Sicherer elektronischer Datenaustausch mit den Gerichten und Strafverfolgungsbehörden

Eckpunktepapier

Niedersachsen

Dokumenteninformation

Autoren	Tobias Waltemathe (IT.N, FG 12)
Version	1.1

Änderungshistorie

Version	Status	Änderung	Datum
0.1	In Erstellung	Erstversion	20.07.2017
0.2	In Erstellung	Abschnitte 1, 2	31.08.2017
0.3	In Erstellung	Abschnitte 3, 4, 5	04.08.2017
0.4	In Erstellung	Abschnitte 6, 7, 8	07.08.2017
0.5	In Erstellung	Anmerkungen Lutz Vorwerk	11.08.2017
0.6	In Erstellung	Anmerkungen von Dr. Hube	21.08.2017
0.7	In Erstellung	Anhang ergänzt	23.08.2017
0.8	In Erstellung	Anmerkungen MJ, Referat 103	28.08.2017
0.9	In Abstimmung	IT.N intern	30.08.2017
1.0	Freigabe IT.N	Abschnitt 5.3 und Abschnitt 1 ergänzt	14.09.2017
1.1	Freigabe	Stellungnahme MJ eingearbeitet	12.10.2017

Inhaltsverzeichnis

1 Informationen zum Dokument

Das Eckpunktepapier soll als Entscheidungsgrundlage für die Festlegung eines Datenaustauschverfahrens aufgrund der neuen Regelungen für den elektronischen Rechtsverkehr von Behörden sowie juristischen Personen des öffentlichen Rechts mit den Gerichten und Strafverfolgungsbehörden ab dem 01.01.2018 dienen.

Den rechtlichen Rahmen bilden das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten (eJustice-Gesetz) vom 10. Oktober 2013 (BGBl. I S. 3786)[1] der Entwurf der Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (E-ERVV)[2] mit Stand vom 26.05.2017 sowie das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5. Juli 2017 (BGBl. I S. 2208 ff.)[3]. Weitergehende Informationen zu möglichen technischen Umsetzungen sind dem Arbeitspapier Neue Regelungen für den Elektronischen Rechtsverkehr mit den Gerichten ab 01.01.2018 mit Stand 26.07.2017, Version 1[4] der Arbeitsgruppe IT-Standards der Bund-Länder-Kommission für Informationstechnik in der Justiz (BLK-AG IT-Standards) entnommen.

Das Eckpunktepapier wurde im Auftrag des MI (Referat 42) erstellt. Zur Einordnung der Thematik sollte eine Darstellung der Rechtslage und der Gründe für die Einführung eines weiteren Datenaustauschverfahrens vorgenommen werden. Auf diesen Erkenntnissen aufbauend sollten infrage kommende Lösungsmöglichkeiten mit ihren Vor- und Nachteilen beschrieben und eine Empfehlung für das geeignetste Verfahren abgeleitet werden. Für die Umsetzung der Empfehlung sollte zudem eine Skizze des weiteren Vorgehens vorgenommen sowie die Schritte zur Einführung vorgeschlagen werden.

Im Rahmen der Erstellung stand gemäß des Auftrages die konkrete Umsetzung der gesetzlichen Anforderungen der E-ERVV auf der Basis von etablierten Technologien und Prozessen im Mittelpunkt der Betrachtungen. Eine kurze strategische Einordnung hinsichtlich zu treffender Entscheidungen bezüglich Infrastruktur und Regelungen für einen einheitlichen, rechtssicheren Übermittlungsweg für elektronische Dokumente von Behörden innerhalb der Landesverwaltung ist in Abschnitt 3 hinterlegt.

Nicht Ziel dieses Eckpunktepapieres ist, die strategische und technische Beurteilung der Auswirkungen auf unterschiedliche Ressorts zu untersuchen.

---

[1] abrufbar unter https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%27bgbl113s3786.pdf%27%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl113s3786.pdf%27%5D__1500974897994

[2] abrufbar unter http://ec.europa.eu/growth/tools-databases/tris/de/index.cfm/search/?trisaction=search.detail&year=2017&num=229&dLang=DE

[3] abrufbar unter http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2208.pdf

[4] BLK-AG IT-Standards (2017) abrufbar unter http://www.egvp.de/behoerdenpostfach/Informationsmaterial_fuer_Behoerden_zu_BeBPo_und_eEB_V1.pdf

2 Rechtslage

Behörden sowie Körperschaften und Anstalten des öffentlichen Rechts sind aufgrund der neuen gesetzlichen Regelungen[5] ab 1. Januar 2018 verpflichtet, einen sicheren Übermittlungsweg für die Zustellung elektronischer Dokumente zu eröffnen. § 130a Abs. 3 ZPO und § 32a Abs. 3 StPO sehen nunmehr vor, dass elektronische Dokumente mit einer qualifizierten elektronischen Signatur zu versehen sind oder von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden müssen. Zulässig ist somit die Übersendung über ein Elektronisches Gerichts- und Verwaltungspostfach (EGVP), soweit alle Dokumente qualifiziert elektronisch signiert sind.

Sichere Übermittlungswege sind nach § 130a Abs. 4 ZPO sowie § 32a Abs. 4 StPO ab dem 1.1.2018 De-Mail mit Anmeldebestätigung, das besondere elektronische Anwaltspostfach (beA), das besondere elektronische Notarpostfach (beN) und das besondere elektronische Behördenpostfach (beBPo), soweit die E-ERVV wie vorgesehen in Kraft tritt[6]. Somit sind auch diese vier Übermittlungswege zulässig. Das beA ist nur für Rechtsanwältinnen und Rechtsanwälte und das beN nur für Notarinnen und Notare vorgesehen.

Darauf aufbauend regelt der Entwurf der ERVV erstmals einheitlich den elektronischen Rechtsverkehr mit den Gerichten der Länder und des Bundes. Dazu zählen Zivil-, Familien-, Arbeits-, Sozial-, Verwaltungs- und Finanzgerichte. Es werden die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs sowie für ein besonderes elektronisches Behördenpostfach (beBPo) definiert. Der elektronische Zugang zu diesen Gerichten soll dadurch für alle Bürgerinnen und Bürger, die Rechtsanwältinnen und Rechtsanwälte, die Behörden und übrigen Verfahrensbeteiligten nach einheitlichen technischen Regelungen eröffnet werden. Im Verordnungsentwurf ist zudem vorgesehen, allen Behörden der Länder und des Bundes sowie den juristischen Personen des öffentlichen Rechts zu ermöglichen, über den sicheren Übermittlungsweg eines beBPo mit den Gerichten, Gerichtsvollzieherinnen und Gerichtsvollziehern zu kommunizieren. Eine qualifizierte elektronische Signatur der eingereichten Dokumente wird dadurch entbehrlich[7].

Durch die Regelungen im Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs ist ab dem 1.1.2018 der elektronische Rechtsverkehr auch im Straf- und Ordnungswidrigkeitenverfahren eröffnet (soweit Bund und Länder nicht von den vorgesehenen opt-out-Möglichkeiten Gebrauch machen). Somit wird es erforderlich, dass auch bei den Landes-Ordnungsbehörden die Voraussetzungen für die Eröffnung des elektronischen Rechtsverkehrs vorliegen; dies umfasst auch Zoll und Steuerfahndung. Die technischen

[5] gemäß § 130a Abs. 4 Nr. 3 ZPO , gleichlautend mit § 55a Abs. 4 Nr. 3 VwGO, § 46c ArbGG, § 65a SGG und § 52a FGO; sowie gemäß § 32a Abs. 4 Nr. 3 StPO, jeweils in der ab 1. Januar 2018 geltenden Fassung

[6] § 32a Abs. 4 Nr. 3 StPO verweist auf Abs. 2 Satz 2, wonach ebenfalls eine Bundes-VO die für die Übermittlung und Bearbeitung geeigneten technischen Rahmenbedingungen bestimmen wird.

[7] http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Elektronischer_Rechtsverkehr_VO.html

Rahmenbedingungen sind ebenfalls in einer (vom BMJV noch zu erarbeitenden) Verordnung zum ERV (bzw. einer Ergänzung zur E-ERVV) festzulegen.

Darüber hinaus führen die Änderungen von § 174 Absatz 3 und 4 ZPO durch das eJustice-Gesetz dazu, dass für elektronische Dokumente, die über den sicheren Übermittlungsweg durch die Gerichte zugestellt wurden, der Empfang durch ein elektronisches Empfangsbekenntnis nachgewiesen werden muss. Dieses ist in strukturierter maschinenlesbarer Form zu übermitteln. Die Strukturdaten werden vom Gericht zur Verfügung gestellt. Das zukünftige Empfangsbekenntnis besteht aus einem Datensatz, der die üblichen Informationen enthält.

Zusätzlich sind gemäß § 2 Absatz 2 E-ERVV bei der Übermittlung elektronischer Dokumente bestimmte Metadaten als strukturierte Datensätze beizufügen.

Zusammenfassend ergeben sich aus diesen neuen gesetzlichen Regelungen ab 1. Januar 2018 somit die folgenden wesentlichen Änderungen:

1. Empfangsbereitschaft der Behörden:
   Behörden und Anstalten des öffentlichen Rechts sind verpflichtet, einen sicheren Übermittlungsweg für die Zustellung elektronischer Dokumente zu eröffnen. Es gilt eine „passive Nutzungspflicht“ für das beBPo oder De-Mail. Landesbehörden müssen die technischen Voraussetzungen für den sicheren Übermittlungsweg erfüllen und den Zugang von Mitteilungen zur Kenntnis nehmen.
2. Zustellung gegen elektronisches Empfangsbekenntnis:
   Ein elektronisches Empfangsbekenntnis muss in strukturierter, maschinenlesbarer Form an das Gericht übermittelt werden, sofern Dokumente elektronisch vom Gericht übermittelt wurden.
3. Übermittlung von Strukturdaten:
   Bei der Übermittlung elektronischer Dokumente an das Gericht sind bestimmte Metadaten als strukturierte Datensätze anzufügen.

Diese Maßnahmen dienen der Etablierung der neuen Übertragungswege, um ab 1. Januar 2022 einen durchgehend elektronischen Schrift- und Dokumentenverkehr mit den Zivil-, Familien-, Arbeits-, Sozial-, Verwaltungs- und Finanzgerichten zu ermöglichen (Nutzungsverpflichtung aus dem eJustice-Gesetz §130d ZPO).

3 Weitere Gründe für die Einführung eines weiteren Datenaustauschverfahrens

Oberstes Ziel zur Einführung eines weiteren sicheren Übermittlungsweges und dem darauf aufsetzenden Datenaustauschverfahren ist die Schaffung eines für Bund und Länder einheitlichen Verfahrens. Dieses erleichtert den Zugang für alle Kommunikationsteilnehmer und stellt in erster Linie einen vertrauenswürdigen Übermittlungsweg mit einfacher Signatur ohne den Einsatz einer qualifizierten elektronischen Signatur sicher.

Darüber hinaus bietet die zusätzliche Übermittlung von strukturierten Daten und sogenannten Metadaten zu den Nachrichten und Dokumenten die Möglichkeit, diese in weiteren Schritten automatisiert zu verarbeiten. Ziel muss es sein, strukturierte Daten und nicht nur Texte zu übertragen. So können Dokumente, beispielsweise ohne diese manuell durch Bedienstete der Gerichte prüfen zu lassen, automatisiert dem jeweiligen Verfahren zugeordnet werden. Die Datensatzformate der spezifischen Strukturdaten werden von der Justiz zentral veröffentlicht oder sind bereits Teile des Standards XJustiz[8]. Folglich sollten zukünftig Verzögerungen minimiert, Aufwände durch die automatische Auswertung und Prüfung reduziert sowie medienbruchbedingte Fehler weitestgehend vermieden werden. Auch lässt sich schnell eine Übersicht über Zustellversuche und weitere historische Arbeitsschritte belegen.

Da alle Behörden der Landesverwaltung ab dem 1. Januar 2018 einen ZPO-und StPO-konformen sicheren Übermittlungsweg eröffnen müssen, bietet sich die Chance, diesen Kanal auch für die einfache und rechtssichere Kommunikation der Behörden untereinander sowie mit Dritten wie zum Beispiel Anwältinnen und Anwälten zu nutzen. In einem weiteren Schritt kann die Anwendung in Kombination mit strukturierten Metadaten ausgebaut werden, um dadurch ebenfalls rechtssichere Prozesse rund um die Zuordnung von elektronischen Dokumenten zu automatisieren. Als Anwendungsbeispiel sei die elektronische Poststelle für die E-Rechnung genannt. Der Datensatz im Format XRechnung samt rechnungsbegleitender Unterlagen wird an ein Postfach gesandt, das die Informationen zur weiteren Verarbeitung weiterleitet, prüft und abschließend im zentralen DMS ablegt bzw. einer eAkte zuordnet.

Zusammenfassend bieten sich aus strategischer Sicht die Chancen,

- den Zugang zu Gerichten zu vereinheitlichen,
- Aufwände zu reduzieren,
- Abläufe zu optimieren und dadurch Verzögerungen zu vermeiden und
- die Infrastruktur und Regelungen für einen einheitlichen, rechtssicheren Übermittlungsweg für elektronische Dokumente von Behörden innerhalb der Landesverwaltung zu schaffen.

8 http://www.xjustiz.de/index.php

4 Anforderungen an ein besonderes elektronisches Behördenpostfach (beBPo)

Die Anforderungen an ein beBPo werden in Kapitel 3 §§ 6-9 E-ERVV definiert.

So muss dieses technisch und funktional

- auf dem Protokollstandard OSCI oder einem diesen ersetzenden Nachfolger beruhen,
- die Kommunikation muss Ende-zu-Ende verschlüsselt sein,
- der Postfachinhaber in ein sicheres elektronisches Verzeichnis eingetragen sein,
- eine Suchfunktion für den Verzeichnisdienst implementiert sein,
- dadurch auch für andere besondere elektronische Postfächer (beA, beN, EGVP) adressierbar sein und
- gemäß der Barrierefreie-Informationstechnik-Verordnung[9] eine Zugänglichkeit für alle Nutzer ermöglichen.

Organisatorisch wird vorausgesetzt, dass

- die Identität des Postfachinhabers in einem Identifizierungsverfahren geprüft und bestätigt wird,
- die zuständige oberste Behörde dazu eine/mehrere öffentlich-rechtliche Stellen bestimmt, welche die Identität der Behörden oder juristischen Personen des öffentlichen Rechts prüfen und im elektronischen Verzeichnis bestätigen,
- und die im Rahmen des Identifizierungsverfahrens prüft, ob die Voraussetzungen erfüllt sind. (Der Antragsteller ist eine inländische Behörde oder juristische Person des öffentlichen Rechts und der Name sowie der Sitz des zu prüfenden Postfachinhabers sind zutreffend bezeichnet.)

Zudem wird hinsichtlich des Zugangs geregelt, dass

- der Postfachinhaber selbst entscheidet (Behördenleitung, gesetzlicher Vertreter), welche natürlichen Personen Zugang zum beBPo erhalten,
- diesen das Zertifikat und Zertifikats-Passwort zur Verfügung stellt und
- eine Dokumentationspflicht (Befugnisse und Berechtigungen, Zertifikatsbereitstellung) besteht.

Zum Abschluss ist noch einmal hervorzuheben, dass die Formulierungen im E-ERVV den Behörden die Wahl lassen, ob sie sich eines beBPo bedienen oder einen anderen sicheren Übermittlungsweg eröffnen. Ein Alternativweg muss jedoch die beschriebenen Anforderungen in jedem Fall erfüllen. Gleichwohl sollte eine einheitliche Lösung angestrebt werden, um eine direkte Interoperabilität der Postfächer untereinander zu gewährleisten.

9 https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html

5 Mögliche Datenaustauschverfahren

Nachfolgend werden rechtssichere Datenaustauschverfahren mit den Gerichten beschrieben.

5.1 Elektronisches Gerichts- und Verwaltungspostfach (EGVP)

Das EGVP ist die seit 2004 etablierte Infrastruktur, um in elektronischer Form rechtswirksam mit teilnehmenden Gerichten und Behörden zu kommunizieren. EGVP garantiert eine sichere und zuverlässige Übertragung durch Nutzung des Standards OSCI-Transport[10]. OSCI steht für Online Services Computer Interface und ist eine Sammlung von Netzwerkprotokollen die in erster Linie auf die Kommunikationsanforderungen der öffentlichen Verwaltung und auf E-Governmentvorhaben zugeschnitten sind. Der Standard beschreibt die vertrauliche und sichere Übermittlung von Nachrichten in einer auf das deutsche Signaturgesetz abgestimmten Sicherheitsumgebung.

Der elektronische Rechtsverkehr mit EGVP wurde durch die Justiz eröffnet und ist in Niedersachsen rechtswirksam geregelt durch die Niedersächsische Verordnung über den elektronischen Rechtsverkehr in der Justiz (Nds. ERVVO)[11]. Aufgrund der sich in Abschnitt 2 dargestellten ändernden Rechtslage ab Januar 2018 wird zukünftig diese Landesverordnung in großen Teilen obsolet und es findet bundesweit überwiegend eine einheitlich geregelte Öffnung der Gerichte und Staatsanwaltschaften statt[12]. Bereits mit Stichtag 01.01.2016 wurde die verpflichtende Nutzung von EGVP für Anwältinnen und Anwälte sowie Notarinnen und Notare mit Änderungen am Gesetz zur Förderung des elektronischen Rechtsverkehres modifiziert. Das EGVP wurde um das besondere elektronische Anwaltspostfach (beA) bzw. das besondere elektronische Notarpostfach (beN) ergänzt. Diese werden von der Bundesrechtsanwaltskammer (BRAK) für Rechtsanwältinnen und Rechtsanwälte sowie der Bundesnotarkammer (BNOTK) für Notarinnen und Notare betrieben.

Die EGVP-Infrastruktur wurde im Jahr 2006 im Rahmen der Maßnahmen zur Erfüllung der EU-Dienstleistungsrichtlinie (EU-DLR, 2006/123/EG) in der niedersächsischen Landesverwaltung eingeführt. Rund 570 öffentliche Einrichtungen und Verwaltungen nutzen das EGVP[13]. Die technische Umsetzung der Einführung verantwortete IT.Niedersachsen. Dazu zählte zum einen als Intermediär der Aufbau und Betrieb einer zentralen virtuellen Poststelle (VPS) und zum anderen die Ausstattung der Behörden mit EGVP-Komponenten wie Anwendungsinstallation, Signaturkarten- und Zertifikatsbereitstellung, die Einrichtung der Postfächer sowie die Aufnahme in den SAFE-Verzeichnisdienst. IT.N bietet den Betrieb von EGVP-Postfächern als Dienstleistung an. Die jährlichen Kosten hierfür liegen derzeit bei 65,00€ pro Postfach (EGVP-Backend Postfach mit 500 MB).

---

[10] http://www.xoev.de/detail.php?gsid=bremen83.c.3355.de
[11] abrufbar unter www.justizportal.niedersachsen.de/download/61965
[12] Ausnahmen bilden z.B. einige Bereiche aus der freiwilligen Gerichtsbarkeit.
[13] abrufbar unter http://www.egvp.de/behoerden/Behoerden_Niedersachsen.pdf

Auf Anwenderseite können verschiedene Ausprägungen von EGVP-Komponenten genutzt werden, um Nachrichten aus der VPS abzuholen, diese zu entschlüsseln und Prüfungen vorzunehmen und zu protokollieren. EGVP ist für die automatisierte Weiterverarbeitung mit XJustiz vorbereitet.

Für Bürgerinnen und Bürger wird ab 2018 ein Onlineformular WEB-EGVP von der Justiz angeboten, mit dem Nachrichten an die Justiz zwar übermittelt aber keine Nachrichten empfangen werden können (Ad hoc-Kommunikation). Andere Benutzergruppen müssen zukünftig ggf. kostenpflichtige OSCI-fähige Software von Drittanbietern nutzen.

Für Niedersachsen besteht seitens MI ein Nutzungsrecht, das EGVP Backend den Kommunen, Kammern und Behörden bereitzustellen. Darüber hinaus besteht mit der Firma Westernacher ein Supportvertrag.

Die BLK-AG IT-Standards weist darauf hin, dass schon vorhandene EGVP-Postfächer die Anforderungen in der jetzigen Form nicht erfüllen und die Zustellung elektronischer Dokumente durch Gerichte ab dem 1. Januar 2018 an solche nicht zulässig sei[14]. Dieses wird damit begründet, dass bestehende EGVP nicht durch ein E-ERVV konformes Identifizierungsverfahren geprüft wurden und über keine postfacheigene Signatur verfügen.

5.2 De-Mail

Mit dem Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (E-Government-Gesetz) wurden ab dem 1. August 2013 die Bundesbehörden unter anderem zur Eröffnung eines De-Mail-Zugangs verpflichtet. Auf Bundesebene wird dafür ein zentrales De-Mail-Gateway betrieben. Einige Bundesländer haben diese Verpflichtung bereits in entsprechende eGovernment-Gesetze aufgenommen.

Diese Regelung gilt jedoch zurzeit noch nicht für niedersächsische Landesbehörden. Die Verbreitung von De-Mail ist dementsprechend sehr gering. Aktuell weist das Teilnehmerverzeichnis für Niedersachsen zwölf Behörden, Kommunen oder Gemeinden mit De-Mail-Adressen aus[15]. Deutschlandweit werden 141 Teilnehmer aus dem Bereich Behörde geführt.

De-Mail kann für sichere und nachweisbare Kommunikation eingesetzt werden und ist ein sicherer Übermittlungsweg im Sinne des § 130a Abs. 4 Nr. 1 ZPO und des § 32a Abs. 4 Nr. 1 StPO. Im Zuge des De-Mail-Gesetzes vom 28. April 2011[16] wurde die Rechtswirksamkeit per Gesetz festgelegt. Der Dienst ist für die Übermittlung sowohl von unstrukturierten als auch von strukturierten Informationen geeignet. Kommunikationspartner können natürliche Personen und alle Arten von Organisationen (juristische Personen sowie Personengesellschaften und öffentliche Einrichtungen) sein[17]. Zur Nutzung

[14] BLK-AG IT-Standards (2017), S. 5
[15] https://www.de-mail.info/verzeichnis.html#land=Niedersachsen&typ=Behoerde, abgerufen am 01.08.2017
[16] http://www.gesetze-im-internet.de/de-mail-g/
[17] http://www.cio.bund.de/SharedDocs/Publikationen/DE/Innovative-Vorhaben/De-Mail/demail_Leitfaden.pdf?__blob=publicationFile

von De-Mail muss sich der Anwender bei einem von dem Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditierten De-Mail-Diensteanbieter (DMDA) anmelden und ein Konto eröffnen. Aktuell gibt es vier privatwirtschaftliche Diensteanbieter[18]. Für den Nachrichtenversand fallen Portokosten an. Sofern beim Empfänger Zustellnachrichten für den Sender generiert werden, erzeugen diese ebenfalls Portokosten.

Zur Nutzung von De-Mail durch Endanwender auf Basis der bestehenden E-Mail-Infrastruktur können vorhandene Clients genutzt werden. Zusätzlich muss hierfür jedoch ein zentrales De-Mail-Gateway aufgebaut, integriert und betrieben werden, um über diesen Weg kommunizieren zu können. Die Anbindung kann zentral bei IT.N durch den Betrieb eines mandantenfähigen Gateways realisiert werden.
Die reine Nutzung eines De-Mail-Webportals ist zwar möglich, wird aber nicht empfohlen, da auf diesem Weg keine Anbindung an eine behördeneigene IT-Infrastruktur, kein automatisierter Versand und keine vollumfängliche Nutzung möglich sind.

Für De-Mail-Postfächer (über ein Webportal oder die Integration über ein Gateway des Diensteanbieters) werden von den Anbietern Basisentgelte und Entgelte pro De-Mail berechnet. Das Basisentgelt beim Anbieter Telekom beträgt z.B. 179,40€ jährlich, die Gebühr pro ausgehender De-Mail 0,33€.

Der Einsatz von De-Mail wurde im Rahmen der Verabschiedung des De-Mail-Gesetzes von Sachverständigen kritisiert, da per Default keine durchgehende Ende-zu-Ende-Verschlüsselung vorliegt[19]. Eine Ende-zu-Ende-Verschlüsselung kann durch den Einsatz von Zertifikaten, zusätzlichen Verschlüsselungsmethoden wie OpenPGP[20] oder S/MIME[21] realisiert werden.

5.3 beBPo

Das beBPo ist ein Teil der bestehenden EGVP-Infrastruktur und stellt eine ERVV-konforme Modifikation dar. Es besteht aus den Komponenten:

- Sende- und Empfangssoftware
- Intermediäre
- Sichere Verzeichnisdienste nach dem SAFE-Standard
- Signatur für den Herkunftsnachweis

---

18 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/DeMail/Akkreditierte_DMDA/Akkreditierte_DMDA_node.html

19 Protokoll der 123. Sitzung des Deutschen Bundestages, S. 10, abrufbar unter http://www.bundesgerichtshof.de/SharedDocs/Downloads/DE/Bibliothek/Gesetzesmaterialien/17_wp/E-Rechtsverkehr_Gerichten_reg/wortproto.pdf?__blob=publicationFile, S.10

20 https://tools.ietf.org/html/rfc2440

21 https://tools.ietf.org/html/rfc2633

Als Sende- und Empfangssoftware für das beBPo kann ein registriertes OSCI-Drittprodukt[22] eingesetzt werden (z.B. der Governikus Communicator als Anwendung des IT-Planungsrates). Alternativ kann mit Hilfe der von der Justiz kostenlos zur Verfügung gestellten Middleware EGVP-Enterprise die Kommunikation des beBPo direkt von Behörden in Fachverfahren integriert werden. Auch die Nutzung einer selbstentwickelten OSCI-konformen Anwendung ist möglich.

Der benötigte Intermediär (VPS) wird bereits von IT.N betrieben.

Ein eigener SAFE-konformer Verzeichnisdienst kann zusätzlich aufgebaut werden. Alternativ können bereits bestehende Verzeichnisdienste der Justiz, der BRAK oder der BNOTK genutzt werden. Diese Verzeichnisdienste bieten die Möglichkeit einer verteilten Administration. Aktuell in Niedersachsen eingerichtete EGVP-Postfächer verwenden bereits den SAFE-Verzeichnisdienst der Justiz.

Für den Herkunftsnachweis wird der Nachricht aus einem beBPo durch die Versendekomponente ein Zertifikat beigefügt, das die Herkunft aus einem beBPo bestätigt. Dieses Zertifikat muss auf einem vertrauenswürdigen Root-Zertifikat basieren, welches für diesen Zweck (Nachweis der Herkunft aus einem beBPo) registriert ist. Dabei handelt es sich um eine Transportsignatur in Form einer fortgeschrittenen Systemsignatur.

Die Ausstellung der Zertifikate sowie den dahinter liegenden Antrags- und Genehmigungsprozess kann durch den SignaturCard Service von IT.N durchgeführt werden. Für die Ausstellung der Zertifikate für den beBPo-Herkunftsnachweis kann alternativ eine von der BLK-AG IT-Standards mit der Bundesnotarkammer erarbeitete Lösung genutzt werden. Über das SAFE-System kann auf eine Webanwendung bei der BNOTK zugegriffen werden. Alle Identitäten, für die die beBPo-Rolle freigeschaltet wurde, können sich dort anmelden, eigenständig ein entsprechendes Zertifikat erstellen und herunterladen. Dieses Zertifikat kann dann in die entsprechende Clientsoftware implementiert werden. Ein Beschluss über das Angebot dieses Service durch die Justiz sowie die kostenfreie Nutzung wird in der 102. Sitzung der Bund-Länder-Kommission für die Informationstechnik in der Justiz im November 2017 erwartet.

Damit aus einem EGVP-Postfach ein beBPo wird, ist diesem im SAFE-Verzeichnisdienst zusätzlich die EGVP-Rolle beBPo zuzuweisen. Diese Rollenzuweisung erfolgt dabei im nach der E-ERVV vorgeschriebenen Identifizierungsverfahren.

Zudem würde die Umsetzung des beBPo eine Überarbeitung der Websites für EGVP und eLearning, einen neuen Supportvertrag sowie die Bereitstellung einer neuen NiC-App erfordern.

IT.N könnte besondere elektronische Behördenpostfächer zukünftig als Dienstleistung anbieten. Hierfür sind ähnliche Kosten zu erwarten wie für EGVP (derzeit 65,00€ jährlich pro Postfach).

[22] http://www.egvp.de/Drittprodukte/index.php

Im Rahmen der Anforderungsermittlung wurde geprüft, ob neben SAFE ein alternativer Verzeichnisdienst genutzt werden könnte. Die Anforderungen an den Verzeichnisdienst für die Verwaltung und Adressierung der beBPo Postfachinhaber werden in der E-ERVV technisch nicht näher definiert. Das Verzeichnis muss sicher, elektronisch, von anderen beBPo-Inhabern per Suche auffindbar und adressierbar sein (E-ERVV § 6). Im Rahmen dieser Definition könnte als Alternative zu SAFE das Deutsche Verwaltungsdiensteverzeichnis (DVDV) eine Alternative darstellen. Dieses wird jedoch organisatorisch und technisch getrennt betrieben und verfügt in der aktuellen Version über keine Schnittstelle zum SAFE-Verbund. Eine Umsetzung der Such- und Adressierbarkeit, um für andere Inhaber von besonderen elektronischen Postfächern ansprechbar zu sein, hätte somit einen administrativen Mehraufwand zur Folge. Eine Synchronisation von Datenbeständen müsste zum heutigen Zeitpunkt manuell durchgeführt werden. Nach Rücksprache mit der Koordinierungsstelle DVDV ist eine neue, flexiblere Version von DVDV für das Jahr 2019 geplant.

6 Beurteilung der Lösungsalternativen

Tabelle 1: Beurteilung der Lösungsalternativen

	EGVP	**De-Mail**	**beBPo auf Basis von EGVP**
Vorteile	■ Sichere und vertrauliche Kommunikation auf Basis von OSCI ■ Flexible Verschlüsselungs- und Signaturmechanismen ■ Starke Verbreitung innerhalb der Justiz und Behörden ■ Etablierte Infrastruktur und Prozesse ■ Entwickelt von der Justiz ■ Vorbereitet für den Versand strukturierter Daten ■ VPS wird zentral im Land betrieben	■ Sichere und vertrauliche Kommunikation rechtswirksam (per Gesetz) ■ Schriftformersatz nach VwVfG ■ Nutzung der bestehenden internen E-Mail-Infrastruktur ■ Automatisierter Versand und Weiterverarbeitung möglich ■ Kann auch für die schriftformersetzende Kommunikation mit Bürgerinnen, Bürgern und Unternehmen eingesetzt werden	■ Die rechtlichen Anforderungen an das beBPo werden von der bereits etablierten Infrastruktur des EGVP erfüllt ■ Technische Vorteile s. EGVP ■ Alle erforderlichen Komponenten stehen für die Behörden bereits zur Verfügung ■ keine qualifizierte elektronische Signatur von Dokumenten für die Einreichung bei Gerichten notwendig
Nachteile	■ Komplizierter Nachrichtenversand mit Signaturkarte, Kartenleser und Passwort	■ Zentrales, mandantenfähiges De-Mail-Gateway zur Provideranbindung und Integration der E-Mail-Infrastruktur notwendig ■ Gateway zur Anbindung an die EGVP-Infrastruktur notwendig, Justiz wandelt De-Mail wieder in EGVP ■ Beschaffung von Zugängen beim DMDA notwendig ■ Zusätzliche Transaktionsgebühren für Versand und Rückantwort ■ De-Mail bisher nicht etabliert	■ Noch kein rechtswirksamer, Schriftformersatz nach VwVfG ■ Nicht für die schriftformersetzende Kommunikation mit Bürgerinnen, Bürgern und Unternehmen einsetzbar

		■ Ende-zu-Ende-Verschlüsselung nur mit zusätzlicher Konfiguration (Krypto-Gateway, Verschlüsselungs-Plug-Ins, Signaturanwendungen) möglich ■ Zusätzliche Klärung datenschutzrechtlicher Fragestellungen notwendig ■ Aufbau von Supportprozessen ■ Vollständige (technische) Verfahrenskonzeption notwendig ■ Vergabeverfahren notwendig	
Beurteilung hinsichtlich ERVV	EGVP ist kein zugelassener sicherer Übermittlungsweg des § 130a Abs. 4 ZPO.	De-Mail erfüllt die Anforderungen.	beBPo erfüllt die Anforderungen.

7 Empfehlung für elektronisches Datenaustauschverfahren zur Umsetzung des eJustice-Gesetzes

Aus den aufgezeigten Vor- und Nachteilen in Tabelle 1 kann abgeleitet werden, dass für einen sicheren Übermittlungsweg für die elektronische Kommunikation mit den Gerichten auf das beBPo gesetzt werden sollte. Auch die Justiz empfiehlt die Verwendung dieser Lösungsalternative, „[…] da es alle fachlichen Anforderungen abbildet und auf die Anbringung von qualifizierten elektronischen Signaturen verzichtet werden kann."[23] Das beBPo beruht auf der Infrastruktur des EGVP, die sich für den elektronischen Rechtsverkehr seit 2004 bewährt habe. Ein wesentlicher Punkt ist zudem, dass alle erforderlichen Komponenten dieser Infrastruktur den Behörden schon jetzt bereitstehen. Zudem besteht ein konkreter zeitlicher Handlungsbedarf, um die Anforderungen zum Januar 2018 erfüllen zu können.

Die Einführung einer De-Mail-Infrastruktur bedarf einer tiefergehenden Analyse-, Planungs- und Beschaffungsphase.

Die Voraussetzungen des § 6 E-ERVV werden durch die EGVP-Infrastruktur und damit auch durch das auf dieser basierenden beBPo erfüllt.

Vor einer endgültigen Entscheidung für das Land Niedersachsen sollte eine Antwort des Bundesministeriums des Innern auf die Prüfbitte zur Nutzung des beA im Verwaltungsverfahren (Beschluss 2017/16 des IT-Planungsrates Bund/Länder) abgewartet werden. Diese steht derzeit noch aus. Konkret hat der IT-PLR das BMI unter Einbeziehung der Fachministerkonferenzen darum gebeten zu prüfen, ob das beA auch bei der Kommunikation mit den Behörden sinnvoll eingesetzt werden könne, um eine durchgängige medienbruchfreie elektronische Kommunikation zwischen Anwaltschaft, Verwaltung und Gerichten zu ermöglichen. Zudem sollen durch das BMI und das BMJV die rechtlichen Rahmenbedingungen überprüft werden, um das beA und damit auch ein beBPo zum schriftformersetzenden Versand von elektronischen Nachrichten nach VwVfG in diesem Kontext nutzen zu können.

[23] BLK-AG IT-Standards (2017), S. 2

8 Weiteres Vorgehen / zu treffende Entscheidungen

Im Dokument der BLK-AG IT-Standards (2017, S. 6-8) werden die allgemeinen technischen und organisatorischen Voraussetzungen für die Nutzung eines beBPo beschrieben. Da die niedersächsische Landesverwaltung bereits über EGVP-Komponenten verfügt, ist der Weg für Behörden, ein bereits vorhandenes EGVP-Postfach in ein beBPo umzuwandeln, bereits vorbeschrieben. Folgende Schritte sind notwendig:

- Bestimmen der beBPo-Prüfstelle(n) des Landes durch die obersten Landesbehörden (nds. IT-Planungsrat)
- Festlegung auf BNOTK als SAFE-Verzeichnisdienstanbieter und IT.N als SAFE-Identitätsadministrator (Berechtigung durch MJ)
- Installation der aktuellen Governikus Version (Intermediär) durch IT.N
- Entscheidung durch MI, für wen Zertifikate ausgestellt werden
- Prüfung der Identität und Zuordnung der EGVP-Rolle beBPo durch die zuständige beBPo-Prüfstelle
- Beschaffung und Einbindung eines fortgeschrittenen Signaturzertifikates, das zur Anbringung des Herkunftsnachweises geeignet ist
- EGVP-Update nach beBPo mit vorangehenden Informationsschreiben durch IT.N
- Migration bestehender EGVP-Postfächer von Behörden und Kommunen nach beBPo und
- Dienstanweisung zur Dokumentation, wer zugangsberechtigt ist, wann das Zertifikat und das Zertifikatspasswort zur Verfügung gestellt wurden und wann die Zugangsberechtigung aufgehoben wurden.

Zudem wird die Justiz kostenlos eine Web-Anwendung bereitstellen, um elektronische Empfangsbekenntnisse anzunehmen und übermitteln zu können. Die Strukturdaten werden im Format XJustiz als Anlage einer EGVP-Nachricht an ein beBPo übermittelt. Diese Anwendung soll auch eine Visualisierungskomponente sowie eine Funktion zur Erzeugung eines rücklaufenden elektronischen Empfangsbekenntnisses beinhalten (BLK-AG IT-Standards, S. 12-13).

Die Definitions- und Schemadateien sowie eine Anwendung zur Übermittlung von weiteren Strukturdaten gemäß § 2 E-ERVV werden noch von der Justiz veröffentlicht. Soweit schon jetzt ein elektronischer Rechtsverkehr mit der Justiz aus Fachanwendungen heraus stattfindet, sollte nach Veröffentlichung der Standards geprüft werden, ob erweiterter Anpassungsbedarf besteht.

Die nachfolgende Abbildung verdeutlicht noch einmal die Funktionsweise von beBPo:

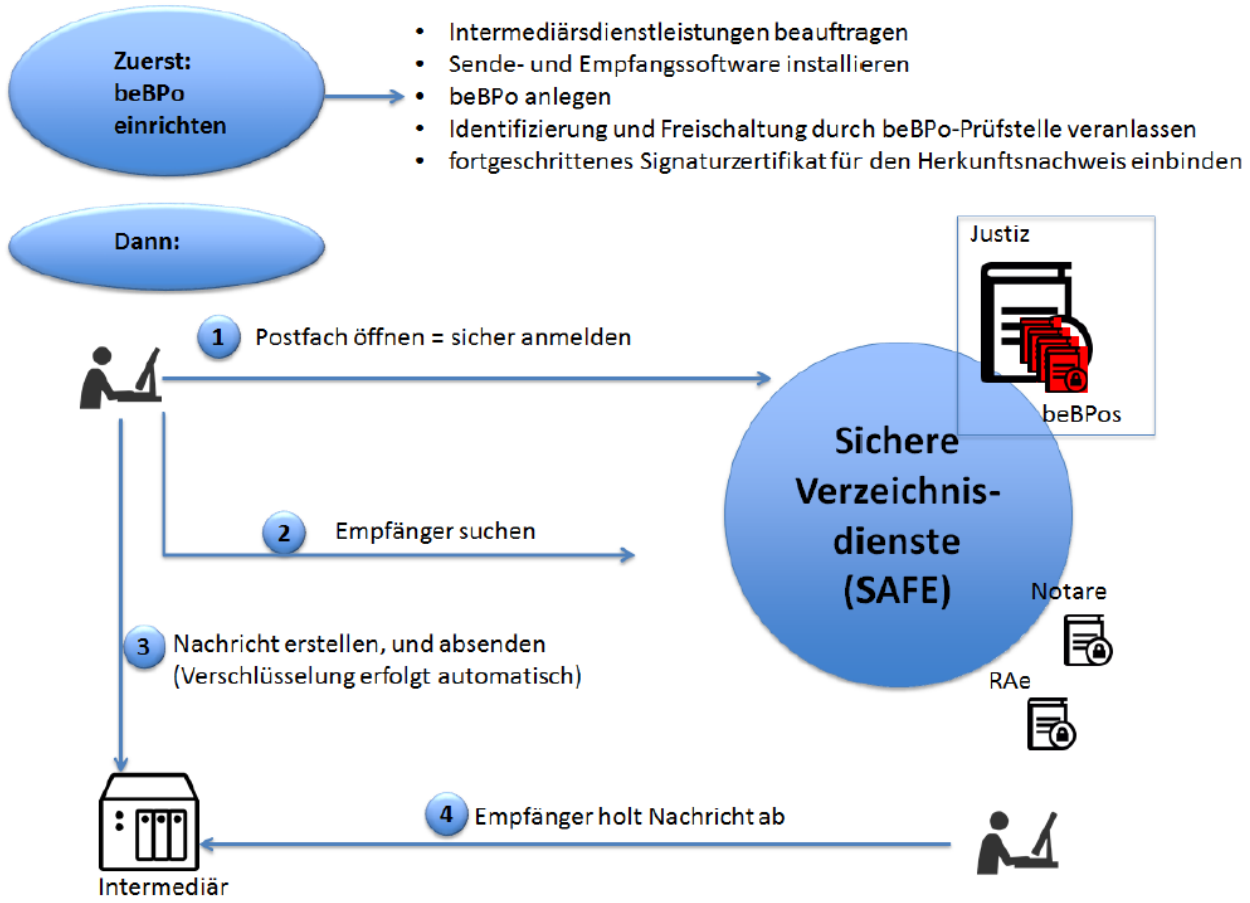


Abbildung 1: Funktionsweise beBPo (BLK-AG IT-Standards (2017), S. 3)

Skizze der Einführung und des Betriebes des neuen Basisdienstes:

- Klärung ob Rollout, Betrieb und Support für Behörden wie bei EGVP extern beauftragt wird (EGVP extern Westernacher)
- Weiternutzung des SAFE-Verzeichnisdienstes der Justiz/Bundesnotarkammer
  - Der Aufbau eines eigenen SAFE-konformen Verzeichnisdienstes wird nicht empfohlen
- Überarbeitung der Webseiten für EGVP und eLearning
- Abschluss eines neuen/erweiterten Supportvertrages für beBPo
- Bereitstellung einer neuen Version der NiC-App
- Implementierung des Zertifizierungsprozesses nach Benennung der Verantwortlichen
- Selbstverwaltung der beBPo-Nutzer durch Behörden
- Rechtswirksame Kommunikation der Behörden untereinander über die beBPos
- NAVO Integration

Die Zuständigkeiten zu den einzelnen Tätigkeiten sind in Tabelle 2 im Anhang aufgeführt.

Anhang

Zuständigkeiten Einführung und Betrieb beBPo

Tabelle 2 gibt eine Übersicht, welche Tätigkeiten im Rahmen der Einführung sowie im laufenden Betrieb von beBPo anfallen. Die Zuständigkeiten werden benannt. Diese Übersicht kann als Grundlage für eine konkrete Aufwandsschätzung und Angebotserstellung dienen.

Tabelle 2: Zuständigkeiten

Einmalige zentrale Aufwände	**Zuständig**	**Anmerkungen, Beschreibung**
Einrichtung der zentralen Prüfstelle	Oberste Landesbehörde, IT.N	Festlegung der Verantwortlichkeiten; Implementierung Zertifizierungsprozess im SignaturCard Service
Installation Intermediär	IT.N	Ein geplantes Update auf das neue Release ist bereits für Oktober 2017 avisiert.
beBPo-NiC-App	IT.N	Das neue SW-Paket beinhaltet lediglich die Umbenennung
Überarbeitung der Dokumentation	MI, ZIB (IT.N)	Webseiten für EGVP, eLearning und Filmmaterial https://www.eu-dlr.niedersachsen.de/egvp_signaturen/egvpostfaecher/ http://intra.app-olg-ce.niedersachsen.de/elearn/egvp/
Informationsschreiben zur Migration durch IT.N	IT.N	Erstellen und verteilen der Migrationshinweise/Einführung eines beBPo
Abschluss Supportvertrag	MI, IT.N, extern	Klärung der Vertragsgrundlage mit Westernacher für den EGVP/beBPo-Support
Rolloutkoordination und Durchführung	IT.N, extern	
Einmaliger Aufwand je Kunde		
Prüfung der Identität und Zuordnung der EGVP-Rolle beBPo	Zentrale Prüfstelle	

Beschaffung eines fortgeschrittenen Signaturzertifikates	IT.N	SignaturCard Service; alternativ: Nutzer (Identität mit beBPo-Rolle) eigenständig
Einrichtung des beBPo	IT.N	Einrichtung des Postfachs in der VPS, Eintrag und Zuweisung der Rolle im SAFE-Verzeichnis, hinterlegen des Zertifikats
EGVP-Update	IT.N	Supportaufwand
Laufender zentraler Betriebsaufwand		
beBPo Support extern	MI, MJ, extern	Neuer Supportvertrag mit Westernacher? https://www.eu-dlr.niedersachsen.de/egvp_signaturen/egvpostfaecher/102705.html
beBPo Support intern	IT.N	
Laufender Betriebsaufwand je Kunde		
Postfach der Virtuellen Poststelle (VPS)		derzeit LS0054, monatliche Abrechnung, Postfach, Speicherplatz, Zertifikat, Support
Laufender organisatorischer Aufwand bei den Kunden		
Dienstanweisung, Dokumentation und Verwaltung der Zugangsberechtigung		

Prozess Einrichtung beBPo

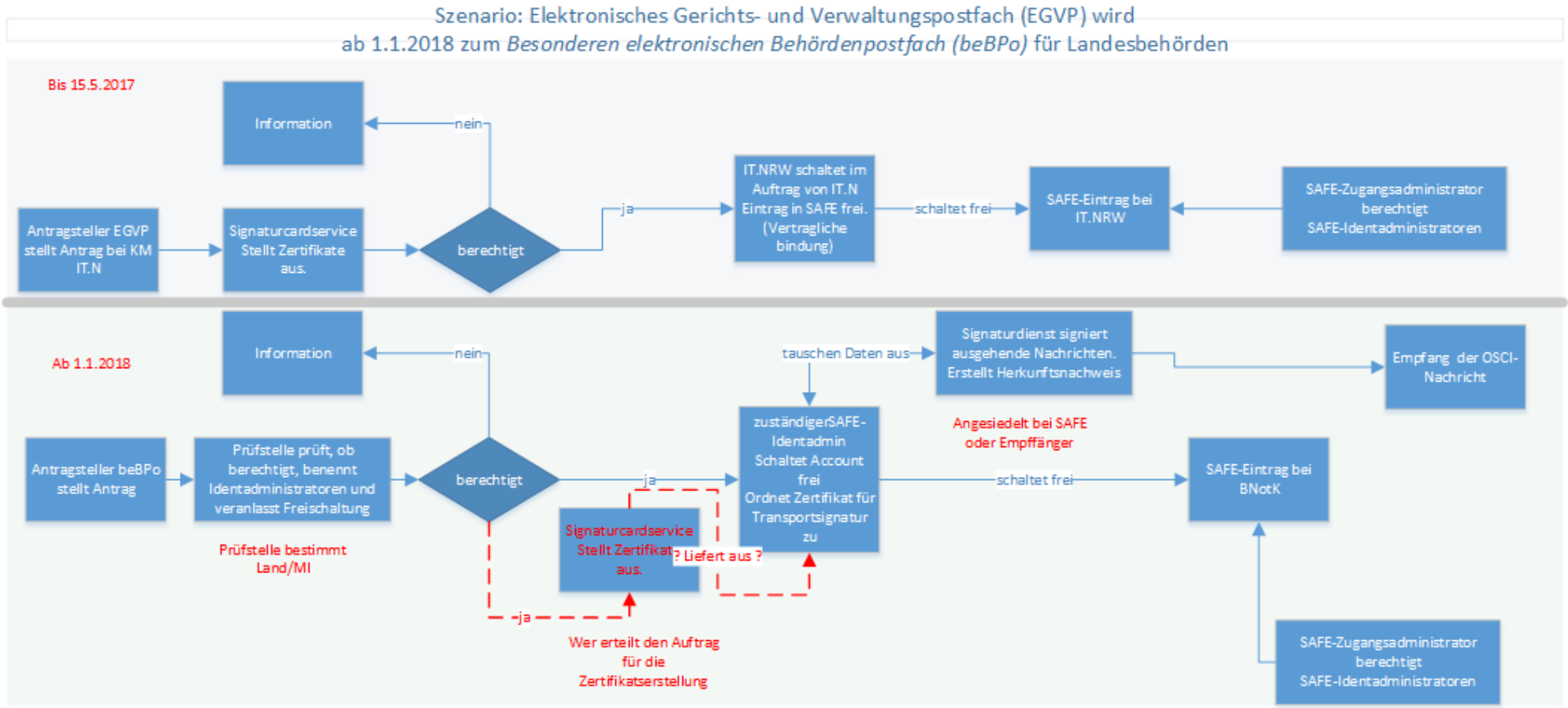
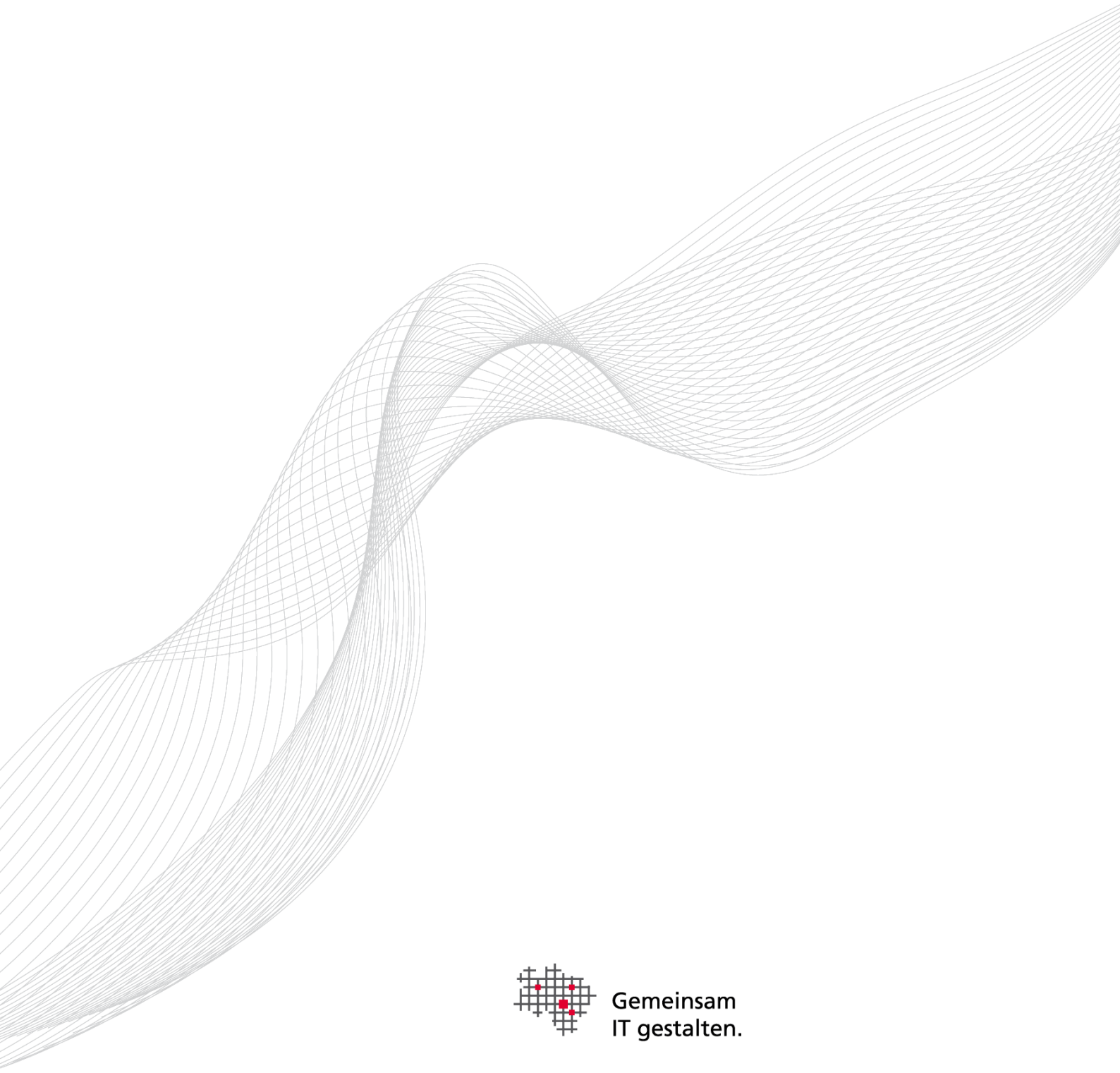


Abbildung 2: Prozess Einrichtung beBPo



Gemeinsam
IT gestalten.

Herausgeber
Landesbetrieb IT.Niedersachsen
Göttinger Chaussee 259
30459 Hannover

Telefon +49 511 9898-0
Telefax +49 511 9898-4901
poststelle@it.niedersachsen.de

www.it.niedersachsen.de

September 2017