
egvp¹.de

Teilnahme von Drittanwendungen¹ am OSCI-gestützten
elektronischen Rechtsverkehr

Anforderungen

Version 1.4 vom 30.09.2021

Status: final

¹ Drittanwendungen sind für den OSCI-gestützten Rechtsverkehr registrierte Drittprodukte (siehe www.egvp.de) oder Fachanwendungen, die ein solches Drittprodukt einbinden.

Inhaltsverzeichnis

Teilnahme von Drittanwendungen am OSCI-gestützten elektronischen Rechtsverkehr	1
1 Zielsetzung und Rahmenbedingungen	3
2 Anbindung an die existierende Infrastruktur und Schnittstellen – allgemeine Anforderungen	3
2.1 Infrastruktur	3
2.2 Schnittstellen und Verschlüsselung	4
2.3 Einrichtung eines Postfachs im SAFE-Verzeichnisdienst der Justiz, Visitenkarte	4
2.4 Mengenbegrenzungen	4
2.5 Austausch von OSCI-Nachrichten	5
3 Architektur	8
3.1 Überblick	9
3.2 OSCI-Grundlagen	9
3.3 OSCI-Rollenmodell	10
3.4 Intermediär	10
3.5 Verzeichnisdienst	11
4 XJustiz	11
5 Anlage Elemente der XJustiz-Nachricht (Anforderung 21)	12

1 Zielsetzung und Rahmenbedingungen

Mit dem „Elektronischen Gerichts- und Verwaltungspostfach“ – im Folgenden als EGVP-Infrastruktur bezeichnet – können elektronische Dokumente rechtswirksam an alle teilnehmenden Gerichte und Behörden schnell und sicher übermittelt werden.

Soweit nicht ausdrücklich abweichend ausgewiesen, gelten die folgenden Mindestanforderungen für alle Softwarelösungen, die Sende- und Empfangskomponenten für die Teilnahme an der EGVP-Infrastruktur bereitstellen (im Folgenden „Drittanwendungen“ genannt).

Dies können

- für den OSCI-gestützten Rechtsverkehr registrierte Drittprodukte (siehe www.egvp.de) oder
- Fachanwendungen, die ein solches Drittprodukt einbinden,

sein.

Die Teilnahme solcher Empfangs- und Sendesoftwarelösungen am OSCI-gestützten Rechtsverkehr setzt die Erfüllung bestimmter Anforderungen voraus.

Für die Teilnahme von sogenannten Drittprodukten am OSCI-gestützten elektronischen Rechtsverkehr sieht die BLK-AG IT-Standards ein **Registrierungsverfahren** vor. Die Anforderungen sind ausführlich auf <http://www.egvp.de/Drittprodukte/index.php> dargelegt.

Für Fachanwendungen, die ein solches Drittprodukt einbinden, sind ebenfalls jeweils bestimmte Anforderungen definiert worden. Einzelheiten geben die Institutionen/Firmen, die ein solches Drittprodukt betreiben bzw. bereitstellen, bekannt.

Die Vorgaben dieses Papiers gelten in Ergänzung der gesetzlichen Regelungen. Detailinformationen zum besonderen Behördenpostfach finden sie hier (<http://www.egvp.de/behoerdenpostfach/index.php>).

2 Anbindung an die existierende Infrastruktur und Schnittstellen – allgemeine Anforderungen

2.1 Infrastruktur

A1: Die Drittanwendung muss auf die bestehende Infrastruktur für den OSCI-gestützten elektronischen Rechtsverkehr (Intermediäre, Verzeichnisdienste) aufsetzen, ohne dass diese angepasst werden muss und sich dort - für den Betreiberverbund kostenneutral - integrieren lassen.

A2: Die Drittanwendung darf auf Dienste und Server der EGVP-Infrastruktur nur in solchen Intervallen zugreifen, welche keine Störungen des Betriebs verursachen. Es werden Zeitabstände von mindestens 15 Minuten empfohlen.

2.2 Schnittstellen und Verschlüsselung

- A3: Die Drittanwendung muss seinen Nutzern den Empfang der an sie versandten OSCI-Nachrichten ermöglichen.
- A4: Die Drittanwendung muss die Nachrichten seiner Nutzer in einer Form verschlüsseln, die gemäß OSCI-Spezifikation entschlüsselt werden kann.
- A5: Die Drittanwendung muss in der Lage sein, die für seine Nutzer von einer anderen Drittanwendung nach den folgenden Vorgaben verschlüsselten Nachrichten entgegenzunehmen und zu entschlüsseln.

2.3 Einrichtung eines Postfachs im SAFE-Verzeichnisdienst der Justiz, Visitenkarte

- A6: Sofern der SAFE-Verzeichnisdienst der Justiz genutzt wird, muss die Drittanwendung seinen Nutzern ermöglichen, sich als Nutzer zu registrieren. Das so genannte „Opting Out“ Verfahren, bei dem keine Registrierung des Nutzers erfolgt, darf nicht angeboten werden. Nachrichten dürfen nur von Identitäten, die in einem SAFE-Verzeichnisdienst registriert sind, versandt werden.
- A7: Mit der Einrichtung des Postfachs im SAFE-Verzeichnisdienst der Justiz sind die festgelegten persönlichen Daten des Nutzers zu erheben; es muss daher gewährleistet sein, dass für jeden registrierten Nutzer folgende Pflichtfelder im SAFE-Verzeichnisdienst veröffentlicht werden:
- Name
 - Strasse
 - Hausnummer
 - Postleitzahl
 - Ort

2.4 Mengenbegrenzungen

- A8: Die für EGVP jeweils geltenden aktuellen Mengenbeschränkungen sind durch die Drittanwendung technisch zu gewährleisten; sie dürfen bei der Nachrichtenerstellung nicht überschritten werden, da ansonsten eine Weiterverarbeitung nicht gewährleistet ist.

A9: Nachrichten, die den Mengenbeschränkungen genügen, müssen mit der Drittanwendung verarbeitet werden können.

A10: Die Mengengrenzungen werden in der ERV-Bekanntmachung geregelt.

2.5 Austausch von OSCI-Nachrichten

A11: Die Trennung zwischen Leser und Empfänger sowie Autor und Sender muss unterstützt werden. Dabei muss lediglich sichergestellt werden, dass der Empfang von und der Versand an Teilnehmer, die eine solche Trennung implementiert haben, möglich ist.

A12: Etwaig einschlägige in den entsprechenden Rechtsverordnungen oder Internetbekanntmachungen geregelten Anforderungen an Dateiformate sind zu beachten.

A13: Es darf nicht möglich sein, eine Nachricht mit ein und demselben Bedienschnitt an mehrere Gerichte und/oder Staatsanwaltschaften zu versenden.

A14: Unmittelbar vor jedem Versand muss geprüft werden, ob das Postfach noch in einem angebundenen SAFE-Verzeichnisdienst registriert ist.

A15: EGVP-Nachrichten dürfen nicht qualifiziert elektronisch signiert werden, da eine Nachrichtensignatur eine Containersignatur darstellt, die gemäß § 4 Abs. 2 der ERVV nicht zugelassen ist. Die Anforderung kann ab sofort und muss bis spätestens 1.11.21 umgesetzt werden.

A16: Die Länge von Dateinamen darf nur 90 Zeichen inkl. der Dateiendungen betragen. In Dateinamen dürfen nur noch alle Buchstaben des deutschen Alphabetes einschließlich der Umlaute Ä, ä, Ö, ö, Ü, ü und ß genutzt werden. Zudem dürfen alle Ziffern und die Zeichen „Unterstrich“ und „Minus“ genutzt werden. Punkte sind nur als Trenner zwischen dem Dateinamen und der Dateinamenserweiterung zulässig. Nur bei konkatenierten Dateinamenserweiterungen, z.B. bei abgesetzten Signaturdateien, dürfen Punkte auch im Dateinamen genutzt werden (z.B. Dokument1.pdf.pkcs7). Die Anforderung kann ab sofort und muss bis spätestens 1.11.21 umgesetzt werden.

A17: Innerhalb des Nachrichtencontainers (project_coco oder vhn_coco) darf kein Text übermittelt werden (kein Nachrichtentext). Die Anforderung kann ab sofort und muss bis spätestens 1.11.21 umgesetzt werden.

A18: In ein- und derselben EGVP-Nachricht dürfen keine Anhänge mit vollständig identischen Dateinamen versandt werden.²

A19: Alle Nachrichten, die über einen sicheren Übermittlungsweg versandt werden, müssen entweder den VHN oder den VHN 2 enthalten. Der VHN 2 kann ab Einführung des eBO angebracht werden.

A20: Sobald alle Teilnehmer des ERV auf den VHN 2 umgestellt haben, müssen alle Nachrichten den VHN 2 enthalten. Einzelheiten sind in der Spezifikation des VHN 2 dokumentiert.

A21: Fachliche Informationen sollen künftig nicht mehr innerhalb der EGVP-Container sondern müssen als Anlage im xml-Format übertragen werden. Diese xml-Anlage muss dem XJustiz-Standard in der jeweils gültigen XJustiz-Version entsprechen. Jeder Nachricht muss deshalb eine XJustiz-XJustiz-Nachricht beigefügt werden, die den Inhalt der Nachricht beschreibt (Begleit-XJustiz-Nachricht). Die Datei muss den Dateinamen xjustiz_nachricht.xml tragen. Sofern diese Begleit-XJustiz-Nachricht bereits von der Fachanwendung des Anwenders an das Drittprodukt übergeben wird, darf das Drittprodukt keine weitere Begleit-XJustiz-Nachricht beifügen. Sofern der Nachricht weitere XJustiz-Datensätze, z.B. bei der Zustellung von Nachrichten anderer Beteiligter, beigefügt werden sollen, muss im Dateinamen eine UUID vorangestellt sein. Beispiel: UUID_xjustiz_nachricht.xml

Nachrichten, die XJustiz-Datensätze in einer älteren Version enthalten, dürfen nicht abgewiesen werden. Es wird empfohlen, keine Versionsvalidierung des XJustiz-Datensatzes beim Empfang der Nachrichten durchzuführen.

² Soweit eine signierte Datei gemeinsam mit einer zugehörigen Signaturdatei übersandt wird, sollen sich die Dateinamen der signierten Datei und der Signaturdatei nur hinsichtlich des Dateiformats unterscheiden (klage.pdf und klage.pdf.pkcs7).

Die XJustiz-Nachricht muss mindestens zu folgende Elementen Angaben enthalten:

- Absender der Nachricht,
- Empfänger der Nachricht,
- Sachgebiet
- Aktenzeichen des Empfängers (Dem Absender muss ermöglicht werden, bei der Übermittlung verfahrenseinleitender Dokumente hier ‚neu‘ einzutragen. Wenn das Aktenzeichen aus sonstigen Gründen noch nicht bekannt ist, muss die Möglichkeit bestehen, den Wert ‚unbekannt‘ einzutragen.)

Zudem muss es dem Nutzer von EGVP-Drittprodukten möglich sein, Angaben zur Sendungspriorität und Vertraulichkeit vorzunehmen, die in den XJustiz-Datensatz aufgenommen werden müssen. Zudem sollen die Metadaten, die in § 2 Abs. 3 der ERVV aufgeführt sind, enthalten sein. In Kapitel 5.2 wird aufgeführt, welche Elemente des generischen XJustiz-Nachrichtenkopfes und der XJustiz-Grunddaten für die Übertragung dieser Metadaten genutzt werden müssen.

Sofern für eine Nachricht ein Betreff angezeigt werden soll, sollen die Werte folgender Elemente der XJustiz-Nachricht verwendet werden: Sachgebiet, Ereignis, Verfahrensgegenstand.

Die Anforderungen können ab sofort und müssen bis spätestens 1.11.21 umgesetzt werden.

A22: Eingangsbestätigung: Nach dem Versenden einer EGVP-Nachricht müssen die NachrichtenID (ELEMENT: MessageId) und Eingangszeitpunkt auf dem Intermediär (ELEMENT: Creation) für den Absender als Eingangsbestätigung bereitgestellt werden. Beide Elemente müssen dem OSCI-Laufzettel, der vom OSCI-Manager signiert wurde, entnommen werden. Die Anforderung kann ab sofort und muss bis spätestens 1.11.21 umgesetzt werden.

A23: Abholbestätigung: Es wird empfohlen, nach dem Versenden und dem Abholen einer EGVP-Nachricht die Inhalte NachrichtenID (ELEMENT: MessageId), Eingangszeitpunkt auf dem Intermediär (ELEMENT: Creation) und Abholzeitpunkt (ELEMENT:reception) für den Absender als Abholbestätigung bereitzustellen. Die drei Elemente müssen dem OSCI-Laufzettel, der vom OSCI-Manager signiert wurde, entnommen werden. Die Anforderung kann ab sofort und sollte bis spätestens 1.11.21 umgesetzt werden.

A24: Die Inhalte des Prüfvermerks müssen dem Empfänger bereitgestellt werden. Sie sind in der Anlage aufgeführt. Die Anforderung kann ab sofort und muss bis spätestens 1.11.21 umgesetzt werden.

A25: Nachrichtenformat: EGVP-Nachrichten müssen zwei ContentContainer beinhalten: den Project-Container und den VHN-Container. Der Project-Container muss vor dem Versand für den Empfänger verschlüsselt werden. Der VHN-Container wird nicht für den Empfänger verschlüsselt. Die in ihm enthaltenen Daten stehen über den Verzeichnisdienst öffentlich zur Verfügung. Die Nachricht muss vor dem Versand für den Intermediär, den der Empfänger nutzt, verschlüsselt werden.

ContentDataOSCI			
	ContentContainer		"project_coco"
		Attachment (n mal)	<Dateiname>
		Attachment	xjustiz_nachricht.xml
	ContentContainer		"vhn_coco"
		Attachment	vhn.xml
		Attachment	Vhn.xml.p7s

Die Umstellung auf die neue Nachrichtenstruktur wird vom Projektbüro der BLK-AG IT-Standards koordiniert. Der Versand in der neuen Nachrichtenstruktur darf erst erfolgen, wenn dies vom Projektbüro der BLK-AG IT-Standards freigegeben wurde.

Drittprodukte müssen das aktuelle EGVP-Transportprofil beim Empfang von Nachrichten solange unterstützen, bis dies durch die BLK-AG IT-Standards abgekündigt ist. Sie sollten das neue Transportprofil ab Einführung des eBO und Freigabe durch die BLK-AG IT-Standards für den Empfang unterstützen, da andernfalls Nachrichten, die von einem eBO versandt werden, nicht empfangen werden können.

3 Architektur

Dieses Kapitel soll Aufschluss über die Rahmenbedingungen geben, die bei der Entwicklung einer Drittanwendung berücksichtigt werden müssen.

3.1 Überblick

Zum Erzeugen von OSCI-Nachrichten ist die Verwendung des definierten einheitlichen Nachrichtenformats erforderlich.

Die Adressbucheinträge aller registrierten EGVP-Nutzer werden über die Kopplung mehrerer SAFE-Verzeichnisdienste zur Verfügung gestellt. Die Verwaltung der Nutzer erfolgt jeweils in einem dieser gekoppelten Verzeichnisdienste.

Der Versand und Empfang von Nachrichten muss gemäß dem Transportprotokollstandard OSCI-1.2 erfolgen.

3.2 OSCI-Grundlagen

In diesem Kapitel werden die Grundlagen zum Protokollstandard OSCI dargestellt.

Mit dem Protokoll OSCI-Transport werden die klassischen Ziele Integrität, Authentizität, Vertraulichkeit und Nachvollziehbarkeit bei der Übermittlung von Nachrichten gewährleistet.

OSCI-Transport basiert auf den vom W3C koordinierten, weltweit anerkannten Standards XML und SOAP. Die Empfehlungen des W3C zur digital signature werden in geeigneter Weise konkretisiert, um die Anforderungen der eIDAS-Verordnung zu erfüllen. Zudem werden für die Verschlüsselungsverfahren ebenfalls genaue Vorgaben gemacht, um auch auf dieser Ebene die Interoperabilität und Herstellerunabhängigkeit sicherzustellen.

Außerdem definiert OSCI-Transport die notwendigen Datenstrukturen für Quittungsmechanismen mit Zeitstempeln.

OSCI-Transport-Nachrichten haben einen zweistufigen "Sicherheitscontainer". Dadurch ist es möglich, Inhalts- und Nutzungsdaten streng voneinander zu trennen und kryptografisch unterschiedlich zu behandeln. Die Inhaltsdaten werden vom sog. Autor einer OSCI-Nachricht so verschlüsselt, dass nur der berechtigte Leser sie dechiffrieren kann. Die Nutzungsdaten werden vom sog. OSCI-Manager für die Zwecke der Nachrichtenvermittlung und die Erbringung der Mehrwertdienste benötigt; sie werden deshalb für den OSCI-Manager verschlüsselt. Der OSCI-Manager kann aber nicht auf die Inhaltsdaten zugreifen. Oft wird hier vom "Prinzip des Doppelten Umschlages" gesprochen: Die verschlüsselten Inhaltsdaten sind wiederum in einen verschlüsselten Container eingebettet. Ein Angreifer kann wegen dieser Verschlüsselungen weder die Nutzungs- noch die Inhaltsdaten abhören.

Jeder Sicherheitscontainer (für Nutzungsdaten und Inhaltsdaten) erlaubt die digitale Signatur und die Verschlüsselung des jeweiligen Inhalts. Dadurch sind Vertraulichkeit, Integrität und Authentizität der Nachrichten gewährleistet.

3.3 OSCI-Rollenmodell

Gemäß dem Rollenmodell der OSCI-Spezifikation werden beim Austausch von OSCI-Nachrichten folgende OSCI-Akteure (Handelnde) unterschieden:

- Autor
- Sender
- OSCI-Manager
- Empfänger
- Leser

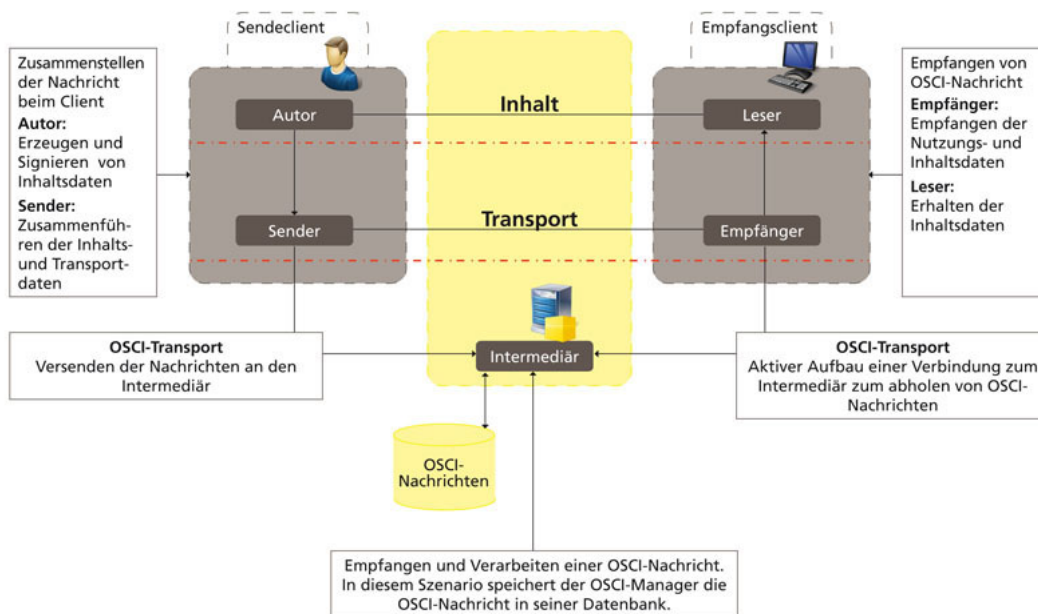


Abbildung 1: Rollen im Überblick

In der EGVP-Infrastruktur können die Rollen Leser und Empfänger sowie Autor und Sender sowohl organisatorisch als auch technisch zusammengeführt werden. Auf diese Weise wird ermöglicht, dass Nachrichten abgeholt und gelesen werden können, ohne dass zwei unterschiedliche Schlüssel zum Empfangen und zum Lesen von Nachrichten verwaltet werden müssen.

3.4 Intermediär

Der Intermediär empfängt und versendet OSCI-Nachrichten. Er ist zentraler Nachrichtenaustauschpunkt und Mittler zwischen Sender und Empfänger.

Zu seinen Aufgaben gehören:

- Überprüfung aller in der OSCI-Spezifikation geforderten Elemente von OSCI-Nachrichten,

- Erstellung einer eindeutigen MessageID, über die jederzeitig eine Identifizierung der durchgeführten Transaktion möglich ist,
- Protokollierung der Kommunikation (hierfür werden Laufzettel erzeugt, auf denen alle Aktionen einer Transaktion protokolliert werden),
- Zertifikatsüberprüfungen sowie
- Speicherung von OSCI-Nachrichten in einer Datenbank in asynchronen Szenarien, wie im Fall des EGVP durch den OSCI-Manager (OSCI-Konto).

3.5 Verzeichnisdienst

Die Adressbucheinträge aller registrierten EGVP-Postfachinhaber werden in föderierten SAFE-Verzeichnisdiensten geführt und zur Empfängerermittlung zur Verfügung gestellt. Jeder Verzeichnisdienst entspricht dem SAFE-Standard.

In den SAFE-Verzeichnisdiensten sind für jeden EGVP-Teilnehmer folgende Informationen hinterlegt sein:

- die persönlichen Daten "Name", "Organisation", "Straße", "Hausnummer", "Postleitzahl" und "Ort" und „Bundesland“
- Verschlüsselungszertifikat(e)
- Verbindungsparameter (URL und Zertifikat) des OSCI-Managers.
- SAFE-Rolle sowie
- die eindeutige, vom System vergebene, Nutzer-ID (= SAFE-ID).

Alle beteiligten Kommunikationspartner nutzen Zertifikate, die zum Zeitpunkt ihrer Anwendung gültig (d.h. nicht abgelaufen und nicht gesperrt) sind.

4 XJustiz

XJustiz ist ein Standard für das Datenaustauschformat im elektronischen Rechtsverkehr. Unter Verwendung von XML-Schema-Dateien werden strukturierte Daten im xml-Format übergeben. Der Standard **XJustiz**, der durch die BLK-Arbeitsgruppe „IT-Standards in der Justiz“ erstellt und von der BLK verabschiedet worden ist, enthält grundlegende Festlegungen für die strukturierten Daten. Der Standard ist auf www.xjustiz.de veröffentlicht.

XJustiz trifft Aussagen über den Austausch von einzelnen verfahrensbezogenen Daten, wie z.B. die Adressen von Prozessbeteiligten oder Angaben über bevorstehende Verhandlungstermine, also über die zwischen den Verfahren zu übermittelnden Inhaltsdaten.

Die XJustiz-Datei muss der EGVP-Nachricht als Anhang (Attachment) mit der invarianten Id "xjustiz_nachricht.xml" beigefügt werden.

Jede EGVP -Nachricht enthält genau eine XJustiz-Datei, weist in der Regel jedoch noch weitere Anhänge auf.

5 Anlagen

5.1 Elemente der XJustiz-Nachricht (Anforderung 21)

Für die Übertragung der oben unter A 21. beschriebenen verpflichtenden und optionalen fachlichen Informationen müssen nachfolgende Elemente des generischen XJustiz-Nachrichtenkopfes und der XJustiz-Grunddaten genutzt werden.

1	die Bezeichnung des Gerichts (§ 2 Abs. 3 der ERVV)	optional
a.	Gericht als Absender	
	Type.GDS.Nachrichtenkopf/Code.GDS.Gericht	
	Type.GDS.Grunddaten/Verfahrensdaten/Type.GDS.Instanzen/Instanzbehörde /Type.GDS.Behörde/Code.GDS.Gericht	
b.	Gericht als Empfänger	
	Type.GDS.Nachrichtenkopf/Code.GDS.Gericht	
	Type.GDS.Grunddaten/Verfahrensdaten/Type.GDS.Instanzen/Type.GDS.Behörde /Code.GDS.Gericht	
c.	das Gericht ist weder Absender noch Empfänger (z.B. bei Kommunikation zwischen RAen)	
	Type.GDS.Grunddaten/Verfahrensdaten/Type.GDS.Instanzen/Type.GDS.Behörde /Code.GDS.Gericht	
2	sofern bekannt, das Aktenzeichen des Verfahrens (§ 2 Abs. 3 der ERVV)	Pflichtfeld
a	Gericht als Absender	
	Type.GDS.Nachrichtenkopf/aktenzeichen.absender	
	Type.GDS.Grunddaten/Verfahrensdaten/Type.GDS.Instanzen/Type.GDS.Aktenzeichen	
b	Gericht als Empfänger	
	Type.GDS.Nachrichtenkopf/aktenzeichen.empfänger	

	Type.GDS.Grunddaten/Verfahrensdaten/Type.GDS.Instanzen/Type.GDS.Aktenzeichen	
c	das Gericht ist weder Absender noch Empfänger (z.B. bei Kommunikation zwischen RAen)	
	Type.GDS.Grunddaten/Verfahrensdaten/Type.GDS.Instanzen/Type.GDS.Aktenzeichen	
3	die Bezeichnung der Parteien oder Verfahrensbeteiligten (§ 2 Abs. 3 der ERVV)	optional
	Type.GDS.Grunddaten/Verfahrensdaten/Type.GDS.Beteiligung/Type.GDS.Beteiligter	
4	die Angabe des Verfahrensgegenstandes (§ 2 Abs. 3 der ERVV)	optional
	Type.GDS.Grunddaten/Verfahrensdaten/Type.GDS.Instanzen/Type.GDS.Verfahrensgegenstand	
5	sofern bekannt, das Aktenzeichen eines denselben Verfahrensgegenstand betreffenden Verfahrens und die Bezeichnung der die Akten führenden Stelle (§ 2 Abs. 3 der ERVV)	optional
	Nur, wenn anwendbar (d.h. es gibt ein weiteres Verfahren, das den Verfahrensgegenstand ebenso behandelt oder behandelt hat (z.B. Vorinstanz bei Berufungen oder Bußgeldbehörde bei OWi-Sachen oder einstweiliges Rechtsschutzverfahren, das parallel zu einem Hauptsacheverfahren geführt wird)	
	Type.GDS.Grunddaten/Verfahrensdaten/Type.GDS.Instanzen/Instanzbehörde	
6	Absender der Nachricht	Pflicht
	Type.GDS.Nachrichtenkopf/Auswahl_Absender	
7	Empfänger der Nachricht	Pflicht
	Type.GDS.Nachrichtenkopf/Auswahl_Empfänger	
8	Sachgebiet	Pflicht
	Type.GDS.Grunddaten/Verfahrensdaten/Type.GDS.Instanzen/Sachgebiet	

5.2 Inhalte des Prüfvermerkes (Anforderung 24)

Grau dargestellte Inhalte sind optional.

	Information	Inhalte	Datenquelle
	Überschrift		

1	Erstellungszeitpunkt des Prüfvermerks	Prüfvermerk vom tt.mm.jjjj, hh:mm:ss	Zeitpunkt der Durchführung der Prüfung
2	kurze Erläuterung	Das Dokument liegt als elektronisches Dokument vor. Die Prüfung des Dokuments hat folgendes Ergebnis erbracht:...	
Angaben zur Nachricht			
3	Eingangszeitpunkt der Nachricht = Eingang auf dem Intermediär	Eingang: tt.mm.jjjj, hh:mm:ss	OSCI-Laufzettel
4	Übermittlungsweg	bea	VHN
		ben	
		beBPo	
		Justiz	
		EGVP ³	
5	Absendende Person	Vorname Nachname	VHN 2 bzw. Visitenkarte bei Nutzung des VHN
6	SAFE-ID des Absenders	Nutzer-ID	VHN 2 bzw. Visitenkarte bei Nutzung des VHN
7	Empfänger	Vorname Nachname	SAFE Verzeichnisdienst
8	Nachrichtenkennzeichen EGVP-Nachricht	EGVP-Nachrichtenkennzeichen	OSCI-Laufzettel
9	Aktenzeichen Absender und Empfänger	Aktenzeichen Empfänger: string Aktenzeichen Absender: string	XJustiz_nachricht.xml, wenn nicht vorhanden, bis 1.11.2021 nachricht_xml

³ Auch für Nachrichten, die aus einem beA verschickt wurden, kann dieses Ergebnis ausgewiesen werden. Dies ist immer dann der Fall, wenn der RA nicht sicher an seinem beA angemeldet war oder eine andere Person (z.B. ein Kanzleimitarbeiter) eine Nachricht aus dem beA des RAs versandt hat.

Angaben zu den Dokumenten

Die Dokumente sollen nach der im XJustiz-Datensatz (wenn beigefügt) unter „nummerImUebergeordnetenContainer“ angegebenen Reihenfolge sortiert werden.

10	Liste der vom Absender übermittelten Dokumente (Signaturdateien sollen nicht aufgenommen werden.)	Anhänge: Dateinamen der Anhänge mit Dateiformat	Attachments
11	Angegebenes Format der übermittelten Dokumente (keine Überprüfung des Formates)	Angegebenes Format: Übernahme des angegebenen Formates aus dem Dateinamen	Attachments (Endung der Dateibezeichnung nach dem letzten Punkt)
Angaben zu qualifizierten elektronischen Signaturen (sonstige Signaturen, z.B. fortgeschrittene Signaturen, sollen nicht aufgeführt werden)			
12	Ersteller der qeS	Ersteller: Vorname_Nachname	Namen des Signierenden (Autor) aus dem Common Name (CN) des Zertifikats
13	Berufsbezogenes Attribut, falls angegeben	Attribut: string	Berufseintrag (Angaben zum Zertifikat des Autors) im Prüfprotokoll (entnommen aus dem Attribut des Zertifikats, Feld „ProfessionInfo“)
14	Zeitpunkt der qeS	Zeitpunkt der Signatur ausweislich der Signaturprüfung: tt.mm.jjjj, hh:mm:ss	Prüfungszeitpunkt
15	Ergebnis der Signaturprüfung	Gültig, ungültig, unbestimmt jeweils als Symbol	Signaturprüfer-gebnis
16	Seriennr. des Signaturzertifikates der qeS	Seriennummer:	
17	Signaturformat Anzeige der Prüfergebnisse nur von denjenigen qeS, die nach Nr.4 a und b ERVB zulässig sind, d.h., falls andere Signaturen	Signaturformat: Spalte „qualifiziert signiert nach ERVB“, mögliche Werte: ja, nein, Containersignatur, Keine Prüfung möglich, da die Signaturdatei keiner Inhaltsdatei	

übermittelt wurden, sollen deren Prüfergebnisse nicht angezeigt werden.	zugeordnet werden konnte, Die letzte Version des Dokuments wurde nicht signiert, Es konnte nicht geprüft werden, ob eine qualifizierte Signatur nach ERVB vorliegt.	
Falls qualifizierte elektronische Containersignaturen angebracht wurden, soll ein Hinweis erfolgen sowie der Status der Signaturprüfung angegeben werden.	Hinweis: Es liegt eine Containersignatur vor	

Beispiel:

Prüfvermerk vom 24.11.2020, 15:26:53

Die unten aufgeführten Dokumente sind elektronisch eingegangen. Die technische Prüfung der elektronischen Dokumente hat folgendes Ergebnis erbracht:

Angaben zur Nachricht:

Sicherer Übermittlungsweg aus einem besonderen Anwaltspostfach.

Eingangszeitpunkt: 24.11.2020, 15:26:24
 Absender: Test-Benutzer ZZZ_Test_EGVP
 Nutzer-ID des Absenders: DE.BRAK_SPT.97becaaa-e41d-4db2-869d-af18ead2158d.c29d
 Aktenzeichen des Absenders: 75/2019 TT

Empfänger: Amtsgericht Berlin
 Aktenzeichen des Empfängers: 7 F 31/20

Betreff der Nachricht: Klage (Der Betreff ist zum 01.11.2021 abgekündigt)
 Text der Nachricht: Der Nachrichtentext ist zum 01.11.2021 abgekündigt.
 Nachrichtenkennzeichen: EGVP_GT116062279832745880678720003948794

Angaben zu den Dokumenten:

Dateiname	Format	Informationen zu(r) qualifizierten elektronischen Signatur(en)				
		Qualifiziert signiert nach ERVB?	durch	Berufsbezogenes Attribut	am	Prüfergebnis
Anlage.pdf	pdf	ja	Testkarte:PN (7723056237474015618)	Testnotar in Teststadt	16.10.2020, 16:53:03	<input checked="" type="checkbox"/> Gültigkeit <input checked="" type="checkbox"/> Integrität
Klage.pdf	pdf	nein				
xjustiz_nachricht.xml	xml	nein				

5.3 Das SAFE-Rollenmodell

Die Sichtbarkeiten für EGVP-Postfachinhaber werden über SAFE-Rollen abgebildet.

Jedem Postfachinhaber wird im SAFE-System der Rollentyp "EGVP" und ein (oder mehrere) bestimmte(r) Rollenwert(e) zugeordnet.

Bei der Suche nach EGVP-Adressaten wird über die Abfrage dieser Rollenwerte gesteuert, welche EGVP-Postfachinhaber der Absender sehen und somit adressieren darf.

Die Festlegung und Pflege der SAFE-Rollen erfolgt durch die BLK- AG IT-Standards in der Justiz.

Sämtliche Sichtbarkeiten werden über bestimmte Rollenwerte abgebildet. Als allgemeine Rollenwerte sind festgelegt:

- egvp_bea
- egvp_ben
- egvp_bebpo
- egvp_ebo
- ozg_postfach
- egvp_justiz
- zuzu
- egvp_buerger
- egvp_behoerde
- buerger_hin
- buerger_rueck
- egvp_test

Nachfolgend sind die allgemeinen Rollenwerte mit den Sichtbarkeitsregeln aufgeführt:

		buerger	behoerde	buerger_hin	buerger_rueck	bea	ben	bebpo	ebo	ozg_postfach	zuzu	justiz	test
		<i>wird gesehen von</i>											
		↓											
buerger	<i>sieht</i> →		+		+			+	+	+		+	
behoerde		+	+	+	+	+	+	+	+	+		+	
buerger_hin		+	+	+	+	+	+	+	+	+	+	+	
buerger_rueck		+	+	+	+	+	+	+	+	+	+	+	
bea			+	+	+	+	+	+	+	+		+	
ben			+	+	+	+	+	+	+	+		+	
bebpo		+	+	+	+	+	+	+	+	+		+	
ebo					+	+	+	+				+	
ozg_postfach					+	+	+	+				+	
justiz		+	+	+	+	+	+	+	+	+	+	+	
test													+

egvp_justiz

Die Rolle egvp_justiz dient der eindeutigen Identifizierung der Justizbehörden bei der Adresssuche.

Für eine Übergangszeit werden die Justizpostfächer somit entweder die Rolle egvp_behoerde oder die Rolle egvp_justiz innehaben können.

egvp_bea

Diese Rolle ist den besonderen elektronischen Anwaltspostfächern vorbehalten.

egvp_ben

Diese Rolle ist den besonderen elektronischen Notarpostfächern vorbehalten.

egvp_bebpo

Diese Rolle ist den Inhabern besonderer Behördenpostfächer vorbehalten und darf nur nach Durchführung des Identifizierungsverfahrens gemäß ERVVO vergeben werden. Die Sichtbarkeiten entsprechen den gesetzlichen Vorgaben. Inhaber von beBPO-Postfächern dürfen die Postfächer der Justiz (egvp_justiz) sowie andere besondere Postfächer (beA, ben, beBPo und eBO) adressieren.

egvp_ebo

Diese Rolle ist den Inhabern besonderer Bürger- und Organisationenpostfächern vorbehalten und wird automatisiert vergeben. eBO-Inhaber erhalten die Rolle in einem automatisierten Prozess im Rahmen des Registrierungs- und Identifizierungsprozesses.

Die Sichtbarkeiten entsprechen den gesetzlichen Vorgaben. Inhaber von eBO-Postfächern dürfen die Postfächer der Justiz (egvp_justiz) sowie andere besondere Postfächer (beA, ben, beBPo) adressieren. Andere eBO-Postfächer können sie nicht adressieren.

ozg_postfach

Diese Rolle ist Nutzern eines OZG – Nutzerkontos vorbehalten. Die Sichtbarkeiten entsprechen den Sichtbarkeiten des egvp_ebo.

zuzu

Bei der Registrierung können eBO-Inhaber, die keine natürlichen Personen sind, im SAFE - Registrierungsclient die Zustimmung zur Zustellung elektronischer Dokumente allgemein erteilen (§ 173 Abs. 4 Satz 3 ZPOnF). Sie erhalten dann zusätzlich zur Rolle egvp_ebo die Rolle zuzu.

egvp_buerger

Die Rolle egvp_buerger ist für Teilnehmer am ERV, die keinen sicheren Übermittlungsweg nutzen, eingerichtet worden. Postfachinhaber mit dieser Rolle können nur Justiz- und andere Behörden (Rollen egvp_behoerde, egvp_bebpo) sowie Inhaber der Rolle buerger_rueck, nicht jedoch andere EGVP-Teilnehmer adressieren.

egvp_behoerde

Die Rolle egvp_behoerde ist ursprünglich für die Justizbehörden und andere Behörden eingerichtet worden. Sie soll nur in historisch gewachsenen Konstellationen weiterhin genutzt werden. Für Justizbehörden ist die Rolle egvp_justiz und für besondere Behördenpostfächer die Rolle egvp_bebpo eingerichtet worden.

buerger_hin

Postfachinhaber mit dem Rollenwert buerger_hin können neben den Behördenpostfächern auch alle Bürgerpostfächer adressieren, werden von diesen jedoch nicht gesehen und können somit keine Rückantworten erhalten.

Diese Rolle wird Gerichtsvollziehern zugeordnet, denen neben der elektronischen Kommunikation mit dem zentralen Vollstreckungsgericht auch das Versenden von Dokumenten an Gläubiger oder Verfahrensbeteiligte ermöglicht werden soll.

buerger_rueck

Postfachinhaber mit dem Rollenwert buerger_rueck können neben den Behördenpostfächern nicht nur auch alle Bürgerpostfächer adressieren, sondern werden von diesen auch gesehen und können somit Rückantworten erhalten.

Dieser Rollenwert wird Gerichtsvollziehern zugeordnet, die die vollumfängliche elektronische Kommunikation bevorzugen und deshalb auch für Verfahrensbevollmächtigte bzw. Gläubiger per EGVP erreichbar sein möchten.

egvp_test

Es ist in bestimmten Konstellationen erforderlich, Tests im Echtsystem durchzuführen. Testpostfächer sollen jedoch nicht für jedermann sichtbar sein, um rechtlich relevante Zustellungen zu vermeiden. Deshalb wurde die Rolle egvp_test eingerichtet. Postfachinhaber mit der Rolle egvp_test können nur anderen Postfächer mit eben dieser Rolle sehen.