Alexander Roßnagel, Gerrit Hornung, Michael Knopp, Daniel Wilke*

De-Mail und Bürgerportale

Eine Infrastruktur für Kommunikationssicherheit

Trotz der wachsenden Bedeutung des Internet für die Kommunikation zwischen Bürgern, Behörden und Unternehmen sind die Sicherheit, Vertraulichkeit und Rechtsverbindlichkeit des elektronischen Rechts- und Geschäftsverkehrs bislang nicht gewährleistet. Die geplanten Bürgerportale sind ein wichtiges Instrument zur Lösung der bestehenden Probleme.

Prof. Dr. Alexander Roßnagel

Vizepräsident der Universität Kassel, Univ.-Prof. für Öffentliches Recht, Leiter der „Projektgruppe verfassungsverträgliche Technikgestaltung (provet)" und Wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR), Saarbrücken
E-Mail: a.rossnagel@uni-kassel.de

Dr. Gerrit Hornung, LL.M.

Geschäftsführer von provet und Wissenschaftlicher Mitarbeiter an der Universität Kassel
E-Mail: gerrit.hornung@uni-kassel.de

Michael Knopp

Ass. iur., Wissenschaftlicher Mitarbeiter der „Projektgruppe verfassungsrechtliche Technikgestaltung (provet)".
E-Mail: michaelknopp@uni-kassel.de

Daniel Wilke, LL.M

Wissenschaftlicher Mitarbeiter der „Projektgruppe verfassungsrechtliche Technikgestaltung (provet)".
E-Mail: d.wilke@uni-kassel.de

1 Unsicheres Internet

Das Internet verdankt seinen extremen Erfolg seinem Konstruktionsprinzip „Keep it Simple and Stupid" (KISS). Es ermöglicht grundsätzlich jedem, am Internet teilzunehmen und mit jedem anderen weltweit zu kommunizieren. Die Kehrseite sind eine Reihe von Defiziten, die es erschweren oder unmöglich machen, bestimmte Formen der Kommunikation von analogen Medien auf das Internet zu übertragen. Niemand weiß sicher, wer sein wirklicher Kommunikationspartner ist. Im Internet kann jeder prinzipiell jede Identität annehmen. Eine verlässliche Zuordnung von Handlungen zu ihrem Urheber ist nicht möglich. Daher kann man nicht sicher sein, ob man eine Nachricht einer bestimmten Person auch sicher und vertraulich zuzustellen kann. Umgekehrt kann auch niemand sicher sein, dass er alle an ihn gerichteten Nachrichten auch tatsächlich – ungelesen, unkopiert und unverändert – empfängt.

Das Internet böte für viele Unternehmen, Ämter, Dienstleister und auch Privatpersonen einige Möglichkeiten, ihre Arbeitsabläufe zu unterstützen, die Erfüllung ihrer Aufgaben zu erleichtern und ihr Handeln effektiver zu gestalten – wenn diese Unsicherheiten nicht wären. So darf etwa ein Arzt Patientendaten oder ein Anwalt Mandantendaten[1] nur über das Internet versenden, wenn er sicher sein kann, dass sie auch tatsächlich bei dem berechtigten Empfänger ankommen. Ämter oder Unternehmen dürfen häufig den Zugang zu bestimmten Daten oder den Abruf von Informationen nur erlauben, wenn sie vorher prüfen konnten, ob der Zugriff durch eine berechtigte Person erfolgt. Viele Bürger vertrauen rechtlich bedeutsame Erklärungen dem Internet nur an, wenn sie sicher sein können, dass sie rechtzeitig und unversehrt beim richtigen Empfänger ankommen. Willenserklärungen werden erst mit Zugang wirksam. Er muss in vielen Fällen nachgewiesen werden können. Da die erforderliche Sicherheit oder Gewissheit im Internet fehlt, wäre es eine Verletzung von Berufspflichten, von gesetzlichen Vorgaben oder der gebotenen Vorsicht, das Internet zu nutzen.[2] Dadurch bleiben aber viele Chancen, die das Internet bietet, ungenutzt.

* Die Autoren haben die Studie „Rechtsfragen" des Projekts Bürgerportale für das Bundesministerium des Innern bearbeitet und einen Gesetzentwurf entwickelt, der in den Entwurf der Bundesregierung mündete.

Siehe zu den Problemen etwa Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, 2000; Goetz, Online-Sicherheit von Patientendaten, 2001; zu den damit verbundenen Rechtsfragen der elektronischen Gesundheitskarte Hornung, Die digitale Identität, 2005, 208 ff., 247 ff., 363 ff. et passim.

1 Zum Datenschutz in der Beziehung zwischen Anwalt und Mandaten siehe mit unterschiedlichen Akzenten einerseits Weichert, NJW 2009, 550 ff.; andererseits Redeker, NJW 2009, 554 ff.

2 So auch Werner/Wegener, CR 2009, 310.

2 Anforderungen an eine sichere Internetkommunikation

Daher wäre es hilfreich, wenn im Internet neben den einfachen, meist kostenlosen, aber unsicheren Diensten auch Dienste angeboten würden, die – mit vertretbaren Vorleistungen und auch vertretbaren Kosten – die erforderliche Sicherheit und Vertrauenswürdigkeit böten und bei Bedarf jederzeit genutzt werden könnten. Manche Unsicherheiten können durch zusätzlichen individuellen Aufwand kompensiert werden – etwa indem man nach vorherigem Schlüsselaustausch frei verfügbare Verschlüsselungsprogramme wie PGP verwendet oder eine E-Mail telefonisch ankündigt und hinterher telefoniert, um zu erfahren, ob sie unversehrt angekommen ist. Bestimmte Defizite lassen sich jedoch gar nicht individuell beseitigen – wie etwa die Unsicherheit, ob eine Nachricht sicher bei einem nicht kooperationswilligen Empfänger zugegangen ist. Besser als umständliche individuelle Hilfsmaßnahmen wäre deshalb eine sichere Infrastruktur im Internet, die bei Bedarf verlässliche Dienstleistungen anbietet, die Vertrauenswürdigkeit und Rechtssicherheit gewährleisten. Dann können diese Dienste auch rechtliche Anerkennung erfahren und ihren Zweck erfüllen, ohne dass im Streitfall umständlich ihre fehlerfreie Anwendung und ihr Sicherheitswert geklärt werden müssen.[3]

Wenn sich an dieser Infrastruktur nur jemand beteiligen könnte, der zuvor sicher identifiziert worden ist und der sich im Einzelfall sicher gegenüber der Infrastruktur anmelden muss, wäre gewährleistet, dass bestimmte Handlungen einer bestimmten Person zugerechnet werden können. Notwendig wäre ein Versanddienst, der sicherstellt und auch bestätigt, dass eine Nachricht beim Empfänger angekommen ist. Umgekehrt wäre es erforderlich, dass ein Postfachdienst einen sicheren Empfang ermöglicht, der einen Zugriff auf die Nachricht nur Berechtigten erlaubt. Ist es wichtig, dass die Identität oder eine Eigenschaft eines Handelnden im Internet festgestellt werden kann, müsste deren Authentisierung durch die verlässliche Bestätigung eines vertrauenswürdigen Dritten möglich sein.

Um sichere Informationen über unbekannte Kommunikationspartner anbieten zu können, bedarf es außerdem eines vertrauenswürdigen Verzeichnis- und Sperrdienstes. Ein sicherer Speicherplatz, der es Nutzern ermöglicht, wichtige elektronische Dateien unter Erhalt der Vertraulichkeit gegen Verlust zu sichern, würde die Palette der fehlenden Dienste ergänzen.[4]

Eine sichere Authentifizierung (allerdings nicht beim elektronischen Erstkontakt)[5] kann zwar auch über den Versand qualifiziert signierter Dokumente erreicht werden. Der öffentliche Schlüssel kann auch zur Verschlüsselung und damit zur Sicherung der Vertraulichkeit genutzt werden. Eine qualifizierte Signatur kann freiwilligen Empfangsbestätigungen ausreichenden Beweiswert verleihen. Dennoch stellen qualifizierte Signaturverfahren für sich kein den Bürgerportaldiensten gleichwertiges Dienstepaket zur sicheren Kommunikation dar.[6] Sie allein gewährleisten nicht die sichere Übertragung, ihr Verzeichnisdienst hat eine andere funktionale Ausrichtung und sie lösen nicht das Problem konfrontativer Zustellungen.

3 Bürgerportale als sichere Infrastruktur

Eine verlässliche Infrastruktur für diese sicheren Dienste sollen Bürgerportale bieten.[7] Ein Bürgerportal ist eine Plattform für die elektronische Kommunikation, die die genannten Dienste anbietet. In ihrem Zusammenwirken ergeben sie die Infrastruktur für rechtssicheres Handeln im Internet. Eine solche Infrastruktur soll das Bürgerportalgesetz ermöglichen, das die Bundesregierung am 20.2. 2009 in den Gesetzgebungsprozess eingebracht hat.[8] Der Entwurf wurde – nach einer kritischen Stellungnahme des Bundesrats[9] – zwar am 23.4.2009 in erster Lesung im Bundestag beraten und an die Ausschüsse überwiesen, konnte aber aus Zeitgründen in der 16. Legislaturperiode nicht mehr verabschiedet werden.

Der Bundestag hatte eine Entschließung verabschiedet, in der der neue Bundestag aufgefordert wurde, eine gesetzliche Regelung zu Bürgerportalen in der 17. Legislaturperiode zu beschließen.[10] Im Koalitionsvertrag von CDU/ CSU und FDP heißt es dazu: „Wir werden ein De-Mail-Gesetz verabschieden und dabei die Erfahrungen aus dem Pilotprojekt und die Stellungnahmen der Datenschutzbeauftragten des Bundes und der Länder berücksichtigen. Hierdurch wollen wir den Unternehmen die Möglichkeit geben, Geschäftsprozesse elektronisch abzuwickeln." Das Konzept der Bürgerportale und auch der Gesetzentwurf zu ihrer Regelung bleiben somit aktuell.

Die sichere Infrastruktur soll von den bisherigen Zugangsanbietern aufgebaut werden. Wenn sie – so das Konzept – neben ihren bisherigen Angeboten zusätzlich Bürgerportale anbieten, können Unternehmen, Behörden und Privatpersonen für ihre rechtssichere Kommunikation auf diese zurückgreifen.[11]

Folgende Dienste sollen oder können von Bürgerportalen angeboten werden:

3.1 Sichere Eröffnung von Bürgerportalen

Damit Bürgerportale Vertrauensanker im Kommunikationsraum des Internet sein können und damit an die Nutzung eines Bürgerportals und seiner Dienste Rechtsfolgen geknüpft werden können, ist eine zuverlässige Identifizierung des Nutzers erforderlich. Das soll durch Sichtvergleich mit einem gültigen staatlichen Ausweisdokument oder durch elektronische Äquivalente wie dem elektronischen Identitätsnachweis mit Hilfe des elektronischen Personalausweises[12] erfolgen. Eröffnet eine juristische Person ein Konto muss der aktuelle Handelsregisterauszug vorgelegt werden (§ 3 Abs. 3 Satz 1 Nr. 2 BPG-E) und eine sichere Identifizierung des anmeldenden Vertreters stattfinden. Um die informationelle Selbstbestimmung zu gewähr-

3 Siehe zum Folgenden auch Roßnagel, Bürgerportale für eine sichere Kommunikation im Internet, in: Klumpp/Kubicek/Roßnagel/Schulz (Hrsg.), Netzwelt – Wege, Werte, Wandel, 2009, 192 ff.

4 Knopp/Wilke/Hornung/Laue, MMR 2008, 723.

5 Siehe zu diesem Problem Roßnagel, DuD 2002, 281 ff.; Hornung, in: Roßnagel (Hrsg.), Allgegenwärtige Identifizierung?, 2006, 53 ff.

6 Dies verkennt Lapp, DuD 2009, 652. Bürgerportale sollen daher auch nicht die qualifizierte Signatur „nach 12 Jahren Misserfolgsgeschichte in den Sattel heben" (Fox, DuD 2009, 387).

7 Zu den damit verbundenen Rechtsfragen siehe Werner/Wegener, CR 2009, 310; Schulz, DuD 2009, 601, Lapp, DuD 2009, 651; Knopp/Wilke/Hornung/Laue, MMR 2008, 723.

8 BR-Drs. 174/09 und BT-Drs. 16/12598.

9 BT-Drs. 16/12598, 36 ff.

10 BT-Drs. 16/13618.

11 Siehe Stach, DuD, 2008, 184 ff.

12 Siehe hierzu näher Roßnagel/Hornung, DÖV, 2009, 301; Roßnagel/Hornung/Schnabel, DuD 2008, 168; Schliesky (Hrsg.), Gesetz über Personalausweise und den elektronischen Identitätsnachweis, 2009.

leisten, kann für ein Bürgerportalkonto auch ein Pseudonym beantragt werden.[13] Diese Möglichkeit wurde trotz der Einwände des Bundesrats[14] zu Recht beibehalten.

Nicht schützen kann die sichere Eröffnung gegen spätere, nicht gemeldete Änderungen der Identifizierungsdaten.[15] Dies ist allerdings bei allen Ausweisen so und daher nicht spezifisch für das Bürgerportal.[16]

3.2 Sichere Anmeldung

Die Vertrauenswürdigkeit sämtlicher Bürgerportaldienste hängt davon ab, dass sich nur der berechtigte Nutzer ihrer bedienen kann. Um das sicherzustellen, ist eine sichere Anmeldung am Bürgerportalkonto erforderlich. Ob sie genutzt wird, soll nach dem Gesetzentwurf (anders die Forderungen des Bundesrats)[17] weitgehend der Nutzer entscheiden. Ihm soll gemäß § 4 BPG-E – der Einfachheit halber – auch möglich sein, sich nur mit Namen und Passwort anzumelden. Neben diesem einfachen Zugang müssen die Bürgerportalbetreiber aber immer auch eine sichere Anmeldestufe anbieten. Sie setzt die Sicherung des Zugangs durch zwei voneinander unabhängige Sicherungsmittel wie Besitz und Wissen voraus (§ 4 Satz 3 BPG-E). Nur unter dieser Voraussetzung dürfte sich ein Anscheinsbeweis für die Authentizität einer Handlung ergeben.[18]

Der Gesetzentwurf legt nicht fest, welche Geheimnisse für die sichere Anmeldung am Bürgerportal in Betracht kommen. Die nähere Ausgestaltung des sicheren Anmeldevorgangs bleibt daher dem akkreditierten Diensteanbieter überlassen.[19] Dieser kann es dem Nutzer auch ermöglichen, sich mithilfe seines elektronischen Personalausweises oder seiner qualifizierten Signatur gegenüber dem Bürgerportal zu identifizieren, weil diese die Sicherungsmittel Besitz und Wissen kombinieren.[20]

Damit durch den einfachen Zugang jedoch nicht die Sicherheitsziele des Bürgerportalkonzepts kompromittiert werden, sind die Nutzungshandlungen für den einfachen Zugang begrenzt. So können beispielsweise vertrauliche Nachrichten nicht eingesehen werden,[21] zugestellte Nachrichten können nicht gelöscht werden.[22] Die Nutzung für den Spam-Versand durch unberechtigte Nutzer wird durch eine quantitative Versandbeschränkung verhindert.[23]

Dadurch dass das Löschen zugestellter Nachrichten nur nach einer sicheren Anmeldung des Nutzers möglich ist, wird sichergestellt, dass dessen Kenntnisnahme nicht durch einen unbefugten Dritten vereitelt werden kann.[24] Da der Zugriff auf Nachrichten, die der Versender als vertraulich eingestuft hat, von der sicheren Anmeldung des Empfängers abhängig ist, dient diese auch dem Schutz solcher Nachrichten vor unbefugter Kenntnisnahme.

Der Empfänger einer über den Versanddienst versandten Nachricht erhält auf Verlangen des Absenders eine beweissichere Bestätigung über dessen sichere Anmeldung. Der Nutzer soll bei jeder zu versendenden Nachricht erneut die Möglichkeit haben, zu entscheiden, ob die Bestätigung erzeugt wird. Die Beweissicherheit der Bestätigung kann etwa durch eine qualifizierte elektronische Signatur des akkreditierten Diensteanbieters gewährleistet werden. Durch diese Bestätigung erhält der Empfänger der elektronischen Nachricht ein belastbares Beweismittel. Eine aus Datenschutzgründen bedenkliche Protokollierung jeder einzelnen Anmeldung kann daher unterbleiben.[25]

3.3 Sicheres Postfach

Für die sichere Kommunikation im Internet ist ein sicheres Postfach erforderlich. Es ermöglicht zusammen mit dem Versanddienst eine sichere Kommunikation zwischen vertrauenswürdigen Sendern und Empfängern. Die Vertrauenswürdigkeit des Postfachs wird dadurch gewährleistet, dass nur der berechtigte Nutzer auf das Postfach zugreifen kann und dieser bei Eröffnung des Postfachs zuverlässig identifiziert worden ist. Der Sender kann sich daher darauf verlassen, dass der in der Bürgerportaladresse angegebene Inhaber des Postfachs mit dem berechtigten Nutzer identisch ist. Will er ganz sicher sein, dass die Nachricht nur von dem gewünschten Empfänger zur Kenntnis genommen werden kann, besteht für ihn die Möglichkeit festzulegen, dass der Empfänger auf die Nachricht nur zugreifen kann, wenn er sich mit der Zugangsstufe der sicheren Anmeldung gegenüber dem Postfach authentifiziert hat (§ 5 Abs. 4 BPG-E). Erst diese Funktion ermöglicht – etwa bei der Übermittlung von Patienten- oder Mandantendaten oder anderer Daten, für die besondere Verschwiegenheitspflichten bestehen – die Erfüllung beruflicher oder dienstlicher Sorgfaltspflichten bei der Nutzung des Internet.

3.4 Sicherer Versanddienst

Das sichere Postfach wird durch einen sicheren Versanddienst ergänzt.[26] Er zeichnet sich zum einen durch eine hohe Ausfallsicherheit aus. Zum anderen schützt er Vertraulichkeit und Integrität der Nachrichten durch Verschlüsselung und Signierung des Nachrichteninhalts auf dem Transportweg. Das schließt Ende-zu-Ende-Sicherheitsmaßnahmen der Nutzer, die für bestimmte Inhalte oder die Kommunikation bestimmter Berufsvertreter erforderlich sind, wie Inhaltsverschlüsselung oder Signaturen durch den Sender nicht aus. Diese Sicherungsmaßnahmen werden vom sicheren Postfach- und Versanddienst unterstützt,[27] allerdings – entgegen der Kritik der Konferenz der Datenschutzbeauftragten[28] – nicht für jede Kommunikation gefordert. Dem liegt die Erwägung zugrunde, dass ein solches Schutzniveau nicht für alle Nachrichten erforderlich ist und zu hohe technische Zugangshürden für die Benutzung des Versanddienstes aufbauen könnte.[29]

Drittens bietet der Versanddienst auf Antrag des Senders eine Versandbestäti-

13 Zur Aufdeckungspflicht siehe 4.3; zu den Voraussetzungen siehe § 16 BPG-E.

14 BT-Drs. 16/12598, 36f.

15 Siehe Lapp, DuD 2009, 654.

16 Siehe aber die Korrekturpflicht nach § 7 Abs. 2 Satz 1 BPG-E.

17 BT-Drs. 16/12598, 36; die Bundesregierung will hier einen möglichst einfachen Zugang ermöglichen, ebd., 44.

18 Siehe hierzu 5.

19 Dies könnte auch in der vorgesehenen Bürgerportalverordnung festgelegt werden.

20 Dies übersieht Lapp, DuD 2009, 654.

21 Siehe den Entwurf der Technischen Richtlinie Bürgerportale, Postfach und Versanddienst Funktionalitätsspezifikation, 19, https://www.bsi.bund.de/cae/ servlet/contentblob/486072/publicationFile/41764/ TR_BP_PVD_FU_pdf.pdf.

22 Siehe Entwurf (Fn. 21), 14.

23 Siehe Entwurf (Fn. 21), 50.

24 Die von Lapp, DuD 2009, 654, befürchtete Zustellungsvereitelung ist daher nicht möglich.

25 Die von Probst, Datenschutz-Berater 2009, 16 geäußerte Befürchtung eines großen Überwachungspotentials ist daher unbegründet.

26 Siehe Werner/Wegener, CR 2009, 310, 312f.

27 Z. B. durch die Verpflichtung der Anbieter zur Übernahme öffentlicher Schlüssel in den Verzeichnisdienst nach § 7 Abs. 1 Satz 1 BPG-E.

28 DuD 2009, 424.

29 Dies bleibt in der Kritik von Lapp, DuD 2009, 653, unberücksichtigt.

gung. In ihr signiert der Anbieter qualifiziert die Prüfsumme der Nachricht, den Empfänger und den Zeitpunkt der Versendung (§ 5 Abs. 7 BPG-E). Um auch ohne förmliche Zustellung Nachrichten mit vertrauenswürdigen Nachweisen zustellen zu können, bieten die Diensteanbieter im Zusammenwirken viertens eine elektronische Zugangsbestätigung an. Der Diensteanbieter des Empfängers bestätigt in dieser auf Antrag des Senders, wann er welche Nachricht im Bürgerportal-Postfach des Empfängers abgelegt hat. Hierfür signiert er die Prüfsumme der Nachricht und einen Vermerk über den Zeitpunkt der Ablage mit einer dauerhaft prüfbaren qualifizierten elektronischen Signatur (§ 5 Abs. 8 BPG-E).

Schließlich soll über Bürgerportale auch eine förmliche Zustellung möglich sein.[30] Da hierbei eine hoheitliche Zustellbestätigung erzeugt wird, werden die Bürgerportalbetreiber mit Hoheitsbefugnissen zur Erzeugung öffentlicher elektronischer Dokumente beliehen (§ 5 Abs. 6 Satz 2 BPG-E).

3.5 Sichere Authentifizierung

Viele Nutzer, die bei der Eröffnung ihres Bürgerportalkontos Identitätsdaten angegeben haben, würden sie gern für eine sichere Authentifizierung gegenüber Dritten nutzen können. Im Rahmen eines freiwilligen Identitätsbestätigungsdienstes nach § 6 BPG-E kann der Portalbetreiber anbieten, diese Daten im Einzelfall auf Anforderung des Nutzers an den Empfänger zu senden und damit die Identität des Nutzers zu bestätigen. Um dem Empfänger die notwendige Sicherheit zu geben, kann dieser Dienst aber nur nach einer sicheren Anmeldung genutzt werden.[31] Die Praxis muss zeigen, welche Funktion dieser Authentisierungsmöglichkeit neben dem elektronischen Identitätsnachweis im neuen elektronischen Personalausweis (§ 18 PAuswG) zukommen kann.[32]

3.6 Sicherer Verzeichnisdienst

Der Verzeichnisdienst nach § 7 BPG-E eröffnet dem Nutzer die Möglichkeit, seine Bürgerportaladresse und seine Identifikationsdaten freiwillig so zu veröffentlichen, dass Dritte die Möglichkeit haben, sie zur Kenntnis zu nehmen und sie für eine Kommunikation mit dem Nutzer zu verwenden. Der Anbieter hat sicherzustellen, dass auf Antrag des Nutzers und anderer Berechtigter die Verzeichnisdaten, die nicht mehr zutreffen oder nicht mehr verwendet werden sollen, unverzüglich gelöscht werden (§ 7 Abs. 2 Satz 1 BPG-E). Da durch die Löschung eine weitere Verwendung der gesperrten Daten verhindert wird, sind Sperrlisten oder Möglichkeiten, die aktuelle Gültigkeit der Daten nachzuprüfen, nicht notwendig. Durch diesen Dienst wird die Vertrauenswürdigkeit des Postfach-, Versand- und Authentisierungsdienstes gestärkt.

Die Nutzung des Verzeichnisdienstes für Spam wird dadurch zumindest erschwert, dass nur mit De-Mail-Adressen an De-Mail-Adressen Nachrichten verschickt werden können und eine direkte Kommunikation mit Internet-E-Mail-Adressen nicht möglich ist. Außerdem darf beim Authentisierungsniveau „normal" nur eine beschränkte Zahl von De-Mails pro Zeiteinheit verschickt werden. Damit kann die Identität des Spam-Absenders festgestellt und dieser rechtlich belangt werden.[33]

3.7 Sicherer Speicherplatz

Das freiwillige Angebot eines Speicherplatzes zur sicheren Ablage von Dateien (§ 8 BPG-E) soll dem Nutzer ermöglichen, für ihn wichtige Dateien zugriffsgesichert und gegen Verlust geschützt in seinem Bürgerportal aufzubewahren.[34] Hierbei kann es sich um beliebige Dateien handeln, zu denen der Zugriffsschutz über das Bestimmen der Sicherheitsstufe der Anmeldung individuell festgelegt werden kann. Der Dienst trägt dem zunehmenden Bedürfnis der Nutzer Rechnung, wichtige Dateien an einem sicheren Ort außerhalb des eigenen, stets gefährdeten Endgeräts gegen den etwaigen Verlust zu sichern, ohne dafür ein erhöhtes Risiko unbefugter Kenntnisnahme in Kauf nehmen zu müssen. Der sichere Speicherplatz ist vom Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme geschützt.[35] Der Anbieter kann weitere Funktionen des sicheren Speicherplatzes anbieten, wie z. B. die Kontrolle und Vornahme notwendiger Übersignierungen für signierte Dokumente,[36] die Bestätigung und Übersendung elektronischer Dokumente an Dritte oder die Freigabe zum Abruf von Dokumenten durch Dritte auf Wunsch des Nutzers.

4 Vertrauenswürdigkeit der Diensteanbieter

Entscheidende Voraussetzung für den Erfolg von Bürgerportalen und ihren Diensten ist das Vertrauen der Öffentlichkeit in ihre Vertrauenswürdigkeit. Notwendig ist daher, dass Sicherheit und Datenschutz nicht nur behauptet, sondern nachgewiesen werden. Aufgrund seiner Schutz- und Gewährleistungsfunktion kommt dem Staat die Aufgabe zu, der Wirtschaft ein entsprechendes Nachweisverfahren anzubieten.[37] Das Bürgerportalgesetz ermöglicht daher eine freiwillige[38] Akkreditierung nach den §§ 17 ff. BPG-E. Sie ermöglicht Anbietern, ihre Dienste als Bürgerportaldienste wirksam aufzuwerten. Sie können die Qualität ihrer Dienste in einem rechtssicheren Rahmen mit definierten Anforderungen verbessern und die Erfüllung dieser Anforderungen gegenüber ihren Kunden nachweisen.

Diese Prüfung und Anerkennung anhand eines bestehenden Rechtsrahmens unterscheidet die Bürgerportaldienste von technisch unter Umständen ähnlich siche-

30 Siehe hierzu 5. sowie Art. 2 BPG-E.

31 Siehe den Entwurf der Technischen Richtlinie Bürgerportale Identifizierungsdienst Light Funktionalitätsspezifikation, 7, https://www.bsi.bund.de/cae/s ervlet/contentblob/486056/publication File/41756/TR_BP_IDL_FU_pdf.pdf.

32 Siehe Schulz, DuD 2009, 602 f.; zum elektronischen Identitätsnachweis siehe Fn. 12.

33 Dies übersieht Lapp, DuD 2009, 653.

34 Siehe auch Schulz, DuD 2009, 602.

35 Siehe zu diesem Hoffmann-Riem, Das Grundrecht auf Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, in: Klumpp/Kubicek/Roßnagel/Schulz (Hrsg.), Netzwelt – Wege, Werte, Wandel, 2009, 165 ff.

36 Siehe z. B. Hackel/Roßnagel, Langfristige Aufbewahrung elektronischer Dokumente, in: Klumpp/Kubicek/Roßnagel/Schulz (Hrsg.): Informationelles Vertrauen für die Informationsgesellschaft, 2008, 199 ff.

37 Siehe Roßnagel, Infrastrukturverantwortung des Staats und Eigenverantwortung des Bürgers, in: Kubicek/Klumpp/Büllesbach/Fuchs/Roßnagel (Hrsg.), Innovation@Infrastruktur, Jahrbuch Telekommunikation und Gesellschaft, 2002, 269 ff.

38 Die Freiwilligkeit der Akkreditierung ergibt sich daraus, dass jeder Anbieter die gleichen Dienste auch ohne Akkreditierung anbieten kann, allerdings ohne die Rechtsvorteile des BPG – dies verkennen Werner/Wegener, CR 2009, 314.

ren Teilangeboten, deren Sicherheit jedoch nicht vorab nachgewiesen ist.[39]

4.1 Akkreditierung

Die Akkreditierung erfolgt auf Antrag der Bürgerportalbetreiber, wenn deren Vertrauenswürdigkeit nach einer behördlichen Überprüfung festgestellt worden ist.[40] Nach §§ 2 i.V.m. 17 Abs. 1 Satz 1 BPG-E soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) diese Überprüfung vornehmen. Nach der Akkreditierung kann der Bürgerportalbetreiber seine Vertrauenswürdigkeit durch ein Gütezeichen nachweisen. Mit ihm kann er auf dem Markt um das Vertrauen seiner Kunden werben.

Staatliche und private Stellen können die nachgewiesene Vertrauenswürdigkeit der akkreditierten Diensteanbieter in ihren Informatikanwendungen berücksichtigen. An diesen Nachweis können andere Gesetze bestimmte Rechtsfolgen knüpfen, die eine solche Vertrauenswürdigkeit voraussetzen.

Die akkreditierten Bürgerportalbetreiber bilden einen Verbund, der die Infrastruktur der Bürgerportale betreibt. Die Zugehörigkeit zum Verbund akkreditierter Bürgerportalbetreiber wird neben dem Gütesiegel durch die Verwendung der Second-Level-Domain „de-mail" zum Ausdruck gebracht. Eine Bürgerportaladresse ist am spezifischen Format und der Verwendung von „de-mail" erkennbar, z. B. „karl.meier@maildienst. de-mail.de". Diese Domain ist allein den akkreditierten Bürgerportalbetreibern vorbehalten. An ihr kann der Rechts- und Geschäftsverkehr erkennen, dass die Mail, die Identifikationsdaten oder die Bestätigung von einem akkreditierten Bürgerportalbetreiber stammen.

4.2 Voraussetzungen der Akkreditierung

Voraussetzung für die Akkreditierung als Bürgerportalanbieter ist gemäß § 18 BPG-E im Wesentlichen, dass er nachweist, dass er

- und die in seinem Betrieb tätigen Personen über die notwendige Zuverlässigkeit und Fachkunde verfügen,
- über eine geeignete Deckungsvorsorge für die möglichen Schadensersatzzahlungen aufgrund von Fehlern als Bürgerportalbetreiber verfügt,
- die Bürgerportaldienste sicher, zuverlässig und im Zusammenwirken mit den anderen akkreditierten Diensteanbietern erbringt, die Pflichten als Bürgerportalanbieter erfüllt und ein geeignetes Sicherheitskonzept erstellt und umgesetzt hat;
- die datenschutzrechtlichen Anforderungen an die Gestaltung und den Betrieb der Bürgerportaldienste erfüllt.

Die letzte Anforderung sollte nach dem Entwurf durch ein Datenschutzaudit nachgewiesen werden, das nach dem zeitgleich geplanten Datenschutzauditgesetz erlangt werden sollte. Diese Anforderung hätte auch die Forderung der Datenschutzbeauftragten erfüllt, im Rahmen der Akkreditierung die tatsächliche Einhaltung datenschutzrechtlicher Standards zu prüfen.[41] Nachdem auch das Datenschutzauditgesetz in der letzten Legislaturperiode nicht verabschiedet wurde, wird der Gesetzgeber entweder beide Gesetze parallel verabschieden oder – was sicher die schlechtere Lösung wäre – ein separates Nachweisverfahren für die Diensteanbieter von Bürgerportalen regeln müssen.

4.3 Anbieterpflichten

Neben dem funktionsgerechten und sicheren Angebot der Dienste des Bürgerportals[42] muss der akkreditierte Anbieter weitere Pflichten erfüllen. Zu ihnen gehören vor allem die

- Information des Nutzers über die möglichen Rechtsfolgen, die eine Benutzung der Bürgerportaldienste nach sich ziehen kann, und über notwendige Sicherungsmaßnahmen zur Nutzung des Bürgerportals,[43]
- Dokumentation aller Vorgänge und Dokumente für 30 Jahre, die der Bürgerportalbetreiber benötigt, um die Erfüllung seiner Pflichten nachweisen zu können,[44]
- Aufdeckung von Pseudonymen in berechtigten Fällen, ohne Missbrauchsmöglichkeiten zu eröffnen,[45]
- Beachtung der Verbraucherschutzregeln,[46]
- Sperrung oder Aufhebung des Bürgerportalkontos auf Wunsch des Nutzers oder auf Verlangen des BSI,[47]
- Ermöglichung des Zugriffs auf Daten im Postfach und im Speicherplatz für drei Monate auch nach Beendigung des Vertragsverhältnisses mit dem Nutzer oder einer Beendigung der Tätigkeit als Bürgerportalbetreiber.[48]

5 Rechtsfolgen

Da mit der Akkreditierung die Vertrauenswürdigkeit eines Bürgerportals bestätigt und durch ein Gütezeichen nachgewiesen wird, ist es möglich, weitergehende Rechtsfolgen an die angebotenen Dienste zu knüpfen, als es ohne Akkreditierung der Fall wäre.[49]

Bisher ist die amtliche Zustellung elektronischer Dokumente nur im Konsens mit dem Empfänger möglich. Denn er muss den Zugang durch eine Empfangsbestätigung bestätigen. Eine konfrontative Zustellung ohne Kooperation des Empfängers ist in Form einer telekommunikativen Übermittlung bisher ausgeschlossen. Das soll nun durch Änderung des § 174 Abs. 3 ZPO und durch Einfügung des § 5a in das VwZG möglich werden. Die amtliche Zustellbestätigung durch den beliehenen akkreditierten Bürgerportalbetreiber ist ein öffentliches elektronisches Dokument, dessen Echtheit und dessen Inhalt nach §§ 371a Abs. 2, 415 und 437 ZPO vermutet wird.[50] Das bringt dem elektronischen Rechtsverkehr einen hohen Zugewinn an Rechtssicherheit.[51]

Im Vergleich zur papierbasierten Zustellung ermöglicht die Zustellung über

39 Aus diesem Grund ist das Bürgerportalgesetz trotz z. B. S/MIME, oder PGP nicht überflüssig – so aber Fox, DuD 2009, 387.

40 Zum Verfahren siehe auch Werner/Wegener, CR 2009, 314.

41 DuD 2009, 424.

42 Siehe hierzu 3.

43 § 9 BPG-E. Eine nähere Ausgestaltung der Informationspflichten kann entgegen der Forderungen der Datenschutzbeauftragten (DuD 2009, 424) auch in der Rechtsverordnung erfolgen. Hinsichtlich möglicher wettbewerbswidriger Werbemaßnahmen darf nicht von einem Projektflyer der Bundesregierung auf ein künftiges Werbeverhalten der Anbieter geschlossen werden – so aber Lapp, DuD 2009, 653. Sie werden gerade aus wettbewerbsrechtlichen Gründen zutreffende und umfassende Informationen anbieten.

44 § 13 BPG-E.

45 § 16 Abs. 1 BPG-E.

46 § 14 BPG-E.

47 § 10 BPG-E.

48 § 12 BPG-E.

49 Siehe auch Werner/Wegener, CR 2009, 312.

50 Daher ist eine eigene Beweisregelung entsprechend § 371a ZPO nicht notwendig – so aber Werner/Wegener, CR 2009, 316.

51 Allerdings sollte gemäß der Kritik der Datenschutzbeauftragten, DuD 2009, 424, eine Zustellung ohne sichere Anmeldung nicht möglich sein.

Bürgerportale sogar, den Inhalt des zugestellten Dokuments im Streitfall zu beweisen, wenn die Zustellungsbestätigung, ebenso wie die in § 5 Abs. 7 BPG-E vorgesehene Versandbestätigung, die Prüfsumme der versendeten Nachricht enthält.

Eine Verkürzung des Rechtsschutzes ist mit dem Verzicht auf eine unmittelbare Übergabe der zuzustellenden Nachricht dagegen nicht verbunden.[52] Auch § 3 VwZG i.V.m. § 180 ZPO erlaubt bereits die Zustellung durch Einlegen in den Briefkasten, wenn niemand angetroffen wird. Die verschiedenen Möglichkeiten, bei anderen Zustellungsarten den Empfang zu verweigern, stellen keine zu schützende Rechtsposition dar. Einzig eine Fristverkürzung im Vergleich zur Zustellung nach § 4 VwZG ist möglich, wird jedoch durch die freiwillige Nutzung von Bürgerportalen, den leichteren Zugriff auf das Bürgerportalpostfach und die Aufklärung über Rechtsfolgen der Bürgerportalnutzung nach § 9 Abs. 1 BPG-E aufgewogen.

Mit der Akkreditierung sind auch nicht ausdrücklich geregelte Rechtsfolgen angestrebt. Dazu zählt der Anscheinsbeweis bei einer sicheren Anmeldung. Aufgrund der vorgeprüften und nachgewiesenen Vertrauenswürdigkeit der Diensteanbieter und der Anmeldung des identifizierten Nutzers mit zwei von einander unabhängigen Sicherungsmitteln im Einzelfall dürften die Gerichte – ähnlich wie bei der Verwendung von EC-Karten[53] – einen widerlegbaren Anschein annehmen, dass der Nutzer selbst von seinem Konto aus im Internet gehandelt hat. Auch dieser Anscheinsbeweis der Verantwortung für bestimmte Handlungen dürfte die Rechtssicherheit im Internet deutlich stärken. Zu beachten ist allerdings, dass dieser Anscheinsbeweis nur die Identität des Handelnden betrifft, nicht jedoch den Inhalt von Willenserklärungen. Sie sind beweissicher auch weiterhin nur mit qualifizierten elektronischen Signaturen nachzuweisen.[54]

Schließlich könnte die Nutzung von Bürgerportalen mehr Rechtssicherheit in der Kommunikation zwischen Bürger und Verwaltung bieten. Nach § 3a Abs. 1 VwVfG kann die Verwaltung dem Bürger nur dann rechtsrelevante Bescheide wirksam elektronisch übermitteln, wenn er hierfür einen Zugang eröffnet hat. Da das Gesetz keine klaren Maßstäbe für eine Zugangseröffnung festgelegt hat,[55] scheuen die Behörden das rechtliche Risiko einer elektronischen Übermittlung und benutzen weiterhin den Postweg. Da ein Bürgerportal explizit das Ziel verfolgt, die Rechtssicherheit rechtsverbindlicher Kommunikation im Internet zu erhöhen, könnte in der Praxis angenommen werden, dass so-

52 A. A. Steppling, NJW 2009, Heft 18, Editorial; Lapp, DuD 2009, 651 f. Siehe dagegen Roßnagel, NJW 2009, Heft 23, XVIII.

53 Siehe BGH, NJW 2004, 3623 ff. m.w.N.; OLG Karlsruhe, MDR 2008, 1112f. Bei der Nutzung von EC-Karten kann der erste Anschein zwar ebenso dafür sprechen, dass der Karteninhaber den Missbrauch der EC-Karte und der PIN grob fahrlässig ermöglicht hat. Auch in diesem Fall haftet der Karteninhaber aber nach den Grundsätzen der Rechtsscheinsvollmacht.

54 Das übersieht Schulz, DuD 2009, 605, nach dem auch die nicht qualifiziert signierten Nachrichten des Postfach- und Versanddienstes „als authentisch und daher rechtssicher gelten" sollen.

55 Kritisch hierzu Roßnagel, NJW 2003, 469ff.

wohl eine Behörde[56] als auch ein Bürger, der ein Bürgerportalkonto eröffnet und gegenüber dem Partner benutzt, damit auch einen Zugang für den Empfang elektronischer Dokumente von diesem Partner eröffnet. Der Bundesregierung hat sich gescheut, diese Rechtsfolge explizit zu normieren, diese Rechtsfolge aber in der Gesetzesbegründung genannt.[57]

6 Akzeptanz der Bürgerportale

Die durch die Akkreditierung sichergestellte Vertrauenswürdigkeit der Bürgerportaldiensteanbieter ist eine wichtige und wirksame Grundlage für die Akzeptanz des Bürgerportalkonzepts. Das Instrument der Akkreditierung und der Erteilung von Gütesiegeln hat in anderen Bereichen seine Eignung bewiesen. In dieser Hinsicht ist es bedauerlich, dass wichtige Protagonisten durch Datenschutzskandale oder gleichzeitig betriebene Überwachungsvorhaben wichtiges Vertrauen in der Bevölkerung verspielt haben.[58]

Eine weitere wichtige Grundlage ist jedoch der erkennbare Nutzen für den einzelnen Bürger, ohne den eine erfolgsnotwendige flächendeckende Verbreitung unwahrscheinlich bliebe. Auf den ersten Blick scheint gerade die beweisbare elektronische Zustellung für den nicht professionellen Nutzer eher Nachteile zu bringen.[59] Da die Eröffnung eines Bürgerportalkontos freiwillig sein soll,[60] könnten sich viele Bürger deshalb dagegen entscheiden. Es war jedoch nie das Ziel des Gesetzes, für Personen eine Lösung zu schaffen, die „heute vor allem Probleme bei der Zustellung verursachen".[61] Wenn ein substantieller Teil der übrigen Bürger ein Bürgerportal nutzen würde, wäre dies für einen Erfolg der Bürgerportale ausreichend.

Für den Nutzen ist die Möglichkeit der zweiseitigen Kommunikation entscheidend, nicht allein die Rolle als Empfänger.[62] Der Nutzer hat als Sender rechtlich relevanter Kommunikation von De-Mail Vorteile, etwa bei beweisbaren Zustellungen von Anträgen oder Einsprüchen, Vertragserklärungen oder verbraucherschutzrechtlichen Widerrufserklärungen. Als Teilnehmer von De-Mail kann er Nachrichten (etwa von Ämtern, Anwälten oder Ärzten) empfangen, die er ohne De-Mail nur per Brief erhalten dürfte. Zudem eröffnet die elektronische Erreichbarkeit für Zustellungen sämtliche Vorteile, die der elektronische Erhalt von Dokumenten mit sich bringt. Die Zustellungsinhalte können beispielsweise leichter weitergegeben, verfügbar gehalten oder bearbeitet werden. Auch die Erforderlichkeit eines aktiven „Abholens" möglicherweise rechtlich bedeutsamer Kommunikationsinhalte,[63] die freilich auch bei jedem herkömmlichen Briefkasten notwendig ist, kann mit mehr Vorteilen als Nachteilen verbunden sein. Während der herkömmliche Briefkasten nur an seinem Standort eingesehen werden kann, ist der Zugriff auf das Bürgerportalkonto von beinahe überall möglich. Auch den Sicherheitsvergleich mit dem herkömmlichen Briefkasten braucht das Konto nicht zu scheuen. Zudem eröffnet die gewährleistete Vertraulichkeit die Möglichkeit zur bequemen E-Mail-Kommunikation mit Berufsgruppen, denen dies bislang eigentlich versperrt oder nur nach einer für den Nutzer nachteiligen Risikoübernahme möglich war.

Ein wichtiger Faktor für die Akzeptanz werden auch die Kosten sein. Hier wird es darauf ankommen, welche Geschäftsmodelle gewählt und wem die Kosten angelastet werden. Werden die Kosten hauptsächlich den Bürgern aufgebürdet und die Vorteile entstehen bei Unternehmen und Behörden, wäre dies Akzeptanz gefährdend.[64] Bisher sind hierzu allerdings noch keine Vorstellungen bekannt und ablehnende Stellungnahmen aufgrund bloßer Vermutungen zumindest voreilig.

Schließlich bleibt darauf hinzuweisen, dass eine Infrastruktur wie Bürgerportale nicht erst dann sinnvoll ist, wenn sie wirklich von jedem Bürger genutzt wird.[65] Wie bei allen bisherigen IT-Infrastrukturen wird es einen gestuften Einführungsprozess geben: Am Anfang werden vor allem Behörden, mittlere und größere Unternehmen sowie Träger freier Berufe (z. B. Anwälte, Ärzte) als Vielfachnutzer („Power-User") die sichere Kommunikationsinfrastruktur nutzen. Nach und nach werden dann Bürger, die in bestimmten Lebensbereichen Vorteile sehen, sich eine Bürgerportaladresse zulegen und deren Verwendung mit steigendem Vertrauen ausdehnen.

Ein solch gestufter Einführungsprozess ist für technische Innovationen typisch und deshalb kein Argument gegen die Sinnhaftigkeit des Vorhabens.

7 Ausblick

Bürgerportale bieten eine Infrastruktur rechtssicherer Kommunikation im Internet. Sie schließen daher eine Lücke für den elektronischen Rechts- und Geschäftsverkehr, die bisher eine Nutzung des Internet für eine Reihe von Zwecken verhindert hat. Sie ermöglichen, die elektronische rechtlich auf die gleiche Stufe wie die papierbasierte Kommunikation zu stellen. Privatbetriebene Bürgerportale führen nicht zu einer „staatsgesteuerten Kommunikation"[66] und nicht zu einer staatlich zentralisierten E-Mail-Kontrolle, sondern nur zu einem sicheren und datenschutzgerechteren Angebot bereits vorhandener E-Mail-Dienste. Ihre Nutzung steht Bürgern, Unternehmen und Verwaltungen frei. Sie werden Bürgerportale nutzen, wenn die höhere Rechtssicherheit ihnen Vorteile verspricht. Diese Vorteile werden wachsen, wenn die rechtliche Integration der Bürgerportale durch die Länder, Standesorganisationen und andere Institutionen fortschreitet. Für die unverbindliche Kommunikation werden die genannten Zielgruppen bei den anderen Internetdiensten bleiben. Bürgerportale erhöhen dadurch nicht nur die Rechtssicherheit, sondern auch die Wahlfreiheit im Internet.

56 Dies übersieht Lapp, DuD 2009, 652.

57 So auch die Gesetzesbegründung, BT-Drs. 16/12598, 33 f.

58 Siehe Werner/Wegener, CR 2009, 316; Heckmann, jurisPR-ITR 3/2009 Anm. 1; Probst, DSB 2/2009, 16.

59 So Lapp, DuD 2009, 651 f.

60 Dies ist eine wesentliche Forderung der Datenschutzbeauftragten, siehe DuD 2009, 424.

61 So Lapp, DuD 2009, 652, der insoweit die Intention des Vorhabens verkennt.

62 Diese übersieht Lapp, DuD 2009, 652.

63 Dies wertet Fox, DuD 2009, 387, als ein „Verlieren" des Anwenders.

64 Fox, DuD 2009, 387; Werner/Wegener, CR 2009, 311: Finanzierung durch eingesparte Porto- und Materialkosten.

65 Dies übersieht Lapp, DuD 2009, 651 ff.

66 So Heckmann, jurisPR-ITR 3/2009, Anm. 1.