

# IT-Grundschutz-basierendes Sicherheitskonzept für die Virtuelle Poststelle des Bundes

Dr. Christian Mrugalla, Dr. Sönke Maseberg

Bundesamt für Sicherheit in der Informationstechnik, Bonn  
datenschutz nord GmbH, Bremerhaven

christian.mrugalla@bsi.bund.de  
smaseberg@datenschutz-nord.de

**Abstract:** Ein wichtiger Baustein für das e-Government in Deutschland ist die Virtuelle Poststelle des Bundes, die im Rahmen der Initiative BundOnline 2005 entwickelt wird und die als zentrales Kommunikations-Gateway Sicherheitsdienste für die gesicherte Kommunikation zwischen Behörden und externen Kommunikationspartnern – wie Bürgern, Wirtschaft und anderen Behörden – bereitstellt. Die Anforderungen, die an einen sicheren und datenschutzkonformen Betrieb der Virtuellen Poststelle gestellt werden, sind nunmehr in einem Sicherheitskonzept formuliert worden, wobei die Methodik des IT-Grundschutzhandbuchs des Bundesamtes für Sicherheit in der Informationstechnik genutzt und adaptiert wurde.

## 1 Die Virtuelle Poststelle des Bundes

Im Rahmen der Initiative BundOnline 2005 ([www.bund.de](http://www.bund.de)) wird die Virtuelle Poststelle (VPS) als Basiskomponente „Datensicherheit“ entwickelt. Anwendungen, welche mit signierten und/oder verschlüsselten Nachrichten umgehen müssen, können dazu die erforderlichen kryptographischen Dienste – wie etwa Signaturerstellung und -prüfung sowie Ver- und Entschlüsselung – nutzen, die die Virtuelle Poststelle serverbasiert zur Verfügung stellt. Die VPS ist eine serverbasierte *Alternative* (nicht Ablösung) zu den bislang üblichen „Ende-zu-Ende-Systemen“. Hiermit verbindet sich die Hoffnung, Hemmschwellen beim Kryptographieeinsatz, die durch Schwierigkeiten in der Anwendung verursacht werden, abzubauen. Die VPS steht allen Bundesbehörden lizenzkostenfrei zur Verfügung.

Entsprechend dem Charakter einer Basiskomponente muss der Aufbau der VPS einen flexiblen Einsatz in unterschiedlichsten Anwendungen erlauben. Aus dieser Anforderung resultiert technisch ein modularer Aufbau mit *einer* offenen Schnittstelle (XML) als „zentralem Eingangstor“ zum kryptographischen Kernsystem für prinzipiell beliebige Client-Server-Anwendungen und Backend-Systeme. Die VPS konzentriert sich dabei auf ihr „Kerngeschäft“ als Kryptographie-Server, ist zustandslos und kann daher gemeinsam mit beliebigen Anwendungen – insbesondere Workflow-Systemen – kooperieren.

Als „Standard-Anwendungen“ unterstützt die VPS die Kommunikation über das Transportprotokoll OSCI (Online Services Computer Interface) [OSCI], das sich immer mehr zum „Quasi-Standard“ im E-Government entwickelt, und die serverbasierte Bearbeitung von verschlüsselten und signierten E-Mails. Die Anbindung von Verzeichnisdiensten im Rahmen von Public-Key-Infrastrukturen (insbesondere der Zertifizierungsdiensteanbieter der qualifizierten elektronischen Signatur nach Signaturgesetz) wird von einer abgesetzten Komponente übernommen, die über XKMS<sup>1</sup> angesprochen wird. Hierdurch wird die Möglichkeit eröffnet, diese oftmals technisch problematische Aufgabe einem externen Anbieter zu übertragen.

Weitere Informationen über Projekt und Produkt „Basiskomponente Datensicherheit“ finden sich aktuell unter <http://www.bsi.bund.de/fachthem/egov/vps.htm>.

## 2 IT-Grundschatzhandbuch

Sicherheitsaspekte sind bereits bei der Entwicklung der Virtuellen Poststelle berücksichtigt worden, allerdings bleiben organisatorische, personelle, infrastrukturelle und technische Maßnahmen umzusetzen. Diese Anforderungen an einen sicheren Betrieb von Virtuellen Poststellen sollten sinnvollerweise in ein umfassendes IT-Sicherheitskonzept integriert werden.

Für die Erstellung eines solchen Konzeptes bietet sich das IT-Grundschatzhandbuch [IT-GSHB] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an, das dazu im Wesentlichen vier Schritte vorsieht:

Die **IT-Strukturanalyse** hat zum Ziel, den IT-Verbund, der in einem solchen Sicherheitskonzept thematisiert wird, in seiner Gesamtheit mit allen organisatorischen, personellen, infrastrukturellen und technischen Komponenten festzulegen. Um für den konkreten IT-Verbund und seine Daten geeignete Sicherheitsmaßnahmen ergreifen zu können, muss der spezifische **Schutzbedarf** identifiziert werden. Die **Modellierung** hat zum Ziel, die für die konkrete Realisierung des IT-Verbunds relevanten Bausteine des IT-Grundschatzhandbuchs zu identifizieren, so dass im daran anschließenden **Basis-Sicherheitscheck** geprüft werden kann, ob die identifizierten Maßnahmen umgesetzt werden.

## 3 Das generische Sicherheitskonzept für die Virtuelle Poststelle

Da das Sicherheitskonzept einer Basiskomponente VPS aufgrund der verschiedenen Einsatzszenarien einer Virtuellen Poststelle auf einem deutlich abstrakteren Niveau agiert, kann die Methodik des IT-Grundschatzhandbuchs zum Teil nicht exakt angewendet werden, sondern muss entsprechend adaptiert werden.

---

<sup>1</sup> Weitere Informationen unter <http://www.oasis-open.org>.

Das nun vorliegende „Generische Sicherheitskonzept für die Kern- und Webkomponenten der Virtuellen Poststelle“ fokussiert auf die von der bremen online services GmbH & Co. KG entwickelten Web- und Kernkomponenten der Virtuellen Poststelle [bos] und thematisiert übergreifende Aspekte von Virtuellen Poststellen, deren Ausführungen bei einer konkreten Realisierung einer VPS in einem konkreten Sicherheitskonzept weiter zu präzisieren sind. Ein Vorzug dieses generischen Sicherheitskonzeptes ist, dass die grundsätzlichen Überlegungen hinsichtlich eines Sicherheitskonzeptes für Virtuelle Poststellen nach IT-Grundschutz – und insbesondere die umzusetzenden Maßnahmen – ausführlich dargelegt sind und damit die Anpassung an eine konkrete Realisierung unter Beachtung der genannten Handlungsempfehlungen unterstützt.

Im generischen Sicherheitskonzept für die Virtuelle Poststelle wurden zunächst in einer auf die Besonderheiten der VPS angepassten Strukturanalyse die für das generische Sicherheitskonzept relevanten Komponenten und Verbindungen aufgelistet. Für die Identifikation des Schutzbedarfs der VPS werden neben den Komponenten und Verbindungen die Funktionalitäten der VPS sowie die von ihr bearbeiteten Datenarten herangezogen. Hinsichtlich der Datenarten ist neben der Frage, wo sie auftreten, von Bedeutung, ob sie übertragen werden. Zu beachten ist dabei, dass über die Art der durch die Fachanwendung bestimmten Inhaltsdaten und die davon abgeleiteten Sicherheitsanforderungen im Rahmen des generischen Sicherheitskonzeptes keine endgültige Aussage getroffen werden kann.

Um für die Virtuelle Poststelle und ihre Daten geeignete Sicherheitsmaßnahmen bei IT-Systemen, Gebäuden, Räumen und Kommunikationsverbindungen ergreifen zu können, wurden relevante Schutzbedarfskategorien definiert und anschließend der Schutzbedarf für die Virtuelle Poststelle identifiziert. Als Grundwerte muss die Virtuelle Poststelle insbesondere die Verfügbarkeit, Integrität, Vertraulichkeit und Verbindlichkeit (im Sinne von Authentizität und Nachweisbarkeit) der von ihr verarbeiteten Informationen gewährleisten, wobei neben dem „Selbstschutz“ der VPS insbesondere der Schutzbedarf der Daten, die durch die VPS abgesichert werden sollen, berücksichtigt werden muss. Auf Grundlage des identifizierten Schutzbedarfs für die Funktionalitäten und Datenarten der VPS wird entsprechend der in der Strukturanalyse analysierten Abhängigkeiten der Schutzbedarf für die einzelnen Komponenten der VPS, für Bereiche und für die Verbindungen festgestellt.

Bei der Identifizierung der Sicherheitsmaßnahmen wurde die VPS zunächst in der Modellierung so konkret wie möglich durch Bausteine des IT-GSHB nachgebildet. Das IT-Grundschutzhandbuch mit seinen umfangreichen Informationen zu Gefährdungen und entsprechenden Maßnahmen unterstützt diesen Prozess wirkungsvoll. Für jede Maßnahme ist dabei zu entscheiden, ob sie anwendungsabhängig relevant ist und – wenn ja –, ob sie umgesetzt ist. Die Entscheidung, ob eine Maßnahme den Gefährdungen in einem konkreten Einsatzszenario hinreichend entgegenwirkt, erfolgt unter Berücksichtigung der jeweiligen Anwendung(en), Datenarten und infrastrukturellen Gegebenheiten. Darüber hinaus werden im generischen Sicherheitskonzept explizite Maßnahmen aufgelistet, die für die Sicherheit der VPS allgemein relevant sind und deshalb beachtet werden müssen.

Die Ausführungen im generischen Sicherheitskonzept sind im Gegensatz zu einem konkreten Sicherheitskonzept deutlich abstrakter formuliert; sie sind hinsichtlich der Anwendung auf eine konkrete Realisierung entsprechend zu präzisieren. Aus diesem Grund sind am Ende eines jeden Kapitels Hinweise und Handlungsempfehlungen aufgeführt, wie aus dem generischen Sicherheitskonzept ein konkretes Sicherheitskonzept für den Einsatz der VPS und die Integration in umfassende IT-Sicherheitskonzepte entwickelt werden kann, in denen dann die spezielle Konfiguration und Ausprägung einer Virtuellen Poststelle mit Servern, Räumen, Anwendungsszenarien und Datenarten berücksichtigt werden.

#### **4 Zusammenfassung**

Die Virtuelle Poststelle des Bundes stellt einen wichtigen Baustein im e-Government in Deutschland dar. Im nun vorliegenden, auf dem IT-Grundschutzhandbuch des BSI basierenden generischen Sicherheitskonzept sind Anforderungen beschrieben, die der Betreiber einer Virtuellen Poststelle zu ihrem sicheren Betrieb umsetzen sollte und die zur Integration in ein umfassendes IT-Sicherheitskonzept weiter zu konkretisieren sind.

Das generische Sicherheitskonzept für die Kern- und Webkomponenten der Virtuellen Poststelle ist, zusammen mit weiteren Informationen und Dokumenten zur VPS, auf der BSI-e-Government-Seite verfügbar: <http://www.bsi.bund.de/fachthem/egov/vps.htm>.<sup>2</sup>

#### **Literaturverzeichnis**

- [bos] bremen online services GmbH & Co. KG, [www.bos-bremen.de](http://www.bos-bremen.de).
- [MaMI04] Sönke Maseberg, Christian Mrugalla, Matthias Intemann, „’Datensicherheit’ in BundOnline 2005 – Die Virtuelle Poststelle des Bundes und ihr generisches Sicherheitskonzept“, DuD – Datenschutz und Datensicherheit 28 (2004) 11, Seiten 660-664.
- [IT-GSHB] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutzhandbuch“, Oktober 2003.
- [LfD-Nds] Der Landesbeauftragte für den Datenschutz Niedersachsen, „Die Virtuelle Poststelle im datenschutzgerechten Einsatz“, 2004.
- [OSCI] Online Services Computer Interface (OSCI), [www.osci.de](http://www.osci.de).
- [VPS-SiKo] bremen online services GmbH & Co. KG, „Generisches Sicherheitskonzept für die Kern- und Webkomponenten der Virtuellen Poststelle“, Version 1.0, 11. August 2004.

---

<sup>2</sup> Für weiterführende Informationen sei auch auf die Literaturangaben verwiesen.