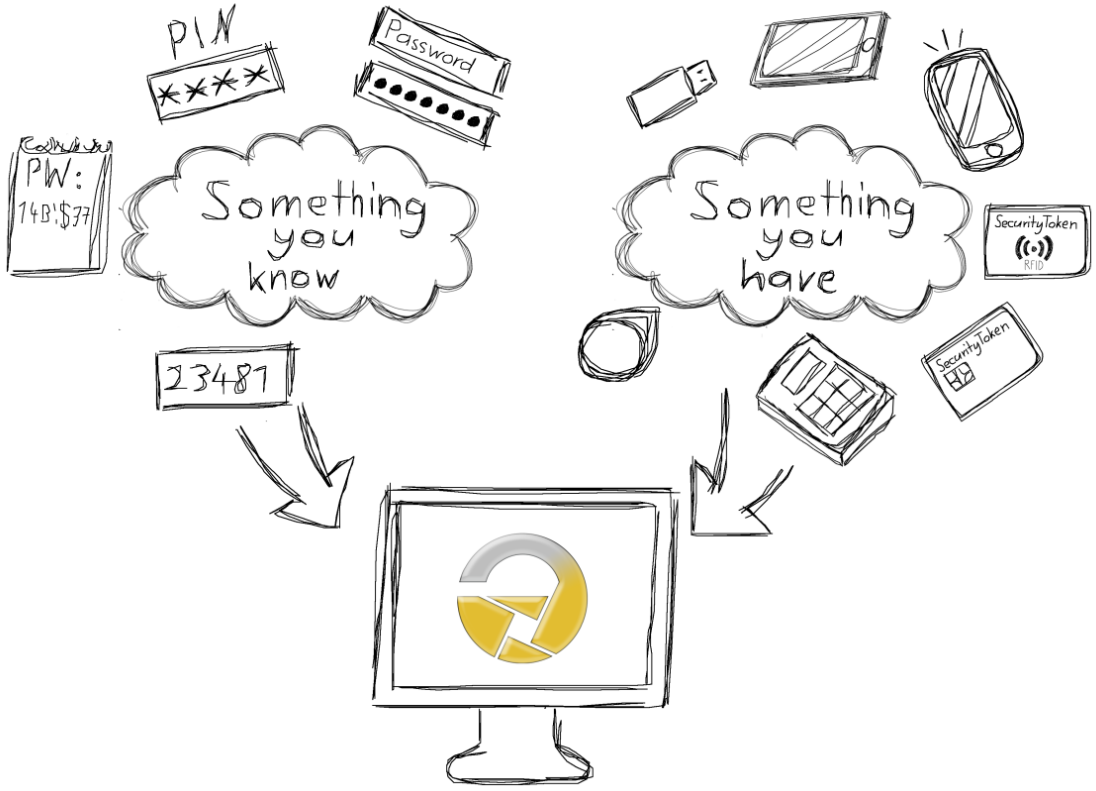
2-Faktor-Authentifizierung
Unser Beitrag zum Schutz Ihrer vertraulichen Daten

digitronic®.net

Secure Logon™ 2.0



- ☑ *modern:* 2-Faktor-Authentifizierung, auch ohne PKI
- ☑ *sicher:* Wissen (PIN) und Besitz (zertifizierter Token) erforderlich
- ☑ *einfach:* schnelles Implementieren auch in große Umgebungen
- ☑ *komfortabel:* zentral verwaltbar (via ADMX-Datei)
- ☑ *flexibel:* Integration der Token in andere Systeme möglich
- ☑ *innovativ:* Anmeldung mit Smartphone*

www.digitronic.net **vertrieb@digitronic.net**

Herausforderung

Anmeldungen an IT-Systemen mit Kennwort leiden an zwei auseinanderstrebenden Anforderungen: Zum einen wird eine hohe Komplexität des Kennworts (Geheimnis) gefordert, damit es sich nicht einfach ausspähen lässt, zum anderen wird eine nicht zu hohe Komplexität verlangt, damit sich die Benutzer ihr Kennwort merken können. Da dabei der Sicherheit zumeist Priorität eingeräumt wird, führen komplexe Kennwortrichtlinien zum berühmten Zettel unter der Tastatur oder zu hohem Supportaufwand für Administratoren, weil vergessene oder mehrfach falsch eingegebene Kennworte zurückgesetzt werden müssen.

Lösung

Die Lösung ist eine 2-Faktor-Authentifizierung (2FA), bei der ein hochkomplexes Geheimnis auf einem sicheren Token abgelegt und mittels Eingabe einer einfacheren PIN freigegeben wird. Das hohe Sicherheitsniveau ergibt sich daraus, dass für eine erfolgreiche Authentifizierung nunmehr zwei Faktoren benötigt werden, der sichere Token mit dem Geheimnis (Besitz) und die zur Freigabe erforderliche PIN (Wissen).

Produkt

Secure Logon™ 2.0 ermöglicht den Zugang zu lokalen und Netzwerkressourcen in Windows-Umgebungen mittels eines SecurityTokens und einer PIN.

Für die clientbasierte Software sind weder eine zentrale Serverkomponente noch eine komplexe Public-Key-Infrastruktur erforderlich. Die Software beinhaltet einen Credential Provider, der sich nahtlos in das Windows-Betriebssystem integriert und die 2FA ermöglicht.

Die für Secure Logon™ 2.0 entwickelte digitronic® Token Engine setzt mit ihrem modularen Aufbau auf eine extrem flexible Architektur und ermöglicht z. B. über ein API den Zugriff auf unterschiedliche Arten von Token.

Leistungsmerkmale

Auf den SecurityToken können mehrere Identitäten abgelegt und an Zielsysteme übergeben werden.

Trotz der dezentralen und unabhängigen Lösung werden gegebene Sicherheitsrichtlinien eingehalten. Ablaufende Kennwörter und/oder PINs sowie Vorschriften zu deren Komplexität werden mit Secure Logon™ 2.0 auch für passive RFID-Token in vollem Umfang unterstützt.

Die Lösung erhöht Sicherheit und Komfort, indem ein Entfernen des SecurityTokens entweder zum Sperren des PCs oder zum Abmelden des Benutzers über einen einstellbaren Countdown führen kann.

Secure Logon™ 2.0 ist über Softwareverteilung (msi-Pakete) zentral ausrollbar und kann über Gruppenrichtlinien (via ADMX-Datei) administriert werden.

Integration in andere Systeme/ Anpassungen

Eine besondere Stärke von Secure Logon™ 2.0 liegt in der hohen Integrationsfähigkeit in andere Systeme, wie Zeiterfassung oder Zugangskontrolle. In den meisten Fällen sind unsere SecurityToken zu diesen Systemen kompatibel.

Zudem eignet sich unsere Lösung z. B. dafür, bestimmte Anwendungen personalisiert zu starten. Gern setzen wir Ihre Anforderungen mit einer Anpassungsentwicklung um.

Machen Sie unser Know-how zu Ihrem Nutzen!

TECHNISCHE DETAILS

Betriebssysteme

Windows 7, 8, 8.1, 10

SecurityToken

☑ digitronic® USB SecurityToken mit Java Card OS (EAL5+-zertifiziert)
☑ Mifare DESFire EV1 (EAL4+), MIFARE DESFire EV2 (EAL5+)
☑ weitere SecurityToken wie IBM/NXP, Giesecke & Devrient, Gemalto, Oberthur oder mit Betriebssystemen wie STARCOS, Multos, TCOS und CardOS auf Anfrage bzw. ohne Support
☑ Android Smartphone*

Standards

PKCS #11, RFID nativ

Kartenlesegeräte

☑ RFID-basierte (nach ISO/IEC 14443) und kontaktbehaftete Leser, wie ReinerSCT cyberJack RFID basis, ReinerSCT cyberJack RFID Komfort, Cherry TC 1200 und Identiv CLOUD 3700F

PIN-Komplexität

☑ alphanumerische PIN und PUK
☑ bis zu 4 Kriterien (Groß-/Kleinbuchstaben, Zahlen, etc.)
☑ Komplexitätsprüfung gegen Dictionary
☑ Festlegung der Mindest- und Maximallänge der PIN
☑ Deltaprüfung zu bestehenden PIN und PUK

*als Prototyp verfügbar

Kurzportrait und weitergehende Angebote

Die digitronic® computersysteme gmbh mit Sitz in Chemnitz realisiert seit 1991 IT-Lösungen auf den Gebieten Kommunikation, IT-Sicherheit und digitale Vertraulichkeit. Mit klarem Fokus auf Zuverlässigkeit, Kundenfreundlichkeit und Funktionalität erarbeiten wir u.a. innovative Lösungen zur Stärkung der Vertraulichkeit schützenswerter Daten.

Unsere **All-In-One-Sicherheitspakete** erfüllen mit den beiden beinhalteten Lösungen 2FA und Verschlüsselung sensibler Daten auf Netzlaufwerken (HiCrypt™ 2.0) die Anforderungen von Prüfungen und Audits der Informationssicherheit nach VDA ISA (TISAX), ISO 27001 sowie Kriterien für kritische Infrastrukturen. Zudem können Sie in diesen Paketen aus verschiedenen Dienstleistungsangeboten diejenigen auswählen, mit denen wir Sie bei der Umsetzung Ihrer Projekte am besten unterstützen.

Kontakt

digitronic® computersysteme gmbh
Oberfrohnaer Str. 62
09117 Chemnitz

Tel.: +49 371 81539 0
Fax: +49 371 81539900
E-Mail: vertrieb@digitronic.net
Web: www.digitronic.net