

# Anbindung der ePayBL an ein Fachverfahren



## Inhalt

<b>1</b>	<b>Einleitung .....</b>	<b>5</b>
<b>2</b>	<b>Erklärungen .....</b>	<b>5</b>
<b>2.1</b>	<b>Grundlage der ePayBL: ePayment .....</b>	<b>5</b>
<b>2.2</b>	<b>Module der ePayBL.....</b>	<b>6</b>
2.2.1	ePayBL Kern.....	6
2.2.2	Konnektor.....	6
2.2.3	Paypage.....	7
2.2.4	Webshop.....	7
2.2.5	Rechnungserstellung.....	8
2.2.6	SEPA-Mandatsverwaltung.....	8
2.2.7	Bezahlterminals.....	9
<b>2.3</b>	<b>ePayBL im Detail.....</b>	<b>10</b>
2.3.1	Unterscheidung von Mandant und Bewirtschafter.....	11
2.3.2	Zertifikats-Nutzung.....	12
2.3.3	Anbindung eines Fachverfahrens an die ePayBL.....	12
2.3.4	Anbindung des Serviceportals (Amt24) an die ePayBL.....	13
2.3.5	Technische Umsetzung.....	14
<b>3</b>	<b>Anbindungsprozess der ePayBL .....</b>	<b>15</b>
<b>3.1</b>	<b>Erstgespräch.....</b>	<b>15</b>
<b>3.2</b>	<b>Vertragsabschluss.....</b>	<b>15</b>
3.2.1	Nutzungsbedingungen .....	15
3.2.2	Zahlungsverkehrsprovider-Vertrag .....	16
<b>3.3</b>	<b>Klärung Geschäftsprozesse zur Umsetzung mit ePayBL .....</b>	<b>18</b>
<b>3.4</b>	<b>Umsetzung .....</b>	<b>18</b>
<b>3.5</b>	<b>Betrieb .....</b>	<b>19</b>
<b>4</b>	<b>Geschäftsprozesse.....</b>	<b>20</b>

<b>4.1</b>	<b>Merkmale der Zahlungsarten .....</b>	<b>20</b>
<b>4.2</b>	<b>PCI DSS.....</b>	<b>21</b>
4.2.1	Was ist PCI DSS? .....	21
4.2.2	Wie wird die PCI Konformität bestätigt?.....	22
4.2.3	Wie unterstützt Sie der SID hierbei? .....	22
<b>4.3</b>	<b>Geschäftsprozesse - Öffentliche Einrichtungen mit eigenem Konto .....</b>	<b>23</b>
4.3.1	Kreditkarte .....	23
4.3.2	PayPal .....	24
4.3.3	giropay.....	26
<b>4.4</b>	<b>Geschäftsprozesse - Landesverwaltungen mit Konto der Hauptkasse .....</b>	<b>27</b>
4.4.1	Kreditkarte .....	27
4.4.2	PayPal .....	28
4.4.3	giropay.....	28
<b>5</b>	<b>Anleitungen .....</b>	<b>30</b>
<b>5.1</b>	<b>Beantragung von Zertifikaten.....</b>	<b>30</b>
<b>5.2</b>	<b>Installation von Browser-Zertifikaten .....</b>	<b>33</b>
5.2.1	Direkter Import von Zertifikaten [User-Zertifikat importieren] .....	35
5.2.2	Manueller Import von Zertifikaten.....	37
<b>5.3</b>	<b>Nutzung des GiroCockpit.....</b>	<b>37</b>
5.3.1	Abruf der Projektdaten zur Einrichtung in der ePayBL .....	37
5.3.2	Stornierung von Kreditkartenzahlungen .....	39
<b>5.4</b>	<b>Hinterlegung der Account-Daten des Zahlungsverkehrsproviders.....</b>	<b>40</b>
5.4.1	Kreditkarte und / oder giropay.....	40
5.4.2	PayPal .....	41
<b>5.5</b>	<b>OSCI – Transport.....</b>	<b>47</b>
5.5.1	Voraussetzung für die Nutzung von OSCI.....	47
5.5.2	Empfang von Daten .....	48
5.5.3	Automatisierter Abruf .....	49
<b>6</b>	<b>Wichtige Links.....</b>	<b>50</b>
<b>7</b>	<b>Glossar .....</b>	<b>50</b>

<b>8</b>	<b>Checkliste.....</b>	<b>52</b>
8.1	Vorbereitung und Vorüberlegung vor dem Erstgespräch .....	52
8.2	Erstgespräch mit dem SID .....	52
8.3	Vertragsabschluss.....	52
8.4	Klärung Geschäftsprozesse zur Umsetzung mit ePayBL .....	53
8.5	Umsetzung .....	53
8.6	Betrieb .....	54

### Dokumentenhistorie

Version	Datum	Änderung
2.0	April 2022	Korrektur Hyperlinks, Ergänzung PayPal-Einrichtung
3.0	März 2023	Komplettüberarbeitung
4.0	Juni 2023	Aktualisierung Checkliste
5.0	August 2023	Ergänzung OSCI – Transport und PCI DSS

## 1 Einleitung

Die Anbindung der Zahlungsplattform ePayBL an ein bestehendes Fachverfahren bringt verschiedene Voraussetzungen und notwendige Umsetzungsschritte mit sich. Daher bietet die vorliegende Handreichung einen Überblick sowie eine detaillierte Darstellung der Tätigkeiten für die Anbindung der ePayBL an ein bestehendes Fachverfahren. Bei Rückfragen dazu sind die Ansprechpartner der Anwendungsbetreuung Zahlungsverkehr wie folgt zu erreichen:

E-Mail: [zv@sid.sachsen.de](mailto:zv@sid.sachsen.de)

**Für die ersten Schritte und zur besseren Planbarkeit finden Sie in Kapitel 8 eine Zusammenfassung aller notwendigen Schritte.** Eine ausführliche Beschreibung der Checklisten finden Sie in Kapitel 3 „Anbindungsprozess der ePayBL“.

## 2 Erklärungen

### 2.1 Grundlage der ePayBL: ePayment

Der Begriff ePayment steht für Online-Zahlungsabwicklung, welche vor dem Hintergrund des Onlinezugangsgesetzes<sup>1</sup> für die Bezahlung von Verwaltungsleistungen zunehmend an Bedeutung gewinnt.

Im Freistaat Sachsen steht die Basiskomponente Zahlungsverkehr (BaK ZV), Projekt- und Software-Markename »ePayBL« (e-Payment Bund und Länder) den öffentlichen Verwaltungen zur medienbruchfreien Abwicklung kostenpflichtiger Verwaltungsdienstleistungen zur Verfügung. Alle zahlungsbezogenen Interaktionen (z. B. Entrichtung einer Gebühr im Antragsverfahren, Bezahlung eines Artikels im Online-Shop etc.) können über die BaK ZV ausgeführt werden. Damit steht allen Verwaltungen des Freistaates Sachsen und dessen Kommunen ein einheitlicher, standardisierter Dienst für sichere Online-Zahlungen beispielsweise mit Kreditkarte, PayPal, SEPA-Lastschrift und giro pay zur Verfügung.

Die BaK ZV stellt eine funktionale Infrastruktur bereit und implementiert organisatorische Regelungen, mit denen die teilweise komplexen Bezahlprozesse abgebildet werden können.

---

<sup>1</sup> Das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen verpflichtet Bund, Länder und Kommunen, bis Ende 2022 ihre Verwaltungsleistungen über Verwaltungsportale auch digital anzubieten.

Die BaK ZV bildet für die haushaltsordnungskonforme Buchung die zentrale Datendrehscheibe zwischen der Web-Anwendung der Verwaltung (z.B. Buchung eines E-Parkscheins), dem Zahlungsverkehrsprovider und dem Haushalts-, Kassen- und Rechnungswesen der Verwaltungen (HKR-Verfahren). Sie unterstützt die Zahlungsüberwachung und die Buchung in den Anwendungen des HKR-Verfahrens. Die Zahlungsabwicklung erfolgt über einen Zahlungsverkehrsprovider, der es ermöglicht Zahlungen per Kreditkarte, giropay oder auch PayPal durchzuführen. Ergänzend bietet die BaK ZV einen Rahmenvertrag für Dienstleistungen eines Zahlungsverkehrsproviders an, aus welchem zu guten Konditionen abgerufen werden kann.

## 2.2 Module der ePayBL

### 2.2.1 ePayBL Kern

Der ePayBL-Kern bildet die zentrale Datendrehscheibe zwischen der Fachanwendung einer Verwaltung, dem Zahlungsverkehrsprovider und dem Haushaltssystem einer Verwaltung. Die ePayBL bietet Webservices an, mit denen Fachanwendungen ihre Bezahlstatus abfragen können. Die Zahlungsabwicklung erfolgt durch externe Zahlungsverkehrsprovider, deren Schnittstellen in der ePayBL eingebunden sind. Nach erfolgreicher Zahlung erzeugt die ePayBL automatisch die zu den getätigten Zahlvorgängen gehörenden Sollstellungen, die in den zugehörigen Haushaltssystemen der Behörde bzw. Kommune importiert werden können. Zudem kann die ePayBL bei Bedarf nach Zahlungseingang die Informationen der Haushaltssysteme zu den Ist-Buchungen entgegennehmen (KABU-Schnittstelle der Hauptkasse). Diese Funktionen werden für alle angebotenen Zahlverfahren unterstützt. Neben diesen Funktionen für die Unterstützung der unmittelbaren Geschäftsprozesse bietet die ePayBL umfassende Möglichkeiten für die Administration und Konfiguration. Das betrifft insbesondere die Verwaltung von Mandanten und Bewirtschaftern, die den Fachverfahren zugeordnet sind.

### 2.2.2 Konnektor

Um die Implementierung der Zahlungsprozesse in ein bestehendes Fachverfahren zu vereinheitlichen und zu vereinfachen, wurde der ePayBL-Konnektor entwickelt. Dieser übernimmt als Bindeglied zwischen ePayBL und Fachverfahren alle Schritte, die für die Abwicklung einer Online-Zahlung notwendig sind und versorgt das Fachverfahren mit Informationen zur Zahlung wie zum Beispiel Zeitpunkt und Ergebnis der Zahlung, Kassenzettel sowie den Betrag und den Status der Zahlung. Durch seine Unabhängigkeit

zur verwendeten ePayBL-Version ermöglicht der ePayBL-Konnektor den Umstieg auf höhere Versionen der ePayBL ohne größere Auswirkungen auf die bestehenden Geschäftsprozesse. Vorteile des Konnektors:

- Zukunftssicher durch Versionsunabhängigkeit
- Schnelle Anbindung von Bezahlverfahren
- Einfache Anbindung an Fachverfahren

### 2.2.3 Paypage

Die Paypage ist eine Weboberfläche für die Auswahl und Abwicklung von Online-Zahlungen. Über die Paypage können Bezahlprozesse ohne großen Aufwand in ein bestehendes Fachverfahren integriert werden. Die Kommunikation mit den Zahlungsverkehrs Providern und mit dem ePayBL-Kern wird zentral über den Konnektor umgesetzt. Neue Zahlverfahren können dadurch ohne größeren Anpassungsaufwand in das Fachverfahren eingebunden werden, da diese nur einmal zentral in der Paypage umgesetzt werden müssen.

Das Design der Paypage kann durch den Mandanten selbst an die eigenen Wünsche bzw. das Aussehen des Fachverfahrens angepasst werden. Die Nutzung der Standard-Paypage erfolgt automatisch, wenn der Mandant selbst kein eigenes Paypage-Layout in der ePayBL hoch lädt (siehe Paypage-Handbuch).

Vorteile der Paypage:

- Dynamisch im Design und Text anpassbar
- Sehr komfortabel im Einsatz: in der Zielsprache des Kunden aufrufbar
- Einfache Anbindung an Fachverfahren mit Hilfe des Paypage-Handbuches

### 2.2.4 Webshop

Bei diesem Modul handelt es sich um ein umfassendes Shopsystem, welches auf Basis der Open-Source Onlineshop-Software Magento Version 1.9 entwickelt und an die ePayBL und insbesondere an die Bedürfnisse der Verwaltung angepasst wurde. Durch Nutzung des ePayBL Webshops kann die Verwaltung Waren und Dienstleistungen mit integrierter Zahlungsabwicklung über ePayBL für den Online-Verkauf anbieten. Damit steht ein moderner und den Erfordernissen der Verwaltung (z. B. Barrierefreiheit, BSI-Zertifizierung) entsprechender Webshop zur Verfügung.

Der ePayBL-Webshop wird mit seinen Standard-Funktionen zur Verfügung gestellt. Das Hosting und das Applikationsmanagement sind durch den Webshop-Anbieter selbst zu organisieren.

Vorteile des ePayBL-Webshops:

- BSI-geprüft und auf Barrierefreiheit getestet
- Responsive Design, auch auf mobilen Endgeräten verwendbar
- Magento-Webshop Open Source basierend (Vielseitigkeit)
- Umfangreiche Funktionalität
- Multistore-fähig
- giropay, Kreditkarte, Vorkasse und Rechnung bereits integriert

### 2.2.5 Rechnungserstellung

Das Modul Rechnungserstellung ermöglicht medienbruchfreie Rechnungsprozesse für kostenpflichtige Verwaltungsdienstleistungen. Über die Rechnungserstellung können elektronische Rechnungen für die vom Kunden/Nutzer erworbene Dienstleistung erstellt und per E-Mail an den Rechnungsempfänger versendet werden. Über eine in der Rechnung enthaltene Verlinkung zur Paypage kann der Rechnungsempfänger die Bezahlung unkompliziert auslösen.

Vorteile der Rechnungserstellung:

- Ohne Installation auf dem Rechner sofort einsatzbereit
- Konfigurierbarer Gebührenkatalog
- Rechnungen in verschiedenen Sprachen
- 4-Augen-Prinzip für Rechnungserstellung (optional)
- Signierung der Rechnungen (optional)
- Massenupload (mittels csv)

### 2.2.6 SEPA-Mandatsverwaltung

Die SEPA-Mandatsverwaltung wurde entwickelt, um die Vorhaltung von zahlungsrelevanten Daten, die zur Abwicklung einer SEPA-Lastschrift zwingend notwendig sind, sicherzustellen. Fachverfahren, die SEPA-Lastschriften technisch abwickeln sollen, dient die



SEPA-Mandatsverwaltung in Verbindung mit der ePayBL als Service-Komponente zur Vereinnahmung von Zahlungen mittels SEPA-Lastschrift. Sie unterstützt das Anlegen und Verwalten von Kreditoren- und Debitorenmandaten (sowohl per Webservice als auch über eine Weboberfläche) und generiert automatisch die erforderlichen Vorabinformationen über den Lastschrifteinzug entsprechend den SEPA-Regeln.

Vorteile der ePayBL SEPA-Mandatsverwaltung:

- Einheitliche, zentrale Mandatsverwaltung für SEPA Mandate (gemäß den Verfahrensregeln für die Abwicklung von SEPA-Zahlungen<sup>2</sup>)
- Wiederholtes Bezahlen ohne neue Lastschriftmandate
- Konsistente und revisionssichere Verwaltung der SEPA-Mandate
- Automatische Erstellung der Bankdateien für den Lastschrifteinzug

### 2.2.7 Bezahlterminals

Insbesondere im Tresengeschäft öffentlicher Einrichtungen werden Bezahlterminals für die Abwicklung von Kartenzahlungen genutzt. Anwendungsbeispiele finden sich beispielsweise in Einwohnermeldeämtern oder in Straßenverkehrsämtern.

Für die Miete von Bezahlterminals hat der SID einen Rahmenvertrag mit einem Dienstleister abgeschlossen, der von allen öffentlichen Einrichtungen in Sachsen genutzt werden kann.

Vorteile der Bezahlterminals:

- Rahmenvertrag mit guten Konditionen
- Benutzerfreundliche Hardware
- Bezahlterminals (mobil/stationär) für dauerhaften Einsatz

Der Abruf von Bezahlterminals erfolgt über das Abruf-Formular unter dem Link:

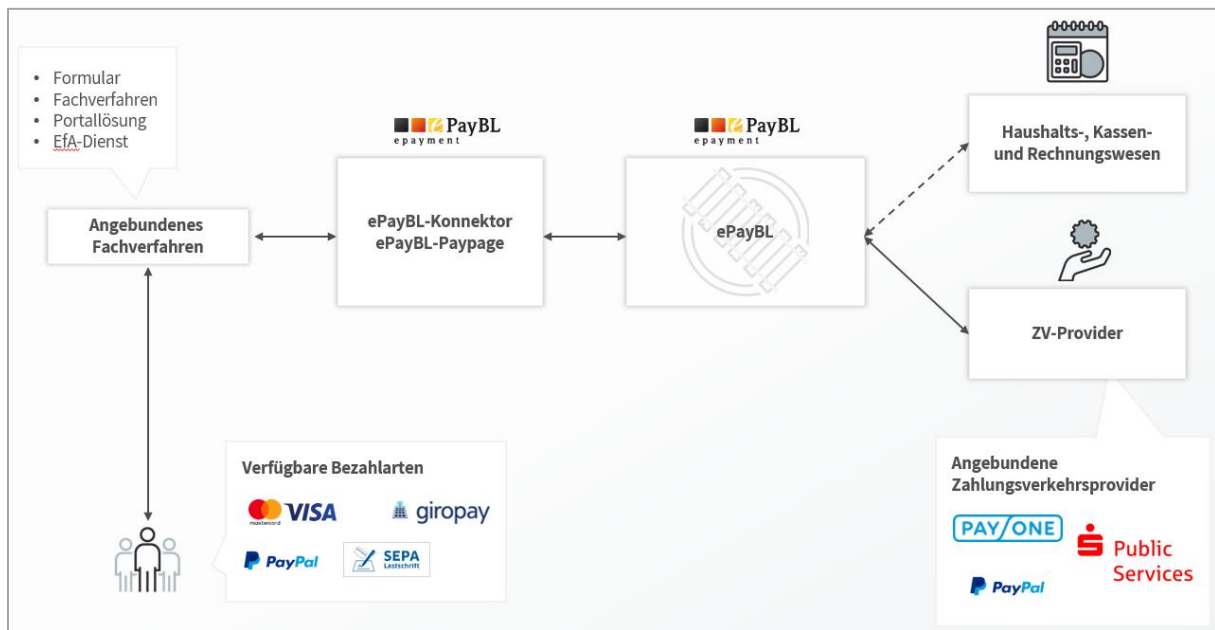
[Abruf Bezahlterminals](#)

---

<sup>2</sup><https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/veroeffentlichungen/verfahrensregeln-sepa-fuer-kontoinhaber-mit-bankleitzahl--743348>

## 2.3 ePayBL im Detail

Ein Bürger oder ein Unternehmen nutzt eine entgeltliche Verwaltungsdienstleistung in einem Service- oder Fachportal. In der Folge werden zahlungsrelevante Daten wie Betrag, Buchungstext und Kassenzeichen vom Fachverfahren über den Konnektor an die ePayBL weitergeleitet.



Damit der Bürger seine Leistungen bezahlen kann, wird er, nachdem diese Daten von der ePayBL an den Zahlungsverkehrsprovider weitergeleitet worden sind, zur ePayBL-Paypage oder direkt (bei Direktanbindung) zum jeweiligen Provider des ausgewählten Zahlverfahrens weitergeleitet und kann seine Zahlung online abschließen. Das Ergebnis der Zahlung wird vom Zahlungsverkehrsprovider an die ePayBL übermittelt.

Anschließend fragt das Fachverfahren bei der ePayBL das Zahl-Ergebnis ab und erteilt dem Fachverfahren die Freigabe der Dienstleistung. Die ePayBL bereitet die Zahlungsdaten für die Weiterverarbeitung in HKR-Systemen auf, woraufhin die Übernahme der Zahlungsdaten in das HKR-System durch die Behörde / Kasse erfolgen kann. Die Dateien für das HKR-System (xFinanz-Dateien, camt.054-Dateien, UmsatzReports, etc.) werden täglich erzeugt und können manuell über das ePayBL-Portal oder per OSCI (weitere Infos siehe [Kapitel 5.5](#)) an den Mandanten übermittelt werden.

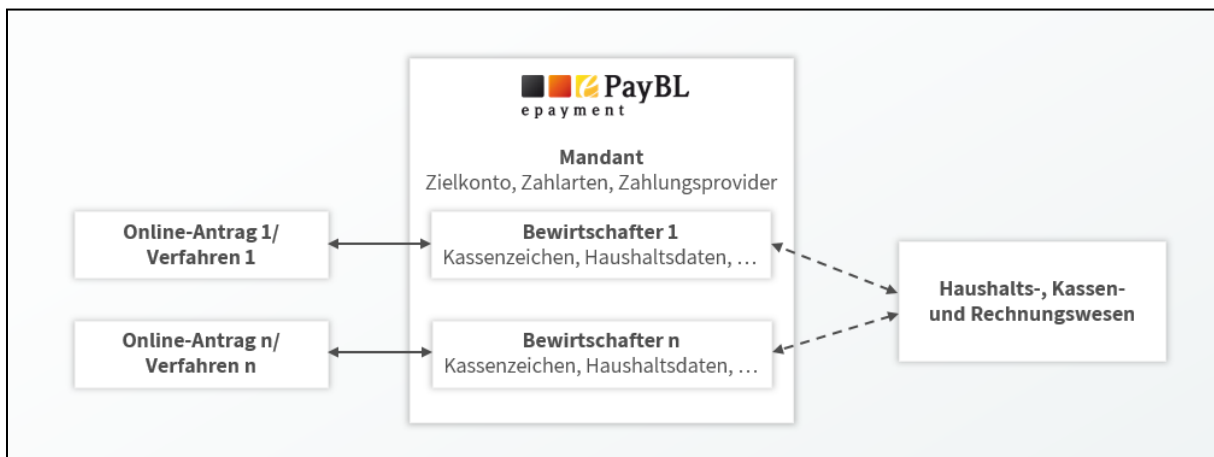
Für die Erfüllung dieses Prozesses erfüllt die ePayBL folgende Funktionen:

- Berichtsfunktion (im ePayBL-Portal)
- Erzeugung und Weiterleitung von Sollstellungen an Kassenverfahren (xFinanz-Datei)
- Aufteilung und Zuordnung von Summengutschriften bei Kreditkarten- und PayPal-Zahlungen (über camt.054-Datei)
- Einfache Anbindung von Fachverfahren und Haushaltssystemen (über den ePayBL-Konnektor)

### 2.3.1 Unterscheidung von Mandant und Bewirtschafter

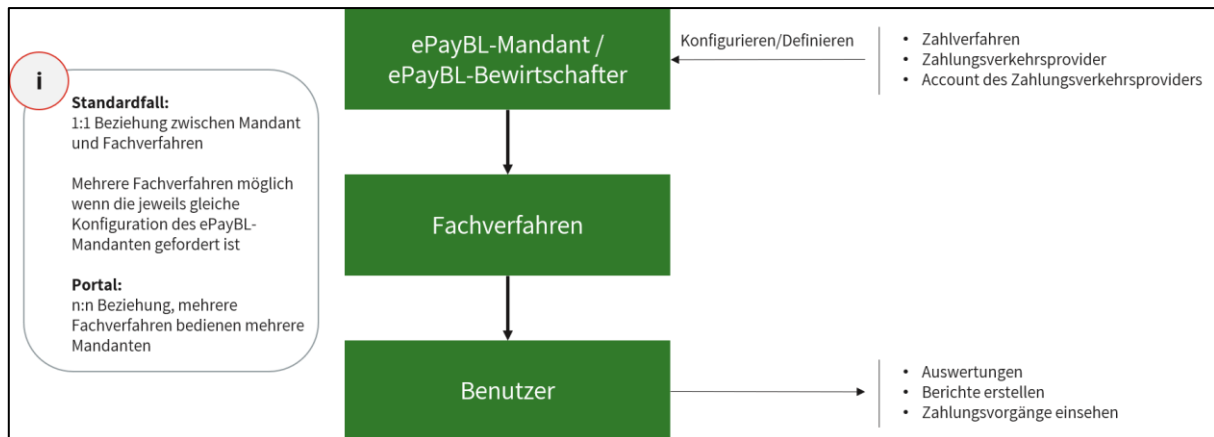
Die wichtigsten Begrifflichkeiten, die unterschieden werden sollten, sind Mandant und Bewirtschafter.

Die Konfigurationsmöglichkeiten unterscheiden sich wie folgt:



Mandant	Bewirtschafter
Account für Zahlungsprovider (Gutschriftskonto für Einnahmen)	Kassenzeichenpool und -länge
Zahlverfahren	Haushaltsparameter
Art der Übermittlung des Kassenzeichens (über Webservice oder durch ePayBL)	

In der nachstehenden Abbildung ist der Standardfall des ePayBL Portals abgebildet.



## 2.3.2 Zertifikats-Nutzung

### 2.3.2.1 Webservice-Zertifikat

Um die Kommunikation zwischen Fachverfahren und ePayBL herstellen zu können, ist die Einbindung eines Webservice-Zertifikats nötig, welches nach Erhalt an den Fachverfahrenshersteller weitergegeben werden muss.

Für die Beantragung eines Webservice-Zertifikats ist der Anleitung in [Kapitel 5.1](#) zu folgen.

### 2.3.2.2 Browser-Zertifikat

In der Mandantenkonfiguration wurden Benutzer angegeben, welche Zugriff auf das ePayBL-Portal erhalten sollen. Um diesen Nutzern den Zugriff auf das ePayBL-Portal zu ermöglichen, ist es notwendig, dass diese Benutzer sich ein personengebundenes Browser-Zertifikat beantragen.

Für die Beantragung eines Browserzertifikats ist der Anleitung in [Kapitel 5.1](#) zu folgen.

## 2.3.3 Anbindung eines Fachverfahrens an die ePayBL

Um ein Fachverfahren an die ePayBL anzubinden, muss dieses über den Konnektor mit der ePayBL kommunizieren. Ziel des ePayBL-Konnektors ist die Bündelung der Aufrufe der ePayBL sowie der ZV-Provider-Schnittstelle, um die Implementierung der Zahlungsprozesse in ein bestehendes Fachverfahren zu vereinheitlichen und deutlich zu vereinfachen.

Der ePayBL-Konnektor wird damit als unsichtbares Bindeglied zwischen ePayBL und Fachverfahren alle Schritte, die für die Abwicklung einer Online-Zahlung notwendig sind,

übernehmen und das Fachverfahren mit Informationen zur Zahlung versorgen. Dazu gehören detaillierte Informationen, wie z.B. Zeitpunkt und Ergebnis der Zahlung, ePayBL-Kassenzeichen und Betrag. Da der ePayBL-Konnektor Bibliotheken in verschiedenen Entwicklungssprachen wie JAVA, .NET oder PHP zur Verfügung stellt, kann die Schnittstelle einfach und mit sehr geringem Aufwand in bestehende Fachverfahren eingebunden werden.

Für die Nutzung gibt es 2 Varianten:

#### Direktintegration im Fachverfahren:

Über den Konnektor werden die Transaktionsdaten an die ePayBL übermittelt. Der Nutzer hat dann im Fachverfahren die Möglichkeit, aus einer durch das Fachverfahren festgelegten Auswahl an Zahlverfahren sein Zahlungsmittel zu wählen, ohne dass eine Weiterleitung auf eine externe Seite erfolgt. Nach Auswahl des Zahlverfahrens erfolgt die direkte Weiterleitung an den Zahlungsprovider. Nach erfolgreicher Zahlung wird der Nutzer wieder zurück in das Fachverfahren geleitet. Ein Vorteil dieser Anbindung ist der, dass der Nutzer sich bis zur Bezahlung mit dem ausgewählten Zahlverfahren immer im Fachverfahren befindet und es keine zusätzlichen Webseitensprünge gibt. Die Entwicklung ist aber aufwändiger.

#### ePayBL-Paypage:

Eine zweite Möglichkeit der Anbindung ist die Nutzung der Paypage in Verbindung mit dem Konnektor. Dazu wird der Nutzer über das Fachverfahren an die Paypage, eine separate Webseite, die durch die ePayBL bereitgestellt wird, weitergeleitet und wählt auf dieser sein gewünschtes Zahlverfahren aus. Der Nutzer wird nach der Auswahl zu dem für das Zahlverfahren zuständigen Zahlungsverkehrsprovider weitergeleitet und nach der Durchführung der Transaktion zurück zum Fachverfahren geführt. Ein Vorteil der Paypage ist der verringerte Entwicklungsaufwand, da das Fachverfahren lediglich die URL der Paypage aufrufen und das Ergebnis der Zahlung an der ePayBL abrufen muss.

### **2.3.4 Anbindung des Serviceportals (Amt24) an die ePayBL**

Die Methoden für die Abwicklung der Zahlung wurden in Amt24 des Freistaates Sachsen bereits integriert. Dadurch wird es möglich, zahlungspflichtige Prozesse auch in Amt24 vollständig abbilden zu können. **Für eine Nutzung von Amt24 setzen Sie sich bitte vorab mit Amt24 in Verbindung.**

### 2.3.5 Technische Umsetzung

Für die Anbindung des Fachverfahrens an die ePayBL stehen im Konnektor verschiedene Methoden bereit.

#### 1. Zahlverfahren (optional)

Mit dieser Methode können die an der ePayBL freigeschalteten Zahlverfahren am Mandanten abgefragt werden. Dies wird benötigt, wenn die ZahlverfahreAuswahl direkt im Fachverfahren stattfinden soll und keine Paypage genutzt wird.

#### 2. Buchungslisten (obligatorisch)

Mit dieser Methode werden alle zahlungsrelevanten Daten an die ePayBL übertragen, um eine neue Buchung anzulegen.

#### 3. Kassenzzeichen (obligatorisch)

Mit dieser Methode kann der Zahlstatus der Transaktion geprüft werden, um festzustellen, ob der Nutzer bereits bezahlt hat oder nicht.

Während eines Onlinezahlvorgangs kann es zu technischen Problemen oder Fehlbedienungen kommen, in dessen Folge der Nutzer trotz einer erfolgreichen Zahlung nicht mehr im Browser zurück in das Fachverfahren geleitet wird. Das Fachverfahren muss daher sicherstellen, dass die Zahlung der Transaktion auch ohne die Rückleitung ins Fachverfahren geprüft werden kann. Das heißt, **der Status des Kassenzzeichens muss zwingend abgefragt werden.**

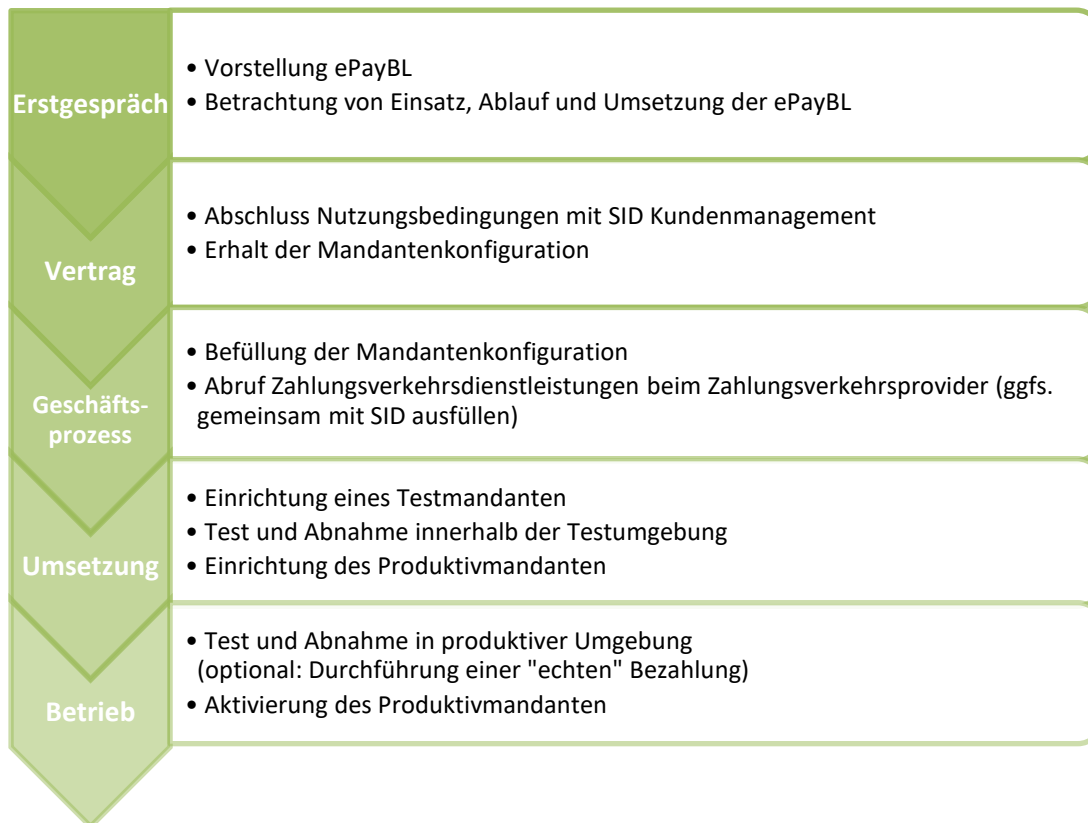
#### 4. Kunde löschen (optional)

Wenn ein Kunde als Bestandskunde in der ePayBL angelegt wurde, kann er mit dieser Methode gelöscht werden

Alle weiteren angebotenen Methoden finden Sie im Integrationshandbuch zum Konnektor.

## 3 Anbindungsprozess der ePayBL

Für die Anbindung der ePayBL an bestehende Fachverfahren hat sich folgender Anbindungsprozess bewährt:



Eine Zusammenfassung aller notwendigen Schritte finden Sie in [Kapitel 8](#).

### 3.1 Erstgespräch

Im Erstgespräch erfolgt die Vorstellung der ePayBL. Ziel soll es sein eine mögliche Lösung für den Einsatz der ePayBL zu finden und die weiteren Schritte bzw. Termine abzustimmen.

### 3.2 Vertragsabschluss

#### 3.2.1 Nutzungsbedingungen

Wenn Sie sich dazu entschieden haben, die Basiskomponente Zahlungsverkehr zu nutzen, muss die Zustimmung zu den Nutzungsbedingungen als vertragliche Grundlage erfolgen, welche Sie zur Nutzung der Basiskomponente Zahlungsverkehr / ePayBL berechtigt.

Das Formular finden Sie unter folgendem Link: [Nutzungsbedingungen BaK ZV](#)

Bei Fragen dazu wenden Sie sich bitte an: [kundenmanagement@sid.sachsen.de](mailto:kundenmanagement@sid.sachsen.de)

Nach der Bestätigung durch den SID erhalten Sie die Mandantenkonfiguration zur Einrichtung eines Testmandanten.

Dieses Dokument wird in einem gemeinsamen Termin mit der Anwendungsbetreuung ausgefüllt und muss im Anschluss an [zv@sid.sachsen.de](mailto:zv@sid.sachsen.de) geschickt werden.

**Hinweis:** Erst nach Bestätigung durch den SID wird die Bereitstellung des Test- und Produktivmandanten möglich.

### 3.2.2 Zahlungsverkehrsprovider-Vertrag

Um Ihren Kunden die Bezahlverfahren Kreditkarte, giropay oder PayPal anbieten zu können, ist ein Vertrag mit einem Zahlungsverkehrsprovider (ZVP) notwendig. Dabei kann auf einen Rahmenvertrag zurückgegriffen werden, welcher zwischen dem SID und dem ZVP Payone abgeschlossen wurde.

#### **Hinweis:**

Der Antrag sollte bereits nach der Rückmeldung des Kundenmanagements zur Bestätigung der Nutzungsbedingungen erfolgen, damit Ihnen die benötigten Daten zur Produktivsetzung vorliegen. Bei Bedarf kann der Antrag im Zweit-Termin gemeinsam ausgefüllt werden.

Unter folgendem Link finden Sie das entsprechende Abrufformular (für Neuabrufe, Änderungen, Kündigungen): [Abruf ZVP](#)



Gemäß §§10-12 Geldwäschegesetz muss für die Einrichtung eines Accounts beim Zahlungsverkehrsprovider zwingend eine Identifizierung des Vertragspartners mit der für sie auftretenden Personen vorgenommen werden.

Hierfür stehen drei Verfahren zur Verfügung:

1. Identitätsprüfung durch „zuverlässige Dritte“
2. Post-Ident Verfahren
3. Video-Ident Verfahren



Alle wichtigen Informationen und weitere Formulare zum Antrag erhalten Sie über die Dateien in der Kopfzeile des Abrufformulars

<b>Regularien und Konditionen:</b> <a href="#">Regularien zur Abwicklung von Online-Zahlungen</a> <a href="#">Bedingungen GiroPay</a> <a href="#">Preisblatt</a>	 
<b>Identifizierungsunterlagen:</b> <a href="#">Identifizierungsmöglichkeiten</a> <a href="#">Vorlage Behördenbestätigung</a> <a href="#">Vorlage Postident</a> <a href="#">Identifizierung über zuverlässige Dritte</a>	
<b>Paydirekt:</b> <a href="#">Antrag für paydirekt</a>	
<b>PayPal:</b> <a href="#">Leitfaden Vertragsabschluss</a>	

### Hinweise zur Befüllung des Formulars

- Wählen Sie als Erstes die ePayBL-Kopfstelle „Sachsen“ und wählen „**Neuvertrag**“.
- Bei „Verwendungszweck“ können Sie einen festen Text (max. 20 Zeichen) vorgeben, der bei den Kreditkarten-Summengutschriften vom Zahlungsverkehrsprovider im Verwendungszweck angegeben wird und über den eine leichtere Zuordnung der Gutschrift ermöglicht wird.
- Bei einer **Stammdatenänderung** müssen nur die Pflichtfelder sowie die sich ändernden Felder ausgefüllt werden. Geben Sie zusätzlich im „Bemerkungen“-Feld kurz an, welche Änderungen durchgeführt werden sollen. (Beispielsweise „Änderung Bankverbindung / Rechnungsadresse“, etc.).
- Bei einer **Kündigung** müssen nur Daten zur Einrichtung sowie der gewünschte Kündigungszeitpunkt ausgefüllt werden.
- **WICHTIG:** Wenn alle Pflichtangaben ausgefüllt wurden, senden Sie das Formular bitte über die Schaltfläche „Abschließen & Versenden“ auf Seite 2 des Formulars ab.

Dieser Antrag muss unterschrieben je nach Identifizierungsart an den Zahlungsverkehrsprovider geschickt werden (siehe Anlage „Identifizierungsmöglichkeiten“ im Abrufformular).

Sollten Sie bereits die Identifizierung erfolgreich beim Zahlungsverkehrsprovider vorgenommen haben, wird der Antrag unterschrieben an [Kundenservice-SID@payone.com](mailto:Kundenservice-SID@payone.com) gesendet.

Nach der Einrichtung des Accounts müssen die Projektdaten im ePayBL-Portal eingepflegt werden (siehe [Kapitel 5.3](#))

### **Hinweis für die Zahlart PayPal:**

Für PayPal benötigen Sie zwingend ein Händlerkonto beim Anbieter PayPal. Dieses muss direkt bei PayPal eröffnet werden (Informationen dazu im Dokument „Leitfaden Vertragsabschluss“ im linken oberen Bereich des Abruf-Formulars).

### **Hinweis für die Zahlart Kreditkarte:**

Durch den Abschluss des Kartenakzeptanzvertrags mit dem Zahlungsverkehrsprovider zur Abwicklung von Kreditkartenzahlungen ermöglichen Sie Ihren Kunden eine komfortable, bargeldlose Zahlungsweise. Damit tragen Sie jedoch auch Verantwortung für die Sicherheit der Kartendaten Ihrer Kunden. Aus diesem Grund sind Sie gemäß dem Kartenakzeptanzvertrag verpflichtet, den Datensicherheitsstandard der Kartenindustrie PCI DSS (Payment Card Industry Data Security Standard) einzuhalten und dies auch nachzuweisen. Dies erfolgt 1x jährlich. (weitere Informationen dazu finden Sie in [Kapitel 4.2](#))

## **3.3 Klärung Geschäftsprozesse zur Umsetzung mit ePayBL**

In einem weiteren Termin werden die aktuellen sowie zukünftigen Geschäftsprozesse betrachtet. Ziel soll es sein eine gemeinsame Grundlage für den Einsatz der ePayBL zu finden und die weiteren Schritte bzw. Termine abzustimmen. Zudem können bei Bedarf die Mandantenkonfiguration und der Antrag zum Abruf der Zahlungsverkehrsprovider-Dienstleistung gemeinsam durchgesprochen und ausgefüllt werden.

Folgende Teilnehmer sollten in diesem Termin anwesend sein:

- Fachverfahrensbetreuer
- Haushalt
- IT-Abteilung
- Projektleitung

## **3.4 Umsetzung**

Liegt der Anwendungsbetreuung die ausgefüllte Mandantenkonfiguration vollständig vor, wird ein Testmandant im Testsystem der ePayBL eingerichtet. Im Anschluss daran erhalten Sie alle für die Entwicklung der Anbindung notwendigen Daten und Dokumente zur Weiterleitung an Ihren Entwicklungs-Dienstleister.

Ist die Umsetzung der Schnittstelle erfolgt, führt die Anwendungsbetreuung einen Abnahmetest durch, um die Umsetzung für das Produktivsystem freizugeben.

Hierfür werden folgende Testfälle durchgeführt:

1. Eine erfolgreiche Zahlung je Zahlverfahren mit Rückkehr in das Fachverfahren
2. Eine erfolgreiche giropay-Zahlung mit Schließen des Browser-Fensters ohne Rückkehr in das Fachverfahren
3. Eine erfolgreiche Zahlung mit vorherigem Wechsel des Zahlverfahrens
4. Abbruch der Zahlung auf der Bezahlseite des Zahlungsverkehrsproviders

**Wichtig:** Testdaten für Testzahlungen per Kreditkarte, giropay etc. finden Sie unter: <https://api.girocheckout.de/girocheckout:testdata>

Können alle 4 Testfälle erfolgreich abgeschlossen werden, erhalten Sie die Freigabe für das Produktivsystem.

### 3.5 Betrieb

Nach Überführung Ihres Mandanten in das Produktivsystem müssen Sie die Account-Daten des Zahlungsverkehrs-Providers hinterlegen (siehe [Kapitel 4.3.1](#) und [Kapitel 4.4](#)). Bevor Sie Ihr Verfahren für die Bürger freigeben, empfehlen wir noch einmal alle Zahlverfahren produktiv zu testen, um eventuellen Fehlern bei der Produktivsetzung vorzubeugen.

## 4 Geschäftsprozesse

Zum Verständnis der jeweiligen Geschäftsprozesse werden diese im Folgenden für die Zahlarten Kreditkarte, PayPal und giropay dargestellt. Dabei wird zwischen öffentlichen Einrichtungen mit eigenem Konto und Landesverwaltungen mit Konto der Hauptkasse unterschieden. Zunächst werden jedoch die Konfigurationsmöglichkeiten der einzelnen Zahlungsarten dargestellt.

### 4.1 Merkmale der Zahlungsarten

In der folgenden Tabelle werden die unterschiedlichen Merkmale der einzelnen Zahlverfahren dargestellt.

	Verwendungszweck	Gutschriftsart	Aufschlüsselung
Kreditkarte	maximal 20 Zeichen zusätzlich zur VU- und RE-Nummer	Sammelgutschrift	camt.054-Datei
giropay	maximal 27 Zeichen [Bewirtschafternummer]/[Kassenzeichen] <u>oder</u> [Kassenzeichen]/[Buchungstext der ersten Buchung] <sup>3</sup>	Einzelgutschrift	-
PayPal	127 Zeichen bei Direktanbindung zu PayPal <u>oder</u> 27 Zeichen bei Zahlungsprovider Abwicklung über ZVP	Sammelgutschrift	camt.054-Datei



#### Einzelgutschrift

Bei giropay-Zahlungen erfolgt die Zahlung direkt als Gutschrift vom Konto des Zahlers auf das Konto der Einrichtung. Für die Zuordnung der Zahlung kann neben dem eindeutigen Kassenzeichen auch die Bewirtschafternummer genutzt werden.

<sup>3</sup> Ist dieser Verwendungszweck ausgewählt, ist eine Aufschlüsselung der Kreditkartenzahlungen über die camt054-Dateien nicht möglich, da diese nur erzeugt werden können, wenn der Verwendungszweck die Bewirtschafternummer enthält.

## Summengutschrift

Bei den Zahlungsarten Kreditkarte und PayPal ist es über Schnittstellen zum Zahlungsprovider in der ePayBL möglich, die Summengutschriften in einer camt.054-Datei zur Verfügung zu stellen. Neben der täglichen Gutschrift der Summe auf das Konto der Einrichtung wird über die Schnittstellen an die ePayBL übermittelt, welche Einzeltransaktionen darin enthalten sind. Die ePayBL erstellt auf Grundlage dieser Informationen eine camt.054-Datei. Im Dateinamen ist die **Referenznummer** enthalten, welche in der Gutschrift als Verwendungszweck angezeigt wird. Über diese ist eine Zuordnung der einzelnen Transaktionen zur Gutschrift des Zahlungsdienstleisters möglich. Im Haushaltssystem kann diese Datei eingespielt werden, um SOLL- Stellungen ausgleichen zu können.

<input type="checkbox"/>	 74425_KREDITKARTE_camt054_CC_20190605_SCHULUNG.xml	3946	05.06.2019 13:25:36
<input type="checkbox"/>	 74425_KREDITKARTE_camt054_CC_20190605_SCHULUNG_Begleitschein.pdf	4416	05.06.2019 13:25:37

## 4.2 PCI DSS

### 4.2.1 Was ist PCI DSS?

PCI DSS ist ein Regelwerk im Zahlungsverkehr, welches sich auf die Abwicklung von Kreditkartentransaktionen bezieht. Der Standard wurde von den fünf wichtigsten Kreditkartenunternehmen (American Express, JCB, MasterCard, Discover Financial Services and Visa) ins Leben gerufen und umfasst die folgenden Sicherheitsanforderungen:

1. Einrichtung und Betrieb eines geschützten Netzwerks
2. Schutz von aufbewahrten und übermittelten Karteninhaberdaten
3. Einrichtung und Betrieb eines Schwachstellen-Management-Systems
4. Umsetzung effektiver Richtlinien zur Zugriffskontrolle
5. Regelmäßige Überwachung und Überprüfung der IT-Infrastruktur
6. Formulierung und Durchsetzung einer Richtlinie zur Informationssicherheit

Weiterführende Informationen zu PCI DSS finden sie auch unter

<https://www.pcisecuritystandards.org/lang/de-de/>.

#### 4.2.2 Wie wird die PCI Konformität bestätigt?

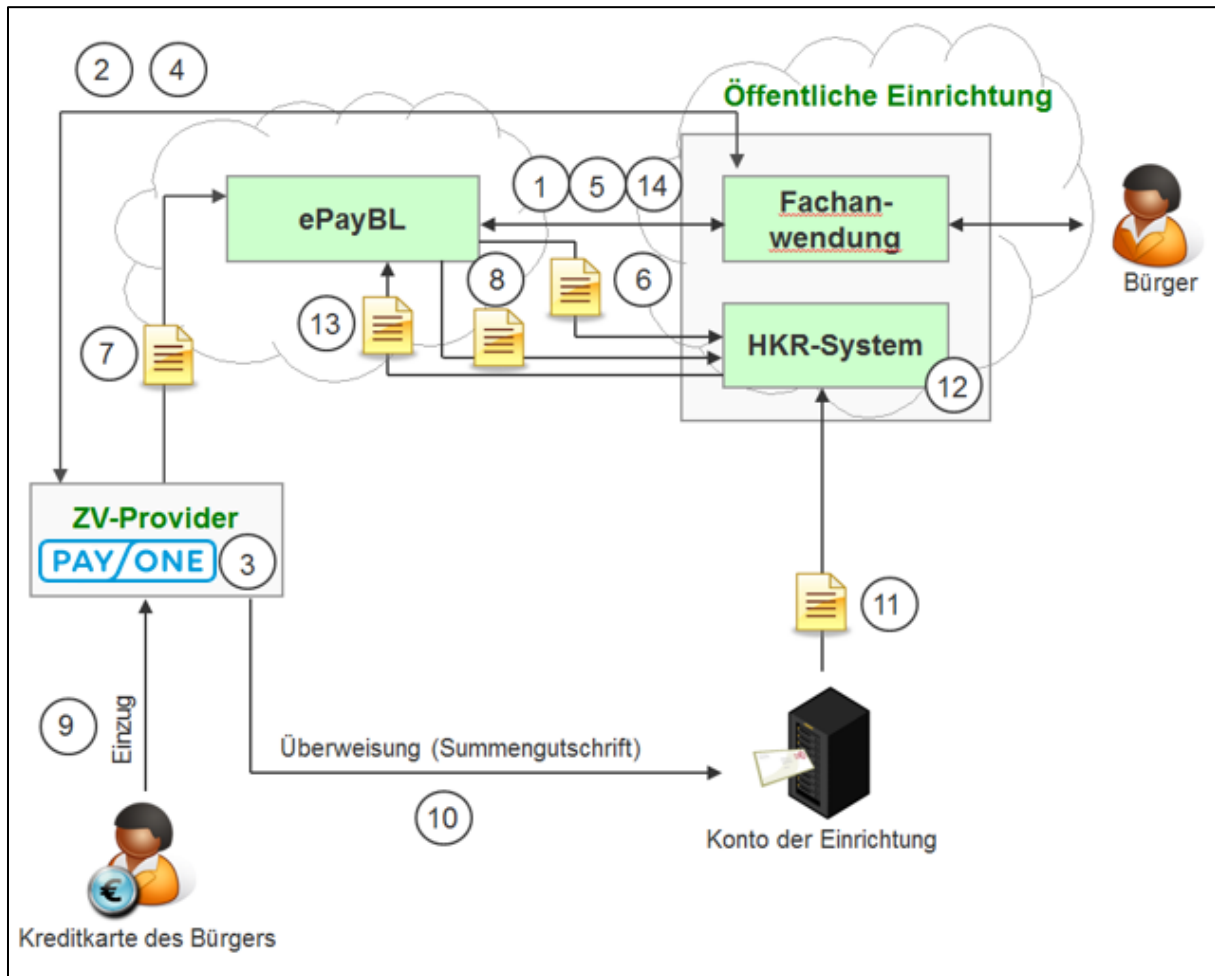
Zur Bestätigung der Konformität gibt es verschiedene Selbstbeurteilungsfragebögen, je nachdem wie hoch der Kontakt zu Kreditkarteninhaberdaten ausfällt. Da die ePayBL selbst keine Kreditkarteninhaberdaten speichert, verarbeitet oder überträgt, erfolgt die Bestätigung der Konformität über den kürzesten Selbstbeurteilungsfragebogen A (SAQ A). Mit dem Fragebogen soll bestätigt werden, dass die URL bei der Kreditkarten-Zahlung bei der Weiterleitung nicht verfälscht wird. Wenn Sie die Paypage nutzen, liegt die Hauptverantwortung auf Seite der ePayBL, da der Kunde von der Paypage aus direkt auf die Eingabeseite der Kreditkarteninhaberdaten von S-Public Services weitergeleitet wird. Sollten Sie die Kreditkarten-Zahlung in Ihr Fachverfahren eingebettet haben (direkte Anbindung), dann müssen die Anforderungen des PCI DSS zusätzlich vom Fachverfahrenshersteller eingehalten werden. Dies ist erforderlich, da die Kunden vom Fachverfahren und nicht von der ePayBL direkt auf die Eingabeseite der Kreditkartendaten von S-Public Services gelangen.

#### 4.2.3 Wie unterstützt Sie der SID hierbei?

Wir als SID haben im aktuellen Rahmenvertrag mit PAYONE vereinbart, dass die Bestätigung des PCI DSS nicht durch Sie selbst als Vertragsinhaber, sondern durch den SID gegenüber PAYONE erfolgt, da wir Ihnen unseren Dienst zur Abwicklung Ihrer Kreditkarten-Zahlungen anbieten. Als Grundlage für die Verifizierung benötigen wir aber dennoch eine Bestätigung von Ihnen, dass Sie als nutzende Behörde, Ihre Mitarbeiter sowie Ihre Fachverfahrenshersteller die PCI Konformität einhalten. Die Konformität muss jährlich gegenüber dem Zahlungsverkehrsprovider bestätigt werden.

### 4.3 Geschäftsprozesse - Öffentliche Einrichtungen mit eigenem Konto

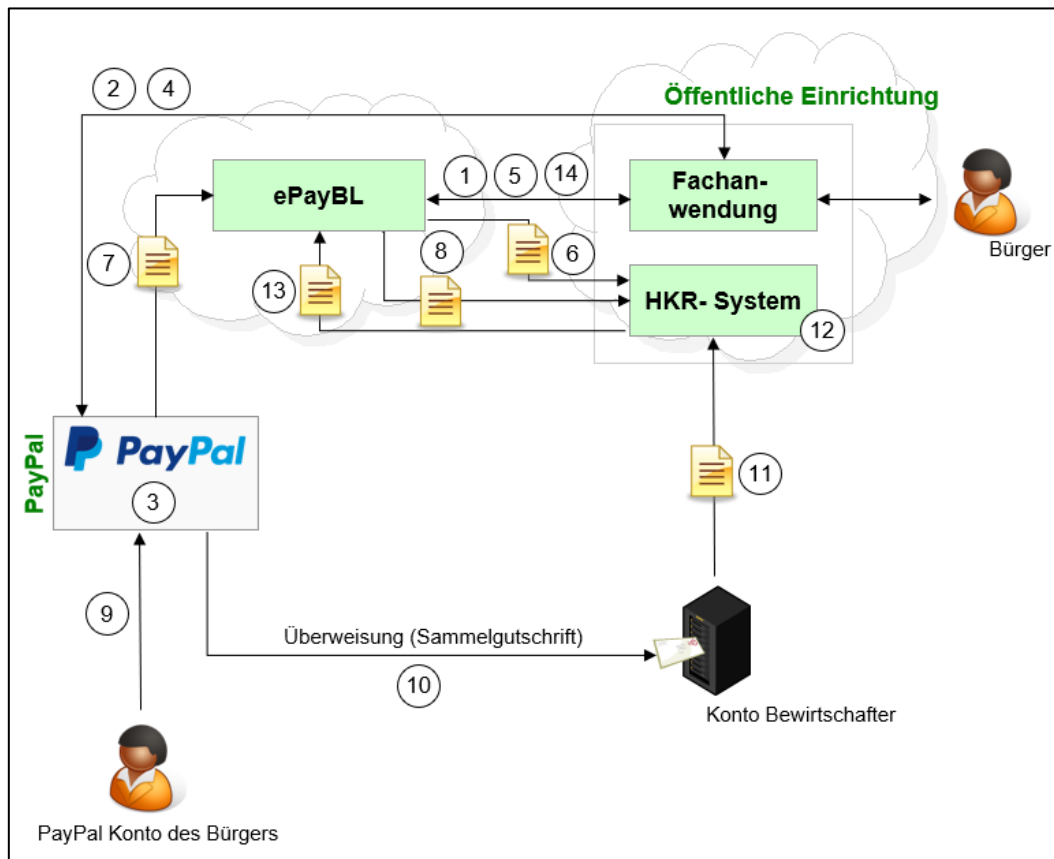
#### 4.3.1 Kreditkarte



Nr.	Beschreibung
1	Übermittlung der Transaktionsdaten an ePayBL und Entgegennahme der URL für die Zahlungsabwicklung
2	Weiterleitung des Zahlungspflichtigen zum ZV-Provider
3	Autorisierung und Abwicklung der Zahlung beim ZV-Provider
4	Weiterleitung des Zahlungspflichtigen zur Fachanwendung
5	Verifizierung der Zahlung durch die Fachanwendung bei ePayBL
6	Optional: Übermittlung einer Datei zum Aufbau von Sollstellung im HKR-System
7	Übermittlung der EPA (Electronic Payment Advice = Transaktionsübersicht) an ePayBL

8	Optional: Übermittlung eines Kontoauszuges (Einzeltransaktionen) für Aufteilung von Summengutschriften durch ePayBL
9	Belastung der Kreditkarte des Bürgers
10	Summengutschrift an das Konto der öffentlichen Einrichtung / des Zahlungsempfängers
11	Übermittlung eines Kontoauszuges durch die Hausbank (Summengutschrift)
12	Optional: Verarbeitung des Kontoauszuges aus Schritt 8 im HKR-System zum Ausgleich von Sollstellungen
13	Optional: Zahlungsanzeige (Ist-Buchung) an ePayBL
14	Optional: Abfrage des Zahlungseingangs durch die Fachanwendung

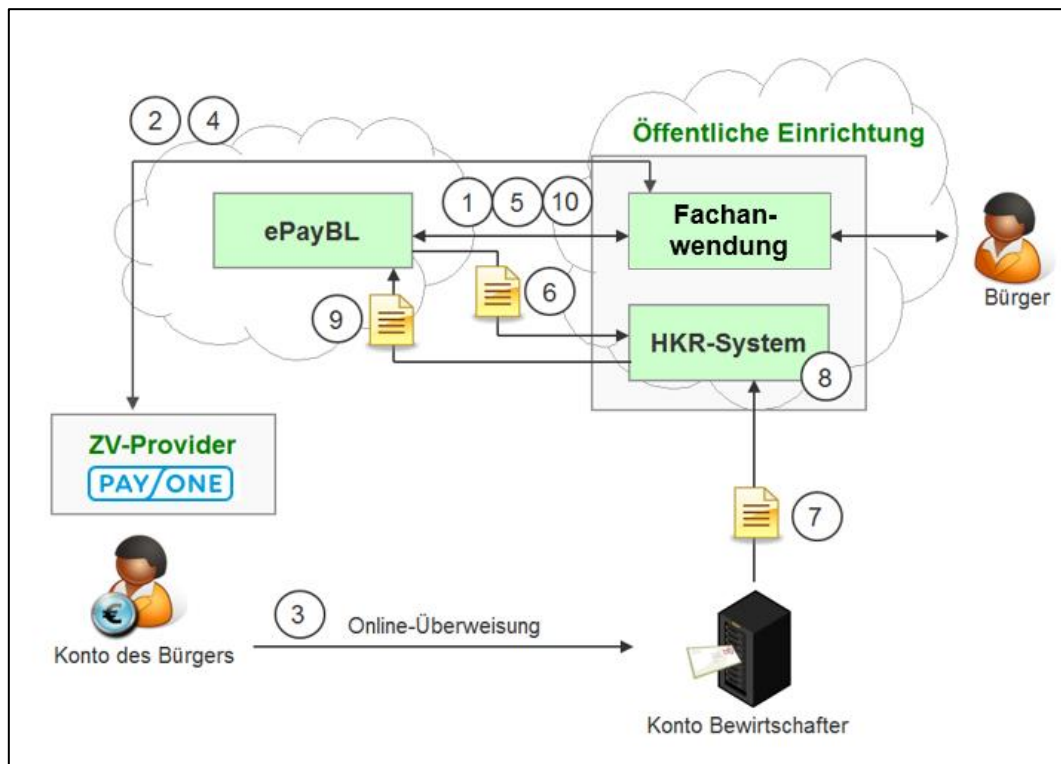
### 4.3.2 PayPal





Nr.	Beschreibung
1	Übermittlung der Transaktionsdaten an ePayBL und Entgegennahme der URL für die Zahlungsabwicklung
2	Weiterleitung des Zahlungspflichtigen zum ZV-Provider / PayPal
3	Autorisierung und Abwicklung der Zahlung beim ZV-Provider / PayPal
4	Weiterleitung des Zahlungspflichtigen zur Fachanwendung
5	Verifizierung der Zahlung durch die Fachanwendung bei ePayBL
6	Optional: Übermittlung einer Datei zum Aufbau von Sollstellung im HKR-System
7	EPA-Import über Sync-API von PayPal
8	Optional: Übermittlung eines Kontoauszuges (Einzeltransaktionen) für Aufteilung von Summengutschriften durch ePayBL
9	Belastung des PayPal Kontos des Bürgers
10	Summengutschrift an das Konto der öffentlichen Einrichtung / des Zahlungsempfängers
11	Übermittlung eines Kontoauszuges durch die Hausbank (Summengutschrift)
12	Optional: Verarbeitung des Kontoauszuges aus Schritt 8 im HKR-System zum Ausgleich von Sollstellungen
13	Optional: Zahlungsanzeige (Ist-Buchung) an ePayBL
14	Optional: Abfrage des Zahlungseingangs durch die Fachanwendung

### 4.3.3 giropay

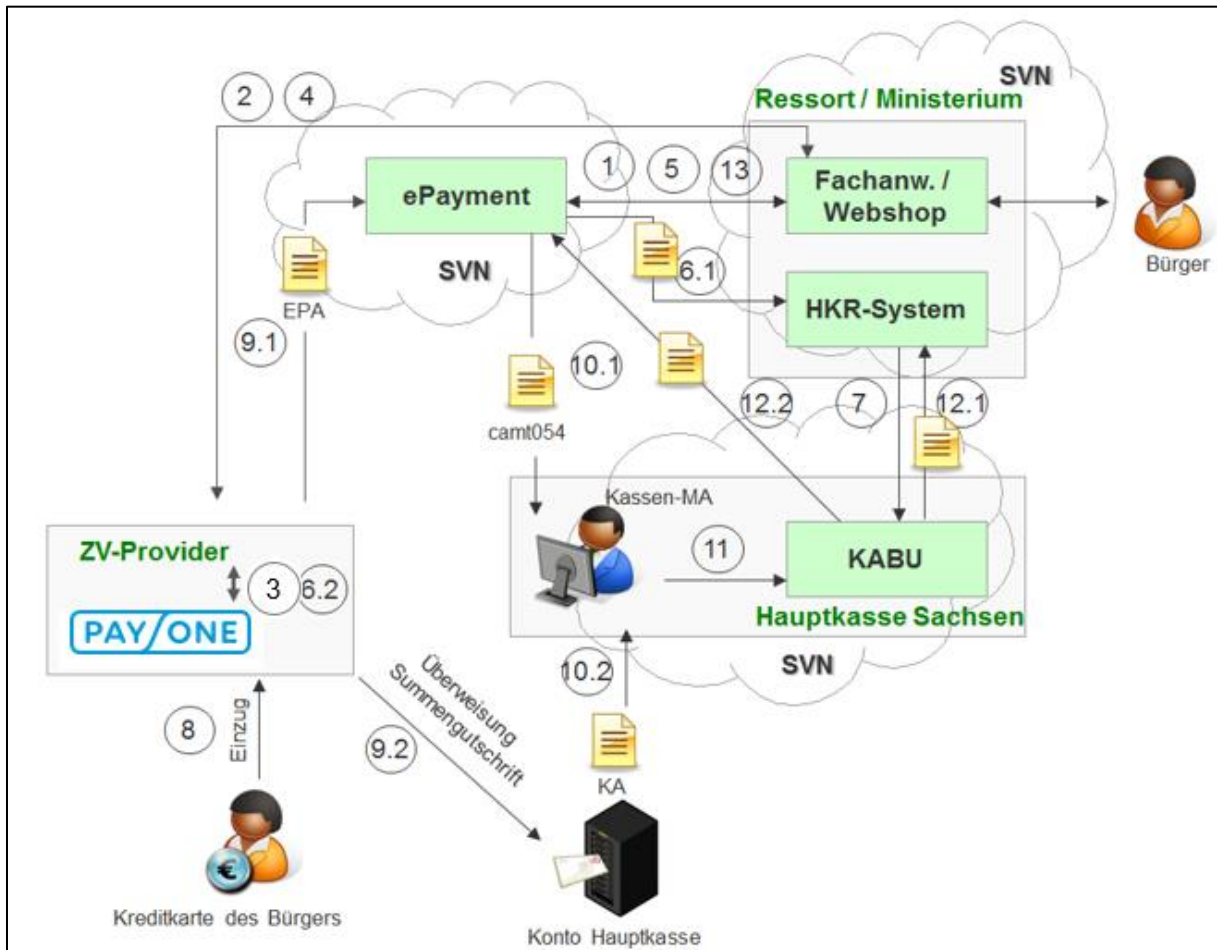


Nr. Beschreibung

1	Übermittlung der Transaktionsdaten an ePayBL und Entgegennahme der URL für die Zahlungsabwicklung
2	Weiterleitung des Zahlungspflichtigen zum ZV-Provider
3	Überweisung aus dem Online-Banking des Bürgers
4	Weiterleitung des Zahlungspflichtigen zur Fachanwendung
5	Verifizierung der Zahlung durch die Fachanwendung bei ePayBL
6	Optional: Übermittlung einer Datei zum Aufbau von Sollstellung im HKR-System
7	Übermittlung eines Kontoauszuges durch die Hausbank
8	Optional: Verarbeitung des Kontoauszuges aus Schritt 7 im HKR-System zum Ausgleich von Sollstellungen
9	Optional: Zahlungsanzeige (Ist-Buchung) an ePayBL
10	Optional: Abfrage des Zahlungseingangs durch die Fachanwendung

## 4.4 Geschäftsprozesse - Landesverwaltungen mit Konto der Hauptkasse

### 4.4.1 Kreditkarte



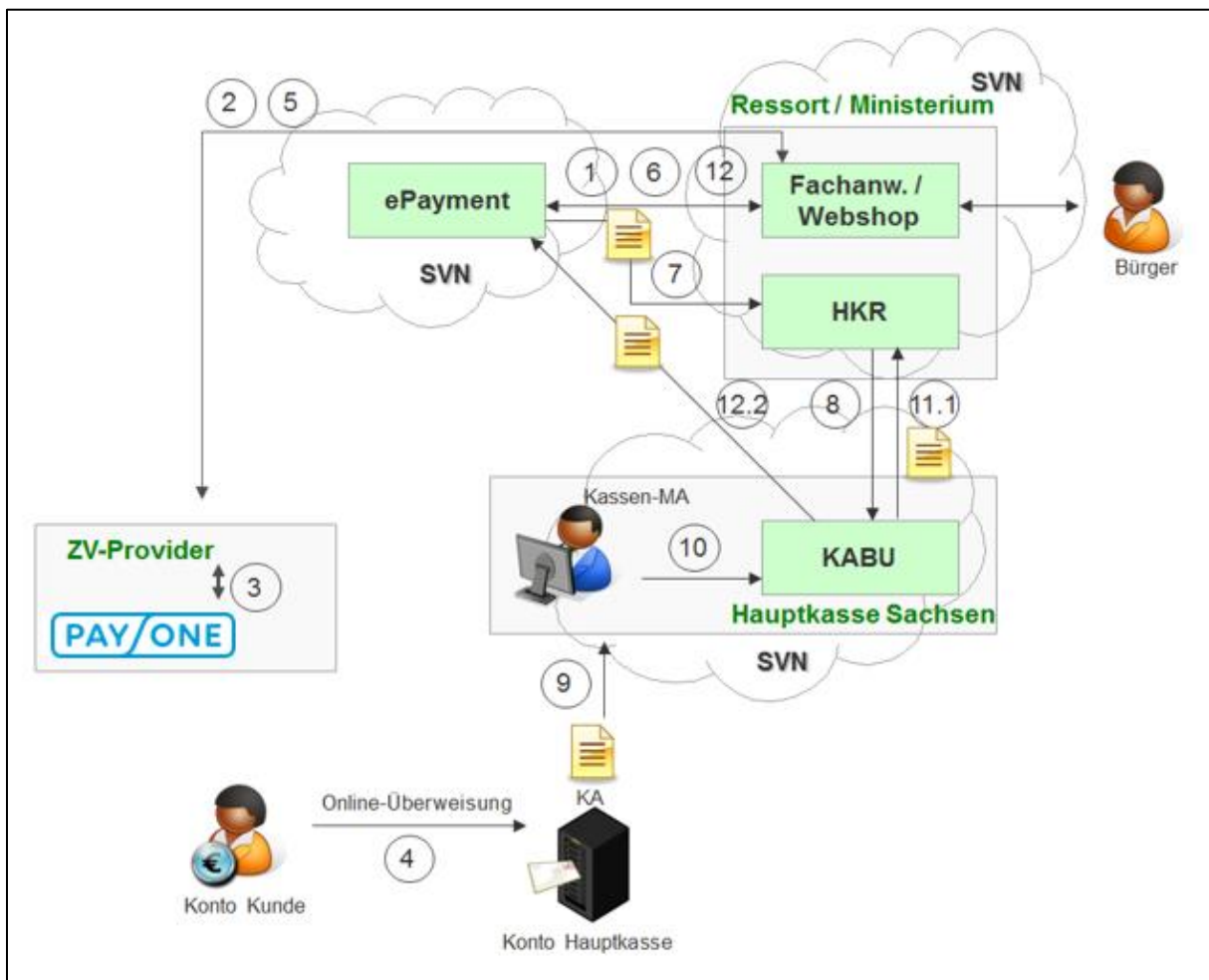
Nr.	Beschreibung
1	Übermittlung der Transaktionsdaten an ePayBL und Entgegennahme der URL für die Zahlungsabwicklung
2	Weiterleitung des Zahlungspflichtigen zum ZV-Provider
3	Autorisierung und Abwicklung der Zahlung beim ZV-Provider
4	Weiterleitung des Zahlungspflichtigen zur Fachanwendung
5	Verifizierung der Zahlung durch die Fachanwendung bei ePayBL (Kassenzeichen als „bezahlt“ kennzeichnen)
6	Übermittlung der HKR-Datei zum Aufbau der Sollstellung (6.1), Verarbeitung der Transaktionen beim ZV-Provider (6.2)
7	Aufbau der Sollstellung im HKR-System
8	Belastung der Kunden-Kreditkarte

9	Übermittlung der EPA (Electronic Payment Advice = Transaktionsübersicht) (9.1) an ePayBL, Gutschrift an das Konto der Hauptkasse (9.2)
10	Übermittlung der KA-Datei (Kontoauszug)
11	Import der camt054-Datei zum Ausgleich der Sollstellung
12	Zahlungsanzeige an HKR und ePayBL
13	Abfrage des Zahlungseingangs durch die Fachanwendung

#### 4.4.2 PayPal

PayPal ist als Zahlverfahren für die Öffentliche Verwaltung mit Konto bei der Hauptkasse nicht freigegeben.

#### 4.4.3 giropay



Nr.	Beschreibung
1	Übermittlung der Transaktionsdaten an ePayBL und Entgegennahme der URL für die Zahlungsabwicklung

2	Weiterleitung des Zahlungspflichtigen zum ZV-Provider
3	Weiterleitung des Kunden an sein Online Banking
4	Überweisung seitens des Kunden und Rückmeldung an den Webshop / die Fachanwendung
5	Weiterleitung des Zahlungspflichtigen zur Fachanwendung
6	Verifizierung der Zahlung durch die Fachanwendung bei ePayBL (Kassenzeichen als „bezahlt“ kennzeichnen)
7	Übermittlung der HKR-Datei zum Aufbau der Sollstellung
8	Aufbau der Sollstellung im HKR-System
9	Übermittlung der KA-Datei (Kontoauszug)
10	Import der KA-Datei im HKR-System zum Ausgleich der Sollstellung
11	Zahlungsanzeige an HKR-System und ePayBL
12	Abfrage des Zahlungseingangs durch die Fachanwendung

## 5 Anleitungen

### 5.1 Beantragung von Zertifikaten

Um in der ePayBL ein Zertifikat beantragen zu können, stehen folgende URLs zur Verfügung.

- Testsystem: <https://zvnis.egov.sachsen.de/paycert>
- Produktivsystem: <https://zvn.egov.sachsen.de/paycert>



sachsen.de E-Government

Herzlich willkommen! Bitte tragen Sie Ihre Mandant-Nummer ein:

**Mandant-Nummer**

[Weiter zum Antrag](#)

[Impressum](#)

Geben Sie Ihre Mandant-Nummer ein und klicken Sie auf [Weiter zum Antrag]

Füllen Sie die Felder entsprechend der Bezeichnung aus und klicken Sie dann auf [Abschicken]. Folgend finden Sie Beispiele, wie Sie den Antrag für Zertifikate ausfüllen können.

## Zertifikatsantrag

Bitte füllen Sie alle Felder aus und betätigen dann den Button 'Abschicken'.

Mandant-Nummer	<input type="text" value="B000000"/>
Vorname (Antragsteller)	<input type="text"/>
Nachname (Antragsteller)	<input type="text"/>
Vorname (Besitzer)	<input type="text"/>
Nachname (Besitzer)	<input type="text"/>
Abteilung (DN-Teil: OU)	<input type="text" value="BaKZVis"/>
Organisation (DN-Teil: O)	<input type="text"/>
Ort (DN-Teil: L)	<input type="text"/>
Bundesland (DN-Teil: ST)	<input type="text"/>
Land (DN-Teil: C)	<input type="text"/>
E-Mail	<input type="text"/>
Passwort	<input type="password"/>
Wiederholung	<input type="password"/>
Zertifikatszweck	<input type="text" value="Bitte auswählen..."/>
Typ	<input type="text" value="Bitte auswählen..."/>

Bezeichnung	Persönliches Browser-Zertifikat	Browser- Gruppenzertifikat	Webservice- Zertifikat
Mandant-Nummer	B000000	B000000	B000000
Vorname (Antragsteller)	Max	Max	Max
Nachname (Antragsteller)	Muster	Muster	Muster
Vorname (Besitzer)	Max	ePayBL	ePayBL
Nachname (Besitzer)	Muster	Shop	Shop

Abteilung	## vorausgefüllt	## vorausgefüllt	## vorausgefüllt
Organisation	Saechsische Informatik Dienste	GRP: Saechsische Informatik Dienste	Fachverfahrenshersteller
Ort	Dresden	Dresden	Dresden
Bundesland	Sachsen	Sachsen	Sachsen
Land	DE	DE	DE
E-Mail	zv@sid.sachsen.de	zv@sid.sachsen.de	zv@sid.sachsen.de
Passwort	*****	*****	*****
Zertifikatszweck	Browser-Zertifikat	Browser-Zertifikat	Webservice-Zertifikat
Typ	Personengebunden es Zertifikat	Gruppenzertifikat	Gruppenzertifikat

Der angegebene Besitzer des Zertifikats muss in der ePayBL als Nutzer angelegt sein. Dieser wird anhand der Mandantenkonfiguration durch die Anwendungsbetreuung in der ePayBL angelegt.

Bitte beachten Sie, dass an die angegebene E-Mail-Adresse ein Link zur Abholung Ihres Zertifikates versendet wird. Weiterhin werden Sie über diese E-Mail-Adresse kurz vor Ablauf Ihres Zertifikates darüber informiert, wie lange es noch gültig ist.

Das Passwort wird später für den Download und die Installation des Zertifikats benötigt. Bitte merken Sie sich das angegebene Passwort daher gut.

Für den Zertifikatszweck gibt es die Auswahl zwischen „Browser-Zertifikat“ und „Webservice-Zertifikat“. Wählen Sie das entsprechende Zertifikat aus. Bei Browser-Zertifikaten haben Sie die Möglichkeit, zwischen Gruppenzertifikaten und personengebundenen Zertifikaten zu wählen.

Für das Produktivsystem müssen immer personengebundene Zertifikate beantragt werden. Bei Testsystemen ist es möglich, ein Gruppenzertifikat zu beantragen, welches dann von mehreren Personen genutzt werden darf.

Nach einem Klick auf [Abschicken] wird der Antrag eingereicht. Sie bekommen eine Bestätigungsmeldung für das erstellte Zertifikat.



## 5.2 Installation von Browser-Zertifikaten

Die Anwendungsbetreuung des Zahlungsverkehrs erhält eine E-Mail über den neu erstellten Zertifikatsantrag.

Nach der Prüfung des Antrags und der Genehmigung des Zertifikats erhalten Sie eine E-Mail mit einem Downloadlink. Sollte der Antrag abgelehnt werden, erhalten Sie eine E-Mail mit entsprechender Begründung.

Sehr geehrte(r) Browser Zertifikat,

Ihr neues Zertifikat für den Mandanten B000000 - Zentrale Dienste wurde aktiviert. Klicken Sie auf die folgende URL, um das Zertifikat herunterzuladen:

<https://zvnis.egov.sachsen.de/paycert/zertifikatsdownloadentry.do?zertifikatsantragId=3002>

Verwenden Sie dazu das Passwort, das bei der Zertifikatsantragstellung festgelegt wurde.

Besitzer des Zertifikates: SID AWB

Mit freundlichen Grüßen  
Ihre ePayment-Betreuung

-----  
Diese Nachricht wurde automatisch durch das System generiert.

Nach dem Anklicken des Links gelangen Sie auf die Seite für den Zertifikatsdownload. Als Passwort muss das Passwort eingegeben werden, welchen Sie zuvor beim Antrag selbst festgelegt haben. Klicken Sie dann auf [Weiter zum Herunterladen].

sachsen.de E-Government

Zertifikatsdownload

Bitte melden Sie sich für den Download mit Ihrem beim Antrag gewählten Passwort an.

ZertifikatsantragId

Passwort

Weiter zum Herunterladen

Mit dem Button [User-Zertifikat importieren] haben Sie die Möglichkeit, das beantragte Zertifikat direkt in den Browser zu importieren. Folgen Sie dafür den Schritten im Kapitel Direkter Import von Zertifikaten.

Durch sich immer ändernde Sicherheitsanforderungen bei den Browsern kann es sein, dass der direkte Import nicht möglich ist. Nutzen Sie in diesem Fall die Schaltfläche [User-Zertifikat herunterladen]. Folgen Sie dafür den Schritten im Kapitel Manueller Import von Zertifikaten.

## Zertifikatsdownload

Hallo *SID AWB*, das beantragte Zertifikat steht zum Download bzw. Import bereit.

User-Zertifikat   Root-Zertifikat

Wenn der Import nicht erwartungsgemäß funktioniert...

Arbeiten Sie sich in folgenden Schritten durch das Browser-Menü, um das heruntergeladene User-Zertifikat in Chrome zu importieren:

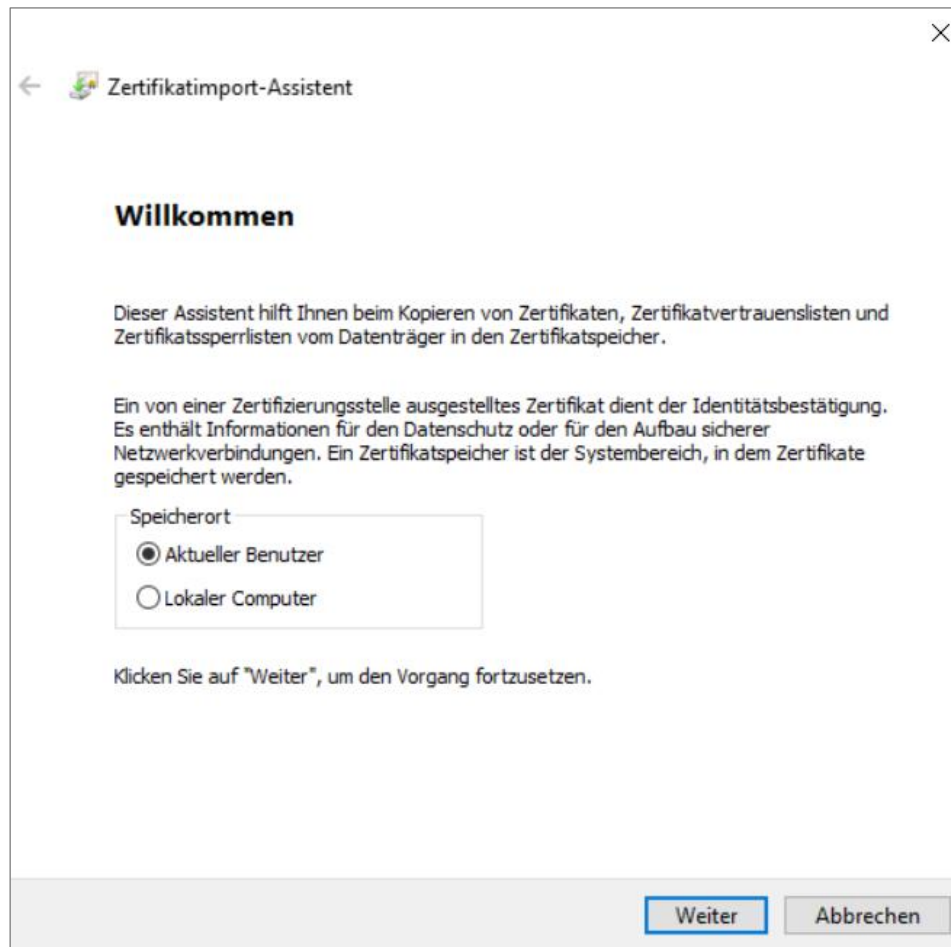
1. Einstellungen
2. Erweiterte Einstellungen anzeigen *(Link)*
3. Zertifikate verwalten *(Button)*
4. Eigene Zertifikate *(Registrierkarte)*
5. Importieren *(Button)*
6. Weiter *(Button)*
7. Durchsuchen *(Button)*
8. Datei öffnen
9. Passwort eingeben
10. Alle Zertifikate in folgendem Speicher speichern *(Option)*
11. Weiter *(Button)*
12. Fertig stellen *(Button)*

User-Zertifikat herunterladen   User-Zertifikat importieren

Anwendung verlassen

### 5.2.1 Direkter Import von Zertifikaten [User-Zertifikat importieren]

Folgen Sie für den Import dem Assistenten und klicken Sie auf [Weiter].



Klicken Sie der nächsten Seite „zu importierende Datei“ auf [Weiter].

Geben Sie das bei der Beantragung festgelegte Passwort ein und setzen Sie Häkchen bei „Schlüssel als exportierbar markieren“ und „Alle Eigenschaften einbeziehen“. Klicken Sie dann auf [Weiter].

← Zertifikatimport-Assistent

**Schutz für den privaten Schlüssel**

Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.

Geben Sie das Kennwort für den privaten Schlüssel ein.

Kennwort:

●●●●●●●●●●

Kennwort anzeigen

Importoptionen:

Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert.

Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.

Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar)

Alle erweiterten Eigenschaften mit einbeziehen

Weiter Abbrechen

Klicken Sie auf der nächsten Seite „Zertifikatsspeicher“ auf [Weiter].

Klicken Sie auf der darauffolgenden Seite auf [Fertigstellen].

Es kann vorkommen, dass Sie beim Fertigstellen des Assistenten eine Sicherheitswarnung bekommen. Diese müssen Sie mit „Ja“ bestätigen.

Die Root-Zertifikate für die ePayBL-Systeme lauten wie folgt:

Testsystem: ePayBL-CA-zvnis

Produktivsystem: ePayBL-CA-zvn

### 5.2.2 Manueller Import von Zertifikaten

Wenn Sie das Zertifikat zuerst herunterladen möchten, öffnet sich das Fenster für das Speichern des Zertifikats. Speichern Sie dieses auf Ihrem PC ab.

Importieren Sie anschließend das Zertifikat in den von Ihnen genutzten Browser.

### 5.3 Nutzung des GiroCockpit

Nach der Einrichtung Ihres Accounts beim Zahlungsverkehrsprovider erhalten Sie die Zugangsdaten für Ihr GiroCockpit. Darin können Sie Ihre Rechnungen sowie deren rechnungsbegründenden Unterlagen und alle Transaktionen, die über Ihren Account abgewickelt wurden, einsehen sowie Kreditkarten-Zahlungen stornieren.

#### 5.3.1 Abruf der Projektdaten zur Einrichtung in der ePayBL

**Schritt 1:** Melden Sie sich mit Ihren Zugangsdaten unter der URL <https://www.girocockpit.de/> am GiroCockpit an.

Sie befinden sich nun auf dem Startbildschirm des GiroCockpits. Über den Button „**Hilfe**“ gelangen Sie zum Handbuch des GiroCockpits, das Ihnen die Funktionen umfänglich erläutert. Das ausführliche Handbuch kann ebenfalls über die URL <http://wiki.girocockpit.de/introduction:start> aufgerufen werden.

**Schritt 2:** Im Bereich „Meine Projekte“ sehen Sie für jedes Zahlverfahren, das Sie beim Zahlungsverkehrsprovider beantragt haben (Kreditkarte, giropay und/oder PayPal), ein sogenanntes „Projekt“ (Achtung: die Bezeichnung der Projekte weicht vom Screenshot ab). Klicken Sie bitte jeweils auf das Projekt-Profil und notieren Sie sich für jedes Projekt die **Projekt-ID** und das **Projekt-Passwort**. Diese Daten werden zur Eintragung in der ePayBL benötigt (Kapitel 5.4).

**Public Services**    **Mein GiroCockpit**    **Abmelden**

Hilfe   

### GiroCockpit für BaKZV\_Test - Kunden-Nr.: 3611882

Kundenkonto bearbeiten    Projekt hinzufügen    Transaktionen    Logins

**Mein Kundenkonto (3611882)**

- > Stammdaten
- > Unternehmen

**Mein Vertrag**

- > GiroCheckout

**Meine Projekte**

- > **BaKZV-GP**
  - > **Profil**
  - > Aktuelle Transaktionen
  - > Archivierte Transaktionen
  - > Preise
  - > Rechnungsanlagen
- > BaKZV-LS
- > BaKZV-KK
- > BaKZV-PP

**BaKZV-GP**

**Projekteinstellungen**

[Projekt bearbeiten](#)

**Zahlungsart**    giropay  
**Projekt-Status**    TEST (**Testdaten anzeigen**)

**Bankverbindung**

**Kontoinhaber**    Hauptkasse  
**Kontonummer**  
**Bankleitzahl**

**Einstellungen für die Shop-Integration**

**Verkäufer-ID**    3611882  
**Projekt-ID**    11363  
**Projekt-Passwort**    [REDACTED]

### 5.3.2 Stornierung von Kreditkartenzahlungen

Sollten Sie eine Kreditkartentransaktion stornieren müssen, wählen Sie unter „Transaktionen“ die jeweilige Transaktion aus. In der Detailansicht kann der Betrag über den Button „Credit“ gutgeschrieben werden.

#### Transaktionsdetails

Zahlungsart	Kreditkarte
Transaktionsart	Verkauf
GiroCheckout Referenz	
Backend ID	
Verkäufer Tx-ID	
Verwendungszweck	
Datum	13.08.2021 09:04:11
Betrag	20,00 EUR
Status	Transaktion erfolgreich (4000)
<b>▼ Pseudokarten Information</b>	
Pseudokartennummer	
Karteninhaber	
Kartennummer	
Ablaufdatum	
<b>▼ Verlauf</b>	
<ul style="list-style-type: none"> <li>• 13.08.2021 09:04:11   Verkauf   20,00 EUR   <span style="background-color: black; color: black;">XXXXXXXXXX</span>   Transaktion erfolgreich (4000)</li> </ul>	
<b>▼ Gutschrift über Projekt Kreditkarte-CHB</b>	
<p><b>Betrag *</b></p> <input style="width: 100%; border: 1px solid #ccc;" type="text" value="20,00"/>	
<input style="border: none; border-radius: 15px; padding: 5px 20px; background-color: #ccc; cursor: pointer;" type="button" value="Credit"/>	

Erstattete Transaktionen sind in der Übersicht aller Transaktionen unter dem Menüpunkt „Erweiterte Suche“ / „Projekte“ / „Kreditkarte CHB“ einsehbar.

## 5.4 Hinterlegung der Account-Daten des Zahlungsverkehrsproviders

Für die Test- und Abnahmephase wird ein ePayBL-Mandant im Testsystem angelegt. In diesem Testmandanten sind bereits alle nötigen Konfigurationen und Testprojektdaten des Zahlungsverkehrsproviders durch die Anwendungsbetreuung Zahlungsverkehr hinterlegt worden.

Um aber mit produktiven ePayBL-Mandanten im späteren Livebetrieb bestimmte Bezahlverfahren anbieten zu können, ist es nötig unter dem Menüpunkt ZV-Providerpflege die Daten des ZV-Providers (Projekt-ID und –Passwort, siehe [Kapitel 5.3.1](#)) zu hinterlegen.

Für Hinterlegung der Daten des ZV-Providers im ePayBL-Portal gibt es für die einzelnen Zahlverfahren verschiedene Vorgehensweisen:

### 5.4.1 Kreditkarte und / oder giropay

Bitte halten Sie für alle folgenden Schritte die Projekt-IDs und zugehörigen Passwörter aus dem GiroCockpit bereit.

**Schritt 1:** Bitte rufen Sie das Portal der ePayBL unter der URL <https://zvn.egov.sachsen.de/portal> auf und loggen sich mit Ihren Zugangsdaten ein.

**Schritt 2:** Wechseln Sie in der Navigation am linken Bildschirmrand in das Menü „ZV-Providerpflege“ und in das Untermenü „GiroSolution“.

The screenshot shows the ePayBL portal interface. The left navigation menu has 'ZV-Providerpflege' highlighted with a red box and arrow labeled '1'. The main content area shows 'GiroSolution Einstellungen' with a table for provider data. The table has columns for 'Zahlungsart', 'Projekt-ID', and 'Projekt-Passwort'. Red arrows point to the 'Projekt-ID' field for Giropay (labeled '2'), the 'Projekt-Passwort' field for Giropay (labeled '3'), the 'Projekt-ID' field for Kreditkarte (labeled '4'), and the 'Speichern' button (labeled '5').

Zahlungsart	Projekt-ID	Projekt-Passwort
Giropay	11363	.....
Kreditkarte	11364	.....
PayPal		
Lastschrift		

Verwendungszweck: [Bewirtschafternummer]/[Kassenzeichen]

Speichern



**Schritt 3:** Tragen Sie nun für jedes beauftragte Zahlverfahren die Projekt-ID und das zugehörige Projekt-Passwort aus dem GiroCockpit (Schritt 2) ein.

**Schritt 4:** Klicken Sie anschließend auf „Speichern“.

Sie haben die Einrichtung von GiroCheckout nun erfolgreich abgeschlossen. Ihre Kunden können ab sofort mit Kreditkarte und/oder giropay via GiroCheckout bezahlen. Im GiroCockpit können Sie in jedem Projekt über das Menü „Aktuelle Transaktionen“ die Zahlvorgänge einsehen.

## 5.4.2 PayPal

**Schritt 1:** Um PayPal nutzen zu können, müssen Sie ein Händlerkonto bei PayPal erstellen.

**Schritt 2:** Um die im ePayBL Portal benötigten Daten (SOAP-Parameter) zu erhalten, muss ein API-Zugriff verfügbar sein. Dieser wird direkt im PayPal-Händlerkonto unter "Kontoeinstellungen" im Abschnitt "Kontozugriff" einmalig angelegt. Klicken Sie dazu bei "API-Zugriff" auf den Link "Bearbeiten".

The screenshot shows the 'Kontoeinstellungen' (Account Settings) page. On the left is a navigation menu with categories like 'Konto und Sicherheit', 'Unternehmensprofil', and 'Produkte und Dienstleistungen'. The 'Kontozugriff' option is highlighted with a yellow box. The main content area is titled 'Kontozugriff' and contains a list of settings:

Category	Description	Action
<b>Login mit PayPal</b>	Websites, bei denen Sie sich mit PayPal eingeloggt haben.	<a href="#">Ändern</a>
<b>API-Zugriff</b>	Nutzen Sie unsere APIs, um PayPal in Ihren Online-Shop oder Warenkorb zu integrieren.	<a href="#">Bearbeiten</a>
<b>Nutzer verwalten</b>	Verwalten Sie zusätzliche Nutzer, die Zugriff auf Ihr Konto haben.	<a href="#">Bearbeiten</a>
<b>Sicherer FTP-Server</b>	Sicherer FTP-Server	<a href="#">Bearbeiten</a>
<b>Dienstanbieter</b>	Verwalten Sie Drittanbieter-Tools, die Sie in Ihrem PayPal-Konto für die Datenübertragung hinterlegt haben.	<a href="#">Anzeigen</a>
<b>Limits</b>	Limits für Ihr Konto.	<a href="#">Anzeigen</a>
<b>Zusätzliche Genehmigungen überspringen für schnellere Zahlungen</b>	Genehmigen Sie Zahlungen in weniger Schritten, wenn Sie diese Kontakte und Firmen bezahlen.	<a href="#">Verwalten</a>

**Schritt 3:** Im Anschluss öffnet sich der Unterbereich "Berechtigung für Ihre Zahlungs-API". Relevant ist hier nun unten der Abschnitt "NVP/SOAP-API-Integration (klassisch)".


### Berechtigung für Ihre Zahlungs-API

Um PayPal-Zahlungen auf Ihrer Website zu akzeptieren, benötigen Sie bzw. Ihr Entwickler eine API-Berechtigung. Über eine API (Application Programming Interface) kann PayPal mit Ihrem Online-Shop oder Warenkorb kommunizieren.

[Mehr erfahren](#) über PayPal-APIs

---

Wie ist PayPal auf Ihrer Website integriert?



#### PayPal-API

Über einen Warenkorbanbieter

##### Vorkonfigurierte Zahlungslösung

Wenn Sie eine Plattform von Drittanbietern, beispielsweise Magento oder Shopify, für Warenkörbe und Online-Shops verwenden oder verwenden möchten, in denen der PayPal-Zahlungsservice bereits integriert ist

[API-Genehmigung erteilen](#) oder [API-Genehmigung verwalten](#)

Benutzerdefinierte Kaufabwicklung

##### Integration des Braintree-SDK

Das Braintree-SDK wurde von Braintree, einem Service von PayPal, entwickelt. Die SDKs lassen sich leicht integrieren und ermöglichen Ihnen, mit PayPal Zahlungen über Ihre Website und Ihre Apps zu empfangen.

[SDK-Berechtigung verwalten](#)

##### NVP/SOAP-API-Integration (klassisch)

Sie oder Ihr Entwickler haben NVP/SOAP- (oder "klassische") APIs integriert, um PayPal-Zahlungen empfangen zu können.

[API-Berechtigung verwalten](#)

**Schritt 4:** Hier wird eine zentrale API-Berechtigung erstmalig angelegt und mit "API-Berechtigung verwalten" verwaltet. Beim Klick darauf öffnet sich die Seite "API-Signatur anzeigen oder entfernen"



**Schritt 6:** Für die Ansicht / Konfiguration der REST-API Credentials (REST-Parameter) öffnen Sie die Seite <https://developer.paypal.com>. Nach Anmeldung wählen Sie oben rechts „Entwickler“ aus.

The screenshot shows the top navigation bar of the PayPal Developer website. The 'Entwickler' (Developer) link is highlighted with a yellow box. Below the navigation bar, the main content area displays 'PayPal Commerce Platform for Business' with a 'CURRENT' status tag. The left sidebar contains a 'DEVELOPER RESOURCES' section with links like 'Get Started', 'Develop', and 'JavaScript SDK'.

**Schritt 7:** Auf der sich dann öffnenden Seite im Bereich Developer klicken Sie auf "APIs".

The screenshot shows the 'APIs' section of the PayPal Developer website. The 'APIs' link in the top navigation bar is highlighted with a yellow box. In the left sidebar, under 'REST APIS', the 'Get Credentials' link is also highlighted with a yellow box. The main content area shows 'Get Started' with a 'CURRENT' status tag and introductory text about setting up a development environment.

**Schritt 8:** Im linken Bereich dann die Auswahl "Get Credentials". In dem Textabschnitt den angezeigten Link auswählen "Log in to the Developer Dashboard".

**REST APIS**

**Get Started**

- Get Credentials
- Get an Access Token
- Make REST API Calls
- Create Sandbox Accounts
- PayPal Security Guidelines
- Rate Limiting Guidelines

API REFERENCE

## Get credentials

To generate REST API credentials for the sandbox and live environments:

1. **Log in to the Developer Dashboard** with your PayPal account.
2. Under the **DASHBOARD** menu, select **My Apps & Credentials**.
3. Make sure you're on the Sandbox tab to get the API credentials you'll use while you're developing code. After you test and before you go live, switch to the Live tab to get live credentials.
4. Under the **App Name** column, select **Default Application**, which PayPal creates with a new Developer Dashboard account. Select **Create App** if you don't see the default app.

**Note:** To get credentials for the [Marketplaces and Platforms](#) product, see that [Get Started](#) page.

**Schritt 9:** Dort unter "My Apps & Credentials" "Live" auswählen. Über den Button „Create App“ muss für die ePayBL eine neue App (beispielsweise „ePayBL-EPA“) erzeugt werden, damit die ePayBL über die in der App hinterlegten REST-Parameter mit der ePayBL kommunizieren kann.

**DASHBOARD**

**My Apps & Credentials**

My Account

**SANDBOX**

- Accounts
- Notifications
- API Calls
- IPN Simulator
- Webhooks Events

**MOCK**

Webhooks Simulator

## My apps & credentials

Sandbox **Live**

### REST API apps

Create an app to receive REST API credentials for testing and live transactions.

App name	Actions
ePayBL-EPA	
ePayBLTestLHD	

**Create App**

**Note:** Features available for live transactions are listed in your [account eligibility](#).

**Schritt 10:** Nach Auswahl dieser angelegten App öffnet sich mit Klick auf den App Namen die Ansicht der Credentials (PayPal account / Client ID / Secret).

PayPal Developer Docs APIs Tools Support PayPal.com

DASHBOARD

**My Apps & Credentials**

My Account

SANDBOX

Accounts

Notifications

API Calls

IPN Simulator

Webhooks Events

MOCK

Webhooks Simulator

Credit Card Generator

Negative Testing

LIVE

## ePayBL-EPA

App display name: ePayBL-EPA

LIVE API CREDENTIALS

Note that not all features are available for live transactions. Features available for live transactions are listed in your account eligibility.

PayPal account:

**Client ID:**

**Secret:**  [Show](#)

**Schritt 11:** Die Daten zu Client ID und Secret sind dann ebenso im ePayBL-Mandant unter PayPal-Einstellungen / REST-Parameter einzutragen.

### PayPal Accountdaten

<b>Mandant</b>	TESTMK - Test mit Konnektor
<b>Bewirtschafter</b>	MK - Mit Konnektor <span style="float: right;">v</span>

### SOAP-Parameter

Händleraccountname *	zv5_api1.sid.sachsen.de
Händleraccountpasswort *	●●●●●●●●
Händleraccount API-Signatur *	AFcWxV21C7fd0v3bYYRCpSS

### REST-Parameter

Client-ID *	AaH8gIPO-kyXKydkCuomkgF_9
Secret *	●●●●●●●●●●●●●●●●●●●●●●●●

## 5.5 OSCI – Transport

Der technische Standard Online Services Computer Interface (OSCI) ermöglicht den elektronischen Austausch von Nachrichten und Dokumenten mit besonders hohen Sicherheitsanforderungen innerhalb und mit der öffentlichen Verwaltung. OSCI wird im Auftrag des IT-Planungsrates von der Koordinierungsstelle für IT-Standards (KoSIT) betrieben und ist als Standard für die Kommunikation mit Behörden verbindlich. Der OSCI-Transport eignet sich für alle Anwendungsfälle der Übertragung vertraulicher Daten/Dokumente, bei denen es einer elektronischen Signatur bedarf. Durch den Einsatz von OSCI kann sichergestellt werden, dass Daten nicht verändert und nur berechtigte Personen bzw. Verfahren Zugriff haben.

### 5.5.1 Voraussetzung für die Nutzung von OSCI

Die Adressierung und Verschlüsselung von Nachrichten erfolgen über Zertifikate. Diese Zertifikate können mit Hilfe der ePayBL erzeugt werden und müssen anschließend an den Bewirtschaftern in der ePayBL bzw. dem OSCI-Client hinterlegt werden. Folgende Zertifikate sind für die OSCI-Kommunikation bei den Kommunikationspartner (ePayBL und OSCI-Client) jeweils notwendig:

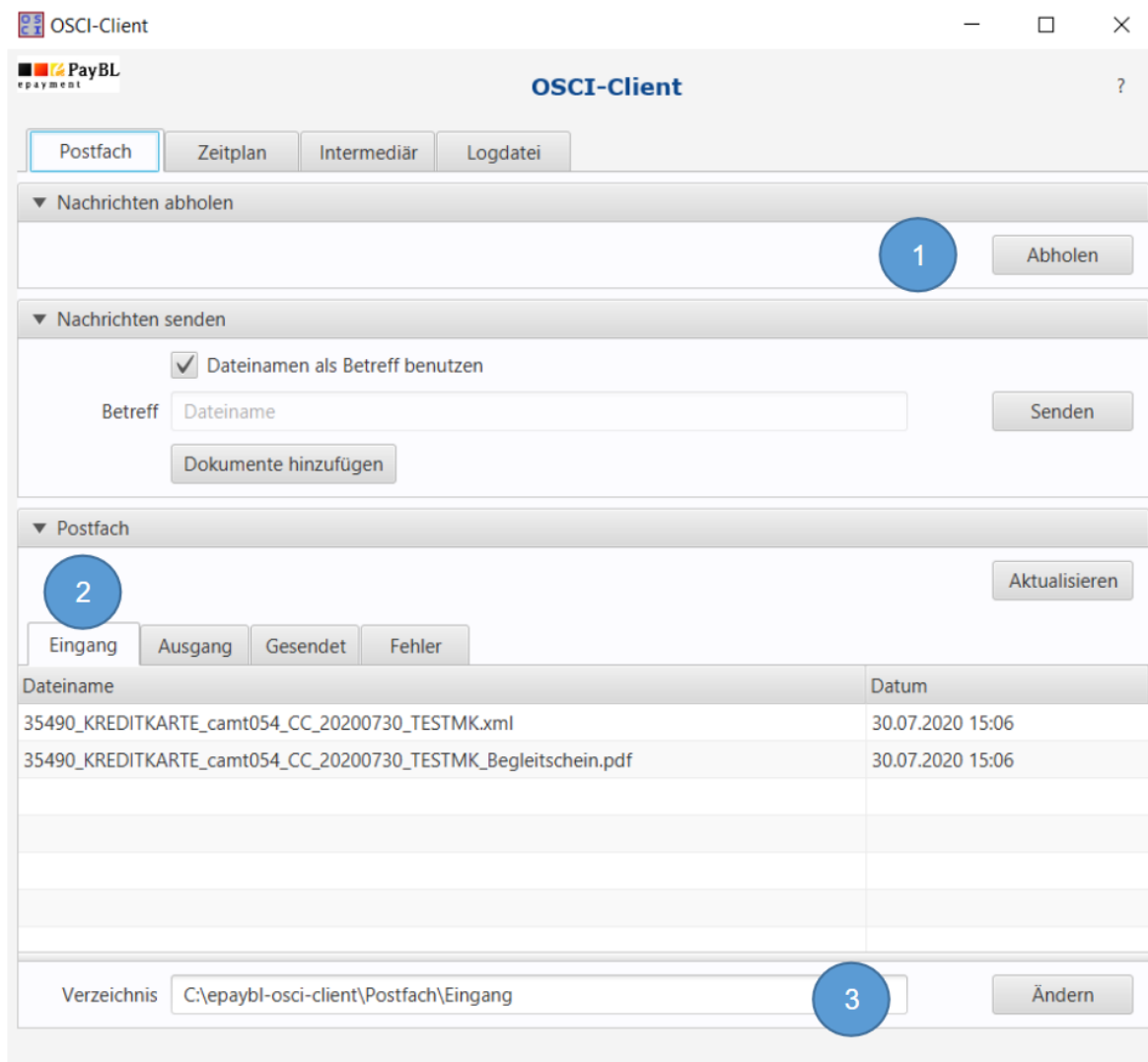
- Absender-Zertifikat: identifiziert den Sender
- Empfänger-Zertifikat: identifiziert den Empfänger

#### **Hinweis:**

Wird der OSCI-Client der ePayBL verwendet, werden die betreffenden Zertifikate bereits fest eingebunden und müssen nach der Bereitstellung des Clients an den Kommunikationspartner nicht mehr geändert werden

### 5.5.2 Empfang von Daten

Der Empfang von Daten, die die ePayBL über den Intermediär bereitgestellt hat (z.B. camt.054-Dateien), erfolgt entweder manuell über den Reiter „Postfach“ oder über einen automatischen Abholdienst. Über dieses Verzeichnis ist der Zugriff auf die übermittelten Dateien zur Weiterverarbeitung in den Haushaltssystemen der Bewirtschafter möglich. Werden Daten manuell vom Intermediär abgeholt, muss im Bereich „Nachrichten abholen“ der Button „Abholen“ bestätigt werden (Nr. 1 in Abbildung 7). Wurden Nachrichten abgeholt, erscheinen die darin übermittelten Dateien entschlüsselt im Posteingang (Nr. 2 in der Abbildung) mit Dateinamen und Datum der Abholung. Die physische Ablage der übermittelten Dateien erfolgt im konfigurierten Ablageverzeichnis auf dem zentralen oder lokalen PC, auf dem der OSCI-Client installiert wurde (Nr. 3 in der Abbildung).





### 5.5.3 Automatisierter Abruf

Für den automatisierten Abruf durch den OSCI – Client, kann ein Zeitintervall eingestellt werden. Über den Reiter „Zeitplan“ muss dazu festgelegt werden, in welchem Rhythmus die Abholung erfolgen soll (Nr. 4 in der Abbildung). Die automatische Abholung kann auch nur in einem bestimmten Zeitfenster aktiviert werden (Nr. 5 in der Abbildung). Standardmäßig ist die automatische Abholung deaktiviert. Um sie zu aktivieren, muss der Status entsprechend gesetzt werden (Nr. 6 in der Abbildung).

OSCI-Client

PayBL  
epayment

OSCI-Client

Postfach Zeitplan Intermediär Logdatei

Modus

stündlich  
 täglich  
 wöchentlich  
 monatlich  
 Intervall: alle 7 Tage

Bitte geben Sie eine Zahl im Wertebereich [1-365] ein.

Zeit

	Datum	Stunde	Minute
Start	29.10.2020	08	50
Ende	29.10.2020	10	50

Status der automatischen Ausführung

Status: Deaktiviert Aktivieren Deaktivieren

## 6 Wichtige Links

Inhalt	Link
Nutzungsbedingungen	<a href="#"><u>Nutzungsbedingungen BaK ZV</u></a>
Abruf-Formular	<a href="#"><u>Abruf ZVP</u></a>
Zahlungsverkehrsprovider- dienstleistungen	
Testsystem Zertifikats- Beantragung	<a href="https://zvnis.egov.sachsen.de/paycert"><u>https://zvnis.egov.sachsen.de/paycert</u></a>
Testsystem ePayBL-Portal	<a href="https://zvnis.egov.sachsen.de/portal"><u>https://zvnis.egov.sachsen.de/portal</u></a>
Testsystem Webservice-URL	<a href="https://zvnis.egov.sachsen.de"><u>https://zvnis.egov.sachsen.de</u></a>
Testdaten für Testzahlungen	<a href="https://api.girocheckout.de/girocheckout:testdata"><u>https://api.girocheckout.de/girocheckout:testdata</u></a>
Produktivsystem Zertifikats- Beantragung	<a href="https://zvn.egov.sachsen.de/paycert"><u>https://zvn.egov.sachsen.de/paycert</u></a>
Produktivsystem ePayBL-Portal	<a href="https://zvn.egov.sachsen.de/portal"><u>https://zvn.egov.sachsen.de/portal</u></a>
Produktivsystem Webservice-URL	<a href="https://zvn.egov.sachsen.de"><u>https://zvn.egov.sachsen.de</u></a>
Beantragung Newsletter	<a href="https://login.mailingwork.de/-optin-form/30355/1/CHwIT"><u>https://login.mailingwork.de/-optin- form/30355/1/CHwIT</u></a>
Abrufformular Bezahlterminals	<a href="#"><u>Abruf Bezahlterminals</u></a>

## 7 Glossar

Begrifflichkeit	Bedeutung
Bewirtschafternummer	Nummer, die zur eindeutigen Zuordnung in der ePayBL dem Fachverfahren zugewiesen wird. Diese wird zudem im Verwendungszweck bei giropay-Zahlungen in der Kombination [Bewirtschafternummer]/[Kassenzeichen] mit angegeben.
camt.054-Datei	Detaillierte Anzeige und Aufschlüsselung von Sammelbuchungen
EPA (Electronic Payment Advice)	Datei mit detaillierten Zahlungsinformationen in Bezug auf Zahlungen mit Kreditkarte
Fachverfahren	IT-Unterstützung für die Beantragung und Durchführung von Dienstleistungen der Verwaltung
HKR	Haushalts-, Kassen- und Rechnungswesen

KABU	Kassenbuchführungs-Verfahren bei der Hauptkasse
Kassenzeichen	Eindeutige Codierung zur Identifikation von Zahlungen in der Buchhaltung
Magento	Hochkonfigurierbares, modulares und quelloffenes Webshop-System
OSCI	Ermöglicht den elektronischen Austausch von Nachrichten und Dokumenten mit besonders hohen Sicherheitsanforderungen innerhalb und mit der öffentlichen Verwaltung
RE-Nummer	Rechnungsnummer
SVN	Sächsisches Verwaltungsnetz
VU-Nummer	Vertrags-Unternehmens-Nummer
Webservice-Zertifikat	Zertifikat der ePayBL für den Zugriff des Fachverfahrens auf die ePayBL
ZV-Provider	Zahlungsverkehrsprovider

## 8 Checkliste

Abkürzungen der Verantwortlichkeiten: M = Mandant, FVH = Fachverfahrenshersteller, AWB = Anwendungsbetreuung Zahlungsverkehr

### 8.1 Vorbereitung und Vorüberlegung vor dem Erstgespräch

Verantwortlichkeit Prozessschritt

M	<ul style="list-style-type: none"> <li>• Skizzierung des Ist-Prozesses und Planung für Soll-Prozess</li> <li>• Klärung, welches Fachverfahren angebunden werden soll</li> </ul>
M, FVH	Erste Kontaktaufnahme und Vorabinformation an den Fachverfahrenshersteller zur späteren Anbindung der ePayBL an das Fachverfahren. Eine Zusammenarbeit zur Einrichtung des Webservice-Zertifikats ist in ca. einem Monat zwingend notwendig.

### 8.2 Erstgespräch mit dem SID

Vorlauf: ca. 2-4 Wochen

Umfang des Termins: ca. 1h

Verantwortlichkeit Prozessschritt

M	Besprechungstermin zu ePayBL mit dem SID vereinbaren
M	Teilnahme am Vorstellungstermin zur ePayBL

### 8.3 Vertragsabschluss

Verantwortlichkeit Prozessschritt

M	Nutzungsbedingungen zustimmen ( <a href="#">Kapitel 3.2.1</a> , Link siehe <a href="#">Kapitel 6</a> )
M	Abruf Zahlungsserviceproviderdienstleistung ( <a href="#">Kapitel 3.2.2</a> ) unter folgendem <a href="#">Link</a> . ( <u>nach positiver Rückmeldung des Kundenmanagements</u> )
	Vorlauf bei Payone: ca. 12 Wochen
AWB	Prüfung und Genehmigung des Antrags

M	<p>genehmigten und unterzeichneten Antrag mit unterzeichneter Behördenbestätigung per E-Mail an <u><a href="mailto:Kundenservice-SID@payone.com">Kundenservice-SID@payone.com</a></u> senden</p> <p>Durchführung Identifizierung der unterzeichnenden Person</p> <p><b>Hinweis:</b> Im Testmandanten sind bereits alle nötigen Konfigurationen und Testprojektdaten des ZV-Providers hinterlegt worden. Die Beantragung in diesem Schritt ist für das Produktivsystem.</p>
---	--

#### 8.4 Klärung Geschäftsprozesse zur Umsetzung mit ePayBL

Vorlauf: ca. 2-4 Wochen

Umfang des Termins: ca. 1-2h

Verantwortlichkeit Prozessschritt

M	<p>Besprechungstermin zur Abstimmung der Geschäftsprozesse mit SID vereinbaren</p> <p>Folgende Teilnehmer des zukünftigen Mandanten sollten anwesend sein:</p> <ul style="list-style-type: none"> <li>○ Fachverfahrensverantwortlicher</li> <li>○ Haushalt</li> <li>○ IT-Abteilung</li> <li>○ Projektleitung</li> </ul>
M, AWB	<p>Besprechen von Ist-/Soll-Prozess Ausfüllen der Mandantenkonfiguration / Antrag Zahlungsverkehrsprovider-Dienstleistung Fragenklärung</p>

#### 8.5 Umsetzung

Verantwortlichkeit Prozessschritt

AWB	<p>Nach positiver Rückmeldung durch das Kundenmanagement erfolgt die Einrichtung des ePayBL-Testmandanten:</p> <p>Einrichtung des ePayBL-Testmandanten und Versand der notwendigen Informationen zur Anbindung an die ePayBL via E-Mail an den Mandant zur Weiterleitung an den Fachverfahrenshersteller</p>
-----	--

M	<p>Webservice-Zertifikat für das Testsystem beantragen und herunterladen unter dem <a href="#">Link</a> (<a href="#">Kapitel 5.1</a>)</p>
M, FVH	<p>Übermittlung von Webservice-Zertifikat und aller Daten an Fachverfahrenshersteller zur Entwicklung der ePayBL-Schnittstelle:</p> <ul style="list-style-type: none"> <li>• Webservice-Zertifikat Testsystem</li> <li>• Passwort Webservice-Zertifikat</li> <li>• <a href="#">Webservice-URL Testsystem</a></li> <li>• Daten zum Testmandanten</li> <li>• vom SID übermittelte Handbücher</li> </ul>
M, FVH	<p>Der Mandant entscheidet über die Art der Anbindung des Fachverfahrens:</p> <ul style="list-style-type: none"> <li>• Direkt-Integration im Fachverfahren oder</li> <li>• über die ePayBL-Paypage.</li> </ul> <p>Fachverfahren an die ePayBL anbinden: Der Fachverfahrenshersteller bindet das Fachverfahren an die ePayBL gemäß Konnektor-Integrationsbuch an. Durchführung von Testzahlungen durch den Fachverfahrenshersteller.</p>
M	Termin zum Abnahmetest (Vorlaufzeit ca. 4 Wochen) mit SID abstimmen
M, FVH, AWB	<p>Abnahmetest durchführen</p> <p>Innerhalb des gemeinsamen Termins mit dem SID werden vier Testfälle durchgeführt:</p> <ol style="list-style-type: none"> <li>1. Eine erfolgreiche Zahlung je Zahlverfahren mit Rückkehr in das Fachverfahren</li> <li>2. Eine erfolgreiche giro-pay-Zahlung mit Schließen des Browser-Fensters ohne Rückkehr in das Fachverfahren</li> <li>3. Eine erfolgreiche Zahlung mit vorherigem Wechsel des Zahlverfahrens</li> <li>4. Abbruch der Zahlung auf der Bezahlseite des Zahlungsverkehrsproviders</li> </ol>
AWB	Freigabe zur Produktivsetzung des Verfahrens, wenn alle Testfälle erfolgreich durchgeführt werden konnten

## 8.6 Betrieb

Verantwortlichkeit	Prozessschritt
AWB	Überführung des Mandanten in das Produktivsystem
M	<p>Webservice-Zertifikat für das Produktivsystem beantragen und herunterladen unter dem <a href="#">Link</a> (<a href="#">Kapitel 5.1</a>)</p>

M	Übermittlung von Webservice-Zertifikat und aller Daten an den FVH: <ul style="list-style-type: none"> <li>• Webservice-Zertifikat Produktivsystem</li> <li>• Passwort Webservice-Zertifikat</li> <li>• <u>Webservice-URL Produktivsystem</u></li> </ul>
M	Hinterlegung der Zahlungsverkehrsprovider-Daten (Projekt-ID, Projekt-Passwort) je Zahlverfahren in der ePayBL ( <u>Kapitel 5.4</u> )
FVH	Umstellung des Fachverfahrens in den Produktivbetrieb
M	Beantragung der Browser-Zertifikate durch die Nutzer des ePayBL-Portals ( <u>Kapitel 5.1</u> )
M	Mitteilung des Produktivsetzungstermins an die AWB
M	Optional: Durchführung produktiver Testzahlungen zur Sicherstellung, dass die Zahlungsverkehrsprovider-Daten korrekt hinterlegt wurden
M, FVH	Produktivsetzung des Verfahrens