Bundesministerium
des Innern

VOMEA® – *Konzept*

Erweiterungsmodul zum Organisationskonzept 2.1

Virtuelle Poststelle und Vorgangsbearbeitungssysteme

www.kbst.bund.de

Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung

KBSt

Schriftenreihe der KBSt

ISSN 0179-7263

Band 62

November 2005

Schriftenreihe der KBSt
Band 62
ISSN 0179 - 7263

Interessenten erhalten die derzeit lieferbaren Veröffentlichungen der KBSt
und weiterführende Informationen zu den Dokumenten beim

Bundesministerium des Innern
Referat IT 2 (KBSt)
11014 Berlin

Tel.: +49 (0) 1888 681 - 2312
Fax.: +49 (0) 1888 681 - 52312

Homepage der KBSt: www.kbst.bund.de
Mail to: Monika.Pfeiffer@bmi.bund.de

Inhaltsverzeichnis

ABBILDUNGSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

Abkürzung	**Erläuterung**
AGB	Allgemeine Geschäftsbedingungen
B2G	Business-to-Government-Beziehung
BGB	Bürgerliches Gesetzbuch
BSI	Bundesamt für Sicherheit in der Informationstechnik
C2G	Citizen-to-Government-Beziehung
FMS	Formularmanagementsystem
FormVAnpG	Formvorschriftenanpassungsgesetz
G2G	Government-to-Government-Beziehung
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IVBB	Informationsverbund Berlin - Bonn
JDBC	Java Database Connectivity
JKomG	Justizkommunikationsgesetz
KoopA ADV	Kooperationsausschuss Automatisierte Datenverarbeitung
OE	Organisationseinheit
OSCI	Online Services Computer Interface

PAO	Postausgangsobjekt
PDF	Portable Document Format
PEO	Posteingangsobjekt
PKI	Public-Key-Infrastucture
S/MIME	Secure Multipurpose Internet Mail Extensions
SAGA	Standards und Architekturen für E-Government-Anwendungen
SigG	Signaturgesetz
SigV	Signaturverordnung
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TIFF	Tagged Image File Format
VBS	Vorgangsbearbeitungssystem
VPS	Virtuelle Poststelle
VwVfG	Verwaltungsverfahrensgesetz
VS-Einstufung	Verschlusssachen-Einstufung
XML	eXtensible Markup Language
XÖV	XML-Beschreibungen für fachspezifische Grunddatensätze der öffentlichen Verwaltung
ZPO	Zivilprozessordnung
ZustRG	Zustellungsreformgesetz

1 MANAGEMENT SUMMARY

Das Erweiterungsmodul „Virtuelle Poststelle“ betrachtet die Einbindung einer Virtuellen Poststelle (kurz: VPS) in die IT-gestützte Vorgangsbearbeitung. Eine VPS ergänzt bisherige Komponenten der IT-Infrastruktur in einer Behörde, die zum Ziel hat, online zu kommunizieren. Als elektronischer Lösungsansatz bietet die VPS sicherheitsrelevante Dienste, um etwa bei Bedarf für die Kommunikation zwischen Behörde und externem Kunden sowohl eingehende als auch ausgehende Daten verschlüsselt und/oder signiert zu übermitteln.

Geschäftsvorfälle (wie etwa ein Verwaltungsakt oder ein Vertrag), die schützenswürdige Daten enthalten, der Schriftform unterliegen oder Fristen beinhalten, stellen Herausforderungen für einen rechtsverbindlichen elektronischen Geschäftsprozess dar. In diesen Fällen werden im papierbasierten Geschäftsgang ausgehende Dokumente handschriftlich unterschrieben bzw. eingehende Dokumente gescannt. Die elektronische Erfassung solcher handschriftlich unterschriebenen Dokumente erfolgt bei Posteingang herkömmlich über das Einscannen des Papierdokuments. Die notwendige Nachweisführung im Postausgang erfolgt z. B. neben Registraturhilfsmitteln in Absendevermerken, Fax-Sendeberichten oder Einschreiberückscheinen. Zur Posteingangsbehandlung gehört es, das aktenrelevante Schriftgut mit Grunddaten in Registraturhilfsmitteln zu erfassen. Ggf. ist eine Empfangsbestätigung für den Nachweis der Fristwahrung zu quittieren. Für den Versand und Empfang per E-Mail ist die Erfassung uneinheitlich sowie vom einzelnen Mitarbeiter abhängig.

Verfolgt eine Behörde das Ziel, diese Abläufe vollständig online abzuwickeln, um die Bearbeitung effektiver zu gestalten, sind äquivalente Lösungen zum rechtsverbindlichen papierbasierten Geschäftsprozess notwendig.

Hierzu gehört u. a. der Einsatz der qualifizierten elektronischen Signatur als Ersatz der handschriftlichen Unterschrift wie auch weitere Funktionen der Postein- und -ausgangsbehandlung. Ein Vorgangsbearbeitungssystem (kurz: VBS) muss hierfür zusätzliche Funktionalitäten und Dienste einbinden, die es selbst nicht anbietet.

Der elektronische Geschäftsprozess, der mittels VBS und VPS abgewickelt wird, unterliegt verfahrensbedingten Vorgaben, wie sie das DOMEA®-Organisationskonzept[1] beschreibt. Als Vorgabe für ein VBS einschließlich Speicher- und Archivsystem gilt, dass die Möglichkeiten zur Sicherung von Integrität, Vertraulichkeit, Verfügbarkeit, Authentizität,

[1] S. http://www.kbst.bund.de/Anlage304127/pdf_datei.pdf

Zeitlicher Bestimmtheit und Nachweisbarkeit der Bearbeitung und der Daten (Schutzziele) gegeben sein müssen.

Aus Sicht der IT-gestützten Vorgangsbearbeitung bestehen Interaktionen zwischen VBS und VPS in verschieden Teilprozessen und zu unterschiedlichen Zeitpunkten. Die Teilprozesse Posteingang, Bearbeitung, Postausgang unterscheiden sich bezüglich der Aufgaben im Umgang mit Dokumenten und bedingen die Nutzung einzelner Dienste der Virtuellen Poststelle. Gemäß den oben genannten Schutzzielen müssen entsprechende kryptographische Dienste sowie Posteingangs- und Postausgangsdienste auf Abruf bereitgehalten werden, die dem Schutzbedarf und der Nachweispflicht des papierbasierten Geschäftsprozesses entsprechen. Sie sind Bestandteil der Abwicklung eines Geschäftsprozesses.

Die äquivalenten (aktenrelevanten) Tätigkeiten zum papierbasierten Geschäftsprozess müssen über die Dauer ihres Lebenszyklus ggf. an den elektronischen Dokumenten, am Vorgang oder an der Akte erkennbar sein.

Aus Geschäftsprozesssicht kann ein externer Partner, unabhängig von den Kommunikationskanälen E-Mail oder Web, mittels VPS mit einem konkreten Mitarbeiter oder einer Organisationseinheit der Behörde sicher kommunizieren. Der Geschäftsprozess lässt sich für die Behörde effizient gestalten, wenn die sicherheitsrelevanten Dienste an zentraler Stelle für alle Benutzer einer Behörde angeboten werden.

- Die Regelungen der Vorgangsbearbeitung, der Inhalt der Daten und Anforderungen aus den Prozessen liefern Vorgaben, welcher Schutzbedarf für aus- und eingehende Daten gilt. Im Rahmen einer Skalierung des Schutzbedarfes wird definiert, welches Schutzniveau für ein- und ausgehende Daten oder Kommunikationskanäle durch die VPS zu gewährleisten ist.

Die Funktionen einer VPS werden je nach Kommunikationskanal an verschiedenen Stellen einzubinden sein. Dem Benutzer bieten sich grundsätzlich drei Zugriffsmöglichkeiten, um auf die sicherheitsrelevanten Funktionen zuzugreifen:

- Web Interface (OSCI),
- E-Mail Interface und
- direkt aus dem VBS (Hintergrundsystem Interface).

Das Web Interface für Datenübermittlung via OSCI eröffnet einen sicheren Nachrichtentransport in den Teilprozessen Versand und Empfang über das Internet. Eine vertrauenswürdige Übermittlungsinstanz (Intermediär) prüft und leitet Nachrichten weiter. Der Intermediär kann bei vertraulichen, verschlüsselten Daten lediglich die Transportinformationen lesen bzw. interpretieren. Damit ist sichergestellt, dass die Inhaltsdaten

ausschließlich vom Autor und vom Empfänger verarbeitet werden können.

Eine VPS ist darüber hinaus in behördeneigene Mailanwendungen (z. B. Exchange-Server) integrierbar und unterstützt den Transport der E-Mails in den Teilprozessen Versand und Empfang. Sie wird nach vordefinierten Regeln aktiv und filtert eingehende kryptographisch behandelte E-Mails zur weiteren Bearbeitung aus.

Die kryptographischen Basisdienste einer VPS können zusätzlich direkt aus dem VBS über ein entsprechendes Interface angesprochen werden. Exemplarisch sind folgende Teilprozesse, die im Rahmen der Bearbeitung aufgerufen werden können: Ad hoc- und Wiederholungsprüfung zur Verifikation von Signaturen und Zertifikaten, kryptographische Bearbeitung von Prozess- und Inhaltsdaten, Verfahren zum Mit- und Schlusszeichnen.

Je nach Teilprozess (etwa Versand, Empfang etc.) und Kommunikationskanal (etwa E-Mail, Web) gestaltet sich die Interaktion von VBS und VPS in eigener Charakteristik.

2 EINLEITUNG

Dieses Kapitel stellt den Aufbau des Dokuments, die gewählte Vorgehensweise sowie die notwendigen thematischen wie auch inhaltlichen Abgrenzungen dar.

2.1 Aufbau und Zweck des Dokuments

Das Erweiterungsmodul „Virtuelle Poststelle“ wendet sich an Projektverantwortliche und -mitarbeiter sowie IT-Leiter in Bundesbehörden, die die IT-gestützte Vorgangsbearbeitung medienbruchfrei ausweiten und um zentrale kryptographische Dienste einer VPS ergänzen wollen.

Dieses Dokument ergänzt das Organisationskonzept des aktuellen DOMEA®-Konzept Version 2.1. Ziel des Dokuments ist es, anhand von typischen Geschäftsabläufen mit Kommunikationspartnern einer Behörde die Einbindung einer Virtuellen Poststelle in die IT-gestützte Vorgangsbearbeitung darzustellen. Das Erweiterungsmodul „Virtuelle Poststelle“ liefert hierfür organisatorisch-technische Herleitungen und Hintergründe, die zum besseren Verständnis der abgeleiteten Anforderungen im DOMEA®-Anforderungskatalog verhelfen. Die Darstellungsweise erfolgt allgemein und behördenunabhängig in einer übertragbaren Form.

Das vorliegende Dokument gliedert sich in vier Kapitel. Im Anschluss an die Managementzusammenfassung und die Einleitung folgen die inhaltlichen Ausführungen.

Das Kapitel 3 beschreibt zunächst die Herausforderung für einen rechtsverbindlichen elektronischen Geschäftsverkehr, der schützenswerte Daten enthält, einer Schriftform unterliegt oder Fristen beinhaltet. Das Ziel, solche Geschäftsvorfälle online und effektiver zu gestalten, verlangt äquivalente Lösungen zum papierbasierten Geschäftsprozess. Aus Sicht eines VBS wird der Bedarf an sicherheitsrelevanten Funktionen und Diensten aufgezeigt, die es selbst nicht anbieten kann. Das Kapitel beschreibt aus dieser Perspektive die verfahrensbedingten Vorgaben für das Zusammenwirken beider Anwendungen. Aus prozessualer Sicht ergeben sich bei der Abwicklung eines Geschäftsvorfalles unterschiedliche Interaktionen zwischen VBS und Virtueller Poststelle. Abschließend geben verfahrensbedingte Anforderungen den Schutzbedarf vor, der für die Kommunikation und für die ein- und ausgehenden Daten von einer VPS zu gewähren ist.

Kapitel 4 beschreibt Funktionen und Komponenten einer Virtuellen Poststelle. Als elektronischer Lösungsansatz liefert die Virtuelle Poststelle kryptographische Grundfunktionen, die vom VBS nicht geleistet werden können. Aus Sicht des VBS bietet die Basiskomponente VPS dabei verschiedene Zugänge zu sicherheitsrelevanten Funktionen.

In Kapitel 5 erfolgt eine prozessorientierte Betrachtung. Dabei werden die Zusammenhänge zwischen den Abläufen auf VPS-Seite und den organisatorisch-technischen Folgetätigkeiten in der Vorgangsbearbeitung dargestellt.

2.2 Vorgehen

Das vorliegende Dokument betrachtet die Einbindung einer „Virtuellen Poststelle“ aus Sicht der Vorgangsbearbeitung. Der zugrunde liegende prozessuale Ansatz geht davon aus, dass die verfahrensbedingten Vorgaben der IT-gestützten Vorgangsbearbeitung die Interaktionen mit einer VPS prägen. Allerdings ergeben sich auch aus den technischen Abläufen und den Komponenten einer VPS organisatorische Konsequenzen für die IT-gestützte Vorgangsbearbeitung.

Der prozessuale Ansatz beschreibt Fälle von verbindlichem elektronischem Geschäftsverkehr als medienbruchfreien Geschäftsprozess. In diesen Fällen unterliegen die ein- und ausgehenden Daten spezifischen Sicherheits- und Schutzbedürfnissen. Um derartige Fälle durchgängig elektronisch abzuwickeln, muss die IT-gestützte Vorgangsbearbeitung um kryptographische Funktionalitäten ergänzt werden. Konsequenter Weise werden zunächst die verfahrensbedingten Vorgaben für die Interaktion zwischen VBS und VPS beschrieben. Anschließend werden die Anforderungen einer VPS als einem äquivalenten elektronischen Lösungsansatz zum rechtsverbindlichen papierbasierten Geschäftsgang bestimmt. Auf dieser Basis lässt sich die Nutzung notwendiger Grundfunktionen einer VPS in verschiedenen Teilprozessen eines Geschäftsgangs beschreiben und die organisatorisch-technischen Folgerungen für das VBS aufzeigen.

2.3 Abgrenzung des Dokuments

Das Erweiterungsmodul „Virtuelle Poststelle“ stellt die Möglichkeit heraus, eine Virtuelle Poststelle als elektronischen Lösungsansatz in die Abläufe der IT-gestützten Vorgangsbearbeitung einzubinden. Mit dem Fokus des Dokuments sind verschiedene Themen abzugrenzen und ggf. auf inhaltlich vertiefende Dokumente zu verweisen.

Dieses Dokument betrachtet Interaktionen zwischen Vorgangsbearbeitungssystem und Virtuelle Poststelle. Auslöser der Interaktionen sind schutzbedürftige E-Mail- oder Web-Kommunikationen mit externen Kommunikationspartnern. Die Kommunikation kann sich dabei im Sinne einer B2G oder C2G Beziehung gestalten. Fälle einer schutzbedürftigen G2G Beziehung werden ebenfalls einbezogen.

Aus prozessualer Sicht bleiben Einzelschritte auf der Seite eines externen Kommunikationspartners unberücksichtigt. Dies betrifft den Einsatz kryptographischer Funktionen sowie organisatorisch technische Heraus-

forderungen wie etwa hinsichtlich der Signierkomponenten, Zertifikatsausstellung, Vergabe von kryptographischen Schlüsseln, Signaturkarten und Nutzung von Attributzertifikaten. Die Sicherheitsbestimmungen der jeweiligen Signaturkartenherausgeber (Trustcenter) informieren hierzu ausführlicher.

Das Dokument betrachtet auf Behördenseite ausschließlich die Anwendungen VPS und VBS, bei E-Mail-Kommunikation wird ebenfalls die Mailanwendung geringfügig in die Betrachtung einbezogen. Unberücksichtigt bleibt die Verwendung einer VPS ohne den Einsatz eines Vorgangsbearbeitungssystems. Je nach Geschäftsprozess und IT-Infrastruktur können weitere Anwendungen das Zusammenwirken von VPS und VBS ergänzen. Die Einbindung von Basiskomponenten oder -anwendungen wie etwa eines Zahlungs- oder eines Formularmanagementsystems wird nicht thematisiert. Zu diesen Themen sollen zu einem späteren Zeitpunkt entsprechende Erweiterungsmodule von der KBSt veröffentlicht werden.

Das vorliegende Erweiterungsmodul verweist zudem an entsprechenden Textstellen auf weitere Erweiterungsmodule, die bestimmte Themen vertiefen. Dies betrifft beispielsweise Inhalte wie Revisionsfestigkeit eines VBS, Langzeitarchivierung und Übersignieren oder innerbehördlichen Austausch von standardisierten Grunddatensätzen.

Die organisatorisch-technische Integration einer VPS in ein VBS wird abstrakt aus Sicht der IT-gestützten Vorgangsbearbeitung vorgenommen. Fragen zur technischen Ausgestaltung und Realisierung einer VPS werden nicht beantwortet. Derartige Informationen liefern etwa OSCI-spezifische Dokumente und spezielle Unterlagen zur Basiskomponente Datensicherheit[2] (VPS als Basiskomponente von BundOnline). Das vorliegende Dokument nimmt lediglich soweit Bezug auf diese Aspekte, wie es zum Verständnis der Integration von Vorgangsbearbeitung und Sicherheitsdiensten erforderlich ist.

[2] Siehe etwa BSI, Fachkonzept für die Virtuelle Poststelle als Basiskomponente Datensicherheit von BundOnline, 2003.

3 PROBLEMKONSTELLATION – NUTZEN EINER VIRTUELLEN POSTSTELLE

3.1 Medienbruchfreier verbindlicher elektronischer Geschäftsverkehr

Geschäftsvorfälle, die schützenswürdige Daten enthalten, der Schriftform (inklusive handschriftlicher Unterschrift) unterliegen oder Fristen beinhalten, stellen Herausforderungen für einen medienbruchfreien[3] Geschäftsprozess dar. Müssen beispielsweise bestimmte Dokumente handschriftlich unterschrieben werden, so sind die Kommunikationsteilnehmer gezwungen, das Übertragungsmedium zu wechseln: Elektronische Dokumente werden ausgedruckt und unterschrieben bzw. handschriftlich gezeichnete Dokumente werden gescannt. Verfolgt eine Behörde das Ziel, Prozesse vollständig online abzuwickeln, um die Bearbeitung effektiver zu gestalten, dann sind äquivalente Lösungen zum rechtsverbindlichen papierbasierten Ablauf notwendig.

Das Verwaltungshandeln mit Rechtsfolge definiert geregelte und verbindliche Handlungsweisen und deren unmittelbare Außenwirkung für den jeweiligen konkreten Einzelfall. Dabei kann rechtsverbindliches Verwaltungshandeln zwischen Behörden und externen Kommunikationspartnern dem Schriftformerfordernis unterliegen.[4]

Beispiele hierfür sind:

- Vertrag bzw. Kommunikation mit Vertragscharakter,
- Verwaltungsakt (z. B. Antragsverfahren, Beihilfebescheid) bzw. Kommunikation mit rechtsverbindlichen Aussagen.

An ein Schriftformerfordernis ist ggf. die handschriftliche Unterschrift eines Beteiligten geknüpft. Konsequenter Weise entstehen im elektronischen Geschäftsgang Medienbrüche in der Kommunikation mit externen Partnern, falls keine qualifizierte elektronische Signatur gebildet und geprüft werden kann.

Für die notwendige Nachweisführung im papierbasierten Postausgang wird z. B. ein Absendevermerk auf den Entwurf angebracht und die Zu-

[3] Zu den Möglichkeiten einen medienbruchfreien Daten- und Dokumentenaustausch zwischen Behörden aufzubauen, siehe das Erweiterungsmodul „Inner- und interbehördliche Kommunikation“, Schriftenreihe der KBSt, Band 65.

[4] Nach BGB § 126(1) muss, wenn durch Gesetz schriftliche Form vorgeschrieben ist, eine Urkunde von dem Aussteller eigenhändig durch Namensunterschrift unterzeichnet werden. Zur elektronischen Form und zur Schriftform siehe BGB §126(3) und 126a(1); Siehe auch FormVAnpG, Gesetz zur Anpassung der Formvorschrift des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr.

stellung in einem Postausgangsbuch vermerkt. Bei Zustellverfahren wie etwa Telefax wird der Sendebericht zum Vorgang genommen oder beim Postversand das Einschreibeverfahren mit Rückschein genutzt. Der Nachweis von aktenrelevanten E-Mails als Papierausdruck bleibt vom Bearbeiter abhängig. Mit diesem Medienbruch bleibt in der Regel auch die Erfassung in einem Postausgangsbuch aus.

Zur Posteingangsbehandlung[5] gehört es, das aktenrelevante Schriftgut mit Grunddaten (wie z. B. Eingangsdatum) in Registraturhilfsmitteln zu erfassen (wie z. B. Posteingangsbuch). Ggf. ist eine Empfangsbestätigung für den Nachweis zur Fristwahrung zu quittieren (Rückschein). Dezentral eingehende E-Mails, sofern diese aktenrelevant sind, werden ausgedruckt und zur Akte genommen. Mit diesem Medienbruch bleibt analog häufig auch die Erfassung in einem Posteingangsbuch aus.

Um die genannten Geschäftsvorfälle vollständig online abzuwickeln, sind äquivalente Lösungen zum rechtsverbindlichen papierbasierten Ablauf notwendig. Hierzu gehört u. a. der Einsatz der qualifizierten elektronischen Signatur als Ersatz der handschriftlichen Unterschrift[6] wie auch weitere Funktionen der Postein- und -ausgangsbehandlung. Ein VBS muss hierfür zusätzliche Funktionen und Dienste einbinden, die es selbst nicht anbieten kann.

Die Medienbrüche in der Interaktion zwischen einer Behörde und einem externen Partner sollen mit Hilfe einer so genannten „Virtuellen Poststelle“ beseitigt werden. Gleichsam muss die Rechtsverbindlichkeit in der Interaktion gewahrt werden. Hierfür muss eine „Virtuelle Poststelle“ auf Behördenseite die sicherheitsrelevanten kryptographische Dienste für unterschiedliche Kommunikationskanäle vorhalten.

Die Einführung elektronischer Unterstützungsmechanismen führt nicht zur Erhörung fachspezifischer rechtlicher Anforderungen. Es kann daher insbesondere im innerbehördlichen (aber auch im interbehördlichen) Austausch von Dokumenten i.d.R. auf die Verwendung von qualifizierten elektronischen Signaturen verzichtet werden (Vermeiden einer Mitzeichnungsflut).

[5] Vgl. DOMEA®-Organisationskonzept, Kap. 4.1

[6] SigG 2001 § 2 Begriffsbestimmungen: „Elektronische Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen (...)“. Das SigG 2001 § 2 unterscheidet verschiedene Erscheinungsformen elektronischer Signaturen: einfach, fortgeschritten, qualifiziert sowie qualifiziert mit Anbieterakkreditierung.

3.2 Interaktion Vorgangsbearbeitungssystem – Virtuelle Poststelle

Der elektronische Geschäftsprozess, der mittels VBS und VPS abgewickelt wird, unterliegt verfahrensbedingten Vorgaben, wie sie das DOMEA®-Organisationskonzept beschreibt.[7] Die Grundprinzipien des Verwaltungshandelns stecken den rechtlichen und organisatorischen Rahmen ab: dauerhafte, klare Arbeitsteilung, Amtshierarchie, Regelgebundenheit des Verwaltungshandelns und Aktenmäßigkeit. Aus Sicht der elektronischen Aktenführung liefern die Prinzipien Aktenmäßigkeit und Regelgebundenheit des Verwaltungshandelns die wesentlichen Vorgaben. Die Regeln und Normen des Verwaltungshandelns verpflichten:

- zur aufgabenbezogenen Aktenführung zusammenhängender Schriftstücke,
- zur Nachvollziehbarkeit der Urheberschaft sowie zum Nachweis von Dokumenten (vollständig und wahr),
- zur Rekonstruktion der Entscheidungs- und Bearbeitungsprozesse und
- zur Revisionsfestigkeit in der Aktenführung.
- Die verbindliche elektronische Akte gewährt über den gesamten Lebenszyklus, dass aktenrelevante Tätigkeiten und Ergebnisse an den Objekten „Dokument“, „Vorgang“ und „Akte“ nachvollziehbar sind.

Als Vorgabe für ein VBS einschließlich Speicher- und Archivsystem gilt, dass die Integrität, Vertraulichkeit, Verfügbarkeit, Authentizität (klassische Schutzziele) sowie Zeitliche Bestimmtheit und Nachweisbarkeit der Bearbeitung und Daten (erweiterte Schutzziele) gegeben sein muss.[8]

Ein elektronischer Lösungsansatz VPS muss für die Posteingangs- und Postausgangsdienste auf Behördenseite die:

- Übertragungssicherheit und die Erfüllung der Anforderungen an den Schutzbedarf gewähren,
- Sicherheitsrelevante kryptographische Bearbeitungs- und Ergebnisdaten elektronisch generieren,
- Sicherheitsdienste aus einem VBS heraus, über Web oder über die Mail-Anwendung anbieten,
- Sicherheitsrelevante Erfassungsdaten erheben und für das VBS (als nachfolgendes System) vorhalten.

Aus Sicht der IT-gestützten Vorgangsbearbeitung können in verschieden Teilprozessen eines Geschäftsganges Dienste einer VPS erforderlich

[7] Siehe DOMEA®-Konzept, Organisationskonzept 2.1, hier die Grundprinzipien des Verwaltungshandelns und den Geschäftsgang.

[8] Siehe auch das Erweiterungsmodul: Technische Aspekte der Archivierung, Kapitel 5.1 Revisionssicherheit.

sein. Dabei unterscheiden sich die Teilprozesse Posteingang, Bearbeitung sowie Postausgang bezüglich der Aufgaben im Umgang mit Dokumenten:

- Posteingang,
  - Teilaufgaben: Annehmen, prüfen, quittieren, erfassen, registrieren und übergeben des Posteingangsobjekts.
- Bearbeitung,
  - Teilaufgaben: Objekt signieren und vertrauensvoll behandeln, prüfen, Metadaten übernehmen und erfassen.
- Postausgang,
  - Teilaufgaben: Annehmen, initiieren, erfassen des Postausgangsobjekts.

Der Schutzbedarf für die Kommunikation und Daten sowie für die Nachweispflicht gilt im elektronischen, wie im papierbasierten Verfahren gleichermaßen. Der Einsatz einer Virtuelle Poststelle soll dazu dienen, im elektronischen Geschäftsverkehr die gleiche oder eine vergleichbare Sicherheit zu bieten, wie ein papierbasierter Geschäftsprozess. Die äquivalenten Einzelschritte zum papierbasierten Geschäftsprozess müssen, insofern diese aktenrelevant sind, an den elektronischen Dokumenten über die Dauer ihres Lebenszyklus erkennbar sein.

Welche verfahrensbedingte Anforderungen aus der Interaktion mit einem Vorgangsbearbeitungssystem hervorgehen, beschreibt das nachfolgende Kapitel anhand der genannten Schutzziele.

3.3 Verfahrensbedingte Anforderungen

Aus Sicht der IT-gestützten Vorgangsbearbeitung müssen gemäß den oben genannten Schutzzielen entsprechende kryptographische Dienste auf Abruf bereitgehalten werden, die dem Schutzbedarf des papierbasierten Geschäftsprozesses entsprechen. Die äquivalenten Verfahren wie etwa elektronische Signaturen und Verschlüsselung sind ggf. an den Objekten Dokument, Vorgang oder Akte nachzuvollziehen. Sie sind Bestandteil der Abwicklung eines Geschäftsprozesses.

3.3.1 Sichere Kommunikation mit einer Behörde

Eine Behörde bietet für die elektronische Kommunikation einem externen Partner je nach Anlass und Schutzbedarf einen entsprechenden Adressaten an. Aus prozessualer Sicht kommen einzelne Mitarbeiter aber auch Organisationseinheiten als Behördenadressaten in Frage. Welcher Adressatentyp angegeben wird, ist für das zugrunde liegenden Verfahren festzulegen und führt bei kryptographisch bearbeiteten Nachrichten zu

organisatorischen und technischen Konsequenzen. Die sicherheitsrelevanten Dienste können sowohl an den Arbeitsplätzen einzelner Mitarbeiter als auch an zentraler Stelle im Geschäftsprozess erledigt werden.

Grundsätzlich bieten sich unabhängig vom Kommunikationskanal (E-Mail, Web) folgende Kommunikationsarten an:

- Ende-zu-Ende und
- Ende-zu-Organisation.

Bei der Ende-zu-Ende Kommunikation sind dezidierte Behördenmitarbeiter die Adressaten. Die konkreten Empfänger können als einzige auf die eingehende Post zugreifen. Besteht die Notwendigkeit Daten am Arbeitsplatz eines Mitarbeiters kryptographisch zu bearbeiten, so ergeben sich daraus konkrete Nachteile. Die Nachteile gegenüber einer zentralen Lösung beziehen sich auf die Bereiche: Schlüsselmanagement, Interoperabilität, Administrations- und Bedienaufwand, Vertreterregelung, und der Inhaltsprüfung auf Schadinhalte (siehe folgend die Vorteile einer zentralen Lösung).

Bei der Ende-zu-Organisation Kommunikation ist der Behördenadressat beispielsweise thematischen Bezügen zugeordnet. Die Wahl des Themas leitet dabei auf die Behörde oder auf einzelne Organisationseinheiten. Alle potenziellen Empfänger einer solchen Benutzergruppe innerhalb der Behörde haben Zugriff auf die eingehende Post. Die Absicherung einer solchen Kommunikation basiert auf einer zentralen Serverkomponente. Im innerbehördlichen Austausch kann auch die Kommunikation von Organisation zu Organisation bestehen. Da in diesem Fokus lediglich die Empfängerseite betrachtet wird, ergeben sich keine weiter zu beachtenden Unterschiede.

In Ergänzung zu den oben aufgeführten Kommunikationsarten sichert eine zentrale Serverkomponente die Kommunikation von einem Endpunkt zu anderen ab:

- Ende-zu-Ende Sicherheit,
- Ende-zu-Organisation Sicherheit.

Die Endpunkte der sicheren Kommunikationswege legen den Punkt des Kommunikationsweges fest, an dem die Sicherheitsfunktionalitäten greifen und entsprechende Sicherheitslösungen eingesetzt werden können.

Die zentrale Lösung für ein Angebot sicherheitsrelevanter Dienste:

- leistet ein einfaches Management kryptographischer Schlüssel innerhalb der Verwaltung,
- reduziert den Administrations- und Bedienaufwand der Sicherheitsfunktionalitäten,
- garantiert verfügbare Vertreter,

- gewährt die Möglichkeit der Prüfung des ein- und ausgehenden Datenverkehrs auf Schadinhalte.

Die Verwaltung ermöglicht dem Kunden ohne Umwege mit ihr zu kommunizieren. Sie tritt dabei einheitlich sowie in geschlossener Form dem Kunden gegenüber.

Welche Sicherheit für die Kommunikation angemessen ist, entscheidet der Schutzbedarf für die ein- und ausgehenden Daten, in Abhängigkeit zum jeweiligen Fachverfahren.

3.3.2 Skalierung des Schutzbedarfs

Aus Sicht der IT-gestützten Vorgangsbearbeitung sind unterschiedliche Schutzziele und -anforderungen bei der Interaktion mit einer Behörde und mit der VPS abzudecken.[9]

Die Regelungen innerhalb der Vorgangsbearbeitung liefern Vorgaben, welcher Schutzbedarf für aus- und eingehende Daten gilt. Der Schutzbedarf ist hinsichtlich der Schutzziele Integrität, Vertraulichkeit, Verfügbarkeit, Authentizität, Zeitliche Bestimmtheit und Nachweisbarkeit zu ermitteln und, wo nötig, von der VPS zu gewähren.

Die eingangs genannten Fallbeispiele (wie etwa Antragsverfahren etc.) begründen in der Regel mindestens einen hohen Schutzbedarf hinsichtlich der Schutzziele. Typisch für die Fälle ist, dass diese schützenswürdige Daten enthalten, der Schriftform (inklusive handschriftlicher Unterschrift) oder Fristen unterliegen. Treten die Fälle in umfassender Zahl auf, können diese Dienstleistungen ggf. als medienbruchfreier elektronischer Geschäftsprozess gestaltet werden. Dies ist zum Beispiel Zielsetzung verschiedener Projekte von BundOnline. Der medienbruchfreie Prozess ist mit angemessenen Sicherheitsfunktionen für ein- und ausgehende Daten auszustatten. Hierzu gehört etwa die Erstellung und Prüfung von qualifizierten Signaturen.

Die Skalierung des Schutzbedarfes weist die VPS an, welche Qualität der Sicherheit (Sicherheitsstufe) für den Einsatz der kryptographischen Funktionen an welchen ein- und ausgehenden Daten oder Datenkanälen zu vollziehen sind. Etwa unter welchen Bedingungen eine qualifizierte oder eine fortgeschrittene Signatur notwendig ist oder welche Schlüsselstärken für Signatur oder Verschlüsselung verwendet werden müssen.

Gleichsam kann der Bedarf für eine VPS entfallen, sofern die Anforderungen für die Kommunikationen in den Geschäftsfällen den Einsatz ei-

[9] Siehe Schutzziele gemäß eGovernment Handbuch: Verschlüsselung und Signatur. Grundlagen und Anwendungsaspekte, 2002; Siehe auch BSI, Fachkonzept für die Virtuelle Poststelle als Basiskomponente Datensicherheit von BundOnline, 2003.

ner qualifizierten Signatur nicht einschließen. In diesen Fällen können die Sicherheitsziele auch durch einfachere kryptographische Anwendungen erreicht werden. Für Forderungen nach einer fortgeschrittenen oder einer einfacheren Signatur oder nach Verschlüsselung bieten ggf. Lösungen wie etwa die PKI-1 Verwaltung[10] oder SSL Kanalverschlüsselungen den angemessenen Schutz.

Da in einer Behörde Geschäftsprozesse mit unterschiedlichen Sicherheitsanforderungen ablaufen, muss eine virtuelle Eingangs- und Ausgangsstelle die Möglichkeit bieten, unterschiedliche Sicherheitsniveaus zu unterstützen. Für den innerbehördlichen Austausch ohne Schriftformerfordernis kann eine fortgeschrittene Signatur gesetzt werden. Beim Massenversand von elektronischen Dokumenten reicht ggf. auch die fortgeschrittene Signatur aus. In anderen Fällen wird ggf. gänzlich auf eine Signatur verzichtet werden können und lediglich die Verschlüsselungsfunktion für vertrauliche Datenübertragung genutzt werden.

Die folgenden Schutzziele werden hinsichtlich der genannten Beispiele betrachtet, für die die Vorgangsbearbeitung einen Schutzbedarf ansetzt.

3.3.3 Integrität

Integrität bedeutet, dass Manipulationen von Dokumenten und Daten über kryptographische Mittel nachprüfbar erkannt werden können. Hierfür werden elektronische Signaturen genutzt. Die erfolgreiche Prüfung der elektronischen Signatur weist die Integrität der übertragenen Dokumente und Daten nach. Dabei ist eine eindeutige Zuordnung von Datei mit Signatur durch das Prüfungsergebnis verbindlich und nachweislich gegeben.

Die Integrität gewährt (in Verbindung mit der Zertifikatsprüfung) zudem die Authentizität der Daten: Die Daten können bei Signaturprüfung dem Kommunikationspartner zugeordnet werden (Siehe Verbindlichkeit und Nichtabstreitbarkeit).

Mit Hilfe geeigneter Mechanismen kann die Integrität über eine definierte Zeit sowie auf allen übertragenen Speicher- und Archivierungsmedien erhalten werden. Signaturen gespeicherter Dokumente mit einer Aufbewahrungsfrist von bis zu 30 Jahren können im Verlauf Ihrer Speicherung im VBS „unsicher“ werden.[11] Die zur Erzeugung verwendeten Schlüssel (Schlüsselalgorithmus) oder Verfahren können nicht mehr als sicher angenommen werden. Zeitstempelsignaturen können als „erneute

[10] Vgl. ZPO § 174(3). Siehe auch KoopA ADV: Architekturmodell für Interoperabilität von eGovernment-Anwendungen in Bund, Ländern und im Kommunalen Bereich in Deutschland, 2003, S. 7. Erhältlich als Download unter der URL: http://www.koopa.de/beschluesse/egovernment.html

[11] Siehe SigV § 4(1) und (2).

Signatur“, bzw. als eine so genannte Übersignatur, verwendet werden, um ein „unsicher“ gewordenes signiertes Dokument nachhaltig zu sichern.[12]

3.3.4 Vertraulichkeit

Personenbezogene oder anderweitig vertrauliche Daten (z. B. Steuer-, Sozialgeheimnis oder Daten, die aus der Natur der Sache geheim sind) müssen vertraulich behandelt werden. Diese Daten sind bei einer elektronischen Übermittlung verschlüsselt und nur durch einen dezidierten Empfänger nach Eingang der Daten zu entschlüsseln.

Kryptographische Verschlüsselungsmechanismen stellen diese Vertraulichkeit her. Vertraulichkeit meint, dass Dokumente und Daten bei der Übertragung vor unzulässiger Einsichtnahme durch Dritte geschützt sind. Da der Eingangsempfänger sowohl eine Behörde als auch ein Behördenmitarbeiter sein kann, muss eine Verwaltung von „Entschlüsselungsschlüsseln“ für Mitarbeiter- und Behörden möglich sein.

3.3.5 Verfügbarkeit

Verfügbarkeit bedeutet, dass der Interaktionsdienst Dokumente und Daten bei Bedarf zustellt sowie benötigte Funktionen bedarfsgerecht bereithält.

3.3.6 Verbindlichkeit und Nichtabstreitbarkeit

Bei der Initiierung wie auch beim Abschluss von Verwaltungshandeln mit Rechtsfolge (Rechtsgeschäft) besteht ggf. aufgrund von Schriftformerfordernis ein Bedarf nach rechtsgültiger Verbindlichkeit.

Es muss in diesem Fall eindeutig erkennbar sein, wer ein Dokument mit rechtsverbindlicher Unterschrift geliefert hat (Authentizität der Daten). Die Herkunft ist eindeutig dem identifizierten Absender und der Erhalt dem identifizierten Empfänger zuzuschreiben.[13] Mit Hilfe der VPS kann die Nicht-Abstreitbarkeit der Übertragung von Dokumenten und Daten sichergestellt werden.

[12] Zur Langzeitarchivierung siehe das Erweiterungsmodul „Technische Aspekte der Archivierung elektronischer Akten, Schriftenreihe der KBSt, Band 67. Dort werden in Kapitel 5.1.3 Archivierungskonzepte und -technologien für eine „beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“ thematisiert. Kapitel 8.2 diskutiert das Signaturgesetz hinsichtlich der Möglichkeit von Übersignierverfahren.

[13] Siehe eGovernment Handbuch: Authentisierung im eGovernment. Mechanismen und Anwendungsfelder der Authentisierung, 2002, S. 23, 30; Siehe auch eGovernment Handbuch: Verschlüsselung und Signatur, Grundlagen und Anwendungstechniken,2002, S. 12f.

Behördenspezifische individuelle Dienstleistungen stehen natürlichen oder juristischen Personen zur Verfügung, nachdem diese sich in ausreichender Form authentisiert haben. Authentizität meint, dass die Beteiligten eindeutig identifiziert sind (z. B. mit dem Einloggen auf dem Webportal). Authentizität ist bei Sensitivität der Daten notwendig wie auch um einzelne Aktivitäten zu Personen sowie IT- Komponenten (etwa Clients, Server) zuzurechnen.[14]

Verbindlichkeit entsteht, indem die Authentizität der Kommunikationspartner eindeutig ist, d. h. der Kommunikationspartner ist real auch derjenige, der er vorgibt zu sein. Hierfür ist der Nachweis der Identität mittels Registrierung, die Vertrauenswürdigkeit der Registrierungsinstanz und die Übergabe der Authentisierungsdaten von Bedeutung.

Die elektronischen Signaturen sind grundsätzlich geeignet, die Identität festzustellen. Die erfolgreiche Prüfung einer Signatur weist die Herkunft nach und gewährt Beweiskraft gegenüber Dritten. Die qualifizierte Unterschrift ist dabei der handschriftlichen Unterschrift bezüglich der Beweiskraft gleichgestellt. Darüber hinaus muss ggf. nachprüfbar sein, ob der Interaktionspartner auch unterschriftsberechtigt ist.[15]

Der Einsatz von Zeitstempelsignaturen, als eine Form der elektronischen Signatur, kann die Beweiskraft gegenüber Dritten gewährleisten (Siehe auch Zeitliche Bestimmtheit).

Ein elektronisch erlassener Verwaltungsakt mit gesetzlichem Schriftformerfordernis stellt nur dann Verbindlichkeit her, wenn dieser mit einer Rechtsbehelfsbelehrung versehen ist und beide qualifiziert elektronisch signiert sind (Sofern die Rechtsbehelfsbelehrung ein Teil der zu signierenden Datei ist, wird dieser Teil gezeichnet).

Misslingt die elektronische Kommunikation mit der Behörde, hat diese die Pflicht, den Bürger zu informieren. Sie muss die technischen Bedingungen nennen, unter denen die Kommunikation erfolgen kann oder Infor-

[14] Siehe eGovernment Handbuch: Authentisierung im eGovernment. Mechanismen und Anwendungsfelder der Authentisierung, 2002.

[15] Siehe VwVfG §37(3); Es regelt u. a. die Verwendung von qualifizierten Schlüsselzertifikaten und qualifizierten Attributzertifikaten im Verwaltungsakt: „Ein schriftlicher oder elektronischer Verwaltungsakt muss die erlassende Behörde erkennen lassen und die Unterschrift oder die Namenswiedergabe des Behördenleiters, seines Vertreters oder seines Beauftragten enthalten. Wird für einen Verwaltungsakt, für den durch Rechtsvorschrift die Schriftform angeordnet ist, die elektronische Form verwendet, muss auch das der Signatur zugrunde liegende qualifizierte Zertifikat oder ein zugehöriges qualifiziertes Attributzertifikat die erlassende Behörde erkennen lassen.“

mieren, dass die Bearbeitung z. B. aufgrund von Virenbefall ausgesetzt wurde.[16]

3.3.7 Zeitliche Bestimmtheit

Dokumente und Daten unterliegen ggf. einer zeitlichen Bestimmtheit. Um Fristen einzuhalten, sind ein- und ausgehende Daten verbindlich zu bestimmen und zu prüfen. Die Nicht-Abstreitbarkeit des Erhalts kann durch unabhängige Dritte geprüft werden. Hierfür ist ein Zeitstempel mittels elektronischer Signatur notwendig.

3.3.8 Nachweisbarkeit

Der gesamte medienbruchfreie Laufweg mit seinen Ergebnissen muss nachvollzogen werden können. Das Verwaltungshandeln mit Rechtsfolge muss beweiskräftige Nachweise über die rechtsverbindlichen Kommunikationen liefern. Ggf. ist die Kommunikation auf ein persönliches Handeln zurück zu führen. Dies bedeutet für die rechtsverbindliche Kommunikation, dass die Authentifizierung zu protokollieren ist und ggf. als Beweis gegenüber Dritten verwertbar ist (ggf. Zeitstempel für Authentisierungsdaten).

Ein Dokument ist der Behörde zugegangen, wenn es in die Verfügungsgewalt der Behörde gelangt: dies ist unter Verwendung einer Virtuellen Poststelle in der Regel der elektronische Postkasten (OSCI-Lösung) oder ein Mailserver.[17] Zur Beweissicherung kann ggf. automatisch und gesichert ein elektronisches Dokument mit Eingangsbestätigung und Zeitbestimmung quittiert werden.

Der elektronisch nachzuweisende Geschäftsvorfall ist über den bereinigten Medienbruch hinaus ausgedehnt. Die Aktenmäßigkeit verlangt, dass der Nachvollzug der Urheberschaft sowie der Nachweis vollständig und wahr sind. Die Nachvollziehbarkeit der beteiligten Komponenten, Prozesse und Dienste muss elektronisch gewährleistet sein.

Bei fehlgeschlagenen Signaturprüfungen oder Unlesbarkeit eines elektronischen Dokuments muss der externe Interaktionspartner unverzüglich von der Behörde auf die Unrichtigkeit und die Notwendigkeit eines neuen

[16] Siehe VwVfG § 3a(3) Elektronische Kommunikation.

[17] Siehe eGovernment-Handbuch, Rechtliche Rahmenbedingungen für eGovernment, 2003, S. 45; Es genügt der Eingang des elektronischen Dokuments in den elektronischen Postkasten der Behörde. Als nicht zugegangen gelten Dokumente, die in nicht lesbarer Form übersendet wurden (S. 46). Vgl. auch ZPO § 130a, Elektronisches Dokument „ein elektronisches Dokument ist eingereicht, sobald die für den Empfang bestimmte Einrichtung (...) es aufgezeichnet hat“. Siehe auch JKomG §55a(2). Siehe auch ZustRG § 174(3).

Antrages bzw. über die fehlgeschlagene Kommunikation hingewiesen werden. Ein entsprechender Benachrichtigungsmechanismus muss die Prüfinformationen weiterleiten.[18]

Aus Sicht des VBS muss für elektronische Akten eine revisionssichere Dokumentation und Archivierung sichergestellt werden, dass die verarbeiteten Dokumente plus Daten der Weiterverarbeitung unveränderbar, vollständig, wahrheitsgemäß und dauerhaft lesbar aufbewahrt werden können. Dabei besteht bei elektronischen Dokumenten mit qualifizierter Signatur die Pflicht, die dauerhafte Überprüfbarkeit der elektronischen Signaturen solange sicherzustellen, wie die elektronischen Dokumente archiviert werden müssen. Akkreditierte Zertifizierungsanbieter stellen diesen Dienst für die von ihnen ausgegebenen Zertifikate bis zu 30 Jahren zur Verfügung. Siehe auch das Kapitel 3.3.3.

[18] Siehe eGovernment-Handbuch, Rechtliche Rahmenbedingungen für eGovernment, 2003, S. 48. Eine ungültige oder nicht vorhandene Signatur macht den Antrag im förmlichen Verfahren immer unwirksam.

4 VIRTUELLE POSTSTELLE

4.1 Funktionen einer Virtuellen Poststelle

Eine VPS ergänzt vorhandene Komponenten der beteiligten IT-Systeme, mit denen eine Behörde über das Internet kommuniziert. Auf Anforderung werden bei der Kommunikation zwischen Behörde und externem Kunden für die Behörde sowohl eingehende als auch ausgehende Daten ver- bzw. entschlüsselt, geprüft und/oder signiert übermittelt. Die VPS übernimmt für diese Anforderungen die sachgerechte Bearbeitung der Daten. Alle VPS-Funktionen stehen für die Web-, E-Mail- und auch für die anwendungsspezifische Kommunikation einer Behörde bereit.

Die Virtuelle Poststelle bietet aus Sicht der IT-gestützten Vorgangsbearbeitung wichtige Funktionen, um die dargelegten verfahrensbedingten Anforderungen zu erfüllen. Die VPS erbringt nicht alle Funktionen selbst, sie tritt ebenfalls als Mittler zu anderen Diensten auf (z. B. Zeitstempeldienst).

Aus Sicht des VBS bietet die VPS die folgenden Grundfunktionalitäten an zentraler Stelle an:

- Ver- und Entschlüsselung der Daten,
- Signaturbildung (qualifizierte, fortgeschrittene) über Dokumente/ Daten und Signaturprüfung,
- Bereitstellen von Zeitstempeln und Zeitstempelprüfung,
- Nutzung interner oder externer Verzeichnisdienste (öffentliche und behördenbezogene private Verschlüsselungsschlüssel, Zertifikate),
- Dokumentation der sicherheitsrelevanten Bearbeitung und der Ergebnisse,
- Quittungsmechanismen.

Hinzu kommen administrative Servicefunktionen der VPS, die abseits der eigentlichen Geschäftsprozesse berücksichtigt werden müssen. Hierzu gehören etwa die Speicherung und Verwaltung privater kryptographischer Schlüssel.

4.2 Zugriffsmöglichkeiten auf eine VPS

Die Darstellung einer Virtuellen Poststelle orientiert sich an den Zugriffsstellen auf sicherheitsrelevanten Funktionen. Eine VPS erscheint als ein Verbund technischer Komponenten, die an verschiedenen Stellen betrieben werden können. Eine VPS bietet dem Benutzer drei Möglichkeiten auf sicherheitsrelevante Funktionen zuzugreifen:

- Web Interface,

- E-Mail Interface und
- direkt aus dem VBS (Hintergrundsystem Interface).

Die zentralen Mechanismen einer Virtuellen Poststelle unterstützen die in Kapitel 3.3.1 angeführten Kommunikationsarten. Je nach Anforderung bearbeitet eine VPS Daten kryptographisch und leitet sie anschließend weiter oder lässt Daten ebenso unbearbeitet passieren.

4.2.1 Web Interface – OSCI

OSCI[19] ist ein offenes auf XML basierendes Kommunikationsprotokoll, mit dem signierte und verschlüsselte Daten übertragen werden können. Neben dem Nachrichtentransport als OSCI-Transport ist die Standardisierung der Inhaltsdaten für den Transport als OSCI-XÖV zu unterscheiden. OSCI-XÖV fasst Standardisierungsbemühungen von XML-Beschreibungen für fachspezifische Grunddatensätze der öffentlichen Verwaltung zusammen.[20] OSCI-Transport ist offen gegenüber allen Formaten von Inhaltsdaten.

Die Infrastruktur von OSCI-Transport besteht aus den Komponenten OSCI-Client, OSCI-Manager und OSCI-Backend-Enabler. Die zwischen diesen Komponenten ablaufende Kommunikation basiert ausschließlich auf dem Austausch von XML-strukturierten OSCI-Nachrichten bzw. OSCI-Paketen via SOAP und HTTP.[21]

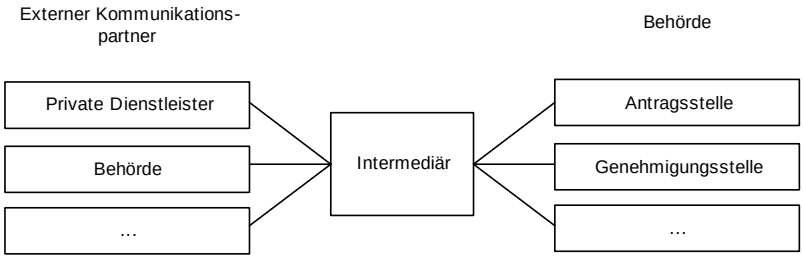

Abbildung 1: Prinzip Intermediär

OSCI-Transport beschreibt den sicheren Nachrichtentransport über das Internet. Grundlegend sind die Sicherheitsprinzipien „doppelter Um-

[19] OSCI steht für Online Services Computer Interface. Siehe hierzu http://www.osci.de.

[20] Siehe OSCI Leitstelle, Informationen über OSCI, Bremen 2004. Beispiele für fachspezifische Grunddatensätze siehe das DOMEA®-Erweiterungsmodul: Inner- und interbehördliche Kommunikation; Siehe auch XML-Infopoint auf den Web-Seiten der KBSt.

[21] OSCI-Transport ist eine für die Zwecke der öffentlichen Verwaltung angepasste Profilierung der XML-basierten SOAP-Spezifikation. Zum Transport der Nachrichten nutzt OSCI die Mechanismen des auf XML basierenden Transportprotokolls SOAP. SOAP-Nachrichten selbst werden wiederum via HTTP/HTTPS (über das Internet) transportiert.

schlag“ und „Intermediär (=OSCI-Manager)“ (siehe Abbildung 1 und Abbildung 2). Der doppelte Umschlag stellt sicher, dass Nachrichten von einer vertrauensvollen Übermittlungsinstanz (Intermediär) weitergeleitet werden, die Inhaltsdaten aber ausschließlich vom Autor und vom Empfänger verarbeitet werden können. Die Ende-zu-Ende verschlüsselten Inhaltsdaten werden in einem Umschlag für den Empfänger und dieser wiederum für den Transport zusammen mit einem Laufzettel in einen Transportumschlag gekapselt.

Ein externer Autor verfügt über eine Client-Anwendung, die über den Web-Browser automatisch gestartet wird und den Zugang zu einer OSCI-Infrastruktur eröffnet. OSCI-Nachrichten können erstellt und signiert werden. Für die Signaturerzeugung wird eine Signaturanwendungskomponente und ggf. ein Kartenleser des Kunden eingebunden.

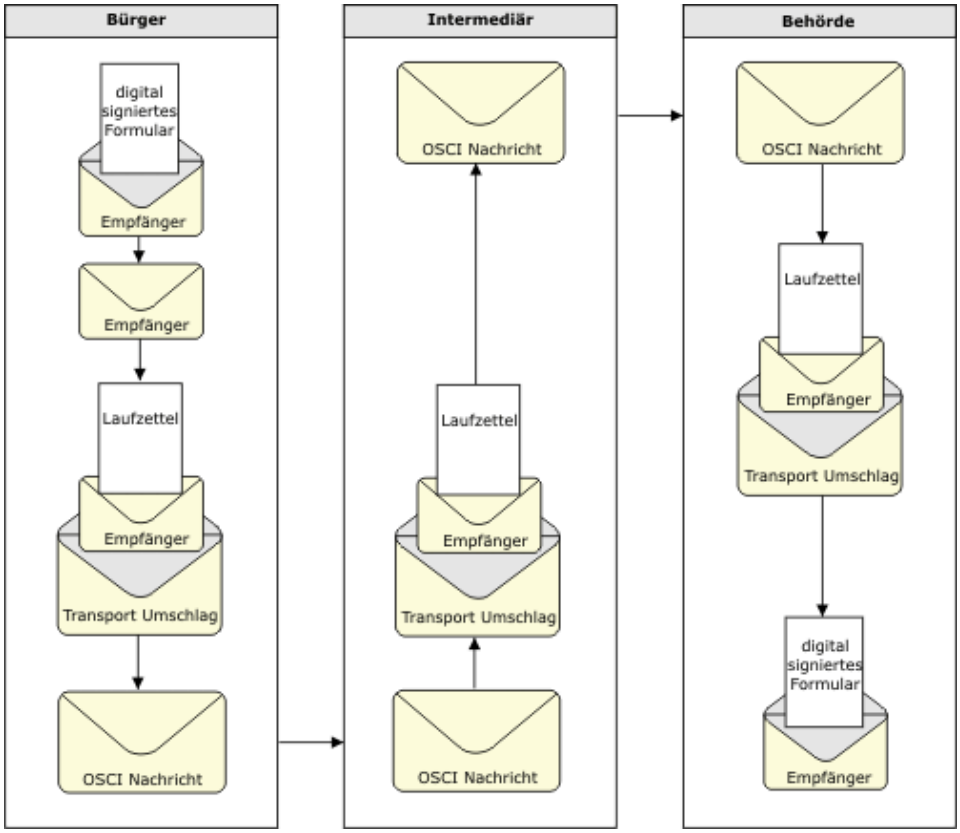

Abbildung 2: Prinzip Doppelter Umschlag[22]

Eine Behörde bzw. ein einzelner Behördenmitarbeiter nutzt hingegen das Interface des VBS, um eine Nachricht zu versenden – die Möglichkeit eines separaten Clients bleibt unberücksichtigt. Das VBS spricht den OSCI Backend Enabler an (z. B. mittels Funktionsaufruf).

[22] Quelle: OSCI.

Zu Beginn einer Kundenbeziehung müssen die externen Partner einer Behörde ihre öffentlichen Verschlüsselungszertifikate der Behörde zukommen lassen bzw. den Verzeichnisdienst bekannt geben, in dem sie verwaltet werden.[23]

Bei erstmaliger Verwendung der VPS erzeugt der Benutzer über das OSCI Web Interface eine OSCI-Nachricht (Zum Aufbau einer OSCI-Nachricht siehe Abbildung 5). Der Benutzer nutzt das Zertifikat des Verschlüsselungsschlüssels vom Empfänger, um ein OSCI-Postfach beim OSCI-Manager anlegen zu lassen, die OSCI-Nachricht zu übergeben und dort abzulegen. Ein OSCI-Postfach wird dabei automatisch angelegt und bleibt dann bestehen.

Der OSCI-Manager öffnet den ihm zugänglichen ersten Umschlag (OSCI-Transportsicherung) und initiiert automatisch die Zertifikatsprüfung (Herkunftsnachweis und Gültigkeitsprüfung). Geprüft wird, welches Benutzerzertifikat zu einer bestimmten Signatur gehört (Herkunft), ob die Erzeugung der Signatur zum Prüfzeitpunkt gültig war (Prüfung des Zertifikats auf Sperrung oder Ablauf) und wer der Inhaber des Zertifikats ist (Identität).

Nach erfolgter Prüfung wird der Posteingang ins entsprechende Postfach gelegt. Das Entnehmen einer Nachricht aus dem OSCI-Postfach initiiert entweder der Empfänger (Mitarbeiter oder OE) manuell oder wird durch das VBS angestoßen. Die OSCI-Nachricht wird vom OSCI-Backend Enabler abgeholt, entschlüsselt und die Signatur mathematisch geprüft. Anschließend wird die OSCI-Nachricht dem VBS im geeigneten Format zur Verfügung gestellt. Dabei werden die Inhaltsdaten einer OSCI-Nachricht und bei Bedarf auch OSCI-Metainformationen dem VBS zur Verfügung gestellt.

4.2.2 Mail Interface

Die sicherheitsrelevanten Funktionen einer VPS lassen sich auch in den Mail-Verkehr einer Behörde einbinden. Die VPS Funktionen sind dabei an zentraler Stelle in der Mail-Transport-Kette innerhalb der Behörde integriert.

Bei Bedarf filtert die Mail-Komponente der VPS aus dem Mailstrom eingehende oder ausgehende Nachrichten (SMTP-Daten) und behandelt diese Daten kryptografisch, z.B. Signaturerzeugung, Ver- oder Entschlüsselung oder Signaturprüfung.

[23] Es bestehen verschiedene Möglichkeiten, Verschlüsselungszertifikate zu verwalten, wie z. B. über einen lokalen Zertifikatsspeicher im VBS, eine nicht-zugängliche Datenbank oder ein File-System.

Nach dem Herausfiltern werden eingehende und von der VPS kryptografisch behandelte Daten dem Mailstrom wieder zugeführt und im Empfänger-Postfach des Mailsystems als entschlüsselte und signaturgeprüfte Nachrichten inklusive der Prüfergebnisse zur Verfügung gestellt. Anschließend kann das VBS über geeignete Importfunktionen diese Daten übernehmen.

Über geeignete Exportfunktionen müssen die Daten des VBS an das Mailsystem übergeben und vom Mailsystem an den jeweiligen Empfänger versendet werden. Im Falle einer erwünschten kryptografischen Behandlung sind dabei explizite Eingriffsregeln für die VPS zu bestimmen. Bei Versendung werden die SMTP-Daten anschließend über die VPS geleitet, kryptografisch bearbeitet, und dem Mailfluss wieder zugeführt.

Eine Schnittstelle zwischen Mailsystem und VPS ermöglicht einen Funktionsaufruf aus dem VBS heraus und damit die Übergabe von SMTP-Daten an das Mailsystem. Gleichsam werden eingehende, von der VPS bearbeitete SMTP-Daten über das Mailsystem dem VBS übergeben.

Die Verschlüsselungszertifikate der Kommunikationspartner können entweder über ein lokales Zertifikatsmanagement (Zertifikatsspeicher) oder über öffentlich zugängliche Verzeichnisdienste verwaltet werden.

4.2.3 Direktzugriff auf VPS Funktionen

Aus Sicht eines VBS kann die Interaktion mit der VPS auch direkt stattfinden. Das VBS greift auf die VPS zu, um etwa ausgewählte Funktionen, wie in Kapitel 4.1 skizziert, durchzuführen. Das VBS muss hierzu in der Lage sein, ein solches Interface aufzurufen, zu steuern und die von der VPS benötigten Datenformate zu erzeugen bzw. auszuwerten.

Ein solches Interface stellt die Interaktion, den Transport der Daten zwischen VBS und VPS und Formatierungsfunktionalitäten zur Unterstützung VBS- und VPS-spezifischer Formate sicher.

5 TEILPROZESSE ZWISCHEN VBS UND VPS

Das folgende Kapitel stellt die organisatorisch-technische Integration der VPS in die Abläufe des VBS heraus.

Die prozessuale Sicht ermöglicht, Anforderungen an die Integration beider Systeme aus den fachlich-organisatorischen Gegebenheiten abzuleiten.

Aus der Sicht des VBS existieren drei Kommunikationskanäle zur VPS (s. 4.2) die über verschiedene Anwendungen bedient werden.

In Abhängigkeit von den Sicherheitsanforderungen sowie der Kommunikationsstrategie gestalten sich die Teilprozesse zwischen VBS und VPS unterschiedlich.

Zu unterscheiden sind die abstrakten Teilprozesse bzw. Beispielszenarien:

- Posteingangsbehandlung – Behörde empfängt Daten:
  - Web,
  - E-Mail.
- Bearbeitung – kryptographische Bearbeitung von Daten:
  - Ad hoc Prüfung,
  - Wiederholungsprüfung zur Verifikation von Signaturen und Zertifikaten,
  - Bearbeitung von Prozess- und Inhaltsdaten,
  - Zeichnungslauf.
- Postausgangsbehandlung – Behörde sendet Daten:
  - Web,
  - E-Mail.

Die Beschreibung von Aufgaben der beteiligten Komponenten erfolgt beispielhaft anhand der Teilprozesse. Den technischen Abläufen auf VPS-Seite werden anschließend die organisatorisch-technischen Konsequenzen für die Weiterverarbeitung in der IT-gestützten Vorgangsbearbeitung gegenübergestellt.

5.1 Behörde empfängt Daten – Posteingang Web

Die Abbildung 4 stellt in einem Flussdiagramm den Teilprozess „Behörde empfängt Daten – Posteingang Web“ dar.

Die VPS übernimmt zu Beginn dieses Teilprozesses die Aufgabe „**Posteingang annehmen**“. Die mit Hilfe von OSCI-Transport vom externen Kommunikationspartner übermittelten Daten, wie etwa ein elektronisch gestellter Antrag und Anhang, werden im OSCI-Postfach des Empfängers abgelegt.

Die VPS übernimmt bei der Annahme der OSCI-Daten die Aufgabe „**Posteingang prüfen**“. Hierbei werden ggf. folgende Dienste erledigt:

- Entschlüsseln,
- Posteingangszeitpunkt für Empfänger quittieren,
- Integrität und Authentizität prüfen,
- Metadaten protokollieren.

Die VPS greift auf den privaten Entschlüsselungsschlüssel des Empfängers (Mitarbeiter oder Organisationseinheit) im Schlüsselverzeichnis zu und entschlüsselt den Eingang.

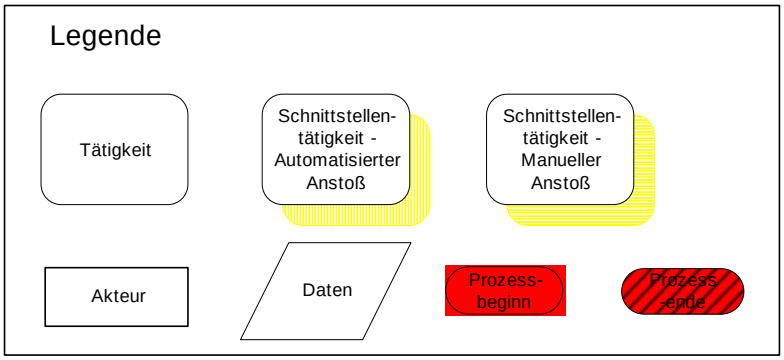

Abbildung 3: Legende

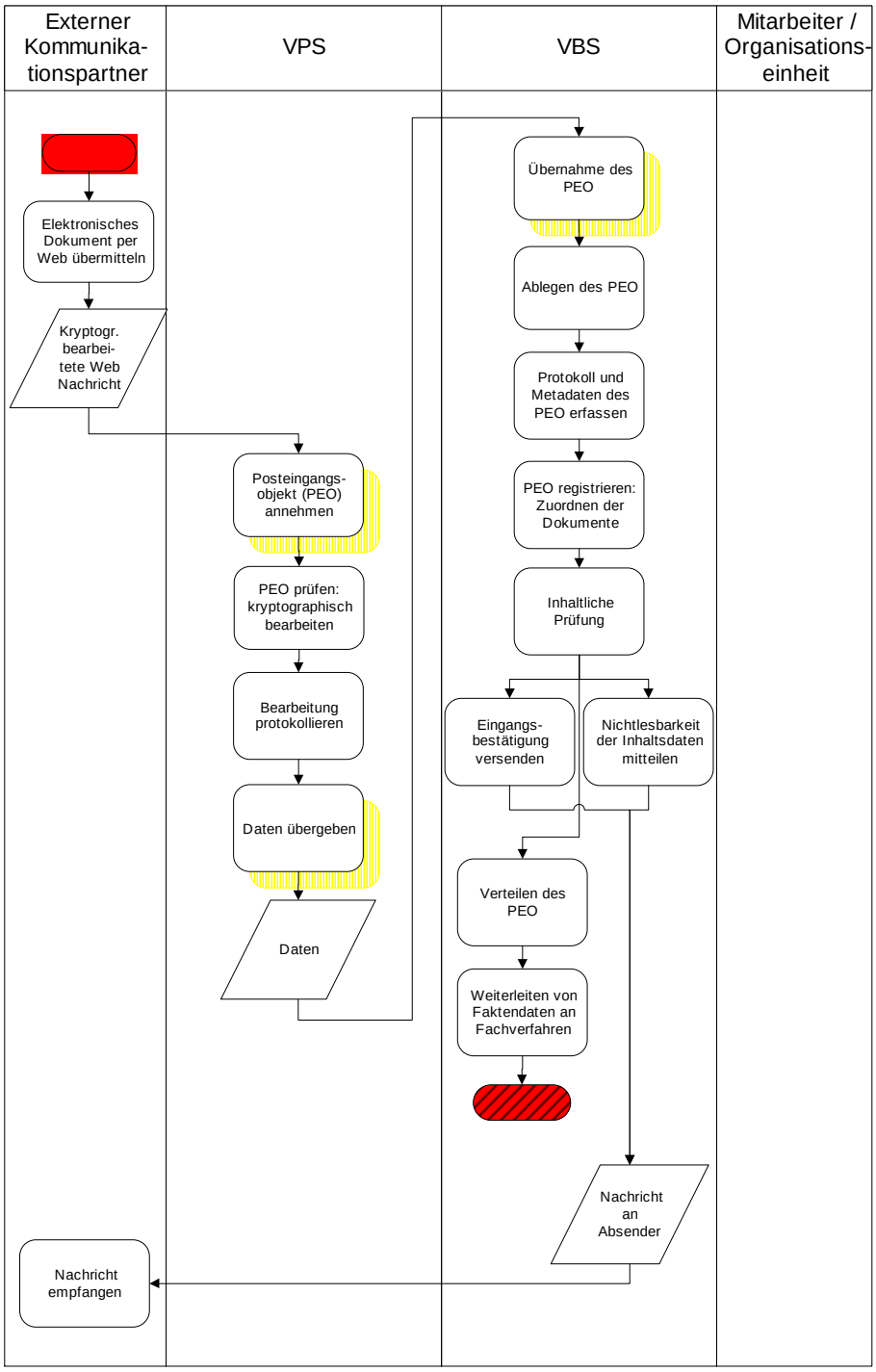

Abbildung 4: Behörde empfängt Daten: Posteingang Web

Der OSCI-Backend-Enabler prüft zeitgesteuert die OSCI-Postfachverwaltung. Bei Eingang neuer, geprüfter OSCI-Nachrichten holt er diese ab, entschlüsselt diese, prüft die Signatur und übergibt sie zur weiteren Verarbeitung.

Ein Posteingang gilt als zugestellt, wenn die OSCI-Nachricht in das OSCI-Postfach übergeben wird. Dieser Posteingangszeitpunkt (Datum und Uhrzeit) wird für den Behördenempfänger in den Log-Files der VPS

protokolliert oder kann bei Bedarf mit Hilfe eines Zeitstempeldienstes quittiert werden.

Der Absender erhält ggf. eine Information via Client-Anwendung, dass seine Nachricht übermittelt wurde. Diese Mitteilung ist als eine unverbindliche Übergabequittierung anzusehen. Eine rechtsverbindliche Quittierung muss im VBS angestoßen werden. Mit einer vom VBS initiierten Eingangsbestätigung können VBS-relevante Referenznummern (wie z. B. Akten-, Vorgangskennzeichen) übergeben werden.

Die verarbeitungsrelevanten Protokoll- und Metadaten sind u. a auf dem Laufzettel der OSCI-Nachricht festgehalten. Auf dem Laufzettel stehen z. B. der Übermittlungszeitpunkt und das Ergebnis der Signaturüberprüfung. Die VPS „**protokolliert die Bearbeitung**“.

Ggf. kann die Nichtlesbarkeit der Signatur automatisch für den Empfänger attestiert werden. Die Nichtlesbarkeit des Inhalts wird von der VPS nicht geprüft. Dies muss bei der Sichtung oder vom Fachverfahren geprüft werden.

Nach dem Öffnen des 2. Umschlages stehen die Inhaltsdaten im Klartext zur Verfügung. Der Zugriff bleibt geschützt, da dieser innerhalb einer sicheren Intranetzone erfolgt und ausschließlich einem spezifischen Empfänger (OE oder Mitarbeiter) als designiertem Adressaten möglich ist.

Der Backend-Enabler stellt dem Hintergrundsystem die Daten als entschlüsselte OSCI-Nachricht und fortgeschriebenem Laufzettel (Bearbeitung und Prüfergebnisse) zur Verfügung. Die übermittelten Daten werden z. B. an ein Datenbank- oder Verzeichnissystem oder auf andere Weise dem VBS übergeben. Mit der „**Übergabe der erfassten Posteingangsobjekte**“ an das VBS enden die Aktivitäten der VPS in diesem Teilprozess.

Das VBS übernimmt die weitere Posteingangsbehandlung. Dies beginnt mit „**Posteingang übernehmen**“ und „**Ablegen des Posteingangs**“. Je nachdem, ob eine Organisationseinheit oder ein einzelner Mitarbeiter der Empfänger war, wurden VPS-Funktionen automatisch oder manuell abgerufen und die Übergabe der Daten initiiert.

Die OSCI-Nachricht liefert die Grundlage für die Datenübergabe vom VPS an das VBS. Das VBS erhält die entschlüsselte OSCI-Nachricht inklusive fortgeschriebenem Laufzettel.

In jeder OSCI Nachricht werden drei Sicherheitsebenen unterschieden: Administrationsebene, Auftragsebene, Geschäftsvorfallsebene. Auf der äußeren Administrationsebene befinden sich unverschlüsselte Daten. Diese Datenelemente steuern unmittelbar den Datenaustausch zwischen zwei direkt kommunizierenden OSCI Teilnehmern. Die Auftragsebene beinhaltet die so genannten Nutzdaten. Diese Daten sind durch den je-

weils sendenden Kommunikationspartner signiert (Signatur) und verschlüsselt (Verschlüsselungskopf). Mit diesen Nutzdaten kann eine Nachricht technisch an den Empfänger übermittelt werden. In der inneren Geschäftsvorfallebene befinden sich die signierten Inhaltsdaten eines konkreten Geschäftsvorfalles. Diese Daten sind Ende-zu-Ende verschlüsselt. Auch der Intermediär hat keine Möglichkeit, auf die Inhaltsdaten zuzugreifen.

Die nachfolgende Abbildung stellt den Aufbau einer OSCI-Nachricht dar.

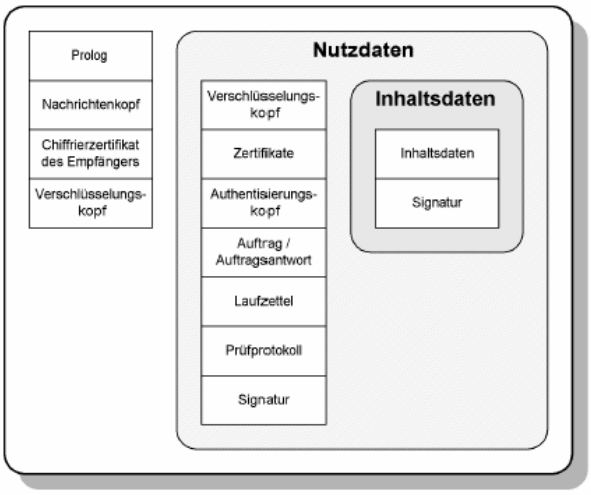

Abbildung 5: Aufbau einer OSCI-Nachricht[24]

Aus Sicht des VBS befinden sich in den Nutzdaten relevante Metadaten, wie z. B.:

- Signaturzertifikat des Absenders,
- Transaktionskennung (z. B. Betreff-Informationen, Kurzbeschreibung),
- Protokollierung von Zeitinformationen (z. B. Einreichung beim Intermediär; Weiterleitung an den Empfänger; ggf. Anforderung eines Zeitstempels),
- Protokollierungen von Prüfergebnissen (z. B. Zertifikatsprüfung)
- Zustellbedingungen (z. B. Zustellungstermin),
- Bearbeitungsstatus des Zustellungsauftrags (angenommen, in Bearbeitung, ausgeführt, zugestellt, fehlerhaft, unbekannt),
- Prioritäten.

Die relevanten Metadaten befinden sich u. a. auf dem Laufzettel. Der Laufzettel enthält alle für den Transport notwendigen Daten. Dieser wird (bei eingehenden Nachrichten) auf dem Client des externen Anwenders

[24] OSCI Leitstelle, OSCI: Die informelle Beschreibung, Eine Ergänzung zur OSCI Spezifikation November 2003.

erstellt und im weiteren Verlauf der Zustellung durch den Intermediär aktualisiert. Auf Abholaufträge antwortet der Intermediär mit den jeweils aktuellen Laufzetteln.[25] Die Verarbeitung der Zustellungsaufträge wird über den Laufzettel gesteuert. Er ist während der gesamten Verarbeitung durch den Intermediär die zentrale Datenstruktur und präzisiert die Zustellungsmodalitäten und die Inanspruchnahme seiner Mehrwertdienste. Der Laufzettel wird dem Empfänger ausgehändigt, eine Kopie verbleibt beim Intermediär.

Das VBS übernimmt alle Objekte der OSCI-Nachricht in seine Ablage.

Um relevante Metadaten ins VBS zu übernehmen wertet das VBS u. a. den Laufzettel aus. Das VBS führt die Aktion „**Posteingang erfassen**“ aus. Die Daten des Posteingangsobjekts (Original-, Inhalts-, Metadaten, Signatur, Prüfungsergebnisse etc.) inklusive einem Laufzettel der VPS liegen unverschlüsselt im VBS in verschiedenen Formaten vor. Das VBS muss XML-Objekte verarbeiten können.

Die OSCI-Nachricht kann entweder direkt als OSCI-Datenobjekt über den OSCI-Backend Enabler zur Verfügung gestellt werden, oder nach Entschlüsselung in Form von Inhalts- und Metadaten in ein Dateisystem oder eine Datenbank überführt werden. Welche Form und welches Format der Übergabe erfolgt, werden von den Anforderungen des VBS und dessen spezifische Integrationsvariante bestimmt.

Das Eingangsobjekt wird im VBS mit Metadaten erfasst:

- Die OSCI-Nachricht ist als Posteingangsobjekt zu erfassen. An diesem Objekt wird die korrekte Entschlüsselung und Signaturprüfung vermerkt (ja/nein). Falls „Nein“, endet die Erfassung.
- Die Inhaltsdaten (etwa Dokumente) eines Posteingangsobjekts sollten als einzelne Objekte erfasst werden können. Am Objekt Dokument sind die Metadaten „Posteingangsdatum“ und „Posteingangsuhrzeit“ ggf. aus dem Laufzettel der OSCI-Nachricht („Übermittlungsprotokoll“) zu übernehmen.
- Ggf. ist das Metadatenfeld „Zeitstempelzeitpunkt“ (Datum/Uhrzeit) als erweitertes Posteingangsdatum bzw. -uhrzeit zu setzen.
- Bei signierten Dokumenten ist am Objekt Dokument zu vermerken: „Niveau der Signatur“ (qualifiziert, fortgeschritten, einfach) sowie „Prüfergebnis erfolgreich“ (ja/nein).
- Die Signatur eines signierten Dokuments ist in den Metadaten zu vermerken (evtl. für Weiterleitung an andere Behörde, Nachprüfung, Übersignierung, Mehrfachsignieren).

[25] Vgl. OSCI Leitstelle, OSCI: Die informelle Beschreibung, Eine Ergänzung zur OSCI Spezifikation November 2003

- Zu jedem Dokument ist der Laufzettel in die Protokollinformationen zum Objekt Dokument zu übernehmen (Bearbeitungsprotokoll einfach einsehbar).
- Die Übernahme von Metadaten (Fremdaktenzeichen etc.) aus den Betreff-Informationen ist möglich (etwa für die Postverteilungslogik).

Der Papierausdruck von elektronisch signierten Dokumenten ist bei Bedarf notwendig.[26] Der Ausdruck muss für die geleistete gültige Signatur (Ergebnis der Signaturprüfung) den Vermerk enthalten:

- Inhaber der Signatur,
- Zeitpunkt der Signaturprüfung,
- welche Zertifikate mit welchen Daten dieser Signatur zugrunde lagen.

Ist ein Posteingang erfasst, erfolgen die Schritte „**Posteingang registrieren**“ und „**Inhaltliche Prüfung**“. Im VBS erhalten die Posteingänge ein neues Aktenkennzeichen oder sie können einem bestehenden Akten- / Vorgangskennzeichen zugeordnet werden. Im Anschluss an eine inhaltliche Sichtung der übermittelten Dokumente und Daten, kann eine rechtsverbindliche Eingangsbestätigung generiert und über die VPS verschickt werden: „**Posteingang bestätigen**“. Die Eingangsbestätigung geht zur Akte bzw. zum Vorgang. Falls die übermittelten Dokumente nicht zu öffnen sind, muss der Absender darüber informiert werden.

Das VBS leitet ggf. abschließend die Übergabe strukturierter Daten an ein Fachverfahren ein.[27] Die Verteillogik erfolgt gemäß der erfassten Metadaten bzw. gemäß den übergebenen Metadaten der OSCI-Nachricht.

5.2 Behörde empfängt Daten – Posteingang E-Mail

Die nachfolgende Abbildung 6 stellt in einem Flussdiagramm den Teilprozess „Behörde empfängt Daten – Posteingang E-Mail“ dar.

Für den Teilprozess „Behörde empfängt Daten“ können der VPS Regeln zur Behandlung des Posteingangs vorgeben werden. Gemäß diesen Regeln wird die VPS aktiv.

Die VPS übernimmt in diesem Teilprozess die Aufgabe, kryptographisch behandelte E-Mails zu filtern und als „**Posteingang anzunehmen**“. Alle anderen E-Mails werden von ihr unbehandelt weiter geleitet.

[26] Siehe etwa den Referentenentwurf Justizkommunikationsgesetz, JKomG § 298(2): Aktenausdruck.

[27] Siehe Erweiterungsmodul „Fachverfahrensintegration“, Schriftenreihe der KBSt, Band 63.

Die VPS erfüllt im Anschluss die Aufgabe den „**Posteingang prüfen**“. Hierbei werden auf Anforderung folgende Dienste erledigt:

- Entschlüsseln
- Posteingangszeitpunkt intern protokollieren
- Integrität und Authentizität prüfen
- Metadaten protokollieren

Bei Bedarf wird zunächst eine Entschlüsselung der Daten durchgeführt. Hierfür benötigt die VPS die privaten Entschlüsselungsschlüssel der Organisationseinheit oder des einzelnen Mitarbeiters einer Behörde. Die VPS greift dazu auf ein entsprechendes VPS-internes Verzeichnis, einen geeigneten Verzeichnisdienst oder einen Schlüsseldatenträger (z. B. Chipkarte) zu.

Ein Posteingang gilt als zugestellt, wenn die E-Mail dem Mailsystem der Behörde übergeben wird. Dies kann ein bestehender zentraler oder dezentraler Mailservereingang der Behörde sein. Dieser Posteingangszeitpunkt (Datum und Uhrzeit) wird für den Behördenempfänger von den nachgelagerten Systemen der VPS (z.B. eines Vorgangsbearbeitungssystems) übernommen und protokolliert. Bei höherem Sicherheitsbedarf kann der Posteingangszeitpunkt mit Hilfe eines Zeitstempeldienstes der VPS protokolliert werden. Über die Mail-Anwendung können Prüfinformationen an das VBS übermittelt werden.

Die VPS erzeugt bei E-Mail-Eingang keine automatische Eingangsquittung (Rückschein) für den Absender. Fordert der Sender eine Eingangsquittung ein, dann kann die nachgelagerte Mail-Anwendung oder das VBS auf der Basis der Prüfinformationen der VPS eine entsprechende elektronische Quittung erzeugen.

Die nachgelagerte Mail-Anwendung oder das VBS können anhand der Prüfinformationen auch Benachrichtigungen an den Absender erstellen, wenn Fehlerzustände oder Virenbefall die weitere Bearbeitung nicht zulassen. Die generierten Nachrichten der Mail-Anwendung sind der VPS zu übergeben.

Die VPS prüft die Struktur der E-Mail und der kryptographisch behandelten Anhänge. Sie prüft nicht den Inhalt und die Struktur der Dokumente. Eine VS-Einstufung kann nicht geprüft werden. Nichtlesbare Formate der Inhaltsdaten werden nicht entdeckt.

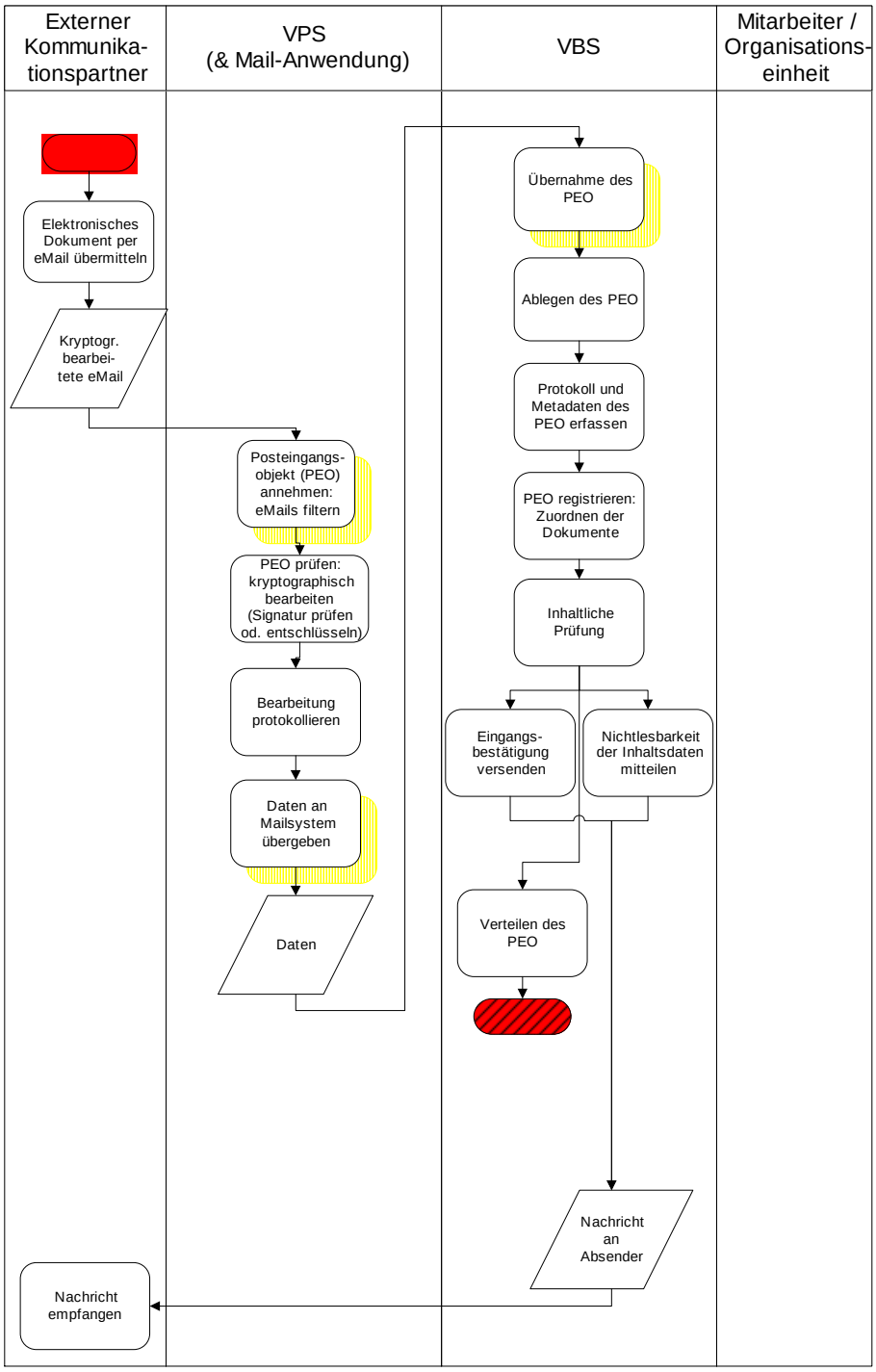

Abbildung 6: Behörde empfängt Daten: Posteingang E-Mail

Die Prüfergebnisse und weitere Metadaten werden protokolliert und der E-Mail hinzugefügt. Die verschlüsselte Originalnachricht wurde aufgelöst in Inhaltsdaten sowie Metadaten mit Laufzettel und Prüfungsergebnissen.

Die VPS stellt über eine entsprechende Schnittstelle die E-Mail zusammen mit den neuen Metadaten in das Mail-Postfach des Empfängers (OE/Mitarbeiter) oder des VBS ein.

Die Aufgabe „**Bearbeitung protokollieren**“ endet mit der Übergabe der Daten.

Mit der „**Übergabe der Posteingangsobjekte**“ an das Mailsystem enden die Aktivitäten der VPS in diesem Teilprozess.

Das VBS übernimmt die weitere Posteingangsbehandlung. Um die Aufgabe „**Posteingang übernehmen**“ zu erledigen, muss das VBS die Posteingangsdaten importieren. VBS-Systeme verfügen hierfür in der Regel über Standard-Importmechanismen (Schnittstelle zu Mailserver).

Das VBS importiert das entschlüsselte Posteingangsobjekt. Dieses beinhaltet im Wesentlichen die Original-Mail im Klartext ohne Signatur als Datenmengen in unterschiedlichen Formaten:

- Inhaltsdaten (z. B. Nachrichtentext, Dateianhänge, XML-Antragsdaten),
- Laufzettel inklusive Metadaten und Prüfungsergebnisse,
- Ggf. generierte Nachrichten der Mail-Anwendung,
- Optional kann von der VPS zusätzlich eine Kopie der (unbearbeiteten) Originalnachricht im S/MIME-Format an das VBS übergeben werden, um die Signatur zu erhalten.

Da die Signatur zur übermittelten E-Mail bei der Prüfung „aufgelöst“ und entfernt wird, kann je nach zugrunde liegendem Verfahren die Speicherung einer Kopie der Originalnachricht im VBS erforderlich werden. Ggf. kann die Originalnachricht und Signatur an ein Archiv weitergegeben werden und separat gespeichert werden. Der Posteingang wird im VBS abgelegt: „**Ablegen von Posteingangsobjekt**“.

Das VBS wertet u. a den Laufzettel in dem nächsten Schritt „**Posteingang erfassen**“ aus. Die Metadaten liegen als Anhang in der E-Mail. Der Importmechanismus muss dessen Struktur prüfen und analysieren. Die aktenrelevanten Daten der Originalnachricht werden im VBS mit Metadaten erfasst:

- Die unbearbeitete Originalnachricht ist ggf. als Posteingangsobjekt zu erfassen (Nachweis der gekapselten Elemente). Am Objekt wird vermerkt, ob die Entschlüsselung und Signaturprüfung erfolgreich verlaufen ist (ja/nein).
- Die enthaltenen verschlüsselten Inhaltsdaten (bzw. Dokumente, XML-Antragsdaten) eines Posteingangsobjekts sind als einzelne Objekte zu erfassen. Am Objekt Dokument sind die Metadaten „Posteingangsdatum“ und „Posteingangsuhrzeit“ zu ergänzen.
- Ggf. ist das Metadatenfeld „Zeitstempelzeitpunkt“ (Datum/Uhrzeit) als erweitertes Posteingangsdatum bzw. -uhrzeit zu setzen.
- Erfolgreiche oder fehlgeschlagene Signaturprüfungen von Dokumenten sind am Objekt zu dokumentieren: „Niveau der Signatur“ (qualifi-

ziert, fortgeschritten, einfach, keine); „2. Prüfergebnis erfolgreich“ (ja/nein).

- Der Laufzettel ist in die Protokollinformationen des Posteingangsobjekts (Kopie der Originalnachricht) zu vermerken.
- Die Übernahme von Metadaten zum Nachrichtentext (Signaturniveau eines Dokumentanhangs etc.) ist bei geeigneter Auswertung möglich.

Der Papierausdruck eines signierten Dokuments einschließlich der Ergebnisse der Signaturprüfung ist möglich.

Ist ein Posteingang erfasst, erfolgen die Schritte „**Posteingang registrieren**“ und „**Inhaltliche Prüfung**“. Im VBS erhalten die Posteingänge ein neues Aktenkennzeichen oder sie werden einem bestehenden Akten- / Vorgangskennzeichen zugeordnet. Im Anschluss an eine inhaltliche Sichtung der übermittelten Dokumente und Daten kann im VBS eine Eingangsbestätigung generiert und über die VPS verschickt werden: „**Posteingang bestätigen**“. Die Eingangsbestätigung geht zur Akte bzw. zum Vorgang. Falls die übermittelten Dokumente nicht zu öffnen sind bzw. die Signaturprüfung fehlgeschlagen ist, muss der Absender darüber informiert werden.

Ggf. werden vertrauliche Dokumente mit Hilfe der VPS nachträglich mit einem Behördenschlüssel verschlüsselt (vgl. Kap. 5.4).

Das VBS leitet ggf. abschließend die Übergabe strukturierter Daten an ein Fachverfahren ein.[28] Die Verteillogik erfolgt gemäß der erfassten Metadaten bzw. gemäß den übergebenen Metadaten der E-Mail-Nachricht.

5.3 Ad hoc- und Wiederholungsprüfung

In den beiden Teilprozessen „Ad hoc Prüfung“ und „Wiederholungsprüfung“ zur Verifikation von Signaturen und Zertifikaten ruft ein Mitarbeiter einer Behörde aus dem VBS heraus die Dienste der VPS auf. Die nachfolgende Abbildung 7 stellt in einem Flussdiagramm das Grundschema beider Teilprozesse dar.

Der „**Aufruf von VPS Funktionen**“ erfolgt aus dem VBS heraus. Ein Benutzer übergibt ein ausgewähltes Objekt mit Hilfe eines entsprechenden Interface an die VPS. Dies kann z. B. ein signiertes oder verschlüsseltes Dokument oder die signierte oder verschlüsselte Kopie einer Original-E-Mail-Nachricht sein.

[28] Siehe Erweiterungsmodul „Fachverfahrensintegration“, Schriftenreihe der KBSt, Band 63.

Nachdem die VPS die Objekte erhalten hat, erfolgt die kryptographische Bearbeitung. Die VPS übernimmt die Aufgaben „**Objekt prüfen**“ und „**Bearbeitung protokollieren**“. Hierbei können folgende Dienste erledigt werden:

- Entschlüsseln (Behörden- / Mitarbeiterschlüssel),
- Signaturen prüfen (Prüfung auf Signaturzeitpunkt, Mathematische Prüfung),
- Zeitpunkt quittieren (Zeitstempel anfordern),
- Integrität und Authentizität prüfen (Herkunftsnachweis),
- Prüfungsergebnisse und eventuelle Fehler bei der kryptographischen Bearbeitung dokumentieren.

Jede signierte Version ist nachträglich einzeln prüfbar.[29] Dabei existieren auch für die Prüfbarkeit Unterschiede: Bei Parallelsignaturen gilt jede Signatur als Originalsignatur – jede Signatur ist für sich zu prüfen. Bei Übersignaturen im Sinne einer Nachhaltigkeitssicherung (z. B. Zeitstempelsignatur) müssen erst die Übersignaturen geprüft werden, um die Originalsignatur prüfen zu können. Die Prüfung der Originalsignatur auf Gültigkeit erfolgt über mehrere Schritte. Zunächst erfolgt die Prüfung der letzten aktuellen Übersignatur und des Zeitstempel (bei Nachhaltigkeitssicherung). Danach werden alle Übersignaturen in zeitlich absteigender Reihenfolge geprüft. Die Gültigkeitsprüfung einer Originalsignatur erfolgt nach der Gültigkeitsprüfung aller Übersignaturen.

Die VPS übergibt als Ergebnis des Funktionsaufrufes die Prüfergebnisse an das VBS zurück: „**Erweitertes Objekt übergeben**“. Abschließend erfolgt die Aufgabe des VBS das erweiterte „**Objekt übernehmen**“. Im VBS werden die erweiterten Protokoll- und Metadaten am „**Objekt erfasst und abgelegt**“.

Das wiederholt geprüfte Objekt wird mit Metadaten erfasst, wie z. B.:

- Die Signatur eines Dokuments ist in den Metadaten zu vermerken,
- Bei signierten Dokumenten ist am Objekt Dokument zu vermerken: „Niveau der Signatur“ (qualifiziert, fortgeschritten, einfach) sowie „Prüfergebnis erfolgreich“ (ja/nein). Metadaten sind historisierend zu führen,
- Der Laufzettel ist zu den Protokollinformationen zum Objekt Dokument hinzuzufügen,

Das erweiterte Objekt wird im VBS ggf. als ein neues Objekt oder als neue Version abgelegt.

[29] Zu XML-Signaturen siehe KBSt, SAGA, Standards und Architekturen für E-Government-Anwendungen, Version 2.0, Band 59, Dezember 2003, Kapitel 9.3.3 Gesicherter Dokumentenaustausch, S. 107. Für die Platzierung von Signaturen bestehen drei Möglichkeiten: Einbettung, Umschlag oder Unabhängigkeit.

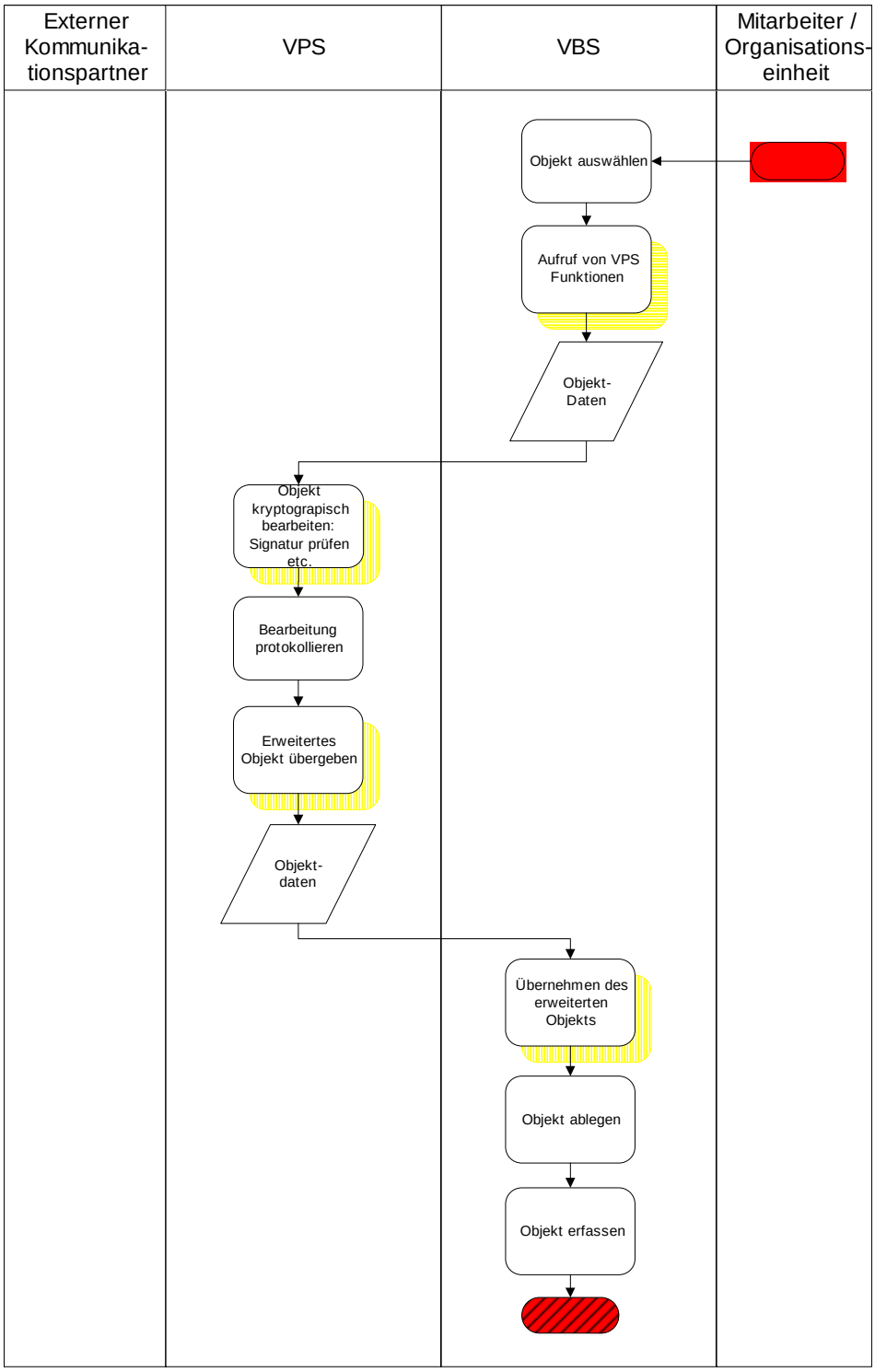

Abbildung 7: Ad hoc- und Wiederholungsprüfung

5.4 Bearbeitung von Prozess- und Inhaltsdaten

Im Teilprozess kryptographische „Bearbeitung von Prozess- und Inhaltsdaten“ lässt ein Behördenmitarbeiter ein Dokument direkt aus dem VBS

heraus bearbeiten. Die nachfolgende Abbildung 8 stellt in einem Flussdiagramm den Teilprozess dar.

Der Initiator erstellt im VBS ein Dokument und erfasst dessen Metadaten: „**Objekt erstellen**“. Aus dem VBS heraus können spezifische „**VPS Funktionen aufgerufen**“ werden. Das VBS formatiert das Objekt in ein von der VPS unterstütztes Format, übergibt das zu bearbeitende Objekt und bestimmt die durchzuführenden kryptographischen Operationen. Die Bearbeitung kann Inhalts- sowie Prozessdaten einbeziehen.

Nachdem die VPS die Objekte erhalten hat, folgt die Aufgabe „**Objekt bearbeiten**“. Hierbei werden ggf. folgende Dienste erledigt:

- Signieren,
- Verschlüsseln, falls Versand vorgesehen,
- Zeitstempel anbringen (Signaturzeitpunkt = Versanddatum/-zeit).

Die VPS protokolliert die Bearbeitung: „**Bearbeitung protokollieren**“.

Nachdem das Objekt innerhalb der VPS bearbeitet wurde, erfolgt die Übergabe zurück an das VBS. Bei der Aktion „**Objekt übergeben**“ übergibt die VPS das kryptographisch bearbeitete Objekt dem VBS und ggf. zusätzliche Metainformationen. Mit der Übergabe des erweiterten Objekts, folgen die Schritte „**Objekt ablegen**“ und „**Objekt erfassen**“.

Das Objekt Dokument ist mit zusätzlichen Metadaten zu erfassen:

- Das Dokument ist als ein neues Objekt oder als eine neue Version anzulegen,
- Signierte Dokumente müssen mit Signatur oder als Signierte Dokumente ohne Signatur mit Referenz auf die Signatur abgespeichert werden,
- Relevante Prüfinformationen des Laufzettels sind als Metadatum abzuspeichern,
- Bei signierten Dokumenten ist am Objekt Dokument zu vermerken: „Niveau der Signatur“ (qualifiziert, fortgeschritten, einfach, keine),
- Der Laufzettel ist in die Protokollinformationen zum Objekt Dokument zu übernommen.

Ein mittels VPS bearbeitetes Objekt kann zu einem späteren Zeitpunkt per E-Mail versandt werden. Zum Versand per E-Mail siehe Kapitel 5.7.

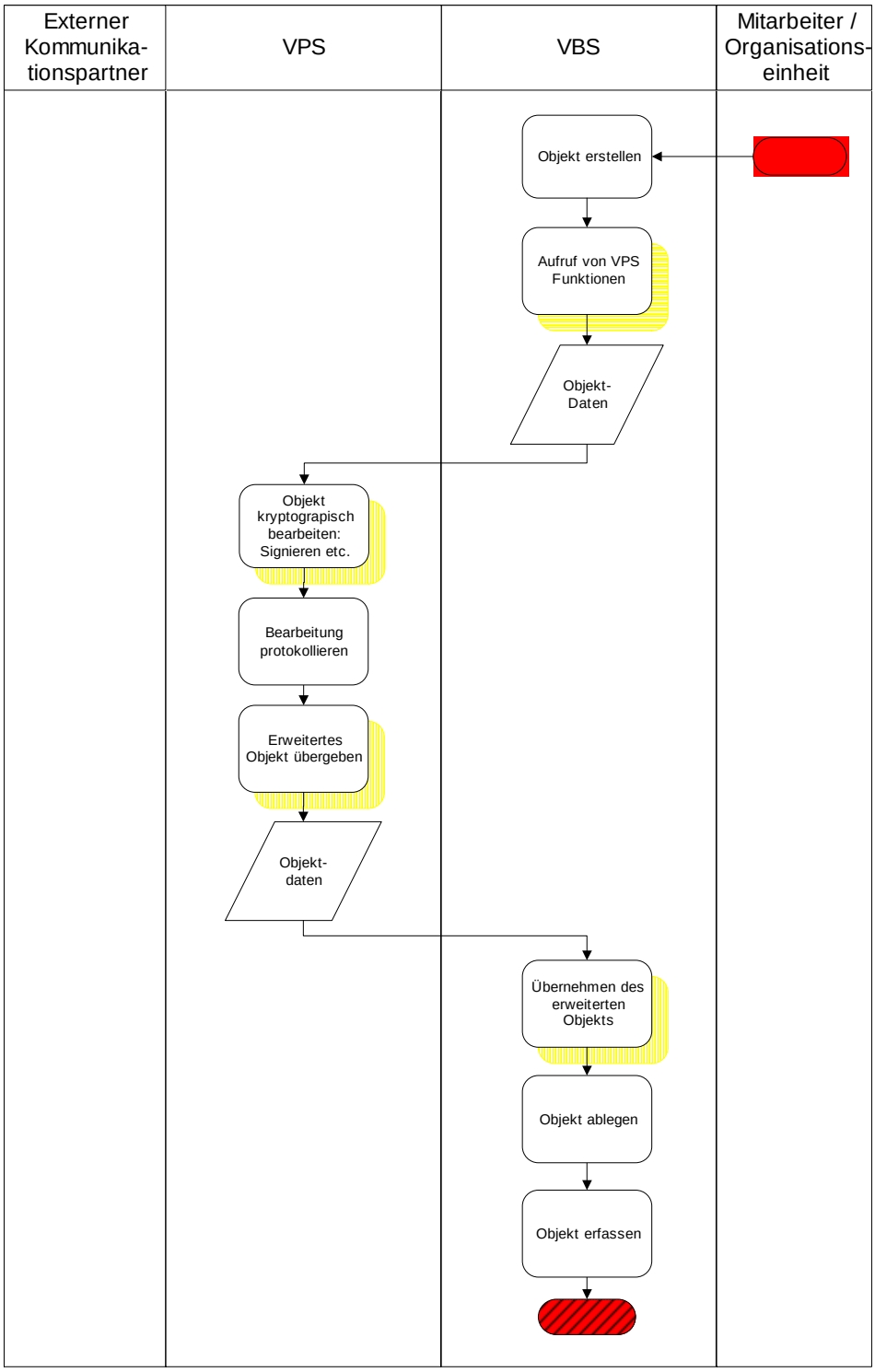

Abbildung 8: Bearbeitung von Prozess- und Inhaltsdaten

5.5 Zeichnungslauf

Ein DOMEA®-Konzept konformes Vorgangsbearbeitungssystem bietet ausreichend Funktionen, um einen gängigen Mit- und Schlusszeich-

nungslauf durchzuführen. Die VPS bietet für bestimmte Anlässe mit erhöhten Sicherheitsanforderungen ergänzende Dienste: Etwa wenn ein bindendes Zeichnungsverfahren mit qualifizierter Signatur eingesetzt werden soll. Ein solcher Zeichnungslauf stellt eine Ausnahme dar.

Im Teilprozess „Zeichnungslauf“ ruft ein Mitarbeiter einer Behörde die VPS über das Vorgangsbearbeitungssystem auf. Die nachfolgende Abbildung 9 stellt in einem Flussdiagramm den Teilprozess dar.

Der Initiator verfügt ein Dokument zum Mitzeichnen und leitet das Zeichnungsverfahren im VBS ein: „**Objekt zum Zeichnen weiterleiten**“. Der Mitzeichnende bzw. Empfänger ruft das Objekt auf. Dieser hat im VBS die Wahl, die Vorlage abzulehnen, zu zeichnen, unter Vorbehalt zu zeichnen oder der Empfänger sieht sich nicht zuständig.

Mit der Entscheidung zur Mitzeichnung, übergibt das VBS das Dokument an die VPS und setzt einen Funktionsaufruf ab: „**Aufruf von VPS Funktionen**“. Die VPS übernimmt die Aufgabe „**Dokument kryptographisch bearbeiten**“. Gemeint ist lediglich die personenbezogene manuelle Einzel- und Mehrfachsignatur und nicht die automatisch gesteuerte Massensignatur. Folgende Funktionen müssen dabei zuvor vom VBS bei Bedarf zur Verfügung gestellt werden:

- der zu verantwortende Textausschnitt muss auszuwählen sein und vom VBS extrahiert werden,
- Damit die Datei im korrekten Zustand signiert wird, ist sicherzustellen, dass versteckte Informationen vor dem Signieren grafisch sichtbar sind (z. B. Darstellungskomponente erstellt TIFF Datei),
- Zusätzlich zur nicht veränderbaren TIFF-Datei kann diese mit einer veränderbaren Datei zur Weiterbearbeitung eindeutig verbunden werden,
- Aufruffunktion zum signieren.

Die VPS zeichnet die Bearbeitung auf: „**Bearbeitung protokollieren**“. Nach erfolgter Signatur führt die VPS die Aufgabe „**Objekt übergeben**“ aus. Die VPS übergibt das signierte Dokument dem VBS.

Mögliche Zeichnungsvorbehalte sind im VBS zu verfassen und zum Dokument zu vermerken.

Mit der Übernahme des erweiterten Objekts, folgt der Schritt „**Objekt erfassen**“. Im VBS ist das signierte Dokument als neue Version mit Meta- und Protokolldaten zu erfassen:

- Objekt ist als neue Version anzulegen.
- Mindestens die folgenden Metadaten sind am Objekt Dokument zu führen: „Dokumentausschnitt“, „signiert, von Mitarbeiter“, „Datum“ und „Signaturniveau“.

- Laufzettel ist dem Vorgangsprotokoll zu übergeben (Bestätigung der VPS Bearbeitung).
- Am Objekt Vorgang ist in den Bearbeitungsprotokollen die Einbindung der VPS und ggf. das Signierniveau zu vermerken.

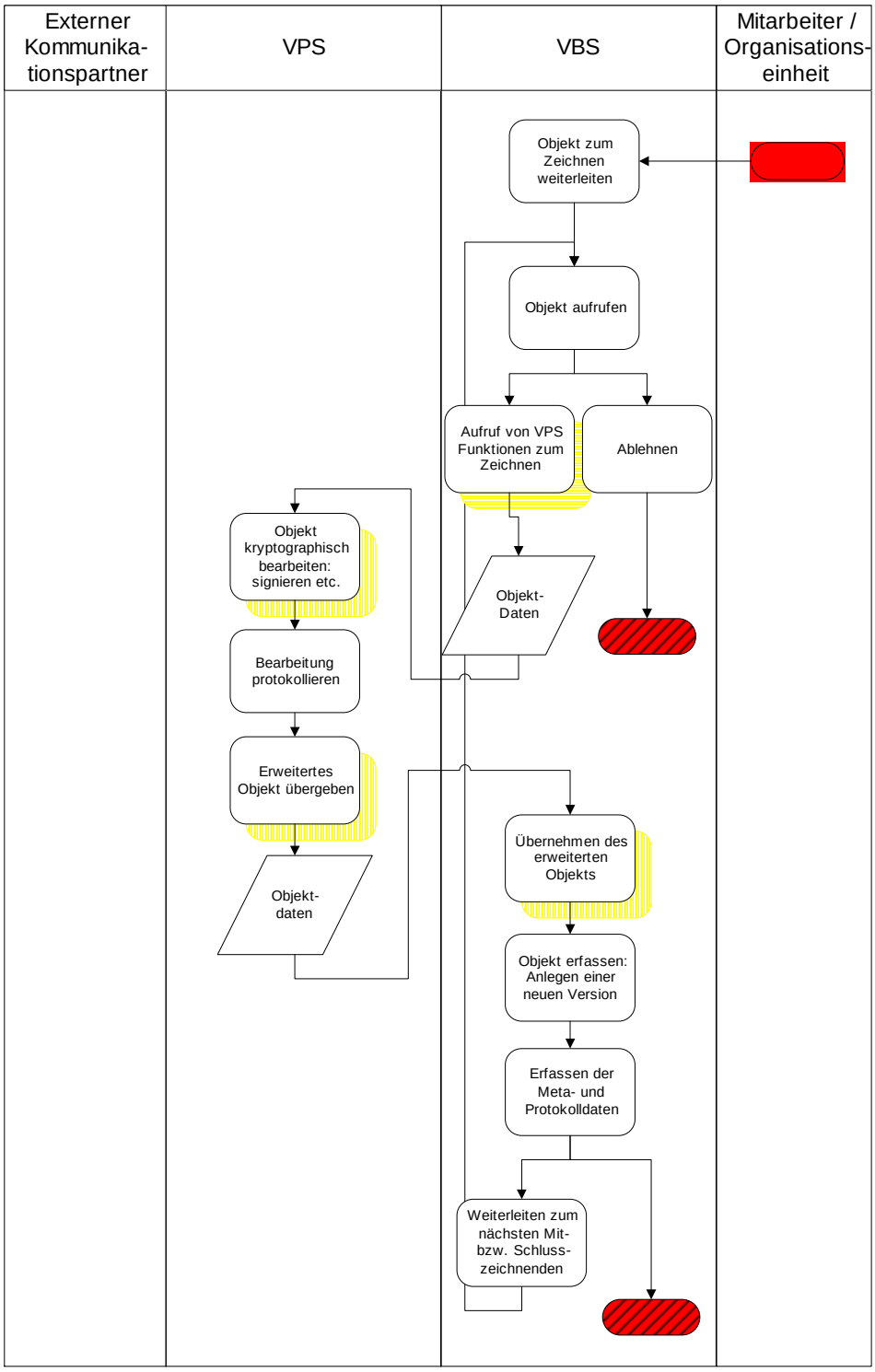

Abbildung 9: Zeichnungslauf

Gemäß vordefiniertem Zeichnungslaufweg sind mehrere Signaturen als Einzelsignaturen auf einem Dokument anzubringen. Im VBS erfolgt das „**Weiterleiten an den nächsten Mit- oder Schlusszeichnenden**“. Das VBS muss hierfür ein Regelwerk zur Verfügung stellen, um für den jeweiligen Vorgang zu bestimmen, ob ein Dokument parallel (z. B. Mitzeichnung) oder in Reihenfolge (z. B. Schlusszeichnung) gezeichnet wird. Das VBS regelt dabei, wer das Dokument zu welchem Zeitpunkt oder in welchem Zustand zeichnen soll und übergibt die Dokumentenversionen in geeigneter Weise an die VPS. Ggf. klammert die Signatur des Schlusszeichnenden die vorausgehend gesetzten Mitzeichnungen.

Jede signierte Version ist nachträglich einzeln prüfbar (siehe vorausgehendes Beispielszenario).

Für die Abgabe eines mehrfach signierten Dokuments an ein Archiv bzw. Langzeitarchiv können die Signaturen separat zum Dokument abgespeichert werden. Die Bezüge zu den Signaturen und Dokumenten müssen erhalten bleiben.

5.6 Behörde sendet Daten – Postausgang Web

Die nachfolgende Abbildung 10 stellt in einem Flussdiagramm den Teilprozess „Behörde sendet Daten – Postausgang Web“ dar.

Die zu versendenden Daten bzw. Dokumente werden im VBS erstellt: „**Postausgangsobjekt erstellen**“. Der „**Postausgang per Web**“ wird initiiert, indem die VPS aus dem VBS heraus aufgerufen wird. Die Vorgangsbearbeitung gibt der VPS vor, welches Signaturniveau wann notwendig ist, und welche zusätzlichen Dokumente als bereits signierte Anhänge beigefügt werden müssen. Ein elektronisches Dokument (z. B. Verwaltungsakt) zuzüglich seiner Anhänge wird zum Versenden an die VPS übergeben. Hierfür stehen zusätzliche, bereits signierte Dokumente, versandfertig auf Abruf (z. B. Rechtsbehelfsbelehrung, AGB etc.) zur Verfügung. Im Bedarfsfall – je nach zugrunde liegendem Schutzbedarf – muss das VBS geeignete Mechanismen zur Verfügung stellen, um zu gewährleisten, dass erkennbar ist, welche Dateninhalte signiert werden.

Für die übergebenen Daten und Dokumente sind im VBS die „**Postausgangsdaten zu erfassen**“. Die Metadaten beziehen sich auf das Ursprungsdokument. Das signierte Dokument geht nach außen. Ggf. ist der Laufzettel einer OSCI-Nachricht mit den Protokollinformationen von der VPS anzufordern und auszuwerten. Der Absender kann ggf. eine Kopie des Postausgangs an sich selbst schicken, um z. B. das signierte Dokument ebenfalls zur Akte verfügen zu können.

Mit dem „**Aufruf von VPS Funktionen**“ werden die Dokumente und Daten vom VBS an die VPS übergeben.

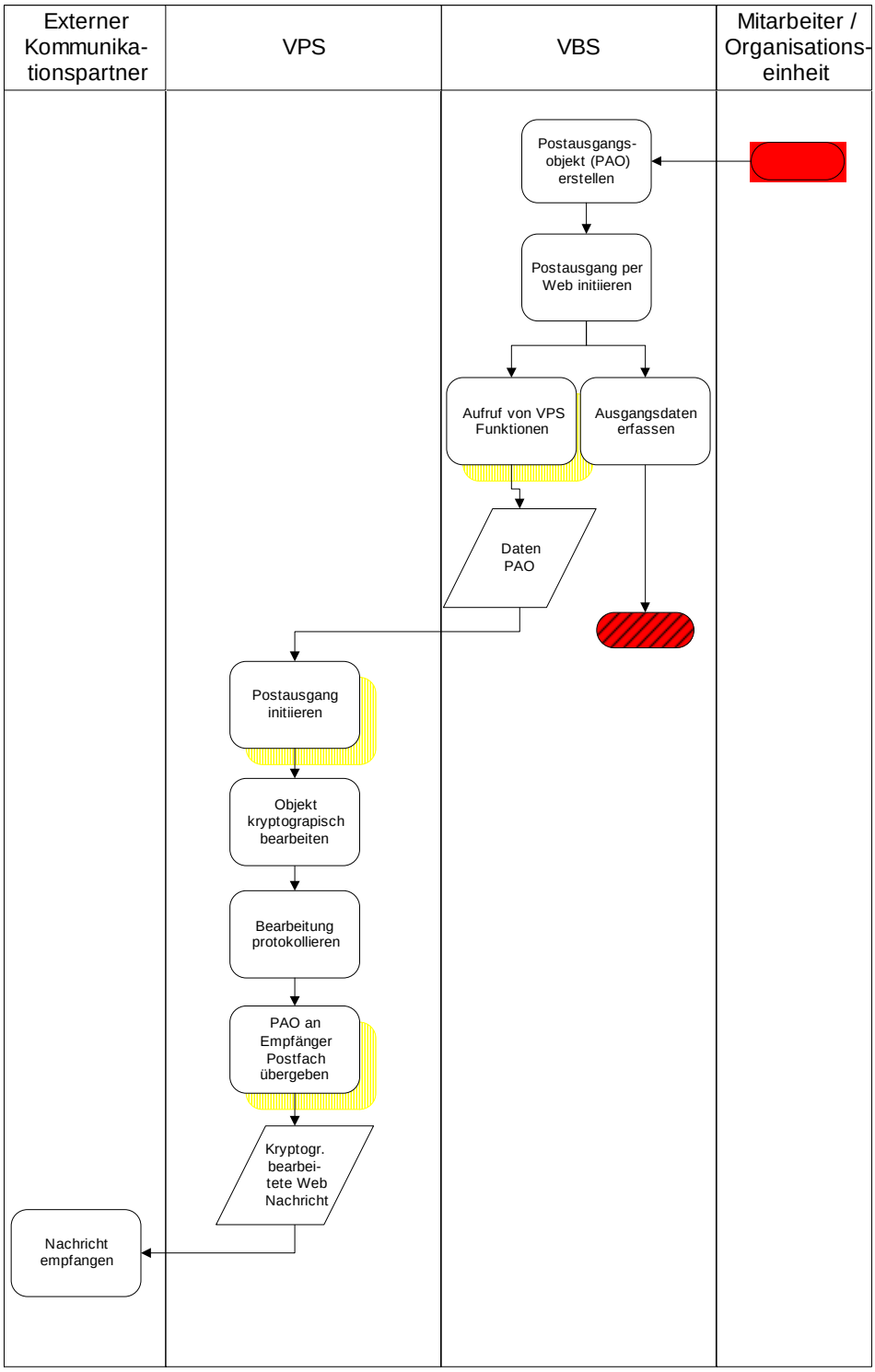

Abbildung 10: Behörde sendet Daten: Postausgang Web

Nachdem die Daten an die VPS übergeben wurden, übernimmt die VPS die Aufgabe „**Postausgang initiieren**“ und „**Objekt kryptographisch bearbeiten**“.

Hierbei werden ggf. folgende Dienste erledigt:

- Empfängername im Adressverzeichnis suchen,
- Signieren,
- Zeitstempel anbringen (Versanddatum),
- Verschlüsseln,
- Optional automatische Quittierung.

Mit dem öffentlichen Verschlüsselungsschlüssel des Empfängers wird die Nachricht verschlüsselt und ist somit nur für den Empfänger lesbar.

Je nach abverlangtem Schutzbedarf ist das Signaturniveau zu wählen. Die VPS verfügt über die notwendigen privaten Signaturschlüssel und kann damit entweder fortgeschrittene oder qualifizierte Signaturen erstellen.

Um eine Anfrage für einen Zeitstempel zu bedienen, kann die VPS einen externen Zeitstempeldienstanbieter unterstützen. Dieser Einsatz wie auch alle anderen Aktivitäten der VPS werden protokolliert: „**Bearbeitung protokollieren**“.

Nachdem die Funktionen durchlaufen sind, erfolgt die Übergabe. Bei der Aktion „**Postausgang übergeben**“ stellt die VPS das Postausgangobjekt in das Postfach des Empfängers ein. Der Teilprozess „Behörde sendet Daten – Postausgang Web“ ist abgeschlossen.

5.7 Behörde sendet Daten – Postausgang E-Mail

Die folgende Abbildung 11 stellt in einem Flussdiagramm den Teilprozess „Behörde sendet Daten – Postausgang E-Mail“ dar.

Die zu versendenden Daten bzw. Dokumente werden im VBS erstellt: „**Postausgangsobjekt erstellen**“.

Um einen „**Postausgang per E-Mail zu initiieren**“ wird das Mailsystem aus dem VBS heraus aufgerufen. Die Dokumente und Daten werden in Form einer E-Mail an das Mailsystem übergeben. Standardmäßig werden Primär- und keine Bearbeitungsinformationen übergeben. Als Metadaten wird mindestens der Betreff, das Akten- bzw. Vorgangskennzeichen der E-Mail-Nachricht als dem Postausgangsobjekt mitgegeben, ggf. können zusätzliche XML-Strukturen angehängt werden.

Die VPS greift auf Grundlage von Postausgangsregeln ein, um ausgehende E-Mails kryptographisch zu behandeln. Der VPS kann vorgeben werden, welche kryptographischen Operationen auf welchem Niveau wann notwendig sind. Derartige Regeln können sich beispielsweise an dem Empfänger oder Absender ausrichten.

Für die übergebenen Daten und Dokumente sind im VBS die „**Postausgangsdaten zu erfassen**“. Die Metadaten beziehen sich auf das Ursprungsdokument. Das signierte und/oder verschlüsselte Dokument geht nach außen. Ggf. ist ein Bearbeitungsprotokoll von der VPS anzufordern und auszuwerten. Der Absender kann ggf. eine Blindkopie des Postausgangs an sich selbst schicken, um z. B. das signierte Dokument ebenfalls zur Akte verfügen zu können.

Um eine Zustellbestätigung zu erhalten, muss der Empfänger aufgefordert werden, den Eingang zu quittieren. Alternativ kann das VBS vom Mailserver eine Bestätigung nach Abgang einholen, falls das Mailsystem diese Funktionalität unterstützt. Der Zustellzeitpunkt ist in den Metadaten der versendeten Objekte zu vermerken.

Das VBS ermöglicht die Übergabe der Daten an das Mailsystem und damit an die VPS: „**Aufruf von VPS Funktionen**“. Eine E-Mail inklusive ihrer Anhänge wird zum Bearbeiten an die VPS übergeben. Je nach Regelung können zusätzliche, bereits signierte Dokumente automatisch angehängt werden (z. B. Rechtsbehelfsbelehrung, AGB etc.).

Nachdem die Daten an das Mailsystem und gemäß einer Regel weiter an die VPS übergeben wurden, löst diese bei der VPS die Aufgabe „**Postausgang initiieren**“ und „**Objekt kryptographisch bearbeiten**“ aus. Hierbei werden auf Anforderung folgende Dienste erledigt:

- Signieren,
- Verschlüsseln,
- Optional (ggf. Qualifizierten) Zeitstempel anbringen (Signaturzeitpunkt = Versanddatum/-zeit),
- Ggf. Fehlermeldung im Mailsystem.

Der Signier- und Verschlüsselungsprozess verläuft in der VPS gemäß einem hinterlegten Postausgangsregelwerk. Dieses legt die Art und den Umfang der kryptographischen Behandlung der E-Mail fest. Die E-Mail und ihre Inhalte werden signiert bzw. verschlüsselt und in eine S/MIME-Nachricht transformiert. Bereits signierte und/oder verschlüsselte Anhänge werden im Rahmen der S/MIME-Nachricht erneut signiert und/oder verschlüsselt.

Die notwendigen Verschlüsselungsschlüssel (öffentlicher Schlüssel des Empfängers) sind mit der Mailadresse in einem internen Verzeichnis hinterlegt oder können über einen geeigneten Verzeichnisdienst abgerufen werden.

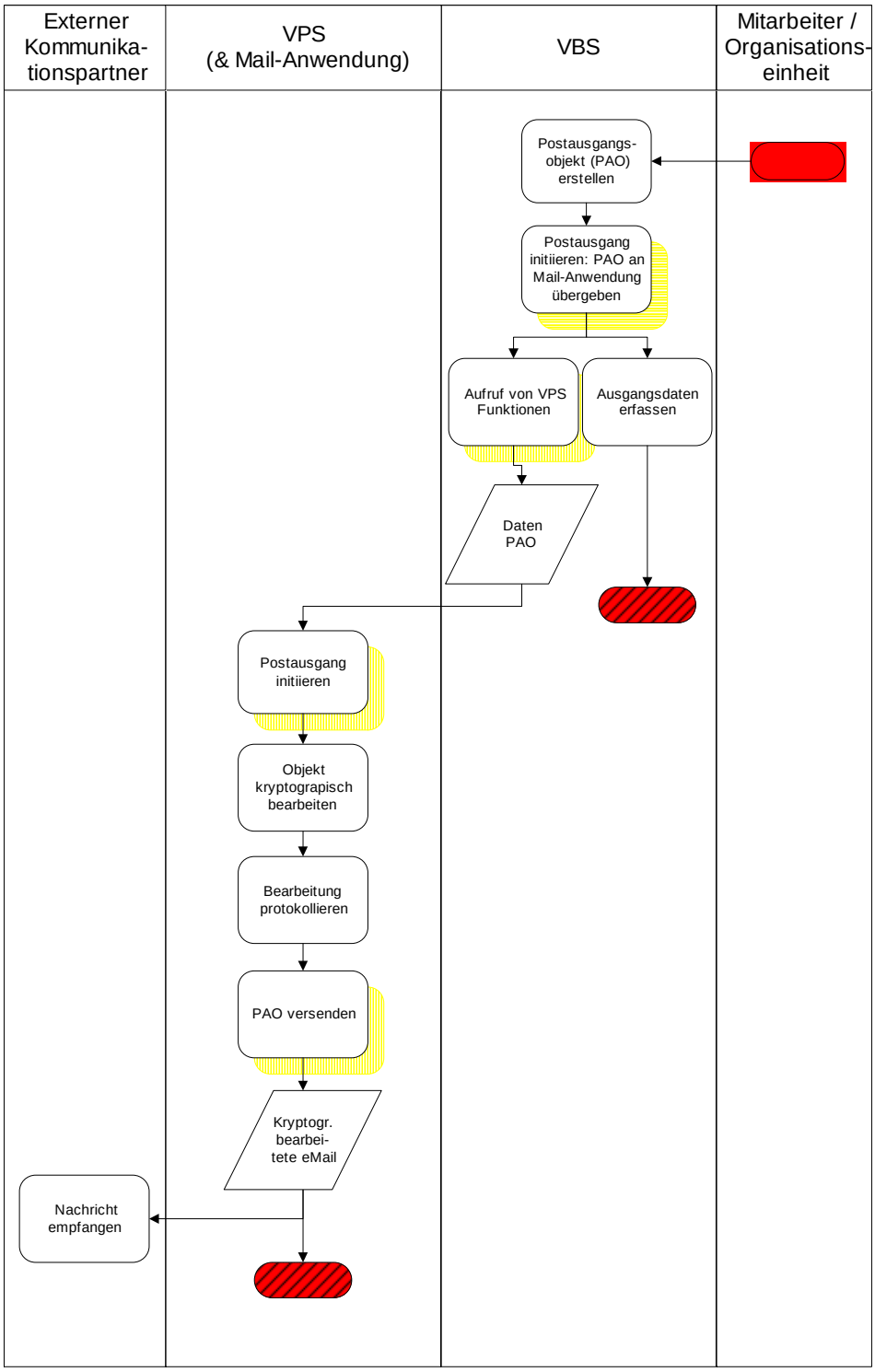

Abbildung 11: Behörde sendet Daten: Postausgang E-Mail

Alle Aktivitäten der VPS werden protokolliert: „**Bearbeitung protokollieren**“.

Nachdem die Funktionen durchlaufen sind, erfolgt die Übergabe: „**Postausgang versenden**“. Die VPS liefert die bearbeitete E-Mail-Nach-

richt bei den nachgelagerten Mailsystemen (z. B. behördeninternes Mail-Relay, IVBB-Mail-Relay) ab. Die VPS erstellt keine automatisierte Ausgangsquittung für das VBS.

Der Teilprozess „Behörde sendet Daten – Postausgang E-Mail“ ist abgeschlossen.