Vertrauenswürdiger Herkunftsnachweis (VHN) 2

Spezifikation

Version 2.2
Stand 09.12.2021

A. Anlass

Das Konzept für den Vertrauenswürdigen Herkunftsnachweis (VHN) wurde für die Einführung der eBOs und für die Anbindung der Postfach- und Versanddienste des Verwaltungsportals im Sinne des § 2 Abs. 2 OZG fortgeschrieben und die erforderliche Standarderweiterungen spezifiziert.

Gleichzeitig wird mit dem VHN 2 sichergestellt, dass nur noch identifizierte Nutzer an der EGVP-Infrastruktur teilnehmen bzw. Nachrichten von nichtidentifizierten Nutzern automatisiert abgewiesen werden können (z.B. bei DoS-Attacken).

Der VHN und der VHN 2 können bis zur Abkündigung des VHN im Parallelbetrieb genutzt werden.

B. Rahmenbedingungen

Der technischen Spezifikation liegen folgenden Annahmen zugrunde:

- Das Schriftformerfordernis nach § 130 a ZPO ist erfüllt, wenn bei der Nutzung eines besonderen Übermittlungsweges der Versand durch den Absender aus seinem besonderen Postfach nach sicherer Anmeldung erfolgt.

- Für Behörden und Organisationen (juristische Personen und nichtrechtsfähige Personenvereinigungen) gilt dabei, dass ein berechtigter Vertreter der Behörde bzw. der Organisation den Versand aus dem beBPo der Behörde bzw. dem eBO der Organisation vornimmt.
  Die Identität der natürlichen Person, die für die Behörde oder Organisation schriftformersetzend versandt hat, ergibt sich geregelt, aus der einfachen Signatur des beigefügten Dokumentes (§ 130a ZPO). Die Behörden/Organisationen müssen somit durch interne – ggf. auch technische – Maßnahmen sicherstellen, dass nur berechtigte Personen Zugriff auf die Versandfunktion des beBPos bzw. des eBOs haben.

- Für die Einrichtung, Verwaltung und Verzeichnung der EGVP-Postfachinhaber werden sogenannte **SAFE-Domainen, die über den Virtuellen Attributservice föderiert sind,** bereitgestellt.

- Die Authentizität und die sichere Anmeldung werden innerhalb dieser SAFE-Domainen und auf der Grundlage der gesetzlichen Vorschriften sichergestellt. Hierfür werden die Post-

fachinhaber in diesen SAFE-Domainen nach den Vorgaben der gesetzlichen Regelungen registriert. Auch die Anmeldung der Postfachinhaber erfolgt nach den Vorgaben der gesetzlichen Regelungen.

- Für das beA stellt die BRAK eine SAFE-Domain bereit.
- Für das beN stellt die BNOTK eine SAFE-Domain bereit.
- Für das beSt stellt die BStBK eine SAFE-Domain bereit.
- Die beBPos und eBOs sind im SAFE public (SAFE-Domain der Justiz) verzeichnet.
- Bei den Postfach- und Versanddiensten des Verwaltungsportals wird die Authentizität und die sichere Anmeldung im Verwaltungsportal sichergestellt. Die für die Adressierung erforderlichen Daten der Inhaber der Nutzer- und Unternehmenskonten werden in SAFE public veröffentlicht.

C. Technische Spezifikation des Herkunftsnachweises VHN 2

- Der VHN 2 ist im xml-Format aufgebaut und trägt den Namen vhn.xml.
- Der VHN2 muss mit einer prüfbaren elektronischen fortgeschrittenen Signatur versehen werden. Mit dieser Signatur wird die Richtigkeit der Angaben im fachlichen Abschnitt der vhn.xml bestätigt.
- Diese fortgeschrittene Signatur muss unter Verwendung eines Signaturzertifikats erstellt werden, das von einer dafür zugelassenen CA ausgestellt wurde.
  Die zugelassenen CAs werden in einer trusted list geführt, die im Auftrag der BLK-AG IT-Standards bereitgestellt wird (siehe auch Kapitel H).
- Der VHN 2 muss jeder EGVP-Nachricht beigefügt werden. Er muss somit auch solchen EGVP-Nachrichten beigefügt werden, die nicht den Anforderungen an die sicheren Übermittlungswege entsprechen (z.B. Nachrichten aus Postfächern mit der Rolle egvp_buerger oder egvp_behoerde). Auf diese Weise kann auf Empfängerseite festgestellt werden, wenn eine EGVP-Nachricht missbräuchlich von einem Nutzer oder einer Anwendung in die EGVP-Infrastruktur eingeschleust wurde, da solche Nachrichten keinen VHN 2 enthalten.
- Um feststellen zu können, ob eine Nachricht über einen sicheren Übermittlungsweg versandt wurde, muss die Information, ob ein sicherer Übermittlungsweg vorlag, vom VHN 2-Dienstbetreiber im VHN 2 vermerkt werden (Feld „Sicherer_Uebermittlungsweg“, mögliche Werte Ja/Nein). Der Wert „Ja“ darf nur angegeben werden, wenn die Identifizierung des Postfachinhabers bei Postfachanlage und Authentifizierung des Postfachinhabers bei der Anmeldung die rechtlichen Vorgaben an sichere Übermittlungswege erfüllt.

- Der VHN 2 wird als OSCI-Attachement in einem extra für diesen Zweck neu spezifizierten OSCI-Container, der den Namen vhn_coco trägt, transportiert. Er besteht aus zwei Dateien, der Inhaltsdatei im xml-Format mit dem Dateinamen vhn.xml und der Signaturdatei mit dem Dateinamen vhn.xml.p7s.

- In der vhn.xml – Datei werden immer die Version des VHN sowie der festgelegte Hashalgorithmus, der für alle Hashwerte des VHN gilt, angegeben.

- Die vhn.xml enthält darüber hinaus einen fachlichen und einen technischen Abschnitt, die als solche gekennzeichnet sind. Der fachliche Abschnitt enthält nachfolgende Informationen.

    - den Hashwert für jede einzelne Anlage (= alle Dateien die in dem project_coco referenziert werden)
    - Angaben zur absendenden Identität = SAFE-ID der absendenden Identität, Titel, Name, Vorname, Berufsträgereigenschaft, Organisation, Organisationszusatz, PLZ, Ort, Bundesland, Land, Straße, Hausnummer, (= SAFE-Visitenkarte)
    - eine Information (ja/nein), ob sich die absendende Identität sicher im Sinne der gesetzlichen Vorschriften am SAFE-System angemeldet hat und somit die Nachricht über einen sicheren Übermittlungsweg versandt wurde

  Die Richtigkeit dieser fachlichen Angaben wird durch die VHN 2 – Signatur bestätigt.

- Der technische Abschnitt enthält folgende Informationen:

    - Name des Produktes, mit dem die EGVP-Nachricht versandt wurde
    - Hersteller des Produktes
    - RegistrierungsID

  In diesem Abschnitt müssen immer die Informationen des zugelassenen OSCI-Drittproduktes aufgeführt werden. Sofern die Nachricht mit einer Fachsoftware erstellt und an ein OSCI-Drittprodukt zum Versand übergeben wurde (z.B. RA-Software), muss diese Fachsoftware hier zusätzlich angegeben werden.

- Die Signatur wird über die gesamte xml-Datei gebildet.

- Die VHN.xsd wird veröffentlicht.

D. Schema VHN2

Element	Typ	Anzahl
Fachlich	fachlichType	1
Absender	visitenkarteType	1
visitenkarteType		
Nutzer_ID	xs:string	1
Titel	xs:string	0..1
Vorname	xs:string	0..1
Name	xs:string	1
Strasse	xs:string	1
Hausnummer	xs:string	1
Postleitzahl	xs:string	1
Ort	xs:string	1
Bundesland	xs:string	1
Land	xs:string	1
Organisation	xs:string	0..1
Organisationszusatz	xs:string	0..1
Berufstraegereigenschaft	xs:string	0..1
Externe_ID	xs:string	0..1
EGVP_Rollenwerte	xs:string	1
Sicherer_Uebermittlungsweg	JaNeinType	1
Dokument	DokumentType	1..n
DokumentType		
Hashwert	xs:base64Binary	1
Algorithm	HashAlgorithm	1
Technisch	technischType	1
HerstellerInformation	HerstellerType	1..n
HerstellerType		
Name_des_Produkts_und_Softwareversion	xs:string	1
Hersteller_des_Produkts	xs:string	1
Registrierungs_ID	xs:string	1

E. Wirkung des vertrauenswürdigen Herkunftsnachweises

Durch den VHN 2 können folgende Anforderungen erfüllt werden:

1. Alle Bestandteile der Nachricht erfüllen das Schriftformerfordernis.
2. Die Nachricht kann dem Inhaber eines besonderen Postfaches eindeutig zugeordnet werden.
3. Die Nachricht ist vollständig und unversehrt eingegangen.
4. Die Anforderungen 1 bis 3 können geprüft werden. Ein Prüfvermerk kann erstellt werden.
5. Durch Übernahme des Prüfvermerkes in die Akte kann dargelegt werden, welche Dokumente einer Akte mit welcher Nachricht übermittelt wurden.
6. Durch Übernahme des VHN 2 in die Akte können die Anforderungen 1 bis 3 auch nachträglich geprüft werden.
7. Die Übernahme der OSCI-Nachricht in die elektronische Akte ist nicht erforderlich, da diese keine zusätzlichen Informationen enthält.

F. Gültigkeit

Der VHN wird nicht zu einem Stichtag durch den VHN 2 ersetzt. Vielmehr kann der VHN für eine Übergangszeit weiterverwendet werden. Für Postfächer, die im SAFE-Verzeichnisdienst der Justiz veröffentlicht sind, kann die Signatur des VHN 2 mittels der bereits bezogenen fortgeschrittenen Signaturschlüssel oder alternativ über den von der Justiz bereitgestellten Signaturdienst erfolgen.
Die Hashwerte müssen base64-codiert werden.

G. Prüfung des VHN 2

Bei einer VHN2-Nachricht müssen folgende Merkmale zum Übertragungsweg verifiziert werden:

1. Gültigkeit und Onlineprüfung der Signatur der vhn.xml
    - Grün = erfolgreiche Signaturprüfung
    - Gelb = Das Prüfergebnis ist unbestimmt (z.B. Nichterreichbarkeit des Verifikationsservers)
    - Rot = Die Signatur ist ungültig
2. Abstammung des Signaturzertifikats von einer der zugelassenen VHN2- CAs

    Liste der zugelassenen CAs siehe Kapitel H
3. Angabe, ob es sich um einen sicheren Übermittlungsweg handelt (vhn.xml -> Feld: sicherer_Übermittlungsweg).

    - Ja: Identifizierungs- und Authenfizierungsniveau entsprechen den gesetzlichen Vorgaben für sichere Übermittlungswege
    - Nein: mindestens eine der gesetzlichen Vorgaben für sichere Übermittlungswege lag zum Zeitpunkt der Anmeldung des Postfachinhaber nicht vor.

Folgende Prüfergebnisse können vorkommen:

I. Prüfergebnisse gesamter EGVP-Verbund:

	Ergebnis der Signaturprüfung vhn.xml.p7s			**Sicherer_ Übermittlungsweg (vhn.xml)**		**Prüfergebnis (Meldungstext)**
VHN-Signatur-CA	grün	gelb	rot	ja	nein	
beA, beN, beBPo, beSt, eBO, OZG	**X**				**X**	Diese Nachricht wurde per EGVP versandt.
		x			**x**	Diese Nachricht wurde per EGVP versandt. Die Prüfung des Herkunftsnachweises war zum Prüfungszeitpunkt nicht möglich.
			x		**x**	Diese Nachricht wurde per EGVP versandt. Die Prüfung des Herkunftsnachweises führte zu dem Ergebnis „ungültig“.
beA	**X**			**X**		Sicherer Übermittlungsweg aus einem besonderen Anwaltspostfach.
		X		**X**		Prüfung des sicheren Übermittlungswegs zum Prüfungszeitpunkt nicht möglich.
			X	**X**		Keine Übermittlung über einen sicheren Übermittlungsweg, weil die Prüfung des Herkunftsnachweises des besonderen Anwaltspostfachs zu dem Ergebnis „ungültig“ führte.
beBPo	**X**			**X**		Sicherer Übermittlungsweg aus einem besonderen Behördenpostfach.
		X		**X**		Prüfung des sicheren Übermittlungswegs zum Prüfungszeitpunkt nicht möglich.
			X	**X**		Keine Übermittlung über einen sicheren Übermittlungsweg, weil die Prüfung des Herkunftsnachweises des besonderen Behördenpostfachs zu dem Ergebnis „ungültig“ führte.

beN	X			X		Sicherer Übermittlungsweg aus einem besonderen Notarpostfach.
		X		X		Prüfung des sicheren Übermittlungswegs zum Prüfungszeitpunkt nicht möglich.
			X	X		Keine Übermittlung über einen sicheren Übermittlungsweg, weil die Prüfung des Herkunftsnachweises des besonderen Notarpostfachs zu dem Ergebnis „ungültig“ führte.
beSt	X			X		Sicherer Übermittlungsweg aus einem besonderen Steuerberaterpostfach.
		X		X		Prüfung des sicheren Übermittlungswegs zum Prüfungszeitpunkt nicht möglich.
			X	X		Keine Übermittlung über einen sicheren Übermittlungsweg, weil die Prüfung des Herkunftsnachweises des besonderen Steuerberaterpostfachs zu dem Ergebnis „ungültig“ führte.
eBO	X			X		Sicherer Übermittlungsweg aus einem besonderen Bürger- und Organisationenpostfach.
		X		X		Prüfung des sicheren Übermittlungswegs zum Prüfungszeitpunkt nicht möglich.
			X	X		Keine Übermittlung über einen sicheren Übermittlungsweg, weil die Prüfung des Herkunftsnachweises des besonderen Bürger- und Organisationenpostfachs zu dem Ergebnis „ungültig“ führte.
Justiz	X				X	Diese Nachricht wurde von der Justiz versandt.
		X			X	Der Versand der Nachricht durch die Justiz kann nicht bestätigt werden, da die Prüfung des Herkunftsnachweises zum Prüfungszeitpunkt nicht möglich war.
			X		X	Der Versand der Nachricht durch die Justiz kann nicht bestätigt werden, da die Prüfung des Herkunftsnachweises zu dem Ergebnis „ungültig“ führte.
EGVP (z.B. für EGVP-Rollen egvp_behoerde, egvp_buerger, egvp_gv)	X				X	Diese Nachricht wurde per EGVP versandt.
		X			X	Der Versand der Nachricht durch einen identifizierten EGVP-Teilnehmer kann nicht bestätigt werden, da die Prüfung des Herkunftsnachweises zum Prüfungszeitpunkt nicht möglich war.
			X		X	Der Versand der Nachricht durch einen identifizierten EGVP-Teilnehmer kann nicht bestätigt werden, da die Prüfung des Herkunftsnachweises zu dem Ergebnis „ungültig“ führte.

OZG	X			X		Sicherer Übermittlungsweg aus dem Postfach- und Versanddienst eines OZG-Nutzerkontos.
		X		X		Prüfung des sicheren Übermittlungswegs zum Prüfungszeitpunkt nicht möglich.
			X	X		Keine Übermittlung über einen sicheren Übermittlungsweg, weil die Prüfung des Herkunftsnachweises aus dem Postfach- und Versanddienst eines OZG-Nutzerkontos zu dem Ergebnis „ungültig“ führte.
Justiz, EGVP	X	X	X	X		Diese Nachricht wurde per EGVP versandt. Achtung! Angaben zum sicheren Übermittlungsweg im VHN nicht korrekt.
Test	X			X		Dies ist eine Testnachricht. Ein Test-VHN war beigefügt.
		X		X		Dies ist eine Testnachricht. Die Prüfung des Herkunftsnachweises (Test-VHN) war zum Prüfungszeitpunkt nicht möglich.
			X	X		Dies ist eine Testnachricht. Die Prüfung des Herkunftsnachweises (Test-VHN) führte zu dem Ergebnis „ungültig“.
	X	X	X		X	Dies ist eine Testnachricht. Es lag keine sichere Anmeldung vor.
keine Signatur oder unbekannte CA oder ungültiges VHN-Schema	X	X	X	X	X	ACHTUNG! Der Absender der Nachricht ist kein identifizierter EGVP-Teilnehmer.

II. Prüfergebnisse nur justizintern:

Die Justiz hat einen Dienstleister mit der Umwandlung von De-Mails in EGVP-Nachrichten beauftragt. Die auf diese Weise erzeugten EGVP-Nachrichten werden mit einem VHN, der mit einer hierfür gesondert bereitgestellten CA signiert ist, versehen.

De-Mail (mit Absenderbest.)	X				X	Sicherer Übermittlungsweg per absenderbestätigter De-Mail.
		X			X	Der Versand über einen sicheren Übermittlungsweg per absenderbestätigter De-Mail kann nicht bestätigt werden, da die Prüfung des Herkunftsnachweises zum Prüfungszeitpunkt nicht möglich war.
			X		X	Der Versand über einen sicheren Übermittlungsweg per absenderbestätigter De-Mail kann nicht bestätigt werden, da die Prüfung des Herkunftsnachweises zu dem Ergebnis „ungültig“ führte.
De-Mail (ohne Absenderbest.)	X				X	Diese Nachricht wurde per De-Mail ohne Absenderbestätigung versandt.
		X			X	Der Versand per De-Mail ohne Absenderbestätigung kann nicht bestätigt werden, da die Prüfung des Herkunftsnachweises zum Prüfungszeitpunkt nicht möglich war.
			X		X	Der Versand per De-Mail ohne Absenderbestätigung kann nicht bestätigt werden, da die Prüfung des Herkunftsnachweises zu dem Ergebnis „ungültig“ führte.

Zusätzlich müssen die Hashwerte der Anlagen mit den Hashwerten der vhn.xml verglichen werden.

Bei Abweichungen sollen folgende Hinweise in den Prüfvermerk aufgenommen werden:

- mehr bzw. andere beigefügte Dokumente als Hashwerte im VHN:
  „Die Dokumente mit folgenden Dateinamen sind nicht im Herkunftsnachweis enthalten:“

- mehr bzw. andere Hashwerte im VHN2 als beigefügte Dokumente:
  „Die im Herkunftsnachweis mit folgenden Hashwerten aufgeführten Dokumente sind der Nachricht nicht beigefügt.“

Beispiel Visualisierung Prüfvermerk:

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	√ Gültigkeit √ Integrität
Klage.pdf	pdf	nein				
xjustiz_nachricht.xml	xml	nein				

Die Dokumente mit folgenden Dateinamen sind nicht im Herkunftsnachweis enthalten.:

Anlage.pdf

Klage.pdf

H. VHN-CAs

Die für den VHN zugelassenen CAs werden auf der Seite der Bundesnotarkammer zum Download angeboten.
Nachfolgend sind die verschiedenen CAs aufgeführt:

https://onlinehilfe.bnotk.de/display/syshilfe/Root-Zertifikate+der+Bundesnotarkammer

I. allgemeine Beschreibung der Attribute:

CN	common name	Name
O	organisation	Organisation
ST	state	Bundesland
C	country	Land

II. Root CA (RSA 4096 bit, SHA-512 RSAPSS)

CN	SAFE Root CA 2017
O	BNotK
C	DE

III. Sub-CAs (RSA 4096 bit, SHA-512 RSAPSS)

1. beBPo-VHN

CN	beBPo VHN CA 2017
O	BNotK
C	DE

2. beA-VHN

CN	beA VHN CA 2017
O	BNotK
C	DE

3. beN-VHN

CN	beN VHN CA 2017
O	BNotK
C	DE

4. Justiz-VHN

CN	Justiz VHN CA 2017
O	BNotK
C	DE

5. eBO-VHN

CN	eBO VHN CA 2021
O	BNotK
C	DE

6. Postfach- und Versanddienst OZG Nutzerkonto - VHN

CN	VHN - Postfach- und Versanddienst eines OZG-Nutzerkontos CA 2021
O	BNotK
C	DE

7. EGVP - VHN

CN	EGVP VHN CA 2021
O	BNotK
C	DE

8. beSt-VHN

CN	beSt VHN CA 2021
O	BNotK
C	DE

9. De-Mail-VHN (nur justizintern)

CN	De-Mail VHN CA 2017
O	BNotK
C	DE

10. Test-VHN

CN	Test VHN CA 2021
O	BNotK
C	DE

IV. Teilnehmerzertifikate (RSA 2048 bit, SHA-512 RSAPSS)

1. beBPo

CN	VHN – besonderes elektronisches Behördenpost-fach
ST	Bundesland
C	DE
serialNumber	Xxxxxxx
UID	DE.Justiz.d03218d-…

2. beA

CN	VHN – besonderes elektronisches Anwaltspostfach
C	DE
serialNumber	Xxxxxxx

3. beN

CN	VHN – besonderes elektronisches Notarpostfach
C	DE
serialNumber	Xxxxxxx

4. Justiz

CN	VHN - Justiz
ST	Bundesland
C	DE
serialNumber	xxxxxxx
UID	DE.Justiz.d03218d-…

5. eBO

CN	VHN – besonderes elektronisches Bürger- und Orga-nisationenpostfach
ST	Bundesland
C	DE
serialNumber	Xxxxxxx

6. OZG

CN	VHN – Postfach- und Versanddienst OZG Nut- zer-konto
ST	Bundesland
C	DE
serialNumber	Xxxxxxx

7. EGVP

CN	VHN – EGVP-Postfach
ST	Bundesland
C	DE
serialNumber	Xxxxxxx

8. beSt

CN	VHN – besonderes elektronisches Steuerberater-postfach
C	DE
serialNumber	Xxxxxxx

9. De-Mail

CN	VHN–De-Mail-Dienst
C	DE
serialNumber	Xxxxxxx

10. Test

CN	VHN–Test
C	DE
serialNumber	Xxxxxxx

V. Bezug der Teilnehmerzertifikate

1. beBPo-VHN

Nutzeraktion: Zertifikatsdownload von ZS-Website
Voraussetzung: freigeschaltete beBPo-Rolle

2. beA-VHN

Bereitstellung an BLK-AG IT-Standards, Übergabe an BRAK

3. beN-VHN

Bereitstellung an BLK-AG IT-Standards, Übergabe an BNotK

4. Justiz-VHN

Nutzeraktion: Zertifikatsdownload von ZS-Website
Voraussetzung: freigeschaltete EGVP-Justiz-Rolle

5. eBO-VHN

Bereitstellung an BLK-AG IT-Standards, Übergabe an VHN-2-Dienstleister (BNotK)

6. EGVP-VHN

Bereitstellung an BLK-AG IT-Standards, Übergabe an VHN-2-Dienstleister (BNotK)

7. **Postfach- und Versanddienst OZG Nutzerkonto VHN**

   VHN Bereitstellung an BLK-AG IT-Standards, Übergabe an Nutzerkontenbetreiber (NN)

8. **beSt-VHN**

   Bereitstellung an BLK-AG IT-Standards, Übergabe an BStBK

9. **De-Mail-VHN (nur justizintern)**

   Bereitstellung an BLK-AG IT-Standards, Übergabe an De-Mail-Dienstleiter (Procilon)

10. **Test-VHN**

    Bereitstellung an BLK-AG IT-Standards, Übergabe nach Anfrage beim Projektbüro der BLK-AG IT-Standards (it-standards@justiz.de)