

Hochsicher Authentisieren. Passwortlos.

Die Lösung für Anmeldungen, Transaktionen
und Signaturen



Schutz für Digitale Identitäten

Onlinediensten mit hohen Anforderungen an Sicherheit und Datenschutz bietet die bisher übliche Authentifizierung mit Benutzername und Passwort keinen ausreichenden Schutz mehr. secunet protect4use schützt digitale Identitäten vor zunehmenden Bedrohungen im Internet und ermöglicht es die stark gestiegenen gesetzlichen Auflagen einzuhalten.

Sicher und komfortabel

Ob bei Webdiensten, Portalen, Plattformen oder Sicherheitsdomänen – überall kommen elektronische Identitäten zum Einsatz, die geschützt werden müssen.

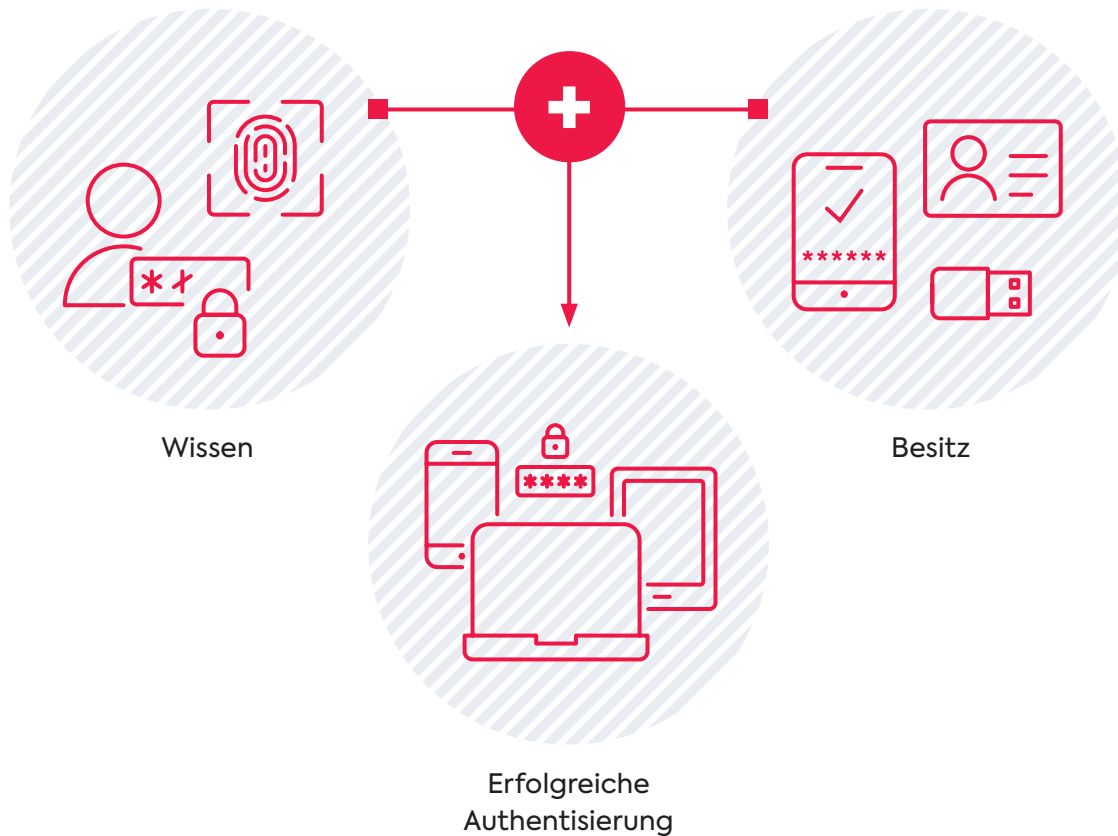
Je nach Anwendungsbereich sind dafür unterschiedliche Sicherheitsniveaus notwendig. Eine 2-Faktor-Authentisierung wird immer wichtiger, denn die übliche Anmeldung mit Benutzername und Passwort reicht aufgrund der Anfälligkeit für Angriffe nicht mehr aus.

Zusätzlich stellen vielfältige gesetzliche Bestimmungen Nutzer*innen tagtäglich vor neue Herausforderungen: Unbekannte Verfahren, verwirrende Login-Passwörter, vielfältige Authentifizierungsprozesse, um dem Sicherheitsbedarf gerecht zu werden. Die Mischung aus Hardware, Software, Passwörtern, PINs und Biometrie-Verfahren, ist für Nutzer*innen aufwändig und findet daher kaum Akzeptanz.

secunet protect4use geht einen neuen Weg:

Die Lösung bietet für Nutzer*innen eine einfache aber sichere Methode zum Authentisieren ihrer Anmeldungen, Transaktionen und Signaturen.

Das Authentifizierungsverfahren ist durch starke Kryptografie implementiert und verschiedene Sicherheitsniveaus können flexibel abgedeckt werden. Daten der Nutzer*innen bleiben vollständig beim Betreiber oder dessen Dienstleister. Die Lösung bietet eine breite Unterstützung der gängigen Plattformen und Browser für Desktop- und Mobilgeräte inklusive der jeweiligen Möglichkeiten der Barrierefreiheit.



State-of-the-art Technologie

Die Authentisierung mit secunet protect4use bietet Nutzer*innen mehrere Möglichkeiten, um sich anzumelden: Entweder mobil mit einem zweiten Endgerät, wie Smartphone oder Tablet, oder via patentierter Desktop-Applikation.

Wird das Smartphone als Token benutzt, so verwendet secunet protect4use den gängigen Zugriffsschutz der Nutzer*innen: Entsperrung durch Fingerabdruck, Gesichtserkennung oder PIN.

Die Lösung kann mit allen gängigen Browsern genutzt werden und ist Plattform-unabhängig. Die mobile Version läuft auf Android und iOS, die Desktop-Version ist für Windows erhältlich. Versionen für Linux oder MacOS sind auf Projektbasis möglich. Die Integration der Lösung in bestehende Systeme ist unkompliziert und während der Migrationsphase im Parallelbetrieb möglich. Die Technologie ist sofort verfügbar und der Roll-Out wird auf Wunsch durch Expert*innen von secunet begleitet.

Vorteile

- Benutzername- und passwortlose Authentisierung
- Einfach integrierbar in bestehende Systeme
- Anpassbare Sicherheitslevel
- Datenhoheit liegt beim Kunden
- Individuelle Lösung im Corporate Design
- Desktop und mobile Anwendung
- Zukunftssichere kryptografische Verfahren
- Revisions sichere Transaktionen

Hochsichere passwortlose Authentisierung

Innovativ und zukunftssicher

Die unterschiedlichen Systeme und Infrastruktur der Anmeldeverfahren benötigen häufig verschiedene Token-Typen.

Sowohl im Hardware-Bereich als auch Software-basiert unterstützt secunet protect4use eine Vielzahl von Möglichkeiten. Neben der Smartcard, USB-Sticks und dem Secure Element des Smartphones lassen sich auch Bestandstoken integrieren, um Kosten zu sparen.

Bei Bedarf und je nach individueller Sicherheitsanforderungen können auch spezielle Token-Typen integriert werden. Im Bereich Gesundheit ist beispielsweise die elektronische Gesundheitskarte (eGK) als Token integriert.

Herkömmliche Authentisierungen				
Anwendung	Benutzer / Passwort			
Wissen/Biometrie	E-Mail	SMS	PushTAN / App	Authenticator / App
Besitz		Handy / Smartphone	Smartphone / Tablet	
Phishing / nicht Real Time	+	+	o	o
Phishing / Real Time	--	--	o	--
Angriffe aus der Ferne auf 2. Faktor	o	o	o	o
Leaks des Dienstes	+	+	--	--
Leaks anderer Dienste / gleicher Faktor	+	+	n/a	o
Usability	--	--	--	--
DSGVO	o	o	+	+

Zero Trust

Durch immer komplexere Systemumgebungen gewinnt auch die Vertraulichkeit immer mehr an Bedeutung. Mehr noch: Zero Trust wird zum Standard. Das Zero-Trust-Konzept „Niemals vertrauen, immer überprüfen“ kommt auch bei secunet protect4use zum Einsatz. Umgesetzt durch das secunet Identity- und Access-Management wird Single-Sign-On einfach und gleichzeitig sicher möglich. Die Datenhoheit bleibt dabei immer beim Dienst bzw. Dienstbetreiber.

Das Sicherheitslevel von secunet protect4use ist zudem skalierbar und deckt das eIDAS-Vertrauensniveau bis substantiell ab.

Die Kommunikation erfolgt über mehrere Kanäle, ist kryptografisch abgesichert und Ende-zu-Ende verschlüsselt.

Hochsichere passwortlose 2FA mit protect4use				
Smartphone-App	Windowsprogramm	App / Programm		Anwendung
Biometrie / kurze PIN	Kurze PIN	Biometrie		Wissen/Biometrie
IOS / Android	Zertifikats-datei	USB-Stick	BT/ NFC/USB Token	Besitz
+	+	+	+	Phishing / nicht Real Time
+	+	+	+	Phishing / Real Time
+	+	+	+	Angriffe aus der Ferne auf 2. Faktor
+	+	+	+	Leaks des Dienstes
+	+	+	+	Leaks anderer Dienste / gleicher Faktor
++	+	+	+	Usability
+	+	+	+	DSGVO

Nachweisfähige Transaktionen – ganz leicht und trotzdem sicher

secunet protect4use bietet mehr als nur die sichere Anmeldung über eine App.

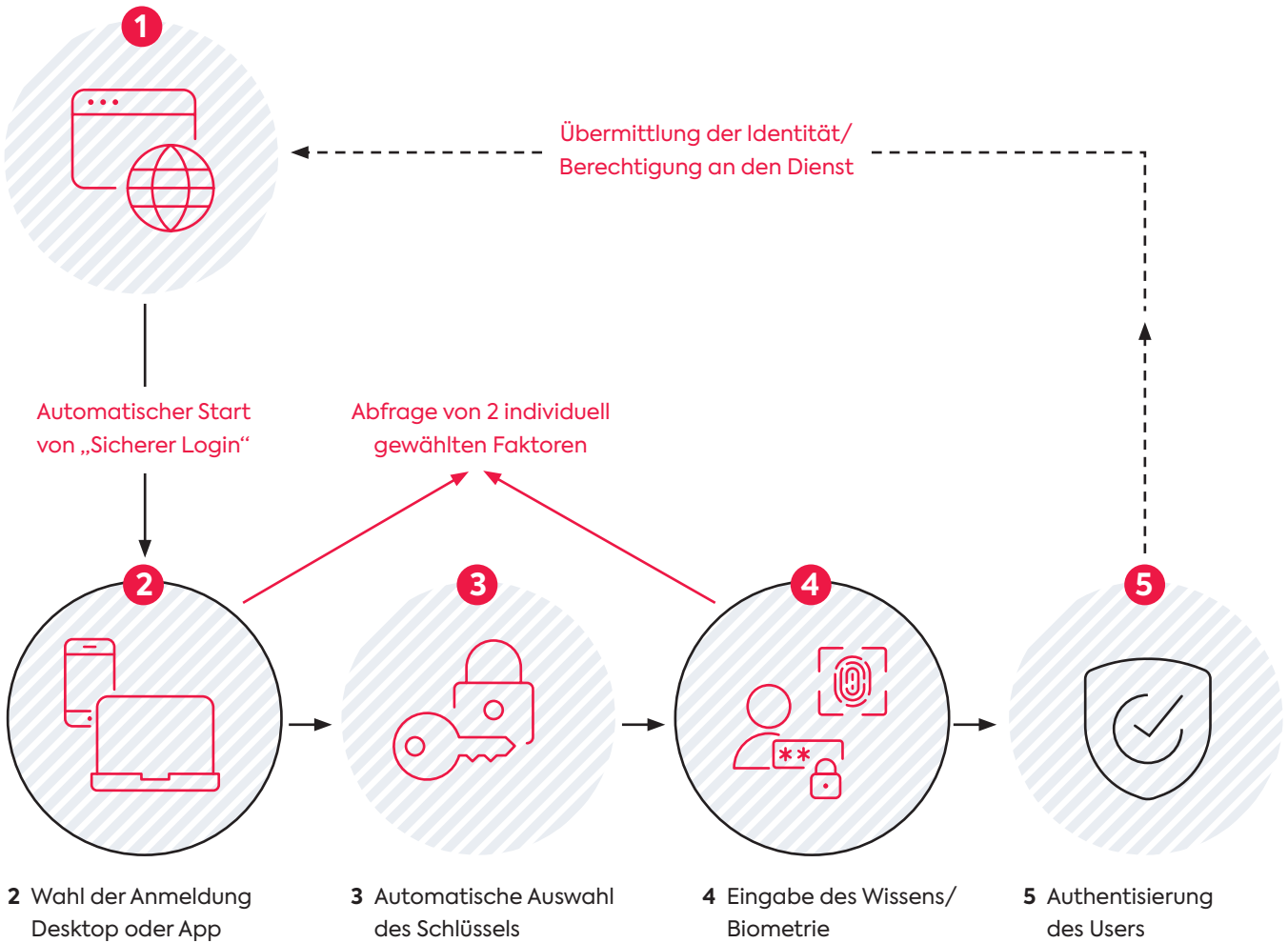
Umfangreiche Funktionen

Nachweisfähige Transaktionsfreigaben wie Anträge, Überweisungen oder Bestellungen gehören ebenso dazu wie zurechenbare Datenübermittlungen und Einreichungen von Dokumenten sowie User-Self-Services

Durch die patentierte Technologie wird die Transaktion revisionsicher und macht so Überweisungen, Bestellungen und Anträge digital und remote möglich.



1 Onlinedienst/Anwendung der Wahl



Individuell und flexibel

Das User Interface lässt sich umfassend konfigurieren und individualisieren. So können nicht nur einige Funktionen selbst angepasst, sondern auch das eigenen Corporate Design und Branding beispielsweise über das Logo, die Farben und die Eingabefelder der Software abgebildet werden. Alternativ kann die protect4use-Funktionalität mittels SDK in die eigene App integriert werden.

Selbstverständlich unterstützen die secunet protect4use Clients die Barrierefreiheit-Schnittstellen der jeweiligen gewählten Plattform.

Made in Germany

secunet protect4use wird in Deutschland bei secunet entwickelt. Neben dem Integrations-support bieten wir auf Wunsch gerne Beratung, Sicherheitsanalysen und Auditierungen an.

secunet – Schutz für digitale Infrastrukturen

secunet ist Deutschlands führendes Cyber-security-Unternehmen. In einer zunehmend vernetzten Welt sorgt das Unternehmen mit der Kombination aus Produkten und Beratung für widerstandsfähige, digitale Infrastrukturen und den höchstmöglichen Schutz für Daten, Anwendungen und digitale Identitäten. secunet ist dabei spezialisiert auf Bereiche, in denen es besondere Anforderungen an die Sicherheit gibt – wie z. B. Cloud, IIoT, eGovernment und eHealth. Mit den Sicherheitslösungen von secunet können Unternehmen höchste Sicherheitsstandards in Digitalisierungsprojekten einhalten und damit ihre digitale Transformation vorantreiben.

Über 1000 Expert*innen stärken die digitale Souveränität von Regierungen, Unternehmen und der Gesellschaft. Zu den Kunden zählen die Bundesministerien, mehr als 20 DAX-Konzerne sowie weitere nationale und internationale Organisationen. Das Unternehmen wurde 1997 gegründet. Es ist im SDAX gelistet und erzielte 2022 einen Umsatz von rund 347 Mio. Euro.

secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit.

secunet Security Networks AG

Kurfürstenstraße 58 · 45138 Essen
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com