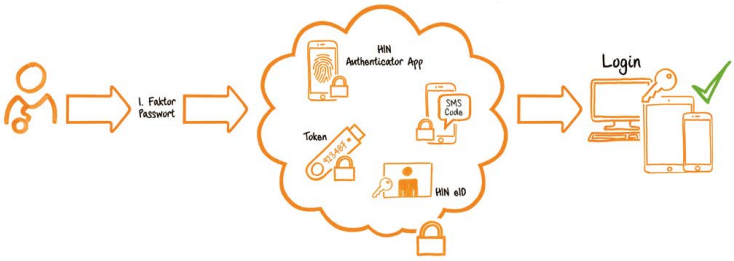
HIN Zwei-Faktor-Authentisierung

Bei der Zwei-Faktor-Authentisierung wird die Identität eines Nutzers beim Zugriff auf einen Online-Dienst mittels zwei unabhängiger Faktoren nachgewiesen, was die Sicherheit erhöht. Zwei-Faktor-Authentisierung ist Standard im Gesundheitswesen – und bei HIN. Für den zweiten Faktor neben Ihrem HIN Login stehen Ihnen drei Möglichkeiten zur Verfügung.



SMS-Code an Ihr Mobiltelefon
Sie registrieren Ihre Mobiltelefon-Nummer einmalig im HIN Kundencenter (servicecenter.hin.ch). Beim Zugriff auf die HIN Plattform wird als zweiter Faktor neben Ihrem HIN Passwort jeweils ein SMS-Code (mTAN) an Ihr Mobiltelefon gesendet. Mittels dieser Variante der Zwei-Faktor-Authentisierung können Sie auch auf das elektronische Patientendossier (EPD) zugreifen.

HIN Authenticator App
Bei Nutzung der HIN Authenticator App erfolgt die Zwei-Faktor-Authentisierung mit Ihrem HIN Passwort und der App. Für die Anmeldung in der App können Sie zwischen einem PIN-Code oder Finger-Scan wählen. Danach kann das Login wahlweise mithilfe eines Bestätigungs-Buttons innerhalb der App oder durch das Generieren eines One-Time-Passwortes erfolgen. Die App ist kostenlos für Android sowie iOS-Geräte verfügbar.

HIN Hardware Token
Der HIN Hardware Token ist ein kleines Gerät, das laufend One-Time-Passwörter generiert. Diese können Sie beim Zugriff auf die HIN Plattform als zweiten Faktor neben Ihrem persönlichen Passwort nutzen. Der Hardware Token ermöglicht die Zwei-Faktor-Authentisierung, ohne dass ein Mobiltelefon benötigt wird. Da er EPD-zertifiziert ist, können Sie ihn als zweiten Faktor beim Zugriff auf das elektronische Patientendossier (EPD) nutzen.

Möchten Sie HIN Hardware Token für Ihre Institution bestellen?
Kontaktieren Sie den HIN Experten Ihrer Region: www.hin.ch/anfrage

Erfahren Sie mehr

- über die HIN Authenticator App und den HIN Hardware Token: www.hin.ch/services/hin-2fa
- über die Zwei-Faktor-Authentisierung: www.hin.ch/zwei-faktor