DriveLock
securing your digital tomorrow

Smartcard Management: herstellerunabhängig & flexibel

Whitepaper

DriveLock
securing your digital tomorrow

Smartcard Middleware – Ihre Investition in eine unabhängige und sichere Zukunft

Was bringt eine Multi-Faktor Authentifizierung?

Nicht erst seit Inkrafttreten der DSGVO sind Unternehmen verpflichtet, zum Schutz von personenbezogenen Daten geeignete technische und organisatorische Maßnahmen zu implementieren. Auch das im März 2019 verabschiedete Geschäftsgeheimnisgesetz (GeschGehG) zwingt Unternehmen, die ihre Geheimnisse schützen wollen, zu einem umfassenden Schutzkonzept. Dazu gehört auf jeden Fall auch die sichere Authentifizierung des Benutzers, bevor dieser Zugang zu diesen Datensätzen erhält. Der Umfang derartiger Maßnahmen muss sich außerdem am Grad der Geheimhaltung orientieren: je schützenswerter das Geheimnis, umso wirkungsvoller und sicherer muss auch die Schutzmaßnahme sein. Das kann bedeuten, dass für den Zugang zu Daten des neuen Prototypen eine Anmeldung mit Passwort nicht mehr ausreichend ist und stattdessen eine Multi-Faktor Authentifizierung mit Smartcard bzw. Token oder eine biometrische Identifizierung in Betracht gezogen werden muss.

Dass Passwörter als einziger Faktor schon längst nicht mehr sicher sind und eine Schwachstelle in jedem Sicherheitskonzept darstellen, ist unserem Bestreben nach Einfachheit geschuldet – insbesondere bei Routineaufgaben wie dem täglichen Anmeldeprozess am eigenen Rechner oder anderen Zugangssystemen im Unternehmen. Es gibt viele Tipps zur sicheren Verwendung von Passwörtern, in der Praxis werden die meisten davon häufig ignoriert. Damit haben Hacker ein leichtes Spiel, können sich so fremde Identitäten aneignen und Zugang zu den Zielsystemen erhalten. Passwörter sollten schon längst durch Multi-Faktor Logins abgelöst werden, das fordert längst auch das BSI.

Bei einer 2F- oder 3F-Authentifizierung wird neben dem Wissen (Passwort, PIN) entweder ein biometrisches Merkmal (z. B. Iris, Fingerabdruck oder Venenscan) und/oder der Besitz (Smartcard oder Token) als zusätzlicher Faktor zur glaubwürdigen Identifizierung eines bestimmten Benutzers herangezogen. Damit reicht es für einen Angreifer nicht mehr aus, nur das Passwort zu bekommen und die Hürde, auch in den Besitz des jeweiligen anderen Faktors zu bekommen, ist deutlich höher. Multi-Faktor Authentifizierung bietet somit ein signifikant besseres Schutzniveau bzw. eine sogenannte starke Authentifizierung, wie sie für den Zugang zu kritischen Infrastrukturen oder für die Absicherung finanzieller Transaktionen schon heute verwendet werden soll.

Was ist eine Smartcard Middleware?

Betriebssysteme und auch immer mehr Anwendungen stellen neben der Anmeldung über Benutzername und Passwort Multi-Faktor Authentifizierungen zur Verfügung, bei denen Smartcards (oder Tokens) zum Einsatz kommen. Auf Smartcards ist der geheime Schlüssel eines Benutzers gespeichert, der zur Anmeldung oder Verschlüsselung von Daten verwendet werden kann.
Um der Anwendung die Kommunikation mit der Smartcard zu ermöglichen, wird eine Smartcard Middleware Software benötigt, welche der Applikation eine standarisierte Schnittstelle bietet und Anfragen darüber in die richtigen Befehle für die Karte übersetzt. Eine herstellerunabhängige Smartcard Middleware ermöglicht eine Verbindung über eine solche Crypto-API zu vielen unterschiedlichen Kartentypen. Der Kern der Middleware ist dabei ein Treiber für das Betriebssystem, der als Übersetzer fungiert und die benötigten kryptografischen Schnittstellen zur Verfügung stellt.

Welche Vorteile bietet mir eine herstellerunabhängige Smartcard Middleware?

Wird in einem Unternehmen eine Smartcard von einem einzigen Hersteller eingesetzt, könnte man auch die angepasste Treibersoftware dieses Anbieters installieren und verwenden. Jedoch gibt es auch bei Smartcards einen Lebenszyklus und die Technologie entwickelt sich ebenfalls ständig weiter. Schlüssellängen und Algorithmen, die bis heute noch als sicher genug angesehen wurden, sollten in der Zukunft nicht mehr eingesetzt werden (1). Karten gehen verloren oder werden beschädigt; ca. 10 % der eingesetzten Smartcards müssen pro Jahr ersetzt werden. Ein Wechsel auf aktuellere Smartcards ist somit unvermeidlich. Da sich Hersteller den Support älterer Karten oft teuer bezahlen lassen, senkt das die Kosten besonders am Ende des Lebenszyklus einer Karte beträchtlich.

Zudem gibt es eine ganze Reihe von Smartcards mit unterschiedlichen Einsatzmöglichkeiten, aus denen Firmen häufig diejenige Karte auswählen, welche die Gesamtzahl an Anforderungen abdeckt – zum entsprechend höheren Gesamtpreis. Diese Anforderungen beinhalten beispielsweise einen einfachen Login am Betriebssystem, die Verschlüsselung von Daten oder E-Mails, der physikalische Zugang zu verschlossenen Räumlichkeiten oder auch das Bezahlen des Mittagessens in der Kantine.
Dank einer herstellerunabhängigen Middleware, die viele verschiedene Kartensysteme gleichzeitig unterstützt, sind Kunden nicht an einen Kartenhersteller gebunden und können sich für die zum Anwendungsfall und das Unternehmen passende Karte entscheiden – falls sinnvoll sogar für Karten unterschiedlicher Hersteller gleichzeitig. Auf diese Weise können unterschiedliche Anforderungen und Funktionen auch schrittweise umgesetzt und eingeführt werden. Ein späterer Wechsel auf neuere Karten und andere Hersteller ist dabei jederzeit und einfach möglich.

Zusätzlich sollte eine moderne Smartcard Middleware auch für die wichtigsten Betriebssystemplattformen Windows, macOS und Linux verfügbar sein, damit der Einsatz der gleichen Smartcard-Technologie auch in heterogenen Umgebungen möglich ist.

Für wen eignet sich eine Smartcard Middleware?

Jedes Unternehmen mit geschäftskritischen Geheimnissen sollte sich nicht länger auf eine schwache Identifikation durch Passwörter verlassen, sondern mindestens eine Zwei-Faktor-Authentifizierung für die Anmeldung einsetzen. Bei Systemumgebungen, die auf der Microsoft-Architektur basieren, stehen für den Administrator alle notwendigen Funktionen für den Betrieb einer dafür notwendigen Public-Key Infrastruktur (PKI) zur Verfügung. Ist diese vorhanden, steht einem Einsatz von Smartcards für die Anmeldung am Rechner nichts mehr entgegen und eine Smartcard Middleware, welche bereits bei einer Neuinstallation eines Rechners auf diesem eingerichtet wird, erleichtert die spätere Auswahl der richtigen Smartcard und reduziert im weiteren Betrieb die Kosten für den Wechsel bzw. den Austausch auf neuere Hardware.

Aber auch für Hersteller, die in eigenen Lösungen eine zusätzliche Smartcard-Authentifizierung anbieten wollen, stellt eine Smartcard Middleware die ideale Lösung dar, um Kunden die größtmögliche Flexibilität zu bieten. Egal, ob es sich dabei um ein neues System zur Zugangskontrolle für Produktions- oder Forschungsbereiche, die Identifikation für einen abteilungsweit verwendeten Drucker, die Authentifizierung an wichtigen industriellen Steuerungssystemen (ICS) oder die Integration in die neue Web-Applikation handelt. Bei Kunden, die bereits Karten einsetzen, ist die Unterstützung der bereits vorhandenen Hardware immer ein wirksames Verkaufsargument.
Eine Smartcard Middleware ermöglicht auch Anbietern von biometrischen Identifizierungslösungen, Kunden einen Mehrwert zu bieten durch die nahtlose Integration verschiedener Authentifizierungsfaktoren in einfache Anmeldeprozesse. So sind komfortable und vor allem sehr sichere Authentifizierungsprozesse möglich, die auch von Kunden bzw. deren Anwendern aufgrund deren Einfachheit akzeptiert werden.

Was bietet DriveLock SmartCard Middleware?

Der Einsatz der DriveLock SmartCard Middleware ermöglicht es, bei einer Vielzahl an Anwendungen (Web-Applikationen, E-Mail oder VPN Clients, Browser, SSO, Festplatten- und Dateiverschlüsselung) eine sichere Multi-Faktor Authentifizierung durchzuführen, so dass auf die Verwendung von unsicheren Passwörtern verzichtet werden kann.

DriveLock SmartCard Middleware stellt alle relevanten kryptografischen Schnittstellen für jedes wichtige Betriebssystem zur Verfügung: Microsoft CSP/KSP und CNG mit Minidriver (für Windows), PKCS#11 (für Linux-Derivate, Windows und macOS) und Apple TokenD (für macOS).
Über 100 unterschiedliche Security Tokens, Smartcard-Typen (JCOP, CardOS, TCOS, SecCOS, ACOS und andere) und Profile (wie z.B. PKCS#15, SSID, SigG, FINeID, CNS, PIV/CAC) werden bereits heute von DriveLock SmartCard Middleware unterstützt, neuere Kartensysteme werden regelmäßig hinzugefügt.

DriveLock SmartCard Middleware erlaubt die Verwendung von RSA Algorithmen zur Erzeugung von Schlüsseln mit einer Länge bis zu 4096 Bit und Kryptoverfahren mit Elliptischen Kurven (ECC) mit einer Schlüssellänge von bis zu 512 Bit.

Durch den Support von biometrischen Identifizierungssystemen wie Fujitsu PalmSecure ist der Einsatz der SmartCard Middleware auch in Umgebungen mit sehr hohen Anforderungen an eine zuverlässige und sichere Benutzerauthentifizierung einfach möglich.

Mit Hilfe der zusätzlichen Management Software „Security Token Configurator" können Karten vor der Ausgabe an den User leicht personalisiert werden. Für den Endanwender steht ein einfaches Tool zur Verfügung, um die Karten-PIN nachträglich anzupassen oder eine durch fehlgeschlagene PIN-Eingaben gesperrte Karte wieder freizuschalten, sofern eine dazu notwendige Super-PIN zuvor eingerichtet wurde.

Quellen:

(1) BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen", Version: 2019-01

Kontaktieren Sie uns!

DriveLock SE
+49 (89) 546 36 49-0
info@drivelock.com

www.drivelock.com