

Sicherheit kann so einfach sein

USB Token: sicher, vielseitig, einfach



ID Hardware

ID Client Security Software

ID Management Systeme

USB Token verbinden auf ideale Weise komplexe Sicherheitsanforderungen mit einfacher Handhabung. Sie finden an jedem Schlüsselbund und in jeder Tasche Platz. Durch die Vielfalt möglicher Features und Ausführungen erfüllen sie sehr individuelle Anforderungen und steigern die User Effizienz. Das macht USB Token zur intelligenten Wahl.

USB Token machen vieles möglich

Sie bieten eine Fülle an Möglichkeiten im geschützten Umfeld eines Smart Card Chips. USB Token speichern private Schlüssel, Passwörter und digitale Zertifikate sicher wie in einem Tresor. Die privaten Schlüssel eines

Benutzers können direkt auf dem USB Token generiert werden und verlassen den Token nie.

Die Nutzung erfolgt ausschließlich im Token. Trotz seiner geringen Größe vereint er sowohl Chipkarte als auch Kartenleser. Man nimmt den Token einfach von einem Arbeitsplatz zum anderen mit. Voraussetzung für den Einsatz ist lediglich ein USB Anschluss am PC.

Technische Spezifikationen für USB Token

USB Token	Treiber				Token Schnittstellen			Chipkarten- betriebssysteme
	WIN PC/SC	CCID	-Linux	MAC OS X	Contactless PKI	MIFARE 4KB	Legic Advant 4KB	
StarKey 100	•	—	•	•	—	—	—	STARCOS SPK 2.3
StarKey 300	•	•	•	•	—	—	—	STARCOS 3.0
CrypToken M2048	•	•	•	•	—	—	—	JCOP21 v2.3.1
IDp 100	•	—	•	◦	—	—	—	i-COS 36
IDp 200	•	—	◦	◦	•	•	(optional)	JCOP41 v2.2.1
IDp 1000	•	•	•	•	—	—	—	JCOP21 v2.3.1
miDentity*	•	—**	•	•	—	—	—	JCOP41 v2.3.1
eToken PRO (Java) v 1.1	•	•	•	•	—	—	—	IDProtect v0106.8015.0508

Detaillierte Informationen zu Chipkarten Betriebssystemen finden Sie auf unserem Chipkarten Datenblatt

• = verfügbar / — = nicht verfügbar / ◦ = in Entwicklung / * mit Flash Memory bis 1 GB, Customized Applikationen auf dem Token / ** Zero-Footprint, Drivers: s (HID)



Doppelt sicher durch Zwei-Faktor-Authentisierung

USB Token bieten sehr hohe Sicherheit durch Zwei-Faktor-Authentisierung: Besitz und Wissen. Das heißt, der Benutzer muss erstens den USB Token besitzen und zweitens die PIN-Nummer wissen. Erst die richtige Kombination ermöglicht den Zugriff auf Daten und Anwendungen. Zugangsdaten des Verwenders lassen sich nicht kopieren, verändern oder unberechtigt nutzen. Das harte Kunststoffgehäuse bietet zusätzlichen Schutz vor äußeren Einwirkungen.

Vielfältiger Einsatz in verschiedenen Umgebungen

USB Token können auf einfache Weise in Sicherheitslösungen eingebunden werden, die über Standard Software Schnittstellen wie MS-CAPI oder PKCS#11 verfügen. Dadurch eröffnen sich vielfältige Verwendungsmöglichkeiten, z.B. für:

- Virtual Private Networks (VPN)
- SSL Client Authentifizierung
- E-Mail Verschlüsselung / Signatur
- Windows Logon
- Single Sign On
- Festplattenverschlüsselung

Lösungen für alle Sicherheitsstufen und Sicherheitsanforderungen

Die eingebauten modernen Kryptoprozessoren bieten Zertifizierung auf verschiedenen Sicherheitsstufen. Für USB Token stehen proprietäre oder Java™ basierte Kartenbetriebssysteme unterschiedlicher Hersteller zur Verfügung. Sie unterscheiden sich technische Features wie die Größe des EEPROM Speichers und durch verschiedene Zertifizierungen (CC, ITSEC, FIPS). Details finden Sie in der Tabelle auf unserem Datenblatt Chipkarten.

USB Token mit kontaktlos Funktion auch für physischen Zugang

USB Token mit Proximity verbinden die klassische Smartcard-Technologie mit den Vorteilen der kontaktlosen Transpondertechnologie. Neben den gängigen Einsatzmöglichkeiten des USB Token, wie z.B. Windows Logon, Benutzer-Authentisierung etc. stellen USB Token mit Proximity diese Funktionen auch kontaktlos zu Verfügung. Darüber hinaus bieten sie zusätzliche Funktionalitäten aus dem Bereich des physischen Zugangs wie z.B. kontaktlose Türöffnung, Einsatz für Zeiterfassungs- und Zahlssysteme auf Basis von beispielsweise Mifare oder Legic.

IDpendant GmbH
Edisonstraße 3
D-85716 Unterschleißheim/München

Telefon +49 89 3700 110-0
Fax +49 89 3700 110-10
info@idpendant.com

www.idpendant.com