

Pre-Boot Authentisierung für Microsoft BitLocker mit drahtloser 2-Faktor-Authentisierung

DIE HERAUSFORDERUNG

Die zunehmenden Compliance Anforderungen, wie z.B. DSGVO konforme Verschlüsselung von personenbezogenen Daten, erfordern die lückenlose Verschlüsselung von Windows Geräten und starke Benutzerauthentisierung am Arbeitsplatz.

Der Einsatz von Festplattenverschlüsselung ist in Unternehmen und Behörden heute fest etabliert. Mit gutem Grund, denn die Verschlüsselung stellt die einzige Möglichkeit zum Schutz der Daten bei Verlust oder Diebstahl des Geräts dar. Für die Umsetzung gibt zahlreiche Möglichkeiten – nicht alle davon sind sinnvoll.

Lesen Sie, wie eine moderne Festplattenverschlüsselung mit Microsoft BitLocker sicher und nutzerfreundlich auf Geräten mit Windows Betriebssystem umgesetzt werden kann.

BITLOCKER OHNE PRE-BOOT AUTHENTISIERUNG (PBA)?

Der Einsatz einer Verschlüsselung ist nur dann sinnvoll, wenn sichergestellt werden kann, dass ausschließlich berechnete Mitarbeiter den Zugriff auf das Gerät erhalten. Entscheidend ist der Zeitpunkt der Authentisierung. Als vollständig geschützt gilt ein Gerät nur, wenn es das Betriebssystem noch nicht geladen hat. Die Authentisierung muss also zu einem Zeitpunkt erfolgen, bevor das eigentliche Windows Betriebssystem geladen wird. Man spricht von einer sogenannten Pre-Boot Authentisierung.

DIE WAHL DER RICHTIGEN AUTHENTISIERUNGSMETHODE

Viele Behörden und Unternehmen verwenden bereits Smartcards in Form des klassischen Mitarbeiterausweises für eine starke Zwei-Faktor-Authentisierung. Sie erhöhen durch den Einsatz von Smartcards die Sicherheit ihrer Systeme und erfüllen damit interne, branchenspezifische und/oder gesetzliche Vorgaben.

Die durchgängige Verwendung bereits vorhandener Smartcards stellt daher für diese Unternehmen die ideale Authentisierungsmethode für die Pre-Boot Authentisierung dar.

DIE GEMEINSAME LÖSUNG:

Drahtlose 2FA für Festplattenverschlüsselung mit Pre-Boot Authentisierung & Single Sign-On



VORTEILE

- ✓ Pre-Boot Authentisierung für Festplattenverschlüsselung mit drahtloser 2-Faktor-Authentisierung (2FA)
- ✓ Für Windows Endgeräte auch ohne Smartcard-Slot
- ✓ Einfache Bedienung für Anwender durch Single Sign-On
- ✓ Zentrale Administration
- ✓ Integrierter HelpDesk
- ✓ Vorhandene Smartcards weiter wie gewohnt nutzen
- ✓ Einfache Integration

NUTZUNGSEINSCHRÄNKUNGEN BEI GERÄTEN MIT WINDOWS BETRIEBSSYSTEM?

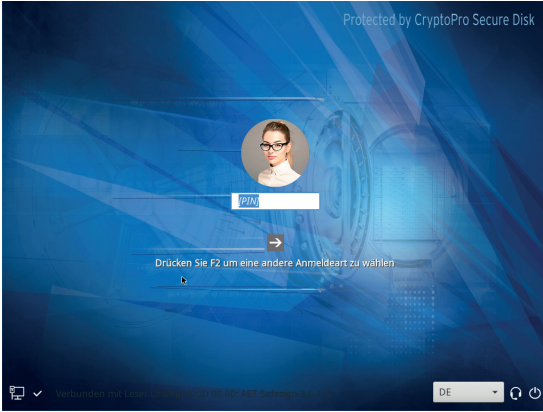
Unterwegs möchten die Nutzer sicher und vor allen Dingen komfortabel auf ihren Notebooks und Tablets arbeiten. Beim mobilen Einsatz auf modernen Notebooks und Tablets werden kabelgebundene Smartcard-Leser aufgrund der umständlichen Handhabung durch die Nutzer schlichtweg abgelehnt. Mit dem Trend zu flacheren und leichteren Notebooks verschwinden zunehmend auch die internen Smartcard-Leser bei modernen Geräten.

Für Unternehmen und Behörden mit Smartcards steht eine moderne Lösung für die sichere und nutzerfreundliche Umsetzung einer Festplattenverschlüsselung für Geräte mit Windows Betriebssystem bereit.

Die Lösung von cpsd erweitert die Funktionalität von Microsoft BitLocker um eine eigene Pre-Boot Authentisierung und ermöglicht die Verwendung von Smartcards zur Authentisierung in der PBA, noch bevor das Windows Betriebssystem geladen wird.

Über den drahtlosen Smartcard-Leser AirID von certgate wird die bereits vorhandene persönliche Smartcard des Mitarbeiters kabellos und bequem per Bluetooth der PBA bereitgestellt.

Nach dem Start des Windows Geräts gibt der Mitarbeiter nur noch seine persönliche PIN in der PBA ein. Das Gerät bootet per Single Sign-On direkt durch bis auf den Windows Desktop. Der Mitarbeiter muss sich kein zweites Mal am Betriebssystem anmelden.



CRYPTOPRO SECURE DISK FOR BITLOCKER

von CPSD

Secure Disk for BitLocker, als eigenständige Pre-Boot-Lösung, ermöglicht den praktikablen Einsatz von Microsoft BitLocker.

Eine umfangreiche, aber einfach zu bedienende zentrale Administration sorgt neben zahlreichen Schnittstellen für eine nachweisliche Compliance durch tagaktuelle Berichte. Dank der Lösung gelingt der BitLocker Rollout einfach und mit optimaler Integration in das bestehende betriebliche Umfeld.

Der bereits in die PBA integrierte Helpdesk ermöglicht den Mitarbeitern eine schnelle Lösung bei Supportfällen und sorgt damit für eine Reduktion der Betriebskosten.

DRAHTLOSER SMARTCARD-LESER AirID

von certgate

Der certgate AirID ist ein drahtloser Smartcard-Leser im „EC-Karten“ Format. Dadurch können Smartcard-Funktionen eines typischen Mitarbeiterausweises kabellos an Windows Geräten genutzt werden.

Neben der CRYPTOPRO SecureDisk for BitLocker-Anwendung ist AirID vielseitig einsetzbar. Alle gängigen Smartcard Use Cases wie beispielsweise E-Mail-Verschlüsselung, digitale Signatur oder VPN können drahtlos per Bluetooth genutzt werden. Alle kontaktlosen Funktionen der Smartcard für Zeiterfassung, Zutritt, Bezahlen oder FollowMe-Printing bleiben mit AirID vollständig erhalten. Darüber hinaus ist der AirID-Smartcard-Leser mit verschiedenen Geräten wie Smartphones oder Tablets auf den gängigen Plattformen Windows, iOS, Android, macOS und Linux einsetzbar.

Über CPSD

Das Team von CPSD entwickelt hochwertige Verschlüsselungslösungen für sicherheitsbewusste Unternehmen und zahlreiche öffentliche Stellen im In- und Ausland.

Seit über 15 Jahren stehen die CryptoPro Produkte für beste Kundenzufriedenheit durch einen ausgewogenen Mix aus Sicherheit, Benutzerkomfort und minimale Verwaltung. Auch zukünftige Sicherheitsanforderungen sind bei unseren Experten in besten Händen. Die Erfahrung aus zahlreichen Kryptographie-Projekten teilen wir gerne und empfehlen die optimale Verschlüsselungsstrategie.

Weitere Informationen zu unseren Verschlüsselungslösungen erhalten Sie unter: <https://www.cpsd.at>

Über certgate

certgate ist einer der führenden IT Security Anbieter für sichere, mobile Kommunikationstechnologien und langjähriges Mitglied der Allianz „IT Security Made in Germany“.

International führende Unternehmen und Behörden, wie die Bundesagentur für Arbeit und staatliche Sicherheitsbehörden im Ausland sichern ihre mobile Kommunikation über certgates patentierte Technologie und Produkte. certgate's Lösungen werden weltweit auch über Partner vertrieben und ermöglichen wirklichen Schutz vor Hackern, mobile data leakage und nicht autorisierten Zugriff – auch durch staatliche Behörden. Bereits heute schützt certgate nachhaltig weltweit für tausende von Anwendern täglich deren mobile Kommunikation und Daten.

Erfahren Sie noch heute, warum sichere Kommunikation von vielen führenden Experten unbedingt empfohlen wird unter: <https://www.certgate.com>

certgate GmbH
Kaiserswerther Straße 45
40477 Düsseldorf
Germany

Phone + 49 (0) 911 93 523-0
E-Mail: info@certgate.com

Web: www.certgate.com

