Die Virtuelle Poststelle im datenschutzgerechten Einsatz

An der Ausarbeitung der Handreichung „Die Virtuelle Poststelle im datenschutzgerechten Einsatz“ waren Dr. Christian Mrugalla und Andreas Schmidt (beide Bundesamt für Sicherheit in der Informationstechnik (BSI)), Dr. Sönke Maseberg (datenschutz nord GmbH), Wolfgang Farnbacher (Informatikzentrum Niedersachsen (IZN), Manfred Malzahn (Nds. Landkreistag), Christoph Sturm (Niedersächsischer Städte und Gemeindebund), Ulrich Mahner (Nds. Städtetag), Harald Hogrefe (Niedersächsisches Ministerium für Inneres und Sport), Iris Metge (Stadt Garbsen), Burckhard Nedden (Landesbeauftragter für den Datenschutz Niedersachsen) und Thomas Knaak (Projektleiter eGovernment in der Geschäftsstelle des Landesbeauftragten für den Datenschutz Niedersachsen) beteiligt. Begleitet wurden die Arbeiten durch die von der Konferenz der Datenschutzbeauftragen des Bundes und der Länder eingesetzte Arbeitsgruppe „eGovernment“. Die Leitung der Arbeitsgruppe lag bei dem Landesbeauftragten für den Datenschutz Niedersachsen.

Ansprechpartner ist Thomas Knaak (thomas.knaak@lfd.niedersachsen.de).

Herausgeber: Landesbeauftragter für den Datenschutz Niedersachsen
Brühlstr. 9, 30169 Hannover
Postfach 2 21, 30002 Hannover

Verantwortlich: Burckhard Nedden

Umschlagslayout: set-up design.print.media
An der Markuskirche 1, 30163 Hannover

Druck: Schlütersche Druck GmbH & Co. KG
Hans-Böckler-Straße 52, 30851 Langenhagen

Hannover, den 22.November 2004

Zur besseren Lesbarkeit wird bei verallgemeinernden Substantiven lediglich das bestimmende grammatische Geschlecht verwendet. Selbstverständlich richtet sich dieser Text an die Angehörigen beider Geschlechter.

Inhaltsverzeichnis

1 Vorwort 1

2 Elektronische Kommunikation im Verwaltungsverfahren 1

3 VPS – Was verbirgt sich dahinter? 2

4 Neue Organisationsformen, Erfordernisse von Kooperationen 3

5 Rechtsrahmen und datenschutzrechtliche Einordnung 4

5.1 Unterschiedliche Rechtsbereiche und Rechtsrahmen 4
5.2 Personenbezogene Daten 6
5.2.1 Bestandsdaten 6
5.2.2 Nutzungsdaten 7
5.2.3 Verkehrsdaten 7
5.2.4 Inhaltsdaten 7
5.3 Datenschutzrechtliche Einordnung der VPS und ihrer Funktionen: Telekommunikation oder Teledienst? 7
5.3.1 Betrieb der VPS durch die öffentliche Stelle selbst 7
5.3.2 Betrieb der VPS durch Dritte 8

6 IT-Sicherheitsziele und Sicherheitsmechanismen 11

7 Funktionale Anforderungen 13

7.1 Funktionale Anforderungen an die VPS des Bundes 14
7.1.1 Grundfunktionalitäten zur Behandlung ein- und ausgehender Daten 15
7.1.2 Funktionen zur Behandlung der in die Behörde eingehenden Daten 17
7.1.3 Funktionen für Anwendungen und Backendsysteme 17
7.1.4 Funktionen zur Verifikation von Signaturen 17
7.1.5 Funktionen zur Authentisierung von Benutzern 17
7.1.6 Funktionen zur Administration der VPS 17
7.1.7 Funktionen zur Prüfung und Nutzung von Zertifikaten 18
7.2 Weitere denkbare funktionale Anforderungen 18
7.2.1 Einbindung von Contentscannern, z. B. zum Blockieren unerwünschter Inhalte 18
7.2.2 Führung eines eigenen Verzeichnisdienstes der externen Kommunikationspartner 18
7.2.3 Interner Zertifikatsverzeichnisdienst 19
7.2.4 Weiterleitung von Eingangsnachrichten an fachlich zuständige Stellen, etwa anhand formaler Kriterien oder inhaltlicher Auswertungen 19
7.2.5 Weitergehende Workflowfunktionalitäten, etwa zur Abbildung von Mitzeichnungsketten (Mehrfachsignaturen) 19
7.3 Komponenten der VPS (Architekturmodell) 20

8 Anforderungen und Handlungsempfehlungen zur Gewährleistung von Datenschutz und Datensicherheit 22

8.1 Herstellung von Vertraulichkeit, Verschlüsselung/Entschlüsselung 22
8.2 Signaturbildung/Signaturprüfung 25
8.3 Bereitstellen von Zeitstempeln, Zeitstempelprüfung 27
8.4 Prüfung auf schädliche Inhalte 28
8.5 Contentprüfung 28
8.6 Authentisierung des Kommunikationspartners 29
8.7 Speicherung der Authentisierungsdaten und Zertifikate der Kommunikationspartner 30
8.8 Generierung eines Laufzettels 31
8.9 Erstellung von Eingangs- und Ausgangsbestätigungen und Behandlung fehlerhafter Vorgänge 31
8.10 Einbindung in Anwendungen 32
8.11 Behandlung von Protokolldaten 32
8.11.1 Protokollierung von IP-Adressen 32
8.11.2 Grenzen der Protokollierung 33
8.11.3 Empfehlungen zur Gestaltung und Verwendung 33
8.12 Anforderungen an ein zentrales OCSP/CRL-Relay 33

9 Notwendige Begleitmaßnahmen 35

9.1 Vorabkontrolle, Einführungskonzept, Dienstvereinbarung/Dienstanweisung 35
9.1.1 Phase 1: Initialisierung 36
9.1.2 Phase 2: Kommunikationsstrategie 36
9.1.3 Phase 3: Analyse einschl. Schutzbedarfsfeststellung 37
9.1.4 Phase 4: Konzeption 38
9.1.5 Phase 5: Realisierung 42
9.1.6 Phase 6: Einführung und Inbetriebnahme 42
9.2 Gestaltung des Sicherheitskonzeptes (Systemdatenschutz) 42
9.3 Dienstvereinbarung / Dienstanweisung 43

10 Betreibermodelle und deren inhaltliche Ausgestaltung 45

10.1 Rollen der VPS 46
10.1.1 Rolle als OSCI-Intermediär 46
10.1.2 Rolle als Operator 46
10.1.3 Rolle als Geschäftsstelle 47
10.2 Vertragliche Anforderungen zum Outsourcing 47

11 Anforderungen und Handlungsempfehlungen zur Gewährleistung von Datenschutz und Datensicherheit eingeführter Anwendungsszenarien 48

11.1 Externer Mail-Benutzer sendet eine E-Mail 48
11.2 Interner Mail-Benutzer sendet eine E-Mail 49
11.3 Externer Browser- oder Anwendungsbenutzer stellt ein Dokument ein 50
11.4 Interner Browser- oder Anwendungsbenutzer stellt ein Dokument ein 51
11.5 Authentisierung eines externen oder internen Browser-Benutzers 51
11.6 Externer oder interner Browser-Benutzer verifiziert ein Dokument 52

11.7 Authentisierung eines externen oder internen Anwendungsbenutzers 52
11.8 Externer oder interner Anwendungsbenutzer verifiziert ein Dokument 53
11.9 Backend-System lässt ein Dokument bearbeiten 53

12 Pilotprojekte/ erste Praxiserfahrungen 54

12.1 BundOnline 2005 54
12.1.1 Leistungsumfang 55
12.1.2 Realisierungsstand 56
12.1.3 Piloten 57
12.1.4 Datenschutz 57
12.1.5 Ansprechpartner 58
12.2 NRW 58
12.3 Niedersachsen 59
12.4 Bremen 60

13 Wichtige Links 60

14 Schlagworte und Abkürzungen 61

14.1 OCSP 61
14.2 CRL 61
14.3 OSCI 61
14.4 LDAP 61
14.5 SSL-Verschlüsselung 61
14.6 Verwaltungsdatenschutzrecht 61
14.7 Signatur/Verschlüsselung 62
14.8 XML 62
14.9 (IT-)Sicherheitsziele 62
14.10 Public-Key-Infrastructure (PKI) 62

1 Vorwort

Diese Handreichung stellt die datenschutzrechtlichen und -technischen Anforderungen, die zu beachtenden Sicherheitsaspekte und die Architektur der Virtuellen Poststelle (VPS) als Basiskomponente des eGovernment vor. Wir möchten mit dieser Handreichung alle diejenigen erreichen, die in den Verwaltungen an zentraler Stelle als Verwaltungschefs, als Organisatoren, als Verfahrensentwickler, als IT-Verantwortliche, als interne Datenschutzbeauftragte oder als Personalvertretungen den Weg ins eGovernment vorbereiten oder schon umsetzen. Wir wenden uns aber natürlich auch an alle, die in den Verwaltungen mit eGovernment-Anwendungen aktuell oder künftig arbeiten und an die Wirtschaftsunternehmen und an die anderen „Kunden“ der Verwaltung, die die neuen Angebote im eGovernment nutzen. Die folgenden Ausführungen gehen ausschließlich von einer dienstlichen Nutzung der VPS aus.

Beschluss der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 29.10.2004

Die Datenschutzkonferenz nimmt die Handreichung „Die Virtuelle Poststelle im datenschutzgerechten Einsatz“ zur Kenntnis und sieht darin eine wichtige Grundlage für die Förderung von eGovernment-Anwendungen in der Verwaltung.

2 Elektronische Kommunikation im Verwaltungsverfahren

Mit der Novellierung des Verwaltungsverfahrensgesetzes des Bundes vom August 2002 wurde der juristische Boden für das eGovernment in der Form des elektronischen Verwaltungsverfahrens bereitet. Die Voraussetzungen für die Nutzung elektronischer Nachrichten in der öffentlichen Verwaltung sind geschaffen, soweit nicht gesetzliche Ausnahmen zugelassen worden sind. Formvorschriften stehen dem Einsatz von E-Mail, Signatur & Co. nicht mehr entgegen. Nach den novellierten Regelungen erfüllen elektronische Dokumente eine gesetzlich geforderte Schriftform, wenn sie mit einer so genannten qualifizierten elektronischen Signatur versehen sind.

Die Möglichkeit der elektronischen Kommunikation im Verwaltungsverfahren wird davon abhängig gemacht, dass der Empfänger einen „Zugang“ eröffnet hat. Die Zugangseröffnung erstreckt sich sowohl auf die elektronische Form selbst wie auf andere technische Rahmenbedingungen der Kommunikation, zu denen beispielsweise die zu verwendenden Dateiformate und Signaturverfahren gehören. Fast alle öffentlichen Stellen und Firmen verfügen über die technische Ausstattung und haben einen Zugang i. S. des Verwaltungsverfahrensgesetzes eröffnet. Indem sie in ihren Informationsangeboten im Internet bzw. auf ihren Briefköpfen E-Mail-Adressen angeben, haben sie ihre Teilnahme am elektronischen Rechtsverkehr konkludent erklärt. Bei den Bürgerinnen und Bürgern sowie bei kleineren Firmen kann dies mit der bloßen Be-

kanntgabe der E-Mail-Adresse nicht vorausgesetzt werden, da die dauerhafte Gewährleistung der technischen Rahmenbedingungen viele etwa bei der Um- und Aufrüstung ihrer Computer überfordern würde.

Es ist jedoch zu erwarten, dass - unabhängig vom Umfang der tatsächlichen Nutzung - kurzfristig die Erwartung an die öffentlichen Stellen herangetragen wird, auch für bisher in Schriftform einzureichende Dokumente einen Zugang für die elektronische Kommunikation zu eröffnen. Die Eröffnung dieses Zugangs setzt erhebliche technische und organisatorische Maßnahmen voraus, um einen angemessenen Datenschutz und die erforderliche Datensicherheit zu gewährleisten. Nur wenn eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz der personenbezogenen Daten gewährleistet ist, wird auch die notwendige Akzeptanz auf Seiten der Bürgerinnen und Bürger sowie der anderen „Kunden“ der Verwaltung zu erreichen sein.

Für das Ver- und Entschlüsseln ein- und ausgehender Informationen, für die Signaturprüfung bei rechtserheblichen Dokumenten oder für die Prüfung auf schädliche Inhalte sind eine aufwändige technische Ausstattung, neuartige Programme und umfangreiches rechtliches und technisches Know-how erforderlich. Würde man dies alles dezentral auf allen Arbeitsplätzen in den Verwaltungen, die am elektronischen Rechtsverkehr teilnehmen, vorhalten, ergäbe sich ein völlig unvertretbarer und wohl auch kaum leistbarer finanzieller und kapazitativer Aufwand für Beschaffungen, Pflege und Wissensvermittlung. Daher ist es zwingend geboten, Möglichkeiten für eine Zentralisierung dieser Sicherheitsfunktionen zu entwickeln, die organisatorisch am ehesten mit Funktionen der bisherigen analogen Posteingangsstellen vergleichbar sind. Für öffentliche Stellen stellt die VPS eine Lösung dar.

Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer Handreichung „Datenschutzgerechtes eGovernment“ erste umsetzungsorientierte Handlungsempfehlungen für die Abwicklung der elektronischen Bürgerkontakte über eine zentrale Stelle gegeben. Der Text der Handreichung ist im Internet unter der Adresse www.lfd.niedersachsen.de oder www.datenschutz.de verfügbar.

Die jetzt vorgelegte Handreichung will dazu beitragen, dass bei der Entwicklung und dem Einsatz einer VPS die Anforderungen von Datenschutz und Datensicherheit im Blick bleiben, und praktische Hinweise dafür geben, wie diese Anforderungen in datenschutzgerechte und datenschutzfreundliche Anwendungen umgesetzt werden können.

3 VPS – Was verbirgt sich dahinter?

Der Betrieb einer VPS erleichtert die Abwicklung einer sicheren, nachvollziehbaren und vertraulichen Kommunikation innerhalb der Behörden sowie zwischen Behörden und externen Kommunikationspartnern. Eine VPS ist damit im Rahmen des eGovernments eine Basiskomponente zur Kommunikationssicherheit mit Querschnittsfunktionalität. Sie stellt über standardisierte Schnittstellen Sicherheitsdienste bereit für die gesicherte Kommunikation zwischen Behörden und externen Kommunikations-

partnern wie Bürgern, Wirtschaft und anderen Behörden und fungiert als zentrales Security-Gateway, welches die Funktionen Authentifizierung, Signaturprüfung und Signaturerstellung sowie Ent- und Verschlüsselung bereitstellt. Die Adressierung der Dokumente erfolgt über deren Zertifikatsdaten oder andere Metainformationen, die eine Weiterleitung an die zuständige Stelle (z. B. Sozialamt, Meldeamt) ermöglichen.

Als Kommunikationskanäle unterstützt die VPS sowohl E-Mail als auch Web-Anwendungen einschl. der Web-Mail-Anwendungen. Weiterhin bedient sie Schnittstellen zu Workflow-, Dokumentenmanagement- und Archiv-Systemen sowie auch zu Fachverfahren. Einbezogen wird insbesondere der vermittelte Austausch von Informationen/Dokumenten mit hohen Anforderungen an Integrität, Authentizität und Vertraulichkeit der Inhalte. Während der Übermittlung kann eine vermittelnde Stelle Mehrwertdienste (z. B. Signaturprüfung, Zeitstempel) erbringen, ohne die Vertraulichkeit zu verletzten. Die Kommunikation ist symmetrisch: jeder Kommunikationspartner kann außer in der Rolle des Senders auch als Empfänger auftreten.

Von der VPS sind die Funktionalitäten einer „Elektronischen Poststelle“ abzugrenzen. In der „Elektronischen Poststelle“ werden die herkömmliche Eingangspost in elektronische Dokumente und ausgehende elektronische Dokumente ggf. wieder in herkömmliche Schriftstücke transformiert. Dies ist für den Aufbau einer elektronischen Akte unerlässlich, sofern eine durchgängig elektronische Kommunikation und Aktenführung nicht möglich ist. Ausführungen zur „Elektronischen Poststelle“ sind allerdings nicht Gegenstand dieser Ausarbeitung.

Wie vor jeder Einführung einer eGovernment-Anwendung bedarf es auch bei der VPS einer Kommunikationsstrategie der öffentlichen Stelle. Hier gilt es schriftlich festzustellen und festzulegen, wann eine Ende-zu-Ende-Kommunikation und wann eine behörden- oder funktionsbezogene Kommunikation erforderlich ist.

4 Neue Organisationsformen, Erfordernisse von Kooperationen

Während in der Vergangenheit das Leitbild des Ordnungsstaates prägend war, hat sich immer mehr das Bild des aktivierenden und gewährleistenden Staates herausgebildet. Zugleich werden immer mehr Aufgaben aus der staatlichen Obhut in private Hände gelegt. Private Stellen nehmen Aufgaben wahr, welche bisher zum staatlichen Tätigkeitsfeld gehören. Dabei baut der öffentliche Sektor vollständig ab und überlässt sie anderen Trägern. Z. B. können die Aufgaben einer VPS auch durch Qutsourcing (Auftragsdatenverarbeitung oder Funktionsübertragung) durchgeführt werden.

Daneben schaffen neue Kooperationsformen intensive Verknüpfungen zwischen einer Vielzahl von Behörden, Verwaltungsträgern und sonstigen Einrichtungen im öffentlichen Sektor (Kooperierende Verwaltung). Völlig neuartige Kooperationen über Entfernungen und Organisationsgrenzen hinweg werden unter anderem die Ansiedlung und Auslastung von Spezialisten von den Beschränkungen lösen, die sich heute aus der Größe der Verwaltungsbehörden und ihrer Einzugsgebiete ergeben. Verwaltungen werden sich darüber hinaus mit Unternehmen in Netzwerken organisieren.

Diese Form der Kooperation (Public-Private-Partnerships) eröffnet neue Möglichkeiten der Aufspaltung von Prozessen auf unterschiedliche Bearbeitungsinstanzen.

Bei der Wahl einer geeigneten und ggf. verselbstständigten Organisationsform für eine VPS und für die von ihr zu leistenden Dienstleistungen geht es um die Frage der organisatorischen Ausgestaltung der Gesamtverantwortlichkeit für den Aufbau und Betrieb. Dabei stehen unterschiedliche rechtliche Formentypen des öffentlichen und des privaten Rechts zur Verfügung. In Betracht kommt der Betrieb in öffentlich-rechtlicher Organisationsform, in privatrechtlicher Organisationsform mit öffentlicher Beteiligung, ein vollständig privater Betrieb oder eine Organisationsform unter Berücksichtigung interner Zusammenarbeit (z. B. kommunale Arbeitsgemeinschaften/Datenzentralen). Die Wahl des konkreten Organisationsmodells hängt von Zweckmäßigkeits- und Rechtmäßigkeitserwägungen ab. Je stärker aber eine Lösung unter Integration Privater im Vordergrund steht, um so mehr liegt die Verselbstständigung des Betriebs der VPS in einer privatrechtlichen Organisationsform nahe, ggf. unter Einbindung Privater bzw. ein vollständiger privater Betrieb.

Organisationsformen	
Öffentlich-rechtliche	**Privatrechtliche**
• Regiebetrieb/Eigenbetrieb • Kommunale Arbeitsgemeinschaften/öffentlich-rechtliche Vereinbarungen oder Zweckverband mit anderen öffentlichen Stellen	• Eigengesellschaft mit anderen öffentlichen Stellen • Gemischtwirtschaftliches Unternehmen mit privaten Dritten • vollständig privater Betrieb

Bei der Auswahl ist auch der Grundsatz der Wirtschaftlichkeit und Sparsamkeit zu beachten. Dabei ist auch die Möglichkeit einer z. B. interkommunalen Zusammenarbeit einzubeziehen.

5 Rechtsrahmen und datenschutzrechtliche Einordnung

Dem Datenschutz kommt die Aufgabe zu, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Dabei müssen vor allem die verfassungsrechtlich unverzichtbaren Prinzipien der Zweckbindung, der Erforderlichkeit, der Datenvermeidung und Datensparsamkeit, der Transparenz sowie die Kontroll- und Korrekturrechte der Betroffenen realisiert werden (siehe hierzu „Datenschutzgerechtes eGovernment“ Kapitel 3 ff. – www.lfd.niedersachsen.de).

5.1 Unterschiedliche Rechtsbereiche und Rechtsrahmen

Für die datenschutzrechtliche Bewertung sind aufgrund der Besonderheiten des deutschen Datenschutzrechts jedoch grundsätzlich drei unterschiedliche Rechts-

bzw. Regelungsbereiche für die Kommunikation **außerhalb** einer öffentlichen Stelle zu beachten.

- **Inhaltsebene:** Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für Verwaltungszwecke unterliegt dem Verwaltungsdatenschutzrecht (2. Abschnitt des BDSG bzw. Landesdatenschutzgesetze). Dieses unterscheidet nicht danach, in welcher Form und auf welchem Weg z. B. eine Verwaltungsauskunft erteilt wird. Auch für die VPS sind somit alle Anforderungen an die Offline-Auskunft zu beachten. Für die Landes- und Kommunalverwaltung gelten grundsätzlich die Regelungen der Landesdatenschutzgesetze, für die Bundesverwaltung die Regelungen des Bundesdatenschutzgesetzes. Diese sind jedoch gegenüber bereichsspezifischen Datenschutzregelungen subsidiär.
- **Transportbehälterebene:** Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für den Zweck, die Kommunikation über das Internet zu ermöglichen, unterliegt dem Online-Datenschutzrecht. Dies gilt aber nur für die Datenverarbeitung, die erfolgt, um diese spezifische Form der Kommunikation zu ermöglichen. Für das Online-Datenschutzrecht enthalten das TDG und TDDSG ausführliche bereichsspezifische Regelungen zum Datenschutz, die für ihren Anwendungsbereich den Landesdatenschutzgesetzen und dem Bundesdatenschutzgesetz vorgehen.
- **Transportebene:** Um über das Internet Informationen zu erhalten, muss eine Telekommunikationsverbindung zwischen dem Anfragenden und dem Auskunftsserver aufgebaut werden. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für das Herstellen und Aufrechterhalten von Telekommunikationsverbindungen unterliegt dem Telekommunikationsdatenschutzrecht. Von dem inhaltlichen Informations- und Kommunikationsangebot ist der technische Telekommunikationsvorgang, der das Übermitteln von Signalen ermöglicht, zu unterscheiden. Die Verwendung personenbezogener Daten, die diesem Zweck dient, ist in § 91 ff. TKG geregelt. Unter das Telekommunikationsrecht fällt der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern und Tönen mittels Telekommunikationsanlagen. Adressat der Regelungen ist aber nur derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt. Nicht erfasst werden vom TKG inhaltliche Aspekte der Kommunikationsbeziehungen der Nutzer der Telekommunikationstechnik. Zu den Telekommunikationsdiensten gehören z. B. der reine E-Mail-Transport und die Internet-Telefonie.

Damit die VPS datenschutzgerecht zum Einsatz kommen kann, ist zu klären, welche der Datenschutzregelungen aus diesen Bereichen konkret zur Anwendung kommen.

Rechtsrahmen der VPS:

Telekommunikationsgesetz (TKG); Teledienstegesetz (TDG-Novelle vom 01.01.2002); Teledienstedatenschutzgesetz (TDDSG-Novelle vom 01.01.2002); Verwaltungsverfahrensgesetz (VwVfG); Signaturgesetz (SigG); Bundesdatenschutzgesetz (BDSG) und länderspezifische Datenschutzgesetze (z. B. NDSG) sowie bereichsspezifische Regelungen; Personalvertretungsrecht; Arbeitschutzgesetz; Bildschirmarbeitsverordnung usw.

5.2 Personenbezogene Daten

Bei der Nutzung der VPS handelt es sich in der Kommunikation mit Dritten (**außerhalb** einer öffentlichen Stelle) rechtlich um die Inanspruchnahme von Telekommunikations- (z. B. der reine Transport von Nachrichten) und Telediensten (z. B. Erteilung einer Eingangsbestätigung durch die Behörde). Dabei fallen - neben den vorgangsbezogenen Daten der Bürgerin oder des Bürgers oder anderer Kunden der Verwaltung - weitere personenbezogene Daten an, die bei der Kommunikation mit der Verwaltung und bei der Vorgangsbearbeitung zur Erledigung von Verwaltungsaufgaben entstehen. Diese personenbezogenen Daten sind im Hinblick auf den Schutzbedarf sowohl einzeln als auch im Gesamtkontext der Anwendung zu bewerten. Wirken verschiedene Stellen bei der VPS mit, ist darauf zu achten, dass die Daten der beteiligten Einrichtungen insgesamt bewertet werden. Die Ausgestaltung der Schutzmaßnahmen muss sich daran orientieren, welche Folgen für einen Betroffenen durch die Beeinträchtigung des Rechts auf informationelle Selbstbestimmung entstehen können und welcher potentielle Schaden für den Betreiber eintreten kann.

Die Kommunikation mit Bürgern, Firmen und Verwaltungen über die VPS erfordert besondere Vorkehrungen in Bezug auf Datenschutz und Datensicherheit. Dabei sind die folgenden rechtlichen Rahmenbedingungen, wie Zweckbindung, Datensparsamkeit und -vermeidung, Berichtigung, Speicherung, Löschung, Freiwilligkeit, Transparenz, Erforderlichkeit, Verhältnismäßigkeit sowie technisch-organisatorische Sicherungen zu beachten.

Die personenbezogenen Daten lassen sich in folgende Datentypen einteilen:

5.2.1 Bestandsdaten

Bestandsdaten sind jene personenbezogenen Angaben, die dem Betroffenen im Rahmen der Vertragsbeziehungen zugeordnet sind. Dazu zählen in erster Line die Daten, die für die Nutzung von angebotenen eGovernment-Anwendungen erforderlich sind. Die Definition dieser Daten ist für die Bereiche der Teledienste und Telekommunikationsdienste identisch. Dies können sein: Name, Anschrift, Adresse, Telefon- oder Telefaxnummer, Geburtsdatum, Bankverbindung, Kreditkartennummer, öffentlicher Schlüssel, User-ID, statische IP-Adressen und ähnliche Angaben. Welche Bestandsdaten im Einzelnen erhoben, verarbeitet oder genutzt werden dürfen, ist im Wesentli-

chen abhängig von der technischen Ausgestaltung der VPS sowie von dem Inhalt der jeweiligen eGovernment-Anwendung.

5.2.2 Nutzungsdaten

Nutzungsdaten sind gem. § 6 Abs. 1 TDDSG Daten, die erforderlich sind, um die Inanspruchnahme von Telediensten zu ermöglichen und diese abzurechnen. Es handelt sich hierbei insbesondere um Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und Angaben über die von den Nutzenden in Anspruch genommenen Teledienste.

5.2.3 Verkehrsdaten

Bei Angeboten, die sich auf die reine Übermittlung von Daten beschränken (z. B. E-Mails), handelt es sich um Telekommunikationsdienste. Die bei der Erbringung dieser Dienste anfallenden Daten sind Verkehrsdaten im Sinne des Telekommunikationsrechts (§ 3 Nr. 30 und § 96 TKG). Verkehrsdaten bei der VPS sind insbesondere E-Mail-Adressen (die auch Bestandsdaten sein können), Zeitpunkte der Sendung bzw. Zustellung und Routing-Informationen (Angaben über diejenigen Rechner, die eine E-Mail durchgeleitet haben). Nicht zu den Verkehrsdaten gehören Angaben mit Bezug zum Inhalt, also auch Bezeichnungen von Datei-Anlagen und sowie der Betreff.

5.2.4 Inhaltsdaten

Die Beurteilung der Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung von Inhaltsdaten bei Telekommunikations- und Telediensten, also der eigentlichen vorgangsbezogenen personenbezogenen Daten, richtet sich nach den Vorschriften des allgemeinen Datenschutzrechts, soweit nicht spezialgesetzliche Regelungen (z. B. die Erhebung von Sozialdaten nach den Vorschriften des Sozialgesetzbuches, Auskünfte zum Meldewesen nach den Meldegesetzen etc.) einschlägig sind. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen ist zusätzlich zu beachten.

5.3 Datenschutzrechtliche Einordnung der VPS und ihrer Funktionen: Telekommunikation oder Teledienst?

Zunächst muss für die datenschutzrechtliche Einordnung danach differenziert werden, ob eine öffentliche Stelle die VPS selbst betreibt oder – ggf. gemeinsam mit anderen Stellen – von Dritten betreiben lässt (siehe dazu Kapitel 4).

5.3.1 Betrieb der VPS durch die öffentliche Stelle selbst

Betreibt die öffentliche Stelle die VPS selbst, so erbringt sie gegenüber den Nutzern (Bürger, Unternehmen usw.) weder einen Telekommunikations- noch einen Teledienst. Zwar ist der technische Vorgang des Empfangens von Nachrichten nach der gesetzlichen Definition (§ 3 Nr. 22 TKG) Telekommunikation. Allerdings handelt es sich hier weder um einen Telekommunikationsdienst i. S. v. § 3 Nr. 24 TKG noch ist die Behörde dann Diensteanbieter i. S. v. § 3 Nr. 6 TKG. Die Behörde erbringt dem

Empfangen keinen „Dienst“. Diese Leistung beschränkt sich auf die Übertragung von Signalen über Telekommunikationsnetze.

Auch das bei der Übertragung geltende Fernmeldegeheimnis (§ 88 TKG) endet mit dem Empfang der Nachrichten bei der als Empfänger bezeichneten Behörde.

Für die Weiterverarbeitung innerhalb der öffentlichen Stelle (Entschlüsseln, ggf. Umschlüsseln, Signaturprüfung, Generierung eines elektronischen Laufzettels, Weiterleiten an die endgültigen Empfänger) gelten daher ausschließlich die Bestimmungen des für die jeweilige Stelle anwendbaren allgemeinen und ggf. bereichsspezifischen Datenschutzrechts.

5.3.2 Betrieb der VPS durch Dritte

Entscheiden sich eine oder mehrere öffentliche Stellen, eine VPS außerhalb der eigenen Organisation als selbstständige Stelle zu betreiben, ergibt sich eine andere Rechtslage. Dabei kommt es nicht darauf an, in welcher Rechtsform diese Stelle betrieben wird. Entscheidend ist allein, dass es sich im datenschutzrechtlichen Sinne um eine eigenständige Daten verarbeitende Stelle handelt. Ebenso wie die Auslagerung einer konventionellen Poststelle auf einen Dritten dazu führt, dass dieser einen Postdienst (sowohl gegenüber der Behörde als auch gegenüber den Kunden) erbringt, kann auch die Auslagerung der VPS dazu führen, dass diese zum Anbieter eines Dienstes wird.

Hierbei ist zu klären, ob ein Telekommunikationsdienst oder ein Teledienst erbracht wird oder ob die Verarbeitung personenbezogener Daten innerhalb der die VPS betreibenden Stelle eine Qualität annimmt, dass von einer inhaltlichen Verarbeitung von Verwaltungsdaten gesprochen werden muss.

Telekommunikation ist nach der Definition in § 3 Nr. 22 TKG der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen. Sie beschränkt sich also auf den reinen Transport von Daten. Teledienste sind hingegen gemäß § 2 Abs. 1 TDG elektronische Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt. Daraus ergibt sich, dass Teledienste auf der Telekommunikation aufsetzen, also einen Mehrwert gegenüber dem reinen Transport darstellen. § 2 Abs. 2 TDG nennt dabei Regelbeispiele für Teledienste, die aber nicht abschließend sind. Jede Funktion innerhalb eines bestimmten Angebots – also auch innerhalb der VPS – muss gesondert betrachtet werden.

Die folgenden Beispiele sollen dies verdeutlichen:

Empfang und zielgerichtete automatisierte Weiterleitung von signierten und verschlüsselten Inhalten

Der reine Transport von Nachrichten ist als Telekommunikationsdienst zu qualifizieren. Hier handelt es sich um die Übertragung von Signalen über Telekommunikationsnetze i. S. v. § 3 Nr. 24 TKG. Diensteanbieter ist hier die VPS betreibende Stelle,

die diesen Dienst geschäftsmäßig, d. h. nachhaltig für Dritte (insbesondere die Behörde) erbringt. Mindestens wirkt diese Stelle an der Erbringung solcher Dienste mit, was für die Eigenschaft als Diensteanbieter ausreicht. Die (angesichts der Verschlüsselung eher theoretische) Möglichkeit, auch die Inhaltsdaten zur Kenntnis zu nehmen, führt zu keinem anderem Ergebnis. Insoweit besteht kein Unterschied zu anderen Telekommunikations- oder zu Postdiensteanbietern, die z. B. E-Mails oder konventionelle Briefe weiterleiten. Auch bei diesen führt die immer bestehende Möglichkeit, den Inhalt der Sendung zur Kenntnis nehmen zu können, nicht dazu, dass sie Daten verarbeitende Stellen hinsichtlich der Inhaltsdaten werden. Entscheidend ist die Zielrichtung des Dienstes, die hier in dem technischen Vorgang besteht, Nachrichten zu empfangen und weiterzuleiten. Damit ist gerade nicht der Auftrag durch die öffentliche Stelle verbunden, die Inhalte der Nachrichten auch nur zur Kenntnis zu nehmen.

Aus dieser grundsätzlichen Einordnung als geschäftsmäßiges Erbringen von Telekommunikationsdiensten i. S. v. § 3 Nr. 10 TKG folgt auch, dass die das VPS betreibende Stelle das Fernmeldegeheimnis nach § 88 TKG beachten muss. Dem Fernmeldegeheimnis unterliegen dabei nicht nur die Inhalte der Nachrichten, sondern auch die näheren Umstände der Telekommunikation, d. h. vor allem die Verkehrsdaten. Insbesondere ist es der Stelle damit nach § 88 Abs. 3 TKG untersagt, sich oder anderen über das für die Erbringung des Dienstes notwendige Maß hinaus Kenntnis vom Inhalt oder den Verkehrsdaten zu verschaffen. Die Stelle muss außerdem bestimmte technische und organisatorische Maßnahmen zum Schutz des Fernmeldegeheimnisses treffen, § 109 TKG.

Entschlüsselung der Absender- und Empfängerinformationen von Nachrichten

Das Entschlüsseln der genannten Informationen kann jedenfalls nicht als Telekommunikationsdienst angesehen werden, da es über den reinen Transport von Signalen hinausgeht. Soweit dem Vorgang des Entschlüsselns ein Telekommunikationsvorgang zugrunde liegt, kann es als Teledienst angesehen werden. Dies gilt jedenfalls so lange, wie es tatsächlich nur um die Absender- und Empfängerinformationen und nicht um das Verschlüsseln der Inhalte selbst geht. Entscheidend für die Einordnung ist nicht der Vorgang des Entschlüsselns selbst, weil dieser nicht zu einer inhaltlichen Veränderung der verschlüsselten Informationen führt. Vielmehr muss es darauf ankommen, welche Daten verschlüsselt werden. Vorliegend handelt es sich um die Informationen, die zur Durchführung des Empfangens und Weiterleitens der Nachrichten erforderlich sind. Der Vorgang des Entschlüsselns dieser Daten kann nicht ohne Weiteres von dem zugrundeliegenden Telekommunikationsdienst getrennt werden.

Automatische Empfangsquittung

Erhalten die Absender elektronische Nachrichten aus der VPS automatisch eine elektronische Empfangsquittung, ist dies ein Dienst, der über das bloße Transportieren der Nachricht hinausgeht. Zwar liegt der Versendung der Quittung Telekommunikation zugrunde, die Generierung der Absenderquittung stellt jedoch einen Mehrwert gegenüber dem reinen Transport der Daten dar und ist damit (auch) als Teledienst

anzusehen. Die Verarbeitung der Nutzerdaten richtet sich in diesem Kontext nach § 6 TDSDSG.

Generierung des elektronischen Laufzettels zur Protokollierung der Verbindungsinformationen

Die Generierung des elektronischen Laufzettels ist dann noch Bestandteil des Telekommunikationsdienstes „Empfangen und Weiterleiten der Nachrichten“, wenn sich dessen Inhalt auf die reine Protokollierung der Verkehrsdaten des genannten Telekommunikationsdienstes beschränkt. Häufig gehen die mit dem elektronischen Laufzettel generierten Informationen jedoch über die Protokollierung bloßer Verkehrsdaten im Rahmen der Telekommunikation hinaus. In diesem Fall ist von einem Teledienst auszugehen, da insoweit ein Mehrwert gegenüber dem reinen Transport von Nachrichten und dessen Protokollierung erbracht wird. Unabhängig davon ist der Zweck dieses Dienstes dann erfüllt, wenn die Nachricht an den Empfänger erfolgreich weitergeleitet wurde. Spätestens zu diesem Zeitpunkt wären dann auch die auf dem Laufzettel gespeicherten Daten nach § 96 Abs. 2 Satz 2 TKG bzw. § 6 Abs. 4 TDDSG zu löschen, wenn sie nicht noch zu etwaigen Abrechnungszwecken erforderlich sind (Weitergabe der Daten an den Anwender bzw. an die Anwendung).

Die über den Transportzeitraum hinausgehende Speicherung des Laufzettels kann nicht damit gerechtfertigt werden, dass das Speichern dieser Daten noch Bestandteil des Telekommunikationsdienstes „Übertragen von signaturgesetzkonformen Formularen“ oder eines selbstständigen Teledienstes ist. Ist der Transport abgeschlossen, findet auch keine Übertragung mehr statt. Die bei der Nutzung dieses Dienstes angefallenen Daten sind dann nicht mehr erforderlich. Deren Speicherung kann daher nicht auf §§ 96 ff. TKG, § 6 TDDSG gestützt werden.

Ab dem Moment, wo die Daten nicht mehr zur Abwicklung des Telekommunikations- bzw. Teledienstes erforderlich sind, handelt es sich nicht mehr um Verkehrsdaten i. S. d. TKG bzw. Nutzungsdaten i. S. d. TDDSG, sondern sie bekommen dann die Qualität als Inhaltsdaten. Sie dienen gerade nicht mehr den in den §§ 96 ff. TKG, § 6 TDDSG genannten Zwecken, sondern sollen die bereits stattgefundene Übertragung eines elektronischen Dokumentes beweisen. Die Daten sind dann den Inhaltsdaten zuzurechen, deren zulässige Verarbeitung sich nach den dafür geltenden Vorschriften richtet.

Problematisch ist, dass die Daten ursprünglich als Verkehrsdaten eines Telekommunikationsdienstes bzw. Nutzungsdaten eines Teledienstes erhoben und gespeichert wurden. Mit der Protokollierung geht eine Änderung des ursprünglichen Erhebungszwecks (insbesondere Ermöglichung der Inanspruchnahme des Dienstes) einher, die nach §§ 96 ff. TKG, § 6 TDDSG nicht ohne Weiteres zulässig ist. Einen solchen Eingriff in das Fernmeldegeheimnis sieht weder das TKG noch das TDDSG vor. Die Protokollierung wäre nur dann möglich, wenn die Daten von vornherein auch als Inhaltsdaten betrachtet werden. Dies wiederum wäre nur im Rahmen einer Datenverarbeitung im Auftrag denkbar. Welche Rechtsvorschriften gelten, hängt letztlich davon ab,

welche Stelle den Transport der Dokumente nachweisen muss. Dann wäre die Speicherung und Nutzung nach Landesdatenschutzrecht zu beurteilen.

Entschlüsselung der Inhaltsdaten

Die Entschlüsselung von Inhaltsdaten und die nicht direkte Weiterleitung führen dazu, dass diese zur Kenntnis genommen werden können und in der VPS zumindest erhoben und gespeichert werden. Dieser Vorgang ist weder als Telekommunikations- noch als Teledienst zu werten. (Beispiel für „direkte Weiterleitung“: Wenn Inhaltsdaten SSL-verschlüsselt in der VPS eingehen, sofort entschlüsselt, mit dem privaten Schlüssel des Empfängers verschlüsselt (z. B. PGP) und sofort weitergeleitet werden, ist das Merkmal einer direkten Weiterleitung erfüllt. Werden jedoch die verschlüsselten Daten für den Empfänger zum Abruf (z. B. POP) bereit gehalten, sind die Voraussetzung einer direkten Weiterleitung nicht erfüllt.). Auch hier könnte deshalb nur die Konstruktion einer Datenverarbeitung im Auftrag gewählt werden.

Vorhalten offener Geschäftsvorfälle in verschlüsselter Form

Beim Vorhalten offener Geschäftsvorfälle handelt es sich um eine Speicherung personenbezogener Daten. Die Tatsache, dass die Dokumente verschlüsselt sind, führt zu keiner anderen Bewertung. Verschlüsselung ist eine technische Maßnahme, um den Zugriff auf die Daten zu verhindern oder zumindest zu erschweren; im Gegensatz zur Anonymisierung hebt sie aber den Personenbezug nicht auf. In diesem Fall handelt es sich nicht um einen Telekommunikations- oder Teledienst.

6 IT-Sicherheitsziele und Sicherheitsmechanismen

Die VPS schafft neue Möglichkeiten zur Automatisierung und Zentralisierung der Kommunikationssicherheit im eGovernment. Dazu bietet sie Dienste zum Erreichen von Authentizität, Vertraulichkeit, Integrität, Verbindlichkeit sowie zu Monitoring und Auditing der Komponenten und Prozesse der VPS. Diese Sicherungsziele werden unabhängig von der eingesetzten Technologien erreicht. Im Folgenden sind alle die Sicherheitsziele zu betrachten, die dem Zweck einer höheren Kommunikationssicherheit dienen, und die Sicherheitsmechanismen, mit denen sie als Funktionen der VPS erreicht werden.

Dienst zur Authentisierung

Mit den Authentisierungsdiensten der VPS werden Web-basierte und andere Anwendungen unterstützt zur Sicherstellung der Authentizität der Herkunft der Inhaltsdaten sowie des Senders und Empfängers der Nutzungsdaten. Insbesondere unterstützt wird die zertifikatsbasierte Authentisierung mit Sicherung der Authentizität der verwendeten Schlüssel durch Zertifikatsprüfungen. Neben diesen Verfahren kann eine VPS auch andere Authentisierungsverfahren, wie etwa PIN/TAN–Verfahren über Schnittstellen bedienen. Grundsätzlich werden von der VPS Authentisierungen sowohl die Serverseite (z. B. geschützte Webseiten) als auch die Clients (sowohl Bürger/Kunden als auch Verwaltungsmitarbeiter) unterstützt.

Dienst zur Herstellung von Vertraulichkeit

Die VPS unterstützt zertifikatsbasierte Verfahren zur Sicherung der Vertraulichkeit von Inhalts- und Nutzungsdaten. Das Niveau definiert die zertifikats-ausgebende PKI, die als Sicherheitsinfrastruktur betrieben wird und das dem Niveau der Zertifikate für andere Verwendungszwecke entsprechen sollte.

Dienst zur Herstellung von Integrität

Hierzu unterstützt die VPS wiederum zertifikatsbasierte Mechanismen zur Sicherung der Integrität der übertragenen Inhalts- und Nutzungsdaten.

Dienst zur Herstellung von Verbindlichkeit (Authentizität und Nachweisbarkeit)

Um die Nicht-Abstreitbarkeit des Ursprungs der Inhaltsdaten sowie des Empfangs von Nutzungsdaten sicherzustellen, werden die Ergebnisse von Zertifikatsprüfungen in einem Prüfprotokoll (Laufzettel) festgehalten. Gleiches gilt für die Protokollierung von Zeitpunkten. Um die Korrektheit nachweisbar sicherzustellen, können über vorgegebene Schnittstellen sowohl externe Zeitstempeldienste als auch Zeit-Server angebunden werden.

Dienst zu Monitoring und Auditing der Komponenten und Prozesse der VPS

Zur Gewährleistung eines sicheren Betriebs der VPS werden die erforderlichen Mechanismen zur Administrierbarkeit, wie die Anlage und Pflege von Log-Dateien sowie das Monitoring der Administration unterstützt. Dazu erfolgt eine Anbindung des VPS-Kernsystems an einen oder mehrere Log-Server.

Bei den o.g. Sicherheitszielen wird im allgemeinen unterschieden zwischen der Authentisierung eines Kommunikationspartners und der Authentizität von Kommunikationsdaten. Bei letzterem Ziel kommt es darauf an, den Urheber eines Datensatzes in nicht abstreitbarer Weise zu ermitteln; dieser muss nicht unbedingt mit dem Absender der Daten identisch sein (z. B. Übersendung einer Steuererklärung durch einen bevollmächtigten Steuerberater). Unter Verweis auf die Forderungen des § 4 Abs. 1 TDDSG (Ermöglichen anonymer und pseudonymer Nutzungen von Teledienstangeboten) sei hinzugefügt, dass die VPS keinerlei Dienste zur Herstellung von Anonymität anbietet. Dies gehört nicht zu ihrem „Leistungsspektrum“. Nach der gesetzlichen Forderung werden aber durch die Anwesenheit einer VPS solche Systeme nicht in ihrer Funktion behindert.

Zur verlässlichen Erbringung der Sicherheitsdienste ist es erforderlich, dass die VPS Maßnahmen zum „Selbstschutz“ ergreift und sowohl die in ihr – temporär – vorliegenden Kommunikationsdaten als primäre Schutzobjekte als auch die zur Bearbeitung dieser Daten erforderlichen Systeme und Daten als sekundäre Schutzobjekte absichert. Diese **nicht-funktionalen Sicherheitsanforderungen** gelten sowohl für den Betrieb der VPS als auch für deren Administration.

Der Sicherheitsbedarf der Anwendungen bestimmt die Stärke der den Sicherheitsdiensten zugrunde liegenden Mechanismen (z. B. Verschlüsselungsalgorithmus). Das

dort geforderte und etwa in der Güte von Zertifikaten bestehende Niveau wird durch die VPS lediglich erhalten und an die anfragenden VPS-Kernsysteme sowie Clients weiter gegeben. Der Schutzbedarf der von der VPS verwalteten Sicherheitsobjekte leitet sich aus dem Schutzbedarf der damit gesicherten Informationswerte ab. Daher sind die Sicherheitsanforderungen an die VPS-Komponenten und -Objekte selbst in der Regel hoch bis sehr hoch. Ausnahmen gelten für den Bereich wenig schutzbedürftiger oder nicht personenbezogener Informationen. Da die VPS aber keine Unterscheidung der von ihr bearbeiteten Inhalte vornimmt, muss das maximal zu erwartende Sicherheitsniveau umgesetzt werden.

Für die verwendeten Sicherungsmittel gilt:

Passwörter – bestimmend ist der Wert der mit diesen Passwörtern abgesicherten Anwendungen und darin enthaltenen Informationen. Beispielsweise kann die Offenlegung der Passwörter zu Datenverlust, unberechtigten Veränderungen und unberechtigter Verbreitung dieser Informationen führen.

Verschlüsselungsschlüssel – bestimmend ist der Wert der mit diesen Schlüsseln gesicherten Informationen. Beispielsweise ist ein Verlust dieser Schlüssel dem Verlust der Daten gleichzusetzen, da dann eine Wiedergewinnung der Informationen nicht mehr möglich ist.

Signaturschlüssel – bestimmend ist der Wert der mit diesen Schlüsseln abgesicherten Geschäftsvorfälle und Transaktionen. Beispielsweise kann die unberechtigte Verwendung eines derartigen Schlüssels zu unberechtigten Transaktionen mit einer rechtlichen Bindewirkung für Behörden und Privatpersonen führen.

Zeitstempel – bestimmend ist der Wert der mit diesen Zertifikaten abgesicherten Transaktionen. Werden nicht akkreditierte Zertifikate dafür genutzt, können die damit belegten Zeitpunkte bestimmter Aktionen ggf. nicht beweisbar festgeschrieben werden.

7 Funktionale Anforderungen

Als Basiskomponente für die Kommunikationssicherheit soll eine Virtuelle Poststelle zahlreiche insbesondere kryptographische Funktionalitäten für die verschiedenen Kommunikationskanäle (vor allem Web-basierte Kommunikation, E-Mails) anbieten. Dabei ist es naheliegend, diese Dienste auch anderen Systemen im „Backend“ der Behörde anzubieten. Beispielhaft seien hier Archivsysteme oder Dokumentenmanagement- und Workflowsysteme genannt.

Die sich aus diesem generellen Auftrag einer VPS möglicherweise ergebenden funktionalen Anforderungen können je nach konkretem Einsatzszenario sehr unterschiedlich ausfallen. So könnte etwa eine kleine Kommune mit nur wenigen vorhandenen IT-Systemen es bevorzugen, dass eine VPS die zur elektronischen Kommunikation erforderlichen Basisdienste weitgehend selbständig erbringt („Sorglos-Lösung“), während eine große Behörde mit starker IT-Durchdringung eher Wert darauf legen dürfte, dass eine Vielzahl von komplexen Verfahren so angebunden werden kann, dass

möglichst wenig Änderungen an den bestehenden Systemen erforderlich sind („transparente Unterstützung“).

Um diesen unterschiedlichen Anforderungen Rechnung tragen zu können, wurde für dieses Kapitel die VPS des Bundes, also die Basiskomponente „Datensicherheit“ in BundOnline 2005 als „Referenzmodell“ verwendet. Informationen zu dieser Lösung, die unter fachlicher Aufsicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) entwickelt wird, finden sich auf der Web-Site http://www.bsi.bund.de/fachthem/egov/vps.htm. Hier bestand die Herausforderung darin, eine Vielzahl (über 100) von Bundesbehörden unterschiedlichster Größe und IT-Ausstattung mit potentiell bis zu 400 eGovernment-Dienstleistungen sicherheitstechnisch zu unterstützen. Dabei wird davon ausgegangen, dass die Kernfunktionalitäten der VPS von jeder nutzenden Behörde selbstständig betrieben werden. Sie sollten nach Ansicht des BSI für alle „typischen“ Anwendungsszenarien eine ausreichende Basis bilden und nach dem heutigen Stand der Technik realisierbar sein. Ab Herbst 2004 werden sie in der VPS des Bundes Version 2.0 zur Verfügung stehen. Ergänzend sind eine Reihe anderer Funktionalitäten vorstellbar, von denen einige in Kapitel 7.2 dargelegt sind.

Zu den genannten funktionalen Anforderungen an eine VPS treten üblicherweise nicht-funktionale Anforderungen. Hierzu gehören etwa die Unterstützung von Schnittstellen zu vorhandenen IT-Systemen, die Benutzerfreundlichkeit der Client-Komponenten, die Skalierbarkeit für hohe Last- oder Verfügbarkeitsanforderungen und auch die in Kapitel 9.2 betrachteten Anforderungen zur Gestaltung eines Sicherheitskonzepts für die VPS. Diese Anforderungen hängen sehr stark vom jeweiligen Einsatzszenario ab und werden daher in dieser Broschüre im Allgemeinen nicht detailliert betrachtet. Nicht-funktionale Anforderungen, die aus Datenschutz-Sicht bedeutsam sind, werden in den Kapiteln 8 und 9 diskutiert.

Wie bereits in Kapitel 3 kurz ausgeführt, ist eine VPS im Sinne dieser Broschüre keine „fertige“ eGoverment-Anwendung, sondern eine unterstützende (Middleware-) Komponente. Dies bedeutet insbesondere, dass ihre Anwendung nur im Rahmen eines übergreifenden eGovernment-Konzepts, das insbesondere eine Kommunikationsstrategie enthalten sollte, sinnvoll ist. In einer Kommunikationsstrategie wird etwa festgelegt, ob im Rahmen einer eGovernement-Dienstleistung Web-basierte oder E-Mail-Kommunikation (oder beides) zum Einsatz kommen soll oder für welche Kommunikationsbeziehungen Ende-zu-Ende-Sicherheit erforderlich ist. Hinweise zur Erstellung eines solchen Strategiepapiers finden sich in Kapitel 9 dieser Broschüre.

7.1 Funktionale Anforderungen an die VPS des Bundes

In diesem Abschnitt werden die Funktionalitäten der VPS des Bundes, wie sie in der ab Herbst 2004 verfügbaren Version 2.0 zur Verfügung stehen, betrachtet. Zur Vermeidung von Missverständnissen sei darauf hingewiesen, dass im Folgenden der Begriff „Unterstützung“ so gemeint ist, dass diese Funktionen nicht komplett durch die VPS selbst erbracht werden, sondern entsprechende *separate* Systeme über offene Schnittstellen von der VPS angesprochen werden können.

7.1.1 Grundfunktionalitäten zur Behandlung ein- und ausgehender Daten

Für die Bearbeitung sowohl der eingehenden als auch der ausgehenden Daten müssen folgende gemeinsamen Funktionen berücksichtigt werden:

- **Verschlüsselung**

  Ermittlung des Verschlüsselungszertifikates des Kommunikationspartners und Verschlüsselung

- **Entschlüsselung der ein-/ausgehenden Daten**

- **Signaturbildung**

  Folgende Alternativen sind zu beachten:

  - Die vorhandene elektronische Signatur des Mitarbeiters soll unverändert weitergegeben werden: Dann ist am Output keine Änderung vorzunehmen.
  - Die Signatur des Mitarbeiters wird durch eine organisationsbezogene (fortgeschrittene oder qualifizierte) elektronische Signatur ersetzt.
  - Die VPS signiert nicht intern signierte Ausgänge mit einer organisationsbezogenen (fortgeschrittenen oder qualifizierten) elektronischen Signatur.

- **Signaturprüfung**
  - Mathematische Signaturprüfung
  - Zertifikatsprüfung
  - Einheitliche Prüfung von Mehrfachsignaturen

- **Bereitstellen von Zeitstempeln**
  - Einholen von qualifizierten Zeitstempeln
  - Erzeugung von Posteingangs- und -ausgangsstempeln mittels interner Zeitangaben und elektronischen Signaturen, die auch zum Integritätsschutz innerhalb der Behörde verwendet werden können.

- **Zeitstempelprüfung**
  - Prüfung gegebenenfalls beigefügter Zeitstempel (auch qualifizierte Zeitstempel externer Anbieter)
  - Prüfung der verwendeten Zeitstempel-Zertifikate

- **Prüfung auf schädliche Inhalte**
  - Einbindung von im Behördennetz vorhandenen Virenscannern (die VPS umfasst keinen eigenen Virenscanner)
  - Weitergehende Inhaltsprüfungen werden durch die VPS des Bundes als *Basiskomponente* nicht unmittelbar unterstützt, da z.Zt. keine fachübergreifend eingesetzten Produkte oder Standards absehbar sind. Die Übergabe von (ent-

schlüsselten) Daten von der VPS an solche Systeme ist jedoch über die *generischen* Schnittstellen der VPS möglich.

- **Nutzung eines internen Verzeichnisdienstes,**

  in dem die Authentisierungsdaten und Zertifikate der Kommunikationspartner gespeichert sind.

- **Dokumentation auf einem Laufzettel (VPS-Laufzettel)**

  Der Laufzettel dient zum Nachvollziehen der Prozessschritte, die das Dokument bei der Bearbeitung durch die VPS durchlaufen hat. Alle relevanten Operationen und Ergebnisse werden auf dem VPS-Laufzettel dokumentiert.

- **Quittungsmechanismen**

  Erstellung und Versand von Quittungen für den Absender, konfigurierbar hinsichtlich des Anlasses (z. B. Eingang, Ausgang), des Inhaltes sowie der Signaturqualität (keine, fortgeschritten oder qualifiziert).

- **Unterstützung der Dokumentation des Postein- und -ausganges**

  Von der VPS bearbeitete Nachrichten können in existierende Posteingangs- und -ausgangsbücher übernommen werden. Dabei sollten Informationen des VPS-Laufzettels, aber nicht die Dokumenteninhalte abgelegt werden.

- **Einbindung in den Mailfluss**
  - „Herausfiltern“ von E-Mails, die durch die VPS kryptographisch bearbeitet werden sollen,
  - Rückgabe der bearbeiteten Mails in den Mailfluss.

- **Einbindung in Anwendungen**
  - Übernahme von Dokumenten aus Anwendungen (Web-Anwendungs-Server, Anwendungs-Server),
  - Besondere Unterstützung der OSCI-basierten Web-Kommunikation

- **Fehlerbehandlungsmechanismen**
  - Konfigurierbar nach Maßgabe des Fachverfahrens; beispielsweise Behandlung unbekannter Signaturformate,
  - Generierung und Versendung von Benachrichtigungen bei fehlerhaften Eingängen (z. B. fehlerhafte Signatur, fehlendes Zertifikat).

- **Behandlung von Output mit höherem Vertraulichkeitsbedarf**
  - *Umverschlüsselung.* Hierbei wird die Nachricht in der VPS zunächst entschlüsselt – so dass sie etwa einem zentralen Virenscanning zugeführt werden kann – und anschließend mit einem behördeninternen Verfahren für den endgültigen Empfänger neu verschlüsselt.

- Weiterleiten von verschlüsselten E-Mails bei Ende-zu-Ende-Sicherheit ohne weitere Aktionen der VPS.

7.1.2 Funktionen zur Behandlung der in die Behörde eingehenden Daten

Für die Bearbeitung der eingehenden Daten müssen zusätzlich zu den gemeinsamen Funktionen folgende spezifischen Funktionen berücksichtigt werden:

- Berücksichtigung von Vertretungsregelungen,
- Regelbasierte Entscheidung über interne verschlüsselte Zusendung von eingehenden Mails und gegebenenfalls Verschlüsselung des bearbeiteten Inputs einschließlich VPS-Laufzettel,
- Definierte Übergabe des bearbeiteten Inputs einschließlich des VPS-Laufzettels an Hintergrundsysteme.

7.1.3 Funktionen für Anwendungen und Backendsysteme

Die oben beschriebenen Dienste sollen über *offene Schnittstellen* ansteuerbar sein. Hierdurch können z. B. Daten aus Vorgangsbearbeitungssystemen, Archiven etc. auf Anforderung kryptographisch bearbeitet werden.

7.1.4 Funktionen zur Verifikation von Signaturen

Diese Funktionen erlauben es internen und externen Benutzern, die Signatur von Dokumenten *direkt* zu verifizieren.

- Die browserbasierte Verifikation ermöglicht dem Benutzer die Auswahl des Dokumentes und gibt ihm Informationen zu Details der Signatur und deren Gültigkeit zurück.
- Anwendungsbasierte Verifikation: Signaturen können über Programmierschnittstellen (API's) integral in der Anwendung geprüft werden.

7.1.5 Funktionen zur Authentisierung von Benutzern

Benutzer können mittels übermittelter Zertifikate authentisiert werden. Über die Dokumentation auf dem VPS-Laufzettel wird der anfragenden Anwendung das Ergebnis weitergereicht.

7.1.6 Funktionen zur Administration der VPS

Für den Betrieb der VPS werden weitere Funktionen benötigt, die zur Administration und zur Wahrung der Sicherheit der VPS eingesetzt werden. Einbezogen werden:

- Authentisierung des Bedienungspersonals,
- Rechteverwaltung der VPS,
- Schlüsselspeicherung und -verwaltung privater Kryptoschlüssel (siehe hierzu Kapitel 8.1),
- Verwaltung von internen Vertretungs- und Berechtigungsregelungen,

- Datensicherung,
- Protokollierung und Unterstützung der Protokollauswertung,
- Update-Funktionen für neue Kryptoverfahren, Kryptoparameter und Zertifikatsformate,
- Unterstützung der Durchführung einer Revision.

7.1.7 Funktionen zur Prüfung und Nutzung von Zertifikaten

- Gültigkeitsprüfung von Zertifikaten bzw. Zertifikatsketten,
- Auffinden von Zertifikaten („Locate Service“) externer Kommunikationspartner, die aus früheren Kommunikationen bekannt sind. Hierbei müssen das Zweckbindungsgebot und Art und Umfang der erteilten Einwilligung des Kunden in die elektronische Kommunikation berücksichtigt werden.
- Zertifikats-Rating: Bereitstellen von Informationen über die „Güte“ eines Zertifikats nach einem *extern vorgegebenen* Klassifikationsschema.

7.2 Weitere denkbare funktionale Anforderungen

Die im Folgenden aufgeführten funktionalen Anforderungen werden im Kontext von Diskussionen um Virtuelle Poststellen häufiger genannt, sind jedoch in der VPS des Bundes Version 2.0 *nicht* umgesetzt.

7.2.1 Einbindung von Contentscannern, z. B. zum Blockieren unerwünschter Inhalte

Neben der aus Sicherheitsgründen obligatorischen Virenprüfung wird häufig gewünscht, dass der eingehende Kommunikationsstrom auch nach weiteren Kriterien gefiltert werden soll. Beispiele hierfür sind das Blockieren unerwünschter Inhalte (Pornographie, Werbung, SPAM, ...) oder das Zurückweisen von Dokumenten, die nicht den formalen Anforderungen eines Fachverfahrens (z. B. hinsichtlich des verwendeten Dateiformats) genügen.

Problematisch ist hierbei, dass derzeit kaum allgemein verbreitete Verfahren und Schnittellen für Contentprüfungen existieren (im Gegensatz etwa zu Virenscannern) und auch die Filterkriterien von Behörde zu Behörde sehr unterschiedlich sein dürften.

Je nachdem, wie „universell“ eine VPS eingesetzt werden soll, können solche Funktionalitäten innerhalb der VPS erbracht werden oder vorhandene Contentscanner bei Bedarf über offene Schnittstellen angebunden werden. Die VPS des Bundes unterstützt mit Blick auf die oben geschilderten Schwierigkeiten die letztgenannte Variante.

7.2.2 Führung eines eigenen Verzeichnisdienstes der externen Kommunikationspartner

Im Rahmen der Kommunikation mit externen Partnern dürfte es häufig sinnvoll sein, zum Beispiel die jeweiligen E-Mail-Adressen oder auch kryptographische Zertifikate

etc. mindestens für die Dauer der Dienstleistungserbringung in einem Verzeichnis abzulegen. Auch dies kann entweder innerhalb einer VPS als auch durch Anbindung eines im Hausnetz der Behörde aufgebauten Verzeichnisdienstes erfolgen.

7.2.3 Interner Zertifikatsverzeichnisdienst

Für die Verschlüsselung von Informationen für eigene Mitarbeiter der Behörde z. B. zum Zwecke der Umverschlüsselung eingehender Informationen oder zur Prüfung interner Signaturen muss die VPS auf kryptographische Zertifikate dieser Mitarbeiter (oder von entsprechenden Systemen) zugreifen können. Auch hier besteht wieder die Alternative des Zugriffs auf bestehende Verzeichnisdienste im Hausnetz oder der Speicherung innerhalb der VPS.

7.2.4 Weiterleitung von Eingangsnachrichten an fachlich zuständige Stellen, etwa anhand formaler Kriterien oder inhaltlicher Auswertungen

Diese „klassische“ Aufgabe einer „analogen“ Poststelle wird häufig auch für die elektronische Version gewünscht. Problematisch ist hierbei einerseits, dass diese Kriterien in besonderer Weise abhängig von den unerstützten Fachverfahren sind. Außerdem dürfte es im Alltag der behördlichen Kommunikation auch immer Fälle geben, in denen eine Nachricht an eine komplett unzuständige Behörde gesendet wird. Es wird also - soweit sich der gegenwärtige Stand der Technik beurteilen lässt - immer die Notwendigkeit geben, eine abschließende Beurteilung durch entsprechende Mitarbeiter manuell durchzuführen. Aus diesem Grund wurde in der VPS des Bundes, die sich auf die kryptographischen Dienste konzentriert, auf die Bereitstellung einer solchen Funktionalität verzichtet.

7.2.5 Weitergehende Workflowfunktionalitäten, etwa zur Abbildung von Mitzeichnungsketten (Mehrfachsignaturen)

Im Rahmen von anspruchsvollen eGoverment-Verfahren besteht häufig die Notwendigkeit, bestimmte Dokumente von mehreren Personen mitzeichnen zu lassen. Hierbei sind zwei Varianten vorstellbar:

- Abbildung der notwendigen Workflow-Logik innerhalb der VPS,
- Nutzung von speziellen Workflowsystemen oder von Fachverfahren, die eine solche Logik mitbringen und die über offene Schnittstellen auf eine VPS zugreifen können.

Für die erste Variante spricht die höhere Servicequalität einer solchen VPS. Für die zweite Variante, die Tatsache, dass die zu unterstützenden Workflows fachspezifisch sehr unterschiedlich sein können. So kann etwa eine fehlende Signatur eines Mitzeichners je nach dessen Rolle im Verfahren ganz unterschiedliche Konsequenzen für den weiteren Prozess haben. Bei der Entwicklung der VPS des Bundes wurde daher der zweiten Variante der Vorzug eingeräumt.

7.3 Komponenten der VPS (Architekturmodell)

Zur Realisierung der Anforderungen ist in der Realisierungsstrategie der VPS als Basiskomponente Datensicherheit der Initiative BundOnline 2005 folgendes Architekturmodell bestimmt worden:

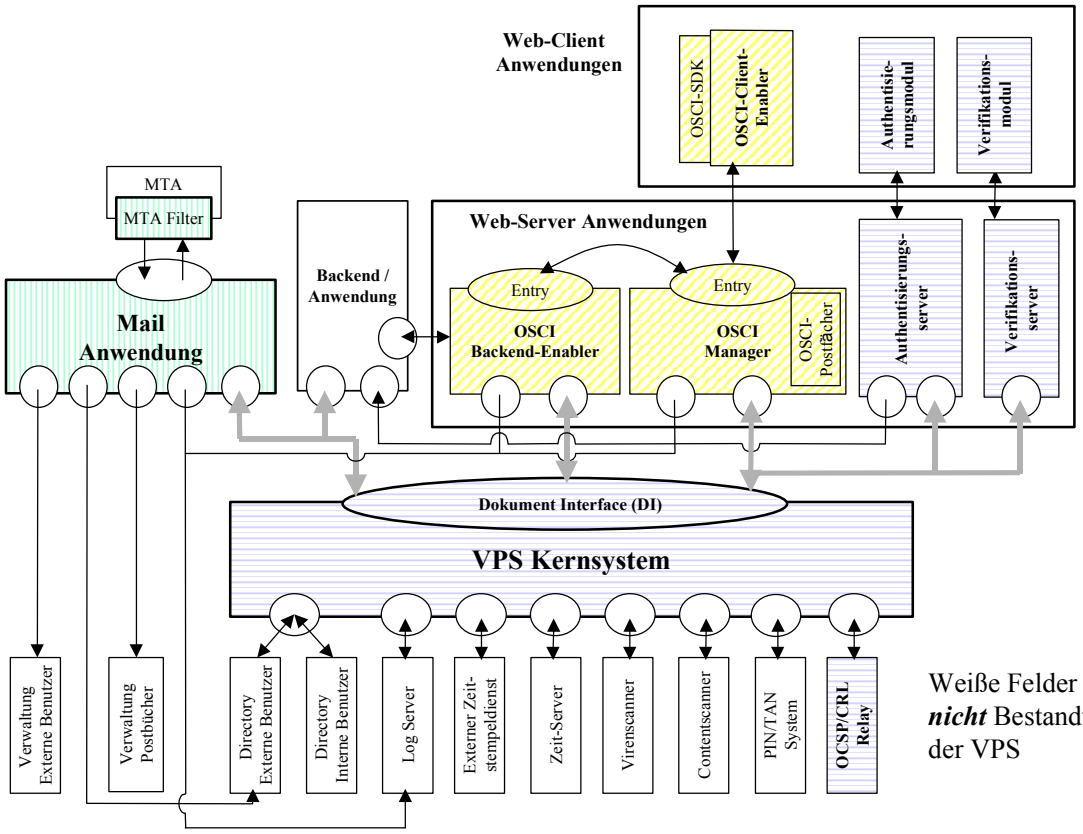

Abbildung: Komponenten der VPS des Bundes (Die Schraffuren haben folgende Bedeutung: Horizontal: Web- und Komponenten der VPS laut Fachkonzept; Vertikal: Mail-Komponenten der VPS laut Fachkonzept; Diagonal: OSCI-Enabler zur Anbindung von OSCI-basierten eGovernment-Dienstleistungen als Erweiterung des Fachkonzepts. Die weiß dargestellten Komponenten bzw. Systeme sind **nicht** Bestandteil der VPS; es handelt sich um externe Systeme, die mit der VPS über offene Schnittstellen kommunizieren.)

Kurzbeschreibung der einzelnen Komponenten

Das **VPS-Kernsystem** ist das „Herzstück“ der VPS. In diesem Modul werden die eigentlichen kryptographischen Operationen durchgeführt, nach einem administrierbaren Regelwerk gesteuert und in einem **VPS-Laufzettel** dokumentiert. Das Kernsystem spricht dazu die der VPS zugeordneten privaten Schlüssel an, die sich auf soft- und/oder hardware-basierten Schlüsselträgern befinden. Zentrales Ein- und Ausgangstor des VPS-Kernsystems ist das **Document-Interface (DI)**, eine XML-basierte

Schnittstelle; sämtliche Kommunikation zwischen dem VPS-Kernsystem und allen übrigen VPS-Komponenten sowie mit Kommunikations- und Backend-Systemen verläuft ausschließlich über diese Schnittstelle. An dieser Stelle soll auch festgehalten werden, dass die VPS insgesamt *zustandslos* ist, die einzelnen Dokumente also rein regelbasiert abarbeitet und (mitsamt dem entstandenen VPS-Laufzettel) wieder zurück gibt. Abgesehen von den zur technischen Revision und Fehlersuche/-behandlung notwendigen Log-Daten speichert die VPS weder die Laufzettel (dies muss ggf. von den entsprechenden Fachanwendungen vorgenommen werden) noch Inhaltsdaten der Kommunikation.

Es gibt folgende Arten von Log-Daten:

- System-Logs, die zur Kontrolle der Funktionalität dienen,
- Administrator-Logs, die die Aktivitäten von Administratoren revisionssicher protokollieren.

☞ Im Wesentlichen bestehen Log-Daten aus einer Auflistung der Aktivitäten mit Angabe des Zeitpunktes sowie des aufrufenden Prozesses. Die Log-Dateien eines sensitiven Systems wie der VPS sind entsprechend dem Grundsatz von Datenvermeidung und Datensparsamkeit technisch so zu gestalten, dass von vornherein so wenige personenbezogene Daten wie möglich verarbeitet werden. Die Protokolldaten dienen ausschließlich dem Zweck, den Betrieb und die Sicherheit der VPS aufrecht zu erhalten. Insbesondere werden in Log-Dateien daher keinerlei Inhaltsdaten gespeichert.

Das **OCSP/CRL-Relay** stellt die Verbindung von VPS-Kernsystem zu externen Verzeichnisdiensten dar und nimmt Aufgaben zur Gültigkeitsprüfung und zum Auffinden von Zertifikaten wahr. Zusätzlich zum aufbereiteten Prüfergebnis liefert das Relay immer auch die (mindestens im Falle qualifizierter Signaturen) signierten Originalauskünfte der Verzeichnisdienste mit. Dies ist wichtig, um einerseits das Prüfergebnis bei Bedarf auch „lokal“ zu verifizieren und andererseits bestimmte Anforderungen im Zusammenhang mit der (Langzeit-) Archivierung erfüllen zu können.

Im OCSP/CRL-Relay wird lediglich die Gültigkeitsprüfung der zu einer Signatur zugehörigen Zertifikate durchgeführt, die mathematische Prüfung der Signatur findet „lokal“ im VPS-Kernsystem statt. Das Relay benötigt und erhält also keinen Zugriff auf die Inhaltsdaten der Kommunikation. Da es sich bei Zertifikaten um signierte Daten handelt, benötigt das OCSP/CRL-Relay aber dennoch die für mathematische Signaturprüfungen notwendigen kryptographischen Funktionalitäten.

Es ist geplant, dieses Relay an zentraler Stelle den Bundesbehörden zur Verfügung zu stellen. Es kann aber bei Bedarf auch dezentral in den Behörden installiert werden. Für Integritätsprüfungen der Zertifikate – nicht der Inhaltsdaten! – verfügt das Relay über eigene kryptographische Routinen.

In Form von Client-Server-Komponenten (sowohl für externe als auch für interne Nutzer) sind die **Authentisierungskomponente** und die **Verifikationskomponente** ausgeprägt**.** Erstere führt kryptographische Authentisierungsprozesse durch und öff-

net oder verweigert damit den Zugang zu bestimmten Informationen oder eGovernment-Anwendungen. Die Verifikationskomponente ermöglicht es, Signaturen von Dokumenten zu überprüfen.

Die Verbindung zu E-Mails findet zunächst über einen **MTA-Filter** statt. Diese Komponente überwacht – nach konfigurierbaren Regeln – den Verkehr des Mailservers darauf hin, ob für die Bearbeitung in der VPS relevante E-Mails im Mailstrom vorhanden sind. Ist dies der Fall, wird die betreffende Mail aus dem Mailstrom zur Bearbeitung durch die VPS abgezweigt. Andere Mails, seien sie kryptographisch nicht bearbeitet oder für die Ende-zu-Ende-Kommunikation vorgesehen, werden „ignoriert". Nach der Bearbeitung durch die VPS werden die Mails ebenfalls durch diesen Filter in den Mailstrom zur internen oder externen Weiterleitung zurück gegeben.

In der **Mail-Anwendung** werden die für die VPS bestimmten E-Mails in das XML-Format des Document-Interface konvertiert (und zum Abschluss wieder zurück konvertiert), ggf. Vertretungsregelungen berücksichtigt und die Verwaltung von Nutzerzertifikaten bedient. Ebenso können hier Quittungen an Absender und Empfänger generiert und versendet werden sowie evtl. in der Behörde vorhandene elektronische Postein- und/oder -ausgangsbücher bedient werden.

In Erweiterung des ursprünglichen Fachkonzepts bietet die Virtuelle Postelle (VPS) als Basiskomponente Datensicherheit im Rahmen von BundOnline 2005 einen sog. **OSCI-Enabler**, der in Form einer verteilten Architektur die OSCI-Kommunikation auf allen drei im Protokoll vorgesehen Ebenen Client – Intermediär – Backend unterstützt. Während die Client-Komponenten über eigene kryptographische Algorithmen verfügen, arbeiten der Backend-Enabler und der die Funktionen des OSCI-Intermediärs realisierende OSCI-Manager mit dem VPS-Kernsystem zusammen. Alle OSCI-Client-Komponenten werden dem externen Nutzer als Java-Web-Start-Applikationen online zur Verfügung gestellt.

☞ Es sei darauf hingewiesen, dass die Intermediärs- und die Backendfunktion der OSCI-Kommunikation sowohl an getrennten Orten als auch gemeinsam bei einer Behörde betrieben werden können. Durch die Trennung der „Briefumschläge" im OSCI-Container ist die Kenntnisnahme der Inhaltsdaten beim Intermediär ausgeschlossen (solange die Backend-Schlüssel nicht kompromittiert sind).

8 Anforderungen und Handlungsempfehlungen zur Gewährleistung von Datenschutz und Datensicherheit

8.1 Herstellung von Vertraulichkeit, Verschlüsselung/Entschlüsselung

☞ Ausgehende Daten sollen verschlüsselt an externe Kommunikationspartner übermittelt werden können.

Dazu müssen die öffentlichen Schlüssel der Kommunikationspartner bekannt sein. Die Speicherung der Schlüssel kann sowohl in einem internen als auch einem externen Verzeichnisdienst erfolgen Die entsprechenden Verzeichnisdienste sind in der Regel nicht Bestandteil der VPS (vgl. dazu Abschnitt 7.2.2 und 7.2.3). Für den Zugriff

auf die Verzeichnisdienste sind daher „passende“ Schnittstellen vorzusehen. Im Falle von internen Verzeichnisdiensten wird dies in der Regel eine LDAP-Schnittstelle sein. Bei externen Diensten sind sowohl LDAP-basierte Abfragen von Zertifikaten und Sperrlisten als auch Online-Status-Auskünfte über OCSP gebräuchlich.

☞ Externe Kommunikationspartner sollen die Möglichkeit haben, verschlüsselte Nachrichten an Dienststellen (bzw. deren Funktionspostfächer) und (soweit eine Kommunikation über Funktionspostfächer nicht sinnvoll erscheint) Einzelempfänger zu senden (Ende-zu-Ende-Verschlüsselung).

Dazu müssen die externen Kommunikationspartner die öffentlichen Schlüssel der Empfänger kennen. Gemäß den Prinzipen der asymmetrischen Kryptographie ist eine solche Veröffentlichung nicht sicherheitskritisch. Insbesondere ermöglicht es die Kenntnis dieser Schlüssel nicht, die Nachrichten zu entschlüsseln.

☞ Bei eingehenden Nachrichten ist im Rahmen einer Kommunikationsstrategie (vgl. Kapitel 9.1.2) festzulegen, welche Nachrichten in der VPS zentral entschlüsselt werden soll und wo ein Ende-zu-Ende-Schutz gewährleistet werden soll.

In der VPS werden die zentral zu entschlüsselnden Nachrichten dann mit dem privaten Schlüssel des jeweiligen Postfachs entschlüsselt. Zur Vermeidung von Missverständnissen sei darauf hingewiesen, dass der genannte „private“ Schlüssel ein Fachterminus der asymmetrischen Kryptographie ist. Hiermit werden alle Schlüssel bezeichnet, die zur Entschlüsselung und zur Erstellung von Signaturen benötigt werden und daher im Gegensatz zum „öffentlichen“ Schlüssel dem Kommunikationspartner nicht bekannt sein dürfen. Auf keinen Fall sollte im Allgemeinen darauf geschlossen werden, dass solche Schlüssel immer einer Person zugeordnet sind. Eine solche Vorgehensweise könnte jedoch nur gewählt werden, wenn die Nachrichten generell keine sensiblen Daten beinhalten, die eine Ende-zu-Ende-Verschlüsselung erfordern, und gleichzeitig den Absendern transparent ist, dass neben dem Empfänger auch die VPS die Nachrichten entschlüsseln kann.

Wenn die VPS über die Möglichkeit verfügen soll, eingehende Nachrichten zu entschlüsseln, käme auch die Verwendung eines eigenen Schlüsselpaars der VPS in Betracht. Der externe Kommunikationspartner würde in diesem Fall die Nachricht mit dem öffentlichen Schlüssel der VPS und nicht mit dem öffentlichen Schlüssel des Empfängers verschlüsseln. Die VPS entschlüsselt die eingehende Nachricht mit dem privaten Schlüssel der VPS. Eine Speicherung privater Schlüssel der Empfänger in der VPS würde dann nicht erfolgen müssen. Auch wäre die Möglichkeit einer Ende-zu Ende-Verschlüsselung mit dem privaten Schlüssel des Empfängers für die Fälle offen gehalten, in denen die Nachrichten sensible Daten enthalten.

Eine Speicherung privater Schlüssel muss aber in jedem Fall besonderen Sicherheitsvorkehrungen unterliegen. Hierdurch muss verhindert werden, dass unbefugte Dritte (z. B. Hacker) Zugriff auf die Daten erhalten, die für die Behörde bestimmt sind. Hierfür ist zum Beispiel die Speicherung in einer besonders geschützten Umgebung erforderlich. Außerdem muss durch technisch-organisatorische Maßnahmen (s. Kapi-

tel 9.2) ein unbefugter Zugriff auf die in der VPS temporär vorliegenden entschlüsselten Nachrichten verhindert werden.

Generell darf eine VPS niemals die Möglichkeit blockieren, bestimmte Kommunikationsbeziehungen über Ende-zu-Ende-Mechanismen abzusichern. Dies gilt unabhängig davon, ob die Entschlüsselung nur von einem Empfänger durchgeführt werden darf oder ob dies durch Nutzung von Gruppenschlüsseln mehreren Mitarbeitern möglich ist. Die entsprechenden Nachrichten sind – sofern hier in der Kommunikationsstrategie Ende-zu-Ende-Sicherheit erlaubt oder gefordert ist – ohne Bearbeitung durch die VPS zu ihren Empfängern durchzuleiten. Dies gilt insbesondere für ausgewählte Mitarbeiter aus den Bereichen Personal und des Personalrates, aber auch einzelne Mitarbeiter in bestimmten Funktionen zählen dazu, wie z. B. der Datenschutzbeauftragte. Entsprechend dürfen die zur Entschlüsselung von Ende-zu-Ende-Nachrichten benötigten Schlüssel nicht in der VPS gespeichert werden!

- ☞ Beim Weitertransport von zentral in der VPS entschlüsselten Nachrichten an den Empfänger ist in der Kommunikationsstrategie festzulegen, ob der jeweilige Schutzbedarf auch innerhalb des Hausnetzes besondere Maßnahmen zur Wahrung der Vertraulichkeit auch gegenüber anderen Behördenmitarbeitern verlangt. Sofern Mechanismen der Transportsicherung wie z. B. VPN-Techniken oder SSL-Verschlüsselung nicht ausreichen oder nicht anwendbar sind, kann in der VPS eine Umverschlüsselung mit dem öffentlichen Schlüssel des Mitarbeiters erfolgen.

Es sei darauf hingewiesen, dass sowohl die Bereitstellung von Ende-zu-Ende-Sicherheit als auch die Anwendung der Umverschlüsselung erfordert, dass die betreffenden Empfänger über die zur Entschlüsselung der Nachrichten erforderlichen Systeme und die notwendigen kryptographischen privaten Schlüssel verfügen müssen. Die Empfänger müssen dann natürlich im Umgang mit den Systemen und insbesondere mit den zum Schutz der privaten Schlüssel erforderlichen Maßnahmen entsprechend geschult sein. Insbesondere bei Nutzung von Ende-zu-Ende-Sicherheit ist aufgrund der fehlenden Möglichkeit einer zentralen Virenprüfung eine Ausstattung der entsprechenden Arbeitsplätze mit aktuellen Virenscannern etc. von besonderer Bedeutung.

Angesichts der aufgezeigten Möglichkeiten zur zentralen und dezentralen Verschlüsselung von Nachrichten sind folgenden Handlungsempfehlungen zu beachten:

- ☞ Erarbeitung eine Kommunikationsstrategie, mit klaren organisatorischen und funktionalen Feststellungen.
- ☞ Beachtung der Transparenz, mit der Maßgabe, dass den Absendern deutlich wird, wo ihre Nachrichten entschlüsselt werden (in der VPS oder an einem Mitarbeiterarbeitsplatz). Im Allgemeinen dürfte davon auszugehen sein, dass ein Absender bei Nutzung einer persönlichen E-Mail-Adresse (z. B. in der Form: <name@behörde.de> annimmt, dass eine Verschlüsselung eine Ende-zu-Ende-Sicherheit bis zu dieser Person zur Folge hat. Sofern dies nicht der Fall ist, also zentrale Verschlüsselung in der VPS mit oder ohne erneute Verschlüsselung stattfindet, ist dies dem Absender in verständlicher Form bekannt zu geben.

8.2 Signaturbildung/Signaturprüfung

Bei der Signatur ist zwischen fortgeschrittener Signatur und qualifizierter Signatur (ggf. mit Anbieter-Akkreditierung) zu unterscheiden. Bei qualifizierten Signaturen müssen die zugehörigen Zertifikate entsprechend den gesetzlichen Anforderungen immer auf eine natürliche Person bezogen sein. Durch Verwendung von Pseudonymen, kann sich diese Person dem Empfänger gegenüber „verbergen". Daneben kann der Signierer durch Attribute und Attributzertifikate die Zugehörigkeit zu einer Behörde, seine Zeichnungsbefugnis oder ein bestehendes Vertretungsrecht dem Empfänger gegenüber verbindlich darlegen. Im Zusammenhang mit dem Einsatz von qualifizierten Signaturen durch Behörden im eGovernment sollte außerdem die gesetzlich mögliche Verwendung von Nutzungsbeschränkungen (z. B. monetärer Art) im Signaturzertifikat sorgfältig erwogen werden.

☞ Die Auswahl der jeweiligen Signaturstufe orientiert sich am Schutzbedarf, am Beweiswert (gegenüber Dritten) oder an Formerfordernissen der ausgehenden Daten.

Grundsätzlich muss die qualifizierte Signatur immer dann eingesetzt werden, wenn das Dokument einem gesetzlichen Schriftformerfordernis unterliegt. Allerdings muss beachtet werden, dass qualifizierte Signaturen im Behörden-Eingang auch ohne unmittelbaren Anlass vorkommen können. Der Kunde ist frei, „höherwertige" Schutzmechanismen zu verwenden als unbedingt nötig. Bei der Erstellung von qualifizierten Signaturen ist zu beachten, dass die damit verbundene hohe Rechtsverbindlichkeit besondere Sorgfalt beim Schutz gegen Missbrauch erfordert. Dabei ist insbesondere auszuschließen, dass es zu einer „wahllosen" Signierung beliebiger ausgehender Dokumente kommt

Für Dokumente, die qualifiziert signiert werden sollen oder müssen, bieten sich bei Vorhandensein einer VPS verschiedene Möglichkeiten an:

- Das Dokument wird vom „letzten" Bearbeiter im Rahmen der in der Behörde geltenden Zeichnungsbefugnisse „im Auftrag" persönlich signiert.
- Das Dokument wird durch den Behördenleiter oder durch eine von ihm beauftragte Person („Poststellenleiter") persönlich signiert.
- Das Dokument wird in der VPS im Rahmen eines kontrollierten Prozesses automatisiert signiert, z. B. bei sog. Massengeschäften („Batch-Signatur).

Die Auswahl einer Variante sollte im Rahmen der Kommunikationsstrategie (vgl. Kapitel 9.1.2) erfolgen. Üblicherweise dürften sich die ersten beiden Varianten immer dann anbieten, wenn die Anzahl der zu signierenden Dokumente „überschaubar" bleibt. Die „lokale" Signaturerstellung vereinfacht im Allgemeinen den Schutz des privaten Signaturschlüssels vor unbefugter Nutzung, bedingt jedoch eine technische Ausstattung und entsprechende Schulung der betreffenden Mitarbeiter.

Im Rahmen der Kommunikationsstrategie sollte ebenfalls festgelegt werden, ob im Zertifikat der Name des Signierers oder ein Pseudonym verwendet werden soll. Im ersten Fall ist die Einwilligung des betreffenden Mitarbeiters erforderlich.

Die automatisierte Signatur (dritte Variante) bietet sich immer dann an, wenn eine erhebliche Menge an Signaturen in kurzer Zeit geleistet werden muss. Bei der Erstellung solcher automatisierter Signaturen sind eine Reihe von technisch-organisatorischen Sicherheitsmaßnahmen zu treffen, die eine missbräuchliche Nutzung dieses Leistungsmerkmals verhindern sollen. Hierzu ist die nach Signaturgesetz vorgeschriebene Herstellererklärung oder Bestätigung entsprechend als „Signaturanwendungskomponente“ genutzter VPS-Teilkomponenten heranzuziehen. Ebenso ist dabei das den Bearbeitungsprozess im zugehörigen eGovernment-Verfahren steuernde System in die Schutzüberlegungen einzubeziehen.

Abschließend sei beim Einsatz von qualifizierten Signaturen ausdrücklich davor gewarnt, die Übertragung einer Zeichnungsbefugnis durch die Weitergabe einer persönlichen Signaturkarte (und der zugehörigen PIN!) an eine andere Person „pragmatisch“ zu regeln. Eine solche Vorgehensweise widerspricht den Anforderungen des Signaturgesetzes. Alle mit dieser Karte geleisteten Signaturen werden im Zweifelsfall immer dem rechtmäßigen Karteninhaber zugerechnet – mit allen damit verbundenen Rechtsfolgen!.

☞ Die Speicherung von „persönlichen“ Signaturschlüsseln; insbesondere von solchen, die für die qualifizierte Signatur vorgesehen sind, ist auszuschließen. Für Schlüssel die zu Erzeugung einer automatisierten Signatur in der VPS vorgesehen sind, gelten die oben dargelegten sicherheitstechnischen Randbedingungen

Die **fortgeschrittene Signatur** kann behördenseitig überwiegend für die Transportsicherung verwandt werden. Sie ermöglicht dem Empfänger die Überprüfung der Authentizität und Integrität der Nachricht. Damit kann überprüft werden, dass die Nachricht von einer Behörde kommt und nicht verändert wurde. Bei der Signierung ausgehender Nachrichten sollte allerdings sicher gestellt werden, dass hierdurch keine Einschränkungen der Lesbarkeit der Nachricht beim Empfänger verbunden ist.

Eine **Überprüfung der Signatur von eingehenden signierten Nachrichten** in der VPS ist jedenfalls aus datenschutzrechtlicher Sicht unproblematisch. Allerdings ist hier darauf zu achten, dass der Prüfprozess vor Manipulation geschützt und ggf. nachprüfbar ist.

☞ Signierter Input sollte, wenn immer möglich, auf Authentizität, Verbindlichkeit und Integrität geprüft werden (Verifikation). Die VPS muss sowohl fortgeschrittene als auch qualifizierte Signaturen prüfen können.

Dabei soll sowohl ein Hash-Wert-Vergleich (Integritätsprüfung) als auch eine Zertifikatsprüfung (Authentizitätsprüfung) durchgeführt werden. Darüber hinaus werden Formerfordernisse und die Vollständigkeit der Zertifikatskette geprüft und (soweit möglich) ein Online-Response auf die OCSP-Liste eines Zertifizierungsdiensteanbie-

ters durchgeführt. Sofern OCSP-Auskünfte nicht zur Verfügung stehen, müssen CRL-Abfragen beim Zertifizierungsdiensteanbieter erfolgen.

Im Rahmen der Kommunikationsstrategie sollte festgelegt werden, wie mit Nachrichten umgegangen werden soll, bei denen die Signaturprüfung fehlschlägt oder (z. B. wegen Nichterreichbarkeit des Verzeichnisdienstes) aktuell nicht möglich ist. Dabei ist einerseits zu beachten, dass außer im Falle eines bestehenden Formerfordernisses eine ungültige Signatur zunächst nicht die Verbindlichkeit oder ggf. die Fristenwahrung berührt. Anderseits ist eine fehlgeschlagene Signaturprüfung immer ein Indiz für eine Unregelmäßigkeit. Daher sollte in solchen Fällen stets versucht werden, mit dem (vermeintlichen) Absender umgehend Kontakt aufzunehmen, um den Sachverhalt zu klären.

☞ Art und Umfang der akzeptierten Signaturformate (z. B. PKCS#7, ISIS-MTT) sollen in einer Positivliste festgelegt und bekannt gegeben werden. Ebenfalls könnten die akzeptierten bzw. vertrauenswürdigen Trust-Center in einer solchen Liste erfasst werden. Letzteres wird solange unerlässlich sein, wie die gängigen Standards in der Praxis noch keine problemlose Interoperabilität garantieren.

8.3 Bereitstellen von Zeitstempeln, Zeitstempelprüfung

In bestimmten Fällen (z. B. eine Angebotsabgabe) ist es sinnvoll, digitale Daten authentisch mit einem bestimmten Zeitpunkt zu verknüpfen. Solche Daten werden dazu mit einer vom Zeitstempeldienst angebotenen vertrauenswürdigen Zeit digital verknüpft und das Ergebnis digital signiert. Anschließend werden die so unterschriebenen Daten an den Teilnehmer zurückgeschickt. Ein Zeitstempel beweist, dass die zugehörigen Daten zum angegebenen Zeitpunkt vorgelegen haben.

Bei Zeitstempeln ist generell zwischen qualifizierten Zeitstempeln nach den Anforderungen des Signaturgesetzes und „sonstigen“ Zeitstempeln zu unterscheiden. Erstere können nur von einem Zertifizierungsdiensteanbieter erstellt werden und müssen die gesetzliche Zeit einhalten. Aus datenschutzrechtlicher Sicht sei noch darauf hingewiesen, dass die Nutzung eines externen Zeitstempelanbieters unproblematisch ist, da diesem nur der Hash-Wert der zu bestätigenden Daten vorgelegt werden muss. Eine Rekonstruktion des Inhalts dieser Daten ist diesem kryptographisch unmöglich.

Zeitstempel werden bislang in erster Linie zur Dokumentation des Zeitpunkts der Signaturerstellung genutzt, um den Nachweis zu erbringen, dass ein ggf. signiertes Dokument zu einem bestimmten Zeitpunkt vorlag.

☞ Ohne einen Zeitstempel kann kein Nachweis dafür erbracht werden, dass das ausgestellte Zertifikat *zum Zeitpunkt der Signatur* noch gültig bzw. nicht gesperrt war.

Für die Überprüfung der Gültigkeit von Zeitstempeln gelten die gleichen Anforderungen wie für die Überprüfung von Signaturen.

Eine weitere Einsatzmöglichkeit für Zeitstempel ist die Nutzung als Eingangs- und Ausgangsdokumentation. Um diese Funktion sinnvoll zu nutzen, muss allerdings zunächst der elektronische Ein- und Ausgangspunkt von Nachrichten und Dokumenten festgelegt werden. Nach herrschender Meinung gilt eine elektronische Nachricht als eingegangen, wenn diese das zentrale Mailsystem des Empfängers erreicht hat. Alle nachfolgenden Prozesse, die das Erreichen des End-Adressaten verhindern könnten, liegen in der Verantwortung des Empfängers und können nicht mehr vom Absender der Nachricht beeinflusst werden. Ein Zeitstempel ist daher für den Nachweis des genauen Eingangszeitpunkts nur bedingt einsetzbar, da die Lücke zwischen dem Eingang auf dem zentralen Mailsystem und dem Eingang in der VPS nicht erfasst wird. Als Ersatz für den Einsatz von Zeitstempeln kann daher auch die Angabe der Systemzeit des Eingangs im Laufzettel der VPS dienen.

☞ Die VPS hat nicht die Aufgabe, Eingangs- und Ausgangsinformationen in so genannten Posteingangs- und Postausgangsbüchern zu sammeln und zusammenzufassen. Durch die strukturierte Bereitstellung der Einzelinformationen ermöglicht sie aber nachgelagerten Anwendungssystemen, diese zu erstellen.

Generell ist zum „Beweiswert“ von Zeitstempeln anzumerken, dass unmittelbar nur gefolgert werden kann, dass die zugrunde liegenden Daten jedenfalls nicht *später* als zum angegebenen Zeitpunkt erstellt wurden. Zum Beweis, dass die Daten nicht mutwillig oder durch einen Fehler *verspätet* gestempelt wurden (etwa um einen nicht fristgerechten Eingang vorzutäuschen), muss das empfangende System insgesamt betrachtet werden. Diese Problematik tritt allerdings bei herkömmlichen (Papier-) Eingangsstempeln ebenfalls auf.

8.4 Prüfung auf schädliche Inhalte

☞ Alle eingehenden (und ausgehenden) Nachrichten sollen nach ihrer Entschlüsselung (oder vor ihrer Verschlüsselung) auf Viren, Trojaner, Würmer usw. gescannt werden.

Diese Funktionalität ist bereits heute obligatorischer Bestandteil der meisten Kommunikationssysteme. Die Prüfung muss nicht durch die VPS durchgeführt werden, sondern kann an ein externes System abgeben werden.

8.5 Contentprüfung

Bei der Contentprüfung (Inhaltsprüfung) werden eingehende Nachrichten auf ihre formale Nutzbarkeit (z. B. Datenformat) hin überprüft. Die Überprüfung erfolgt automatisiert.

☞ Der Informationsgehalt und Informationswert einer Nachricht soll in der VPS nicht überprüft werden.

Diese Prüfung wird noch in der Rolle des Operators (s. Kap. 10.1) wahrgenommen.

☞ Auch ausgehende Nachrichten sollten Inhaltsprüfungen unterzogen werden können. Dazu gehört u.a. auch die Eliminierung von Metainformationen z. B. in Office-Dokumenten.

Darüber hinaus gehende Prüfungen (z. B. die Auswertung des Inhalts auf Schlüsselwörter, um Dokumente klassifizieren und darauf aufbauend zuordnen zu können) gehen über diesen formalen Ansatz hinaus. Sie werden daher in der Rolle der Geschäftsstelle wahrgenommen. Auf die besonderen datenschutzrechtlichen Anforderungen an die Zweckbestimmung von Daten und auf die Einhaltung des Fernmeldegeheimnisses wird an dieser Stelle hingewiesen. Sie sind bei der Auswahl des Betreibermodells von besonderer Bedeutung.

☞ Zu den darüber hinaus gehenden Prüfungen kann auch eine Spam-Prüfung (Ausfilterung unerwünschter Werbung, pornographischer Inhalte usw.) gehören. Dabei sollten die Spam-Filter an zentraler Stelle unter Beteiligung der Adressaten gepflegt werden.

Da die Kommunikationsadressen veröffentlicht werden, um einem unbestimmten Absenderkreis die Kommunikation zu eröffnen, ist mit einem erhöhten Anteil von Spam-Mails für diese Adressen zu rechnen.

Bei der Contentprüfung handelt es sich nicht um eine kryptographische Kernfunktion, sie kann daher auch von externen Systemen übernommen werden. Die VPS stellt in der Regel nur eine entsprechende Schnittstelle bereit. Zum Zeitpunkt der Erstellung dieser Broschüre haben sich auf dem Markt keine „Standard-Content-Scanner“ mit zugehörigen Schnittstellen etablieren können.

8.6 Authentisierung des Kommunikationspartners

Unter der elektronischen Authentisierung versteht man die Identifikation durch eine Komponente auf Basis eines elektronischen Merkmals. In der Regel dient sie zur Identifikation von Anwendern oder Client-Komponenten gegenüber System- oder Server-Komponenten. Der Authentisierungsvorgang besteht aus folgenden Schritten:

- Die Informationen zum Benutzerzertifikat werden eingeholt. Je nach Anwendungsszenario kann das Auslesen durch eine Komponente der VPS oder durch eine in eine (Fach)Anwendung integrierte Komponente erfolgen.
- Das ausgelesene Benutzerzertifikat wird an das Kernsystem der VPS übergeben und verifiziert.
- Das kryptographische Authentisierungsverfahren (etwa ein Challenge-Response-Verfahren) wird mittels des im Zertifikat enthaltenen öffentlichen Schlüssels durchgeführt. Ziel ist der für die Authentisierung entscheidende Nachweis, dass tatsächlich mit dem „Besitzer“ des zugehörigen privaten Schlüssels kommuniziert wird.
- Das Ergebnis der Verifikation wird einer anfragenden Anwendung in Originalform oder in aufbereiteter Form (VPS-Laufzettel) zur Verfügung gestellt.

☞ Die VPS prüft *nicht* die Berechtigung des Benutzers für den Zugriff auf eine (Fach)Anwendung. Dies ist, wie die Prüfung der Berechtigung für die Nutzung interner Funktionalitäten, Angelegenheit der (Fach)Anwendung.

8.7 Speicherung der Authentisierungsdaten und Zertifikate der Kommunikationspartner

Nach § 3a Abs. 1 VwVfG (und entsprechender Regelungen für andere Rechtsbereiche) ist die Kommunikation zwischen Bürger und Verwaltung nur zulässig, "soweit der Empfänger hierfür einen Zugang eröffnet". Diese Regelungen betreffen sowohl die Verwaltung als auch private Kommunikationspartner, d. h. Bürger bzw. Mittler (d. h. Berufsgruppen, die im Auftrag Dritter regelmäßig Kontakt mit bestimmten Verwaltungsteilen haben, z. B. Notare, Rechtsanwälte, Architekten etc.) und Institutionen der Wirtschaft. Die Eröffnung eines Zugangs setzt zunächst zwangsläufig und logisch voraus, dass eine entsprechende technische Einrichtung zur Verfügung steht. Weiterhin muss diese auch für die Kommunikation mit der Behörde "freigegeben" sein, dabei kann es sich um eine ausdrückliche oder konkludente Öffnung des Zugangs handeln.

Um externen Kommunikationspartnern elektronische Nachrichten zustellen zu können, müssen diese zuvor ihr Einverständnis erklärt und eine entsprechende Zugangsmöglichkeit (-adresse) bekannt gegeben haben. Dabei treten folgende Fragestellungen auf:

- Welche Möglichkeiten gibt es, die Einverständniserklärung der externen Kommunikationspartner mit möglichst geringem Aufwand einzuholen?
- In welcher Form können die Kommunikationspartner und ihre „Zugangsdaten“ für die VPS verfügbar gemacht werden?
- Wie kann der externe Kommunikationspartner seine Einverständniserklärung zurückziehen?
- Kann die Einverständniserklärung nur für bestimmte Teilbereiche erklärt werden (Zweckbindung) und wenn ja, wie kann diese Information für die angesprochenen Anwendungssysteme verfügbar gemacht werden?

Beschaffung, Hinterlegung, Änderung und Stornierung einer derartigen Einverständniserklärung sind nicht Sache der VPS; sie müssen aber trotzdem gesondert betrachtet und geregelt und sollten im Rahmen der Festlegung der Kommunikationsstrategie behandelt werden.

Für den elektronischen Nachrichtenaustausch mit Privatpersonen oder „kleineren“ Unternehmen ist folgendes zu beachten:

- ☞ Einverständniserklärungen für den Empfang elektronischer Nachrichten müssen vorhanden sein.
- ☞ Der Empfänger muss technisch in der Lage sein, die von der Verwaltung signierte Nachricht (zumindest) zu lesen. Das ist, je nach verwendetem Signatur- oder Verschlüsselungsformat, nicht selbstverständlich.
- ☞ Der Empfänger sollte technisch in der Lage sein, die von der Verwaltung angebrachte Signatur zu verifizieren, d. h. zu überprüfen. Dies ist insbesondere für Er-

klärungen mit hohem „Rechtswert“ für (schrift-)formgebundene Mitteilungen der Verwaltung (z. B. Bescheide) wichtig.

- ☞ Der Absender muss technisch in der Lage sein, die Nachricht ggf. so zu verschlüsseln, dass (ausschließlich) der Empfänger diese entschlüsseln kann. Bei der E-Mail-Kommunikation erfordert dies regelmäßig, dass ein Zertifikat des Empfängers vorliegt und der Absender dieses „richtig“ einsetzen kann. Web-basierte Kommunikationsformen erlauben hier flexiblere Mechanismen (OSCI oder SSL/TLS).

8.8 Generierung eines Laufzettels

Während ein Dokument oder eine Nachricht die VPS durchläuft (bzw. einzelne Module der VPS in Anspruch genommen werden), sollen alle Prozessschritte sowie deren jeweilige Ergebnisse in einem Protokoll (Laufzettel) umfassend dokumentiert werden. Zweck des Laufzettels ist dabei die gesammelte und strukturierte Bereitstellung von Informationen, die für die weitere Bearbeitung durch den Empfänger eine Bedeutung haben (z. B. Gültigkeit von Signaturen).

- ☞ Die Zugehörigkeit eines Protokolls zu der jeweiligen Nachricht oder dem Dokument muss eindeutig sein. Eine Manipulation des Protokolls muss ausgeschlossen sein. Es sollte möglich sein, den Laufzettel durch die VPS zu signieren.
- ☞ Die Laufzettel werden nach der Bearbeitung durch die VPS nicht gespeichert, sondern zusammen mit der Nachricht an den Empfänger weiter geleitet. Aus Transparenzgründen sollte es möglich sein, auch dem Absender einen Laufzettel, ggf. zusammen mit einer Empfangsquittung, zuzustellen.

8.9 Erstellung von Eingangs- und Ausgangsbestätigungen und Behandlung fehlerhafter Vorgänge

Um eine Kommunikationsbeziehung transparent zu machen, ist eine (automatische) Reaktion der VPS zur Benutzerinformation erforderlich. Sie umfasst im Wesentlichen:

- ☞ Die Erstellung und den Versand von Quittungen für korrekt eingegangene bearbeitungsfähige (externe) oder versendete (interne) Nachrichten und Dokumente an den Absender.
- ☞ Werden im Rahmen von Signatur- und Inhaltsprüfungen sowie bei der Ver- und Entschlüsselung Fehler festgestellt, ist der Absender (und ggf. auch der Empfänger) zu informieren.

In den bisherigen Ausführungen wurde grundsätzlich festgestellt, dass die VPS keine Dokumente und Nachrichten speichert. Aus Sicherheitsgründen sollte von diesem Ansatz allerdings in begründeten Ausnahmefällen abgewichen werden:

- ☞ Dokumente und Nachrichten mit schädlichem Inhalt sind nach Möglichkeit in einer gesicherten Umgebung ("Quarantäne") zu Beweiszwecken temporär zu speichern. Ist dies aus Sicherheits- oder Kapazitätsgründen nicht möglich oder sinnvoll, sind sie zu löschen.

- ☞ Für den Umgang mit Dokumenten und Nachrichten mit unvollständiger oder fehlerhafter Signatur oder mit Dokumenten und Nachrichten, die nicht entschlüsselt werden konnten, sind besondere organisatorische Regelungen zu treffen.
- ☞ Die Administrationsregeln für diesen Bereich sollten gesondert festgelegt werden.

8.10 Einbindung in Anwendungen

Eine Schnittstelle erlaubt die Übernahme von Dokumenten aus Anwendungen (Web-Anwendungs-Server, Anwendungs-Server) und die Unterstützung von Systemen, die OSCI-konforme Daten verarbeiten. Die zur Verfügung gestellte Funktionalität deckt die kryptographischen Funktionen ab. Die Unterstützung der entsprechenden Formate und Protokolle (Client-/Backend-Enabler, Intermediär) leisten Anwendungen, die auf der VPS aufsetzen.

- ☞ Es muss eine Schnittstelle zwischen der Anwendung und der VPS definiert und realisiert werden, über die die Funktionen und die Übertragung der zu bearbeitenden Dokumente bzw. Daten durchgeführt werden kann. Die Funktionsgruppen Verschlüsselung, Entschlüsselung, Signaturbildung, Signaturprüfung, Zeitstempel, Prüfung auf schädliche Inhalte, Authentisierung müssen berücksichtigt werden.
- ☞ Bei der Beschreibung der zu unterstützenden Schnittstellen sind die funktionalen, rechtlichen und sicherheitsspezifischen Anforderungen der Anwendung aufzuzeigen.
- ☞ Das DV-Konzept der Anwendung ist um die Beschreibung der in der VPS intern verwendeten Datenobjekte zu erweitern.

8.11 Behandlung von Protokolldaten

8.11.1 Protokollierung von IP-Adressen

Die Frage, ob IP-Adressen personenbezogen sind, ist von großer Bedeutung, weil an verschiedenen Stellen des Internets IP-Adressen - teilweise zusammen mit anderen Nutzungsdaten - protokolliert werden und durch Zusammenführen dieser Daten Profile über das Nutzungsverhalten erstellt werden können. Auf jeden Fall sind statische IP-Adressen personenbezogene Daten, da diese einen direkten und andauernden Bezug zu dem Nutzenden enthalten und auf diesen ohne weiteres rückschließen lassen. Mit Hilfe Dritter ist es darüber hinaus aber bereits jetzt in vielen Fällen möglich, Internet-Nutzer und -Nutzerinnen auch bei nicht-statischen IP-Adressen zu identifizieren. Dynamische IP-Adressen müssen daher ebenfalls als personenbezogene Daten behandelt werden, da sie durch Zusammenführung mit den dahinter stehenden Zuordnungstabellen den Rückschluss auf bestimmbare Personen zulassen (vgl. §§ 3 Abs. 1 BDSG, 1 Abs. 2 TDDSG). Als Folge dieser Zuordnung sind für das Erheben, Verarbeiten, Nutzen und auch Löschen von IP-Adressen die Vorschriften für Verkehrs- bzw. Nutzungsdaten anzuwenden.

8.11.2 Grenzen der Protokollierung

Das Internet setzt voraus, dass die daran Beteiligten eindeutige Adressen verwenden. Jeder Rechner im Netz muss über eine IP-Adresse verfügen, die theoretisch von allen am Kommunikationsvorgang Beteiligten gespeichert werden kann. Mit Analyseprogrammen ist es möglich, diese Daten detailliert auszuwerten. Möglich sind sowohl Nutzungsstatistiken mit angebotsbezogenen Aussagen (wie häufig wurde eine Seite aufgerufen, zu welcher Tageszeit und an welchen Wochentagen sind Zugriffshäufungen) als auch nutzerbezogene Aussagen (welcher Browsertyp wird bevorzugt, regionale Zuordnung der Rechner). Mit individualisierten Auswertungen ließen sich auch die Interessen der einzelnen Nutzerinnen und Nutzer ausforschen (Nutzerprofile).

8.11.3 Empfehlungen zur Gestaltung und Verwendung

- ☞ Der Umfang der Protokolldaten sollte nach dem Grundsatz der Erforderlichkeit festgelegt, im Verfahrensverzeichnis dokumentiert und Nutzern bekannt gegeben werden (Datum, Uhrzeit, Rechner- oder Benutzerkennung, Fehlercode, Anzahl der übertragenen Bytes, Rechner- oder Benutzeridentifikation, eventuell Zieladresse des angeforderten Dokuments, Fehlercode der Übertragung).
- ☞ Die Verwendung der Protokolldaten muss an genau definierte Zwecke gebunden werden, so zum Beispiel zur Aufrechterhaltung der Systemsicherheit, zur Analyse und Korrektur technischer Fehler im Netz, zur Optimierung der Rechnerleistungen im Netzwerk, zur Ermittlung der Kosten verbrauchter Ressourcen zwecks interner Leistungsverrechnung sowie zur Kontrolle der Einhaltung dienst-/arbeitsrechtlicher Vorgaben. Der Zweck "Systemsicherheit" ist kein Freibrief für eine umfassende Protokollierung. Eine regelmäßige Speicherung der IP-Adressen ist unzulässig.
- ☞ Die Verwendungszwecke sind aus Gründen der Transparenz im Verfahrensverzeichnis zu dokumentieren, sie müssen den Nutzern vor Einstieg in das Angebot bekannt gegeben werden.
- ☞ Der Zugriff auf die Protokolldaten muss innerhalb der Behörde durch eine Dienstvereinbarung geregelt werden.
- ☞ Die Speicherungsdauer der Protokolldateien ist so kurz zu halten, wie dies zur Erfüllung der beschriebenen Zwecke erforderlich ist. Der Zeitrahmen von einem Monat sollte nach Möglichkeit nicht überschritten werden
- ☞ In begründeten Fällen von Missbrauch oder beim Verdacht strafbarer Handlungen kann eine weitergehende Einsicht in die Protokolldaten vorgenommen werden. Dabei sollte ein Verfahren gewählt werden, das die betroffene Person von dem Verdacht in Kenntnis setzt.

8.12 Anforderungen an ein zentrales OCSP/CRL-Relay

Nach dem Fachkonzept der VPS kann die Komponente OCSP/CRL-Relay grundsätzlich lokal eingerichtet und betrieben werden, wie jede andere der VPS auch. Um die Anbindung der Verzeichnisdienste von Zertifizierungsdiensteanbietern (ZDA) effizient administrieren zu können, wurde das OCSP/CRL-Relay allerdings so entworfen, dass

es auch zentral betrieben werden kann und damit vielen VPSn dient. Inzwischen wird seitens des Bundes auch der Betrieb dieser zentralen Komponente geplant und zeitnah umgesetzt.

Bei Nutzung der durch das zentrale OCSP/CRL-Relay angebotenen Funktionen sind nachfolgend genannte Datenschutzanforderungen zu beachten.

Ermitteln von Zertifikatsstatistiken

Das Relay führt die zur Validierung des Zertifikats notwendigen Prüfschritte durch und fasst die Ergebnisse zusammen. Eine abschließende Interpretation des Ergebnisses findet im Relay aber nicht statt.

Lokalisation von Zertifikaten anhand bestimmter Attribute

Hier werden die Zertifikate zu einer bestimmten E-Mail-Adresse gefunden und zugeordnet.

☞ Bei der Beschaffung fehlender Zertifikate aus öffentlich zugänglichen oder internen Datenbanken sind die Zweckbindung sowie das Recht auf Berichtigung, Sperrung und Löschung durch die betroffenen Zertifikatsinhaber zu beachten.

Extrahieren und Bereitstellen von Informationen aus Zertifikaten

Alle die Informationen, die Aussagen über den Sicherheitswert von Zertifikaten beinhalten, wie z. B. Nutzungsbeschränkungen, werden extrahiert und in Form von XML-Daten zur Verfügung gestellt.

Die Dienste des Relays werden dem anfragenden VPS-Kernsystem über eine einheitliche Schnittstelle via XKMS V 2.0 zur Verfügung gestellt. Als zentrale Einrichtung soll das OCSP/CRL-Relay Zertifikate anhand bestimmter Attribute (z. B. E-Mail-Adresse) lokalisieren, gültige Zertifikatsketten bilden und Informationen aus übermittelten Zertifikaten extrahieren. Diese sollen dann den anfragenden Anwendungen zur Verfügung gestellt werden.

Bei den im Relay verarbeiteten Zertifikatsdaten handelt es sich grundsätzlich um öffentlich zugängliche Daten. Einschränkungen können sich bei einer erweiterten Funktionalität hinsichtlich des Auffindens benötigter Zertifikate ergeben bzw. an der Berücksichtigung von Mandanten unterschiedlicher Anforderungen innerhalb des Relays.

Ergänzend sei angemerkt, dass das Relay alle Auskünfte der Verzeichnisdienste nicht nur in aufbereiteter Form, sondern auch im (signierten) Original an das abfragende System weitergibt. Dies kann sowohl für ergänzende „lokale“ Prüfungen als auch für Zwecke der Langzeitarchivierung nützlich bzw. erforderlich sein.

Anforderungen an den Zugriff auf die Relay-Daten und dessen Verfügbarkeit

☞ Sollen andere Instanzen als Kernsysteme Virtueller Poststellen Zugriffsrechte auf das Relay erhalten, sind die **Vertraulichkeit und Authentizität von Anfragen** zu sichern.

☞ Da die angebotene Dienstleistung des Relays für den Betrieb aller angeschlossenen VPSen notwendig ist, sind für die Sicherheitsziele **Verfügbarkeit und Systemsicherheit** besonders hohe Anforderungen zu beachten.

Anforderungen an den zentralen Relaybetreiber

Grundsätzlich kann ein zentrales Relay sowohl von einer öffentlichen Stelle als auch einer nichtöffentlichen Stelle betrieben werden. Ggf. ergeben sich hier aus dem Schutzbedarf der bearbeiteten Daten Einschränkungen.

☞ Für den zentralen Relaybetrieb muss entsprechend **geeignetes und qualifiziertes Personal** eingesetzt werden. Um das erforderliche Sicherheitsniveau der VPS an sich zu sichern, bedarf es für den zentralen Betrieb einer geeigneten Gestaltung der vertraglichen Bindung des externen Dienstleisters, insbesondere hinsichtlich der technisch-organisatorischen Maßnahmen.

☞ Die **Anbindung der Verzeichnisdienste** von Trust-Centern sollte die Verfügbarkeit der Auskünfte sicherstellen und alle gängigen Protokolle unterstützen.

☞ Von besonderer Bedeutung ist die Administration vor und während des Relaybetriebs. So sollen folgende **Administrationsrollen** unterschieden werden:

- Serveradministratoren (Datenbank und Betriebssystem-Zugriff, Betriebsüberwachung, Protokollierung),
- Netzwerkadministratoren (Betreuung der Netzwerkkomponenten, Protokollierung),
- Relayadministratoren (Konfiguration des Relays, Nutzeradministration, Trust-Center-Anbindung, Protokollierung, Vier-Augen-Prinzip),
- Schlüsseladministratoren (Konfiguration der Relay-Zertifikate und Einbindung der Root-Zertifikate, HSM-Zugriff, Protokollierung, Vier-Augen-Prinzip).

☞ Im Relaybetrieb ist eine **revisionssichere Protokollierung** durchzusetzen. Dazu dienen Monitoring-Mechanismen (via Syslog, SNMP etc.), die Durchsetzung von dezidierten Rechtebeschränkungen, die Regelung der Zugriffe auf den Log-Server, die Einbeziehung des behördlichen oder betrieblichen Datenschutzbeauftragten bei Kontrollen sowie bei der Erstellung und Durchsetzung eines Revisionskonzepts.

9 Notwendige Begleitmaßnahmen

9.1 Vorabkontrolle, Einführungskonzept, Dienstvereinbarung/Dienstanweisung

Im Rahmen einer gesamtheitlichen Betrachtungsweise sind die organisatorischen, technischen, personellen, finanziellen, rechtlichen und datenschutzrechtlichen Konsequenzen der Einführung der VPS in der jeweiligen Behörde im Vorfeld zu analysieren und zu bewerten.

Dieses Kapitel zeigt die zeitliche Abfolge notwendiger Aktivitäten für die Einführung der VPS angelehnt an den Phasenplänen des eGovernment-Handbuches des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auf.

9.1.1 Phase 1: Initialisierung

Der Einsatz einer VPS wirkt sich innerhalb der Behörde auf verschiedene Verantwortungsbereiche und Organisationseinheiten aus, so dass es geboten ist, die Einführung der VPS durch ein Projektteam vorbereiten und durchführen zu lassen.

Eine Beteiligung folgender Funktionsträger ist empfehlenswert:

IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Personalvertretung, Teamleiter vorhandener und betroffener eGovernment-Projekte, Fachverantwortliche von betroffenen Fachverfahren, Justitiariat, Revision, Poststelle bzw. der Registratur, Archivar, IT-Bereich ggf. auch des externen Dienstleisters, ggf. weitere Mitarbeiter aus den jeweils betroffenen Behördenbereichen bei Analyse der Anforderungen und Rahmenbedingungen, Konzeption und Realisierung der VPS.

Öffentliche Stellen des Bundes und der Länder bzw. der behördlich bestellte Datenschutzbeauftragte entsprechend der landesgesetzlichen Regelungen haben grundsätzlich vor Einführung automatisierter Verarbeitungen zu prüfen, ob die mit der automatisierten Verarbeitung verbundenen besonderen Risiken für die Rechte und Freiheiten der Betroffenen wirksam beherrscht werden können. Diese Risikoabschätzung ist im Rahmen einer Vorabkontrolle (§ 4 d Abs. 5 und 6 BDSG) durchzuführen.

Mitbestimmungsrechte des Personalrates sind je nach bundes- oder landesgesetzlicher Regelung bei der Gestaltung der Arbeitsplätze, bei der Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigen zu überwachen, bei der Einführung grundlegend neuer Arbeitsmethoden oder bei der Festlegung oder Veränderung des Umfangs der automatisierten Verarbeitung personenbezogener Daten der Beschäftigten zu beachten. Teilweise bestehen auch landesgesetzlich Regelungen, nach denen die Dienststelle einem Personalratsmitglied die Teilnahme an Projektgruppen, Planungsgruppen oder vergleichbaren Gruppen, die beteiligungspflichtige Maßnahmen vorbereiten, gestatten soll.

9.1.2 Phase 2: Kommunikationsstrategie

Mittels einer Kommunikationsstrategie, die alle Aspekte der elektronischen Kommunikation beinhaltet (neben natürlichen und juristischen Personen auch Anwendungen), ist die Abwicklung der sicheren Kommunikation der Behörde im Außen- und Innenverhältnis unter Einsatz einer VPS neu zu entscheiden. Es ist zu hinterfragen, ob eine vorhandene Ende-zu-Ende-Kommunikation in eine behörden- bzw. organisations- oder funktionsbezogene Kommunikation (zentrale Mailadresse als eine Art Auffangfunktion) umgestaltet werden kann. Hierzu ist im Rahmen einer organisatorischen Betrachtungsweise eine Klärung des Realisierungsbedarfs herbeizuführen.

9.1.3 Phase 3: Analyse einschl. Schutzbedarfsfeststellung

Die gewonnenen Erkenntnisse sind im Rahmen einer Analyse - unter Berücksichtigung der Schutzbedarfsfeststellung - sukzessiv für eine künftige Modellierung der Arbeitsabläufe mittels der VPS aufzubereiten.

Anhaltspunkt für einen Schutzbedarf „niedrig bis mittel“ könnte z. B. sein, wenn

- eine Beeinträchtigung des informationellen Selbstbestimmungsrechts durch den Einzelnen noch als geringfügig eingeschätzt würde;
- ein möglicher Missbrauch personenbezogener Daten nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen hätte;
- für den Betreiber der Anwendung nur eine geringe Ansehens- oder Vertrauensbeeinträchtigung zu erwarten wäre.

Anhaltspunkt für einen Schutzbedarf „hoch“ könnte z. B. sein, wenn

- eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen möglich erscheint;
- ein möglicher Missbrauch personenbezogener Daten erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen hätte;
- für den Betreiber der Anwendung eine breite Ansehens- oder Vertrauensbeeinträchtigung zu erwarten wäre.

Anhaltspunkt für einen Schutzbedarf „sehr hoch“ könnte z. B. sein, wenn

- eine besonders bedeutende Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen möglich erscheint;
- ein möglicher Missbrauch personenbezogener Daten für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten würde;
- für den Betreiber der Anwendung eine landes- bzw. bundesweite Ansehens- oder Vertrauensbeeinträchtigung denkbar ist.

Auf der Grundlage der gewonnenen Erkenntnisse ist über

- ☞ das notwendige Mechanismen- und Zertifikatsniveau für Verschlüsselungs-, Authentisierungs- und Signaturzertifikate orientiert an den Anforderungen aus Schutzbedarf, Beweiswert, Formerfordernis,
- ☞ die Notwendigkeit einer Ende-zu-Ende-Verschlüsselung sowie die Erstellung von qualifizierten Signaturen,
- ☞ die Einrichtung von behörden- bzw. organisations- oder funktionsbezogenen Postfächern,

- den Umgang mit Dokumenten, die eine bestimmte juristische Qualität erfüllen müssen (z. B.: Sicherstellung der Nachsignierung vor Ablauf der Gültigkeit der kryptographischen Algorithmen),
- den Einsatz von Verschlüsselungstechnik zur Transportsicherung,
- die zentrale oder dezentrale kryptographische Behandlung der ausgehenden Post

zu entscheiden.

Gesondert betrachtet werden muss in diesem Zusammenhang die Frage, ob aus rechtlichen Gründen (Schriftformerfordernis) die Anbringung einer qualifizierten Signatur erforderlich ist.

Bei der Frage der Auswahl und des Einsatzes bestimmter Zertifikate muss das gewünschte Einsatzfeld betrachtet werden. Aus Sicht des VPS-Einsatzes können Zertifikate im Innen- und im Außenverhältnis der Behörde (z. B.: zur internen Ver- bzw. Umschlüsselung, Authentisierung von Behördenmitarbeitern, Vorgangsbearbeitung, Authentisierung der Behörde oder Organisationseinheit, Authentisierung von Servern und Clients) erforderlich sein.

9.1.4 Phase 4: Konzeption

Für die Konzeption der VPS ist

- eine Ist-Aufnahme der IT-Komponenten und der bestehenden IT-Infrastruktur (Server-Systeme, verwendete E-Mail- und Web-Server, Firewalls, Anbindung an externe Netze, Netzbetreiber, Bandbreiten, etc.) zur Planung der konkreten physikalischen und logischen Anbindung der VPS,
- eine Ist-Aufnahme der IT-Organisation (Rollen, Aufgaben, Befugnisse, Qualifikationen, etc.) zur Entscheidung der Ergänzung oder Modifizierung der Organisationsstruktur,
- eine Auswahl des Standortes und des Betreibermodells,
- eine Entscheidung zur Anbindung von Verfahren und von weiteren Funktionalitäten,
- eine Festlegung organisatorischer und technischer Sicherheitsmaßnahmen

erforderlich.

Auswahl des Standortes

Bei der Wahl des Standortes sind folgende Lösungen denkbar:

- die Behörde betreibt an ihrem einzigen Standort bzw. an jedem ihrer Standorte eine VPS und setzt innerhalb der Behörde an ihrem einzigen Standort bzw. jedem ihrer Standorte
  - in zentraler Zuständigkeit eine nachgelagerte Poststelle,
  - in dezentraler Zuständigkeit mehrere nachgelagerte Poststellen,

  - ein abgestimmtes zentrales und dezentrales System von nachgelagerten Poststellen ein,

☞ die Behörde betreibt an einem Standort eine VPS und bindet die anderen Standorte über sichere Netze an die VPS an und setzt innerhalb der Behörde

  - in zentraler Zuständigkeit eine nachgelagerte Poststelle,
  - in dezentraler Zuständigkeit mehrere nachgelagerte Poststellen,
  - ein abgestimmtes zentrales und dezentrales System von nachgelagerten Poststellen ein,

☞ die Behörde schließt sich an eine durch Dritte zentral betriebene VPS an und setzt selbst eine nachgelagerte Poststelle

  - in zentraler Zuständigkeit innerhalb der eigenen Behörde,
  - in dezentraler Zuständigkeit innerhalb der eigenen Behörde,
  - in einem abgestimmten zentralen und dezentralen System ein.

Je nach Größenordnung der Behörde können bei einer zentralen Lösung einer VPS eine Vielzahl von Anwendungsszenarien zu bedenken sein, die sich im Detail erheblich unterscheiden. Für komplexe Anwendungsszenarien ist daher auch ein abgestimmtes zentrales und dezentrales System als Alternative denkbar. Bei einer solchen Architektur kann eine zentrale Poststelle Basisdienste übernehmen (z. B. Signaturverifikation, Transportsicherung, Zeitstempelprüfung), spezielle Anforderungen (z. B. die interne Verteilung) kann dann eine nachgelagerte Poststelle durchführen.

Anbindung von Verfahren

Sofern die VPS durch Fachanwendungen oder Hintergrundsysteme (Archivsysteme, Postbuchanwendung, Dokumentenmanagementsysteme, Workflow-Management-Systeme, Ausschreibungsprogramme, etc.) genutzt werden soll, ist eine Anpassung der bestehenden Applikationen bzw. Integration der VPS-Schnittstellen erforderlich.

Auch im Rahmen einer Web-Anwendung ist im Bereich der Benutzer- und Stammdatenverwaltung eine Erweiterung des Benutzerregistrierungsprozesses notwendig, damit die öffentlichen Zertifikate der externen Kommunikationsteilnehmer, die eine Registrierung zur Benachrichtigung wünschen, in einem Verzeichnisdienst gespeichert werden.

Anbindung und Bereitstellung weiterer Funktionalitäten

Die Positionierung der weiteren Funktionalitäten der VPS (z. B: Zeitstempeldienst, Zertifikatsanbieter) ist zu entscheiden. Sie wäre grundsätzlich in drei Varianten realisierbar:

- Alle Funktionalitäten sind integraler Bestandteil der VPS und können nur über deren Schnittstellen angesprochen werden.

- Die Funktionalitäten werden auf einer niedrigeren Architekturebene positioniert und könnten für weitere eGovernment-Anwendungen über einzelne zu definierende Schnittstellen direkt angesprochen werden.
- Die Basisdienste werden unterhalb der Modulebene identifiziert und realisiert.

Insgesamt ist die Anbindung und Bereitstellung folgender Funktionalitäten zu entscheiden:

Aufsetzen bzw. Anpassen von Verzeichnisdiensten, Veröffentlichung von Zertifikaten, Auswahl und Anbindung externer Zertifizierungsdiensteanbieter und Beantragung der Zertifikate

Folgende Verzeichnisse sind erforderlich:

- Verzeichnis für die zu nutzenden Zertifikate im Innenverhältnis,
- Verzeichnis für Zertifikate der Behörde zur Kommunikation durch externe Kunden mit der Behörde (Zertifikate im Außenverhältnis),
- Zertifikats-Verzeichnisses der externen Kunden.

Der Aufbau eines internen oder die Nutzung eines externen Verzeichnisdienstes ist zu entscheiden. Die Verzeichnisdienste sind vor unberechtigtem Zugang und Zugriff zu schützen. Die dauerhafte Verfügbarkeit sowie die Integrität der in den Verzeichnissen abgelegten Daten ist sicherzustellen. Ein interner Verzeichnisdienst ist in das Sicherheitskonzept der Behörde aufzunehmen. Aufgrund des Schutzbedarfs der damit gesicherten Informationswerte ist von einem hohen Schutzbedarf auszugehen.

Sofern die VPS-einsetzende Behörde Public-Key-Infrastructure (PKI) eines externen Dienstleisters nutzen will, sind die Nutzung des Verzeichnisses sowie die Rahmenbedingungen (z. B. Verfügbarkeit, Transportsicherungsmittel) vertraglich und technisch abzuklären. Dabei ist auch sicher zu stellen, dass möglichst wenige personenbezogene Daten gespeichert werden.

Anbindung OCSP/CRL-Relay

Die Komponente OCSP/CRL-Relay kann lokal oder zentral eingerichtet und betrieben werden. Sofern aus Sicht der Behörde die Dienstleistung eines externen OCSP/CRL-Relays in Anspruch genommen werden soll, ist ein entsprechender Dienstleister auszuwählen und die Inanspruchnahme vertraglich abzusichern.

Anbindung eines Zeitservers und /oder eines qualifizierten Zeitstempels

Es ist zu entscheiden, ob

- der Einsatz eines eigenen Zeitservers oder
- die Mitnutzung eines Zeitsignals einer anderen Behörde oder
- der Einsatz eines qualifizierten Zeitstempels eines Zertifizierungsdiensteanbieters

betrieben werden soll.

Um auch für nicht qualifizierte Zeitstempel eine ausreichende Qualität gewährleisten zu können, sollte die Systemzeit der jeweiligen VPS mit Hilfe des Network Time Protokolls (NTP) mit der Zeit eines Zeitservers synchronisiert werden.

Bei Einbindung eines qualifizierten Zeitstempeldienstes ist analog zur Auswahl des Zertifikatanbieters ebenfalls eine technische Prüfung der Schnittstellen auf Kompatibilität zur VPS durchzuführen und die Inanspruchnahme vertraglich abzusichern.

Bei der Nutzung des Zeitstempels zur Eingangs- und Ausgangsdokumentation muss der elektronische Ein- und Ausgangszeitpunkt der Behördeninfrastruktur festgelegt werden. Außerdem sollte durch technisch-organisatorische Maßnahmen sichergestellt werden, dass die Zeitstempel nachweisbar tatsächlich zum Zeitpunkt des Ein- bzw. Ausgangs (und nicht später) angebracht wurden. Diese Maßnahmen können sich nicht auf die VPS beschränken, sondern müssen das Kommunikationssystem insgesamt betrachten.

Einbindung von Viren- und Contentscanning

Die Einbindung von im Behördennetz vorhandenen Virenscannern ist zu berücksichtigen. Sofern weitergehende Inhaltsprüfungen erfolgen sollen, ist eine Übergabe von entschlüsselten Daten von der VPS an anzubindende Systeme über generische Schnittstellen der VPS zu berücksichtigen.

Betrieb eines Log-Servers

Zur Nutzung der von der VPS generierten Log-Meldungen - System-Logs und Administratoren-Logs (z. B. zu den Ereignissen: Mail-Empfang und Versand, Authentisierung eines Benutzers, Fehlerzustände etc.) - ist der Betrieb eines Log-Servers sowie einer Auswertestation erforderlich, welche die Informationen in regelmäßigen Abständen abfragt, verdichtet und archiviert. Diese Komponenten gehören nicht zum VPS-Kernsystem und müssen dementsprechend durch die Behörde beigestellt werden.

Festlegung organisatorischer und technischer Sicherheitsmaßnahmen

- ☞ Erstellung bzw. Fortschreibung des IT-Sicherheitskonzeptes, der IT-Sicherheitspolicy sowie des IT-Notfallkonzeptes,
- ☞ Erstellung einer Risikofolgenabschätzung und einer Verfahrensbeschreibung,
- ☞ Abschluss einer Dienstvereinbarung / Erlass einer Dienstanweisung zur Nutzung der VPS. Mögliche Regelungsinhalte können der Ziffer 9.3 entnommen werden.
- ☞ Erstellung einer Migrationsplanung,

  Im Rahmen dieser Planung sind alle notwendigen Umstellungsmaßnahmen in zeitlicher Abfolge zur Sicherstellung der Erreichbarkeit und verlustfreien Kommunikation der Behörde während der Einführung der VPS festzulegen.
- ☞ Erstellung eines Qualifizierungsplans für Administratoren und Benutzer.

9.1.5 Phase 5: Realisierung

Nach Test und der Vorabkontrolle durch den Datenschutzbeauftragten oder die öffentliche Stelle kann dann die Realisierung des Konzeptes erfolgen. Die Beteiligung des Personalrates ist zu berücksichtigen.

Eine Bereitstellung von Informationen auf der Homepage der Behörde für externe Kommunikationspartner zur Nutzung der VPS ist vorzubereiten.

Weiter ist eine Anpassung von innerbetrieblichen Anweisungen, Beschreibungen, Plänen und Dokumentationen, die durch die VPS-Implementierung berührt werden, vorzunehmen.

9.1.6 Phase 6: Einführung und Inbetriebnahme

Nach erfolgreichem Abschluss der notwendigen funktionalen Tests, des Pilotbetriebs, einer anschließenden IT-Sicherheitsrevision, der Qualifizierung des Personals und der Umsetzung aller organisatorischen Maßnahmen werden die neuen VPS-Dienstleistungen dann – ggf. schrittweise – in Betrieb genommen.

9.2 Gestaltung des Sicherheitskonzeptes (Systemdatenschutz)

Die VPS ist unter Sicherheitsaspekten entwickelt worden. Dazu sind Maßnahmen, mit denen die VPS möglichen Gefährdungen selber entgegen treten kann, implementiert worden.

Gleichwohl bleiben organisatorische Maßnahmen umzusetzen, um zusammen mit den technischen Maßnahmen die Sicherheitsziele der VPS zu erfüllen – insbesondere für Datensicherung, Notfallvorsorge und Revision. Diese organisatorischen Maßnahmen, d. h. die Bedingungen, unter denen die VPS sicher betrieben werden kann, werden typischerweise in einem IT-Sicherheitskonzept festgeschrieben,. Für eine solche Aufgaben bietet das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine hervorragende Herangehensweise, da zunächst mit der IT-Strukturanalyse und der Schutzbedarfsfeststellung die konkrete Realisierung der VPS und die Anforderungen spezifiziert und anschließend mit den Bausteinen des IT-Grundschutzhandbuchs in der Modellierung nachgebildet werden. Der Basis-Sicherheitscheck bietet anschließend eine Kontrolle, um die empfohlenen Maßnahmen mit der Realität abzugleichen und ggf. eine Realisierungsplanung für die Beseitigung von Defiziten oder die Optimierung der Sicherheit in der Zukunft vorzunehmen.

Um die Arbeit zur Erstellung eines Sicherheitskonzeptes der VPS zu erleichtern, ist ein „generisches Sicherheitskonzept für die Kern- und Webkomponenten der VPS“ erstellt worden, dass entsprechend dem momentanen Entwicklungsstand auf

- das VPS-Kernsystem,
- das OCSP/CRL-Relay,
- die Web-Client-Anwendungen sowie

- die Web-Server-Anwendungen

fokussiert, die im Rahmen des Projekts BundOnline 2005 von bremen online services GmbH & Co. KG entwickelt wurden.

In diesem generischen Sicherheitskonzept ist auf abstraktem Niveau für die Architektur und typische Einsatzszenarien entsprechend der Vorgehensweise des IT-Grundschutzhandbuchs eine IT-Strukturanalyse, eine Schutzbedarfsfeststellung sowie eine Modellierung mit ergänzender Sicherheitsanalyse durchgeführt worden. Das generische Sicherheitskonzept enthält Hinweise darauf, um daraus ein konkretes Sicherheitskonzept für eine konkrete Realisierung der VPS zu entwickeln, die dann die spezielle Konfiguration und Ausprägung der VPS mit Servern, Räumen, Anwendungsszenarien etc. berücksichtigt.

Das generische Sicherheitskonzept enthält damit Anforderungen,

- die der Betreiber von Komponenten der VPS umsetzen muss (vgl. Betreibermodelle),
- die in einem separaten Sicherheitskonzept jedoch weiter spezifiziert werden müssen und
- unter denen die VPS sicher betrieben werden kann, d. h. ihre postulierten Sicherheitsziele vollständig gewährleisten kann.

Das generische Sicherheitskonzept für die Kern- und Webkomponenten der VPS ist verfügbar unter http://www.bsi.bund.de/fachthem/egov/vps.htm.

9.3 Dienstvereinbarung / Dienstanweisung

Für den Einsatz der VPS und zur Steuerung des Verwaltungshandels sind Regelungen in Dienstvereinbarungen oder Dienstanweisungen notwendig.

Dienstvereinbarung

Inhalte einer Dienstvereinbarung können Eckpunkte über die Verarbeitung und Nutzung der personenbezogenen Daten der Beschäftigen, Daten- und Persönlichkeitsschutz, Rechte des Personalrates, Arbeitsplatzgestaltung und Arbeitsschutz, Benutzerbetreuung, Weiterbildungsangebote sein.

Dienstanweisung

Im Rahmen einer Dienstanweisung zur Nutzung der VPS sollten u.a. folgende Regelungen Berücksichtigung finden:

- ☞ Festlegung der Postfächer (behörden-, organisations-, funktionsbezogen; zentral oder dezentral bzw. benutzerbezogen in Abhängigkeit von den Ergebnissen der örtlichen Kommunikationsanalyse),
- ☞ Regelungen zur Organisation und Verwaltung der Postfächer, Zuständigkeiten und Verantwortungsbereiche – insbesondere dort wo es zu fach- oder amtsübergreifender Verantwortlichkeit kommt,

- ☞ Regelung zum Einsatz der verschiedenen Signaturen (fortgeschritten, qualifiziert bzw. qualifiziert mit Anbieterakkreditierung, Verwendung eines Pseudonyms),
- ☞ Verpflichtung zur Eintragung der Behördenangabe nach § 37 Abs. 3 VwVfG im qualifizierten Zertifikat oder im qualifizierten Attributzertifikat nach dem SigG,
- ☞ Regelungen zur Zugangseröffnung, Zugangsbeschränkung (z. B.: Ausschreibungen, Charakter, Geschäftsverkehr, Attachements, Attribute),
- ☞ Verfahrensregelungen zur elektronischen Kommunikation mit dem Bürger (Notwendigkeit der Einverständniserklärung für die elektronische Nachrichtenübermittlung sowie deren Beschaffung, Hinterlegung Änderung und Stornierung),
- ☞ Entscheidung zur Zulässigkeit oder zum Ausschluss der Privatnutzung (Nutzung der Signaturkarte als Amts- oder Funktionsträger),
- ☞ Sicherstellung von Datenschutz und Datensicherheit (getrennte Aufbewahrung von PIN und Signaturkarte, Ablage und Nutzung der Verschlüsselungszertifikate, Zugriff auf öffentliche Schlüssel der Kommunikationspartner),
- ☞ Regelungen zum Umgang und zur Verantwortung bei Gruppenzertifikaten, Verschlüsselungszertifikaten,
- ☞ Bestimmungen zum Aufbau- und zur Ablauforganisation (z. B.: zur Sicherstellung des Anwendungs-, Sicherheits-, Schlüsselmanagements und zur Sicherstellung der Kontrollrechte),
- ☞ Festlegung von Bearbeitungsregeln für ein- und ausgehende elektronische Post:
  - Bestimmungen zur Vertretungsregelung und zur Verwaltung von internen Vertretungs- und Berechtigungsregelungen,
  - Festlegung eines Rollen- und Zugriffsrechtekonzeptes (z. B.: Administrator, Revisor, Sachbearbeitung),
  - Sicherstellung der regelmäßigen Abfrage der Postfächer,
  - Entscheidung zur Erstellungsform der Empfangsquittungen für externe und ggf. auch interne Nachrichten,
  - Bearbeitungsregelungen für Input und Output mit höherem Vertraulichkeitsbedarf (Umverschlüsselung, Weiterleitung von verschlüsselten E-Mails bei Ende-zu-Ende-Sicherheit ohne weitere Aktionen der VPS),
  - Verfahrensregelungen zur Behandlung nicht geeigneter Eingänge (z. B. Speicherung von Nachrichten mit unvollständiger oder fehlerhafter Signatur oder von Dokumenten und Nachrichten, die nicht entschlüsselt werden konnten, Behandlung von Dokumenten und Nachrichten in einem nicht akzeptablen Datenformat),
  - Verfahrensregelungen zum Umgang mit bestimmten Prüfergebnissen (z. B. Zertifikatsprüfung: „Status undefiniert“),

- Sicherstellung einer Information an den Absender und ggf. den Empfänger bei Nachrichten, die fehlerhaft sind oder einen schädlichen Inhalt haben, o. ä.,
- Sicherstellung einer temporären Speicherung von Nachrichten mit schädlichem Inhalt in einer gesicherten Umgebung zu Beweiszwecken,
- Festlegung von Weiterleitungsregelungen,
- Verpflichtung zum Einsatz von Signatur- und Verschlüsselungszertifikaten nach dem Schutzstufenkonzept,
- Vorgaben zur Aufbewahrungsform von Verifikationsdaten (z. B: Übermittlungsprotokoll, Prüfprotokoll, Laufzettel der Transaktion),
- Sicherstellung der Nachsignierung vor Ablauf der Gültigkeit der kryptographischen Algorithmen,
- Sicherstellung der Zeitstempelnutzung,
- Festlegung der Zeichnungsbefugnisse,
- Regelungen zur Trennung von Signatur und Verschlüsselung mit gesicherter Ablage der Schlüssel (Schlüsselmanagement, Sperrlistenabfrage, Interner Verzeichnisdienst).

☞ Verpflichtung zur Datensicherung und Datenarchivierung (Übernahme in ein elektronisches Archiv) und Festlegung von Formaten mit Eignung für eine Langzeitspeicherung.

10 Betreibermodelle und deren inhaltliche Ausgestaltung

Die zunehmende Verlagerung der Datenverarbeitung auf andere Stellen erhöht das Gefährdungspotenzial für das Recht auf informationelle Selbstbestimmung. Werden im Rahmen der elektronischen Abwicklung Verwaltungsaufgaben oder einzelne Arbeitsabläufe auf eine andere Stelle übertragen, sind besondere datenschutzrechtliche Bestimmungen zu beachten. Dies wirft die Frage auf, wie dieser Vorgang datenschutzrechtlich bei einer VPS zu bewerten ist, insbesondere welche Voraussetzungen für eine rechtmäßige Übertragung vorliegen müssen und ob es Grenzen für eine derartige Übertragung gibt. Das Datenschutzrecht unterscheidet hierzu zwischen Datenverarbeitung im Auftrag und der Funktionsübertragung.

Bei der Auftragsdatenverarbeitung liegt die datenschutzrechtliche Verantwortung für die Verarbeitung und Nutzung der personenbezogenen Daten beim Auftraggeber, der „Herr“ seiner Daten bleibt. Er normiert die Anforderungen an die technischen und organisatorischen Maßnahmen zur Datensicherung und insbesondere zur Gewährleistung der Vertraulichkeit beim Auftragnehmer. Dem Auftragnehmer wird nur die tatsächliche Verarbeitung oder Nutzung nach Weisung und unter materieller Verantwortung des Auftraggebers, gewissermaßen als sein verlängerter Arm, übertragen. Bei der Datenverarbeitung im Auftrag wird damit lediglich eine „Hilfsfunktion“ der eigentlichen Aufgabe ausgelagert, ohne dass der Auftragnehmer einen eigenen Handlungs- oder Entscheidungsspielraum hat.

Werden dagegen die der Verarbeitung zugrunde liegenden Aufgaben oder Geschäftszwecke ganz oder teilweise abgegeben, erbringt der Übernehmende über die technische Durchführung hinaus materielle Leistungen mit Hilfe der überlassenen Daten oder bestehen Handlungs- und Entscheidungsspielräume bei der Erledigung der Aufgabe, liegt eine Funktionsübertragung vor. In diesem Fall wird der Auftragnehmer zur Daten verarbeitenden Stelle und hat für die materiell-rechtlichen Aspekte der Datenverarbeitung zu sorgen. Eine Funktionsübertragung ist nur zulässig, soweit eine Übermittlungsbefugnis existiert.

10.1 Rollen der VPS

Um für die VPS Betreibermodelle definieren und deren inhaltliche Ausgestaltung vornehmen und insbesondere datenschutzrechtlich einordnen zu können, werden den Funktionalitäten der VPS entsprechend drei Rollen identifiziert:

1. OSCI-Intermediär,
2. Operator,
3. Geschäftsstelle.

Ausprägungen und mögliche Betreibermodelle werden im Folgenden diskutiert.

10.1.1 Rolle als OSCI-Intermediär

Die OSCI-Kommunikation ist eine Funktionalität der VPS, in der ein OSCI-Intermediär Nachrichten empfängt und weiterleitet bzw. sie in Postfächern zur Abholung bereitstellt. Entsprechend des OSCI Transport 1.2-Protokolls können dabei OSCI-konforme Nachrichten ver- und entschlüsselt und Signaturen erstellt und geprüft werden. Darüber hinaus generiert der OSCI-Intermediär einen Laufzettel zur Protokollierung von Verbindungs- und Prüfinformationen. Der OSCI-Intermediär öffnet nur den „äußeren Briefumschlag“ einer OSCI-Kommunikation.

Die Rolle als Intermediär ist datenschutz-rechtlich als Teledienst zu bewerten (vgl. Abschnitt 5.3). Dieser „Provider“ kann von einer öffentlichen oder nicht-öffentlichen Stelle betrieben werden.

10.1.2 Rolle als Operator

Der Operator öffnet und schließt Briefumschläge mit Inhaltsdaten und prüft elektronische Signaturen, die die Integrität und Authentizität von Dokumenten und insbesondere Zertifikaten gewährleisten sollen. Technisch gesehen entschlüsselt er eingehende verschlüsselte Nachrichten und verschlüsselt ausgehende Nachrichten, die im Klartext vorliegen. Darüber hinaus beinhaltet die Aufgabe die Prüfung der mathematischen Korrektheit der Signatur sowie die Prüfung der Gültigkeit der zugehörigen Zertifikate. Entscheidend ist, dass der Operator Inhaltsdaten nicht gezielt zur Kenntnis nimmt, sondern automatisiert abarbeitet.

Die Rolle als Operator ist datenschutzrechtlich nicht mehr als Teledienst zu bewerten (vgl. Abschnitt 5.3).

Der Operator kann von einer Behörde selber betrieben werden oder im Rahmen eines Outsourcings durch einen Betreiber, der auch eine nicht-öffentliche Stelle sein kann, im Sinne einer Auftragsdatenverarbeitung erfolgen, sofern das einschlägige Datenschutzgesetz die Verarbeitung personenbezogener Daten einer öffentlichen Stelle durch eine andere öffentliche oder nicht-öffentliche Stelle zulässt und dem Outsourcing zu einer nicht-öffentlichen Stelle keine übergeordneten Rechtsnormen entgegenstehen .

10.1.3 Rolle als Geschäftsstelle

Die Geschäftsstelle nimmt Inhaltsdaten und Prüfergebnisse vom Operator entgegen und wertet sie aus – etwa, um sie der zuständigen Stelle zukommen zu lassen.

Die Rolle der Geschäftsstelle ist datenschutz-rechtlich weder als Teledienst noch als Auftragsdatenverarbeitung zu bewerten (vgl. Abschnitt 5.3). Da die Geschäftsstelle Inhaltsdaten eigenverantwortlich zur Kenntnis nimmt und auswertet, liegt beim Outsourcing eine Funktionsübertragung vor. Diese ist nur zulässig, sofern eine Übermittlungsbefugnis existiert.

10.2 Vertragliche Anforderungen zum Outsourcing

Sollen Aufgaben einer VPS – wie in Abschnitt 10.1 ausgeführt – durch Outsourcing (Auftragsdatenverarbeitung oder Funktionsübertragung) durchgeführt werden, ist bei der Ausgestaltung der Verträge zum Dienstleister wichtig, den Umfang der Dienstleistung exakt zu definieren.

Während im Gegensatz zur Funktionsübertragung bei der Auftragsdatenverarbeitung der Auftraggeber für die Datenverarbeitung verantwortlich bleibt, sind insbesondere hier die folgenden vertraglichen und technischen Aspekte für die Ausgestaltung der Verträge zu Dienstleistern wichtig:

- ☞ Benennung der Pflichten des Auftraggebers, der für die Datenverarbeitung verantwortlich bleibt,
- ☞ Formulierung der Kontrolltätigkeiten des Auftraggebers,
- ☞ Definition der Pflichten des Auftragnehmers, der personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach den Weisungen des Auftraggebers verarbeitet und die Zweckbindung beachtet,
- ☞ Beachtung der datenschutzrechtlich geforderten Rahmenbedingungen, inklusive Sicherheitskonzept, das die technisch-organisatorischen Maßnahmen dokumentiert,
- ☞ Sicherstellung der Kontrollrechte des behördlichen Datenschutzbeauftragten und der Datenschutzaufsichtsstellen,
- ☞ Beschreibung der Dokumentation,
- ☞ Beachtung des Datengeheimnisses, auch für die mit der Durchführung der Arbeiten beschäftigten Mitarbeiter,

- ☞ Aufnahme von Regelungen hinsichtlich der Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB bezüglich der verarbeiteten Daten und der zugehörigen Datenträger und hinsichtlich der Vorgehensweise bei Insolvenz- oder Vergleichsverfahren oder sonstigen Ereignissen,
- ☞ Zusicherung, dass Auskünfte durch den Auftragnehmer nur nach Zustimmung durch den Auftraggeber erfolgen. Verantwortlich und damit haftbar bleibt der Auftraggeber gegenüber den Betroffenen, falls ein Betroffener wegen einer unzulässigen oder unrichtigen Datenverarbeitung einen Schaden erleidet. Vertragliche Klärung des Binnenverhältnisses zwischen Auftraggeber und Auftragnehmer,
- ☞ Beschreibung von technischen und organisatorischen Details zur Zusammenarbeit,
- ☞ Formulierung von Kündigungsfristen, etwa wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen des Bundesdatenschutzgesetzes oder eines einschlägigen Landesdatenschutzgesetzes vorliegt.

11 Anforderungen und Handlungsempfehlungen zur Gewährleistung von Datenschutz und Datensicherheit eingeführter Anwendungsszenarien

11.1 Externer Mail-Benutzer sendet eine E-Mail

Initiierender Akteur: Externer Mail-Benutzer

Weitere Akteure: Interner Mail-Benutzer
Interner Browser-Benutzer
Interner Anwendungsbenutzer

Kurzbeschreibung: Eingehende Mail wird bearbeitet und weitergeleitet

Datenflüsse: Mail senden; Mail empfangen

Ziel: Mail wird an interne Empfänger weitergeleitet

Funktionalitäten	**Fundstelle:**
Authentisierung des Kommunikationspartners	**8.6**
Behandlung von Input mit höherem Vertraulichkeitsbedarf	**8.1**
Behandlung von Protokolldaten	**8.11**
Bereitstellen von Zeitstempeln/ Zeitstempelprüfung	**8.3**
Contentprüfung	**8.5**
Dienstvereinbarung	**9.3**
Dokumentation auf einem Laufzettel	**8.8**

Erstellung von Eingangs- und Ausgangsbestätigungen und Behandlung fehlerhafter Vorgänge	**8.9**
Fehlerbehandlungsmechanismen	**8.4/8.5**
Generierung des Laufzettels	**8.8**
Nutzung eines internen Verzeichnisdienstes	**8.1**
Prüfung auf schädliche Inhalte	**8.4**
Quittungsmechanismen	**8.9**
Signaturbildung/ Signaturprüfung	**8.2**
Speicherung der Authentisierungsdaten und Zertifikate der Kommunikationspartner	**8.7**
Vertraulichkeit, Verschlüsselung/ Entschlüsselung	**8.1**
Weiterleitung des Inputs	**8.1**

11.2 Interner Mail-Benutzer sendet eine E-Mail

Initiierender Akteur: Interner Mail-Benutzer

Weitere Akteure: Externer Mail-Benutzer
Externer Browser-Benutzer
Externer Anwendungsbenutzer

Kurzbeschreibung: Ausgehende Mail wird bearbeitet und weitergeleitet

Datenflüsse: Mail senden; Mail empfangen

Ziel: Mail wird an externe Empfänger weitergeleitet

Funktionalitäten	**Fundstelle:**
Authentisierung des Kommunikationspartners	**8.6**
Behandlung von Input mit höherem Vertraulichkeitsbedarf	**8.1**
Behandlung von Protokolldaten	**8.11**
Bereitstellen von Zeitstempeln/ Zeitstempelprüfung	**8.3**
Contentprüfung	**8.5**
Dienstvereinbarung	**9.3**
Dokumentation auf einem Laufzettel	**8.8**
Entfernen von Metainformationen im Output (insbesondere in Office-Produkten)	**8.5**
Erstellung von Eingangs- und Ausgangsbestätigungen und Behandlung fehlerhafter Vorgänge	**8.9**
Fehlerbehandlungsmechanismen	**8.4/8.5**
Generierung des Laufzettels	**8.8**
Nutzung eines internen Verzeichnisdienstes	**8.1**
Prüfung auf schädliche Inhalte	**8.4**

Quittungsmechanismen	**8.9**
Signaturbildung/ Signaturprüfung	**8.2**
Speicherung der Authentisierungsdaten und Zertifikate der Kommunikationspartner	**8.7**
Vertraulichkeit, Verschlüsselung/ Entschlüsselung	**8.1**
Weiterleitung des Inputs	**8.1**

11.3 Externer Browser- oder Anwendungsbenutzer stellt ein Dokument ein

Initiierender Akteur: Externer Browser-Benutzer
Externer Anwendungsbenutzer

Weitere Akteure: Interner Mail-Benutzer
Interner Browser-Benutzer
Interner Anwendungsbenutzer

Kurzbeschreibung: Eingehendes Dokument wird bearbeitet und weitergeleitet

Datenflüsse: Dokumente einstellen und abholen, Authentisierung, Verifikation von Signaturen

Ziel: Dokument wird an interne Empfänger weitergeleitet

Funktionalitäten	**Fundstelle:**
Authentisierung des Kommunikationspartners	**8.6**
Behandlung von Input mit höherem Vertraulichkeitsbedarf	**8.1**
Behandlung von Protokolldaten	**8.11**
Bereitstellen von Zeitstempeln/ Zeitstempelprüfung	**8.3**
Contentprüfung	**8.5**
Dienstvereinbarung	**9.3**
Dokumentation auf einem Laufzettel	**8.8**
Einbindung in die Anwendungen	**8.10**
Erstellung von Eingangs- und Ausgangsbestätigungen und Behandlung fehlerhafter Vorgänge	**8.9**
Fehlerbehandlungsmechanismen	**8.4/8.5**
Generierung des Laufzettels	**8.8**
Nutzung eines internen Verzeichnisdienstes	**8.1**
Prüfung auf schädliche Inhalte	**8.4**
Quittungsmechanismen	**8.9**
Signaturbildung/ Signaturprüfung	**8.2**
Speicherung der Authentisierungsdaten und Zertifikate der Kommunikationspartner	**8.7**
Vertraulichkeit, Verschlüsselung/ Entschlüsselung	**8.1**
Weiterleitung des Inputs	**8.1**

11.4 Interner Browser- oder Anwendungsbenutzer stellt ein Dokument ein

Initiierender Akteur: Interner Browser-Benutzer
Interner Anwendungsbenutzer

Weitere Akteure: Externer Mail-Benutzer
Externer Browser-Benutzer
Externer Anwendungsbenutzer

Kurzbeschreibung: Ausgehendes Dokument wird bearbeitet und weitergeleitet

Datenflüsse: Dokumente einstellen und abholen, Authentisierung, Verifikation von Signaturen

Ziel: Dokument wird an externe Empfänger weitergeleitet

Funktionalitäten	**Fundstelle:**
Authentisierung des Kommunikationspartners	**8.6**
Behandlung von Input mit höherem Vertraulichkeitsbedarf	**8.1**
Behandlung von Protokolldaten	**8.11**
Bereitstellen von Zeitstempeln/ Zeitstempelprüfung	**8.3**
Contentprüfung	**8.5**
Dienstvereinbarung	**9.3**
Dokumentation auf einem Laufzettel	**8.8**
Einbindung in die Anwendungen	**8.10**
Entfernen von Metainformationen im Output (insbesondere in Office-Produkten)	**8.5**
Erstellung von Eingangs- und Ausgangsbestätigungen und Behandlung fehlerhafter Vorgänge	**8.9**
Fehlerbehandlungsmechanismen	**8.4/8.5**
Generierung des Laufzettels	**8.8**
Nutzung eines internen Verzeichnisdienstes	**8.1**
Prüfung auf schädliche Inhalte	**8.4**
Quittungsmechanismen	**8.9**
Signaturbildung/ Signaturprüfung	**8.2**
Speicherung der Authentisierungsdaten und Zertifikate der Kommunikationspartner	**8.7**
Vertraulichkeit, Verschlüsselung/ Entschlüsselung	**8.1**
Weiterleitung des Inputs	**8.1**

11.5 Authentisierung eines externen oder internen Browser-Benutzers

Initiierender Akteur: Externer Browser-Benutzer

Interner Browser-Benutzer

Weitere Akteure: PIN/TAN, PKI-1, Trust-Center

Kurzbeschreibung: Authentisierung eines Browser-Benutzers

Datenflüsse: Authentisierung, Verifikation von Signaturen

Ziel: Browser-Benutzer ist authentifiziert

Funktionalitäten	**Fundstelle:**
Authentisierung des Kommunikationspartners	**8.6**
Dienstvereinbarung	**9.3**
Einbindung in die Anwendungen	**8.10**
Fehlerbehandlungsmechanismen	**8.4/8.5**
Nutzung eines internen Verzeichnisdienstes	**8.1**
Signaturbildung/ Signaturprüfung	**8.2**
Speicherung der Authentisierungsdaten und Zertifikate der Kommunikationspartner	**8.7**

11.6 Externer oder interner Browser-Benutzer verifiziert ein Dokument

Initiierender Akteur: Externer Browser-Benutzer
Interner Browser-Benutzer

Weitere Akteure: PKI-1, Trust-Center

Kurzbeschreibung: Signiertes Dokument wird verifiziert und das Prüfprotokoll an den Browser-Benutzer weitergeleitet

Datenflüsse: Authentisierung, Verifikation von Signaturen

Ziel: Prüfprotokoll an Browser-Benutzer

Funktionalitäten	**Fundstelle:**
Dienstvereinbarung	**9.3**
Fehlerbehandlungsmechanismen	**8.4/8.5**
Signaturbildung/ Signaturprüfung	**8.2**
Speicherung der Zertifikatsdaten	**8.7**

11.7 Authentisierung eines externen oder internen Anwendungsbenutzers

Initiierender Akteur: Externer Anwendungsbenutzer

Interner Anwendungsbenutzerbenutzer

Weitere Akteure: PIN/TAN, PKI-1, Trust-Center

Kurzbeschreibung: Authentisierung eines Anwendungsbenutzer

Datenflüsse: Authentisierung, Verifikation von Signaturen

Ziel: Anwendungsbenutzer ist authentifiziert

Funktionalitäten	**Fundstelle:**
Authentisierung des Kommunikationspartners	**8.6**
Dienstvereinbarung	**9.3**
Einbindung in die Anwendungen	**8.10**
Fehlerbehandlungsmechanismen	**8.4/8.5**
Nutzung eines internen Verzeichnisdienstes	**8.1**
Signaturbildung/ Signaturprüfung	**8.2**
Speicherung der Authentisierungsdaten und Zertifikate der Kommunikationspartner	**8.7**

11.8 Externer oder interner Anwendungsbenutzer verifiziert ein Dokument

Initiierender Akteur: Externer Anwendungsbenutzer
Interner Anwendungsbenutzer

Weitere Akteure: PKI-1, Trust-Center

Kurzbeschreibung: Signiertes Dokument wird verifiziert und das Prüfprotokoll an den Anwendungsbenutzer weitergeleitet

Datenflüsse: Authentisierung, Verifikation von Signaturen

Ziel: Prüfprotokoll an Anwendungsbenutzer

Funktionalitäten	**Fundstelle:**
Dienstvereinbarung	**9.3**
Einbindung in Anwendungen	**8.10**
Fehlerbehandlungsmechanismen	**8.4/8.5**
Signaturbildung/ Signaturprüfung	**8.2**
Speicherung der Zertifikatsdaten	**8.7**

11.9 Backend-System lässt ein Dokument bearbeiten

Initiierender Akteur: Backend-System

Kurzbeschreibung: Dokument wird bearbeitet und zurückgegeben

Datenflüsse: Dokumente einstellen und abholen

Ziel: Dokument wird an Backend-System zurückgegeben

Funktionalitäten	**Fundstelle:**
Authentisierung des Kommunikationspartners	**8.6**
Behandlung von Protokolldaten	**8.11**
Bereitstellen von Zeitstempeln/ Zeitstempelprüfung	**8.3**
Contentprüfung	**8.5**
Dienstvereinbarung	**9.3**
Dokumentation auf einem Laufzettel	**8.8**
Einbindung von Anwendungen	**8.10**
Erstellung von Eingangs- und Ausgangsbestätigungen und Behandlung fehlerhafter Vorgänge	**8.9**
Fehlerbehandlungsmechanismen	**8.4/8.5**
Generierung des Laufzettels	**8.8**
Nutzung eines internen Verzeichnisdienstes	**8.1**
Prüfung auf schädliche Inhalte	**8.4**
Signaturbildung/ Signaturprüfung	**8.2**
Speicherung der Authentisierungsdaten und Zertifikate der Kommunikationspartner	**8.7**
Vertraulichkeit, Verschlüsselung/ Entschlüsselung	**8.1**
Weiterleitung des Inputs	**8.1**

12 Pilotprojekte/ erste Praxiserfahrungen

12.1 BundOnline 2005

Im Rahmen von BundOnline 2005 will die deutsche Bundesverwaltung alle onlinefähigen Dienstleistungen bis zum Jahr 2005 im Internet anbieten. Um hier Synergieeffekte zu erschließen werden im Rahmen dieser Initiative zentrale **Basiskomponenten** zur Verfügung gestellt und im Rahmen von entsprechenden **Kompetenzzentren** zusätzliche, externe Beratungskapazitäten erbracht. **Als BundOnline 2005 Basiskomponente „Datensicherheit“ wird eine „Virtuelle Poststelle“ (VPS) entwickelt und als Produkt bereitgestellt.** Diese Komponente wird sowohl für die elektronischen Kommunikationswege Web und E-Mail als auch für die Bedürfnisse von Backend-Systemen kryptographische Operationen (Verschlüsselung, Signatur, Authentisierung) jeweils behördenweit zentralisiert bündeln.

12.1.1 Leistungsumfang

Die VPS des Bundes liegt als „Referenzarchitektur“ den Ausführungen dieser Broschüre zu Grunde (vgl. Kapitel 7). Ihre Funktionalität und Architektur wurde daher bereits ausführlich beschrieben. Knapp zusammengefasst erbringt die VPS des Bundes folgende Funktionen in serverbasierter Form:

- Verschlüsselung und Entschlüsselung,
- Umverschlüsselung zentral entschlüsselter Eingangsdaten mit einem internen Verfahren zur Weiterleitung im Hausnetz,
- Signaturbildung und -prüfung mit skalierbaren Signaturniveau,
- Abwicklung (des kryptographischen Anteils) von Authentisierungsverfahren,
- Bereitstellen von Zeitstempeln (Erzeugung interner und Einholung externer, insbesondere qualifizierter Zeitstempel),
- Zeitstempelprüfung,
- Einbindung von im Behördennetz vorhandenen Virenscannern,
- Dokumentation aller Aktionen der VPS auf einem Laufzettel (VPS-Laufzettel),
- Erstellung und Versand von Quittungen für den Absender; konfigurierbar hinsichtlich des Anlasses (z. B. Eingang, Ausgang), des Inhaltes sowie der Signaturqualität (keine, fortgeschritten oder qualifiziert),
- Einbindung interner und externer Verzeichnisdienste,
- Lokalisieren von Zertifikaten in öffentlich zugänglichen Verzeichnisdiensten,
- Administrationsfunktionen.

Diese Funktionalitäten werden gemeinsam für E-Mail- und Web-basierte Kommunikation sowie und für die Bedürfnisse von Backend-Systemen innerhalb der Behörde angeboten. Diese einheitliche Bereitstellung der kryptographischen Funktionen, Algorithmen und Schlüssel verfolgt das Ziel, den kryptographie-spezifischen Administrationsaufwand gering zu halten und die Bereitstellung der eGovernment-Dienstleistungen aus sicherheitstechnischer Sicht zu optimieren. Besonders wichtig ist für eine *Basiskomponente*, dass verschiedene Anwendungen mit unterschiedlichsten Anforderungen unterstützt werden können. Hier kommt der breiten **Skalierbarkeit der Sicherheitsfunktionaliäten**, insbesondere der Signaturmechanismen von der einfachen bis zur qualifizierten Signatur, eine besondere Bedeutung zu. Dabei spielt übrigens die „Umgehung“ der oft beklagten Interoperabilitätsprobleme eine nicht zu unterschätzende Rolle. Eine wichtige Anforderung an die Gestaltung der VPS ist, dass für die Behörden in allen Bereichen, in denen dies notwendig oder gewünscht ist, **die „klassische“ Ende-zu-Ende-Sicherheit ohne Einschränkung möglich bleiben muss.**

Kennzeichnendes Merkmal der Architektur der VPS des Bundes ist die bewusste Beschränkung auf das Leistungsspektrum eines Kryptographieservers. Es werden ge-

zielt solche Funktionalitäten angeboten, die für eine größere Anzahl von eGovernment-Dienstleistungen oder Kommunikations-Systemen gemeinsam nutzbar sind. Aus diesem Grund wird die „finale“ Version der VPS des Bundes z. B. zwar eine Schnittstelle zu Virenscannern, aber nicht zu anderen Contentscannern anbieten. Bei letzteren ist zur Zeit keine Technologie erkennbar, die unabhängig von fachspezifischen Anforderungen einen *allgemeinen* Nutzen bietet.

Das XML-basierte Transportprotokoll **OSCI** (Online Services Computer Interface), das auf dem Web-Services Standard SOAP basierend kryptographische Sicherheitsmechanismen wie Verschlüsselung, Signatur und Authentisierung in skalierbarer Form zur Verfügung stellt, berücksichtigt in besonderem Maße die Anforderungen an Kommunikationssicherheit im eGovernment. Wesentliches Merkmal ist die Aufteilung der Kommunikation auf die Rollen Client – Intermediär – Backend. In Erweiterung des ursprünglichen Konzepts umfasst die Virtuelle Postelle (VPS) einen sog. **OSCI-Enabler**, der in Form einer verteilten Architektur die OSCI-Kommunikation auf allen drei im Protokoll vorgesehenen Ebenen unterstützt. Dieser OSCI-Enabler besteht auf den drei OSCI-Ebenen im Wesentlichen aus jeweils „angereicherten“ API’s, welche die Einbindung von Fachapplikationen über OSCI oder auch auf Client-Seite die direkte Interaktion des Benutzers ermöglichen.

Eine eigenständige Anwendung ist das **Elektronische Gerichts- und Verwaltungspostfach (EGVP),** das allen Bundesbehörden im Rahmen von BundOnline 2005 ebenfalls lizenzkostenfrei zur Verfügung gestellt wird. Hierbei können in einer Art „Web-Mail“ Freitexte und beliebige Anhänge abgesichert über die Mechanismen von OSCI in asynchronen Kommunikationsszenarien übertragen werden. Für die Nutzer werden alle benötigten Komponenten (mit Ausnahme der Signaturkarte und des Chipkartenlesers für die qualifizierte Signatur) als JAVA Web-Start-Applets über das Web bereitgestellt.

Die VPS unterstützt damit Behörden und eGovernment-Kunden beim Einsatz des OSCI-Protokolls auf allen drei Ebenen (Client-Intermediär-Backend), zwingt aber nicht dazu, es einzusetzen.

12.1.2 Realisierungsstand

Die Bereitstellung der VPS für die Bundesbehörden erfolgt im Rahmen von BundOnline 2005 in einem mehrphasigen Prozess. Am Anfang stand die Entwicklung eines Fachkonzepts und eines DV-technischen Grobkonzepts durch IBM Global Services unter fachlicher Leitung des BSI. Anschließend wurde nach einer Marktsichtung die Entscheidung getroffen, dieses Konzept durch Weiterentwicklung und Integration zweier existierender Produkte, nämlich Governikus von bremen online services für die Web- und Kernkomponenten sowie Julia MailOffice von ICC für die Mailkomponente, umzusetzen. **Seit dem 01.01.2004 steht eine erste Version der VPS für Bundesbehörden zur Verfügung;** über eine Zwischenversion im Frühjahr 2004 soll **im Herbst 2004 eine Version, welche das Konzept in allen wesentlichen Punkten umsetzt, zur Verfügung stehen**.

Wesentlicher Bestandteil der Realisierung ist die Erarbeitung eines **generischen Sicherheitskonzepts**, dass die einsetzenden Behörden in die Lage versetzen soll, die VPS als zentrales Sicherheitssystem in existierende oder auszubauende Sicherheitskonzepte und -architekturen optimal zu integrieren.

12.1.3 Piloten

Seit dem 01.01.2004 befindet sich eine erste Version der VPS beim **Luftfahrtbundesamt (LBA)** in Braunschweig im Pilotbetrieb. Mit ihrer Hilfe wird die BundOnline 2005-Dienstleistung „Strahlenschutz für fliegendes Personal“ unterstützt. Hierbei geben die in Deutschland registrierten Fluggesellschaften Angaben über die Flugstunden ihres fliegenden Personal – ausschließlich in elektronischer Form - an das LBA weiter. Diese Daten werden zum Zwecke der Ermittlung der (bei Flügen erhöhten) Strahlenbelastung ausgewertet und an das Bundesamt für Strahlenschutz weitergeleitet. Die Meldung der Fluggesellschaft muss mit der qualifizierten Signatur eines (zeichnungsberechtigen) Mitarbeiters versehen sein. Die Kommunikation erfolgt Web-basiert mit Nutzung der OSCI-Mechanismen. Bereits im ersten Monat konnten über 180 qualifiziert signierte Anträge problemlos bearbeitet werden, ohne dass die Nutzung von Zertifikaten nur eines Anbieters vorgegeben werden musste. Informationen zu dieser eGovernment-Dienstleistung stellt das LBA unter der URL: http://www.lba.de/deutsch/betrieb/strahlensch/strahlensch.htm zur Verfügung.

Eine weitere BundOnline 2005-Pilotdienstleistung mit VPS-Einsatz wird ab dem Sommer 2004 durch das **Bundesamt für Naturschutz (BfN)** in Bonn erbracht. Die Dienstleistung CITES Online ermöglicht es, die für die Erlaubnis der Ein- und Ausfuhr von Tier- und Pflanzenarten, die nach dem Washingtoner Artenschutzabkommen geschützt sind, erforderlichen Anträge in elektronischer Form einzureichen. Diese müssen qualifiziert signiert sein. Die Kommunikation erfolgt ebenfalls Web-basiert mittels OSCI. Informationen des BfN hierzu sind unter http://www.bfn.de/04/index.htm verfügbar.

Im Rahmen des BundOnline 2005-Projekts **Elektronischer Rechtsverkehr** werden zunächst das **Bundesverwaltungsgericht** in Leipzig und der **Bundesfinanzhof** in München die rechtssichere und rechtsverbindliche elektronische Kommunikation mit den zugelassenen Rechtsanwälten einführen. Dabei kommt das „Elektronische Gerichts- und Verwaltungspostfach“ (EGVP) zum Einsatz.

Weitere eGovernment-Dienstleistungen aus BundOnline 2005 werden im Laufe der Jahre 2004 und 2005 ihren Betrieb mit der VPS aufnehmen. Es werden dabei sowohl Web-basierte als auch E-Mail-gestützte Kommunikationswege unterstützt. Eine ständig aktualisierte Übersicht der laufenden BundOnline 2005-Dienstleistungen ist auf der zentralen Informationsplattform http://www.bundonline2005 verfügbar.

12.1.4 Datenschutz

Da die VPS des Bundes als „Referenzarchitektur“ dieser Broschüre dient, lassen sich praktisch alle hier gegebenen Handlungsempfehlungen als Hinweise für den datenschutzgerechten Einsatz dieser Basiskomponenten ansehen.

Die VPS des Bundes trägt als Basiskomponente Datensicherheit wesentlich zu einer sicheren und verbindlichen elektronischen Kommunikation im eGovernment zwischen der Verwaltung und ihren Kunden bei. Durch das zentrale Angebot von Sicherheitsdienstleistungen wie Verschlüsselung, Signatur oder Authentisierung werden diese oft komplexen kryptographischen Funktionen leichter administrierbar und auch automatisiert für einen massenhaften Einsatz nutzbar. Selbstverständlich müssen dazu Prinzipen der datenschutzgerechten Technikgestaltung in Realisierung und Betrieb berücksichtigt werden. So erfolgt in der VPS keine dauerhafte Speicherung der Inhaltsdaten. Hierdurch wird dem Gebot der Datensparsamkeit und der Zweckbindung Rechnung getragen. Die VPS steht grundsätzlich auch zur Nutzung in anonymisierter oder pseudonymisierter Form zur Verfügung. Die Skalierbarkeit der Sicherheitsmechanismen und die verschiedenen Modelle zur Umverschlüsselung erlauben es, individuellen Schutzbedürfnissen auch in Bezug auf personenbezogene Daten zu genügen.

Durch die im OSCI-Protokoll vorgesehene kryptographische Trennung in Inhalts- und Nutzungsdaten hat der OSCI-Intermediär keine Möglichkeit, auf die ggf. personenbezogenen Inhaltsdaten zuzugreifen. Mit der VPS-Architektur kann durch das Zusammenspiel von OSCI-Manager, VPS-Kernsystem und OCSP/CRL-Relay die Intermediärs-Rolle realisiert werden. Durch die Trennung in Inhalts- und Nutzungsdaten werden die Vorgaben des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) konsequent umgesetzt. Hierdurch ergeben sich weitreichende Möglichkeiten auch für eine externe Beauftragung von Dienstleistern.

12.1.5 Ansprechpartner

Die VPS des Bundes ist die Basiskomponente „Datensicherheit“ der Initiative BundOnline 2005. Informationen zu BundOnline 2005 findet man über http://www.bundonline2005.de

Ansprechpartner beim BSI:

Dr. Christian Mrugalla

Bundesamt für Sicherheit in der Informationstechnik

Referat I 1.1

Postfach 200363

53133 Bonn

E-Mail: egov@bsi.bund.de

Informationen im Web: http://www.bsi.bund.de/fachthem/egov/vps.htm

12.2 NRW

Die Virtuelle Poststelle des Bundes basiert auf der Software Governikus von bremen online services für die Kern- und Webkomponenten.

Eine Ausprägung der Clients und Backends zu Governikus wurde für Nutzer und Behörden in NRW nach den Anforderungen des Landes entwickelt und ist derzeit bei

verschiedenen Landesbehörden in Erprobung. Zentrale Plattform ist der im Landesrechenzentrum auch für andere Anwendungen installierte Governikus. Als Besonderheit ist ein zentrales Mail-Gateway integriert, so dass Behörden signierte Nachrichten nach der Signaturprüfung durch Governikus auch als E-Mail mit anliegendem Prüfprotokoll erhalten können. Das System kann nach der Verabschiedung des Elektronik-Anpassungsgesetz im Juli 2004 und die damit verbundene Änderung des Verwaltungsverfahrensgesetzes für das Land NRW in den Wirkbetrieb gehen, sobald Behörden den Zugang für die elektronische Kommunikation mit qualifizierten elektronischen Signaturen nach dem Signaturgesetz eröffnet haben.

Eine modifizierte Ausprägung von Clients und Backends von Governikus ist in der Justiz in NRW in verschiedenen Gerichten in Erprobung. Hier werden die Nachrichten um gerichtsspezifische Metadaten ergänzt, die eine Weiterverarbeitung mit dem jeweiligen Dokumentenmanagementsystem erleichtern.

Ansprechpartner IM NRW

Dr. Markus Brakmann

+49(0)2118712056

markus.brakmann@im.nrw.de

Ansprechpartner Justiz

Götz Heine

OVG Münster

+49 (0251) 505307

goetz.heine@ovg.nrw.de

Informationen im Web: http://www.im.nrw.de und http://www.im.nrw.de/inn/159.htm

12.3 Niedersachsen

Die für Nordrhein-Westfalen entwickelte Client- und Backend-Software als Anwendung auf Governikus wurde erfolgreich in Niedersachsen mit vier Gemeinden getestet, damit die Kommunen sich auch dort auf das geänderte Verwaltungsverfahrensgesetz vorbereiten können. Betreiber des zentralen Governikus war dort die HannIT als Rechenzentrum der Region Hannover, unterstützt wurde das Projekt durch den niedersächsischen Städtetag, der die Ergebnisse auch als Muster für andere Gemeinden dokumentiert hat. Der niedersächsische Städte- und Gemeindebund sowie der niedersächsische Landkreistag haben das Projekt ebenfalls begleitet, außerdem je ein Vertreter des Innenministeriums und des niedersächsischen Datenschutzbeauftragten.

Ansprechpartner

Torsten Sander

GF der HannIT

+49 (0511) 616 21421

torsten.sander@hannit.de

12.4 Bremen

Die Virtuelle Poststelle des Bundes basiert auf der Software Governikus von bremen online services für die Kern- und Webkomponenten sowie Julia MailOffice von ICC für die Mailkomponente.

Eine Ausprägung von Clients und Backends von Governikus ist in der Justiz in Bremen in verschiedenen Gerichten in Erprobung. Hier werden die Nachrichten um gerichtsspezifische Metadaten ergänzt, die eine Weiterverarbeitung mit dem jeweiligen Dokumentenmanagementsystem erleichtern.

Ansprechpartner

Heide Vathauer

Freie Hansestadt Bremen - Der Senator für Finanzen

+49 (0) 421 361 10709

HVathauer@finanzen.bremen.de

13 Wichtige Links

In der Handreichung sind zu den wesentlichen Aussagen und Empfehlungen Internet-Adressen zur weiteren Recherche aufgenommen worden. An dieser Stelle finden Sie noch einmal die wichtigsten übergreifenden Internet-Adressen zum Thema „VPS“.

Linkadressen	**Stelle – Inhalt**
www.bsi.bund.de/fachthem/egov/vps.htm	Informationen zur VPS des Bundes auf den Seiten des Bundesamts für Sicherheit in der Informationstechnik
www.osci.de	Informationen zum Datenformats- und Datentransport-Standard OSCI, zur OSCI-Leitstelle sowie dem Stand der damit verbundenen Projekte.
www.archisig.de	Informationen zur langfristigen und beweiskräftigen Aufbewahrung elektronisch signierter Dokumente
www.bos-bremen.de/service/kap5_4.html	Mit den hier verfügbaren **Anwendertools** können Governikus-Anwendungen getestet werden. Dazu stehen verschiedene Funktionen wie Signatur, PIN-Verwaltung und GeldKarten-Zahlung zur Verfügung. Mit dem ebenfalls verfügbaren **Zertifikatsmanager** kann eine Signaturkarte

	freigeschaltet oder die PIN geändert werden. Ebenso besteht die Möglichkeit, sich das Signaturniveau der verwendeten Karte anzeigen zu lassen. Mit dem **Testformular** kann die Funktionsweise von Governikus von der Nutzerseite aus getestet werden (mit qualifizierter Signatur, Software-Zertifikat oder ohne Signatur). Alle Tools benötigen ein installiertes Java ™ Web Start (8,3 MB).

14 Schlagworte und Abkürzungen

14.1 OCSP

Das Protokoll OCSP (Online Certificate Status Protocol) dient der Online-Statusabfrage von Zertifikaten in Verzeichnisdiensten.

14.2 CRL

In einer CRL (Certificate Revocation List) werden die Zertifikate eines Verzeichnisdienstes erfasst, die durch dessen Betreiber widerrufen wurden.

14.3 OSCI

Der Begriff OSCI (Online Services Computer Interface) beschreibt eine Familie von Protokollen zur Standardisierung von Daten und deren Transport im eGovernment. So werden im Teil A Daten in einer Geschäftsprozess-bezogenen XML-Struktur beschrieben. Der Teil definiert dann Mechanismen für einen sicheren Transport dieser Daten.

14.4 LDAP

Das LDAP (Lightweight Directory Access Protocol) spezifiziert den einfachen Zugang zu Verzeichnisdiensten über TCP/IP-Netze, z. B. zum Abruf von Sperrlisten (↑ CRL).

14.5 SSL-Verschlüsselung

Das Protokoll SSL (Secure Sockets Layer) dient der sicheren Kommunikation zwischen Client und Server über das Internet und nutzt beispielsweise das RSA-Kryptoverfahren (Rivest, Shamir, Adleman).

14.6 Verwaltungsdatenschutzrecht

Für die Bundesverwaltung bzw. Landesverwaltung gelten grundsätzlich die Regelungen des Bundesdatenschutzgesetz (BDSG) bzw. die Regelungen der Landesdatenschutzgesetzes (z. B. in Niedersachsen das NDSG). Dieses sind jedoch gegenüber

bereichsspezifischen Datenschutzregelungen subsidiär. Daher gehen z. B. die Regelungen des Niedersächsischen Meldegesetzes (NMG) dem NDSG vor. Das NDSG kommt nur insoweit zur Anwendung, als in ihm Rechtsfragen geregelt sind, die nicht Gegenstand des NMG sind.

14.7 Signatur/Verschlüsselung

Elektronische Signaturen sind „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“ (§ 2 SigG). Damit werden alle möglichen Formen der technischen Realisierung beschrieben. Die digitale Signatur ist darüber hinaus ein Sicherungsmechanismus für elektronische Daten, bei dem aus der Information mittels eines geheimen Schlüssels ein Wert erzeugt wird, der mithilfe des zugehörigen öffentlichen Schlüssels verifiziert werden kann.

Die Verschlüsselung ist ein mathematisches Verfahren zum Schutz der Vertraulichkeit elektronischer Daten. Sie kann als asymmetrische Verschlüsselung (das Schlüsselpaar besteht aus einem öffentlichen Schlüssel zur Erzeugung des Chiffrats und einem privaten Schlüssel zur Entschlüsselung desselben) oder als symmetrische Verschlüsselung (Ver- und Entschlüsselung geschehen mit demselben Schlüssel) betrieben werden.

14.8 XML

Die Sprache XML (Extensible Markup Language) ist einer Erweiterung der für Web-Seiten entwickelten Sprache HTML. Daten können darin nach frei definierbaren Regeln dargestellt und für eine spätere Weiterverarbeitung aufbereitet werden.

14.9 (IT-)Sicherheitsziele

Im eGovernment sind vor allem die IT-Sicherheitsziele Vertraulichkeit (Daten dürfen nur Befugten zugänglich sein), Authentizität (Kommunikationspartner ist derjenige, der er vorgibt zu sein), Integrität (Unversehrtheit der Daten und Informationen), Nicht-Abstreitbarkeit (Verbindlichkeit und Beweisbarkeit einer Transaktion) und Verfügbarkeit (Informationen und Dienste können wie vorgesehen abgerufen und genutzt werden) von Bedeutung.

14.10 Public-Key-Infrastructure (PKI)

Eine PKI ist eine Sicherheitsinfrastruktur, die es ermöglicht, in nicht gesicherten Netzen (wie dem Internet) auf Basis eines von einer vertrauenswürdigen Stelle – einem TrustCenter - ausgegebenen Schlüsselpaares verschlüsselt Daten auszutauschen bzw. Signaturen zu erzeugen und zu verifizieren. Mit PKI-1 wird die PKI der öffentlichen Verwaltung bezeichnet.