

Sicheres E-Government

Beitrag und Funktion der Virtuellen Poststelle

Kurt Klinner, BSI

E-Government wirkt in zwei Richtungen: einerseits sollte damit die Modernisierung und Optimierung der Prozesse in der öffentlichen Verwaltung gelingen. Andererseits birgt es durch mehr Transparenz in Kommunikation und Transaktion erhebliches Potenzial, die Handlungs-, Partizipations- und Entscheidungsmöglichkeiten von Bürgern, Verwaltung und Politik deutlich zu verbessern. Die politisch-strategische Herausforderung liegt auf der Hand, Akzeptanz und Erfolg hängen entscheidend von der Qualität und Benutzerfreundlichkeit der Online-Dienstleistungen ab, dabei ist Datensicherheit ein entscheidendes Qualitätsmerkmal.

Der Einsatz moderner Kommunikationstechnologie erweist sich als geeignetes Instrument, die Effizienz und Effektivität der Verwaltungsabläufe zu erhöhen. Die elektronische Abbildung von Verwaltungsprozessen allein schafft indessen noch keine moderne Verwaltung. In einem strategischen Ansatz erfolgt die Festlegung inhaltlicher Erfordernisse und Zielsetzungen einer Verwaltungsmodernisierung, die insbesondere einhergeht mit einer Aufgabenkritik und einer Analyse der Verwaltungsprozesse sowie deren Optimierung und Reorganisation. Mit der Vorgabe des Bundeskanzlers „alle internetfähigen Dienstleistungen der Bundesverwaltung bis zum Jahre 2005 online bereitzustellen“ ist die strategische Leitaussage gesetzt. Zur Unterstützung des Wandels, dem die E-Government-Initiative den Weg bereitet, wurden mit dem Umsetzungsplan zentrale Aufgaben für eine zentrale Koordination bei der Projektgruppe BundOnline 2005 im Bundesinnenministerium zusammengefasst und durch die zentrale Bereitstellung von Basiskomponenten und Kompetenzzentren ergänzt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist mit der Konzeption und Realisierung der Basiskomponente „Datensicherheit“ sowie mit dem Aufbau und dem Betrieb des Kompetenzzentrums „Datensicherheit“ im Rahmen der E-Government-Initiative betraut worden.

Nach der Definition im E-Government-Handbuch bezeichnet „Electronic Government (E-Government) ... die Nutzung elektronischer Informations- und Kommunikationstechnik zur Einbeziehung des Kunden in das Handeln von Regierung und öffentlicher Verwaltung“¹. Damit sind alle Behörden aufgefordert, ihre IT-Infrastrukturen auf sicherer Basis zu öffnen und ein sicheres Dienstleistungsangebot über das Internet bereitzustellen. Akzeptanz und Erfolg von E-Government-Dienstleistungen hängen essentiell von der Qualität und Benutzerfreundlichkeit der Kommunikation ab, insbesondere ist Sicherheit hierbei als zentrales Qualitätsmerkmal zu erkennen. Die Vorteile des elektronischen Verwaltungshandelns liegen auf der Hand: Für Bürgerinnen und Bürger steht die Dienstleistung rund um die Uhr an sieben Tagen in der Woche zur Verfügung. Der Behördengang und Wartezeiten vor den Amtsstuben können damit entfallen. Bei Wirtschaft und Verwaltung können zusätzliche Rationalisierungseffekte genutzt werden. Da vertrauliche und verbindliche Daten über das Internet übertragen werden, erwarten Bürger und Unternehmen als Kommunikationspartner der Verwaltung zu recht, dass mit dem Angebot von Dienstleistungen über das Internet keine Einschränkungen der Vertraulichkeit und Integrität ihrer Daten oder der

¹ E-Government-Handbuch des BSI, Köln 2002, E-Government-Glossar; <http://www.e-government-handbuch.de>

Verbindlichkeit des Verwaltungshandelns verbunden sind. Dies bedingt, dass die Anforderungen an organisatorische, technische und personelle Ressourcen durch die Migration zu onlinefähigen Dienstleistungen, nicht nur quantitativ, sondern auch qualitativ steigen.

Als Basis eines sicheren E-Government werden neben den üblichen Standardsicherheitsmaßnahmen² heute als gängige Technologien Verschlüsselung und digitale Signatur eingesetzt, um damit Vertraulichkeit, Integrität und Authentizität zu schützen. Durch das Formanpassungsgesetz und das dritte Gesetz zur Änderung verfahrensrechtlicher Vorschriften ist sowohl im Privatrecht als auch im Verwaltungsrecht die qualifizierte elektronische Signatur der eigenhändigen Unterschrift gleichgestellt. Mit dem Regierungsbeschluss vom 16.01.2002 zur „Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung“ ist die Bundesverwaltung gefordert, elektronische Signaturen und Verschlüsselung von den Kommunikationspartnern zu akzeptieren bzw. selbst einzusetzen. Mit diesem Beschluss werden drei Ziele verfolgt:

- Einführung von E-Mail-Sicherheit. Unter der Annahme dass keine Formvoraussetzungen zu beachten sind, sollen fortgeschrittene Signaturen zum Einsatz kommen, der Vertraulichkeitsaspekt wird im Vordergrund gesehen;
- bei E-Government-Dienstleistungen kommen qualifizierte elektronische Signaturen zum Einsatz, wo es erforderlich oder geboten ist (insbesondere bei Schriftformerfordernis);
- Gewährleistung des IT-Grundschutz als Mindestschutz und Nutzung einheitlicher Standards.

Der Bürger bleibt daher grundsätzlich (solange nicht gesetzliche Vorschriften z.B. eine qualifizierte Signatur verlangen oder die elektronische Kommunikation in Spezialfällen ausschließen) frei in der Wahl der von ihm eingesetzten Kommunikations- und Sicherheitstechnik; die Verwaltung ist grundsätzlich gefordert, die gesamte Bandbreite an Kommunikations- und Kryptotechnik zu bedienen. Für den wirtschaftlichen Einsatz bei den Behörden des Bundes soll die Ausstattung der Arbeitsplätze mit interoperablen technischen Lösungen erfolgen, die alle Arten der elektronischen Kommunikation zwischen Bundesverwaltung und deren Kommunikationspartner ermöglichen. Die Verwaltung hat daher ihre Kommunikationsendpunkte mit einer universellen Kryptotechnik zur Ver- und Entschlüsselung, zur Signaturprüfung und – Erstellung sowie zur Zertifikatsverwaltung auszustatten. Mit der Aufrechterhaltung einer Ende-zu-Ende-Sicherheit, bei der an allen Mitarbeiter-Arbeitsplätzen die dazu notwendige Kryptotechnik zum Einsatz kommt, sind in der Praxis bisweilen erhebliche Probleme zu beobachten:

- mangelndes Wissen um Einsatz und Anwendung komplexer Kryptotechnik,
- mangelnde Interoperabilität der eingesetzten Verfahren,
- ablauforganisatorische Hemmnisse in Vertretungsfällen und
- damit einhergehend die fehlende Akzeptanz der Kryptotechnik.

Den genannten Problemen kann oft wirksam durch die Einrichtung zentraler Stellen (Ende-zu-Organisations-Sicherheit), an denen kryptographisch behandelte Kommunikationsströme entschlüsselt, Signaturen verifiziert und die Informationen entsprechend weiterleitet bzw. auf dem Rückweg entsprechend verschlüsselt und signiert werden, begegnet werden. Mit der Basiskomponente „Datensicherheit“ wird ein „uni-

² Standardsicherheitsmaßnahmen sind beschrieben im IT-Grundschutzhandbuch des BSI

verselles“ System für den zentralen Einsatz der Kryptographie zur Verfügung stehen; sie soll die sichere elektronische Kommunikation zwischen Behörden und externen Kontakten, wie Bürger oder Unternehmen, auf Behördenseite praktisch erleichtern und dadurch unterstützen.

Für Behörden stellt sich das Problem, die gesamte Bandbreite an Kommunikations- und Kryptotechnik zu bedienen. Dabei sind E-Mail und Web-Applikation für die Kommunikation im Rahmen von E-Government als Basistechnologien anzusehen. Aus Behördensicht kann grundsätzlich von einer Präferenz für Web-Anwendungen ausgegangen werden, da damit strukturierte Daten medienbruchfrei an Hintergrundsysteme übergeben werden können. Es wird jedoch auch Prozesse geben, in denen auf eine E-Mail-Kommunikation nicht verzichtet werden kann, zumal dem Bürger die Freiheit in der Wahl der Kommunikationskanäle offen steht.

Die nachstehenden Anwendungsszenarien sind damit für die Virtuelle Poststelle relevant:

- Kommunikation im Input- bzw. Output zwischen internen und externen E-Mail-Benutzern,
- Kommunikation im Input bzw. Output über den WEB-Browser, z.B. durch Einstellen oder Abholen von Dokumenten
- Kommunikation im Input bzw. Output über eine Web-Anwendung, z.B. durch Ausfüllen eines Antrages in einer Online-Sitzung.

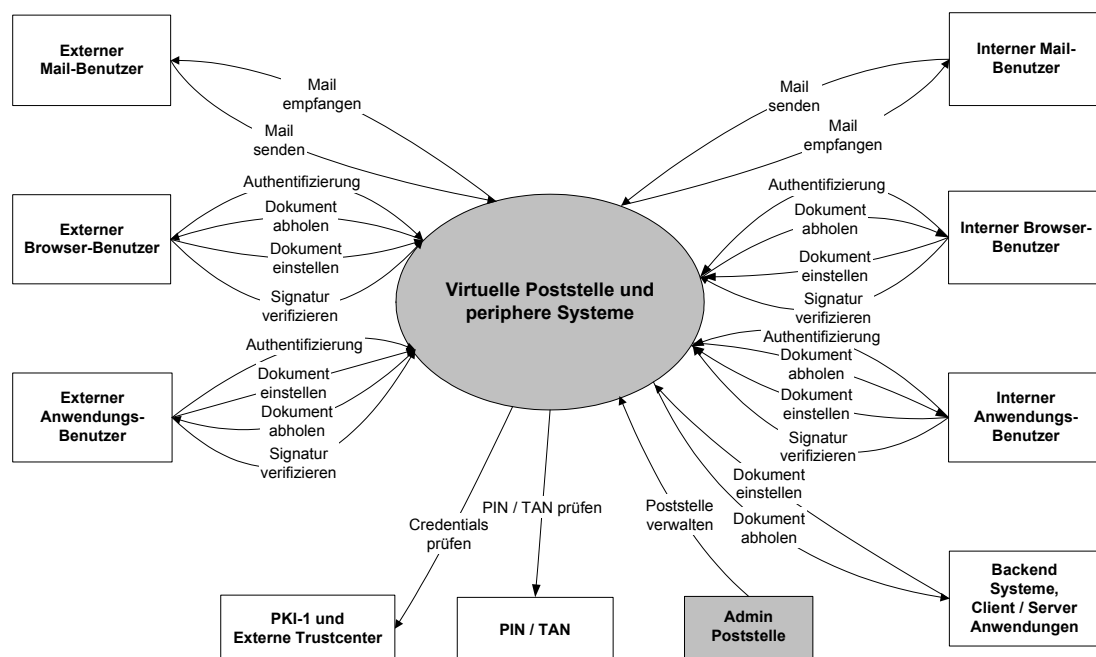


Abbildung 1: Anwendungsszenarien der Virtuellen Poststelle

Die Virtuelle Poststelle wird dazu

- eingehende Datenströme entschlüsseln, wenn sie dazu die Berechtigung besitzt,
- ausgehende Datenströme bei Bedarf verschlüsseln,
- Signaturen und Zertifikate prüfen,
- Zeitstempel bereitstellen oder prüfen,

- Prüfungsergebnisse auf einem Laufzettel dokumentieren,
- Quittungsmechanismen bedienen,
- Daten an Hintergrundsysteme weiterleiten und
- Fehlerbehandlungsmechanismen bereitstellen.

Als zentrale Einrichtung muss die Virtuelle Poststelle in der Lage sein, organisatorische Bedingungen, wie z. B. Vertretungsregelungen zu berücksichtigen. Einer solchen Lösung sind allerdings auch prinzipielle Grenzen gesetzt. So ist z.B. durch die Entschlüsselung auf dem zentralen Gateway die Vertraulichkeit innerhalb des Intranets der Behörde nicht mehr vollständig gegeben. Bei Bedarf kann sie durch Umschlüsselung aufrecht erhalten werden. Insbesondere bei hoch vertraulichen oder sensiblen personenbezogenen Informationen ist vor dem Hintergrund der Sicherheitsanforderungen und der verbleibenden Restrisiken zu entscheiden, ob der Einsatz einer Virtuellen Poststelle möglich, die Ende zu Ende-Kommunikation als Alternative gewählt werden sollte, oder ob andere Mechanismen der Absicherung einzusetzen sind.

Bei Einsatz der Virtuellen Poststelle ist daneben auch weiterhin eine Ende-zu-Ende-Kommunikation möglich.

Im vorliegenden Konzept³ - „Fachkonzept für die Virtuelle Poststelle als Basiskomponente Datensicherheit“⁴ - wird die Virtuelle Poststelle in nachstehende Grobkomponenten gegliedert:

- Mail-Anwendung
- Kommunikations-Gateways
- Security Server
- Security Modul
- Administration

Die Kommunikations-Gateways, der Security Server und das Security Modul bilden das Kernsystem der VPS (VPS-Kernsystem).

Die Mail-Anwendung dient der Anbindung von E-Mail-Systemen. Sie behandelt eingehende, kryptographisch vom Absender abgesicherte E-Mails durch Generierung einer Quittung und Übergabe der Quittung an das Mailsystem, mit den Informationen Eingangszeitpunkt und Erfolg der Entschlüsselung / Signaturprüfung, Übergabe der Zertifikate an die Verwaltung der externen Benutzer und gegebenenfalls Versenden von Fehlermeldungen.

Bei ausgehenden E-Mails werden hier die vom E-Mail Client mitgegebenen Steuerinformationen in die Scriptsprache des VPS Regelinterpreters übersetzt und gegebenenfalls Fehlermeldungen per E-Mail an den Absender versandt, wenn z.B. ein Empfängerzertifikat nicht gefunden werden konnte.

Die Kommunikations-Gateways werden realisiert als Mail-, Dokument und Web-Gateway und dienen der Anbindung der Mail-Anwendung, von Backend- oder Anwendungsservern bzw. Web-Anwendungen. Es handelt sich um Übergabepunkte für kryptographisch behandelte E-Mails, Dokumente oder Daten und deren entschlüssel-

³ <http://www.bsi.bund.de/fachthem/egov/vps.htm#Publikationen>

⁴ entwickelt durch Firma IBM Deutschland GmbH, IBM Global Services in Zusammenarbeit mit dem BSI

ter bzw. geprüfter Rückgabe mit der Dokumentation der Ergebnisse von Zertifikats- und Zeitstempelprüfungen. Im Security Server werden alle sicherheitsrelevanten und kryptographischen Funktionen gesteuert oder ausgeführt. Im Security-Modul werden die notwendigen elementaren kryptographischen Funktionen und Algorithmen in einer gesicherten, manipulationsgeschützten Umgebung ausgeführt und dem Security Server zur Verfügung gestellt. In der Administration werden Anwendungsmangement und Sicherheitsmangement sowie Schlüsselmanagement unterschieden. Für Funktionen wie Viren- oder Content-Scanning stehen Schnittstellen zu Standardprodukten zur Verfügung.



Abbildung 2: Funktionsskizze VPS

Mit Abschluss der konzeptionellen Arbeiten ging eine Marktsichtung einher, da eine lauffähige erste Version bis Ende des Jahres 2003 zur Verfügung stehen sollte. Neben den Anforderungen zur Unterstützung E-Mail-basierter Kommunikation sowie Web-basierter Anwendungen sollte die Lösung natürlich auch SAGA-konform⁵ sein und z.B. den OSCI-Standard⁶ unterstützen. Bereits vor der Marktsichtung war klar dass es bislang kein Produkt gab, welches für die kryptographische Unterstützung

⁵ SAGA, „Standards und Architekturen für eGovernmentanwendungen“, Schriftenreihe der KBSt Februar 2003

⁶ OSCI: "Online Services Computer Interface", <http://www.osci.de>

sowohl der E-Mail-Kommunikation als auch der Web-Kommunikation eingesetzt werden konnte. Es erwies sich weiterhin als zweckmäßig, zwischen Web- und Kernkomponenten einerseits und dem SMTP-Gateway zur Verarbeitung von E-Mails andererseits zu unterscheiden. In der Bewertung der existierenden Lösungen zeigte die Bremer Lösung Governikus⁷ im Bereich der Web-basierten Kommunikation die größte Deckung zu den skizzierten Anforderungen. Auch die bestehenden Rechte des Bundes an diesem Produkt flossen in die Entscheidung, die Web- und Kernkomponente der Virtuellen Poststelle durch Fortentwicklung von Governikus zu realisieren, ein.

Für die Bereitstellung der Mail-Komponente wurde in einem ergänzenden Vergabeverfahren das Produkt JULIA Mail-Office⁸ mit hoher Konformität zu den definierten Anforderungen und eine für die geplante Integration geeigneten flexiblen Architektur ausgewählt. Die Entwicklung des VPS-Kernsystems auf der Basis des vorliegenden Konzeptes sowie die Integration der beiden Lösungen wird derzeit in einem gemeinsamen Projekt vorangetrieben. Ziel ist die Migration zu der im Konzept dargestellten Architektur, die voraussichtlich im Herbst 2004 erreicht sein wird. Danach umfasst die Gesamtlösung folgende Komponenten:

- das SMTP-Gateway als Mail-Anwendung
- das VPS-Kernsystem
- ein VPS-Authetisierungsmodul mit Client- und Serverkomponente
- ein VPS-Verifikationsmodul mit Client- und Serverkomponente
- das OCSP/CRL-Relay
- den OSCI-Manager bestehend aus Client-Enabler, OSCI-Postfach und Backend-Enabler und den
- den Secure Messenger.

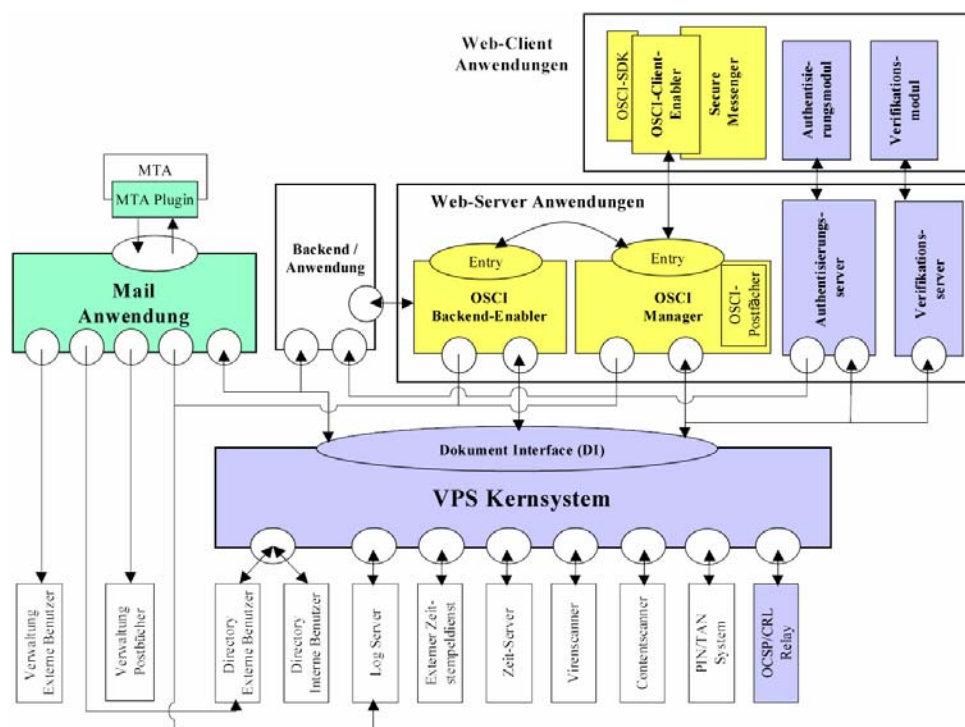


Abbildung 3: Komponenten Virtuelle Poststelle

⁷ Firma. bremen online services GmbH & Co. KG (bos), Bremen

⁸ Firma InfoTesyS Comuter Consulting GmbH (ICC), Köln

OSCI-Manager und Secure Messenger unterstützen die Implementierung von OSCI 1.2 basierten Anwendungen. Sollen Anwendungen, die nicht OSCI-basiert arbeiten eingebunden werden, kann das Dokumenten-Gateway genutzt und VPS-Authentisierungsmodul bzw. VPS-Verifikationsmodul in die Client- oder Serveranwendung integriert werden. Der OSCI-Client-Enabler ist eine auf den Client-Rechner applizierte Anwendung, die Aufgabe hat, die Eingabedaten z.B. aus einer Bildschirmmaske in das OSCI-Datenformat „einzupacken“ und die erforderlichen Verschlüsselungen vorzunehmen und gegebenenfalls Signaturen anzubringen. Für die Signaturerzeugung spricht er den Kartenleser des Kunden an. Zum Lieferumfang der VPS des Bundes gehört auch als PlugIn für den Client-Enabler der Secure Messenger, der eine Übertragung von Textnachrichten mit den OSCI-Mechanismen realisiert und als Web-Mail-Anwendung angesehen werden kann.

Der OSCI-Manager realisiert gemeinsam mit dem Kernsystem und dem OSCP/CRL-Relay die Rolle des Intermediärs aus dem OSCI-Protokoll. Zu den Kernaufgaben gehört die „Öffnung des äußeren Briefumschlags“ und die Überprüfung von Transportsignaturen. Der OSCI-Manager kann OSCI-Postfächer anlegen und verwalten, in denen Nachrichten auch in verschlüsselter Form bei asymmetrischen Kommunikationsszenarien zwischengespeichert werden. Die Nutzdaten der Kommunikation werden entsprechend des Rollenprofils des OSCI-Intermediärs innerhalb des OSCI-Managers nicht entschlüsselt.

Der OSCI-Backend-Enabler öffnet in Kooperation mit dem VPS-Kernsystem den „inneren Briefumschlag“ der OSCI-Datensätze und bereitet die jetzt im Klartext vorliegenden Nutzdaten zur weiteren Verarbeitung durch das Hintergrundsystem auf. Die Integration des VPS-Kernsystems sowie die Einbindung des OSCI-Backend-Enablers in die Hintergrund-Anwendung erfolgt durch einen anwendungsspezifischen Adapter über den die Verarbeitungssysteme angeschlossen werden können.

Die Realisierung einer E-Governmentanwendung stellt sich für die Behörde als Anwendungsentwicklungsprojekt dar, welches die Gestaltung von Front- und Back-Ends und die Einbindung oder Entwicklung von Hintergrundsystemen umfasst. Die virtuelle Poststelle ist die Basiskomponente zur sicheren Abwicklung der Kommunikation und ist damit Sicherheitsdienstleister für E-Government-Anwendungen. Sie stellt Komponenten für Client- und Serveranwendungen sowie Schnittstellen zu Hintergrund- und Archivierungssystemen zur Verfügung. Sie sollte nicht als universelle E-Government-Maschine missverstanden werden, die jede E-Government-Dienstleistung bereit zu stellen in der Lage wäre.

Weiterführende Informationen zur Virtuellen Poststelle finden Sie über das Portal des Bundes unter <http://www.bund.de/BundOnline-2005/Basiskomponenten-und-Kompetenzzentren-.7194.htm> und auf den Seiten des BSI unter <http://www.bsi.bund.de/fachthem/egov/vps.htm>.