Informationsblatt

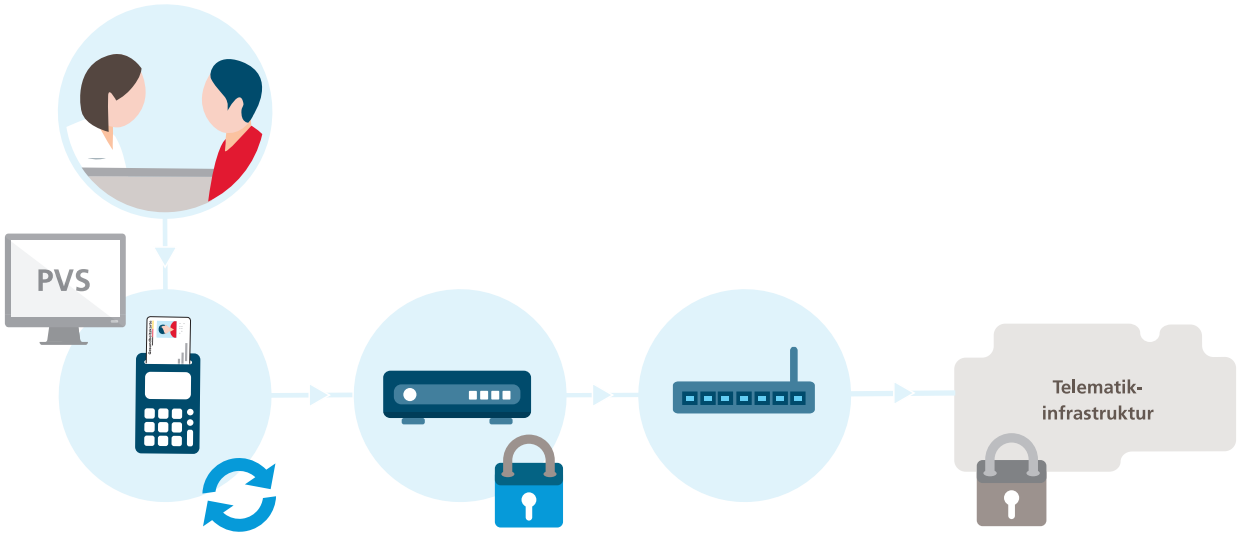
Anschluss einer medizinischen Einrichtung

So funktioniert der Zugang zur Telematikinfrastruktur praktisch!

Die Anbindung der Praxis, des Medizinischen Versorgungszentrums oder des Krankenhauses an das digitale Netz des Gesundheitswesens erfolgt mithilfe des Konnektors. Dafür gibt es zwei unterschiedliche Szenarien, zwischen denen Ärzte, Zahnärzte und Psychotherapeuten wählen können.

1. Integriertes Szenario (Standard-Szenario)

Beim integrierten Szenario werden Konnektor und Kartenterminal(s) mit dem Praxisnetzwerk (LAN) verbunden. Die Praxis geht bei diesem Szenario als Ganzes ans Netz, ist aber durch Technik mit hohem Sicherheitsniveau optimal geschützt. Nur bei diesem Szenario kann die medizinische Einrichtung alle Anwendungen des digitalen Netzes des Gesundheitswesens nutzen.



gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Damit stehen der Praxis eine vollständige Anbindung weiterer Anwendungen und zukünftige Ausbaustufen von bestehenden Anwendungen zur Verfügung. Das integrierte Szenario ist auch das Szenario mit dem maximalen Nutzerkomfort. Mit diesem Szenario kann aus dem Praxisnetz heraus der Sichere Internetzugang (Secure Internet Service) genutzt werden. Es erlaubt die Aktualisierung der Versichertenstammdaten am Empfang, das sofortige Einlesen der Stammdaten in das Praxisverwaltungssystem, den Versand elektronischer Dokumente von jedem beliebigen Praxisrechner sowie die Nutzung von künftigen Anwendungen der elektronischen Gesundheitskarte wie etwa Notfalldaten oder elektronischer Medikationsplan. Nur dieses Szenario ermöglicht eine vollständige Prüfung der qualifizierten Signatur der Notfalldaten.

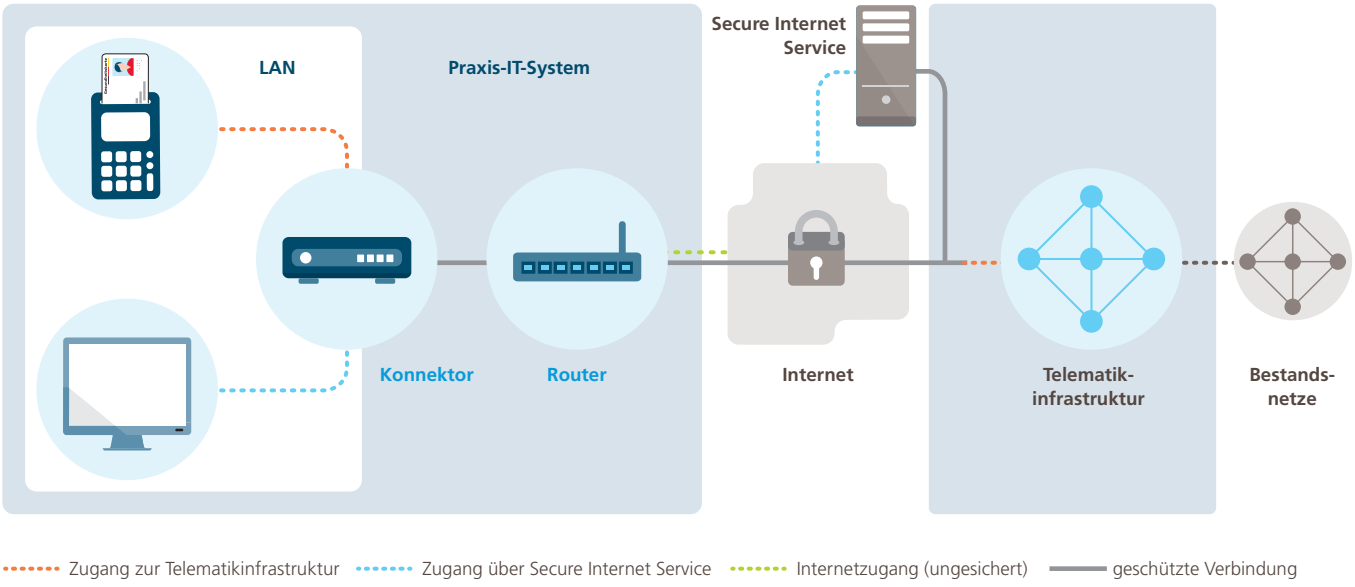
Betriebsarten zur Integration des Konnektors

Je nachdem, wie der Konnektor in das Netzwerk der Praxis oder des Krankenhauses eingebracht wird, ergeben sich Unterschiede bei den verfügbaren Funktionen, Diensten und der Sicherheit. Unabhängig von der gewählten Betriebsart sollte die Verbindung zwischen dem Praxisverwaltungssystem und dem Konnektor durch Verschlüsselung und Authentisierung abgesichert werden (zum Beispiel durch Transport Layer Security). Dies garantiert einen durchgängigen Schutz bei der Übermittlung von medizinischen Daten.

Reihenbetrieb

Im Reihenbetrieb befinden sich alle Komponenten im selben Praxisnetzwerk (LAN) und erhalten Zugang über den Konnektor zur Telematikinfrastruktur. Durch die integrierte Firewall des Konnektors und den optionalen und gegebenenfalls kostenpflichtigen Secure Internet Service wird das LAN optimal vor unautorisierten Zugriffen von außen geschützt.

→ Diese Betriebsart ist leicht zu konfigurieren und gewährleistet eine vertrauliche Übertragung medizinischer Daten.

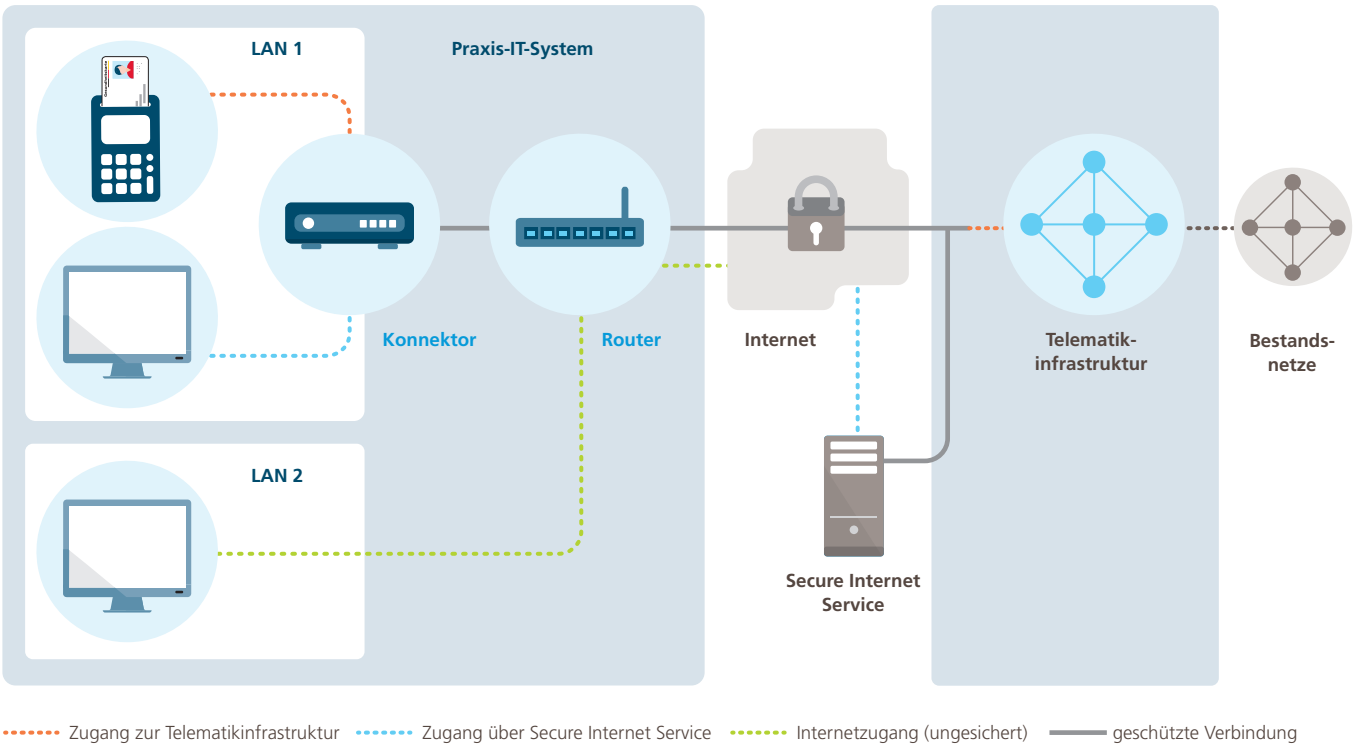


Netztrennung

Bei einer Netztrennung wird zusätzlich zum Praxisnetzwerk im Reihenbetrieb (hier LAN 1) ein zweites Netzwerk (LAN 2) eingerichtet, um einen direkten Zugriff auf das Internet zu ermöglichen. Komponenten des LAN 1 haben nur Zugang zur Telematikinfrastruktur und nutzen optional den Secure Internet Service, wohingegen Komponenten des LAN 2 ausschließlich einen Zugang zum Internet haben, der nicht über den Secure Internet Service abgesichert wird. Diese Betriebsart kann beispielsweise genutzt werden, um mit einem separaten Computer in das Internet zu gelangen. Der Nachteil ist jedoch, dass dieser Computer (LAN 2) nicht über den Secure Internet Service abgesichert wird.

→ Durch die integrierte Firewall des Konnektors ist das LAN 1 sowohl vor Zugriffen aus dem Internet als auch aus dem LAN 2 geschützt. Die Komponenten im LAN 2 sind allerdings nicht durch den Konnektor abgesichert. Die Konfiguration aller beteiligten Komponenten in der Praxis ist bei dieser Betriebsart etwas aufwendiger; gegebenenfalls ist ein zusätzlicher Netzwerkverteiler (Switch) erforderlich.

Die Netztrennung bietet eine hohe Sicherheit im LAN 1 und damit einen durchgängigen Schutz bei der Übermittlung medizinischer Daten. Durch das LAN 2 kann die Praxis zudem alle verfügbaren Internetdienste nutzen.



Der Konnektor ist am ehesten mit einem Router vergleichbar. Er besitzt jedoch einen deutlich größeren Funktionsumfang und ein sehr hohes Sicherheitsniveau. Die Konnektoren werden vom Bundesamt für Sicherheit in der Informationstechnik zertifiziert und von der gematik zugelassen.

Der Konnektor stellt ein sogenanntes virtuelles privates Netzwerk her, in dem elektronische Anwendungen unter Einsatz moderner Verschlüsselungstechnologien völlig abgeschirmt vom sonstigen Internet genutzt werden können.

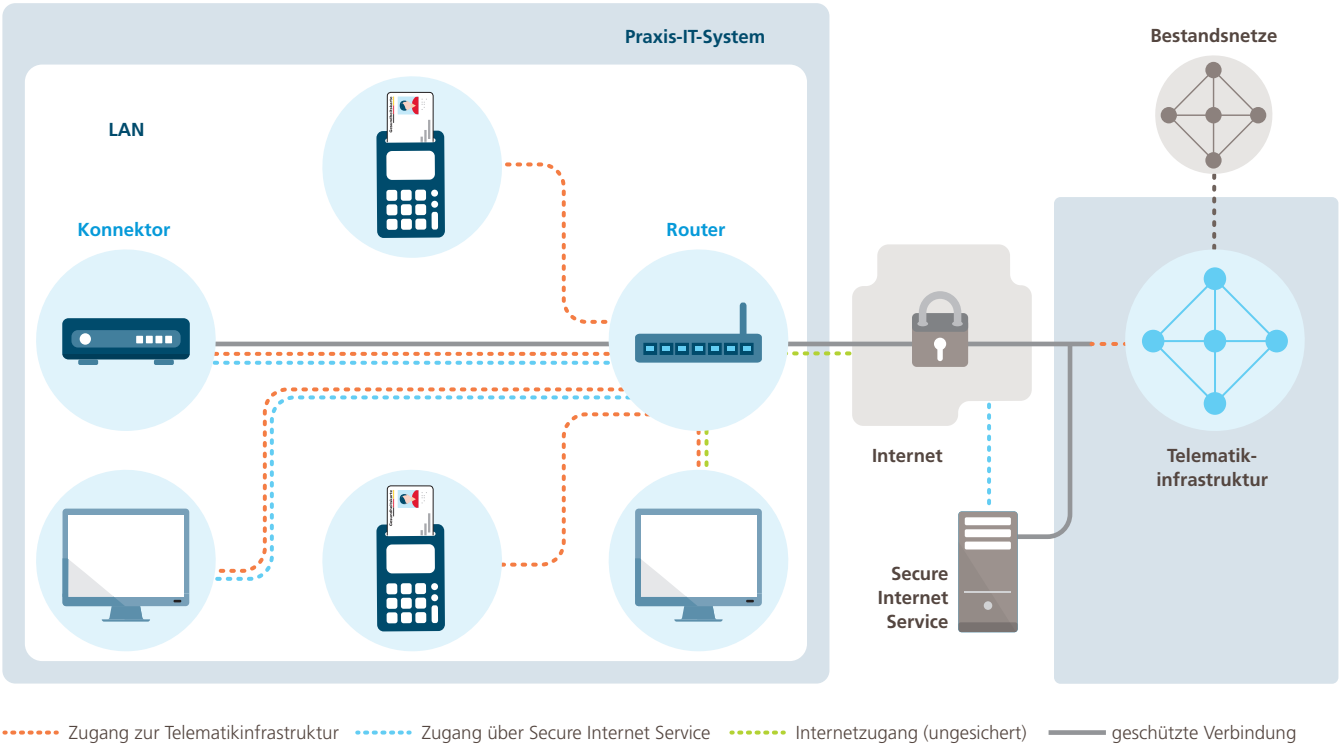
Parallelbetrieb

Im Parallelbetrieb sind alle Komponenten mittels eines Netzwerkverteilers (Switch/Router) miteinander verbunden. Die Komponenten zur Verarbeitung medizinischer Daten nutzen den Konnektor, um die Telematikinfrastruktur oder den optionalen Secure Internet Service zu erreichen. Die restlichen Komponenten erhalten über den Router direkten Anschluss an das Internet.

→ Ein bereits bestehendes LAN kann um den Konnektor ergänzt und weitergenutzt werden. Über den Router ist das Internet unabhängig vom Zugang zur Telematikinfrastruktur und mit allen Diensten verfügbar. Das Netzwerk ist flexibel konfigurierbar (nur Secure Internet Service/nur Internet/ Secure Internet Service plus Internet).

→ Wichtig: Im Parallelbetrieb ist keine Komponente des LAN durch den Konnektor vor unautorisierten Zugriffen geschützt. Ohne zusätzliche Sicherungsmaßnahmen haben alle Komponenten im LAN Zugriff aufeinander (somit auch eine potenzielle Schadsoftware auf einem der Geräte). Außerdem besteht kein Schutz vor Angriffen aus dem Internet. Zudem müssen alle Netzwerkkomponenten bei dieser Betriebsart unterschiedlich konfiguriert werden.

Da der Konnektor nicht als Firewall im LAN fungiert, ist der Parallelbetrieb nur für medizinische Einrichtungen geeignet, die bereits ein größeres LAN etabliert haben und über entsprechende Sicherheitsfunktionen gemäß dem Bundesamt für Sicherheit in der Informationstechnik verfügen.



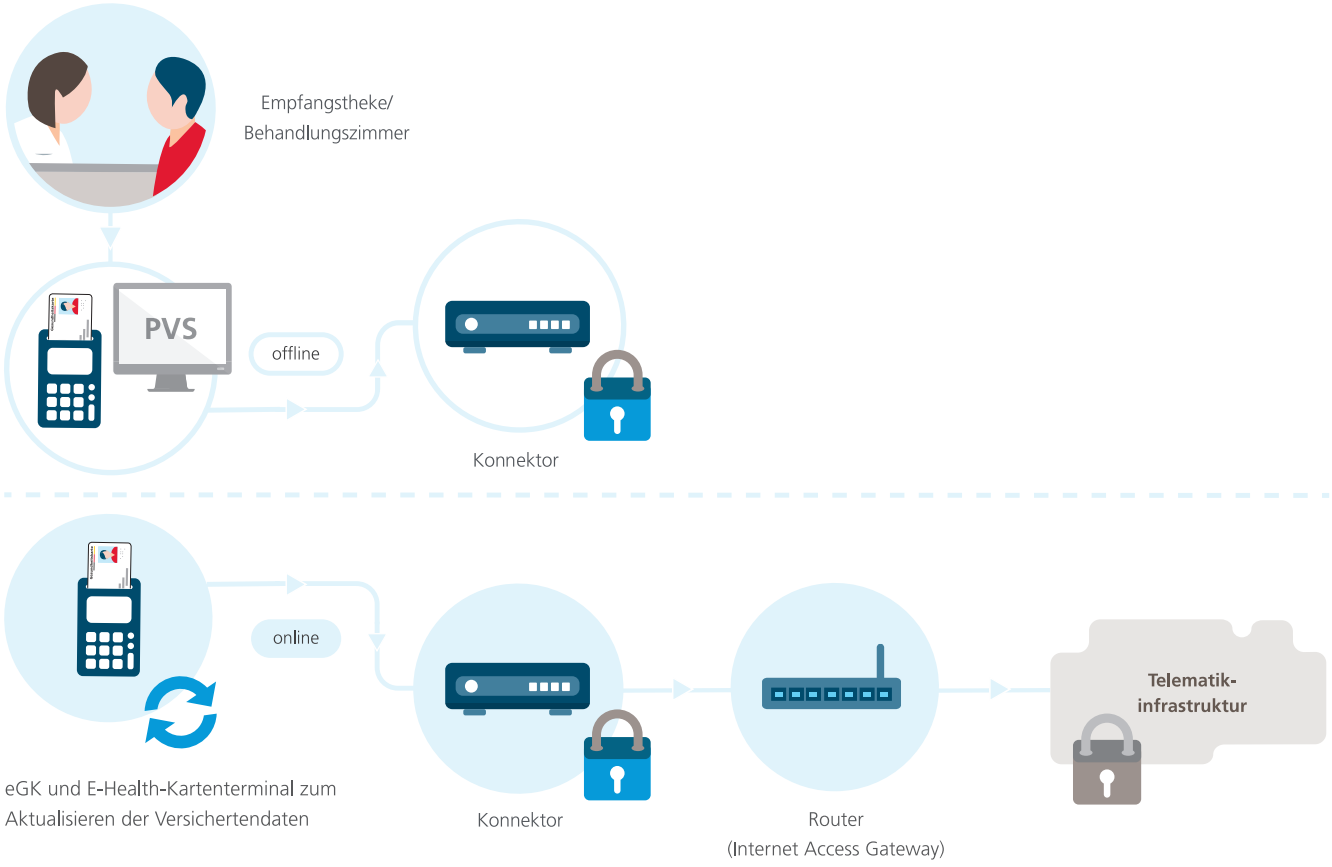
Ein Router ist die zentrale Komponente (Standard-Gateway) in einem Netzwerk (LAN), an die alle Datenpakete gesendet und von dort aus an den jeweiligen Empfänger weitergeleitet werden. Der Router kann ein Netzwerk auch mit einem anderen Netzwerk verbinden – zum Beispiel mit einem anderen LAN oder bei bestehender Verbindung (beispielsweise über ein DSL-Modem) auch mit dem Internet. Damit alle Geräte in einem Netzwerk erreichbar sind, bietet der Router die Funktion, diesen Geräten automatisch Adressen zuzuordnen. Ein Router hat zunächst keine Sicherheitsfunktionen, wird aber meist um eine solche (beispielsweise eine Firewall) ergänzt.

Überblick Betriebsarten Konnektor

	Reihenbetrieb	**Netztrennung**	**Parallelbetrieb**
Schutz durch Sicherheits-funktionen des Konnektors	ja	ja (nur LAN 1)	nein
Secure Internet Service	ja	ja (nur LAN 1)	ja
Nutzung von Internetdiens-ten außerhalb des Secure Internet Service	nein	ja (nur LAN 2)	ja
Einrichtungs- und Administrationsaufwand	mittel	mittel	niedrig
Empfehlung für	Praxis-IT-Umgebungen ohne Internetzugang bzw. bei ausschließlicher Nutzung des Secure Internet Service	Praxis-IT-Umgebungen, die auf zusätzliche Internet-dienste angewiesen sind	Praxis-IT-Umgebungen mit komplexen Netzwerken und eigenem Sicherheitssystem

2. Stand-alone-Szenario mit physischer Trennung

Beim Stand-alone-Szenario mit physischer Trennung erfolgt die Online-Prüfung der Versichertenstammdaten an einem separaten Kartenterminal und Konnektor mit Netzzugang, die in keiner Weise mit dem Praxis-IT-System verbunden sind. Damit ist es nicht einmal theoretisch möglich, dass sich Hacker über das Internet unerlaubten Zugang zu den Praxisrechnern verschaffen. Für dieses Szenario werden ein zweites Kartenterminal und ein zweiter Konnektor benötigt, um die Versichertendaten der elektronischen Gesundheitskarte auch mit dem Praxisverwaltungssystem einlesen zu können. Mit diesem zweiten Konnektor und Kartenterminal können dann auch die Notfalldaten angelegt, ausgelesen und aktu-alisiert werden. Außerdem erfordert der Einsatz eines zweiten Konnektors eine weitere SMC-B (Praxisausweis).



Praxisbeispiel:
Ein Patient kommt in diesem Quartal zum ersten Mal in die Praxis und gibt seine elektronische Gesundheitskarte am Empfang ab. Die Medizinische Fachangestellte steckt beim Stand-alone-Szenario mit physischer Trennung die elektronische Gesundheitskarte in das Kartenterminal mit Anbindung an die Telematikinfrastruktur zur Überprüfung und gegebenenfalls Aktualisierung der Versichertenstammdaten. Danach wird die Karte gezogen und in das Kartenterminal am Praxis-Computer gesteckt, damit die aktuellen Stammdaten in das Praxisverwaltungssystem eingelesen werden können.

Beim Stand-alone-Szenario können vom Praxisverwaltungssystem aus keinerlei Online-Funktionen (elektronische Befundübermittlung etc.) genutzt werden.

Weitere Informationsangebote: Das Informationsblatt »Technische Ausstattung einer medizinischen Einrichtung« und eine FAQ-Liste mit Fragen und Antworten finden Sie auf den Webseiten der gematik.

Wir vernetzen das Gesundheitswesen. Sicher.

Impressum

Herausgeber:
gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
Friedrichstraße 136
10117 Berlin

Redaktion:
gematik, Unternehmenskommunikation

Gestaltung:
DreiDreizehn GmbH, Berlin

Stand:
1. Oktober 2017

2017-10-IB-AME

Gender-Hinweis: Zugunsten des Leseflusses wird in dieser Publikation meist die männliche Form verwendet. Wir bitten, dies nicht als Zeichen einer geschlechtsspezifischen Wertung zu deuten.