egvp:de

Teilnahme von Drittanwendungen[1] am OSCI-gestützten elektronischen Rechtsverkehr

Anforderungen

Version 1.0 vom 21.07.2017

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

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-gestützen 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.

Hinweis: Die Vorgaben dieses Papiers gelten für herkömmliche EGVP-Postfächer. Für besondere Postfächer nach § 130 a ZPOnF werden derzeit zusätzliche Anforderungen abgestimmt, die rechtzeitig vor dem 1.1.2018 veröffentlicht werden.

Inhaltsverzeichnis

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) ohne deren Änderung aufsetzen 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 EGVP-Schnittstellenspezifikation, einschließlich des Nachrichtenformats von EGVP und der Zugriffsbeschreibung des jeweils genutzten SAFE-konformen Verzeichnisdienstes muss von der Drittanwendung eingehalten werden.

A4: Die Drittanwendung muss seinen Nutzern den Empfang der an sie versandten OSCI-Nachrichten ermöglichen.

A5: Die Drittanwendung muss die Nachrichten seiner Nutzer in einer Form verschlüsseln, die gemäß OSCI-Spezifikation entschlüsselt werden kann.

A6: Die Drittanwendung muss in der Lage sein, die für seine Nutzer mit dem EGVP verschlüsselten Nachrichten entgegenzunehmen und zu entschlüsseln.

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

A7: Sofern der SAFE-Verzeichnisdienst der Justiz genutzt wird, muss die Drittanwendung seinen Nutzern ermöglichen, sich als Nutzer zu registrieren. Die Drittanwendung darf aber als Option das so genannte „Opting Out“ Verfahren anbieten, bei dem keine Registrierung des Nutzers erfolgt. Sofern die opting out Funktion von

Drittanwendungen umgesetzt wird, dürfen die Nachrichten, die ohne Einrichtung eines Postfaches versendet werden, keine visitenkarte.xml und visitenkarte.xsl in den additionals enthalten.

A8: Mit der Einrichtung des Postfachs im SAFE-Verzeichnisdienst der Justiz sind die in der „Visitenkarte“ festgelegten persönlichen Daten des Nutzers zu erheben; es muss daher gewährleistet sein, dass für jeden registrierten Nutzer alle Pflichtfelder der „Visitenkarte“ in ihrer jeweils aktuellen Fassung ausgefüllt werden.

2.4 Mengenbegrenzungen

A9: Die für EGVP jeweils geltenden aktuellen Mengenbeschränkungen (siehe www.egvp.de, derzeit maximal 100 Anhänge bei einem Maximalvolumen von 30 MB pro Nachricht) sind durch die Drittanwendung technisch zu gewährleisten; sie dürfen bei der Nachrichtenerstellung nicht überschritten werden, da ansonsten eine Weiterverarbeitung nicht gewährleistet ist.

A10: Nachrichten, die den Mengenbeschränkungen genügen, müssen mit der Drittanwendung verarbeitet werden können.

A11: Künftige Änderungen der Mengenbegrenzungen sind möglich und werden über www.justiz.de und www.egvp.de bekannt gemacht.

2.5 Versand von OSCI-Nachrichten durch das Produkt

A12: Die 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 Bedienschritt 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.

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. Dazu gehören auch die Verwendung der definierten Nachrichtentypen und die Übermittlung der Herstellerinformationen.

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 des deutschen Signaturgesetzes 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 Quittungs-mechanismen 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

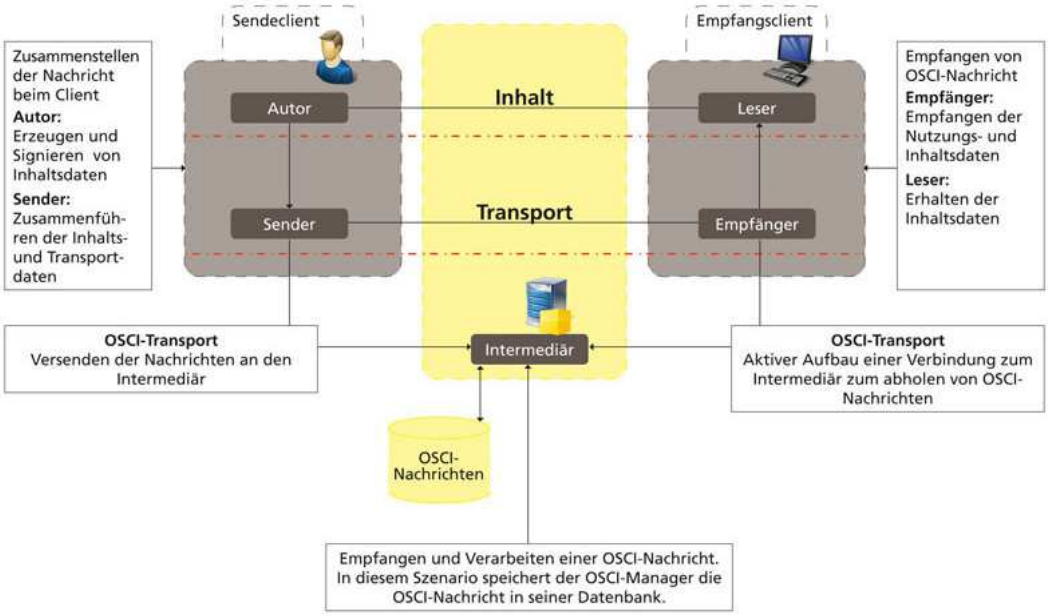

Abbildung 1: Rollen im Überblick

In der EGVP-Infrastrutur sind die Rollen Leser und Empfänger sowie Autor und Sender derzeit sowohl organisatorisch als auch technisch zusammengeführt. 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.

Hinweis: Ab 01.01.2018 muss von allen Drittanwendungen die Trennung zwischen Leser und Emfpänger sowie Autor und Sender unterstützt werden. Dabei muss lediglich sichergestellt werden, dass der Empfang von und der Versand an Teilnehmer, die eine solche Trennung implementiert haben, möglich ist.

3.4 OSCI-Manager

Der OSCI-Manager 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 (die Durchführung erfolgt über das Kernsystem und das OCSP/CRL-Relay) 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 muss dem SAFE-Standard entsprechen.

In den SAFE-Verzeichnisdiensten müssen 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 müssen Zertifikate nutzen, die zum Zeitpunkt ihrer Anwendung gültig (d.h. nicht ab- gelaufen und nicht gesperrt) sind.

3.6 Eingangsbestätigung

Es wird empfohlen, nach dem Versenden einer EGVP-Nachricht eine Eingangsbestätigung mit dem Inhalt des vom OSCI-Manager signierten OSCI-Laufzettels und folgenden weiteren Informationen zu erstellen:

- Nachrichtenkennzeichen
- Nachrichtentyp
- Aktenzeichen des Absenders,
- Aktenzeichen des Empfängers,
- Eingangszeitpunkt auf dem Server (Ende des Empfangsvorgangs),
- Inhabername des Verschlüsselungszertifikats des OSCI-Managers,
- Inhabername des Signaturzertifikats des OSCI-Managers,
- Name des OSCI-Managers
- Name des Absenders laut Visitenkarte
- Übersicht über das Verschlüsselungszertifikat des Absenders,
- Name des Empfängers laut Visitenkarte,

- Übersicht über das Verschlüsselungszertifikat des Empfängers sowie Nutzer-ID des Empfängers,
- Übersicht über die Signaturzertifikate der Autoren (wenn vorhanden),
- Name der übermittelten Dokumente und
- Herstellerinformationen

Hintergrundinformation zum EGVP:

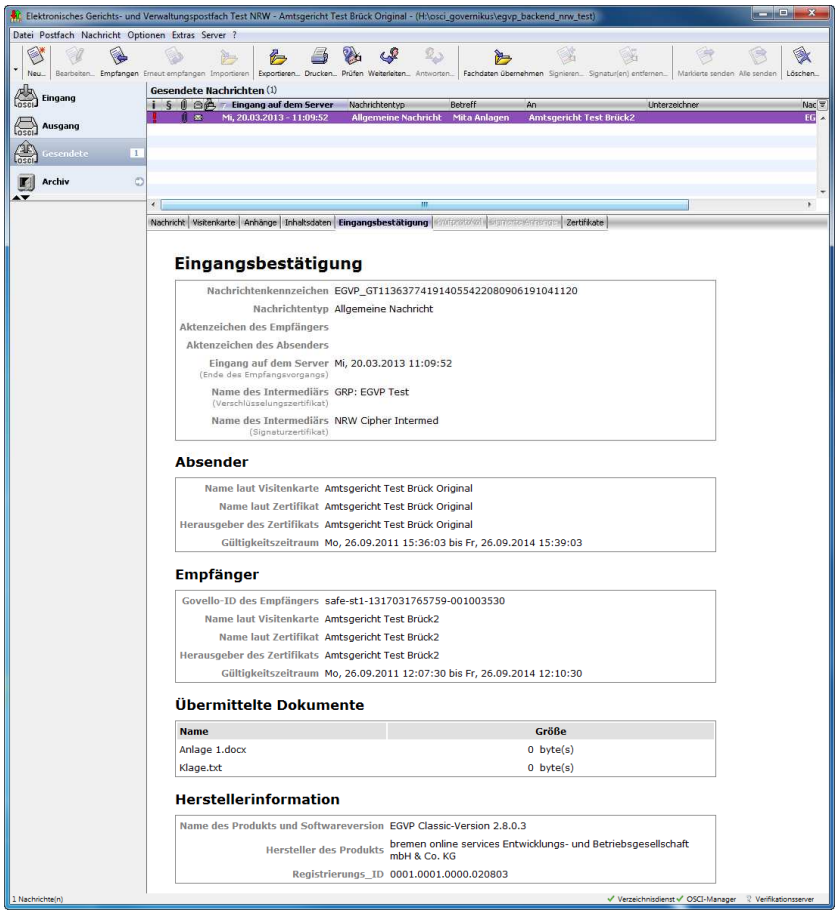

Abbildung 2: Eingangsbestätigung (Beispiel)

3.7 Prüfprotokoll (HTML-Format)

Es wird empfohlen, ein Prüfprotokoll zu erstellen. Das Prüfprotokoll liefert dem Empfänger einer EGVP-Nachricht eine Handlungsgrundlage zur weiteren Verarbeitung. Es stellt üblicherweise die Visualisierung der vom OSCI-Manager erhaltenen Antwort auf einen Abholungsauftrag (ResponseToFetchDelivery) dar. Diese beinhaltet üblicherweise den vom OSCI-Manager signierten Laufzettel.

Das Prüfprotokoll sollte mindestens folgende Informationen darstellen:

- Zusammenfassung und Struktur: Gesamtprüfergebnis, Betreff (entspricht dem Nachrichtentyp), Nachrichtenkennzeichen, Absender, Empfänger, Eingang auf dem Server, Nachrichtenstruktur (Autoren, Inhaltsdaten, Anhänge),

- Signaturprüfungen,
- Detailansicht der Zertifikate und
- weitere Informationen.

Hintergrundinformation zum EGVP

Abbildung 3: Prüfprotokoll Zusammenfassung (Beispiel)

3.8 Prüfergebnis für signierte Anhänge (HTML-Format)

EGVP-Nachrichten können Anhänge mit sich führen, die bereits Signaturen enthalten. Diese Signaturen werden nicht vom OSCI-Manager geprüft. Es wird empfohlen, eine Signaturprüfung durchzuführen und die Ergebnisse dieser Prüfungen in einem Prüfprotokoll darzustellen, das für jeden signierten Anhang überlicherweise folgende Informationen beinhaltet:

- Zusammenfassung und Struktur: Gesamtprüfergebnis, Signaturform, Autor, Namen der signierten Datei,
- Signaturprüfungen: Name des Autors, Aussteller des Zertifikats, Signaturniveau, Signierzeitpunkt, Zeitpunkt der Durchführung der Prüfung, verwendeter Hashalgorithmus, Status zu Integrität und Identität,
- Ergebnis der Signaturprüfung,
- Informationen über das Zertifikat für den Signaturschlüssel jedes Autors (sofern vorhanden, wird das zugehörige Berufsattribut oder ggf. das zugehörige Attributzertifikat dargestellt),

- Detailansicht über die verwendeten Zertifikate und
- Ggf. weitere Informationen.

Hintergrundinformation zum EGVP

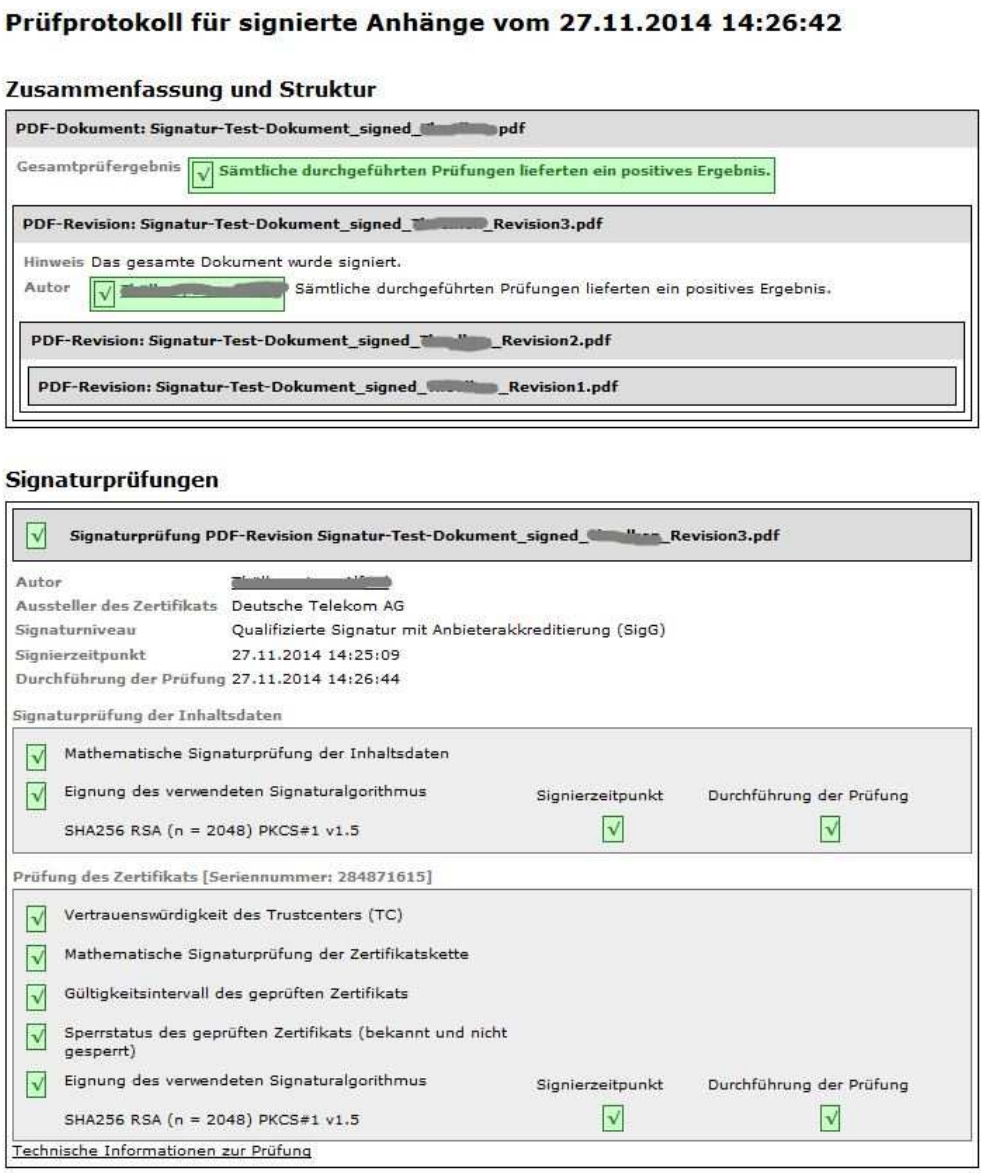

Abbildung 4: Prüfergebnis für signierte Anhänge (Beispiel)

3.9 Transfervermerk

Hintergrundinformation zum EGVP

Gemäß § 298 Absatz 2 der Zivilprozessordnung und der analogen Vorschriften in den einzelnen Verfahrensordnungen (§ 55b Absatz 4 Satz 2 der Verwaltungsgerichtsordnung, § 52b der Finanzgerichtsordnung und § 65b Sozialgerichtsgesetz) kann von einem elektronischen Dokument ein Ausdruck

für die Akten gefertigt werden. Dieser Ausdruck muss einen so genannten Transfervermerk enthalten, der folgende Informationen ausweist:

- *Ergebnis der Integritätsprüfung des Dokuments,*
- *Inhaber der Signatur lt. Signaturprüfung und*
- *Zeitpunkt für die Anbringung der Signatur lt. Signaturprüfung.*

Außer der Angabe, ob es sich bei der Signatur um ein qualifiziertes Zertifikat handelt und der Nachrichten-ID, ohne die eine eindeutige Zuordnung des Transfervermerks zur Nachricht nicht möglich wäre, enthält der Transfervermerk inhaltlich keine über die Anforderung des § 298 Abs. 2 ZPO hinausgehenden Angaben. Der Umfang des Transfervermerks ist in der Regel nicht größer als eine DIN-A4-Seite.

Der Transfervermerk wird direkt nach dem Empfang bzw. der Prüfung einer OSCI-Nachricht erstellt. Ihm zugrunde liegt der Metadatencontainer. Er wird nicht im Verwaltungsfenster angezeigt. Lediglich beim Drucken einer OSCI-Nachricht kann der Transfervermerk mit ausgedruckt werden.

Der Transfervermerk umfasst zwei Bereiche: OSCI und signierte Anhänge.

Transfervermerk

erstellt am: 27.11.2014, 14:37:22

(weitere Details und Anmerkungen können Sie dem separaten Prüfprotokoll entnehmen)

Prüfergebnis der OSCI-Nachricht: egvp_hb_14170954251051830202600942892048

Eingang auf dem Server: 27.11.2014, 14:37:08
(Ende des Empfangsvorgangs) (lokale Serverzeit)

Inhaltsdaten: nachricht.xml, nachricht.xsl, visitenkarte.xml, visitenkarte.xsl, herstellerinformation.xml

Anhänge: Test.docx.p7s, Signatur-Test-Dokument_signed_[redacted].pdf, Signatur-Test-Dokument_signed_[redacted].pdf, Test.pdf, Test.docx

Signiert durch	Signiert am (lokale Systemzeit der Signaturanbringung)	Qualifiziertes Zertifikat	Integrität (mathematische Signaturprüfung)
[redacted]	27.11.2014, 14:37:08	ja	gültig

Prüfergebnis signierte Anhänge:

Signatur-Test-Dokument_signed_[redacted].pdf

Signiert durch	Signiert am (soweit feststellbar)	Qualifiziertes Zertifikat	Integrität (mathematische Signaturprüfung)
[redacted]	06.05.2014, 16:24:35	ja	ja

Signatur-Test-Dokument_signed_[redacted].pdf

Signiert durch	Signiert am (soweit feststellbar)	Qualifiziertes Zertifikat	Integrität (mathematische Signaturprüfung)
[redacted]	27.11.2014, 14:25:09	ja	ja

Test.pdf

Signiert durch	Signiert am (soweit feststellbar)	Qualifiziertes Zertifikat	Integrität (mathematische Signaturprüfung)
[redacted]	05.11.2014, 16:19:33	ja	ja

Abbildung 5: Transfervermerk (Beispiel)

4 Nachrichtenformat

OSCI-Nachrichten sind Nachrichten mit einer festgelegten Struktur, die mittels des OSCI-Transportprotokolls übermittelt werden.

EGVP-Nachrichten sind eine besondere Form von OSCI-Nachrichten, da sie einige zusätzliche Informationen (z. B. Herstellerinformationen) beinhalten.

EGVP-Nachrichten müssen zwei ContentContainer beinhalten: den Govello-Container und den Project-Container.

4.1 Govello-Container

Der Govello-Container kann bis zu zwei OSCI-Contents enthalten, deren Inhalt und Bedeutung festgelegt sind.

Einer dieser OSCI-Contents wird mit "additional_infos" benannt und enthält den OSCI-Betreff, das Signaturniveau und die Nutzer-ID.

```
user_id=govello-1177574098093-000000071
signature_level=qu
subject=betreff
```

Listing 1: Beispiel für den OSCI-Content "additional_infos"

Folgende Angaben für das Signaturniveau sind möglich:

Eintrag	Beschreibung
`signature_level=qu`	Das Signaturniveau qualifiziert wird gefordert
`signature_level=ad`	Das Signaturniveau fortgeschritten wird gefordert
`signature_level=no`	Keine Anforderung an das Signaturniveau

Tabelle 1: Signaturniveau

Hinweis: Die Betreffzeile muss UTF-8 kodiert sein.

Sofern Signaturen vorliegen, enthält ein zweiter OSCI-Content namens "local_timestamps" eine Zuordnung von Autoren zu Signierzeitpunkten. Die OSCI-RefID ist festgelegt auf "govello_coco".

```
dAXGUdNn4eKHa/nLROzbSU6b6Ug=1193150928890
```

Listing 2: Beispiel für den OSCI-Content "local_timestamps":

Ein Autor wird anhand des base64-codierten Fingerabdruckes seines Signaturzertifikats identifiziert. Der Signaturzeitpunkt wird durch die Anzahl der Millisekunden, die seit dem 1.1.1970, 00:00 Uhr (Unixzeit nach POSIX-Standard) vergangen sind, berechnet.

Hinweis: Diese Vorgaben gelten nur noch bis zum 31.12.2017, da ab dem 1.1.2018 die Signatur der EGVP-Nachricht (des Inhaltsdatencontainers) gemäß RVO ERV nicht mehr erlaubt ist, da es sich bei dieser Signatur um eine sogenannte Containersignatur handelt. Die dann geltende Spezifikation wird rechtzeitig veröffentlicht.

4.2 Project -Container

Für den Project -Container ist die OSCI-RefID festgelegt auf "project_coco", der Project -Container beinhaltet folgende Inhalte:

- ein OSCI-Attachment für jeden Anhang,
- jeweils ein OSCI-Content für die XML- und XSLT-Struktur für das Erzeugen der Nachrichten-HTML-Seite,
- jeweils ein OSCI-Content für die XML- und XSLT-Struktur für das Erzeugen der Visitenkarten-HTML-Seite,
- ein OSCI-Content für Informationen zu den verwendeten Softwareprodukten

ContentDataOSCI			
	ContentContainer		`"project_coco"`
		Content *	`"nachricht.xml"`
		Content *	`"nachricht.xsl"`
		Content	`"visitenkarte.xml"`
		Content	`"visitenkarte.xsl"`
		Content	`"hersteller.xml"`
		Attachment (n mal) *	`<Dateiname>, z. B. "xjustiz_nachricht.xml"`
	ContentContainer		`"govello_coco"`
		Content	`"additional_infos"`
		Content **	`"local_timestamps"`

Tabelle 2: ContentDataOSCI

* optional

** nur bei signierten Nachrichten

Beim Signieren einer EGVP-Nachricht wird nur dieser Project -Container signiert.

Hinweis: Diese Vorgaben gelten nur noch bis zum 31.12.2017, da ab dem 1.1.2018 die Signatur der EGVP-Nachricht (des Inhaltsdatencontainers) gemäß RVO ERV nicht mehr erlaubt ist, da es sich bei dieser Signatur um eine sogenannte Containersignatur handelt. Die dann geltende Spezifikation wird rechtzeitig veröffentlicht.

Beide OSCI-ContentContainer werden unmittelbar vor dem Versenden für den Empfänger der EGVP-Nachricht verschlüsselt.

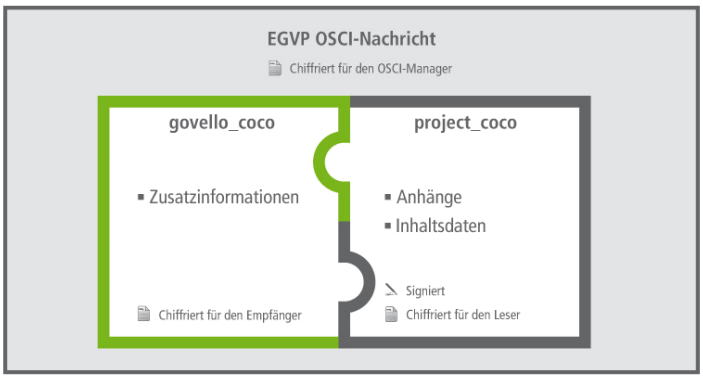

Abbildung 6: Aufbau einer OSCI-Nachricht

4.2.1 Aufbau der Inhaltsdaten nachricht.xml & nachricht.xsl

Die Inhaltsdaten der Nachricht werden in einer XML-Struktur abgelegt (OSCI-Content "nachricht.xml"). Beispieldateien in den Formaten .xml, .xsd, .xsl sind auf www.egvp.de veröffentlicht.

Hintergrundinformation zum EGVP:

Die in der XSLT-Struktur beschriebene Transformation zu HTML wird vom Anwendungs-Client verwendet, um die Nachricht im Verwaltungsfenster in der Registerkarte "Nachricht" darzustellen (zur Darstellung wird derzeit HTML 3.2 - nur innerhalb von Java darstellbar - verwendet).

4.2.1.1 Schema nachricht.xml

Die folgende Abbildung zeigt das Schema des XML-Containers <Nachricht>.

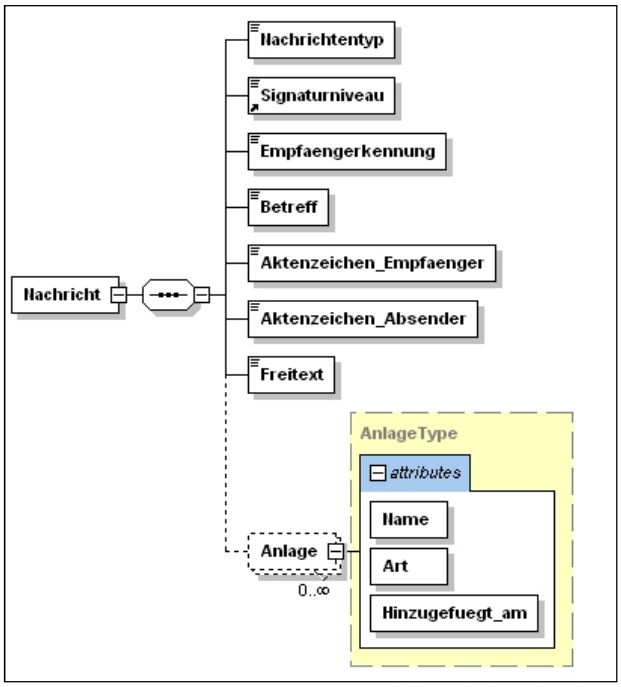

Abbildung 7: Schema des Containers <Nachricht>

Der XML-Container <Nachricht> beinhaltet folgende Attribute und Elemente:

Name	Beschreibung
<Nachrichtentyp>	Die Liste der zugelassenen Nachrichtentypen wird durch die BLK-AG IT-Standards bestimmt.
<Signaturniveau>	Die Signaturniveaus "A=qualifizierte Signatur mit Anbieterakkreditierung", "Q=qualifizierte Signatur", "F=fortgeschrittene Signatur" und "kein Symbol=ohne Signatur" müssen darstellbar sein.
<Empfaengerkennung>	Hier wird die eindeutige Nutzer-ID (SAFE-ID) des Empfängers dargestellt.
<Betreff>	Zu einer Nachricht muss ein Betrefftext eingegeben werden.
<Aktenzeichen_Empfaenger>	Zu einer Nachricht kann ein Aktenzeichen des Empfängers angegeben werden.
<Aktenzeichen_Absender>	Zu einer Nachricht kann ein Aktenzeichen des Absenders angegeben werden.
<Freitext>	Zu einer Nachricht kann ein Nachrichtentext eingegeben werden, der maximal 5.000 Zeichen umfassen darf.
<Anlage Art Hinzugefuegt_am Name />	Folgende Zeichen sind in Dateinamen von Anhängen und Inhaltsdaten erlaubt: • Alle Buchstaben des Alphabets (Groß- und Kleinschreibung) • Alle Ziffern • Alle Umlaute (Groß- und Kleinschreibung) Das Verwenden von externen Inhalten in den Inhaltsdaten ist nicht erlaubt, da es ein generelles Sicherheitsrisiko darstellt und dazu führen kann, dass es in Umgebungen, die das Nachladen solcher Inhalte blockieren, zu Funktionsstörungen kommt.

Tabelle 3: XML-Container <Nachricht>

Hintergrundinformation zum EGVP:

Die Nachricht wird dann wie folgt im Verwaltungsfenster des Anwendungs-Clients dargestellt:

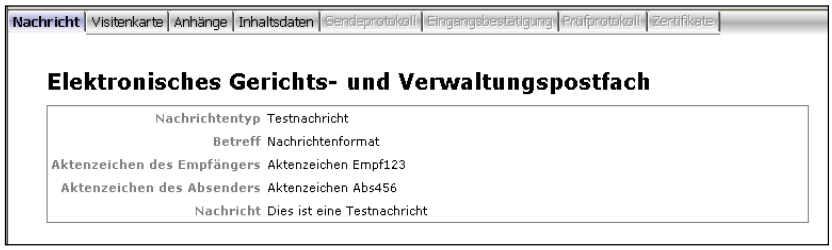

Abbildung 8: Darstellung einer Nachricht

4.2.2 Aufbau der Inhaltsdaten visitenkarte.xml & visitenkarte.xsl

Die Inhaltsdaten für die Visitenkarte der Nachricht werden in einer XML-Struktur abgelegt. Beispieldateien in den Formaten .xml, .xsd, .xsl sind auf www.egvp.de veröffentlicht.

Hintergrundinformation zum EGVP:

Die in der XSLT-Struktur beschriebene Transformation zu HTML wird vom Anwendungs-Client verwendet, um die Visitenkarte im Verwaltungsfenster in der Registerkarte "Visitenkarte" darzustellen.

4.2.2.1 Schema visitenkarte.xml

Die folgende Abbildung zeigt das Schema des XML-Containers `<Visitenkarte>`.

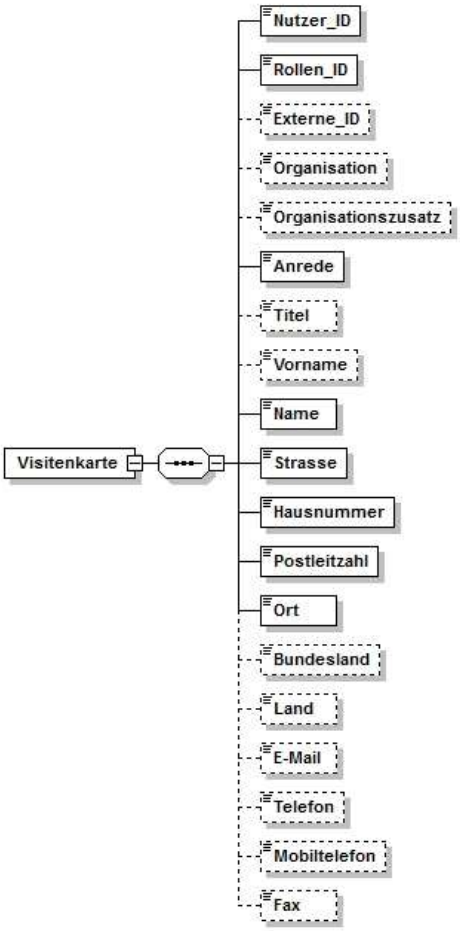

Abbildung 9: Schema des Containers <Visitenkarte>

Zulässige Zeichen für die Attribute der Visitenkarte

Beim Ausfüllen der Visitenkarte sind folgende reguläre Ausdrücke erlaubt:

- Feld "Telefonnummer":

  [+()-/0-9]{2,}

  Das bedeutet, dass z. B. folgende Zeichen zugelassen sind:

  - Alle Ziffern
  - Die Sonderzeichen +()-/
  - Mindestens zwei Zeichen

  Das erlaubt z. B. die Eingabe "+49 (421) 20495-60"

- Feld "E-Mail":

  [A-Za-z0-9.!#$%&'*+\\-/=?^_`{|}~]{2,}@[\\w.\\-_]{2,}\\.[a-zA-Z]{2,6}

  Das erlaubt z. B. die Eingabe "info@bos-bremen.de"

- Alle weiteren Felder:

  [\\w &'()+,\\-./\\p{InLatin-1Supplement}\\p{InLatinExtended-A}]{2,}

  Das bedeutet, dass z. B. folgende Zeichen zugelassen sind:

  - Alle Buchstaben des Alphabets (Groß- und Kleinschreibung)
  - Alle Ziffern
  - Alle Umlaute (Groß- und Kleinschreibung)
  - Die Sonderzeichen _&`()+-.,/§
  - Leerzeichen

Die Mindestlänge der Einträge beträgt jeweils zwei Zeichen.

Ein normales oder geschütztes Leerzeichen (Alt-255) ist nicht am Anfang und am Ende eines Eintrags erlaubt.

Der XML-Container <Visitenkarte> beinhaltet neben den Daten der Visitenkarte noch folgende Elemente:

Name	Beschreibung
<Nutzer_ID>	Nutzer-ID, die vom Verzeichnisdienst vergeben wird (entspricht der SAFE-ID)
<Rollen_ID>	Gibt die SAFE-Rolle des Rollentyps egvp an.

Tabelle 4: XML-Container <Visitenkarte>

Achtung: In der Visitenkarte des EGVP wird zusätzlich das Attribut <Externe_ID> geführt. Hier wird die XJustiz-ID des Gerichtes eingetragen. Die XJustiz-ID kann von EGVP-Teilnehmern als Adressinformation genutzt werden. Drittanwendungen dürfen jedoch keine externe ID verwenden.

Hintergrundinformation zum EGVP:

Die Visitenkarte wird dann wie folgt im Verwaltungsfenster des EGVP dargestellt:

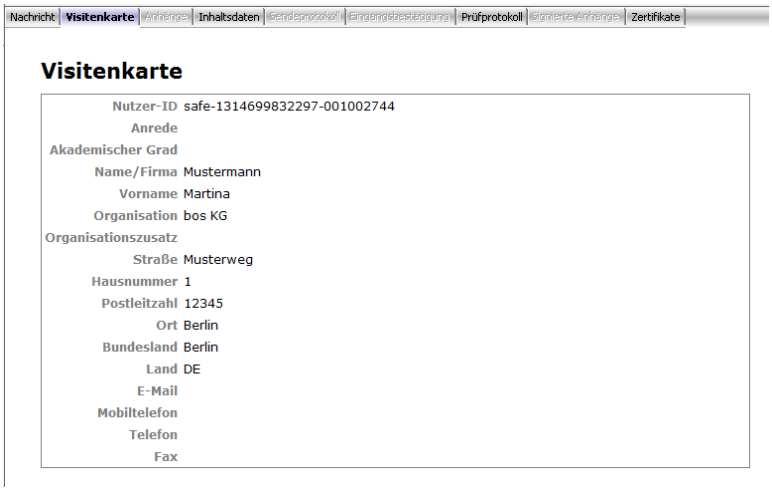

Abbildung 10: Darstellung einer Visitenkarte

4.2.3 Aufbau der Inhaltsdaten hersteller.xml

Die Informationen über das bzw. die absendenden Produkte der Nachricht müssen in einer XML-Struktur abgelegt werden. Beispieldateien in den Formaten .xml und .xsd sind auf www.egvp.de veröffentlicht.

Die folgende Abbildung zeigt das Schema des Containers <Herstellerinformation>.

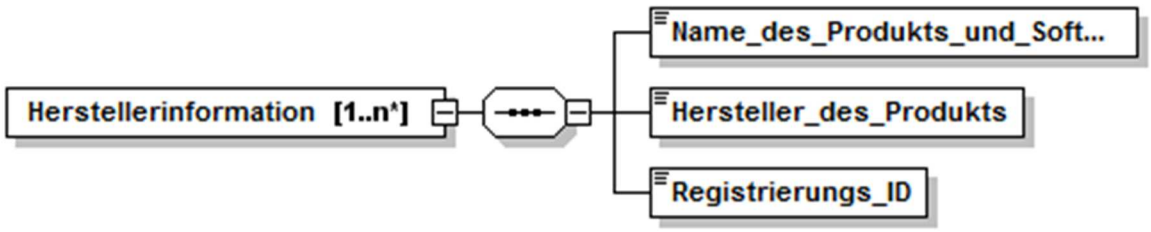

Abbildung 11: Schema des Containers <Herstellerinformationen>

Der XML-Container `<Herstellerinformationen>` beinhaltet folgende Attribute und Elemente:

Name		Beschreibung
`<Herstellerinformation/>`		
	`<Name_des_Produkts_und_Softwareversion>`	Name und Version des Produkts
	`<Hersteller_des_Produkts >`	Name des Herstellers
	`<Registrierungs_ID>`	ID des Drittproduktes bzw. der Fachanwendung, die das Drittprodukt einbindet

Tabelle 5: XML-Container <Herstellerinformation>

4.3 Nachrichtentypen

Eine EGVP-Nachricht muss die Angabe eines Nachrichtentypen enthalten (Pflichtangabe bei der Nachrichtenerstellung). Der Nachrichtentyp wird als OSCI-Betreff verwendet und kann als Unterscheidungskriterium für die Weiterverarbeitung genutzt werden. Da der OSCI-Betreff als Element der Nutzungsdaten auch in der Datenbank des OSCI-Managers gesehen werden kann, kann er auch z. B. zum Accounting oder für statistische Auswertungen verwendet werden.

Name des Nachrichtentyps	**Nachrichtentyp**
Allgemeine Nachricht	OSCI-Nachricht (erstellt mit dem Nachrichtenfenster) Default-Nachrichtentyp
HR-Beteiligter	Handelsregisternachricht - Verfahrensbeteiligter
Mahn-Antrag	ProfiMahn-Antragsdaten vom Antragsteller bzw. Prozessbevollmächtigen an das Mahngericht (einschließlich Online-Mahnantrag, OptiMahn usw.)
Testnachricht	Einreichung von Testnachrichten

Tabelle 6: Nachrichtentypen

4.4 Signierte Anhänge

Die zu einer OSCI-Nachricht hinzugefügten Anhänge können signiert sein. Folgende Szenarien müssen beachtet werden, da sie bei der Erstellung des EGVP- Prüfprotokolls unterstützt werden:

- PKCS#7 (Dateitypen .p7, .p7s, .p7m und .pkcs7): Alle Signaturen werden erkannt und auf Integrität geprüft. Die zugehörigen Autorenzertifikate werden auf Identität geprüft. Liegt die Signatur ohne Dokumenteninhalt vor, so wird dieser ausschließlich anhand seines Namens ermittelt: "beispiel.tif.p7" ist die Signaturdatei zu "beispiel.tif".
- ZIP-Container (Dateitypen .zip oder .zip.p7, .zip.pkcs7 etc.): ZIP-Dateien werden in der ersten Ebene analysiert. Enthaltene PKCS#7-Strukturen werden wie oben beschrieben behandelt, mit der Ausnahme, dass in der Nachrichtensicht nur die ZIP-Datei, nicht aber deren Inhalte dargestellt werden. Alle in einer ZIP-Datei gefundenen und geprüften Autorenzertifikate werden in der Nachrichtenübersicht aufgeführt.
- PDF-Inline (Dateityp .pdf): Die Signaturen eines PDF-Dokuments werden geprüft. Ebenso werden Sammlungen von PDF-Dokumenten in einer PDF-Datei geprüft. Es werden nur PDF-Dateien, die in einem PDF enthalten sind, geprüft.

Die verschiedenen Signaturtypen werden detailliert in dem vom BSI veröffentlichten Dokument "Grundlagen der elektronischen Signatur" erläutert.

Der Dateityp eines eingebetteten Dokuments (enveloping-Signaturformat) muss immer im Dateinamen enthalten ist. Der Dateiname der PKCS7-Datei darf nicht verändert werden (Beispiel: Dateiname.doc.pkcs7). Andernfalls kann die Datei nicht geöffnet werden.

5 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.xjusitz.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 soll 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.

Übergangsweise, d.h. bis alle Projekte auf “xjustiz_nachricht.xml” als Anhang umgestellt haben, wird erlaubt, anstelle dieses Anhangs die XJustizdaten direkt als Inhalte der “nachricht.xml” und “nachricht.xsl” zu übertragen.