Technische Daten

Authentisierungkomponente zur Integration in bestehende Kundensysteme	■ Bereitstellen der Server-Applikation als JAR-File oder nach Abstimmung ■ Unterstützung von Server-Hochverfügbarkeit und Clusterbetrieb (Cloud-Ready) ■ Server-Anforderungen: PostgreSQL 14, Java 17+; getestet mit Ubuntu 22.04 LTS ■ Identity Management: Anbindung an bestehendes Active Directory, LDAP, Radius oder SQL-DB (weitere auf Anfrage); Zugriff auf SQL-Datenbankserver erforderlich ■ Authentisierungsvorgang über REST-API mit Callback oder Polling
IAM/SSO-Projektlösung	■ Bereitstellung als VM mit Soft-Appliance mit integriertem Identitätsmanagement: Stand-Alone-Betrieb oder Sync mit bestehendem Active Directory oder LDAP ■ Authentisierungsvorgang über OpenID Connect oder SAML ■ Kompatibel mit: BigBlueButton, FreeRADIUS, GitLab, Google Cloud Identity/ Workspace, Matrix-Messenger, Microsoft Office 365 inkl. Teams, Jenkins, Dependency-Track, Nextcloud, eID PKI, Grafana, PowerDNS, Proxmox. Reverse Proxy, Palo Alto Web Application Firewall, Salesforce
Desktop Client	■ Download auf secunet.com ■ Windows 10+11, 64 Bit: Alle Versionen vor Support-Ende mit allen verfügbaren wichtigen Updates und Sicherheits-Updates entsprechend der jeweils aktuellen Microsoft-Vorgaben; Sondereditionen nur auf Anfrage (Linux) ■ Unattended Installation möglich ■ PC-Anforderungen: Microsoft-Mindestanforderungen sind abhängig von Systemkonfiguration, Bildschirmauflösung ≥ 1024×768 (XGA), bei Verwendung von Hardware-Token: erforderliche Schnittstellen und Zugriffsberechtigungen
Mobile Clients, konfigurierbar	■ Client für Android ab Version 6, verfügbar im Google Play Store ■ Client für iOS ab Version 13, verfügbar im Apple App Store
Client-Aufruf	■ Patentierte Methode über System-Link aus Web-Browsern (Chrome, Safari, Firefox, Edge oder Opera) sowie aus eigenen Programmen/anderen mobilen Apps
Sprachen	■ Deutsch und Englisch, weitere auf Anfrage
Barrierefreiheit	■ Unterstützung der plattformspezifischen Möglichkeiten
Kompatibilität	■ Neue Versionen 12 Monate abwärtskompatibel zu allen Releases der Server-Applikation
Software Development Kit (SDK)	■ Ermöglicht Integration in eigene mobile App für Android und iOS – Linux oder MacOS auf Anfrage
Absicherung der Kommunikation	■ Zweiter Kanal für Client-Server-Kommunikation, HTTPS/TLS ■ Zusätzliche unabhängige, kryptografische Absicherung ■ Echte Ende-zu-Ende-Verschlüsselung
Push-Nachrichten	■ Versand über einen von secunet betriebenen Push-Proxy (nur bei Verwendung der universellen mobilen Clients)
Soft-Token	■ Soft-Token, passwortgesichert, kopierbar ■ Soft-Token Plus: PIN-gesichert, servergestützte Schutzfunktionen, z.B. Sperrung - fehlgeschlagener Login-Versuche / Mobile Backup zur Wiederherstellung
Hardware-Token für Windows	■ USB-Sicherheitssticks von secunet ab 4. Generation mit speziellem Java-Applet ■ elektronische Gesundheitskarte (eGK) ■ USB Token und StarSign Crypto USB Token S basierend auf StarSign Crypto ■ Microsoft CNG–API: Generische Unterstützung, z.B. für Smart Cards ■ Auf Anfrage: Zusätzliche kundenspezifische HW-Token oder vorhandene Smartcards
Smartphone als Token für Desktop Computer	■ SE (Secure Element) im Smartphone (Android) ■ Authentisierungsvorgang initiieren: Scannen eines QR-Codes oder Push-Benachrichtigung ■ Out-of-Band-Authentisierung bei Push-Nachrichten ■ Abhängig von Gerät und Version des Betriebssystems: Secure Element / Enclave; ggf. Soft-Token Plus als Fallback ■ Biometrische Verfahren oder PIN-Verfahren