DIGITALES GESUNDHEITSWESEN

KURZÜBERSICHT AUTHENTICATOR

WAS ist der Authenticator?

Generell:

- **Software**
- wird von der **gematik GmbH kostenlos** zur Verfügung gestellt

Funktion:

- **Sichere Authentisierung mittels SMC-B bzw. eHBA an digitalen** Gesundheits-Anwendungen
- Bindeglied zwischen den Komponenten der Telematikinfrastruktur (TI) und **webbasierten Anwendungen**, bei denen eine kartenbasierte Authentifizierung der Anwender notwendig ist

Zielgruppe:

- Alle Organisationen bzw. Leistungserbringer mit SMC-B bzw. eHBA
- die **Zugriff auf digitale Gesundheitsanwendungen** erhalten möchten
- bei denen eine **Authentifizierung über die Telematikinfrastruktur** gegeben ist

FÜR WELCHE ANWENDUNGEN benötige ich den Authenticator?

Erste Anwendung (seit 1.1.2023):

- **Zentrales Vorsorgeregister der Bundesnotarkammer (ZVR)** für Ärzte und Ärztinnen
- Feststellung, ob
  - Vorsorgevollmachten,
  - Betreuungsverfügungen,
  - Patientenverfügungen oder
  - Widersprüche gegen das Ehegattennotvertretungsrecht

  für einen Patienten im ZVR registriert sind (wenn medizinisch erforderlich)
- Alle Organisationen bzw. Leistungserbringer, die den Zugriff auf das ZVR über die Telematikinfrastruktur nutzen möchten, benötigen den Authenticator als technisches Bindeglied für die Authentifizierung
- Inhalte der Dokumente können nach erfolgreicher Authentifizierung online eingesehen werden

Weitere Anwendungen, bei denen die Nutzung des Authenticators geplant ist:

- **WANDA** (= Weitere Anwendungen für den Datenaustausch)
- **TIM** (TI-Messenger)
- **DEMIS** (Deutsches Elektronisches Melde- und Informationssystem)

WAS brauche ich für den Authenticator?

Voraussetzung für die Nutzung des Authenticators ist ein Anschluss an die Telematikinfrastruktur (TI)

Technische Voraussetzungen:

- **Betriebssystem**: Authenticator ist aktuell unter Windows lauffähig, später auch für MAC OS und Linux geplant
- **TI-Anschluss** sowie eine SMC-B oder ein eHBA inkl. Karten-PIN (es hängt dabei von der Anwendung ab, welche Karte benötigt wird)

Inbetriebnahme:

- Download des Authenticators
- Authenticator wird **lokal betrieben**, d.h. Installation und Administration durch den Leistungserbringer bzw. die Institution
- **Konfiguration** der Konnektor-Einstellungen sowie des IP-Routings und ggf. der Firewall-Freischaltung

WIE nutze ich den Authenticator?

Nutzung:

- lokal über den Desktop
- Aufruf aus einer Web-Anwendung heraus (z.B. ZVR)
- **Achtung: Wenn man eine Anwendung nutzen möchte, die den Authenticator benötigt, muss dieser vorher installiert werden**

Ablauf:

- **Aufruf** der Web-Anwendung durch den Anwender
- **Anmeldung** in der Web-Anwendung
- Authenticator startet **Prüfung der Identität** des Anwenders automatisch
- Anwendung entscheidet, ob für die Identitätsprüfung **die SMC-B oder der eHBA** benötigt wird
- Authenticator prüft automatisch, ob die entsprechende **Karte** gesteckt ist - falls nicht, wird der Anwender aufgefordert, sie zu stecken
- **PIN-Eingabe** durch Anwender
- Nach erfolgreicher Überprüfung kann die Anwendung genutzt werden

Weitere Informationen

Allgemeiner Überblick und Link zum Download:
https://fachportal.gematik.de/hersteller-anbieter/komponenten-dienste/authenticator

Detaillierte Informationen, Handbuch und FAQ:
https://wiki.gematik.de/display/GAKB/Authenticator+Wissensdatenbank