KASSENÄRZTLICHE BUNDESVEREINIGUNG

SPEZIFIKATION 116117 TERMINSERVICE AUTHENTISIERUNG

Kassenärztliche Bundesvereinigung

Herbert-Lewin-Platz 2

10623 Berlin

www.kbv.de

Inhalt

Änderungshistorie:

VERSION	DATUM	AUTOR	KAPITEL	ÄNDERUNG	STATUS
1.0	06.12.2024	kv.digital	alle	redaktionelle Änderungen nach Kommentierung	in Kraft
			3	Ergänzung Voraussetzungen um Praxisausweis (SMC-B oder SMB) und TI-Gateway	
			4	Ergänzung Use Cases um Praxisausweis (SMC-B oder SMB) und TI-Gateway	
0.1	14.10.2024	kv.digital	alle	Initiale Erstellung	Entwurf

1 EINLEITUNG

Dieses Dokument spezifiziert das Authentisierungsverfahren für externe Systeme zur Nutzung von Diensten des 116117 Terminservice.

2 GRUNDSÄTZLICHES

Das in dieser Spezifikation beschriebene Authentisierungsverfahren orientiert sich am Verfahren für die Anmeldung von Primärsystemen von Leistungserbringern am E-Rezept-Fachdienst. Dieses Verfahren ist durch die gematik u.a. im Dokument "Spezifikation Implementierungsleitfaden Primärsysteme - E-Rezept" beschrieben.

Der 116117 Terminservice nimmt dabei die Rolle eines Fachdienstes analog zum E-Rezept-Fachdienst ein.

Der in der [gemILF_PS_eRp] beschriebene Identity Provider (Zentraler IDP, vormals Smartcard IDP) wird durch einen eigenen Identity Provider der kv.digital GmbH ersetzt.

Es werden in dem hier beschriebenen Authentisierungsverfahren Praxen anhand der telematikID sowie domainID und keine Personen authentisiert.

3 VORAUSSETZUNG

Praxen müssen folgende Voraussetzungen für die Nutzung des Authentisierungsverfahrens erfüllen:

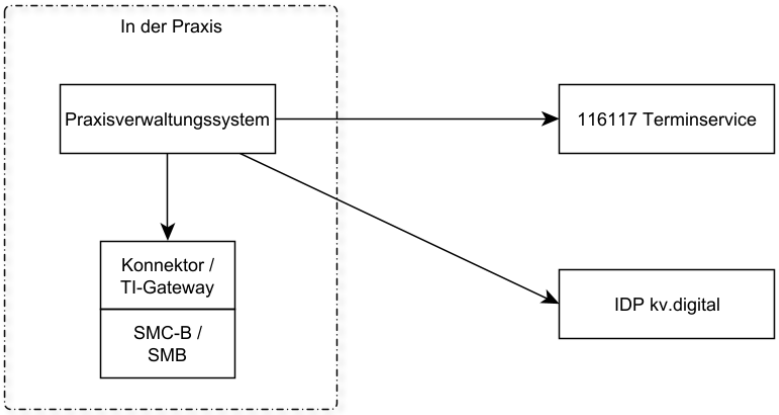
- die Praxis benötigt einen Zugang zur Telematikinfrastruktur (TI),
- die Praxis benötigt einen gültigen Praxisausweis (SMC-B oder SMB),
- der Praxisausweis muss im Verzeichnisdienst der TI mit telematikID beginnend mit "1-20" und ihre BSNR als domainID hinterlegt sein,
- die Praxis muss Zugriff auf ihren Konnektor oder ihr TI-Gateway haben und
- die Praxis muss Zugriff auf das Schlüsselmaterial und die Zertifikate des Praxisausweises über ihren Konnektor bzw. TI-Gateway haben.

4 USE CASES

Für die Authentisierung und Nutzung des 116117 Terminservice werden grundsätzlich 2 Use Cases unterstützt.

4.1 PRAXISVERWALTUNGSSYSTEM (PRIMÄRSYSTEM)

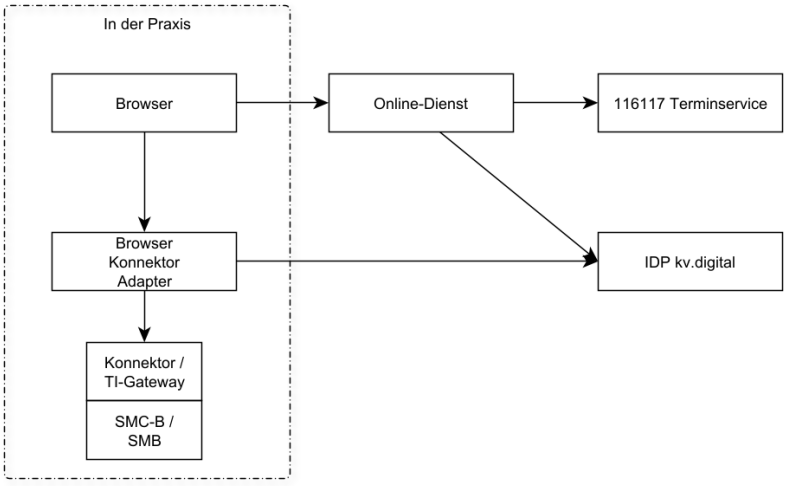
Das erste Use Case ist, dass in einer Praxis ein Praxisverwaltungssystem (Primärsystem) installiert ist und direkten Zugriff auf den Konnektor oder das TI-Gateway und damit auch auf den Praxisausweis (SMC-B oder SMB) hat. Das Praxisverwaltungssystem kommuniziert direkt mit dem 116117 Terminservice.



1 Use Case Praxisverwaltungssystem

4.2 ONLINE-DIENST

Im zweiten Use Case nutzen Praxismitarbeitende einen Online-Dienst über einen Browser. Der Online-Dienst hat keinen direkten Zugriff auf den Konnektor oder das TI-Gateway der Praxis und damit auch keinen direkten Zugriff auf den Praxisausweis (SMC-B oder SMB). Der Online-Dienst kann im "Namen der Praxis" direkt mit dem 116117 Terminservice kommunizieren.



2 Use Case Online-Dienst

5 ANFORDERUNGEN

5.1 GRUNDLAGE

Die Grundlage für die Spezifikation des hier beschriebenen Authentisierungsverfahrens sind das Kapitel "5.1 Allgemein" und seine Unterkapitel in [gemILF_PS_eRp]. Alle nachfolgenden Angaben beziehen sich auf die Version 1.10.0.

5.2 ÜBERGREIFENDE FESTLEGUNG

Es gelten alle Anforderungen aus "Kapitel 5.1 Allgemein" und seinen Unterkapiteln, sofern nachfolgend keine Änderungen oder Ergänzungen dokumentiert sind.

5.3 ÄNDERUNGEN

In allen Anforderungen wird "E-Rezept" durch "116117 Terminservice" ersetzt.

SPEZIFIKATION SKAPITEL	ANFORDERUNG	ÄNDERUNGEN
5.1.1 Kommunikation zu den Diensten der TI		Text ausgetauscht mit: "Praxisverwaltungssysteme (Primärsysteme) nutzen TLS-Verbindungen für die Kommunikation zum 116117 Terminservice Fachdienst und dem Identity Provider."
	A_19451-01 - PS: Lokalisierung E-Rezept-Fachdienst	Text ausgetauscht mit: "Hersteller von Praxisverwaltungssystemen (Primärsystemen) oder Online-Diensten entnehmen die URLs zu Fachdiensten des 116117 Terminservice den spezifischen Anwendungsdokumentationen."
	A_19744 - PS: Endpunkt Schnittstelle E-Rezept	Anforderung entfällt und muss nicht umgesetzt werden.
	A_19234 - PS: Kommunikation über TLS-Verbindung	Text ausgetauscht mit: "Das Primärsystem MUSS mit dem 116117 Terminservice Fachdienst ausschließlich über TLS kommunizieren."
	A_19235 - PS: Unzulässige TLS-Verbindungen ablehnen	Text ausgetauscht mit: "Das Primärsystem MUSS bei jedem Verbindungsaufbau den Dienst der kv.digital GmbH anhand seines TLS-Zertifikats authentifizieren und MUSS die Verbindungen ablehnen, falls die Authentifizierung fehlschlägt."

SPEZIFIKATION SKAPITEL	ANFORDERUNG	ÄNDERUNGEN
	A_21568 - PS: HTTP-Header X-erp-user	Anforderung entfällt und muss nicht umgesetzt werden.
	A_21569 - PS: HTTP-Header X-erp-resource	Anforderung entfällt und muss nicht umgesetzt werden.
5.1.2 Verschlüsselte Kommunikation zur VAU des E-Rezept Fachdienstes		
	A_19741 - PS: Umsetzung sicherer Kanal zur VAU des E-Rezept-Fachdienstes	Anforderung entfällt und muss nicht umgesetzt werden.

<table>
<tr><th>SPEZIFIKATION SKAPITEL</th><th>ANFORDERUNG</th><th>ÄNDERUNGEN</th></tr>
<tr><td>5.1.3 Zertifikatsprüfung</td><td></td><td>Text geändert
von:
<table>
<tr><th>AKTIVITÄT</th><th>ZERTIFIKAT DER TI</th><th>ZERTIFIKATSTYP</th><th>ROLLEN-OID</th><th>NUTZUNG</th></tr>
<tr><td>TLS-Verbindungsaufbau zum E-Rezept-Fachdienst</td><td>nein</td><td>TLS Internet Zertifikat</td><td>n/a</td><td>aktiv</td></tr>
<tr><td>TLS-Verbindungsaufbau zum Verzeichnisdienst der TI</td><td>nein</td><td>TLS Internet Zertifikat</td><td>n/a</td><td>aktiv</td></tr>
<tr><td>TLS-Verbindungsaufbau zum IDP</td><td>nein</td><td>TLS Internet Zertifikat</td><td>n/a</td><td>aktiv</td></tr>
<tr><td>Aufbau sicherer Kanal zur VAU des E-Rezept-Fachdienstes</td><td>ja</td><td>C.FD.ENC</td><td>oid_erp-vau</td><td>aktiv</td></tr>
<tr><td>Nur für PS der abgebenden LEI: Signaturzertifikat Fachdienst</td><td>ja</td><td>C.FD.SIG</td><td>oid_erezept</td><td>aktiv</td></tr>
</table>
zu:
<table>
<tr><th>AKTIVITÄT</th><th>ZERTIFIKAT DER TI</th><th>ZERTIFIKATSTYP</th><th>ROLLEN-OID</th><th>NUTZUNG</th></tr>
<tr><td>TLS-Verbindungsaufbau zum 116117 Terminservice Dienst</td><td>nein</td><td>TLS Internet Zertifikat</td><td>n/a</td><td>aktiv</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>SPEZIFIKATION SKAPITEL</th><th>ANFORDERUNG</th><th>ÄNDERUNGEN</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>AKTIVITÄT</th><th>ZERTIFIKAT DER TI</th><th>ZERTIFIKAT STYP</th><th>ROLLEN-OID</th><th>NUTZUNG</th></tr>
<tr><td>TLS-Verbindungsaufbau zum Verzeichnisdienst der TI</td><td>nein</td><td>TLS Internet Zertifikat</td><td>n/a</td><td>aktiv</td></tr>
<tr><td>TLS-Verbindungsaufbau zum IDP der kv.digital</td><td>nein</td><td>TLS Internet Zertifikat</td><td>n/a</td><td>aktiv</td></tr>
<tr><td>~~Aufbau sicherer Kanal zur VAU des E-Rezept-Fachdienstes~~</td><td>~~ja~~</td><td>~~C.FD.ENC~~</td><td>~~oid_erp-vau~~</td><td>~~aktiv~~</td></tr>
<tr><td>~~Nur für PS der abgebenden LEI: Signaturzertifikat Fachdienst~~</td><td>~~ja~~</td><td>~~C.FD.SIG~~</td><td>~~oid_erezept~~</td><td>~~aktiv~~</td></tr>
</table>
</td></tr>
<tr><td>5.1.3.1 Zertifikatsprüfung von Zertifikaten der TI</td><td></td><td></td></tr>
<tr><td></td><td>A_20764 - PS: Prüfung TI-Zertifikate</td><td>Anforderung entfällt und muss nicht umgesetzt werden.</td></tr>
<tr><td>5.1.4 Authentifizierung der LEI</td><td></td><td>Text geändert
von:
"Hierfür wird am Authorization-Endpunkt des IDP-Dienstes ein "AUTHORIZATION_CODE" beantragt, der nach erfolgreicher Verifikation am Token-Endpunkt des IDP-Dienstes gegen ein "ID_TOKEN" und ein "ACCESS_TOKEN" getauscht wird."
zu:
"Hierfür wird am Authorization-Endpunkt des IDP-Dienstes ein "AUTHORIZATION_CODE" beantragt, der nach erfolgreicher Verifikation am Token-Endpunkt des IDP-Dienstes gegen ~~ein "ID_TOKEN" und~~ ein "ACCESS_TOKEN" getauscht wird."</td></tr>
</table>

SPEZIFIKATION SKAPITEL	ANFORDERUNG	ÄNDERUNGEN
5.1.4.1 Übergreifende Festlegungen zur Nutzung des IDP-Dienstes		
	A_20654 - Registrierung des Primärsystems	Anforderung entfällt und muss nicht umgesetzt werden.
	A_20655 - Regelmäßiges Einlesen des Discovery Document	Text geändert von: "Der Downloadpunkt wird als Teil der organisatorischen Registrierung des Primärsystems beim IDP-Dienst übergeben." zu: "Der Downloadpunkt wird von der kv.digital GmbH veröffentlicht."
	A_20656-01 - Prüfung der Signatur des Discovery Document	Anforderung entfällt und muss nicht umgesetzt werden.
	A_20657 - Prüfung der Signatur des Discovery Document	Anforderung entfällt und muss nicht umgesetzt werden.
	A_20658 - Sicheres Löschen der Token	Text geändert von: "Das Primärsystem MUSS, wenn es absichtlich gestoppt oder deaktiviert wird, vorhandene "ACCESS_TOKEN", "ID_TOKEN" und "AUTHORIZATION_CODE"-Objekte sicher aus dem RAM löschen." zu: "Das Primärsystem MUSS, wenn es absichtlich gestoppt oder deaktiviert wird, vorhandene "ACCESS_TOKEN"~~, "ID_TOKEN"~~ und "AUTHORIZATION_CODE"-Objekte sicher aus dem RAM löschen."

SPEZIFIKATION SKAPITEL	ANFORDERUNG	ÄNDERUNGEN
	A_21337 - Löschung von TOKEN bei zeitlichem Ablauf	Text geändert von: "Das Primärsystem MUSS vorhandene "ACCESS_TOKEN", "ID_TOKEN" und "AUTHORIZATION_CODE"-Objekte nach Ablauf ihrer Gültigkeit sicher löschen." zu: "Das Primärsystem MUSS vorhandene "ACCESS_TOKEN"~~, "ID_TOKEN"~~ und "AUTHORIZATION_CODE"-Objekte nach Ablauf ihrer Gültigkeit sicher löschen."
	A_21338 - Sichere Speicherung der Token	Text geändert von: "Das Primärsystem MUSS empfangene "ACCESS_TOKEN", "ID_TOKEN" und "AUTHORIZATION_CODE"-Objekte gegen unberechtigten Zugriff schützen." zu: "Das Primärsystem MUSS empfangene "ACCESS_TOKEN"~~, "ID_TOKEN"~~ und "AUTHORIZATION_CODE"-Objekte gegen unberechtigten Zugriff schützen."
5.1.4.2 Abruf von Token beim IDP-Dienst		
	A_20671-01 - Einreichen des AUTHORIZATION_CODE beim Token-Endpunkt	Text geändert von: 'Das Primärsystem erhält nun den signierten "ID_TOKEN" und den "ACCESS_TOKEN" vom Token-Endpunkt und prüft die Signatur des "ID_TOKEN".' zu: 'Das Primärsystem erhält nun ~~den signierten "ID_TOKEN" und~~ den "ACCESS_TOKEN" vom Token-Endpunkt~~ und prüft die Signatur des "ID_TOKEN"~~.'
	A_20672-01 - Annahme des ID_TOKEN	Anforderung entfällt und muss nicht umgesetzt werden.
	A_20674 - Formale Prüfung der Signatur des ID_TOKEN	Anforderung entfällt und muss nicht umgesetzt werden.
	A_20675 - Gültigkeitsprüfung der Signatur des ID_TOKEN innerhalb der TI	Anforderung entfällt und muss nicht umgesetzt werden.

6 REFERENZEN

- [gemILF_PS_eRp]: Spezifikation Implementierungsleitfaden Primärsysteme - E-Rezept,
  - aktuelle Version: https://gemspec.gematik.de/docs/gemILF/gemILF_PS_eRp/latest/
  - Version 1.10.0: https://gemspec.gematik.de/docs/gemILF/gemILF_PS_eRp/gemILF_PS_eRp_V1.10.0/
  - Kapitel 5.1 in Version 1.10.0: https://gemspec.gematik.de/docs/gemILF/gemILF_PS_eRp/gemILF_PS_eRp_V1.10.0/#5.1