authega®

Übersicht zu Registrierungs-/Loginarten

1 Allgemeine Informationen

Bei authega® handelt es sich um eine IT-Sicherheitsplattform, die den Zugriff auf die Dienste des Mitarbeiterservice Bayern ermöglicht.

Bei einer Registrierung mit authega® kann zwischen verschiedenen Arten des Logins mit unterschiedlichen Vor- und Nachteilen gewählt werden (siehe Abbildung 1).

	authegaLight	**authega**Basis	**authega**Spezial	**authega**Plus
	Benutzername + Passwort	Persönliches Zertifikat auf Ihrem **Computer**	Persönliches Zertifikat auf Ihrem **Sicherheitsstick**	Persönliches Zertifikat von Ihrer **Signaturkarte**
Sicherheit	niedrig	hoch	**sehr hoch**	**sehr hoch**
Kosten	**keine**	**keine**	41 Euro	50 bis 150 Euro*
Bedienung	**einfach**	**einfach**	**einfach**	komplex
Bewertung	✪	✪ ✪	✪ ✪	✪

Ein-Faktor-Authentifizierung (Wissen)

Zwei-Faktor-Authentifizierung (Besitz und Wissen)

Abbildung 1: Registrierungs-/Loginarten bei authega®

Um die Identität eines Benutzers zu gewährleisten, ist im Rahmen des regulären Registrierungsprozesses die Personalnummer und das Geburtsdatum anzugeben. Ist die Kombination korrekt, wird eine E-Mail an die angegebene E-Mail-Adresse und ein Brief mit einem Registrier-Geheimnis (dem sog. Aktivierungscode) an die im Personalsystem hinterlegte Postadresse verschickt.

Nach der Zwei-Wege-Registrierung und Anmeldung über authega® stehen verschiedenste Fachverfahren zur Verfügung (abhängig von den im Autorisierungsmanagement hinterlegten Rechten).

2 authegaLight

authegaLight kommt nur in besonderen Einzelverfahren nach gesonderter datenschutzrechtlicher Prüfung zum Einsatz. Bei **authega**Light erfolgt die Anmeldung mit Benutzername und Passwort (Ein-Faktor-Authentifizierung). Mit **authega**Light wird ein performantes und bedienungsfreundliches Anmeldeverfahren angeboten. Dennoch genügt auch hier der Registrierungsprozess im Vergleich zu anderen bekannten Diensten mit Benutzername und Passwort höheren Datenschutzanforderungen, da im Rahmen der vollständigen Registrierung ein Registrier-Geheimnis an die E-Mail-Adresse und ein zweites Registrier-Geheimnis an die Postadresse des Nutzers gesandt wird. Die Möglichkeiten zum Identitätsdiebstahl sind hierdurch deutlich eingeschränkt. Der Registrierprozess kann nur durch korrekte Eingabe des an die Postadresse übermittelten Registrier-Geheimnisses erfolgreich abgeschlossen werden.

3 authegaBasis

Bei **authega**Basis handelt es sich um eine Zwei-Faktor-Authentifizierung, d.h. zur Anmeldung wird sowohl ein Faktor Besitz (Software-Zertifikat), als auch ein Faktor Wissen (Passwort) benötigt. Damit erfüllt **authega**Basis eine deutlich höhere Sicherheit als **authega**Light.

Es existieren zwei unterschiedliche **authega**Basis Versionen (mit JavaScript oder mit Java-Applet) mit jeweils unterschiedlichen Vorteilen. Die Vorteile der JavaScript-Variante liegen in der einfachen Bedienbarkeit, barrierefreien Ausrichtung und schnellen Reaktionszeit. Die Java-Applet-Variante kann hingegen bei Behörden eingesetzt werden, die noch den Internet Explorer 9 im Einsatz haben.

3.1 authegaBasis (mit JavaScript)

Bei **authega**Basis wird ein Software-Zertifikat im lokalen Speicher des Browsers bzw. als Datei auf dem Computer gespeichert. Da das Software-Zertifikat bei neueren Browsern direkt im Browser gespeichert wird, handelt es sich hierbei um eine performante, bedienungsfreundliche und in hohem Maße barrierefreie Anmeldung. Voraussetzung für **authega**Basis mit JavaScript ist ein aktueller Browser (bedienungsfreundliche Nutzung erst ab Internet Explorer 10) und aktiviertes JavaScript.

3.2 authegaBasis (mit Java-Applet)

Bei **authega**Basis mit Java-Applet wird ebenfalls ein Software-Zertifikat als Datei auf dem Computer gespeichert (vgl. 3.1). **authega**Basis mit Java-Applet ist weniger performant als **authega**Basis mit JavaScript, bietet jedoch den Vorteil auch bei älteren Browserversionen nutzbar zu sein. Voraussetzung ist eine aktuelle Java Runtime Umgebung. Ein Nachteil liegt in dem niedrigeren Grad der realisierbaren Barrierefreiheit begründet.

4 authegaSpezial

Bei **authega**Spezial handelt es sich um ein Anmeldeverfahren, bei dem das Zertifikat auf einem **speziellen USB-Sicherheitsstick** gespeichert wird. Durch die Nutzung dieses Sicherheitssticks wird eine weitere Erhöhung der Sicherheit im Vergleich zu **authega**Basis insbesondere dadurch geboten, dass die beliebige Vervielfältigung des Zertifikates durch Kopieren und Einfügen nicht möglich ist. Der Sicherheitsstick muss durch den Benutzer/die Benutzerin beschafft werden.

5 authegaPlus

authegaPlus nutzt als Faktor ein - analog zu **authega**Spezial - auf einem physischen Träger (z.B. Smartcard) gespeichertes Zertifikat. Hierbei wird in authega® das auf der jeweiligen Smartcard (vergleichbar einer Bankkarte) befindliche Fremdzertifikat (z. B. der bayerischen Verwaltungs-PKI) hinterlegt. Es ist zu beachten, dass sämtliche im Fremdzertifikat enthaltenen Informationen, also insbesondere auch personenbezogene Daten, durch authega® gespeichert werden. Über diesen Umstand wird im Rahmen der *datenschutzrechtlichen Hinweise*[1] bei der Registrierung aufgeklärt.

[1] Vgl. https://www.authega.bayern.de/authega/declarationOfConsent.auth.