

Telematik-Konnektor

Die Telematik-Infrastruktur (TI) nutzt zwar die vorhandenen Internet-Anschlüsse, ihre Teilnehmer befinden sich aber in einem eigenen privaten und abgesicherten Netz (virtuelles privates Netzwerk VPN). Den Zugang zu diesem eigenen Netz stellt der Telematik-Konnektor als sogenannter VPN-Router sicher. Er baut eine auf Netzebene gesicherte Verbindung (IPsec) zur zentralen TI-Plattform über das Internet auf. Sensible Daten, die über diese Verbindung transportiert werden, sind zusätzlich auf Transportebene geschützt (TLS).

In seiner Funktion als Firewall auf Netz- und Anwendungsebene schützt der Telematik-Konnektor sowohl die Systeme der Praxis vor Angriffen aus dem Internet und vor unberechtigten Zugriffen aus der zentralen TI-Plattform. Telematik-Konnektor und zentrale TI-Plattform können nicht auf die in der Arztsoftware gespeicherten Daten zugreifen, und Daten aus diesen Systemen werden nur auf Anforderung auf die eGK geschrieben oder an Dienste der TI übertragen. Außerdem enthält der Telematik-Konnektor einen Sicherheitschip, auf dem die privaten Schlüssel gespeichert sind, die für spätere Anwendungen wie die elektronischen Befundübermittlung benötigt werden. Diese müssen unbedingt vor Missbrauch geschützt werden, so dass der Telematik-Konnektor zwingend an einem Zutrittsgeschützten Ort (z.B. abschließbarer Serverschrank) platziert werden muss.

Viele Ärztinnen und Ärzte mißtrauen dem Anschluß an die TI, weil sie befürchten, dass über den Telematik-Konnektor ein Datenzugriff auf ihre Patientendaten erfolgen könnte. RED Medical bietet dagegen einen zusätzlichen Schutz: alle Daten werden außerhalb des physischen Zugriffs der TI in einem sicheren Rechenzentrum gespeichert und zusätzlich Ende-zu-Ende-verschlüsselt. Damit wird technisch sichergestellt, dass kein Unbefugter Zugriff auf die gespeicherten Daten hat (security by design).