Deutscher Bundestag **Drucksache 16/11542**

16. Wahlperiode 05. 01. 2009

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Hans-Joachim Otto (Frankfurt), Christoph Waitz, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 16/11268 –

Planungen der Bundesregierung zur Einführung von De-Mail

Vorbemerkung der Fragesteller

Die Bundesregierung plant die Einführung eines De-Mail-Dienstes, mit dem neben bereits bestehenden Möglichkeiten der verschlüsselten und mithin sicheren elektronischen Kommunikation eine Infrastruktur für sicheren Mail-Versand geschaffen werden soll. Über De-Mail sollen Bürgerinnen und Bürger im Rahmen der Weiterentwicklung von E-Government-Anwendungen sicher mit Behörden kommunizieren können.

Die Förderung der rechtssicheren, datensicheren und zuverlässigen elektronischen Kommunikation zwischen Behörden und Unternehmen sowie Bürgerinnen und Bürgern ist für die Informationsgesellschaft von erheblicher Bedeutung.

Allerdings ist bislang nicht hinreichend klar, warum der Staat hier eine eigene Infrastruktur aufbauen muss statt auf bestehende Möglichkeiten zurückzugreifen. Der im Aufbau von De-Mail liegende Eingriff in marktwirtschaftliche, aber auch technische Entwicklungen muss genau geprüft werden.

Datensicherheit und Datenschutz sind unabdingbare Voraussetzung für das Vertrauen der Bürgerinnen und Bürger sowie Unternehmen in E-Government. Nur wenn Datenschutz und Datensicherheit groß geschrieben werden, werden E-Government-Anwendungen auch von den Nutzern angenommen. Daher müssen beim Projekt De-Mail diese Aspekte besonders gewürdigt werden.

Die EU-Dienstleistungsrichtlinie führt erfreulicherweise zu einem Schub bei der Entwicklung von E-Government in der Bundesrepublik Deutschland. In Bund, Ländern und Kommunen wird mit Hochdruck daran gearbeitet, die Voraussetzungen zur Umsetzung der Richtlinie zu schaffen. Hierbei muss jedoch das Augenmerk auch darauf liegen, den Zugang zu Behörden mittels elektronischer Kommunikation so einfach wie möglich zu gestalten. Neue Hürden aufzubauen, indem ein neues System genutzt werden soll, laufen diesem Zweck jedoch zuwider.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 22. Dezember 2008 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

1. Aus welchen Gründen hält die Bundesregierung es für erforderlich, statt auf schon verfügbare sichere elektronische Kommunikationsmöglichkeiten zurückzugreifen, einen neuen E-Mail-Service „De-Mail“ zu schaffen?

Die heute schon vorhandenen Systeme sind technische Lösungen, die sichere elektronische Kommunikation in einem bestimmten Einsatzbereich (z. B. ein Land oder eine Stadt mit ihren Bürgerinnen und Bürgern, im Bereich der Justiz, Wirtschaftsunternehmen mit ihren jeweiligen Kundinnen und Kunden) auf viele verschiedene Weisen und auf verschiedenen Sicherheitsniveaus umsetzen. Die Akzeptanz solcher Systeme bei Bürgerinnen und Bürgern ist entsprechend gering. Einzelne technische Lösungen sind keine Alternative zu einer in Bezug auf Sicherheits-, Datenschutz- und Interoperabilitätsanforderungen einheitlichen Infrastruktur. Die Ausbildung einer Infrastruktur – die „De-Mail“ – ermöglicht die vertrauliche und verbindliche elektronische Kommunikation aller mit allen (Wirtschaft, Bürger, Verwaltung, sonstige Organisationen) auf einem einheitlichen und definierten Sicherheits- und Datenschutzniveau.

2. Welche Gründe sprechen gegen die Nutzung von schon vorhandenen E-Mail-Strukturen unter Hinzuziehung sicherer Verschlüsselungsmethoden?

Sichere Verschlüsselungsmethoden gewährleisten lediglich den Schutz der Vertraulichkeit einer Nachricht. Authentizität von Absender und Empfänger sind damit i. d. R. nicht gesichert. Auch lassen sich damit Versand und Zustellung einer Nachricht nur sehr schwer nachweisen. Die verschlüsselten Internet-E-Mails können z. B. auf dem Transportweg gelöscht werden, ohne dass dies bemerkt wird. Die Rechtsverbindlichkeit einer lediglich verschlüsselten E-Mail ist deshalb für zahlreiche Geschäfts- und Verwaltungsprozesse nicht ausreichend.

Die Technologien (z. B. bei Ende-zu-Ende-Verschlüsselung und/oder Signaturen) setzen vielfach voraus, dass der Nutzer selbst die entsprechenden Software-Komponenten installiert, zugehörige Zertifikate für seine Kommunikationspartner verwaltet und geeignet mit den privaten Schlüsseln umgeht. Hier haben die Erfahrungen der vergangenen Jahre gezeigt, dass eine flächendeckende Verbreitung solcher Lösungen nur sehr schwer zu erreichen ist. Bei De-Mail können diese Aufgaben, für die der Nutzer bisher selbst verantwortlich war, von vertrauenswürdigen Anbietern durchgeführt werden. Die privatwirtschaftlichen Anbieter müssen dazu in einem Akkreditierungsverfahren nachweisen, dass sie hohe Voraussetzungen an IT-Sicherheit, Datenschutz und Verbraucherschutz erfüllen. Damit kann der Nutzer einen Webbrowser oder einen Standard-E-Mail-Client für sichere Kommunikation verwenden.

3. In welchem Verhältnis soll De-Mail zur im Rahmen der Einführung des elektronischen Personalausweises geplanten Funktionalität des elektronischen Identitätsnachweises stehen?

Der elektronische Identitätsnachweis des künftigen elektronischen Personalausweises soll von der De-Mail in zweierlei Hinsicht genutzt werden können. Einerseits soll damit eine Online-Erstidentifizierung und damit die Beantragung eines De-Mail-Accounts möglich sein. Andererseits kann der elektronische Personalausweis zum Anmelden am De-Mail-Account auf einem hohen Sicherheitsniveau verwendet werden.

4. Warum ist es erforderlich, neben der Einführung des elektronischen Identitätsnachweises eine eigene technische Infrastruktur für elektronische Kommunikation aufzubauen statt bestehende Strukturen mittels Verschlüsselungstechnologien in Verbindung mit dem neuen Personalausweis oder anderen derartigen Karten zu nutzen?

Auch mit einer verschlüsselten E-Mail-Kommunikation in Verbindung mit dem elektronischen Personalausweis können Versand und Zustellung von Nachrichten sowie deren Integrität und Verbindlichkeit nur schwer nachgewiesen werden. Im Übrigen wird auf die Antwort zu Frage 1 verwiesen.

5. Wie bewertet die Bundesregierung es aus datenschutzrechtlichen Aspekten, dass alle Bürgerinnen und Bürger, die an De-Mail teilnehmen möchten, ihre bestehende E-Mail-Adresse bekannt geben müssen, um diese dann mit dem Zusatz De-Mail für die Kommunikation mit Behörden nutzen zu können, insbesondere vor dem Hintergrund, dass viele Menschen gerade zum Schutz ihrer persönlichen Daten anonyme oder kryptische Adressen verwenden?

Die bestehenden E-Mail-Adressen von Bürgerinnen und Bürgern bleiben von den Regelungen zu De-Mail völlig unberührt und können wie bisher weiter verwendet werden. Bürgerinnen und Bürger, die an De-Mail teilnehmen möchten, erhalten hierfür eine eigene De-Mail-Adresse, die i. d. R. das Format „vorname.name.123@providerxy.de-mail.de“ hat. Darüber hinaus ist jeder De-Mail-Provider verpflichtet, seinen Kundinnen und Kunden pseudonyme De-Mail-Adressen anzubieten. Diese werden durch einen Zusatz besonders gekennzeichnet – z. B. „ps_hansi@providerxy.de-mail.de“.

6. Ist aus datenschutzrechtlichen Gründen vorgesehen, dass unter dem System De-Mail auch neue E-Mail-Adressen kreiert werden können?

Ja, so genannte pseudonyme Adressen, siehe Antwort zu Frage 5.

7. Werden die den De-Mail-Adressen zugrunde liegenden E-Mail-Adressen der teilnehmenden Bürgerinnen und Bürger, falls ja, an welcher Stelle, gespeichert?

Wie in Antwort zu Frage 5 dargelegt, gibt es keine „den De-Mail-Adressen zugrunde liegenden E-Mail-Adressen“.

8. Werden die De-Mail-Adressen der Bürgerinnen und Bürger generell oder in bestimmten Fällen mit Melderegisterdaten in Verbindung gebracht, abgeglichen, verknüpft oder im Melderegister gespeichert?

Es gibt keinen automatischen oder verpflichtenden Eintrag von De-Mail-Adressen in ein Melderegister. Die derzeitigen Überlegungen sehen lediglich vor, dass Bürgerinnen und Bürger ihre De-Mail-Adresse freiwillig in ein Melderegister eintragen lassen können.

9. Soll die Kommunikation mit dem nach der EU-Dienstleistungsrichtlinie erforderlichen einheitlichen Ansprechpartner oder mit Behörden generell ausschließlich über De-Mail möglich sein, bzw. ist geplant, eine Umstellung auf die ausschließliche Nutzung dieses Dienstes zu welchem Zeitpunkt vorzunehmen?

Eine ausschließliche Nutzung der De-Mail im Rahmen der EU-Dienstleistungsrichtlinie mit den einheitlichen Ansprechpartnern oder mit Behörden ist nicht geplant.

10. Falls ja, welche Kosten entstehen hierdurch bei Unternehmen im In- und Ausland?

Entfällt

11. Welche Überlegungen hat die Bundesregierung dahingehend angestellt, dass mit der Erforderlichkeit einer Teilnahme am De-Mail-System für die Kommunikation mit Behörden statt der Weiternutzung bestehender sicherer elektronischer Kommunikationswege die Teilnahme an E-Government-Services erschwert statt erleichtert wird?

Für die Kommunikation mit Behörden ist eine Teilnahme am De-Mail-System nicht verpflichtend. De-Mail ist ein möglicher Kanal für die Kommunikation von Bürgerinnen und Bürgern mit Wirtschaft und Verwaltung, der aufgrund seiner definierten Sicherheit, Einfachheit und Einheitlichkeit die Teilnahme an E-Government-Services erheblich erleichtern wird.

12. Welche Kosten entstehen für den einzelnen Nutzer von De-Mail, z. B. für die Erlangung der Adresse, Speicherplatz auf den Servern u. a. im virtuellen Dokumentensafe etc.?

Die genauen Preise wird jeder Anbieter individuell im Wettbewerb um die Kunden festlegen. Da es auch den De-Mail-Providern darum geht, möglichst viele Kunden zu akquirieren, ist davon auszugehen, dass die Preismodelle auch für Bürgerinnen und Bürger attraktiv sein werden.

13. Ist geplant, dass allen Bürgerinnen und Bürgern automatisch De-Mail-Adressen zugewiesen werden, ggf. bei Ausstellung des elektronischen Personalausweises?

Nein

14. Wurde durch das Bundesamt für Sicherheit in der Informationstechnologie (BSI) oder eine andere staatliche Institution bereits ein Sicherheitsprofil erstellt, das die grundlegenden Anforderungen an den allgemeinen mobilen Datenverkehr innerhalb von oder zwischen staatlichen Institutionen definiert, und wenn ja, wie ist dieser ausgestaltet worden?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Sicherheitsprofil für mobile Synchronisationsdienste erstellt, welches Sicherheitsanforderungen spezifiziert, um u. a. E-Mails zwischen Behördennetzen und mobilen Endgeräten sicher synchronisieren zu können.

15. Falls solch ein Standard noch nicht erarbeitet wurde, wann rechnet die Bundesregierung mit einer entsprechenden Vorlage?

Auf die Antwort zu Frage 14 wird verwiesen.

16. Plant die Bundesregierung die Entwicklung einer eigenen Lösung für den mobilen Datenverkehr?

Nein, die Bundesregierung beauftragt keine eigenen Entwicklungen, sondern beschafft gemäß der jeweiligen (Sicherheits-)Anforderungen der Behörden Lösungen am Markt.

17. Falls ja, welche Kosten werden dafür veranschlagt, und wann soll die entsprechende Lösung verfügbar sein?

Auf die Antwort zu Frage 16 wird verwiesen.

18. Welche wettbewerblichen Konsequenzen für an „De-Mail“ teilnehmende und entsprechend zertifizierte Provider erwartet die Bundesregierung?

Die Möglichkeit, sich akkreditieren zu lassen, steht jedem interessierten Unternehmen offen. Die zukünftigen akkreditierten De-Mail-Provider werden miteinander im Wettbewerb um De-Mail-Kunden stehen. Um beispielsweise die Interoperabilität ihrer Dienste zu sichern, müssen sie auf bestimmten Ebenen zusammenarbeiten.

19. Wie wird das Zertifizierungsverfahren ausgestaltet, und wer entscheidet über die Zulassung von Providern?

Soweit möglich setzt das geplante Zertifizierungsverfahren auf bestehende Verfahren auf und ergänzt sie um dienstspezifische Besonderheiten. Das BSI veröffentlicht in Form Technischer Richtlinien die zu erfüllenden Zertifizierungskriterien hinsichtlich Funktionalität, Interoperabilität und IT-Sicherheit und nimmt in dem Bereich die Zertifizierung vor. Von Bund oder Ländern anerkannte Auditoren überprüfen die Erfüllung dieser Zertifizierungskriterien im Bereich Daten- und Verbraucherschutz. Konnten alle erforderlichen Zertifizierungen vom De-Mail-Provider erfolgreich abgeschlossen werden, wird er auf Antragstellung und Vorlage der erforderlichen Nachweise von der zuständigen Behörde, entsprechend dem Entwurf zum Bürgerportalgesetz das BSI, akkreditiert und kann damit seinen De-Mail-Betrieb aufnehmen. Die Akkreditierung muss regelmäßig erneuert werden.

20. Ist geplant, neben dem üblichen Rechtsweg ein Schlichtungsverfahren für Provider einzuführen, denen die Zertifizierung für „De-Mail“ versagt wird?

Das Zertifizierungsverfahren orientiert sich an den heute üblichen Verfahren für die Sicherheitszertifizierung (z. B. nach Common Criteria oder gemäß ISO 27001 auf Basis von IT-Grundschutz). Die Akkreditierung von De-Mail-Providern obliegt der zuständigen Behörde. Ein eigenes Schlichtungsverfahren ist nicht geplant.

21. Ist die Bundesregierung der Ansicht, dass sie angesichts des von ihr in dieser Wahlperiode massiv ausgeweiteten Telekommunikations-Überwachungsregimes sowie der verschärften Vorratsdatenspeicherungspflichten und der angestrebten erweiterten polizeilichen Ermittlungsbefugnisse im Onlinebereich durch eine Mehrheit der Bürger als vertrauenswürdiger Ansprechpartner in Angelegenheiten elektronischer Kommunikation angesehen wird?

Bei De-Mail handelt es sich um eine sichere dezentrale Lösung, die von staatlich zertifizierten und akkreditierten Providern aus der Privatwirtschaft bereitgestellt wird. Der Staat schafft einen rechtlichen Rahmen und die regulatorischen Voraussetzungen für eine vertrauenswürdige elektronische Kommunikation für alle. Eine Zertifizierung der einzelnen Dienste und Komponenten der De-Mail-Provider ermöglicht geprüfte statt nur geglaubte Sicherheit, hebt das Sicherheits- und Datenschutzniveau, garantiert die weitgehende Einheitlichkeit der Dienste und fördert die Transparenz. Bürgerinnen und Bürger können deshalb zu Recht Vertrauen in die neue Infrastruktur haben. Zudem haben sie die Möglichkeit, sich einen De-Mail-Provider ihres Vertrauens auszuwählen.

22. Welche Funktion soll der mit De-Mail geplante virtuelle Dokumentensafe haben?

Akkreditierte De-Mail-Provider können einen zertifizierten virtuellen Dokumentensafe („De-Safe“) anbieten, damit ihre Kundinnen und Kunden De-Mails und andere elektronische Dokumente langfristig, sicher und vertraulich ablegen können. Ein De-Safe ist immer eindeutig einem De-Mail-Konto zugeordnet und gestattet nur Zugriffe durch den Inhaber dieses Kontos.

23. Wozu ist dieser erforderlich, und was spricht dagegen, Dokumente per De-Mail jeweils an den Empfänger zu schicken statt diese auf einen Server hochzuladen und dort liegen zu lassen?

Die Konzeption sieht genau diese Variante vor, nämlich Dokumente per De-Mail jeweils an den Empfänger zu versenden und keineswegs auf einem Server (De-Safe) zum Download zur Verfügung zu stellen. Damit dient der De-Safe lediglich der sicheren Ablage eigener Dokumente – ohne Zugriffsmöglichkeiten durch Dritte.

24. Wie bewertet die Bundesregierung die Akzeptanz eines derartigen virtuellen Dokumentensafes bei den Bürgerinnen und Bürgern wie auch bei Unternehmen angesichts des allgemeinen Vertrauens in staatliche Datensicherheit, einmal vor dem Hintergrund aktueller Datenschutzskandale z. B. bei Meldedaten und zum anderen vor dem Hintergrund der zunehmenden Überwachungsbefugnisse und -maßnahmen von Sicherheitsbehörden?

Die De-Safes befinden sich bei den privaten De-Mail-Providern. Ein staatliches Zertifizierungsverfahren hinsichtlich IT-Sicherheit und Datenschutz gewährleistet geprüfte Sicherheit und Vertraulichkeit und erhöht das Vertrauen in die privaten Provider. Dieses Konzept bietet gute Voraussetzungen für Akzeptanz bei Bürgerinnen und Bürgern.

25. Gibt es vergleichbare Systeme in anderen Staaten, insbesondere der EU, und wie sind gegebenenfalls die Erfahrungen damit?

In anderen Ländern gibt es – wie in Deutschland auch – eine Reihe von Ansätzen, die sich auf die elektronische Kommunikation bestimmter Zielgruppen beschränken, z. B. zwischen oder mit Behörden bzw. zwischen großen Unternehmen. Ein übergreifender Ansatz wie bei der De-Mail, bei dem es um die elektronische Kommunikation zwischen Bürgerinnen und Bürgern, Wirtschaft und Verwaltung geht, ist nicht bekannt.

26. Falls nein, welche Probleme könnten bei der Umsetzung der EU-Dienstleistungsrichtlinie für die Bundesrepublik Deutschland entstehen, wenn Unternehmen oder natürliche Personen aus dem EU-Ausland nicht auf dem üblichen elektronischen Kommunikationsweg an die Behörden herantreten können, sondern erst Teilnehmer von De-Mail werden müssen?

Die üblichen elektronischen Kommunikationswege wie besonders E-Mail sind für die Kommunikation im Rahmen der EU-Dienstleistungsrichtlinie nur bedingt bis gar nicht geeignet. De-Mail bietet für die elektronische Kommunikation mit den einheitlichen Ansprechpartnern im Rahmen der EU-DLR – im Gegensatz zu z. B. normaler E-Mail – erhebliche Vorteile. Ein verpflichtender Einsatz der De-Mail, um aus dem EU-Ausland mit deutschen Behörden elektronisch kommunizieren zu können, wird daraus nicht abgeleitet.

27. In welcher Weise sind Länder und Kommunen in die Entwicklung von De-Mail eingebunden?

Länder und Kommunen wurden auf vielfältige Weise einbezogen, durch Veranstaltungen und Treffen mit Vertretern von Ländern und Kommunen, sowie durch den Austausch mit der OSCI-Leitstelle in Bremen, dem Deutschen Städtetag, Vitako, der Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e. V. Darüber hinaus werden sich die spezifischen kommunalen Anforderungen durch die Pilotierung der De-Mail in der Region Friedrichshafen nachhaltig im Projekt niederschlagen.

28. Welche Kosten entstehen bei den Kommunen für die Implementierung der notwendigen technischen Infrastrukturen zur Nutzung von De-Mail durch ihre Behörden?

Um an De-Mail teilzunehmen, kann sich eine Behörde/eine Stadt bei einem Provider einen Account für juristische Personen einrichten, der selbst Unterpostfächer für z. B. verschiedene Abteilungen, Referate oder auch Mitarbeiter enthalten kann. Bei der Behörde ist die Implementierung eines Gateways erforderlich, das in einer einfachen Version als Open-Source-Software bereitgestellt werden soll. Auf den Arbeitsplatzrechnern der Mitarbeiter ist i. d. R. keine zusätzliche Software nötig, da auf die bestehende E-Mail-Infrastruktur zurückgegriffen werden kann.

Im laufenden Betrieb fallen für die De-Mail-nutzenden Behörden voraussichtlich Kosten für den Versand von De-Mails an, ggf. können auch Flat-Rates zwischen Behörde/Stadt/Land und dem Provider vereinbart werden. Die Höhe dieser Kosten wird unter Marktbedingungen zwischen Provider und Nutzer vereinbart.

Durch De-Mail ergeben sich erhebliche Porto- und Prozesskosteneinsparungen, weil in der Kommunikation mit dem Bürger teure Medienbrüche in erheb-

lichem Ausmaß vermieden werden können. Werden nur 8 bis 9 Prozent der Papierpost in der öffentlichen Verwaltung durch De-Mail abgelöst, ergibt sich ein Einsparvolumen von 100 bis 150 Mio. Euro pro Jahr.

29. Welche Kosten entstehen insbesondere für das Vorhalten von Speicherplatz für den virtuellen Dokumentensafe?

Es ist nicht anzunehmen, dass Behörden De-Mails oder elektronische Dokumente in großem Umfang in ihren De-Safes bei De-Mail-Providern speichern werden. Dieser Dienst richtet sich vornehmlich an Bürgerinnen und Bürger bzw. kleinere Organisationen, die selbst eine langfristige und sichere Speicherung nicht gewährleisten können.

30. Welche rechtlichen Rahmenbedingungen werden für die Nutzung von De-Mail für die Bürgerinnen und Bürger, die den Service nutzen, gelten, insbesondere im Hinblick auf Haftungsfragen bei Verlust von Passwörtern, die die Integrität z. B. des virtuellen Dokumentensafes gefährden können?

Über die allgemeingültigen Regelungen hinaus wird voraussichtlich eine spezifische Haftungsregelung festgelegt, die derzeit noch abgestimmt wird.

31. Welche Sicherheit für im virtuellen Dokumentsafe gespeicherte Daten gegen Datenverlust und zum Schutz von deren Vertraulichkeit und Integrität sollen im Rahmen von De-Mail getroffen werden?

Die Dokumente im De-Safe werden standardmäßig verschlüsselt abgelegt und nur bei Abruf durch den (authentifizierten) Nutzer durch den De-Mail-Provider entschlüsselt. Durch organisatorische Maßnahmen, die entsprechend zertifiziert werden müssen, wird gewährleistet, dass der Provider nicht unberechtigterweise auf die Daten des Nutzers zugreifen kann. Bei Bedarf kann der Nutzer auch einzelne, alle oder bestimmte Kategorien seiner Dokumente zusätzlich clientseitig verschlüsseln und im De-Safe ablegen.

32. Plant die Bundesregierung gesetzgeberische Schritte, die das Vorhaben flankieren, insbesondere im Hinblick auf die teilnehmenden Telekommunikationsprovider auf der einen, die Behörden auf der anderen Seite, und wenn ja, welche?

Das Vorhaben wird durch gesetzgeberische Schritte begleitet mit dem Ziel, für die potentiellen Diensteanbieter Rechtssicherheit zu schaffen und ihnen zu ermöglichen, die Rechtsqualität der Dienste (gleichbedeutend mit De-Mail-Diensten) im Internet zu steigern. Außerdem sind Änderungen des Zustellrechts geplant.

33. Welche Aussagen zur Zukunftssicherheit und Nachhaltigkeit von De-Mail kann die Bundesregierung vor dem Hintergrund der schnellen technischen Weiterentwicklung treffen?

Die Konzepte werden den aktuellen Entwicklungen angepasst. Damit werden auch die Zertifizierungskriterien für IT-Sicherheit, Interoperabilität, Datenschutz und Funktionalität regelmäßig aktualisiert.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333