherheitsstandards auch eine Gefahr für die Interoperabilität der verschiedenen Systeme dar.

Identitätsdefinitionen wie von ENISA definierten ‚IDABC authentication level', die in EU-Projekten wie STORK bereits verwendet werden, sollten in der EU Verordnung benannt werden. Eine Festlegung auf AAL3 oder besser AAL4 wären aus Sicht der Akzeptanz durch die EU-Bürger begrüßenswert. Sicherheitsanforderungen die Produkte betreffen, sollten auf Basis der international harmonisierten Common Criteria definiert werden.

4. Der Verordnungsentwurf muss das Ziel der Förderung von Akzeptanz gegenüber elektronischen Identitäten bei Behörden, Industrie und Bürger berücksichtigen.

i. Personenzuordnung zu Identifikationsdaten im Zusammenspiel mit Grundprinzipien des Datenschutzes

Der Entwurf der EU-Verordnung berücksichtigt ab Kapitel III (Vertrauensdienste) Belange des Datenschutzes. Im Kapitel II (Identifizierung) sind diese Belange bisher nicht abgebildet, obwohl hier Bürger und Wirtschaft erheblich empfindlicher reagieren. Dies ist sicherlich der Neuheit der Thematik geschuldet. Anforderungen des „Privacy by Design“, also die Zweckbindung der Daten zur Erreichung von Datensparsamkeit und Datenvermeidung, finden sich bisher in keiner Weise in diesem Anforderungsteil.

Es muss beispielsweise möglich sein, eine bedarfsgerechte Steuerung der zu übertragenen persönlichen Daten zu implementieren, also nur die benötigten Daten zu übertragen.

Häufig wird in sozialen Netzen oder für Zugangslösungen in der Industrie bzw. Banken ein ***Pseudonym*** anstelle des Namens verwendet. Das ist eine im Sinne des Datenschutzes und insbesondere der Datensparsamkeit sehr zu begrüßende und zu fördernde Funktion. Der EU Verordnungsentwurf lässt diese Funktion für die Identifizierung nicht zu (siehe Art. 6, Absatz c). Der vorliegende EU Verordnungsentwurf wird in diesem Punkt als unzureichend bewertet.

Manche Dienste im Internet benötigen nur eine ***Altersverifikation*** z.B. zum Zwecke des Jugendschutzes. Dabei wird nicht das Geburtsdatum übertragen, sondern nur das Erreichen des geforderten Alters des Nutzers. Zum Herunterladen z.B. von Spielen, Programmen, neuen Software-Versionen sind zudem die Übermittlung von Name oder Adresse nicht erforderlich. Zum Zwecke der Datensparsamkeit sollten derartige ***anonymisiert*** Dienste in der EU Verordnung berücksichtigt werden (Ergänzung zu Art. 6, Absatz c). Dazu zählen u.a. auch elektronische Wahlen, sofern diese rechtlich zulässig sind.

Der EU Verordnungsentwurf stellt aus Industriesicht im Kapitel II eine zu starke Einschränkung dar, die pseudonyme und anonyme Anwendungen sowie Alters- und Wohnortverifikationen werden nicht berücksichtigt. Aus Datenschutzgründen sollten diese Optionen zur Datensparsamkeit Berücksichtigung finden. Mehrere Identitäten bzw. Rollen sollten zulässig sein.

ii. Verständliches Rahmenwerk

Für viele Nutzer ist es sehr wichtig, seine Kommunikationspartner zu kennen. Insbesondere wenn persönliche Daten von ihm verlangt werden ist ein Teil der Nutzer sehr sensibel, andere Teile jedoch nicht.
Ein System, welches mit personenbezogenen Daten umgeht, sollte für ALLE Nutzergruppen gleichermaßen geeignet sein. Internet-Betrügern sollte ihr Handeln möglichst schwer gemacht werden.
Zu beachten ist hier, dass ein nationales oder EU-weites System für Identitätsmanagement eine möglichst starke Vertrauensstellung bei allen beteiligen Gruppen und auch in den Medien haben sollte.

Besonderes Augenmerk verdient hier die gegenseitige Identifizierung, insbesondere wenn Dritte in der Kommunikation beteiligt sein, was im Internet als Normalfall einzuschätzen ist.
Nur wenn alle Beteiligte wissen, mit wem sie sicher kommunizieren, wird ein System mit dem vertrauliche Daten transportiert werden, auf Dauer akzeptiert.

Die Einführung von qualifizierten Website-Zertifikaten im §37 des Entwurfs könnte das Sicherheitsbedürfnis von Bürgern und Wirtschaft zu erfüllen, sie müssten jedoch für den Abruf von personenbezogenen Daten immer vorgeschrieben sein.
In der jetzigen Form erfüllen diese Zertifikate keinen Zweck, da lediglich die Anerkennung durch die Mitgliedsstaaten vorgeschrieben wird, in der Realität funktionieren solche Zertifikate nur über die Nutzung durch den Anbieter, beispielsweise beim Online-Shopping.

iii. Einheitlicher Datensatz

Für eine Kommunikation über Ländergrenzen hinweg, muss ein Datensatz der personenbezogenen Daten definiert sein, der für wesentliche Geschäftsprozesse in allen Mitgliedsstaaten verwendbar ist. Bisher geht der Entwurf nicht auf diese Daten ein.
Jeder Prozess erfordert bestimmte Daten. Die meisten Behördenprozesse beispielsweise Vorname, Name. Einige Prozesse benötigen jedoch auch einen Geburtsnamen.

Es können jedoch auch aus Datenschutzgründen, beispielsweise bei Nutzung in der Wirtschaft, zu viele Daten enthalten sein.
Beispielsweise kann ein Personendatensatz eine Sozialversicherungsnummer oder Ähnliches enthalten. Somit kann dieses Identitätsmittel in Deutschland für viele Prozesse aus rechtlichen Gründen nicht verwendet werden.
Für die Akzeptanz der Nutzer und unionsweiten Einsatzmöglichkeiten sollte ein Datensatz definiert sein, der den Beteiligten Rechtsicherheit und Vertrauen verschafft.

5. Die Regelung zu Übergangsfristen im Verordnungsentwurf muss überdacht werden

Da die technischen und organisatorischen Anforderungen erst in delegierten Rechtsakten und Durchführungsrechtsakten festgelegt werden, ist eine Festlegung des Inkrafttretens der Regelungen der Verordnung relativ zum Veröffentlichungsdatum der Verordnung problematisch. Die Umsetzungsfrist muss sich vielmehr an der Veröffentlichung der delegierten Akte orientieren, da erst zu diesem Zeitpunkt die umzusetzenden Anforderungen bekannt und geregelt sind.

Die Anforderungen an die Betreiber von Vertrauensdiensten greifen ggfs. tief in die Sicherheitskonzeption bzw. die Konzeption der Geschäftsprozesse der Betreiber ein. Daher sollte der Umsetzungsaufwand, sowohl zeitlich als auch finanziell, nicht unterschätzt werden. Zwar sieht der Kommissionsvorschlag eine Übergangsfrist für bereits ausgegebene qualifizierte Zertifikate und Signaturerstellungseinheiten vor (Artikel 41), eine Übergangsfrist für die Betreiber von

Vertrauensdiensten ist aber nicht vorgesehen, sodass die Anforderungen 20 Tage nach Veröffentlichung der Verordnung umgesetzt sein müssen (Artikel 42).

Im Bereich der Vertrauensdienste sollte für die Umsetzung der technischen und organisatorischen Anforderungen ein Zeitraum von wenigstens einem Jahr ab Veröffentlichung der vollständigen Vorgaben vorgesehen werden, nicht wie bisher im Vorschlag niedergelegt 20 Tage ab Veröffentlichung der Verordnung.

Im Bereich der elektronischen Identitäten sind keine Übergangsfristen vorgesehen. 6 Monate nach Inkrafttreten der Verordnung soll die Kommission die Liste notifizierter eIDs erstmals veröffentlichen (Artikel 7 (2)). Da die Verordnung lediglich Rahmenbedingungen für die Notifizierung vorgibt, ist die konkrete Ausgestaltung (im Rahmen der Vorgaben für die Notifizierung und der delegierten Akte/Durchführungsrechtsakte) weiterhin nationale Zuständigkeit. Ggfs. ist daher eine Anpassung nationalen Rechts nach Inkrafttreten der Verordnung bzw. Veröffentlichung der delegierten Akte notwendig, bevor eine nationale eID notifiziert werden kann.

Eine Rechtssetzung im sensiblen Bereich der Verarbeitung personenbezogener Daten sollte mit der gebotenen Sorgfalt erfolgen. Um eine Wettbewerbsverzerrung in dieser Anpassungsphase zu vermeiden, sollte die Liste notifizierter eIDs durch die Kommission erst nach einer angemessenen Übergangsfrist erstmalig veröffentlicht werden. Diese Frist sollte so bemessen sein, dass alle nationalen eIDs sowohl rechtlich als auch technisch/organisatorisch an die Vorgaben der Verordnung vor Erstveröffentlichung angepasst werden können. Eine solche Frist könnte -- abhängig von den notwendigen Anpassungen -- zwei Jahre betragen.

Einzelne Artikel:

1) **Art 2 (2) Anwendungsbereich**

Der Absatz ist unklar formuliert. Die in diesem Artikel angeführten „freiwilligen privatrechtlichen Vereinbarungen“ treffen zunächst auf die überwiegende Anzahl der deutschen ZDA zu. Eine Zurechnung zu der mit diesem Verordnungsentwurf adressierten Gruppe muss über komplizierte Ableitungen und Interpretationen erfolgen und ist somit klärungsbedürftig.
Es ist somit nicht klar, ob ein privatwirtschaftlicher Dienst, der Identifizierungsdaten mit Hilfe eines staatlichen Identifizierungssystems wie der nationalen ID-Karte erhebt und diese Daten für ein eigenes zum Teil auch gesetzlich reguliertes Identifizierungssystem nutzt, unter Absatz (1) oder (2) fällt, da in den nachfolgenden Begriffsbestimmungen in Art 3 diese Frage noch verstärkt wird. Grundsätzlich sind hier die meisten europäischen Postdienste betroffen.

2) **Art 3 (30) i.V.m. Art 37 Definition qualifiziertes Zertifikat für die Websiteauthentifizierung**

Es wird leider aus dem Verordnungsentwurf nicht klar, welchen Zweck diese Art von Zertifikaten neben den heute üblichen in den Browsern hinterlegten SSL-Zertifikaten haben könnte. Anbieter von SSL-Zertifikaten müssen für die Auf-

nahme in die Browserlisten, Webtrust oder ETSI-Zertifizierungen bestehen und werden anschließend durch den Browser als sicher angezeigt.

Qualifizierte Zertifikate für die Websiteauthentifizierung erfüllen diese Anforderung zunächst nicht. Sie werden so nur genauso wie andere, auch außereuropäische Zertifikate nach Durchführung der Zertifizierung in die Browser aufgenommen.

Eine gegenseitige Authentifizierung (wie beispielsweise an der Hotelrezeption) stellt für den Bürger zweifelsfrei dar, wer seine personenbezogenen Daten abfragt und stellt somit die Voraussetzung für einen selbstbestimmten, vertrauensvollen Umgang mit den eigenen Daten dar.

Daher könnte die Verwendung dieser neuen Zertifikate generell für den Abruf von personenbezogenen Daten mittels der notifizierten Identifizierungssysteme analog der deutschen Berechtigungszertifikate verpflichtend eingeführt werden.

Eine solche Maßnahme gibt Bürgern die Möglichkeit zu prüfen, wer ihre personenbezogenen Daten abrufen möchte und eröffnet so auch die Möglichkeit Daten- und Verbraucherschutzanforderungen durchzusetzen. Daher sollte die Beschränkung auf Websiteauthentifizierung entfallen und generell auf Webservice-Anbieter, die ein notifiziertes Identifikationssystem verwenden, erweitert werden.
Eine mögliche Weiterführung wäre die Verpflichtung aller Webdienste, zum technischen Datenschutz der personenbezogenen Daten ihrer Nutzer.

Die konkrete technische Ausgestaltung (X.509, CV) sollte national geregelt werden und zum Identifizierungsdienst passen.

3) Art 5 Gegenseitige Anerkennung und Akzeptierung i.V.m. Art 6 Bedingungen für die Notifizierung

Über die gegenseitige Anerkennung und Akzeptanz wird der heutige, in einigen Bereichen problematische Zustand fehlender EU-Vorgaben bezüglich der angemessenen Sicherheitsanforderungen an ID-Systeme der Mitgliedsstaaten in die Zukunft fortgeschrieben. Auch wenn es zu erwarten ist, dass EU-Mitgliedsstaaten aus Eigeninteresse (z.B. Haftung oder Schwarzgeld- und Terrorismusbekämpfung) selbst einen heute üblichen Sicherheitsstandard bei der Entwicklung von eID-Systemen für ihre Länder zu Grunde legen, wäre eine Vorgabe sehr zu begrüßen.
Der besondere Bedarf von angemessenen Sicherheitsstandards leitet sich bei Online-Geschäften aus der fehlenden persönlichen Präsens ab, da hier psychologische Missbrauchshürden fehlen. Gerade die Nutzung der nationalen Identifizierungssysteme im Bereich der Schwarzgeldbekämpfung stellt hier besondere Anforderungen an die Sicherheit.
Die Klärung der Haftungsfrage ist aus Sicht des Bitkom ein begrüßenswerter Schritt.

4) Art. 6 I d) Zwang zur Kostenfreiheit von Authentifizierungsmöglichkeiten

In diesem Artikel wird die die Notifizierung von nationalen Systemen von einer kostenlosen Authentifizierungsmöglichkeit abhängig gemacht. Falls privatwirtschaftliche Dienste wie unter ‚1) Art 2 (2) Anwendungsbereich' beschrieben, unter diese Verordnung fallen, entsteht somit ein Problem für anbietende Unternehmen.

Für einen Authentifizierungsprozess entstehen jedoch Kosten. Wenn das Unternehmen zu einer Kostenfreiheit gezwungen ist, sinkt jedoch die Bereitschaft, einen solchen Dienst überhaupt anzubieten.

Falls es Gründe geben sollte, die zu dieser äußerst kontraproduktiven Regelung geführt haben, sollte für diese streng geprüft werden, ob eine strikte Preisregulierung wirklich notwendig ist und auf welche Anwendungsfälle dies begrenzt werden muss.
Die bestehende Regelung führt jedoch je nach Auslegung des Anwendungsbereiches zu einem unkalkulierbaren Kostenrisiko für anbietende Unternehmen, was dazu führen würde, dass nationale Systeme möglicherweise gar nicht notifiziert werden.
Dadurch wäre der gesamte Bereich der Identifizierungsdienste komplett ausgehebelt.

5) Art 8 Koordinierung

Die bloße Vorschrift zur Koordinierung ist aus derzeitiger Sicht nicht ausreichend. Hier wäre es begrüßenswert, eine Stelle z. B. ENISA zu benennen, die diese Koordinierung vorantreibt.

6) Art 9 Haftung

Die Begrenzung der Haftung für Vertrauensdienste auf fahrlässig verursachte Schäden gleicht die Haftungsanforderungen für Vertrauensdienste-Anbieter an die allgemeine Lebenspraxis in Deutschland an und ist somit als Fortschritt anzusehen, es sollte hier eine konkrete Mindestversicherungsumme EU-weit definiert werden um gleiche Voraussetzungen im Wettbewerb zu schaffen.

7) Art 17 Beginn der Erbringung qualifizierter Vertrauensdienste

Die Erklärung, das ausgestellte Zertifikate im Sinne des Art 20 (2) dieselbe Rechtswirkung wie eine handschriftliche Unterschrift haben und nach Art 20 (4) auch unionsweit akzeptiert werden müssen, sobald der qualifizierte Vertrauensdienst seine Tätigkeit angezeigt hat, stellt an die Validierung qualifizierter Zertifikate große Anforderungen, da die validierende Stelle nicht notwendigerweise Zugang zu allen eingegangenen Anzeigen innerhalb der Union haben kann, falls hier zu Zeitverzögerungen bei der Übermittlung der Vertrauenslisten an die Kommission kommt. Es entsteht hier ein kurzes Zeitfenster in dem nicht zuverlässig validiert werden kann. Somit kann der Empfänger (validierende Stelle) nicht sicher feststellen, ob es sich überhaupt um einen qualifizierten Vertrauensdienst innerhalb der Europäischen Union handelt. Die Rechtswirkung sollte

somit von der Veröffentlichung in den Vertrauenslisten abhängig sein und nicht von der Anzeige.

8) Art 19 Anforderungen an qualifizierte Vertrauensdienste

Der EU Verordnungsentwurf Art 19 legt für Vertrauensdienste-Anbieter weder Mindestversicherungssummen noch Haftungsobergrenzen fest. Dies sollte sowohl zum Schutz von Verbrauchern als auch zum Schutz von Anbietern erfolgen.

9) Art 19 (2) g) Anforderungen an qualifizierte Vertrauensdienste

Die Aufzeichnung von einschlägigen Informationen ist sinnvoll, jedoch unscharf formuliert. Hier sollten die mindestens aufzuzeichnenden Informationen benannt werden, da ein Gerichtsverfahren nicht notwendigerweise im Land des Vertrauensdienstes stattfinden muss. Dahinter steht die Frage, wie kann beispielsweise nach 10 Jahren festgestellt werden, welche Person hinter einem Zertifikat steht? Ebenso sollte es ein Unionsweit gleiches Verfahren für die Aufbewahrung von diesen Informationen nach Beendigung eines qualifizierten Vertrauensdienstes geben (beispielsweise Übergabe an Aufsichtsstelle etc).

10) Art 22 Anforderungen an qualifizierte Signaturerstellungseinheiten

Es wäre sehr hilfreich gewesen, mindestens im erläuternden Kommentar zum Verordnungsentwurf auf Normen wie prEN 14169 und EN 14890 hinzuweisen.

11) Art 38 Befugnisübertragung

Die Kommission darf für die meisten Artikel 'delegierte Rechtsakte' veröffentlichen. D.h. die getroffenen Regelungen sind nicht starr, sondern können ständig durch neue Regelungen geändert werden. Die Auswirkungen auf ausgegebene Produkte, Produkte im Lager der Hersteller oder Produkte in Entwicklung sind unklar. S. dazu auch DIN Kommentar 8 sowie DIN Kommentar 2

12) Anhang II Anforderungen an qualifizierte Signaturerstellungseinheiten

Die Anforderungen in Anhang II sind ähnlich zu den Anforderungen aus Annex III der EU Direktive 1999/93/EG. Dort werden allerdings keine Mindestanforderungen hinsichtlich Sicherheitsevaluierungen oder Algorithmen festgelegt. Dies wurde bisher durch die nationale Gesetzgebung getan, was nun gemäß Punkt (15) des EU Verordnungsentwurfes nicht mehr möglich ist. Dies kann die Reduzierung des Sicherheitsniveaus von sicheren Signaturerstellungseinheiten zur Folge haben. vgl. dazu auch DIN Kommentar 9.

13) Anhang IV Anforderungen an qualifizierte Zertifikate für Website-Authentifizierung

Die Nutzer von qualifizierten Zertifikaten für die Website-Authentifizierung werden im Gegensatz zu (b), in (c..e) auf juristische Personen eingeschränkt. Hier liegt sicherlich ein editorischer Fehler vor.

Anhang –
Kommentare aus den Arbeitsgremien des DIN e.V.

Das DIN Deutsches Institut für Normung e. V. ist privatwirtschaftlich organisiert mit dem rechtlichen Status eines gemeinnützigen Vereins. Die Mitglieder des DIN sind Unternehmen, Verbände, Behörden und andere Institutionen aus Industrie, Handel, Handwerk und Wissenschaft.
Hierfür bringen rund 28.000 Expertinnen und Experten ihr Fachwissen in die Normungsarbeit ein. Das DIN ist laut eines Vertrages mit der Bundesrepublik Deutschland die zuständige deutsche Normungsorganisation für die europäischen und internationalen Normungsaktivitäten.

Anmerkung: Da es sich um den Entwurf für eine EU Verordnung handelt, bedeutet das, dass diese Verordnung in allen Ländern unmittelbar gilt, sobald sie in Kraft tritt. Da EU Recht höher zu bewerten ist als nationales Recht, kann man durchaus davon sprechen, dass damit betroffene nationale Gesetze und Verordnungen wie das Deutsche Signaturgesetz und die Deutsche Signaturverordnung ‚ersetzt werden' (s. auch Kap. 3 des Entwurfs).

1.) Punkte (21): Technologieneutralität. Das könnte den Stand der Signaturkarte als Smartcard schwächen.

2.) Punkte (49). Die Kommission soll die Befugnis erhalten Rechtsakte zu verschiedenen Aspekten zu erlassen. Es ist unklar, welche Modalitäten erfüllt sein müssen, um Rechtsakte zu erlassen (einfache Mehrheit, Einstimmigkeit, ...). Siehe dazu auch Kommentar zu Artikel 38 unter Nummer 8.

3.) Punkt (15) des Entwurfes ist unklar. "Dies schließt besondere nationale technische Vorschriften aus, wonach ausländische Beteiligte beispielsweise eine bestimmte Hardware oder Software zur Überprüfung oder Validierung der notifizierten elektronischen Identifizierung beschaffen müssten". Welche Auswirkung hat das auf die Gültigkeit/Anwendbarkeit Technischer Richtlinien (z.B. BSI), Algorithmenkataloge (BNetzA, BSI), die Vorschrift bestimmte Kartenleser für die Signaturerstellung verwenden zu müssen ('Komfortleser'), etc.?

4.) Artikel 15: Ein Sicherheitskonzept für Vertrauensdienste-Anbieter scheint nicht verpflichtend notwendig zu sein. Das könnte zu einer Reduzierung der Sicherheitsstandards bei Vertrauensdienste-Anbietern im Vergleich zum jetzigen Stand in Deutschland führen.

5.) Artikel 19: Es scheinen weder Mindestversicherungsgrenzen noch Haftungsgrenzen für Vertrauensdienste-Anbieter definiert zu sein. Die Haftung wird typischerweise auch an beauftragte Dritte weitergeben. Das kann eine unlimitierte Haftung für einen Kartenhersteller bedeuten.

6.) Artikel 20: Gemäß (17) soll der Anwendungsbereich so eingeschränkt sein, dass Gesetze mit expliziten Formvorschriften ausgenommen sind (z.B. Testament). Das findet sich aber in Artikel 20 nicht wieder.

7.) Artikel 23: Eine Bestätigung ('Zertifizierung') gemäß den Signaturvorgaben scheint nach wie vor optional möglich zu sein, ist aber nicht verpflichtend. Ge-

mäß Punkt (15) des EU Verordnungsentwurfes darf aber kein Staat so eine Zertifizierung verpflichtend fordern.

8.) Artikel 38: Die Kommission darf für die meisten Artikel 'delegierte Rechtsakte' veröffentlichen. D.h. die getroffenen Regelungen sind nicht starr, sondern können ständig durch neue Regelungen geändert werden. Die Auswirkungen auf ausgegebene Produkte, Produkte im Lager der Hersteller oder Produkte in Entwicklung sind unklar.
Die Zusammensetzung und vor allen Dingen die Voraussetzungen für den Erlass eines Rechtsaktes ist unklar (einfache Mehrheit, Einstimmigkeit, etc. s. dazu auch Kommentar zu Punkt (49) oben).

9.) Anhang II: Anforderungen an qualifizierte Signaturerstellungseinheiten: Im Prinzip hat sich an den Anforderungen wenig geändert. Es wird allerdings keine verpflichtende Sicherheitsevaluierung gefordert (s. dazu auch Artikel 23). Bei der EU Direktive 1999/93/EG Annex III gab es ebenfalls keine konkrete Anforderung nach einer Sicherheitsevaluierung, die veröffentlichten Normen (im Speziellen prEN14169) haben das aber nahegelegt. Es gibt keinen Verweis auf einen Algorithmenkatalog. Diese Aspekte wurden bisher durch die nationale Gesetzgebung geregelt. Gemäß Punkt (15) des EU Verordnungsentwurfes wird das künftig aber nicht mehr möglich sein, was eine Reduzierung des Sicherheitsniveaus im Vergleich zum Stand heute in Deutschland zur Folge haben könnte.

10.) Die Rolle von beauftragten Dritten für Vertrauensdiensteanbieter wird explizit nur für den Akt der Registrierung diskutiert. Es ist daher unklar, ob Kartenhersteller als beauftragte Dritte Dienste wie zum Beispiel Schlüsselgenerierung auf der Karte durchführen dürfen oder nicht. Dies könnte eine Einschränkung der Wertschöpfungskette von Kartenherstellern darstellen.

11.) Ergebnis: Es scheint als wären durch die neue Verordnung die formalen Mindestanforderungen an sichere Signaturerstellungseinheiten signifikant reduziert werden (eine Sicherheitsevaluierung wird nicht verpflichtend gefordert; es werden keine Algorithmenkataloge und technischen Richtlinien referenziert, die eingehalten werden müssen und die Regelung über nationale Gesetzgebung erscheint durch Punkt (15) des EU Verordnungsentwurfes nicht mehr möglich; es gibt allerdings eine Referenz auf Normen, die im EU Amtsblatt veröffentlicht werden können, s. Artikel 22).