Secure Boot Stick

Die hochsichere Zugriffslösung für Terminalserver, VDI und Webanwendungen

100%ige Trennung geschäftlich und privat

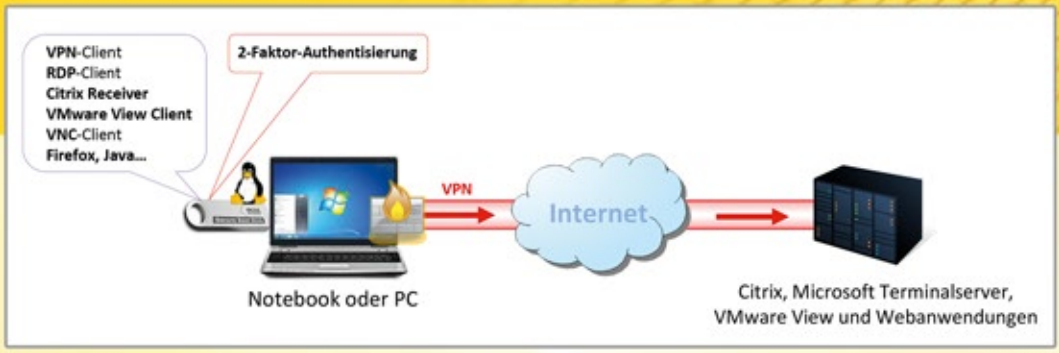
Von jedem beliebigen PC aus

- Gesicherte Umgebung
- 2-Faktor-Authentisierung
- Zentrale Konfiguration
- Alles auf dem Stick

ECOS SECURE BOOT STICK

Hochsicher ins Unternehmensnetz

Der ECOS Secure Boot Stick ermöglicht einen hochsicheren Zugang zu einer Terminalserver- oder Virtual Desktop-Infrastruktur sowie zu Webanwendungen aus einer gesicherten Umgebung heraus. Damit wird eine absolute Trennung zwischen der geschäftlichen und der privaten Nutzung des PCs sichergestellt.



Einfach	Hochsicher	Datenschutz	Günstig
- Booten vom Stick - LAN/WLAN/UMTS/LTE - Zentrale Konfiguration - Sämtliche Software auf dem Stick	- ECOS Secure Linux - Starke 2-Faktor Authentisierung - Firmware und Clients speziell gesichert - Integrierte Firewall	- Absolute Trennung, geschäftlich und privat - Lokale HD inaktiv - Ext. Datentransfer nur nach Freigabe - Instant Logout	- Einfache Integration - Easy Enrollment - Zentrales Management - Supportarm

Einfach

Nach Anschließen des Bootsticks startet der Heim- oder Fremd-PC aus einer gesicherten Linux-Umgebung. Dabei erfolgt der Zugang zum Unternehmen per LAN, WLAN, UMTS, LTE oder über Anmeldung an einem HotSpot. Ferner werden alle Sticks zentral konfiguriert, so dass der Anwender ohne Eingabe von Verbindungsparametern sofort starten kann. Für maximale Usability befindet sich auf den Sticks sämtliche Software für einen Zugriff auf eine Terminalserver- oder Virtual Desktop-Infrastruktur sowie Webanwendungen, wie z.B. OWA.

Hochsicher

Die Sicherheitsmerkmale des ECOS Secure Boot Sticks sind hierbei das speziell gehärtete ECOS Secure Linux-Betriebssystem, welches vor jeglichen Schadprogrammen schützt und die starke 2-Faktor-Authentisierung. Nach dem Prinzip „Haben und Wissen" benötigt der Anwender neben seinem persönlichen Stick auch das zugehörige Passwort zur Authentisierung. Außerdem sind Firmware und Konfiguration auf schreibgeschützten und verschlüsselten Partitionen abgelegt. Die integrierte Firewall sorgt für einen sicheren Betrieb auch in potentiell unsicheren Netzen.

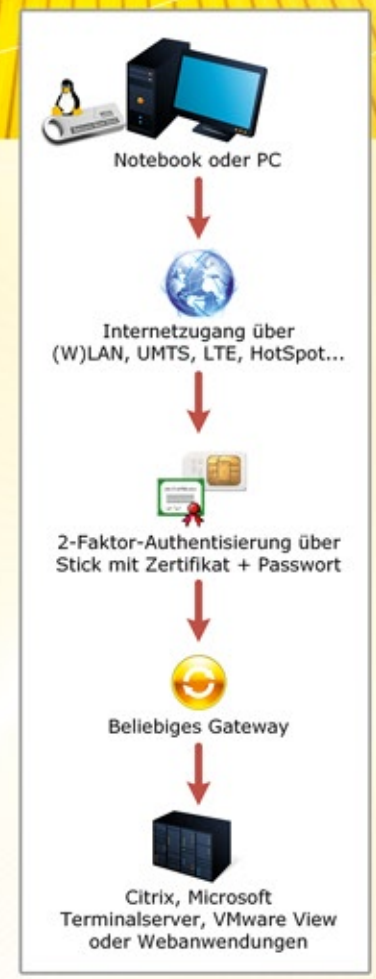
Datenschutz

Der ECOS Secure Boot Stick trennt betriebliche und private Nutzung eines PCs, indem er die lokale Festplatte erst gar nicht aktiviert. Bildlich gesprochen liegt die ganze Intelligenz auf dem Firmen-Stick und der PC dient lediglich als private Peripherie. Für den User kann externes Speichern oder Drucken von Daten nur nach expliziter Freigabe durch den Administrator verfügbar gemacht werden. Einem unbefugten Einsehen des Bildschirms beugt der Instant Logout vor. Mit Abziehen des Sticks fährt der PC in Sekundenschnelle herunter, ohne die Session zwangsweise zu beenden.

Günstig

Der ECOS Secure Boot Stick setzt auf vorhandene Backend-Systeme auf und lässt sich sehr einfach in Ihre bestehende IT-Infrastruktur integrieren. Ferner erleichtert das Easy-Enrollment den Rollout-Prozess. Hierbei erhalten alle Anwender einen baugleichen Stick, der erst nach Eingabe des individuellen Aktivierungscodes personalisiert wird. Benutzer- und Zugriffsrechte werden vom zentralen Management-Tool aus remote verwaltet. Somit vereint der ECOS Secure Boot Stick einfache Inbetriebnahme und bequeme Nutzung um den alltäglichen Supportaufwand deutlich zu minimieren.

Der ECOS Secure Boot Stick im Detail



Gesicherte Umgebung

Mit dem Booten des ECOS Secure Linux-Betriebssystems wird die lokale Festplatte und das sich darauf befindliche Windows nicht angesprochen, und damit evtl. vorhandene Viren und Trojaner nicht aktiviert. Das ECOS Secure Linux übernimmt außerdem die Hoheit über die angeschlossene Hardware, so dass eventuelle Schädlinge im BIOS oder UEFI keinen Einfluss haben.
Firmware und Client-Software befinden sich auf einer schreibgeschützten, verschlüsselten Partition und sind damit unangreifbar für eine mögliche Schadsoftware z.B. auf einer aufgerufenen Website.

Beliebiger Internetzugang

Der ECOS Secure Boot Stick bietet die notwendigen Treiber für einen Zugang über LAN, WLAN, UMTS, LTE oder HotSpot.

Sichere 2-Faktor-Authentisierung

Der ECOS Secure Boot Stick dient als starke 2-Faktor-Authentisierung. Auf den Stick befindet sich ein Zertifikat, welches an die Hardware-ID des Sticks gekoppelt ist. Optional ist der Stick auch in einer Variante mit integrierter Smartcard erhältlich.

Höchste Sicherheit – maximaler Datenschutz

Mit Einsatz des ECOS Secure Boot Sticks erfolgt eine strikte Trennung zwischen Unternehmensdaten und privaten Daten. Ferner ist es dem Anwender nicht möglich, Daten auf ein externes Speichermedium zu kopieren oder auszudrucken, ohne explizite Freigabe durch den Administrator. Auch das Erstellen von Screenshots wird wirkungsvoll verhindert.
Das Arbeiten in einer gesicherten Umgebung verhindert zudem ein Mitlesen von Bildschirminhalten, z.B. durch einen Trojaner. Ebenso wird die Ausführung in einer virtuellen Umgebung unterbunden.
Da die interne Festplatte nicht angesprochen wird, sind jegliche Spuren wie etwa Verbindungsdaten ausgeschlossen.
Durch die integrierte Firewall kann der ECOS Secure Boot Stick auch in unsicheren Umgebungen, wie z.B. WLAN Hotspots, Hotels, Internetcafés oder auch im Netzwerk eines Heimanwenders betrieben werden.

Gewohnte Arbeitsplatzumgebung

Nach dem Aufbau der Verbindung stehen alle Anwendungen und Daten des Arbeitsplatzes in gewohnter Weise zur Verfügung.

Unterstütze Zielsysteme

Der ECOS Secure Boot Stick enthält alle notwendigen Clients für einen Zugriff auf Microsoft Terminalserver (2000, 2008, 2008 R2, 2012, RDS), Citrix (XenApp, XenDesktop), VMware View und Webserver.

Nutzung lokaler Ressourcen

Berechtigungen lassen sich auf Anwender-, Gruppen- und Rollenebene für alle oder ausgewählte Geräte erteilen. Nach Freigabe durch den Administrator können Dateien aus der Session auf ein externes Speichermedium kopiert oder ausgedruckt werden.

Internationaler Einsatz

Mit Tastaturtreiber für über 50 Sprachen und Länder ist auch ein internationaler Einsatz gewährleistet. Die Benutzeroberfläche selbst ist in Deutsch und Englisch verfügbar.

Anbindung lokaler Netzwerk-Devices

Speziell für die Einrichtung von Telearbeitsplätzen lassen sich lokale IP-Telefone und Netzwerkdrucker durchrouten und somit ins Unternehmensnetz einbinden.

ECOS Secure Boot Stick

ECOS Secure Boot Stick Plus

Integration in die IT-Infrastruktur

Als Gegenstelle für den ECOS Secure Boot Stick kann ein beliebiges IPsec- oder Open-VPN-fähiges Gateway zum Einsatz kommen. Alternativ können die virtuelle ECOS System Management Appliances oder ECOS Secure Gateway Appliance als SSL-VPN-Gateway eingesetzt werden.

Easy Enrollment

Das ECOS Easy-Enrollment wurde geschaffen um den Roll-Out-Prozess zu automatisieren. Dies ermöglicht es jedem Anwender einen baugleichen Stick mit identischer Vorab-Konfiguration auszuliefern. Erst mit der Eingabe seines individuellen Aktivierungscodes wird der Stick mit den Userdaten gekoppelt und so zu seinem persönlichen ECOS Secure Boot Stick.

Remote Aktualisierung

Sobald ein neues Softwareupdate bereitsteht und vom Administrator freigegeben ist, wird dies bei der nächsten Nutzung des ECOS Secure Boot Sticks automatisch im Hintergrund geladen. Dabei erfolgt eine Verifikation des Zielservers und Integritätsprüfung des geladenen Images.

Hardwaretreiber

ECOS legt einen besonderen Schwerpunkt auf die permanente Aktualisierung der integrierten Treiber um stets sicherzustellen, dass der ECOS Secure Boot Stick in vollem Umfang mit der neuesten Hardware betrieben werden kann.

Verlorengegangene Sticks

Geht einmal ein ECOS Secure Boot Stick verloren, so wird dieser vom Administrator zentral gesperrt und die Lifetime-Lizenz auf einen bereitgestellten Ersatzstick übertragen.

Zentrale Management Appliance, VPN-Gateway und Authentisierungsserver

Die ECOS System Management Appliance dient der zentralen Verwaltung aller ECOS-Produkte. Optional kann sie auch als VPN-Gateway und Authentisierungsserver für die ECOS Secure Boot Sticks eingesetzt werden. Hierbei handelt es sich um eine virtuelle Appliance zum Betrieb unter VMware, Citrix XenServer, Hyper-V, Oracle VirtualBox oder auf zertifizierter Hardware.

Übersicht Leistungsdaten

- Gehärtetes ECOS Secure Linux
- UEFI Secure Boot Unterstützung
- Applikationen: RDP, Citrix Receiver, VMWare View, VNC-Client, NoMachine, Firefox mit Java-Unterstützung
- Unterstützte Zielsysteme: Microsoft Terminalserver (2000, 2008, 2008 R2, 2012, RDS, RDP-Freigabe), Citrix (Presentation Server, XenApp, XenDesktop), VMware View, oder Webserver
- Optional: NCP-Client, AnyConnect, ThinPrint-Client
- Integrierter IPsec- und SSL-VPN-Client
- Auch als Variante mit integrierter Smartcard erhältlich
- Integrierte Firewall
- Verbindung über Proxyserver konfigurierbar
- Zertifikatsbasierte Anmeldung am VPN-Gateway, sichere 2-Faktor-Authentisierung mit Passwort oder PIN
- Signieren, Verschlüsseln sowie Windows Smartcard Logon durch PC/SC Forwarding (ECOS Secure Boot Stick Plus)
- Mehrere Profile zum Zugriff auf unterschiedliche Applikationen/-Server auf einem ECOS Secure Boot Stick möglich
- Zentrales Management für Sticks & Zertifikate
- Benutzersynchronisation mit Active Directory oder anderen Verzeichnisdiensten möglich (in Verbindung mit SMA100/SGA)
- Lauft ab Intel Pentium 3, AMD Athlon, Mac mit Intel Prozessor

ECOS TECHNOLOGY GMBH
Sant-Ambrogio-Ring 13a
D-55276 Oppenheim

Tel: +49 (6133) 939-200
Fax: +49 (6133) 939-334
info@ecos.de

ecos