Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

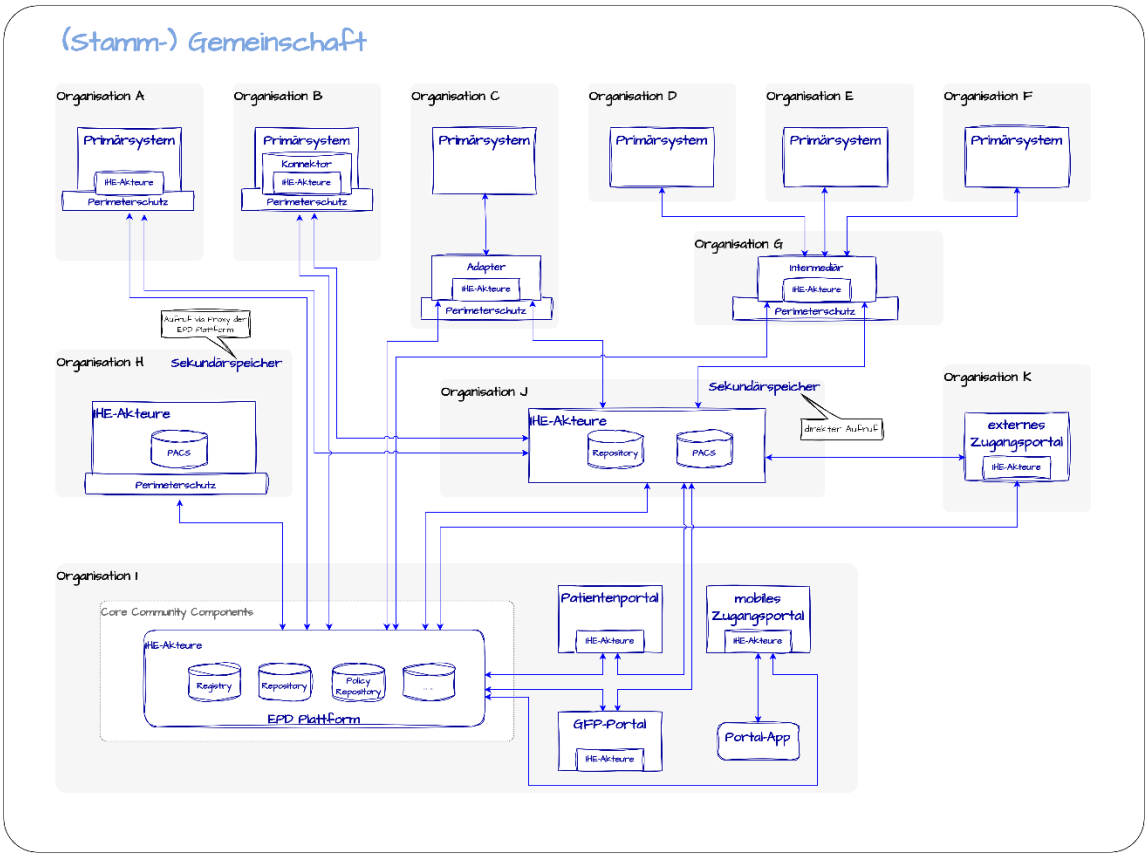
Bundesamt für Gesundheit BAG
Abteilung Digitale Transformation

Faktenblatt

Datum: 25.11.2024

Zertifizierung von externen Systemen im Kontext EPD

Die Akzeptanz und die Verbreitung des elektronischen Patientendossiers (EPD) in der Bevölkerung, bei den Gesundheitseinrichtungen (GE) und Gesundheitsfachpersonen (GFP) hängt wesentlich vom Nutzen und dem Vertrauen der Bevölkerung in die Sicherheit des EPD ab. Eine Anbindung mehrwertbietender externer Systeme an den EPD-Vertrauensraum1 ist deshalb grundsätzlich erwünscht, solange die Einhaltung von Datenschutz und Datensicherheit sowie die Interoperabilität beim EPD gewährleistet wird. Viele unterschiedliche technische Systeme greifen lesend und / oder schreibend auf das EPD zu und können in nachfolgender Systemlandschaft abgebildet werden:



[1] Als EPD-Vertrauensraum werden im Kontext dieses Faktenblattes die EPD-Plattform plus deren Schnittstellen zu externen Systemen verstanden. In anderen Kontexten werden unter dem EPD-Vertrauensraum die EPD-Plattform und alle an das EPD angebundenen Systeme verstanden. Dies ist hier explizit nicht gemeint.

Weitere Informationen:
Diese Publikation erscheint ebenfalls in französischer und italienischer Sprache.

Begriffserklärung

Adapter	Applikationen, welche Schnittstellen zur Protokollübersetzung von proprietären zu EPD konformen Schnittstellen bereitstellen und von Primärsystemen zur Anbindung an das EPD genutzt werden (1 zu 1 Verbindung zwischen Primärsystem und EPD).
EPD Plattform	alle Applikationen bzw. Applikationskomponenten, die von einer Gemeinschaft für den Betrieb des EPD benötigt werden.
Externes Zugangsportal	Applikationen, welche von Dritten betrieben werden und mit denen Patienten und Patientinnen auf das EPD lesend zugreifen können.
Intermediär	Applikationen, über welche eine beliebige Anzahl von Institutionen ihre Primärsysteme an das EPD für den lesenden und schreibenden Zugriff anbinden können (n zu 1 Verbindung zwischen Primärsysteme und EPD).
Konnektor	Software Bibliotheken und Komponenten, welche vorgefertigte Funktionen zum Zugriff auf das EPD bereitstellen und in die Produkte (Primärsystem, Adapter, Technischer Benutzer, etc.) integriert werden.
Mobiles Zugangsportal	Server-Teil einer Web-Applikation, welche von den (Stamm-)Gemeinschaften betrieben wird und einer Portal-App den Zugriff auf die EPD Plattform über EPD konforme Schnittstellen ermöglicht.
Perimeter-schutz	Im Kontext dieses Faktenblattes werden darunter folgende Sicherheitssysteme verstanden: Border Access Router (AR), Web-Application Firewall (WAF) mit Proxy-Services, Anti-Viren Schutzsysteme, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Demilitarisierte Zonen (DMZ).
Portal App	Mobiler Client der Web-Applikation, der mit dem mobilem Zugangsportal kommuniziert und dadurch den Zugriff auf die EPD-Plattform ermöglicht.
Primärsystem	System, das in einer Arztpraxis oder einem Spital zur Verwaltung von medizinischen Daten genutzt wird, wie z.B. ein Praxis- oder Klinikinformationssystem.
Sekundär-speicher	Applikationen, die von Institutionen betrieben werden und in denen Daten des EPD gespeichert sind.
Technischer Benutzer	Funktionalität in einem System, welche das automatische Hochladen von Dokumenten im EPD ermöglicht.
Zugangsportal	Applikationen, welche von den Gemeinschaften betrieben werden und mit denen die EPD Nutzer (z.B. Gesundheitsfachpersonen, Patienten und Patientinnen) auf das EPD lesend und schreibend zugreifen können.

Weitere Informationen:
Diese Publikation erscheint ebenfalls in französischer und italienischer Sprache.

Zertifizierungsgrenze

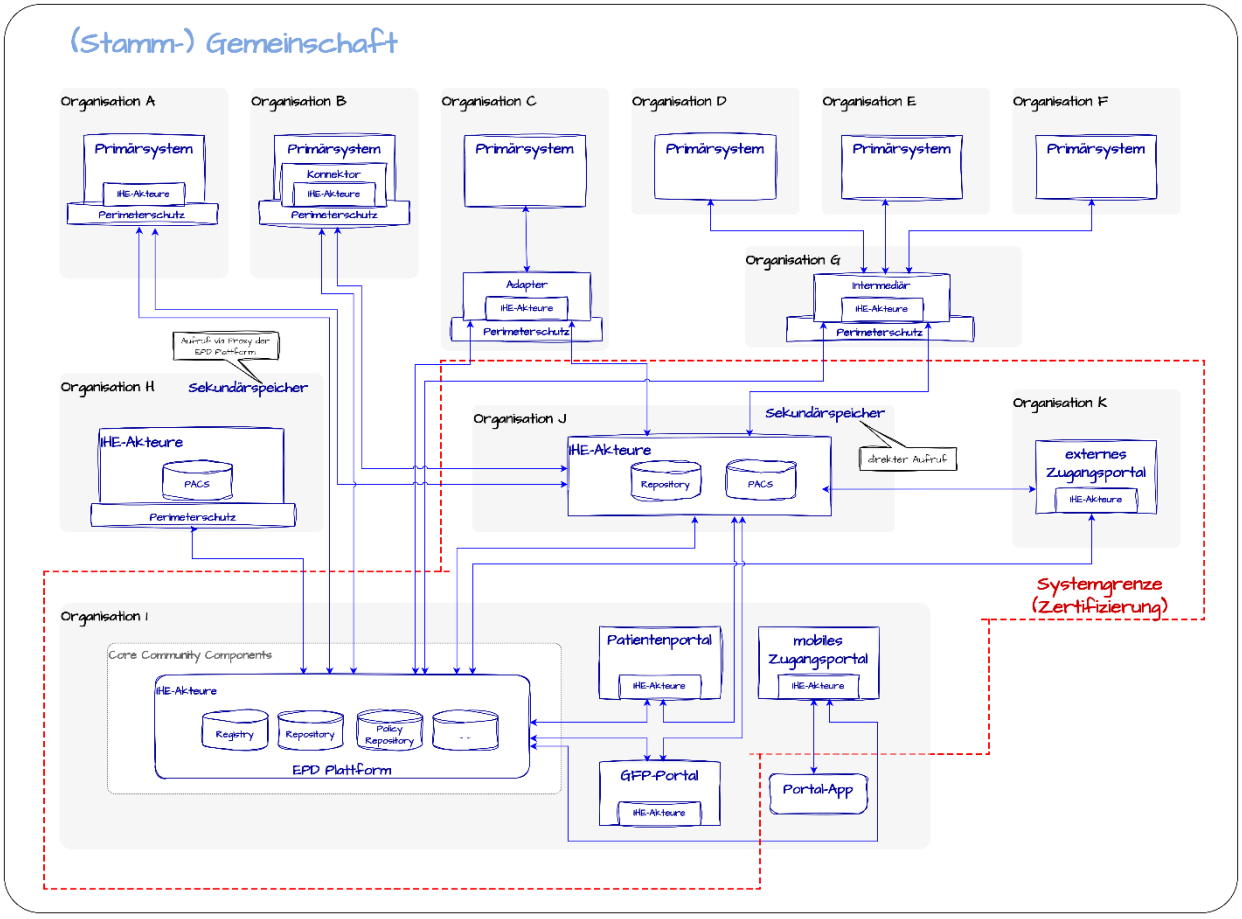
In Abwägung von Risiken und Nutzen der Anbindung externer Systeme an das EPD hat das BAG entschieden, dass die im Folgenden genannten Systeme bis auf Weiteres nicht der Zertifizierung gemäss EPDG unterliegen[2,3]:

- Primärsystem
- Konnektor
- Adapter
- Intermediär
- Sekundärspeicher ohne integriertem Zugriffsberechtigungssystem (indirekter Aufruf über Proxy der EPD-Plattform)
- Technischer Benutzer
- Portal-App

Folgende Systeme der Gemeinschaften und Stammgemeinschaften unterliegen demnach weiterhin der Zertifizierung:

- EPD-Plattformen
- Interne Zugangsportale
- Mobile Zugangsportale
- Sekundärspeicher mit integriertem Zugriffberechtigungssystem (direkter Aufruf)
- Externe Zugangsportale

Die Zertifizierungsgrenze sieht also wie auf der abgebildeten Graphik aus:



[2] Die Zertifizierungspflicht für bereits jetzt zertifizierungspflichtige Systeme gemäss Anhang 2 EPDV-EDI wird von dieser Entscheidung nicht berührt.

[3] Je nach technologischer Entwicklung kann es notwendig sein, weitere Systeme in Anhang 2 der EPDV-EDI aufzunehmen und damit der Zertifizierungspflicht zu unterstellen.

Weitere Informationen:
Diese Publikation erscheint ebenfalls in französischer und italienischer Sprache.

Bei der Risikobewertung geht das BAG von folgenden Prämissen aus:

- Der EPD-Vertrauensraum ist aufgrund der für ihn gesetzlich vorgeschriebenen Anforderungen an Datenschutz und Datensicherheit als sicher, nach dem aktuellen Stand der Technik zu betrachten.
- Der EPD-Inhaber gefährdet nur sein eigenes EPD, wenn er mit einer Portal-App auf sein EPD zugreift. Die Daten aus anderen EPD sind dadurch nicht gefährdet.
- Gesundheitseinrichtungen (GE) und Gesundheitsfachpersonen (GFP) sind verantwortlich für die Systeme, die sie nutzen. Die (Stamm-)Gemeinschaften machen den GE im Rahmen des Vertrags für die Anbindung an die (Stamm-)Gemeinschaft Vorgaben zu den erlaubten Systemen gemäss Anhang 2 EPDV-EDI. Drittanbieter, die Leistungen für die GE oder GFP erbringen, handeln immer im Auftrag einer GE oder GFP, wobei diese grundsätzlich für die Handlungen der Beauftragten verantwortlich sind.
- Alle beteiligten Anbieter der genannten Systeme handeln verantwortungsvoll und führen ein Datenschutz- und Datensicherheitsmanagement auf dem aktuellen Stand der Technik (z.B. ISO/IEC 27001)
- (Stamm-)Gemeinschaften verpflichten ihre angeschlossenen Gesundheitseinrichtungen die Anforderungen an Datenschutz und Datensicherheit der EPDV-EDI auf alle zur Anbindung ans EPD genutzten Systeme wie Adapter, Intermediär oder technischer Benutzer
- Bei Aspekten, die nicht im EPDG geregelt sind, greifen andere Regelungen wie Datenschutzvorgaben (eidgenössische und kantonale), MepV und auch arbeitsrechtliche Vorgaben.

Weitere Informationen:
Diese Publikation erscheint ebenfalls in französischer und italienischer Sprache.