

ECOS SecureBootStick®

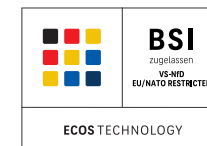
# Hochsicherer Fernzugriff auf Daten und Anwendungen

Im Homeoffice, im mobilen Einsatz oder für externe Dienstleister

- ♦ BSI-Zulassung für VS-NfD, EU/NATO RESTRICTED
- ♦ Für Firmen, Fremd- und Privat-PC
- ♦ Einfach, flexibel, hochsicher

**IT-Security Solutions**

Made in Germany



# ECOS SecureBootStick®

## Datenfernzugriff - einfach, flexibel, hochsicher

Mit Beginn der Corona-Pandemie wurden Arbeitsplätze so weit wie möglich ins Homeoffice verlagert.

Die IT musste innerhalb kürzester Zeit entsprechende Lösungen bereitstellen. Eine Herkulesaufgabe, bei der die IT-Security vielerorts auf der Strecke geblieben ist. Bei der aktuellen Bedrohungslage zeigt sich mehr denn je, dass der Schutz vor Cyberangriffen und Spionage von existentieller Wichtigkeit ist.

Während die IT-Infrastruktur mit großen Anstrengungen geschützt wird, bleibt der Heimarbeitsplatz oft die Schwachstelle. Auch vermutlich noch so unwichtige Daten und unkritisches Benutzerverhalten kann einem Angreifer im Rahmen eines Langzeitangriffs wichtige Informa-

tionen liefern, für einen gezielten Angriff auf das Unternehmen.

An diesem neuralgischen Punkt setzt der ECOS SecureBootStick an. Das zugrundeliegende Sicherheitskonzept ist so konzipiert, dass der Stick auch auf einem mit Schadsoftware verseuchten PC in einem gefährdeten Netz, gefahrlos betrieben werden kann. Trotzdem schützt die Lösung hochwirksam vor Angriffen und Spionage. Für die Produktvarianten SX und ZX besteht sogar eine BSI-Zulassung für die Verarbeitung von Daten mit Geheimhaltungsgrad VS-NfD und das sogar in Verwendung mit einem privaten Notebook oder PC.

### Vorteile

- ◆ **Flexibel** einsetzbar, mit einem gängigen Firmen-Notebook oder privatem PC
- ◆ **Einfache** Administration, nahtlose Integration in die IT-Infrastruktur
- ◆ **Hochsicher**, dank einer Kaskadierung zahlreicher Sicherheitsmechanismen
- ◆ **Garantiert**, mit BSI-Zulassung für VS-NfD, EU/NATO RESTRICTED

### ECOS SecureBootStick® Produktfamilie

- ◆ Der ECOS SecureBootStick **CL** bietet Kunden ein hohes Sicherheitsniveau zu einem besonders attraktiven Preis.
- ◆ Der ECOS SecureBootStick **HE** bringt die bewährte Lösung, dank eines speziell entwickelten hardwareverschlüsselten und mit zahlreichen Sicherheitsfeatures ausgestatteten USB-Sticks, auf ein neues Sicherheitsniveau.
- ◆ Der ECOS SecureBootStick **FX** bietet, wie der HE, zahlreiche in Hardware gegessene Sicherheitsfeatures. Ergänzend verfügt er über eine integrierte Smartcard sowie eine integrierte Tastatur zur Eingabe der PIN direkt am Stick.
- ◆ Der ECOS SecureBootStick **SX** ist weitgehend identisch mit dem FX, verfügt jedoch über eine BSI-Zulassung für den Zugriff auf Daten und Anwendungen mit Geheimhaltungsgrad VS-NfD, EU/NATO RESTRICTED und das sogar in Verbindung mit einem privaten PC.
- ◆ Der ECOS SecureBootStick **ZX** ermöglicht mit seinem Einschub für Karten im Format ID-1 die Nutzung von PKI-Karten und Ausweisen zur Nutzer-Authentisierung. Darüber hinaus ist er baugleich und softwaretechnisch identisch mit dem SX.



## Ideal für Unternehmen und Behörden mit hohen Sicherheitsanforderungen

### Hochsicher ins Behörden-/Unternehmensnetz

Der ECOS SecureBootStick ermöglicht einen hochsicheren Zugang zu einer Terminalserver- oder Virtual-Desktop-Infrastruktur und Webanwendungen aus einer geschützten und gekapselten Umgebung heraus.

Mit dem Stick bootet ein gängiger PC das speziell gehärtete ECOS Secure Linux-Betriebssystem. Die interne Festplatte bleibt ausgeschaltet, sodass möglicherweise auf der Festplatte vorhandene Schadsoftware niemals zum Zuge kommt.

Mit Abschalten der internen Festplatte wird eine 100%ige Trennung zwischen der beruflichen und der privaten Nutzung des PCs sichergestellt. Firmware und Applikationen befinden sich auf dem Behörden- oder Firmen-Stick. Der private PC dient damit nur noch als private Peripherie.

### Sämtliche Software auf dem Stick

Der Stick enthält die notwendigen Clients für einen hochsicheren Zugriff auf Microsoft RDSH (ehemals Windows Terminalserver), Citrix Virtual Apps und Desktops (ehemals XenApp und Xen-Desktop), VMware Horizon (ehemals VMware View), sowie PCs mit Remote-Desktop-Freigabe. Für den Zugriff auf Webanwendungen sind ein Firefox- sowie ein Chromium-Browser auf dem Stick integriert.

### Einfache Implementierung und Administration

Die integrierten VPN-Clients terminieren gegen ein bereits bestehendes VPN-Gateway unter Ver-

wendung von IPsec oder OpenVPN. In Verbindung mit Citrix ADC (ehemals Citrix Netscaler) ist eine Anbindung über https möglich. Alternativ zu dem integrierten VPN-Client stehen, unter Berücksichtigung zusätzlicher Herstellerlizenzen, auch ein Cisco AnyConnect (per SSL), sowie ein Client für Juniper und F5 zur Verfügung. Für die BSI-zugelassenen ECOS SecureBootStick SX/ZX wird gemäß SecOps eine genua genuscreen als VPN-Gateway vorausgesetzt.

Mit dem ECOS Easy-Enrollment lässt sich auch eine große Anzahl an Zugängen innerhalb kürzester Zeit ausrollen. Dabei erhält jeder Anwender einen identisch vorkonfigurierten Stick. Über das zentrale Management werden persönliche Aktivierungs-codes generiert bzw. beim FX/SX persönliche Smartcards ausgestellt, über welche die Sticks ihre userspezifische Konfiguration erhalten. Beim ZX erfolgt die Kopplung an eine bereits vorhandene PKI-Karte bzw. einen persönlichen Ausweis über die Synchronisation der öffentlichen Schlüssel. Dank des zentralen Managements, lassen sich alle Sticks zentral verwalten und remote aktualisieren.

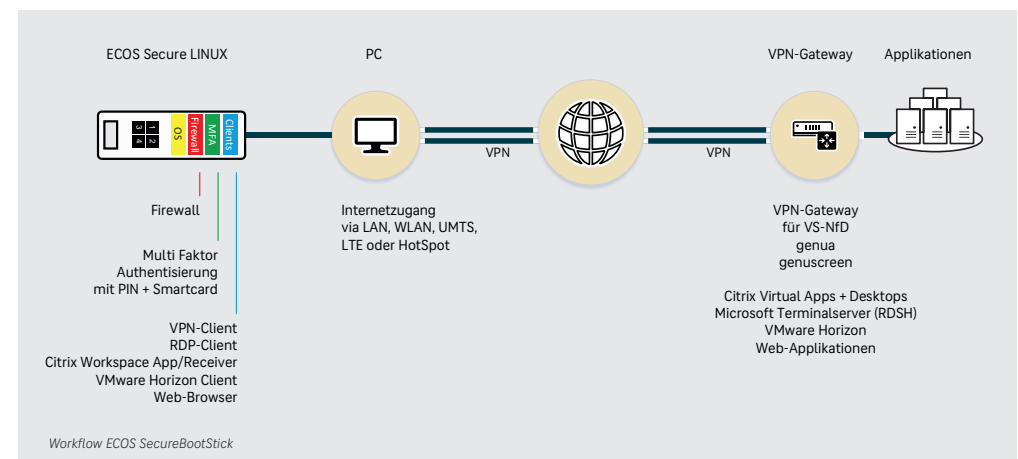
### Multi-Faktor-Authentisierung

Der Secure Boot Stick bietet nicht nur die Sicherheit einer geschützten und gekapselten Umgebung, er dient auch gleichzeitig als starke Multi-Faktor-Authentisierung. In der Produktvariante CL wird die Personalisierung des Sticks über ein Zertifikat realisiert, welches an die Hardware-ID des Sticks gekoppelt ist. Ab dem HE erfolgt die Kopplung an den Stick über einen

kryptografischen Schlüssel in der Hardware. In den Produktvarianten FX/ SX/ZX wird die Authentisierung zusätzlich um eine Smartcard ergänzt.

### Einfach und flexibel für Anwender

Die Nutzung des Secure Boot Sticks ist für die Anwender denkbar einfach. Nach Einschalten und Eingabe der PIN bootet der PC und führt die Nutzer zu einer Auswahl der freigegebenen Systeme oder Anwendungen. Beim Betrieb via WLAN erfolgt die Eingabe des Schlüssels genauso einfach wie beim Smartphone und wird für die künftige Anmeldung verschlüsselt abgespeichert. Nach der Auswahl des gewünschten Systems oder der gewünschten Anwendung befindet sich der Anwender in der vertrauten Umgebung.





safe and smart

| Funktionsübersicht ECOS SecureBootStick®   | CL      | HE      | FX      | SX      | ZX      |
|--|---------|---------|---------|---------|---------|
| <b>BSI-Zulassung</b>   |         |         |         |         |         |
| Zugelassen für die Verarbeitung von Daten bis zum Geheimhaltungsgrad VS-NfD, EU/NATO RESTRICTED                        |         |         |         | ✓       | ✓       |
| <b>Applikationen</b>   |         |         |         |         |         |
| RDP-Client, Citrix Workspace App, VMware Horizon (per RDP, PCoIP, BLAST), Firefox, Chromium, VPN-Client für IPsec      | ✓       | ✓       | ✓       | ✓       | ✓       |
| Citrix HDX RealTime Media Engine zur Optimierung d. Audio-/Video-Übertragung bei Skype for Business & Microsoft Teams  | ✓       | ✓       | ✓       | ✓       | ✓       |
| Microsoft Remote FX zur Optimierung der Audio-Qualität in Verbindung mit RDP   | ✓       | ✓       | ✓       | ✓       | ✓       |
| <b>Unterstützte Zielsysteme</b>  |         |         |         |         |         |
| Microsoft RDSH, WTS ab 2000, RDS, RD-Freigabe, Citrix Virtual Apps und Desktops, VMware Horizon oder Webserver         | ✓       | ✓       | ✓       | ✓       | ✓       |
| <b>VPN</b>   |         |         |         |         |         |
| Anbindung an beliebiges Gateway über IPsec, OpenVPN oder https   Anbindung an genua genuscreen über IPsec              | ✓  -    | ✓  -    | ✓  -    | -  ✓    | -  ✓    |
| Weitere VPN-Clients: Cisco AnyConnect, Juniper, F5 (ggf. zusätzliche Lizenzen erforderlich)                            | ✓       | ✓       | ✓       |         |         |
| <b>Kompatibilität</b>  |         |         |         |         |         |
| Integrierter Smartcard-Reader für PKI-Karten mit CardOS 5.X und JCOP im Format ID-1 (Dienstausweis, BW-Truppenausweis) |         |         | ✓  -    | ✓  -    | -  ✓    |
| Kompatibel mit allen gängigen 64-Bit-PCs und Tablets mit x86 Architektur   | ✓       | ✓       | ✓       | ✓       | ✓       |
| UEFI Secure Boot-Unterstützung   | ✓       | ✓       | ✓       | ✓       | ✓       |
| <b>Multi-Faktor-Authentisierung</b>  |         |         |         |         |         |
| Software-Zertifikat, gekoppelt an die Hardware-ID des Sticks   Hardware-Anker   Smartcard                              | ✓  -  - | ✓  ✓  - | ✓  -  ✓ | ✓  -  ✓ | ✓  -  ✓ |
| Passwort-Eingabe am Bildschirm   Integrierte Tastatur zur PIN-Eingabe am Stick   | ✓  -    | ✓  -    | -  ✓    | -  ✓    | -  ✓    |
| <b>Sicherheit</b>  |         |         |         |         |         |
| Gehärtetes ECOS Secure Linux-Betriebssystem  | ✓       | ✓       | ✓       | ✓       | ✓       |
| Digital signierte Bootloader, Firmware und Applikationen mit Verifikation im »Chain-of-Trust«-Verfahren                | ✓       | ✓       | ✓       | ✓       | ✓       |
| Integrierte Firewall als Schutz vor Angriffen im gleichen Netz und Blockieren von Ping-Anfragen                        | ✓       | ✓       | ✓       | ✓       | ✓       |

ECOS Technology GmbH  
 Sant' Ambrogio-Ring 13 a-b  
 55276 Oppenheim Germany

+49 6133 939 200  
 info@ecos.de

www.ecos.de