gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Elektronische Gesundheitskarte und Telematikinfrastruktur

Online-Produktivbetrieb (OPB)

Migrationsstrategie Release 3.1.2

Version:	1.10.0
Revision:	3
Stand:	22.11.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemStrat_Mig_R3.1.2]

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um eine Erstveröffentlichung für das Release 3.1.2.

Dokumentenhistorie

Ver-sion	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	20.03.17		Initiale Version	gematik
1.2.0	19.06.17		Änderungen zu Release R1.6.4	gematik
1.3.0	12.07.17		Änderungen zu Release R1.6.4-1	gematik
1.4.0	07.11.17		Änderungen zu Release R1.6.4-2	gematik
1.5.0	06.02.18		Änderungen zu Release R2.1.1	gematik
1.6.0	14.05.18		Änderungen zu OPB R2.1.2	gematik
1.7.0	08.11.18		Änderungen zu OPB R2.1.3	gematik
1.8.0	18.12.18		Änderungen zu OPB R3.0.0	gematik
1.9.0	12.07.19		Änderungen zu OPB R3.1.0	gematik
1.10.0	22.11.19		Änderungen zu OPB R3.1.2	gematik

Inhaltsverzeichnis

Dokumentinformationen 2
Änderungen zur Vorversion 2
Dokumentenhistorie 2
Inhaltsverzeichnis 3
1 Einordnung des Dokuments 4
1.1 Zielsetzung 4
1.2 Zielgruppe 4
1.3 Geltungsbereich 4
1.4 Abgrenzung des Dokuments 4
2 Einleitung 6
3 Migrationsaspekte 7
3.1 Migrationsrelevante Änderungen 8
3.2 Migration der Produkttypen 13
3.2.1 MIRÄ_004 – Parallelbetrieb ORS1/OPB1 – KSR 13
3.2.2 MIRÄ_006 – eIDAS - Erstellung und Validierung QES sowie Ablösung xTV durch SignaturProxy 14
3.2.3 MIRÄ_007 – Sicherstellung der Interoperabilität der Signaturschnittstelle des Konnektors 15
3.2.4 MIRÄ_009 – Verhinderung inkorrekter Fehlerbehandlung im PS 15
3.2.5 MIRÄ_010 – TSL ohne QES-Zertifikate / dadurch Anpassungen an QES-Zertifikatsprüfung 16
3.2.6 MIRÄ_011 – Neuer Produkttyp Service Monitoring 16
3.2.7 MIRÄ_012 – RSA nach ECC- Migration – TSL-Dienst zuerst 17
3.2.8 MIRÄ_013 – Abkündigung von TLS 1.1 ab PTV3 Konnektoren 19
Anhang A – Verzeichnisse 20
A1 – Abkürzungen 20
A2 – Glossar 20
A3 – Tabellenverzeichnis 20
A4 – Referenzierte Dokumente 21
A4.1 – Dokumente der gematik 21
Anhang B – Anforderungsänderungen 22
Anhang C – Nicht mehr migrationsrelevante Änderungen 29

1 Einordnung des Dokuments

1.1 Zielsetzung

Die technische Migrationsstrategie Release R3.1.2 ist Bestandteil des Dokumentenpakets für das Release R3.1.2. Zielsetzung des Dokuments ist es, funktionale Abhängigkeiten auf Spezifikationsniveau bei der Migration von Produkttypen der TI im Release R3.1.2 darzustellen.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von Produkten der TI.

1.3 Geltungsbereich

Dieses Dokument enthält Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Wichtiger Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzung des Dokuments

Dieses Dokument selbst enthält keine normativen Festlegungen zur Telematikinfrastruktur, sondern greift lediglich normative Festlegungen aus den Konzepten und Spezifikationen des Dokumentpakets zum Release R3.1.2 auf und stellt funktionale Abhängigkeiten dar, die bei der Migration von Produkttypen der TI zu berücksichtigen sind.

Zeitliche Aussagen werden nur getroffen, sofern hierzu Gesellschafterbeschlüsse vorliegen oder sich zeitliche Abhängigkeiten aus Gesetzen oder sonstigen Richtlinien/Normen (z. B. technische Richtlinien des BSI) ergeben.

Die in diesem Dokument dargestellten Migrationsaspekte gelten primär für die Produktivumgebung der TI. Grundsätzlich sind sie auch in der Referenz- und Testumgebung der TI anwendbar. Hier können aber zusätzlich zu betrachtende Migrationsaspekte existieren.

Da dieses Dokument nur Aussagen zur Kompatibilität auf Spezifikationsebene zwischen betroffenen Produkttypen trifft, ist eine abschließende Kompatibilitätsprüfung in jedem Fall durch geeignete Testmaßnahmen der Produkte sicherzustellen.

2 Einleitung

In diesem Dokument werden Abhängigkeiten bei der Migration einzelner Produkttypen der TI im Release R3.1.2 dargestellt.

Dadurch, dass in dieser Migrationsstrategie auch alle relevanten Produkttypversionen betrachtet werden, für die sich noch Produkte in der Produktivumgebung im Einsatz befinden, adressiert diese Migrationsstrategie alle funktionalen Aspekte, die bzgl. der Migration der TI zum Zeitpunkt der Veröffentlichung dieses Dokumentes zusammen zu betrachten sind. Relevante Inhalte aus älteren Migrationsstrategien werden damit in dieses Dokument übernommen. Ältere Migrationsstrategien brauchen daher bei der Migration der TI nicht herangezogen zu werden.

Dieses Dokument ist folgendermaßen gegliedert:

Kapitel 3.1 gibt eine Übersicht aller migrationsrelevanten Änderungen nebst betroffenen Produkttypen, die funktionale Abhängigkeiten zwischen den Produkttypen aufweisen, die in einer Migrationsbetrachtung zu berücksichtigen sind. Alle anderen Änderungen der TI haben keine funktionalen Abhängigkeiten, die im Rahmen einer Migration zu berücksichtigen sind.

Kapitel 3.2 enthält für alle migrationsrelevanten Änderungen eine detaillierte Betrachtung der bei der Migration zu berücksichtigenden Abhängigkeiten sowie eine oder mehrere Migrationspfade, die aufzeigen, wie und in welcher Reihenfolge die betroffenen Produkttypen in der Produktivumgebung aktualisiert werden müssen.

3 Migrationsaspekte

Anhand der bei der Migration der TI zu betrachtenden Produkttypversionen wird in Kapitel 3.1 im Detail auf die einzelnen Inkompatibilitäten eingegangen.

3.1 Migrationsrelevante Änderungen

Im Kontext eines neuen Dokumentenreleases der TI können Änderungen der TI wie beispielsweise Erweiterungen der TI oder Fehlerkorrekturen erfolgen, die einen oder mehrere Produkttypen betreffen. Bei der Migration der betroffenen Produkttypen der TI bei diesen Änderungen Abhängigkeiten bestehen, die eine bestimmte Reihenfolge bei der Aktualisierung in der Produktivumgebung oder spezifische Migrationsschritte erfordern. Folgende Tabelle gibt eine Übersicht über alle derartigen migrationsrelevanten Änderungen, die bei der Migration der TI auf das Release R3.1.2 zu betrachten sind. Diese Änderungen stellen den maßgeblichen Betrachtungsgegenstand dieser Migrationsstrategie dar.

Tabelle 1: Liste der migrationsrelevanten Änderungen mit Auswirkungen auf betroffene Produkttypen

ID-Kürzel (IK-Kürzel)	Änderung mit Release	Titel	Beschreibung	Von der Änderung betroffene Produkttypen und Komponenten	Betroffene PTV (mit PTV < als)
MIRÄ_004	R1.6.3	Parallelbetrieb ORS1/OPB1 – KSR	Die notwendige Unterscheidung der Update-Pakete für Konnektoren und eHealth-Kartenterminals wird über eine strukturierte Benennung der Update-ID und die Funktionalität des Konnektors, Update-Pakete unterschiedlicher Zugehörigkeit (Produktivbetrieb und Erprobungsmaßnahmen) anzeigen zu können, erreicht.	Konnektor (VSDM)	1.9.0-0 r1.0.1
				Konnektor (QES)	2.10.0-0 r1.1.0
MIRÄ_006 (IK08, IK09, IK10, IK11, IK13)	R1.6.4	eIDAS – Erstellung und Validierung QES sowie Ablösung xTV durch SigProxy	Die Vertrauensliste (VL) der BNetzA ersetzt die BNetzA-Root-CA als Vertrauensanker für QES-Signaturzertifikate: Verweise auf die BNetzA-Root-CA und den BNetzA-OCSP-Responder werden entfernt und die Funktionalität des OCSP-Proxys wird auf die Sperrprüfung von X.509-Zertifikaten der HBA-Vorläuferkarten reduziert. Die Vertrauensliste der BNetzA wird integritätsge-	Konnektor (QES)	2.10.0-0 r1.1.0
				TSP X.509 nonQES – Komp	1.7.0 r1.2.1
				TSL-Dienst	1.7.0 r1.0.1
				Primärsystem (QES relevante Schnittstellen)	n/a

ID-Kürzel (IK-Kürzel)	Änderung mit Release	Titel	Beschreibung	Von der Änderung betroffene Produkttypen und Komponenten	Betroffene PTV (mit PTV < als)
			schützt durch den TSL-Dienst in der TI bereitgestellt, wofür der TSL-Dienst eine neue Identität aus der X.509-Komponenten-PKI erhält. Weiterhin werden die Normen für die Signaturformate XAdES, CAdES und PAdES an den Stand des Durchführungsbeschluss (EU) 2015/1506 der Kommission angepasst sowie die Stelle korrigiert, an der OCSP-Responses in einer CAdES-Signatur eingebettet werden müssen. Darüber hinaus löst der Signaturproxy, als zum Konnektor gehörige externe Komponente in der Leistungserbringerumgebung, den xTV ab und übernimmt die Anzeige von zu signierenden/prüfenden Daten.		
MIRÄ_007 (IK12)	R1.6.4	Sicherstellung der Interoperabilität der Signaturschnittstellen der Konnektoren.	Mit der Änderung wird der Kontext bzw. die Bedeutung eines über die Operationen `ExternalAuthenticate` und `VerifyDocument` für die PKCS#1-Signatur übergebenen Binärstrings festgelegt sowie dessen Verarbeitung durch den Konnektor. Diese Festlegung dient der übergreifenden Interoperabilität bzgl. oben genannter Schnittstelle für PKCS#1 Signaturen.	Konnektor (QES)	2.10.0-0 r1.1.0
				Primärsystem (QES relevante Schnittstellen)	n/a
MIRÄ_009 (IK15)	R1.6.4-2	Verhinderung inkorrekter Fehlerbehandlungen in Primärsystemen	Die Korrektur soll verhindern, dass der PS-Hersteller für den Fehler 3039 eine inkorrekte Fehlerbehandlung durchführt.	Konnektor (VSDM)	1.10.2-0
				Konnektor (QES)	2.11.2-0
				Primärsystem	n/a
MIRÄ_010 (IK16,	R2.1.2	TSL ohne QES-Zertifikate / dadurch		TSL-Dienst	1.8.0-0
				OCSP Responder Proxy	2.1.0-0

ID-Kürzel (IK-Kürzel)	Änderung mit Release	Titel	Beschreibung	Von der Änderung betroffene Produkttypen und Komponenten	Betroffene PTV (mit PTV < als)
IK17, IK18)		Anpassungen an QES-Zertifikatsprüfung	Die QES-CA-Elemente werden aus der TSL entfernt. In die TSL werden zusätzlich Informationen zu den OCSP Responder Proxys für QES in der TI aufgenommen. Der OCSP Responder Proxy leitet OCSP-Anfragen für QES ins Internet weiter und sendet die Antwort zurück an den OCSP-Client.	Konnektor PTV2 (QES)	2.12.0-0
				Konnektor PTV3 (eMP/AMTS, NFDM)	3.1.0-0
MIRÄ_011 (IK19)	R2.1.2	Neuer Produkttyp Service Monitoring	Für den neuen Produkttyp Service Monitoring müssen die Zertifikate C.NK.VPN und C.FD.TLS-C beim TSP X.509 (nonQES) Komp abrufbar sein.	TSP X.509 (nonQES) Komp	1.8.1-0
				Service Monitoring	1.0.0-0
MIRÄ_012 (IK20)	R3.1.0	RSA nach ECC-Migration – TSL-Dienst zuerst	Die gematik hat im Dokumentenrelease OPB R3.1.0 Festlegungen für die Umstellung der kryptographischen Verfahren der TI von RSA-2048 auf ECC-256 für die X.509 PKI für die Produkttypen der TI (außer Karten) getroffen.	TSL Dienst	2.0.0-0
				OCSP-Responder Proxy	2.3.0-0
				Trust Service Provider X.509 (nonQES) – eGK	1.8.0-0
				Trust Service Provider X.509 (nonQES) – HBA	1.8.0-0
				Trust Service Provider X.509 (nonQES) – SMC-B	1.11.0-0
				Trust Service Provider X.509 (nonQES) – Komp	1.10.0-0
				Trust Service Provider X.509 QES	1.9.0-0
				Namensdienst	1.6.1-0
				Konfigurationsdienst	1.8.2-0
				Sicherheitsgateway Bestandsnetze	1.7.2-0

ID-Kürzel (IK-Kürzel)	Änderung mit Release	Titel	Beschreibung	Von der Änderung betroffene Produkttypen und Komponenten	Betroffene PTV (mit PTV < als)
				VPN-Zugangsdienst	1.8.0-0
				Zeitdienst	1.5.3-0
				Zentrales Netz der TI	1.5.5-0
				Intermediär VSDM	1.6.0-0
				Verzeichnisdienst	1.4.0-0
				Fachdienste VSDM	1.6.0-0
				Fachdienst KOM-LE	1.3.0-0
				Clientmodul KOM-LE	1.3.0-0
				KTR-AdV	1.0.0-0
				ePA-Aktensystem	1.1.0-0
				Signaturdienst	1.0.0-0
				Schlüsselgenerierungsdienst ePA	1.0.0-0
				Basis-Consumer	1.0.0-0
				KTR-Consumer	1.0.0-0
				Spezifikation Service Monitoring	In Vorbereitung
				Konnektor PTV4 (ePA)	4.1.0-0
				eHealth-Kartenterminal	1.3.0-0
				Mobiles Kartenterminal	1.4.0-0
				Frontend des Versicherten ePA	1.1.0-0
				Primärsysteme	
MIRÄ_013	R3.1.2			Konnektor PTV3	3.5.0-0

ID-Kürzel (IK-Kürzel)	Änderung mit Release	Titel	Beschreibung	Von der Änderung betroffene Produkttypen und Komponenten	Betroffene PTV (mit PTV < als)
(IK21)		Abkündigung von TLS 1.1 ab PTV3-Konnektoren	Zwischen Primärsystem und PTV3-Konnektor muss TLS 1.2 oder höher verwendet werden.	Primärsysteme	

3.2 Migration der Produkttypen

Dieses Kapitel enthält für alle in Kapitel 3.1 benannten migrationsrelevanten Änderungen eine detaillierte Betrachtung der bei der Migration zu berücksichtigenden Abhängigkeiten. Hierbei werden ein oder mehrere Migrationspfade aufgezeigt, wie und in welcher Reihenfolge die betroffenen Produkttypen in der Produktivumgebung aktualisiert werden müssen, ohne dass es (außerhalb definierter Wartungsfenster) zu Einschränkungen in der Verfügbarkeit der TI kommt. Hierbei ist unter „Abhängigkeiten (Deployment)/Reihenfolge“ folgende Syntax zu unterscheiden:

- „1, 2, 3, …“: Die Reihenfolge der Aktualisierung der Produkttypen ist strikt einzuhalten, da ansonsten Inkompatibilitäten auftreten (erst „1“, dann „2“ und dann „3“).
- „1, 2, 2, 3“: Eine synchrone Umstellung einzelner Produkttypen ist zwingend einzuhalten, da bspw. keine Abwärtskompatibilität besteht (beide mit „2“ markierten Produkttypen müssen synchron – z. B. in einem gemeinsamen Wartungsfenster – umgestellt werden).
- „1, 2a, 2b“: Eine Aktualisierung der Produkttypen kann in beliebiger Reihenfolge durchgeführt werden (Die mit „2a“ und „2b“ markierten Produkttypen können in beliebiger Reihenfolge aktualisiert werden.)

Bei der definierten Reihenfolge müssen alle Produkte der betrachteten Produkttypen in der Produktivumgebung analysiert werden.

3.2.1 MIRÄ_004 – Parallelbetrieb ORS1/OPB1 – KSR

Tabelle 2: Migrationsaspekte für MIRÄ_004 – Parallelbetrieb ORS1/OPB1 – KSR

Beschreibung	Die notwendige Unterscheidung der Update-Pakete für Konnektoren und eHealth-Kartenterminals wird über eine strukturierte Benennung der Update-ID und die Funktionalität des Konnektors, Update-Pakete unterschiedlicher Zugehörigkeit (Produktivbetrieb und Erprobungsmaßnahmen) anzeigen zu können, erreicht. Die hier dargestellte, resultierende Lösung für das Ziel-Release ersetzt die Änderungen zu R1.6.2.	
Inkompatibilitäten	keine	
Abhängigkeiten (Deployment)		
Reihenfolge	**PT**	**Erforderliche PTV**
1a	Konnektor (VSDM)	1.10.2-0
1b	Konnektor (QES)	2.11.2-0
Migrationsaspekte	Ohne diese Änderung kann bei parallel zum Produktivbetrieb stattfindenden Erprobungen (z. B. ORS1) von Leistungserbringern bzw. DVOs beim Aktualisieren der Firmware von Konnektoren und eHealth-Kartenterminals nicht eindeutig zwischen Firmware-Versionen aus dem	

	Produktivbetrieb bzw. von Erprobungsmaßnahmen unterschieden werden. Es besteht die Gefahr, dass falsche Firmware-Versionen eingespielt werden.

3.2.2 MIRÄ_006 – eIDAS - Erstellung und Validierung QES sowie Ablösung xTV durch SignaturProxy

Tabelle 3: Migrationsaspekte für MIRÄ_006 – eIDAS - Erstellung und Validierung QES sowie Ablösung xTV durch SignaturProxy

Beschreibung	Die Vertrauensliste (VL) der BNetzA ersetzt die BNetzA-Root-CA als Vertrauensanker für QES-Signaturzertifikate: entsprechende Verweise auf die BNetzA-Root-CA und den BNetzA-OCSP-Responder werden entfernt und die Funktionalität des OCSP-Proxys wird auf die Sperrprüfung von X.509-Zertifikaten der HBA-Vorläuferkarten reduziert. Die Vertrauensliste der BNetzA wird integritätsgeschützt durch den TSL-Dienst in der TI bereitgestellt, wofür der TSL-Dienst eine neue Identität aus der X.509-Komponenten-PKI erhält. Weiterhin werden die Normen für die Signaturformate XAdES, CAdES und PAdES an den Stand des Durchführungsbeschluss (EU) 2015/1506 der Kommission angepasst. Außerdem wird die Stelle korrigiert, an der OCSP-Responses in einer CAdES-Signatur eingebettet werden müssen. Darüber hinaus löst der Signaturproxy, als zum Konnektor gehörige externe Komponente in der Leistungserbringerumgebung, den xTV ab und übernimmt die Anzeige von zu signierenden/prüfenden Daten.	
Inkompatibilitäten	IK08	Der TSL-Dienst der Basis-Releases R1.5.6 und R1.6.2 bietet den Download der BNetzA-VL nicht an. Bei dem Versuch eines Downloads der BNetzA-VL eines Ziel-Release-QES-Konnektors von einem Basis-Release-TSL-Dienst wird der QES-Konnektor in den Betriebsmodus „kritischer Betriebszustand“ geschaltet.
	IK09	Die in IK08 beschrieben Inkompatibilität tritt ebenfalls auf, sofern ein Basis-Releases-QES-Konnektor (R1.5.6) versucht, vom TSL-Dienst der Version 1.6.0 (existiert im Ziel-Release parallel zur aktuellsten PTV 1.7.0-2), die BNetzA-VL zu laden. Ein solcher Versuch resultiert ebenfalls im Betriebsmodus „kritischer Betriebszustand“ des aufrufenden QES-Konnektors.
	IK10	Die Signaturschnittstelle des QES-Konnektors wird um den neuen verpflichtenden Parameter `JobNummer` erweitert, der einen zu bearbeitenden Signaturauftrag identifiziert.
	IK11	Durch die Änderung in der ETSI-Vorgabe gegenüber der vorher maßgebenden Version 2.1.1 ändert sich der Speicherort für die Einbettung von OCSP-Responses in die Signatur im CAdES-Fall von „revocation-values“ zu „SignedData.crls.other“.
	IK13	Die Clientsystemschnittstelle des Signaturproxys wurde im Bezug auf den Parameterwert TvMode = "NONE" überarbeitet. Für die Antwortnachricht der SignDocument Operation wird festgelegt, welche Rückgabewerte es für Dokumente gibt,

	die vom Benutzer im Signaturproxy durch Deselektion von der Signatur ausgeschlossen wurden.	
Abhängigkeiten (Deployment)		
Reihenfolge	**PT**	**Erforderliche PTV**
1	TSP X.509 Komp	1.8.0-1
2	TSL-Dienst	1.7.0-2
3	Konnektor (QES)	2.11.2-0
4	Primärsystem (QES-relevante Schnittstellen)	n/a
Migrationsaspekte	Primärsysteme, die vormals die Signaturschnittstelle des Konnektors direkt angesprochen haben und dies weiter tun möchten, benötigen jetzt den neuen Parameter `JobNummer`. Alternativ kann der lokal beim Primärsystem installierte Signaturproxy angesprochen werden, der eine kompatible Schnittstelle implementiert.	

3.2.3 MIRÄ_007 – Sicherstellung der Interoperabilität der Signaturschnittstelle des Konnektors

Tabelle 4: Migrationsaspekte für MIRÄ_007 – Sicherstellung der Interoperabilität der Signaturschnittstelle des Konnektors

Beschreibung	Mit der Änderung wird der Kontext (Bedeutung) eines über die Operationen `ExternalAuthenticate` und `VerifyDocument` für die PKCS#1-Signatur übergebenen Binärstrings sowie dessen Verarbeitung durch den Konnektor festgelegt. Diese Festlegung dient der übergreifenden Interoperabilität bzgl. oben genannter Schnittstelle für PKCS#1-Signaturen.	
Inkompatibilitäten	IK12	Ohne diese Festlegung ist keine übergreifende Interoperabilität bzgl. der Schnittstellen `ExternalAuthenticate` und `VerifyDocument` für PKCS#1 Signaturen gegeben.
Abhängigkeiten (Deployment)		
Reihenfolge	**PT**	**Erforderliche PTV**
1a	Konnektor (QES)	2.11.2-0
1b	Primärsystem (QES-relevante Schnittstellen)	n/a
Migrationsaspekte	keine	

3.2.4 MIRÄ_009 – Verhinderung inkorrekter Fehlerbehandlung im PS

Tabelle 5: Migrationsaspekte für MIRÄ_009 – Verhinderung inkorrekter Fehlerbehandlung im PS

Beschreibung	Die Korrektur soll verhindern, dass der PS-Hersteller für den Fehler 3039 eine inkorrekte Fehlerbehandlung durchführt.	
Inkompatibilitäten	IK15	Primärsysteme, die die Änderung nicht umsetzen, führen bei oben genannter Fehlermeldung ggf. falsche Korrekturmaßnahmen durch.
Abhängigkeiten (Deployment)		

Reihenfolge	PT	Erforderliche PTV
2a	Primärsystem	n/a
2b	Konnektor (VSDM)	1.10.2-0
2c	Konnektor (QES)	2.11.2-0
Migrationsaspekte	Auf eine Rotmarkierung der Inkompatibilität wird an dieser Stelle verzichtet, da Primärsysteme keine Produkttypen der TI darstellen.	

3.2.5 MIRÄ_010 – TSL ohne QES-Zertifikate / dadurch Anpassungen an QES-Zertifikatsprüfung

Tabelle 6: Migrationsaspekte für MIRÄ_010 – TSL ohne QES-Zertifikate / dadurch Anpassungen an QES-Zertifikatsprüfung

Beschreibung	Die QES-CA-Elemente werden aus der TSL entfernt. In die TSL werden zusätzlich Informationen zu den OCSP Responder Proxys für QES in der TI aufgenommen. Der OCSP Responder Proxy leitet OCSP-Anfragen für QES ins Internet weiter und sendet die Antwort zurück an den OCSP-Client.	
Inkompatibilitäten	IK16	In der durch den TSL-Dienst des OPB R2.1.2 zur Verfügung gestellten TSL sind die QES-CA-Elemente nicht mehr enthalten. Bei Ausführung einer QES-Zertifikatsprüfung gem. TUC_PKI_030 nach altem Stand wird der Fehler CA_CERT_MISSING (1027) zurückgeliefert.
	IK17	In der durch den TSL-Dienst in früheren Releases zur Verfügung gestellten TSL sind die Zusatzinformationen zu den OCSP Responder Proxys für QES in der TI nicht enthalten.
	IK18	Der OCSP Responder Proxy mit dem Stand vor OPB R2.1.2 verarbeitet keine QES OCSP-Anfragen.

Abhängigkeiten (Deployment)		
Reihenfolge	PT	Erforderliche PTV
1	TSL-Dienst	1.8.0-0
1	OCSP Responder Proxy	2.1.0-0
2a	Konnektor PTV2 (QES)	2.12.0-0
2b	Konnektor PTV3 (eMP / AMTS, NFDM)	3.1.0-0
Migrationsaspekte	keine	

3.2.6 MIRÄ_011 – Neuer Produkttyp Service Monitoring

Tabelle 7: Migrationsaspekte für MIRÄ_011 – Neuer Produkttyp Service Monitoring

Beschreibung	Für den neuen Produkttyp Service Monitoring müssen die Zertifikate C.NK.VPN und C.FD.TLS-C beim TSP X.509 (nonQES) Komp abrufbar sein.	
Inkompatibilitäten	IK19	In der bisherigen Version des Zertifikatsmanagementsystems TMS gibt es für den Produkttyp Service Monitoring keine Berechtigungen, die Zertifikate C.NK.VPN und C.FD.TLS-C abzurufen.

Abhängigkeiten (Deployment)		
Reihenfolge	**PT**	**Erforderliche PTV**
1	TSP X.509 (nonQES) Komp	1.8.1-0
2	Service Monitoring	1.0.0-0
Migrationsaspekte	keine	

3.2.7 MIRÄ_012 – RSA nach ECC- Migration – TSL-Dienst zuerst

Tabelle 8: Migrationsaspekte für MIRÄ_012 – RSA nach ECC- Migration – TSL-Dienst zuerst

Beschreibung	Die gematik hat im Dokumentenrelease OPB R3.1.0 Festlegungen für die Umstellung der kryptographischen Verfahren der TI von RSA-2048 auf ECC-256 für die X.509 PKI für die Produkttypen der TI (außer Karten) getroffen. Für die geordnete Umstellung ist eine bestimmte Reihenfolge beim Rollout der ECC-fähigen Produkte wichtig. Dafür hat die gematik ihre TI-Produkttypen kategorisiert: • **Zentrale Server (TLS/IPsec):** zentrale Dienste der TI-Plattform und fachanwendungsspezifische Dienste mit IPsec oder TLS-Serveranteilen • **Zentrale Clients (TLS):** zentrale Dienste der TI-Plattform und fachanwendungsspezifische Dienste mit TLS-Clientanteilen • **Dezentrale Komponenten**: dezentrale Komponenten der TI-Plattform mit IPsec und TLS-Anteilen • Clientsysteme Der Rollout erfolgt in drei Schritten. Dabei muss jeder Schritt abgeschlossen sein, bevor der nächste Schritt erfolgen kann. Schritt 1: Die Verfügbarkeit einer ECC-fähigen TSL ist Grundvoraussetzung; daher wird der TSL-Dienst als erster Produkttyp umgestellt. Schritt 2: Dann werden die Zentralen TLS- und IPsec-Server sowie die Zentralen TLS-Clients umgestellt. Schritt 3: Danach können die Dezentralen Komponenten und die Clientsysteme umgestellt werden.

Inkompatibilitäten	IK20	Der TSL-Dienst ab PTV 2.0.0-0 stellt an einem neuen, weiteren Downloadpunkt die neue RSA-ECC-TSL zur Verfügung. Dort sind die für den ECC-Betrieb der Produkte der TI notwendigen Zertifikate aufgeführt. Jeder Produkttyp der ECC-fähig ist (definiert in OPB R3.1.0), benötigt den neuen TSL-Dienst (in RU, TU und PU).

Abhängigkeiten (Deployment)

Reihenfolge	PT	Erforderliche PTV
1	TSL Dienst	2.0.0-0
2a	OCSP-Responder Proxy	2.3.0-0
2b	Trust Service Provider X.509 (nonQES) – eGK	1.8.0-0
2c	Trust Service Provider X.509 (nonQES) – HBA	1.8.0-0
2d	Trust Service Provider X.509 (nonQES) – SMC-B	1.11.0-0
2e	Trust Service Provider X.509 (nonQES) – Komp	1.10.0-0
2f	Trust Service Provider X.509 QES	1.9.0-0
2g	Namensdienst	1.6.1-0
2h	Konfigurationsdienst	1.8.2-0
2i	Sicherheitsgateway Bestandsnetze	1.7.2-0
2j	VPN-Zugangsdienst	1.8.0-0
2k	Zeitdienst	1.5.3-0
2l	Zentrales Netz der TI	1.5.5-0
2m	Intermediär VSDM	1.6.0-0
2n	Verzeichnisdienst	1.4.0-0
2o	Fachdienste VSDM	1.6.0-0
2p	Fachdienst KOM-LE	1.3.0-0
2q	Clientmodul KOM-LE	1.3.0-0
2r	KTR-AdV	1.0.0-0
2s	ePA-Aktensystem	1.1.0-0
2t	Signaturdienst	1.0.0-0
2u	Schlüsselgenerierungsdienst ePA	1.0.0-0
2v	Basis-Consumer	1.0.0-0
2w	KTR-Consumer	1.0.0-0
2y	Spezifikation Service Monitoring	In Vorbereitung
3a	Konnektor PTV4 (ePA)	4.1.0-0
3b	eHealth-Kartenterminal	1.3.0-0
3c	Mobiles Kartenterminal	1.4.0-0

3d	Frontend des Versicherten ePA	1.1.0-0
3e	Primärsysteme	
Migrationsaspekte	Siehe Beschreibung	

3.2.8 MIRÄ_013 – Abkündigung von TLS 1.1 ab PTV3-Konnektoren

Tabelle 9 Migrationsaspekte für MIRÄ_013 – Abkündigung von TLS 1.1 ab PTV3-Konnektoren

Beschreibung	Das Bundesamt für Sicherheit in der Informationstechnik hat mit der Veröffentlichung der technischen Richtlinie TR-02102-2 die Protokollversion TLS 1.1 als unsicher eingestuft und empfiehlt die Verwendung von TLS 1.2 oder höher. Aufgrund der Vorgaben des BSI werden PTV3-Konnektoren TLS 1.1 nicht mehr unterstützen. Beim Aufbau einer TLS-gesicherten Verbindung zwischen Primärsystem und PTV3-Konnektor muss daher TLS 1.2 oder höher verwendet werden.	
Inkompatibilitäten	IK21 Der Konnektor unterstützt – neben TLS1.2 – nur in den Produkttypversionen 1 (PTV1) und 2 (PTV2) die TLS-Version 1.1. Nur mit diesen Produkttypversionen können Primärsysteme TLS-Version 1.1 verwenden. Ab der Konnektor-Produkttypversion 3 (PTV3) bietet der Konnektor TLS nur noch TLS 1.2 oder höher an. Primärsysteme, die bereits heute TLS1.2 oder höher unterstützen, sind von diesem Migrationsaspekt nicht betroffen.	
Abhängigkeiten (Deployment)		
Reihenfolge	**PT**	**Erforderliche PTV**
1	Primärsysteme	
2	Konnektor PTV3	3.5.0-0
Migrationsaspekte	s. Beschreibung	

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
i.V.	In Vorbereitung
PT	Produkttyp
PTV	Produkttypversion
PTSB	Produkttypsteckbrief
PTSBV	Produkttypsteckbriefversion (Dokumentenversion des Produkttypsteckbriefs)
r	Kennzeichner Dokumentenversion
R	Kennzeichner Release

A2 – Glossar

Das Glossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 – Tabellenverzeichnis

Tabelle 1: Liste der migrationsrelevanten Änderungen mit Auswirkungen auf betroffene Produkttypen 8

Tabelle 2: Migrationsaspekte für MIRÄ_004 – Parallelbetrieb ORS1/OPB1 – KSR 13

Tabelle 3: Migrationsaspekte für MIRÄ_006 – eIDAS - Erstellung und Validierung QES sowie Ablösung xTV durch SignaturProxy 14

Tabelle 4: Migrationsaspekte für MIRÄ_007 – Sicherstellung der Interoperabilität der Signaturschnittstelle des Konnektors 15

Tabelle 5: Migrationsaspekte für MIRÄ_009 – Verhinderung inkorrekter Fehlerbehandlung im PS 15

Tabelle 6: Migrationsaspekte für MIRÄ_010 – TSL ohne QES-Zertifikate / dadurch Anpassungen an QES-Zertifikatsprüfung 16

Tabelle 7: Migrationsaspekte für MIRÄ_011 – Neuer Produkttyp Service Monitoring 16

Tabelle 8: Migrationsaspekte für MIRÄ_012 – RSA nach ECC- Migration – TSL-Dienst zuerst 17

Tabelle 9 Migrationsaspekte für MIRÄ_013 – Abkündigung von TLS 1.1 ab PTV3 Konnektoren 19

Tabelle 10: Dokumente der gematik 21

Tabelle 11: Anforderungsgrundlage für migrationsrelevante Änderungen 22

Tabelle 12: Liste der nicht mehr migrationsrelevanten Änderungen 29

A4 – Referenzierte Dokumente

A4.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer entnehmen Sie bitte der aktuellen, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

Tabelle 10: Dokumente der gematik

[Quelle]	Herausgeber: Titel
[gemDokLK_R3.1.2]	gematik: Dokumentenlandkarte Online-Produktivbetrieb (Stufe 1) – OPB1, Festlegung der Versionsstände Release R3.1.2
[gemGlossar]	gematik: Glossar

Anhang B – Anforderungsänderungen

In diesem Anhang werden zur Übersicht die neuen bzw. geänderten Anforderungen in den Dokumenten in Kapitel 3.1 benannten migrationsrelevanten Änderungen zugrunde liegen, zusammengestellt. Diese Information ist lediglich informativ. Die vollständige Menge der Änderungen kann den in [gemDokLK_R3.1.2] aufgelisteten Dokumenten und Produkttypsteckbriefen entnommen werden.

Tabelle 11: Anforderungsgrundlage für migrationsrelevante Änderungen

ID	Titel MIRÄ	Afo-ID	Quelle (Referenz)
MIRÄ_004	Parallelbetrieb ORS1/OPB1 – Störungsampel	TIP1-A_6714	gemSpec_St_Ampel
MIRÄ_006	eIDAS – Erstellung und Validierung QES	TIP1-A_5844 TIP1-A_5846 TIP1-A_5847 TIP1-A_5850 TIP1-A_5854 TIP1-A_5857 TIP1-A_5858 TIP1-A_5859 TIP1-A_5860 TIP1-A_5861 TIP1-A_5862 TIP1-A_5863 TIP1-A_5864 TIP1-A_5855 TIP1-A_5856	gemSpec_OCSP_Proxy
		TIP1-A_4630 TIP1-A_4646 TIP1-A_4649 TIP1-A_4657 TIP1-A_4672 TIP1-A_4673 TIP1-A_4683 TIP1-A_6730 TIP1-A_6731 TIP1-A_6732 TIP1-A_4693 TIP1-A_6729 TIP1-A_4696 TIP1-A_5449 TIP1-A_4701 TIP1-A_4702 TIP1-A_6733 TIP1-A_6728 TIP1-A_4509	gemSpec_Kon
		GS-A_4698 GS-A_5483 GS-A_4750 GS-A_5484 GS-A_4896	gemSpec_PKI

ID	Titel MIRÄ	Afo-ID	Quelle (Referenz)
		GS-A_4940	
		TIP1-A_4055 TIP1-A_4056 TIP1-A_4060 TIP1-A_5120 TIP1-A_6750 TIP1-A_6751 TIP1-A_6752 TIP1-A_6753 TIP1-A_6754 TIP1-A_6755 TIP1-A_6756 TIP1-A_6757 TIP1-A_6758 TIP1-A_4448 TIP1-A_6759 TIP1-A_6760 TIP1-A_4099 TIP1-A_6761 TIP1-A_6762 TIP1-A_6763 TIP1-A_6764 TIP1-A_6765 TIP1-A_6766 TIP1-A_6767	gemSpec_TSL
	eIDAS – Ablösung xTV durch SignaturProxy	TIP1-A_4514 TIP1-A_5013 TIP1-A_4522 TIP1-A_4527 TIP1-A_4626 TIP1-A_5682 TIP1-A_5538 TIP1-A_4631 TIP1-A_5150 TIP1-A_4632 TIP1-A_4633 TIP1-A_5531 TIP1-A_5532 TIP1-A_4634 TIP1-A_4640 TIP1-A_4992 TIP1-A_4646 TIP1-A_4648 TIP1-A_4649 TIP1-A_4650 TIP1-A_4651 TIP1-A_4652 TIP1-A_4653 TIP1-A_4654 TIP1-A_5544 TIP1-A_5545 TIP1-A_4655 TIP1-A_4656 TIP1-A_5404 TIP1-A_4657	gemSpec_Kon gemSpec_Kon_SigProxy gemILF_PS

ID	Titel MIRÄ	Afo-ID	Quelle (Referenz)
		TIP1-A_4658 TIP1-A_4659 TIP1-A_4660 TIP1-A_4661 TIP1-A_4662 TIP1-A_4663 TIP1-A_5151 TIP1-A_4664 TIP1-A_4665 TIP1-A_4666 TIP1-A_4668 TIP1-A_4669 TIP1-A_5664 TIP1-A_4670 TIP1-A_4671 TIP1-A_4672 TIP1-A_5539 TIP1-A_5540 TIP1-A_4673 TIP1-A_5405 TIP1-A_4676 TIP1-A_5665 TIP1-A_5010 TIP1-A_5034 TIP1-A_5666 TIP1-A_5667 TIP1-A_5439 TIP1-A_4677 TIP1-A_4678 TIP1-A_4679 TIP1-A_4680 TIP1-A_4681 TIP1-A_6729 TIP1-A_5687 TIP1-A_5688 TIP1-A_5689 TIP1-A_5668 TIP1-A_5669 TIP1-A_5686 TIP1-A_5692 TIP1-A_5693 TIP1-A_5670 TIP1-A_5683 TIP1-A_5671 TIP1-A_5680 TIP1-A_5681 TIP1-A_5690 TIP1-A_5672 TIP1-A_5673 TIP1-A_5685 TIP1-A_5695 TIP1-A_5684 TIP1-A_5691 TIP1-A_5674 TIP1-A_5675	

ID	Titel MIRÄ	Afo-ID	Quelle (Referenz)
		TIP1-A_5676 TIP1-A_5677 TIP1-A_5678 TIP1-A_5679 TIP1-A_5694 GS-A_5519 GS-A_5520 GS-A_5521 GS-A_5522 TIP1-A_5695	
MIRÄ_007	Sicherstellung der Interoperabilität der Signaturschnittstelle des Konnektors	TIP1-A_5439	gemSpec_Kon gemProdT_Kon_PTV2
MIRÄ_009	Verhinderung inkorrekter Fehlerbehandlung im PS	n/a	gemILF_PS
MIRÄ_010	TSL ohne QES-Zertifikate/ dadurch Anpassungen an QES-Zertifikatsprüfung	GS-A_4750 GS-A_5517 TIP1-A_7219 TIP1-A_5849 GS-A_5065 TIP1-A_2035 TIP1-A_2044 TIP1-A_5172 TIP1-A_2066 TIP1-A_2069 TIP1-A_4044 TIP1-A_4851	gemSpec_PKI gemSpec_TSL gemSpec_OCSP-Proxy gemKPT_PKI_TIP gemProdT_TSL gemProdT_Kon gemProdT_OCSP_Proxy gemProdT_X.509_TSP_QES gemProdT_Kon_PTV3 gemProdT_Kon_PTV2
MIRÄ_011	Neuer Produkttyp Service Monitoring	TIP1-A_2098 GS-A_4219 GS-A_4155 GS-A_5028	gemKPT_Arch_TIP gemSpec_ServiceMon gemProdT_ServiceMon gemKPT_PKI_TIP gemRL_TSL_SP_CP gemSpec_X.509_TSP gemSpec_Perf
MIRÄ_012	RSA nach ECC- Migration – TSL-Dienst zuerst	A_14491 A_15312 A_15341 A_15542 A_16176 A_17089 A_17090 A_17094 A_17124 A_17125 A_17126 A_17148 A_17157 A_17183 A_17205 A_17206 A_17207 A_17208	gemILF_PS gemILF_PS_ePA gemILF_PS_NFDM gemKPT_Arch_TIP gemKPT_PKI_TIP gemProdT_Aktensystem_ePA gemProdT_Basis_Consumer gemProdT_FD_KOMLE gemProdT_FD_VSDM gemProdT_gematik-Root-CA gemProdT_Intermediär_VSDM gemProdT_Kon_PTV4 gemProdT_KSR gemProdT_KTR-AdV gemProdT_NamD gemProdT_OCSP_Proxy gemProdT_SG_BestNetze gemProdT_TSL

ID	Titel MIRÄ	Afo-ID	Quelle (Referenz)
		A_17209 A_17210 A_17220 A_17221 A_17239 A_17240 A_17288 A_17295 A_17322 A_17342 A_17344 A_17345 A_17359 A_17360 A_17370 A_17371 A_17374 A_17377 A_17464 A_17472 A_17483 A_17484 A_17521 A_17548 A_17549 A_17550 A_17575 A_17578 A_17600 A_17658 A_17664 A_17665 A_17680 A_17681 A_17682 A_17683 A_17684 A_17685 A_17686 A_17687 A_17688 A_17689 A_17690 A_17746 A_17750 A_17759 A_17768 A_17774 A_17775 A_17784 A_17804 A_17820 A_17821 A_17837 A_17951	gemProdT_VPN_ZugD gemProdT_VZD gemProdT_X.509_TSP_nonQES_eGK gemProdT_X.509_TSP_nonQES_HBA gem- ProdT_X.509_TSP_nonQES_Komp gem- ProdT_X.509_TSP_nonQES_SMC-B gemProdT_X.509_TSP_QES gemProdT_ZeitD gemProdT_ZentrNetz gemRL_QES_NFDM gemSpec_Au- thentisierung_Vers gemRL_TSL_SP_CP gemSpec_Autorisierung gemSpec_Basis_KTR_Consumer gemSpec_CM_KOM-LE gemSpec_FD_KOM-LE gemSpec_FM_ePA gemSpec_FM_ePA_KTR_Consumer gemSpec_FM_NFDM gemSpec_Frontend_Vers gemSpec_Kon gemSpec_Kon_SigProxy gemSpec_Krypt gemSpec_KSR gemSpec_KT gemSpec_KTR-AdV gemSpec_MobKT gemSpec_Perf gemSpec_PKI gemSpec_SGD_ePA gemSpec_SigD gemSpec_Systemprozesse_dezTI gemSpec_VPN_ZugD gemSpec_Card- Proxy

ID	Titel MIRÄ	Afo-ID	Quelle (Referenz)
		A_2382 GS-A_4213 GS-A_4642 GS-A_4648 GS-A_5207 GS-A_5612 KOM-LE-A_2020 NFDM-A_2113 NFDM-A_2123 TIP1-A_2072 TIP1-A_4056 TIP1-A_4059 TIP1-A_4373 TIP1-A_4397 TIP1-A_4506 TIP1-A_4512 TIP1-A_4517 TIP1-A_4518 TIP1-A_4545 TIP1-A_4546 TIP1-A_4569 TIP1-A_4579 TIP1-A_4585 TIP1-A_4616 TIP1-A_4617 TIP1-A_4620 TIP1-A_4621 TIP1-A_4622 TIP1-A_4647 TIP1-A_4648 TIP1-A_4651 TIP1-A_4652 TIP1-A_4653-02 TIP1-A_4654 TIP1-A_4655 TIP1-A_4676 TIP1-A_4680 TIP1-A_4691 TIP1-A_4693 TIP1-A_4695 TIP1-A_4697 TIP1-A_4698 TIP1-A_4699 TIP1-A_4700 TIP1-A_4701 TIP1-A_4703 TIP1-A_4704 TIP1-A_4720 TIP1-A_4834 TIP1-A_5010 TIP1-A_5034	

ID	Titel MIRÄ	Afo-ID	Quelle (Referenz)
		TIP1-A_5153 TIP1-A_5437 TIP1-A_5439 TIP1-A_5446 TIP1-A_5478 TIP1-A_5487 TIP1-A_5488 TIP1-A_5517 TIP1-A_5662 TIP1-A_5665 TIP1-A_5674 TIP1-A_6018 TIP1-A_6019 TIP1-A_6123 TIP1-A_6132 TIP1-A_6899 TIP1-A_6976 TIP1-A_6980 TIP1-A_6984 TIP1-A_6987	
MIRÄ_13	Abkündigung von TLS 1.1 ab PTV3-Konnektoren	n.v.	gemProdT_Kon_PTV3

Anhang C – Nicht mehr migrationsrelevante Änderungen

In diesem Anhang werden zur Übersicht nicht mehr migrationsrelevante Änderungen aufgeführt. Diese Information ist lediglich informativ. Die vollständige Beschreibung der jeweiligen Änderung kann einer früheren Version dieser Migrationsstrategie entnommen werden.

Tabelle 12: Liste der nicht mehr migrationsrelevanten Änderungen

ID-Kürzel (IK-Kürzel)	Änderung mit Release	Titel	Beschreibung	Von der Änderung betroffene Produkttypen und Komponenten	Betroffene PTV (mit PTV < als)
MIRÄ_001 (IK01)	R1.6.2	Interoperable Umsetzung IPsec/IKEv2	Erst unter Anwendung von [RFC7427] (in Ergänzung zu [RFC5996]) ist eine interoperable Verwendung von SHA-2 für den Aufbau von Security Associations (SA) zwischen Konnektor und VPN-Zugangsdienst, entsprechend dem Internet Key Exchange Protocol Version 2 (IKEv2), möglich.	Konnektor (VSDM)	1.8.0 r1.0.0
				Konnektor (QES)	2.1.0 r1.1.0
				VPN-Zugangsdienst	1.6.0 r1.0.0
MIRÄ_002 (IK02)	R1.6.2	Rollenprüfung bei Registrierung des Konnektors am VPN-ZugD	Beim Verbindungsaufbau des Konnektors zum Registrierungsservice des VPN-Zugangsdienstes muss der Konnektor die technische Rolle des Serverzertifikats prüfen. Hierzu ist zusätzlich die Einführung von Zertifikaten mit einer neuen technischen Rolle durch die X.509-Komponenten-PKI notwendig. Entsprechende Zertifikate müssen durch den VPN-Zugangsdienst (Registrierungsdienst) verwendet werden.	TSP X.509 nonQES – Komp	1.7.0 r1.2.0
				Konnektor (VSDM)	1.8.0 r1.0.0
				Konnektor (QES)	2.1.0 r1.1.0
				VPN-Zugangsdienst	1.6.0 r1.0.0
MIRÄ_003	R1.6.2	Parallelbetrieb ORS1/OPB1 – Störungsampel	Die Störungsampel wird erweitert, um den Status der TI für den Produktivbetrieb und möglicher paralleler Erprobungsmaßnahmen (z. B. ORS1) über getrennte Service-Bäume darzustellen.	Störungsampel	1.6.0 r1.0.0

ID-Kürzel (IK-Kürzel)	Änderung mit Release	Titel	Beschreibung	Von der Änderung betroffene Produkttypen und Komponenten	Betroffene PTV (mit PTV < als)
MIRÄ_005 (IK05)	R1.6.3	Sicherstellung der Interoperabilität von Primärsystemen mit verschiedenen Konnektoren	Die Änderung vereinheitlicht die Verarbeitung von Konnektor-Subscriptions in Primärsystemen, um Fehlerquellen durch unterschiedliche Verarbeitung von Event-Subscriptions zu vermeiden. Hinweis: Es ist allerdings davon auszugehen, dass OPB-Primärsysteme nicht in Interaktion mit ORS1-Konnektoren treten.	Konnektor (VSDM)	1.9.0-0 r1.0.1
				Konnektor (QES)	2.10.0-0 r1.1.0
				Primärsystem	n/a
MIRÄ_008 (IK14)	R1.6.4	Verbesserung der Interoperabilität durch einheitliche TLS-Verbindungsabsicherung	Zu Kartenterminals, die im interoperablen Modus (wie bspw. in ORS1) betrieben werden, können Konnektoren keine Verbindung mehr aufbauen. Erst KTs, die den Anforderungen gemäß OPB1-Release-1.6.4 genügen, können sich wieder mit den OPB-Konnektoren verbinden.	eHealth-KT	1.2.1-0 r1.0.0
				Konnektor (VSDM)	1.10.0-0 r1.0.2
				Konnektor (QES)	2.11.0-0 r1.0.2