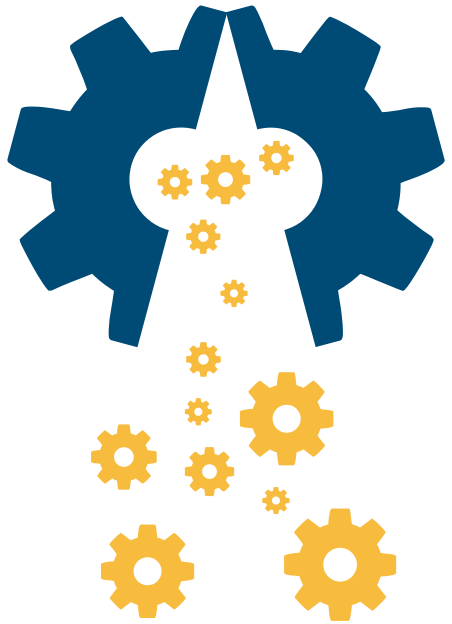
IT-Sicherheitsverordnung Portalverbund – ITSiV-PV

Arbeitshilfe im Digitalisierungsprogramm Föderal
Stand: 20.07.2023

OZG
Onlinezugangsgesetz

Die ITSiV-PV definiert Maßnahmen zur Aufrechterhaltung der Informationssicherheit bei der Umsetzung des Onlinezugangsgesetzes

ITSiV-PV: Einordnung



Die Vorgaben der ITSiV-PV fußen auf § 5 Satz 1 des OZG und finden in dessen Zuständigkeitsbereich Anwendung.

1. Der Portalverbund bildet die **Verbindung zwischen Verwaltung, Bürgerinnen und Bürgern sowie Organisationen** im Internet.

2. Durch die Vernetzung des Portalverbunds sowie die Abhängigkeit der Komponenten im fachlichen Prozess, ergibt sich ein **Verbundrisiko, welches besonders adressiert werden muss**.

3. Die zentralen Komponenten des Portalverbunds müssen angemessen gegen IT-Sicherheitsrisiken abgesichert sein. Der **Bund ist zur Festlegung der erforderlichen Mindeststandards hierfür** ermächtigt.

4. Risiko-Owner für die Informationssicherheit ist **die jeweilige für den Betrieb verantwortliche Stelle** (Bund/Land/Kommune).

Der Portalverbund beinhaltet mehr IT-Komponenten als nur das Online-Gateway (PVOG)

Definition Portalverbund

IT-Sicherheitsverordnung Portalverbund – ITSiV-PV

§ 1 (Begriffsbestimmungen)

„Portalverbund“ ist nach § 2 Absatz 1 OZG eine technische Verknüpfung der Verwaltungsportale von Bund und Ländern, über die der Zugang zu Verwaltungsleistungen auf unterschiedlichen Portalen angeboten wird.

IT-Komponenten im Portalverbund sind IT-Anwendungen, Basisdienste und Schnittstellen, die für den Betrieb des Verbundes und für die Abwicklung der Verwaltungsleistungen im Portalverbund erforderlich sind. Dazu zählen u. a. das Online Gateway des Portalverbundes, die interoperablen Nutzerkonten von Bund und Ländern mit elektronischen Postfächern, das Datenschutzcockpit, der Datensafe, der elektronische Bezahldienst und die Suchfunktion

Der Portalverbund ist die Summe der zentralen IT-Komponenten, welche zum Online-Zugang von Verwaltungsleistungen erforderlich sind

Zur Differenzierung der Mindestvorgaben der Absicherung unterscheidet die ITSiV-PV in unmittelbar und mittelbar angebundene Komponenten

Differenzierung mittelbar und unmittelbar angebunden

	Mittelbar angebundene Komponenten	Unmittelbar angebundene Komponenten
Einstufung der Sicherheitsrisiken	Komponenten, deren Angriff/Ausfall ein geringeres Risiko für den Zugang zu Verwaltungsleistungen bedeutet	Komponenten, deren Angriff/Ausfall ein erhebliches Risiko für den Zugang zu Verwaltungsleistungen bedeutet
ITSiV-PV	Ein geringeres Risiko ergibt sich, wenn die Komponenten keine technische Schnittstelle zum Portalverbund besitzen, bzw. deren Daten nicht unmittelbar in den Prozess zur Beantragung der Verwaltungsleistung einfließen (nachgelagerte Prozesse)	Ein erhebliches Risiko ergibt sich, wenn die Komponenten eine technische Schnittstelle Portalverbund besitzen, deren Daten unmittelbar in den Kernprozess der Beantragung der Verwaltungsleistung einfließen (Kernprozess Online-Zugang)

Die Differenzierung beruht auf der fachlichen Abhängigkeit der jeweiligen Komponente und den Risiken, welche auf die Komponente wirken.

Für unmittelbar angebundene Komponenten sind besondere Anforderungen an die Absicherung zu gewährleisten

Absicherung der Komponenten

Mittelbar angebundene Komponente	**Unmittelbar angebundene** Komponente

• Sicherheitskonzept nach IT-Grundschutz
  • Basis-Absicherung 200-2
  • (BSI-Standards 200-1, 200-2 und 200-3)
• Alternativ: Vergleichbarer Standard des Landes
	• Technische Maßnahmen nach dem Stand der Technik
	  • Standards in Form von Technischen Richtlinien des BSI [1]
	  • BSI TR-03160 Servicekonten
	  • BSI TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1
	  • BSI TR-03147 Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen
	  • BSI TR-03116-4 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4
	  • Evtl. weitere technische Richtlinien, die gem. § 2 Abs. 3 ITSiV-PV verbindlich werden.
	• Sicherheitskonzept nach IT-Grundschutz
	  • Umsetzung BSI-Standards 200-1, 200-2 und 200-3 oder ISO 27001
	  • Mindestniveau: Standard-Absicherung nach BSI-Standard 200-2
	• Web-Checks / Pentest
	• Notfallmanagement

[1] Siehe Anlage zur ITSiV-PV

Für IT-Komponenten im Portalverbund ist zusätzlich die Einreichung einer Eigenerklärung verpflichtend

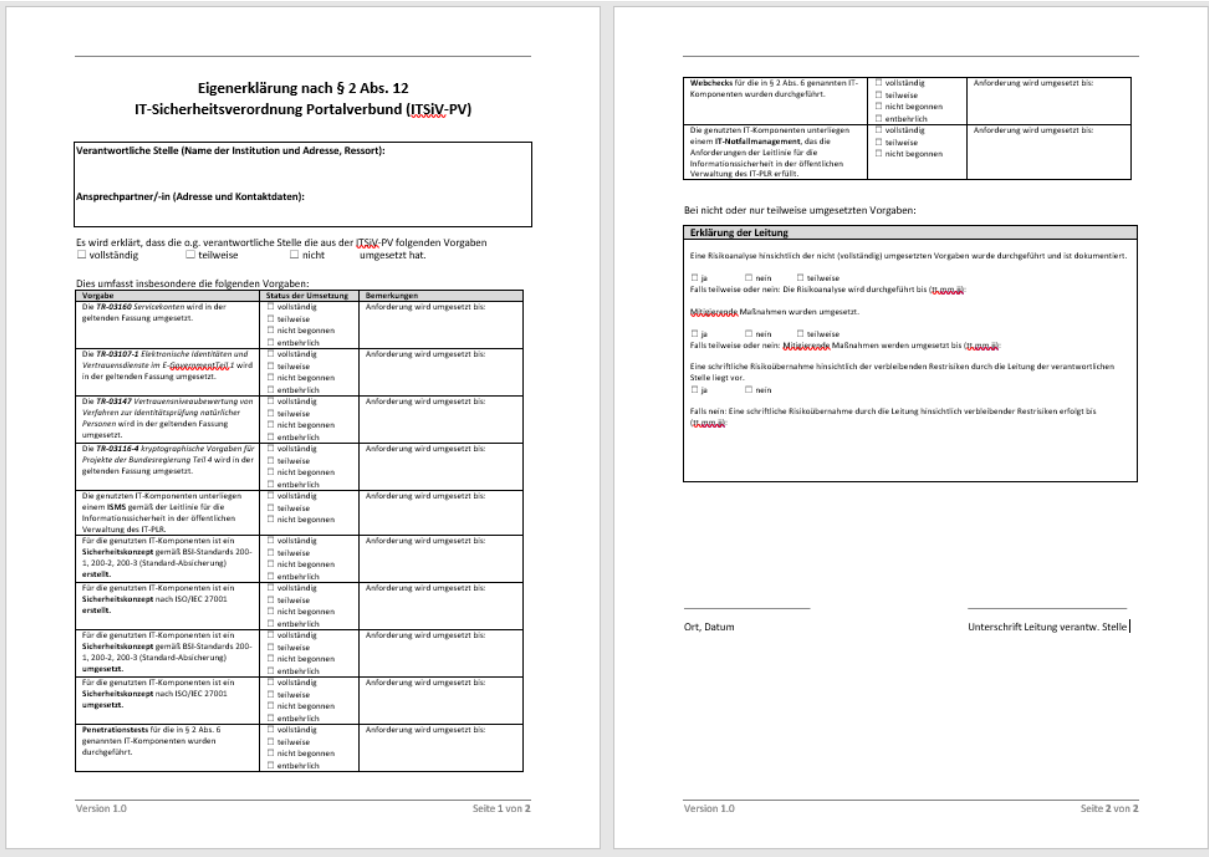
Darstellung Eigenerklärungen

Eigenerklärung

Nur Notwendig für IT-Komponenten im Portalverbund. Dazu zählen u. a. das Online Gateway des Portalverbunds, die interoperablen Nutzerkonten von Bund und Ländern mit elektronischen Postfächern, das Datenschutzcockpit, der Datensafe, der elektronische Bezahldienst und die Suchfunktion.

Verantwortliche Stellen in den Ländern hinterlegen die Eigenerklärung jährlich bis **zum** 01.01. bei der **jeweiligen zentralen Stelle des Landes.**

Muster Eigenerklärung unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Oeffentliche_Verwaltung/Eigenerklaerung_IT-Sicherheitsverordnung_PVV.html



Eigenerklärung nach § 2 Abs. 12
IT-Sicherheitsverordnung Portalverbund (ITSiV-PV)

Verantwortliche Stelle (Name der Institution und Adresse, Ressort):

Ansprechpartner/-in (Adresse und Kontaktdaten):

Es wird erklärt, dass die o.g. verantwortliche Stelle die aus der ITSiV-PV folgenden Vorgaben
☐ vollständig ☐ teilweise ☐ nicht umgesetzt hat.

Dies umfasst insbesondere die folgenden Vorgaben:

Vorgabe	Status der Umsetzung	Bemerkungen
Die ***TR-03160*** *Servicekonten* wird in der geltenden Fassung umgesetzt.	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	Anforderung wird umgesetzt bis:
Die ***TR-03107-1*** *Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1* wird in der geltenden Fassung umgesetzt.	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	Anforderung wird umgesetzt bis:
Die ***TR-03147*** *Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen* wird in der geltenden Fassung umgesetzt.	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	Anforderung wird umgesetzt bis:
Die ***TR-03116-4*** *kryptographische Vorgaben für Projekte der Bundesregierung Teil 4* wird in der geltenden Fassung umgesetzt.	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	Anforderung wird umgesetzt bis:
Die genutzten IT-Komponenten unterliegen einem **ISMS** gemäß der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-PLR.	☐ vollständig ☐ teilweise ☐ nicht begonnen	Anforderung wird umgesetzt bis:
Für die genutzten IT-Komponenten ist ein **Sicherheitskonzept** gemäß BSI-Standards 200-1, 200-2, 200-3 (Standard-Absicherung) **erstellt.**	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	Anforderung wird umgesetzt bis:
Für die genutzten IT-Komponenten ist ein **Sicherheitskonzept** nach ISO/IEC 27001 **erstellt.**	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	Anforderung wird umgesetzt bis:
Für die genutzten IT-Komponenten ist ein **Sicherheitskonzept** gemäß BSI-Standards 200-1, 200-2, 200-3 (Standard-Absicherung) **umgesetzt.**	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	Anforderung wird umgesetzt bis:
Für die genutzten IT-Komponenten ist ein **Sicherheitskonzept** nach ISO/IEC 27001 **umgesetzt.**	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	Anforderung wird umgesetzt bis:
Penetrationstests für die in § 2 Abs. 6 genannten IT-Komponenten wurden durchgeführt.	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	Anforderung wird umgesetzt bis:

Version 1.0 Seite 1 von 2

Webchecks für die in § 2 Abs. 6 genannten IT-Komponenten wurden durchgeführt.	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	Anforderung wird umgesetzt bis:
Die genutzten IT-Komponenten unterliegen einem **IT-Notfallmanagement**, das die Anforderungen der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-PLR erfüllt.	☐ vollständig ☐ teilweise ☐ nicht begonnen	Anforderung wird umgesetzt bis:

Bei nicht oder nur teilweise umgesetzten Vorgaben:

Erklärung der Leitung

Eine Risikoanalyse hinsichtlich der nicht (vollständig) umgesetzten Vorgaben wurde durchgeführt und ist dokumentiert.

☐ ja ☐ nein ☐ teilweise
Falls teilweise oder nein: Die Risikoanalyse wird durchgeführt bis (tt.mm.jjjj)

Mitigierende Maßnahmen wurden umgesetzt.

☐ ja ☐ nein ☐ teilweise
Falls teilweise oder nein: Mitigierende Maßnahmen werden umgesetzt bis (tt.mm.jjjj)

Eine schriftliche Risikoübernahme hinsichtlich der verbleibenden Restrisiken durch die Leitung der verantwortlichen Stelle liegt vor.
☐ ja ☐ nein

Falls nein: Eine schriftliche Risikoübernahme durch die Leitung hinsichtlich verbleibender Restrisiken erfolgt bis (tt.mm.jjjj)

Ort, Datum

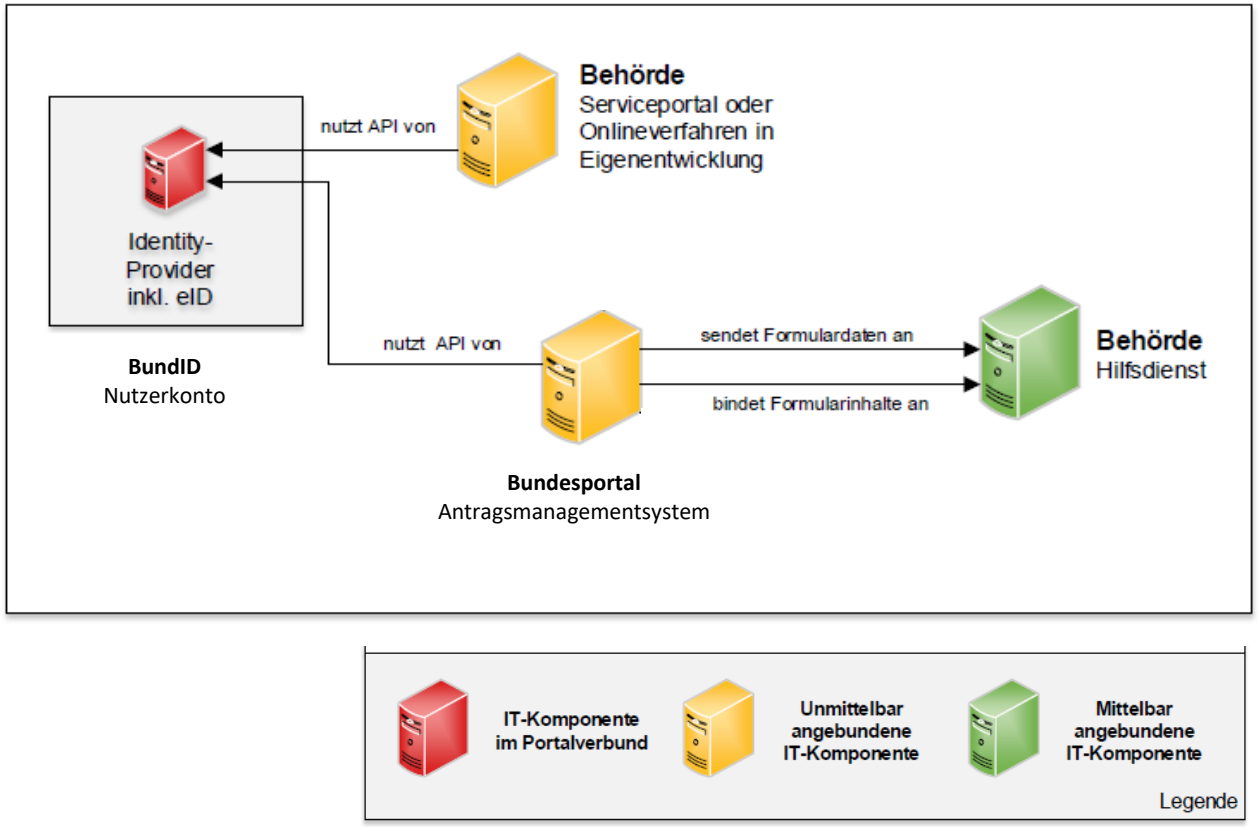
Unterschrift Leitung verantw. Stelle

Version 1.0 Seite 2 von 2

Exemplarische Einstufung eines „typischen“ OZG-Onlinedienstes

Anbindung an Nutzerkonto als Identity-Provider

Systemarchitektur



Prototypische Einstufung

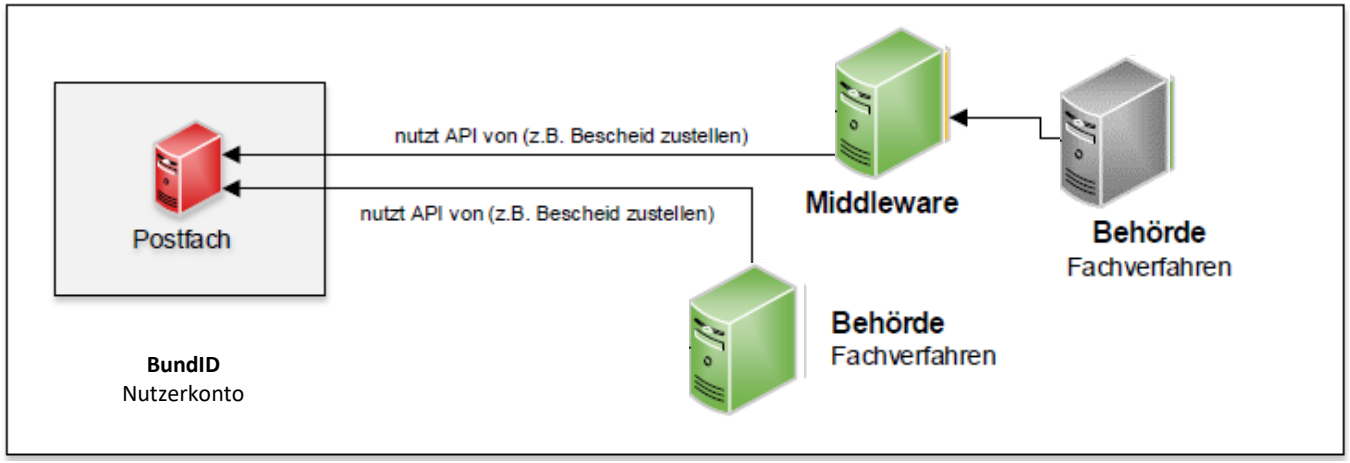
Nutzerkonten von Bund und Ländern sind Komponenten **im Portalverbund (+ Eigenerklärung erforderlich).**

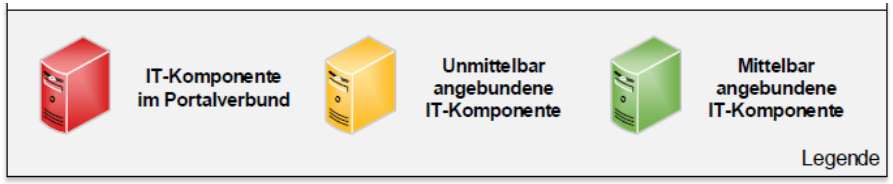
Der Onlinedienst mit technischer Schnittstelle zum Nutzerkonto ist eine **unmittelbar** angebundene Komponente. Dies erfordert für den Onlinedienst eine Umsetzung der Anforderungen nach §2 ITSiV-PV (u.a. Standardabsicherung IT-Grundschutz, Web-Checks, Pentest). Eine Eigenerklärung ist für unmittelbar angebundene Komponenten **nicht** notwendig.

Exemplarische Einstufung eines Fachverfahrens

Anbindung an das Nutzerkonto Postfach

Systemarchitektur





Prototypische Einstufung

Fachverfahren sind grundsätzlich nicht Teil des OZG. Sie unterliegen jedoch indirekt den Vorgaben der ITSiV-PV, sofern sie an Komponenten des Portalverbundes oder unmittelbar angebundene Komponenten angebunden sind. Dies ist beispielsweise der Fall, wenn Fachverfahren an das Postfach der BundID, oder an das Bundesportal angebunden sind.

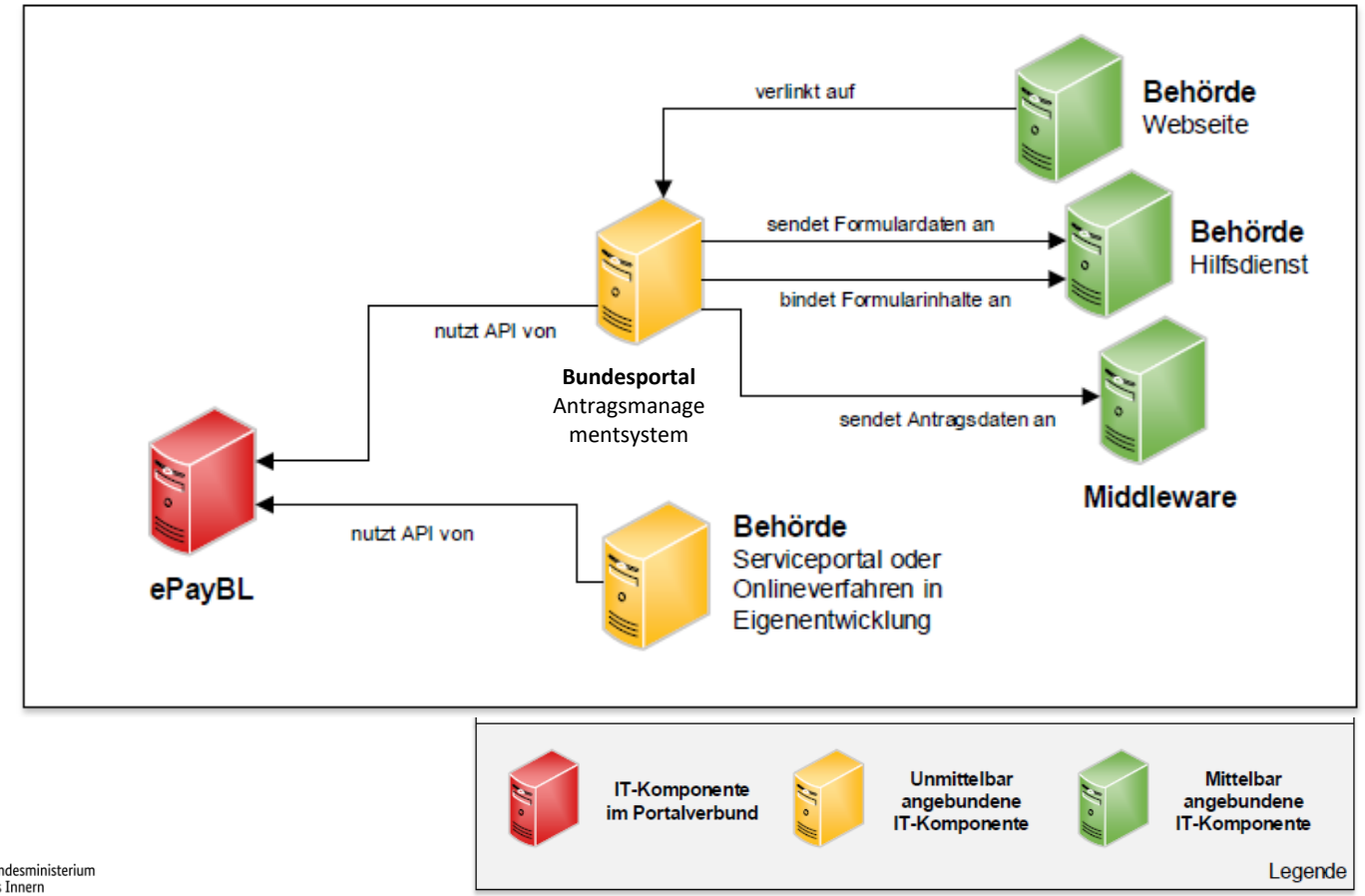
Das BMI/BSI stufen **Fachverfahren als mittelbar angebunden ein[1],** d.h. Mindestanforderung wäre die Umsetzung des §3 der ITSiV PV (Basisabsicherung IT-Grundschutz). Eine Eigenerklärung ist für mittelbar angebundene Komponenten **nicht** notwendig.

[1] **Besonderheit:** Wenn das Fachverfahren dasselbe System wie der Onlinedienst benutzt, dann zählen die höheren Anforderungen (unmittelbar).

Exemplarische Einstufung einer Komponente des Portalverbundes (ePayment als Teil des Portalverbundes)

Anbindung an Bezahlkomponente ePayBL

Systemarchitektur



Prototypische Einstufung:

Die Paymentkomponente ist Teil des Portalverbundes.

Komponenten mit technischer Schnittstelle sind **unmittelbar** angebundene Komponenten.

Daher Standardabsicherung BSI Grundschutz, Einhaltung techn. Richtlinien, Notfallmanagement, (Webchecks, Pentests), Eigenerklärung **notwendig**.

FAQ zur ITSiV-PV

Stand: 20.04.2023

Frage	Antwort
Worauf fußt die ITSiV-PV und wo findet diese Anwendung?	Die Vorgaben der ITSiV-PV fußen auf §5 Satz 1 des OZG und finden im Zuständigkeitsbereich des Portalverbundes Anwendung. Der in der Verordnung bezeichnete „Portalverbund“ ist nach § 2 Absatz 1 OZG eine technische Verknüpfung der Verwaltungsportale von Bund und Ländern, über die der Zugang zu Verwaltungsleistungen auf unterschiedlichen Portalen angeboten wird.
Wann handelt es sich um Komponenten **im Portalverbund?**	IT-Komponenten im Portalverbund sind zentrale IT-Anwendungen, Basisdienste und Schnittstellen, die für den Betrieb des Verbundes und für die Abwicklung der Verwaltungsleistungen im Portalverbund erforderlich sind. Dazu zählen u. a. das Online Gateway des Portalverbunds, die interoperablen Nutzerkonten von Bund und Ländern mit elektronischen Postfächern, das Datenschutzcockpit, der Datensafe, der elektronische Bezahldienst und die Suchfunktion.
Worauf basiert die Einstufung einer mittelbaren bzw. unmittelbaren Anbindung?	Die Einstufung basiert auf der technischen Anbindung an eine Komponente des Portalverbunds sowie den sich daraus ergebenden Risiken u.a. für die Verfügbarkeit des Portalverbunds. Zudem ist bei der Einstufung zu beachten, ob die Komponente in den Zuständigkeitsbereich des OZG fällt.
Wann handelt es sich um eine **unmittelbare Anbindung**? Unterliegt diese der ITSiV-PV?	Unmittelbar an den Portalverbund angeschlossene IT-Komponenten sind Komponenten, die über technische Schnittstellen Daten unmittelbar mit dem Portalverbund austauschen. Dazu zählen z. B. die von öffentlichen Stellen betriebenen Fach- und Themenportale sowie (EfA-)Online-Dienste, die an die Nutzerkonten von Bund und Ländern angeschlossen sind. In diesem Fall ergeben sich erhöhte Sicherheitsrisiken aufgrund der Zugriffsmöglichkeiten auf Schnittstellen. Dies erfordert eine Umsetzung der Anforderungen nach **§2 ITSiV-PV.**

FAQ zur ITSiV-PV

Stand: 20.04.2023

Frage	Antwort
Wann handelt es sich um eine **mittelbare Anbindung**? Unterliegt diese der ITSiV-PV?	Eine mittelbare Anbindung an den Portalverbund liegt vor, wenn öffentliche Stellen (z. B. Kommunen) Komponenten nicht eigenverantwortlich betreiben, sondern lediglich mitnutzen und hierzu ihre IT-Systeme an sie anschließen. Beispiel: eine Kommune stellt ihre digitalen Verwaltungsleistungen in ein übergeordnetes, von einer anderen Stelle betriebenes Portal ein oder nutzt einen von einer anderen Stelle betriebenen (EfA-)Online-Dienst. Dies wird als vergleichsweise geringeres Gefährdungspotenzial eingeschätzt. Es ist demnach eine Umsetzung der Maßnahmen des **§3 ITSiV-PV** notwendig.
Sind behördenseitige Komponenten zur Sachbearbeitung (=Fachverfahren) Teil des OZG und unterliegen diese der ITSiV-PV?	Fachverfahren sind grundsätzlich nicht Teil des OZG. Sie unterliegen jedoch indirekt den Vorgaben der ITSiV-PV, sofern sie an Komponenten des Portalverbundes oder unmittelbar angebundene Komponenten angebunden sind. Dies ist beispielsweise der Fall, wenn Fachverfahren an das Postfach der BundID oder an das Bundesportal angebunden sind. Das BMI/BSI stufen Fachverfahren als mittelbar angebunden ein (wenn ausschließlich eine Schnittstelle zu Portalverbund über Postfachschnittstelle der BundID besteht), d.h. Mindestanforderung wäre die Umsetzung des §3 der ITSiV PV.
Was ist ein OZG-Onlineantrag?	Ein OZG-Onlineantrag, synonym auch nur Onlineantrag ist eine Komponente zur Online-Beantragung von Behördenleistung mit direktem Zugang durch den Endnutzer (Bürger:innen/Organisationen) via Webzugang (Browser). Dabei wir der Onlineantrag als einzelner Vorgang definiert. Zu unterscheiden ist davon ein Onlinedienst, welcher in der Definition des OZG als ein technisches System anzusehen ist.

FAQ zur ITSiV-PV

Stand: 20.04.2023

Frage	Antwort
Wann sind Eigenerklärungen notwendig?	Eigenerklärungen sind nur für Komponenten des Portalverbundes notwendig. Dazu zählen u. a. das Online Gateway des Portalverbunds, die interoperablen Nutzerkonten von Bund und Ländern mit elektronischen Postfächern, das Datenschutzcockpit, der Datensafe, der elektronische Bezahldienst und die Suchfunktion.
Wie oft sind Eigenerklärungen einzureichen?	Die Eigenerklärung ist jährlich einzureichen. Stichtag 01.01.
Wo finde ich eine Mustervorlage zur Eigenerklärung und wo ist diese Erklärung einzureichen?	Verantwortliche Stellen in den Ländern hinterlegen die Eigenerklärung bei der jeweiligen zentralen Stelle des Landes. Eine Muster-Eigenerklärung findet sich unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Oeffentliche_Verwaltung/Eigenerklaerung_IT-Sicherheitsverordnung_PVV.html
Weiterführende Informationen & Hilfsmittel	https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Online-Zugangsgesetz/IT-Sicherheitsverordnung_PVV/IT-Sicherheitsverordnung_ITSiV-PVV.html