



Anbindung an KV-Connect V4.1

Herausgeber: kv.digital GmbH

Copyright © kv.digital GmbH, 2021

Alle Rechte vorbehalten. Nachdruck und Vervielfältigung einschließlich Speicherung und Nutzung auf optischen und elektronischen Datenträgern nur mit Zustimmung der kv.digital GmbH.

Inhaltsverzeichnis

1 Änderungshistorie	3
2 Vorbemerkung	6
2.1 Zweck des Dokumentes	6
2.1.1 Mitgeltende Dokumente.....	6
2.2 Geltungsbereich	7
3 Anforderungen für die Anbindung an KV-Connect.....	8
3.1 KV-Connect Integration in das Softwaresystem.....	8
3.1.1 Anbindung des KV-Connect Clients über POP3 und SMTP.....	9
Ablauf.....	9
Ablaufdiagramme.....	10
3.1.2 Anbindung an KV-Connect über die REST-Serverschnittstelle	9
Ablauf.....	10
Ablaufdiagramme.....	10
3.1.3 KV-Connect Updates der kv.digital GmbH.....	10
3.1.4 KV-Connect Benutzerzertifikat.....	11
3.2 KV-Connect MIME-Header-Felder	11
3.2.1 MIME-Header-Feld "X-KVC-Sendersystem"	11
3.2.2 MIME-Header-Feld "X-KVC-Dienstkennung"	12
3.2.3 MIME-Header-Feld "Subject"	13
3.2.4 MIME-Header-Feld "Message-ID"	13
3.2.5 MIME-Header-Feld "BCC"	13

1 Änderungshistorie

Vers.	Datum	Autor	Kap.	Änderung	Status
4.1.1	26.03.2021	kv.digital GmbH	2	Korrektur Referenz für [FD_REST]	in Kraft
			3	Anpassung von Referenzen aufgrund des neuen Update-Servers der KBV	
4.1	07.02.2020	kv.digital GmbH	alle	Umfirmierung KV Telematik GmbH in kv.digital GmbH	außer Kraft
4.1	27.06.2019	KV Telematik GmbH	2 3	Aufnahme RFC 8551 für die Verwendung von RFC-konformen Zeilenumbrüchen Anpassung Fallback-Wert Präzisierung <ul style="list-style-type: none"> • Kapitel Anbindung des KV-Connect Clients über POP3 und SMTP • Anbindung an KV-Connect über REST-Serverschnittstelle • KV-Connect Benutzerzertifikat Aufnahme neuer Anforderungen <ul style="list-style-type: none"> • Prüfung des KV-Connect Server-Zertifikats • Prüfung der Nachrichtensignatur • Verwendung von RFC-konformen Zeilenumbrüchen • Verwendung des MIME-Header-Felds "BCC" 	außer Kraft
4.0.2	07.05.2018	KV Telematik GmbH	3.1.3	Anpassung Gültigkeitsdauer Benutzerzertifikat	außer Kraft
4.0.1	12.05.2017	KV Telematik GmbH	2.1.1 3.1.2	redaktionelle Änderungen <ul style="list-style-type: none"> • Austausch Dokument und Referenz [FD_REST] • Aktualisierung Referenz [REST_SN] und [REST_Krypto] • Konkretisierung [KVCC] • Aktualisierung Referenz "Aktuelle Hinweise" 	außer Kraft
4.0	15.07.2016	KV Telematik GmbH	alle	Komplettüberarbeitung der Dokumentation	außer Kraft
3.1.7		KV Telematik GmbH	4	Präzisierung zum MIME-Header-Feld X-KVC-Sendersystem	erledigt
3.1.6	26.01.2016	KV Telematik GmbH	4	Abkündigung von KV-Connect Clientversionen	erledigt

Vers.	Datum	Autor	Kap.	Änderung	Status
3.1.5	19.10.2015	KV Telematik GmbH	4, 5, 6, 7	Ergänzende Erläuterung zum MIME-Header-Feld X-KVC-Dienstkennung Ergänzende Erläuterung zur Abkündigung von KV-Connect Client Versionen Ergänzende Erläuterung zum LDAP	erledigt
3.1.4	04.08.2015	KV Telematik GmbH	5, 6, 7	Umstellung des LDAP-Servers auf LDAPS	erledigt
3.1.3	08.05.2015	KV Telematik GmbH	4	Ergänzende Erläuterung und Anpassung des Beispiels zum MIME-Header-Feld X-KVC-Dienstkennung	erledigt
3.1.2	01.02.2015	KV Telematik GmbH	4	Änderung Schreibweise X-KVC-Sendersystem, KV-Connect	erledigt
3.1.1	01.08.2014	KV Telematik GmbH	1, 3, 3.1.1, 3.1.2, 4, 5, 6	Ersetzen der Referenzen vom Projektportal auf das Partnerportal. Ergänzende Erläuterung zum MIME-Header-Feld X-KVC-Sendersystem. Ergänzende Erläuterung und Anpassung des Beispiels zum MIME-Header-Feld X-KVC-Dienstkennung Einfügen der URLs für das Referenzsystem 2 Anpassung Dokumentationslink Produktivsystem	erledigt
3.1.0	30.04.2014	KV Telematik GmbH	1.1, 3, 3.1, 3.2.3, 6	Anpassung Corporate Identity. Kapitel 3.1 „KV-CONNECT MIME-Header-Felder“ eingefügt. Entfernung temporärer Informationen in den Kapiteln 1.1, 3 und 3.2.3. Verdeutlichung der URLs in den Kapiteln 4 und 6 Aktualisierung der LDAP-URL in Kapitel 6	erledigt
3.0.1	03.02.2014	KV Telematik GmbH	Alle	Austausch der Logos sowie Anpassung auf die neue GmbH. Anpassung der Referenzen, da sich Versionsnummern referenzierter Dokumente geändert haben.	erledigt
3.0	24.07.2013	KV-Telematik ARGE	1.1, 3, 3.1.4	D2D-Connector und Client-Versionen abgekündigt	erledigt
2.0	13.05.2013	KV-Telematik ARGE	1.1, 3, 4, 5, 6	Überarbeitung und Anpassung auf Universaldistribution	erledigt

Vers.	Datum	Autor	Kap.	Änderung	Status
1.1.1	13.02.2013	KV-Telematik ARGE	1.1	Überarbeitung	erledigt
1.1	08.08.2012	KV-Telematik ARGE	alle	Überarbeitung	erledigt
1.0	02.08.2012	KV-Telematik ARGE	alle	Initial	erledigt

Herausgeber:
KV Telematik GmbH

Diese Spezifikation wird unter CC-BY-SA 3.0 veröffentlicht. ([Vollständiger Lizenztext](#), [Allgemein verständliche Erklärung](#))

2 Vorbemerkung

2.1 Zweck des Dokumentes

Das Dokument "Anforderungen an die Anbindung an KV-Connect" beschreibt die verschiedenen Möglichkeiten, ein Softwaresystem (PVS, KIS etc.) an KV-Connect anzubinden. In diesem Dokument werden neben den Anforderungen auch die zu beachtenden Schnittstellen und die eingesetzten Standards benannt und Besonderheiten beschrieben. Technische Detailinformationen finden sich in den mitgeltenden Dokumenten, die an den entsprechenden Stellen referenziert werden.

2.1.1 Mitgeltende Dokumente

Das Dokument wird durch verschiedene RFCs, der Dokumentation des KV-Connect Clients sowie der Dokumentation der REST-Serverschnittstelle und der entsprechenden Kryptographie sowie Ablaufdiagramme ergänzt. Die entsprechenden Dokumente werden mit ihren Bezugsquellen in den jeweiligen Abschnitten benannt.

Darüber hinaus werden die Spezifikationen der Schnittstellen für die Kommunikation als auch die Hinweise zur Anbindung an KV-Connect im kostenfrei nutzbaren Partnerportal veröffentlicht und ständig aktuell gehalten. Die URL des Partnerportals lautet: <https://partnerportal.kv-telematik.de>

Kürzel	Kurzbeschreibung	Dateiname
RFC1939	RFC 1939	http://tools.ietf.org/html/rfc1939
RFC4954	RFC 4954	http://tools.ietf.org/html/rfc4954
RFC5321	RFC 5321	http://tools.ietf.org/html/rfc5321
RFC5322	RFC 5322	http://tools.ietf.org/html/rfc5322
RFC2045	RFC 2045	http://tools.ietf.org/html/rfc2045
RFC8551	RFC 8551	https://tools.ietf.org/html/rfc8551
FDAREST	Flussdiagramm Empfang über REST	Anbindung_REST_Empfang_KV_Connect_1_0_2.pdf
FDVREST	Flussdiagramm Versand über REST	Anbindung_REST_Versand_KV_Connect_1_0_1.pdf
REST_SN	Schnittstellenbeschreibung der REST-Serverschnittstelle	https://partnerportal.kv-telematik.de/pages/viewpage.action?pagId=11927560 Übersicht über alle Spezifikationen: Tabelle KV-Connect, Spezifikation KV-Connect Server
REST_Krypto	Kryptographie für REST	https://partnerportal.kv-telematik.de/pages/viewpage.action?pagId=11927560 Übersicht über alle Spezifikationen: Tabelle KV-Connect, Spezifikation KV-Connect Server

Kürzel	Kurzbeschreibung	Dateiname
KVCC	Beschreibung des KV-Connect Clients in der aktuellsten Version	https://partnerportal.kv-telematik.de/pages/viewpage.action?pageld=11927560 Übersicht über alle Spezifikationen: Tabelle KV-Connect, KV-Connect Client
ANWID	Übersicht der Anwendungsübergreifenden Identifikatoren	https://partnerportal.kv-telematik.de/pages/viewpage.action?pageld=22250205
SPKEY	Spezifikation Keystorelokation	https://partnerportal.kv-telematik.de/display/ZERTLOC10/Spezifikation+Keystorelokation+1.0

2.2 Geltungsbereich

Das vorliegende Dokument gilt für alle Softwaresysteme, die die Anbindung von KV-Connect realisieren. Um die Anforderungen an die Softwaresysteme zu beschreiben, werden Anforderungskriterien verwendet. Die Anforderungskriterien müssen im Softwaresystem implementiert sein.

Beispiel:

[KVC-AnbXXX] Der MIME-Header jeder KV-Connect Nachricht MUSS das Feld "XY" gemäß [1234] enthalten.

Dieses Beispiel hat an dieser Stelle lediglich den Präsentationszweck und hat keinen Bezug zur Fachlichkeit des Dokuments.

3 Anforderungen für die Anbindung an KV-Connect

In den nachfolgenden Abschnitten werden die Anforderungskriterien für die Anbindung von KV-Connect in unterschiedlicher Detaillierungstiefe beschrieben, die für alle Softwaresysteme gelten.

Sofern Anforderungskriterien in anderen Spezifikationen definiert sind, wird auf diese Spezifikationen verwiesen.

3.1 KV-Connect Integration in das Softwaresystem

Zur Integration in das Softwaresystem (PVS, KIS etc.) ist KV-Connect flexibel konzipiert und bietet je nach Anforderung grundsätzlich zwei unterschiedliche Schnittstellen an:

1. Integration KV-Connect Client über Standard E-Mail-Schnittstellen (smtp/pop3) → Anbindung des KV-Connect Clients über POP3 und SMTP gemäß [KVCC] in der aktuellsten Version
2. Integration KV-Connect Serverschnittstelle (REST) und native Anbindung → Anbindung an KV-Connect über die REST-Serverschnittstelle gemäß [REST_SN]

[KVC-Anb010] Die Integration von KV-Connect in das Softwaresystem MUSS über die Anbindung des KV-Connect Clients gemäß [KVCC] oder die Anbindung über die REST-Serverschnittstelle gemäß [REST_SN] erfolgen.

Im KV-Connect Postfach eines Anwenders können Nachrichten der verschiedensten Anwendungen ankommen. Das System muss in der Lage sein, den Anwender über vorliegende Nachrichten in Kenntnis zu setzen, auch wenn die betreffende Anwendung nicht oder nicht in vollem Umfang unterstützt wird.

[KVC-Anb020] Das System MUSS in der Lage sein, für alle im KV-Connect Postfach des Anwenders liegenden Nachrichten die Headerinformationen „From“, „Date“, „X-KVC-Dienstkennung“ und „Subject“ dem Anwender anzuzeigen und die Nachricht auf Anforderung des Anwenders vom Server abzurufen und lokal bereitzustellen.

Prüfung des KV-Connect Server-Zertifikats auf Gültigkeit und Vertrauenswürdigkeit

[KVC-Anb021] Das System MUSS das Zertifikat des KV-Connect Servers auf Gültigkeit prüfen. Dazu MUSS das Root-Zertifikat des KV-Connect Servers im System als vertrauenswürdig hinterlegt sein. Verbindungen mit anderen Zertifikaten MÜSSEN systemseitig abgelehnt werden.

Prüfung der Nachrichtensignatur auf Gültigkeit und Echtheit

[KVC-Anb022] Das System MUSS die Signatur jeder empfangenen KV-Connect Nachricht auf Gültigkeit prüfen. Fällt die Signaturprüfung negativ aus, MUSS die Nachricht systemseitig verworfen und dem Anwender dies mitgeteilt werden.

RFC-konforme Zeilenumbrüche in MIME- und S/MIME-Nachrichten: Jede MIME-Entität muss in eine universelle, kanonische Form konvertiert werden. Das heißt, dass sowohl für den Einbau in die S/MIME-Struktur als auch für die Signaturerzeugung alle Zeilenumbrüche auf <CR><LF> zu setzen sind (RFC 2045, RFC 8551).

[KVC-Anb023] In den zu versendenden MIME- und S/MIME-Nachrichten ist als Zeilenumbruch ausschließlich die Kombination <CR><LF> erlaubt.

3.1.1 Anbindung des KV-Connect Clients über POP3 und SMTP

Der KV-Connect Client ermöglicht das Versenden und Empfangen von MIME-Nachrichten über die Mail-Schnittstellen SMTP (RFC 5321) und POP3 (RFC 1939). Hierzu fungiert der KV-Connect Client als E-Mail-Server auf dem lokalen System. Er übernimmt hierbei auch die Ver- und Entschlüsselung sowie die Signatur. Der KV-Connect Client kommuniziert über MIME-Nachrichten nach RFC 2048 mit dem Primärsystem. Im Rahmen des Versands werden die vom Primärsystem erzeugten MIME-Nachrichten über SMTP angenommen und mittels des Benutzerzertifikats des Absenders signiert. Anschließend verschlüsselt der KV-Connect Client die KV-Connect Nachricht inkl. der vorhandenen Anlagen mittels des Benutzerzertifikats des Empägers (oder mehrerer Empänger) und versendet die so entstandene S/MIME-Nachricht. Der Empfang der Nachrichten verläuft entsprechend. Für die Erstellung der Signatur und die Entschlüsselung ist ein Benutzerzertifikat notwendig, das bei der ersten Verwendung des KV-Connect Clients über eine lokale Konfigurationswebseite angelegt werden muss. Das Benutzerzertifikat wird in einem privaten Keystore abgelegt und ist über eine PIN geschützt, die beim Abrufen und Senden von KV-Connect Nachrichten mit dem Kennwort übermittelt werden muss. Für die Prüfung der Signatur und Verschlüsselung werden die Zertifikate der jeweiligen Kommunikationspartner verwendet. Diese werden über die PKI von KV-Connect bereitgestellt.

Die Verbindung zwischen dem System und dem KV-Connect Client ist mittels TLS/SSL abgesichert. Hierbei kommt SMTP Auth nach RFC 4954 mit Plain oder Login Authentisierung für SMTP nach RFC 4616 zum Einsatz. Aus diesem Grund wird SMTP über Port 465 und POP3 über Port 995 angesprochen. Diese Ports sind konfigurierbar.

Ablauf

Versand über SMTP:

Das System generiert eine MIME-Nachricht, die auch Anlagen enthalten kann. Diese MIME-Nachricht wird mittels SMTP an den KV-Connect Client übergeben. Der KV-Connect Client behandelt die MIME-Nachricht kryptographisch. Hierzu ist es erforderlich, den Keystore des Benutzers über eine PIN zu entsperren. Die PIN wird mit dem SMTP-Kennwort übermittelt. Sofern die Kryptographie fehlerfrei durchgeführt werden konnte, wird die S/MIME Nachricht versendet. Ein Auftreten von Fehlern bei der Kryptographie führt zum Abbruch des Versandvorgangs. Fehlermeldungen werden über SMTP-Statuscodes abgebildet.

Empfang über POP3:

Das Primärsystem fragt mittels POP3-Kommandos am KV-Connect Client an, ob neue S/MIME-Nachrichten zum Abruf bereit stehen. Sofern neue Nachrichten vorhanden sind, werden diese mithilfe der entsprechenden POP3-Befehle abgeholt. Die dazu notwendige PIN des privaten Keystores wird mit dem POP3-Kennwort übermittelt. Wurde die PIN korrekt angegeben, wird die S/MIME-Nachricht kryptographisch behandelt. Im Anschluss prüft der KV-Connect Client die Signatur der S/MIME-Nachricht und erzeugt im Fall einer fehlerhaften Signatur eine entsprechende Fehlermeldung, die als „synthetische“ Mail (Originalnachricht wird angehängt) dem Empfänger zur Verfügung gestellt wird. Nach erfolgreicher Entschlüsselung wird die MIME-Nachricht dem Primärsystem zur Verfügung gestellt. Hat das Primärsystem die MIME-Nachricht erfolgreich empfangen, so übermittelt es die POP3-Befehle zum Löschen der Nachricht auf dem Server an den KV-Connect Client.

3.1.2 Anbindung an KV-Connect über die REST-Serverschnittstelle

Mittels der REST-Serverschnittstelle besteht die Möglichkeit, das System direkt an den KV-Connect Server anzubinden. In diesem Fall entfällt eine lokale Installation des KV-Connect Clients. Die Funktionen des KV-Connect Client müssen durch das System realisiert werden. Neben der Kommunikation über die REST-Serverschnittstelle muss das System die kryptographische Behandlung der ein- und ausgehenden KV-Connect Nachrichten übernehmen. Die Kommunikation mit der REST-Serverschnittstelle erfolgt über eine SSL-geschützte Verbindung. Zur Authentifizierung beim Zugriff auf die Ressourcen wird BASIC Authentication

verwendet. Details hierzu sind, ebenso wie die Kryptographie sowie die Schnittstelle, unter [REST_SN] beschrieben.

Ablauf

Versand:

Das System generiert eine MIME-Nachricht, die auch Anlagen enthalten kann. Im Anschluss müssen die Zertifikate des Empfängers bzw. der Empfänger abgerufen werden. Sollte ein Zertifikat nicht vorhanden sein, so ist eine Fehlermeldung auszugeben und der Versandvorgang ist abzubrechen. Sofern alle Zertifikate vorhanden sind, ist die MIME-Nachricht entsprechend der beschriebenen Verfahren (siehe [REST_SN]) zu signieren und zu verschlüsseln. Anschließend wird die S/MIME-Nachricht versendet. Sollte der Versand nicht erfolgreich sein, so ist eine Fehlermeldung auszugeben und der Versand abzubrechen.

Empfang:

Das System fragt mittels entsprechender REST-Befehle am KV-Connect Server an, ob neue S/MIME-Nachrichten für den Nutzer vorliegen. Wenn dies der Fall ist, wird die neue S/MIME-Nachricht über ihre Message-ID abgerufen. Im Anschluss wird die Nachricht entschlüsselt und die Signatur der Nachricht geprüft. Sollte die Signatur nicht in Ordnung sein, so ist eine Warnmeldung auszugeben. Die S/MIME-Nachricht wird anschließend lokal als MIME-Nachricht gespeichert und über die jeweiligen REST-Befehle vom KV-Connect Server gelöscht. Für den Fall, dass der Löschvorgang nicht erfolgreich abgeschlossen werden kann, ist eine Fehlermeldung auszugeben. Sollte die Entschlüsselung nicht erfolgreich sein, so muss eine Fehlermeldung ausgegeben werden und der Empfangsvorgang ist abzubrechen. In diesem Fehlerfall bleibt die S/MIME-Nachricht auf dem KV-Connect Server gespeichert.

Ablaufdiagramme

Die Ablaufdiagramme, die den Empfang und den Versand mithilfe der REST-Serverschnittstelle aufzeigen, liegen als eigenständige PDF-Dokumente vor ([FDAREST] [FDVREST]).

3.1.3 KV-Connect Updates der kv.digital GmbH

Die kv.digital GmbH betreibt und entwickelt KV-Connect. Hierzu stellt die kv.digital Dokumentationen zum KV-Connect Client, der REST-Serverschnittstelle und der entsprechenden Kryptographie sowie die Spezifikationen von Anwendungen kostenfrei zur Implementierung im Softwaresystem im Partnerportal der kv.digital GmbH bereit. Des Weiteren stellt die kv.digital auch den KV-Connect Client bereit und aktualisiert diesen regelmäßig.

KV-Connect unterliegt ständig wechselnden Anforderungen und kann daher nicht statisch sein. Aus diesem Grund aktualisiert die kv.digital GmbH regelmäßig die Dokumentation zum KV-Connect Client und den KV-Connect Client selbst, die Dokumentationen der REST-Serverschnittstelle und der entsprechenden Kryptographie sowie die Spezifikationen von Anwendungen.

[KVC-Anb030] Durch geeignete organisatorische Maßnahmen MUSS sichergestellt sein, dass Aktualisierungen von KV-Connect, die über das Update der KBV oder den Technischen Newsletter der kv.digital GmbH zur Verfügung gestellt werden, bis zum entsprechenden Gültigkeitsbeginn im System implementiert werden.

[KVC-Anb040] Wird der von der kv.digital GmbH zur Verfügung gestellte KV-Connect Client genutzt, MUSS das System sicherstellen, dass dieser dem Anwender zur Verfügung steht und nur in einer von der kv.digital GmbH unterstützten Version zum Einsatz kommt.

⚠️ unterstütze Versionen des KV-Connect Clients

Nach Möglichkeit werden zusätzlich zur aktuellen Version die beiden letzten Versionen des KV-Connect Clients unterstützt. Bei funktionalen Erweiterungen ist die Abwärtskompatibilität nicht immer gewährleistet. In diesem Fall wird durch die kv.digital GmbH darüber informiert, dass die neueste Version des Clients zu verwenden ist.

Unter "[Übersicht über alle Spezifikationen](#)": Tabelle KV-Connect werden alle Spezifikationen der unterstützten Versionen des KV-Connect Clients veröffentlicht. Des Weiteren wird mit dem Update der KBV regelmäßig über abgekündigte KV-Connect Client-Versionen informiert (Dokument "Aktuelle Hinweise" unter [https://update.kbv.de/ita-update/KV-Connect/](ftp://ftp.kbv.de/ita-update/KV_Connect/)).

3.1.4 KV-Connect Benutzerzertifikat

Zum verschlüsselten und signierten Versand und Empfang der KV-Connect Nachrichten wird ein so genanntes Benutzerzertifikat oder auch Userzertifikat für den jeweiligen KV-Connect Account benötigt. Ein Benutzerzertifikat ist nur für die im Zertifikat angegebene Dauer gültig. Jedes Zertifikat enthält die Datumsangaben Gültig ab und Gültig bis, die die Grenzen der Gültigkeitsdauer festlegen. In der Spezifikation Keystorelokation [SPKEY] werden Ablage und Update von Benutzerzertifikaten in Keystores beschrieben.

[KVC-Anb050] Die Ablage des Benutzerzertifikats MUSS gemäß [SPKEY] erfolgen und dokumentiert sein. Die Dokumentation MUSS um die Information ergänzt werden, an welcher Stelle im Dateisystem das Benutzerzertifikat gespeichert wird.

[KVC-Anb060] Systemseitig MUSS sichergestellt sein, dass der Anwender auf Dateisystemebene jederzeit Zugang zum Benutzerzertifikat für den Export/Import hat.

[KVC-Anb070] Die Aktualität des Benutzerzertifikats MUSS systemseitig sichergestellt sein. Das System MUSS durch einen entsprechenden Warnhinweis auf dem Bildschirm den Anwender 150 Tage vor Ablauf des Benutzerzertifikats auf den Umstand hinweisen. Zusätzlich MUSS die Meldung enthalten, wie der Anwender sein Benutzerzertifikat erneuern kann. Die Meldung MUSS wöchentlich erfolgen, bis das Zertifikat erneuert wurde. Für den Abgleich ist das Systemdatum des eingesetzten Systems heranzuziehen.

[KVC-Anb080] Systemseitig MUSS sichergestellt sein, dass vorgefundene Benutzerzertifikate des Empfängers, deren Gültigkeit abgelaufen sind, nicht mehr zum Verschlüsseln von KV-Connect Nachrichten verwendet werden (nur REST-Schnittstelle).

3.2 KV-Connect MIME-Header-Felder

3.2.1 MIME-Header-Feld "X-KVC-Sendersystem"

[KVC-Anb090] Der MIME-Header jeder KV-Connect Nachricht muss das Feld "X-KVC-Sendersystem" enthalten.

[KVC-Anb100] Das "X-KVC-Sendersystem" MUSS erkennen lassen, welches System für die Erstellung der fachlichen Inhalte und in diesem Zusammenhang mit den Umgang eventueller Rückmeldungen und deren Inhalte verantwortlich ist.

Der Feldinhalt besteht aus zwei Teilen, die durch Semikolon getrennt werden und somit hierarchisch voneinander abhängen:

Feldteil	Beschreibung	Pflichtfeld
1	<p>Beispiele</p> <ul style="list-style-type: none"> • Name des Praxisverwaltungssystem • Name des Labordateninformationssystem • Name des Krankenhausinformationssystem • Name des Dokumentationssystem • Name des Kombinationssystem • etc. 	ja
2	Version der Software	ja

Ein (fiktives) Beispiel: "IT-Doktor;V1.2"

Das MIME-Header Feld "X-KVC-Sendersystem" ist case-insensitive; trotzdem sollte die vorgegebene Schreibweise verwenden.

Der Feldinhalt ist hingegen case-sensitive: Es ist darauf zu achten, dass innerhalb eines Produkts die Schreibweise des Produktnamens und ggf. der Version immer identisch verwendet wird.

3.2.2 MIME-Header-Feld "X-KVC-Dienstkennung"

[KVC-Anb110] Der MIME-Header jeder KV-Connect Nachricht MUSS das Feld "X-KVC-Dienstkennung" enthalten.

[KVC-Anb120] Der Feldinhalt der "X-KVC-Dienstkennung" MUSS gemäß der jeweiligen Anwendungsspezifikation gefüllt sein.

[KVC-Anb130] Ist die Dienstkennung für die Anwendung nicht spezifiziert, für die die Nachricht vorgesehen ist, MUSS als Fallback-Wert die X-KVC-Dienstkennung der Anwendung "eNachricht" in einer von der kv.digital GmbH unterstützten Version verwendet werden.

Das Feld besteht aus drei Teilen, die durch Semikolon getrennt werden: <anwendungskürzel>{-<typ>};<sendungstyp>:<spezifikations-version>.

Feldteil	Beschreibung	Pflichtfeld
1	Name der Anwendung bzw. des Dienstes, ggf. ergänzt durch den Typ	ja
2	Sendungstyp	nein*

3	Spezifikations-Version	nein*
---	------------------------	-------

*abhängig von der konkreten Anwendungsspezifikation

Das MIME-Header Feld "X-KVC-Dienstkennung" ist case-insensitive; trotzdem sollte die vorgegebene Schreibweise verwendet werden.

Der Feldinhalt ist hingegen case-sensitive: Der Feldinhalt wird von der jeweiligen Anwendung spezifiziert und wird sich nicht allein an den unterschiedlichen Schreibweisen unterscheiden.

Es ist darauf zu achten, dass der Feldinhalt die Schreibweise der Spezifikation entspricht und immer identisch verwendet wird.

3.2.3 MIME-Header-Feld "Subject"

[KVC-Anb140] Der Feldinhalt des "Subjects" MUSS gemäß der jeweiligen Anwendungsspezifikation gefüllt sein.

[KVC-Anb150] Ist für eine Anwendung der Feldinhalt des "Subjects" nicht spezifiziert, so darf dieser keine datenschutzrelevanten Informationen enthalten.

3.2.4 MIME-Header-Feld "Message-ID"

[KVC-Anb160] Der MIME-Header jeder KV-Connect Nachricht MUSS das Feld "Message-ID" gemäß [RFC 5322] enthalten.

3.2.5 MIME-Header-Feld "BCC"

Das Setzen und Befüllen des Header-Feldes "BCC" ist bei KV-Connect nicht vorgesehen. Somit ist in allen Nachrichten das Header-Feld "BCC" nicht erlaubt.

[KVC-Anb170] Das Header-Feld "BCC" DARF NICHT im MIME-Header von KV-Connect Nachrichten enthalten sein.