safe and smart

ECOS SecureBootStick®

Hochsicherer Fernzugriff auf Daten und Anwendungen

- **Einfach**
- **Flexibel**
- **Hochsicher**

IT-Security Solutions
Made in Germany

BSI zugelassen VS-NfD EU/NATO RESTRICTED

ECOS TECHNOLOGY

Datenfernzugriff - einfach, flexibel, hochsicher

Unsere Arbeitswelt erfordert eine zunehmende Flexibilisierung von Arbeitszeit und Arbeitsort. Die Einrichtung von Heimarbeits- oder alternierenden Telearbeitsplätzen oder mobilen Arbeitsplätzen stößt jedoch oft an Grenzen. Für abgesicherte Notebooks stehen nicht die Mittel zur Verfügung oder der administrative Aufwand ist zu groß. Private Geräte sind aus Sicherheitsgründen nicht erlaubt.

Mit wachsender Bedrohungslage steigen zudem die Anforderungen an die IT-Security enorm. Dies gilt nicht nur bei der Nutzung eigener Geräte außerhalb des Unternehmens, sondern auch bei der Anbindung externer Dienstleister und Kunden. Auch vor Bedrohungen innerhalb der realen Welt, z.B. durch Naturkatastrophen, schützen sich Verantwortliche durch die Einrichtung von Notfallarbeitsplätzen. Mit dem ECOS SECURE BOOT STICK sind Behörden, Unternehmen und Einrichtungen erstmals in der Lage, unter Berücksichtigung höchster Sicherheitsanforderungen, private und fremde PCs zuzulassen, sogar für die Bearbeitung von Dokumenten mit Geheimhaltungsgrad VS-NfD. Damit werden Administrationsaufwand und Kosten im Vergleich zu bisherigen Lösungen deutlich reduziert sowie die Anwenderzufriedenheit und vor allem die Sicherheit signifikant erhöht.

Vorteile auf einen Blick:

+ Gehärtetes ECOS Secure Linux-Betriebssystem
+ 100%ige Trennung berufliche/private Nutzung
+ Sämtliche Software auf dem Stick
+ Multi-Faktor-Authentisierung per Smartcard
+ Integrierte Firewall
+ Zentrales Management
+ Remote-Aktualisierung
+ Datensafe zur Ablage von Dokumenten*
+ BSI-Zulassung für VS-NfD, EU-/NATO RESTRICTED**

* Secure Boot Stick FX, SX, ZX
** Secure Boot Stick SX, ZX

ECOS SecureBootStick Produktfamilie

Mit dem ECOS SecureBootStick können Anwender und Anwaenderinnen innen hochsicher von einem beliebigen PC auf Daten und Anwendungen im Unternehmen oder in der Behörde zugreifen. Je nach Kunde sind die Sicherheitsanforderungen jedoch unterschiedlich hoch.

Der ECOS SecureBootStick CL bietet Kunden ein hohes Sicherheitsniveau zu einem besonders attraktiven Preis. Seit der ersten Version, welche 2007 auf den Markt kam, ist ein hohes Maß an Expertise in Sachen Sicherheit, Integration in die Infrastruktur und Hardware-Kompatibilität in dieses Produkt und seine permanente Weiterentwicklung eingeflossen.

ECOS SecureBootStick CL

Der ECOS SecureBootStick HE bringt die bewährte Lösung, dank eines speziell entwickelten hardwareverschlüsselten und mit zahlreichen Sicherheitsfeatures ausgestatteten USB-Sticks, auf ein neues Sicherheitsniveau.

ECOS SecureBootStick HE

Der ECOS SecureBootStick FX bietet, wie der HE, zahlreiche in Hardware gegossene Sicherheitsfeatures. Ergänzend verfügt er über eine integrierte Smartcard sowie eine integrierte Tastatur zur Eingabe der PIN direkt am Stick. Dabei sind sämtliche Verschlüsselungen und Prozesse über die Smartcard abgesichert.

Der ECOS SecureBootStick SX ist das Flaggschiff der Produktfamilie. Weitgehend identisch mit dem FX, verfügt der SX 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..

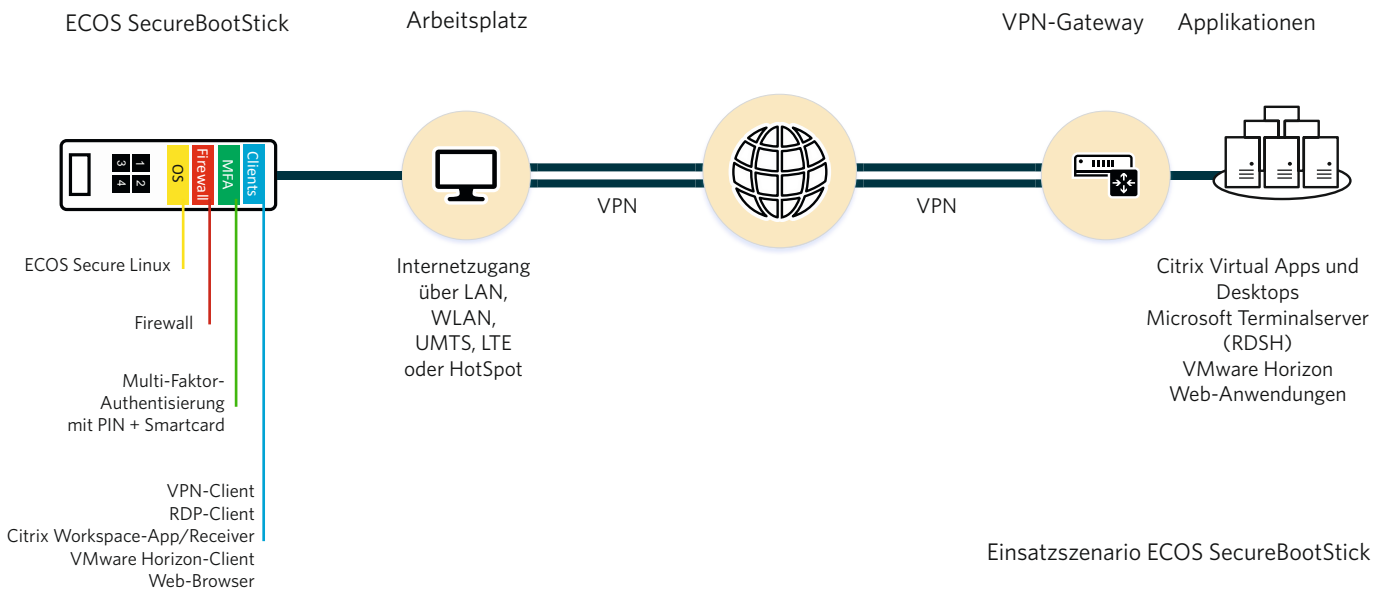
ECOS SecureBootStick FX/SX

Der ECOS SecureBootStick ZX ermöglich 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. Wie sein Pendant, hat der ZX auch die BSI-Zulassung für VS-NfD, EU-/NATO RESTRICTED.

ECOS SecureBootStick GX/ZX

Hochsicher ins Behörden-/Unternehmensnetz

Sämtliche Produkte der Secure Boot Stick Familie ermöglichen einen hochsicheren Zugang zu einer Terminalserver- oder Virtual-Desktop-Infrastruktur und Webanwendungen aus einer gesicherten und gekapselten Umgebung heraus.



Einsatzszenario ECOS SecureBootStick

Mit dem Stick bootet ein beliebiger 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.

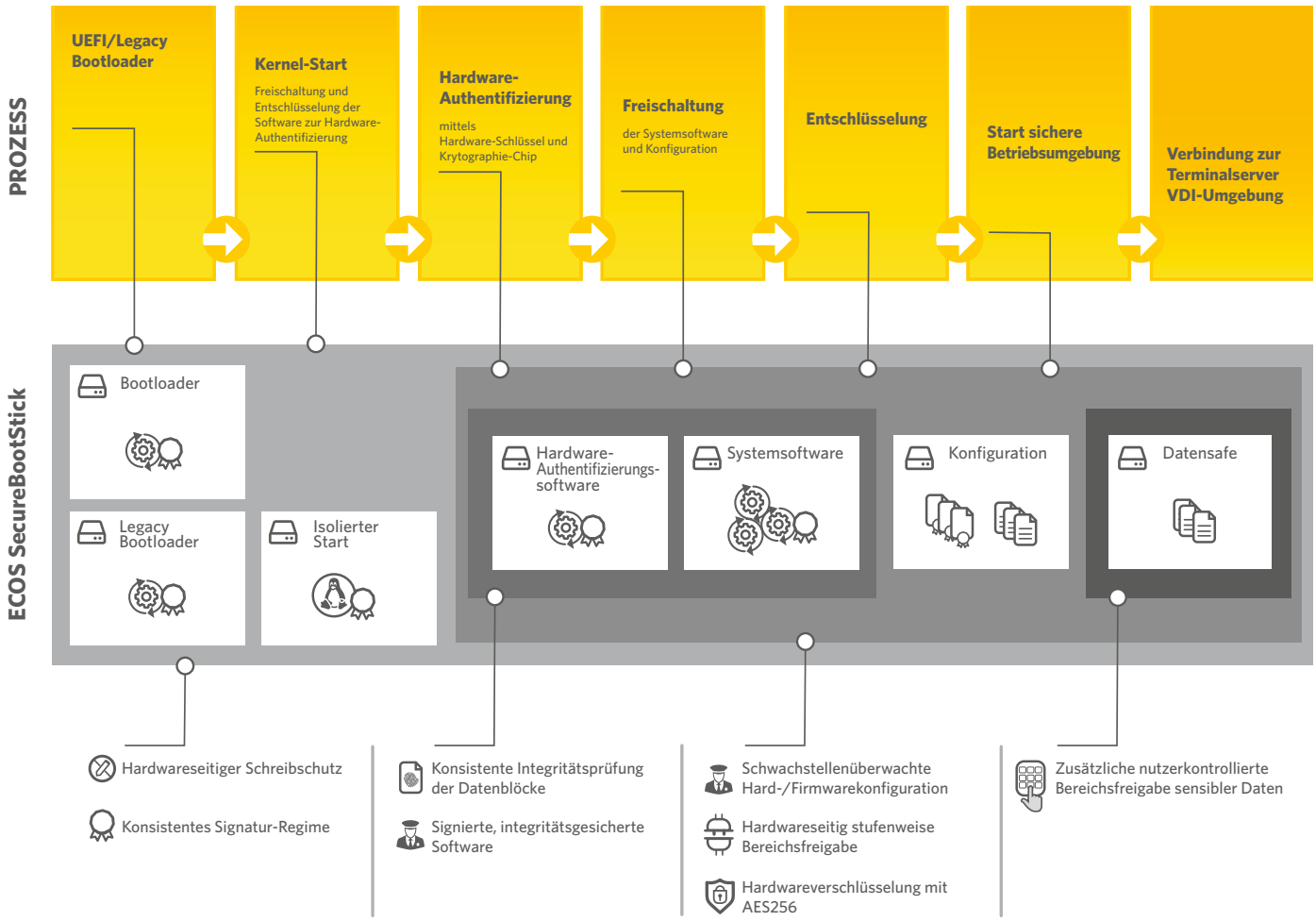
Sämtliche Software auf dem Stick

Der Stick enthält die notwendigen Clients für einen hochsicheren Zugriff auf Microsoft RDSH (ehemals Windows Terminalserver), Citrix Virtual Apps und Desktops (ehemals XenApp und XenDesktop), 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 Verwendung 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), ein Client für Juniper und F5 zur Verfügung. Für die BSI-zugelassenen ECOS SecureBootStick SX/ZX wird gemäß Einsatz und Betriebsbedingungen für VS-NfD 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 Aktivierungscodes 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, welches im Folgenden noch näher beschrieben wird, lassen sich alle Sticks zentral verwalten und remote aktualisieren.



Aufbau des ECOS SecureBootStick HE, FX, SX, ZX

Maximale Kompatibilität

Mit der Einbindung privater Endgeräte steigen die Anforderungen an die Kompatibilität. So sind auf dem Secure Boot Stick die Treiber für alle marktgängigen PCs und x86-basierten Tablets implementiert. Dies umfasst Grafiktreiber, LAN-, WLAN-, UMTS- und LTE-Treiber, sowie einen Browser zur Anmeldung am HotSpot. Für eine optimale Übertragung von Audio- und Videosignalen, im Speziellen auch in Verbindung mit Microsoft Skype for Business und Microsoft Teams, wurde die Citrix HDX RealTime Media Engine integriert. In Verbindung mit RDP sorgt Microsoft RemoteFX für eine bestmögliche Audioqualität. Für die Nutzung auf Gastrechnern im Ausland sind die Tastaturtreiber für über 90 Sprachen und Länder auf dem Stick enthalten.

Über das Forwarding von USB- und LAN-Port lassen sich lokale Drucker oder IP-Telefone anbinden. Entsprechende Rechte zum Drucken von Dokumenten werden über das zentrale Management vergeben. Auch die Unterstützung sonstiger USB-Devices wie z.B. Fußpedale für Diktiergeräte wird in gewissem Umfang unterstützt.

Aufbau des ECOS SecureBootStick

Bei der Konzeptionierung des ECOS SecureBootStickstanden höchste Sicherheitsanforderungen an erster Stelle. So unterteilt

Einsatzszenarien

Der ECOS SecureBootStick kommt bei Kunden in den verschiedensten Bereichen zum Einsatz.

Vereinbarkeit von Beruf und Familie fördern

Bei der Entscheidung für einen neuen Karriereschritt ist vielen Bewerberinnen und Bewerbern die Vereinbarkeit von Beruf und Familie wichtiger als die monetäre Vergütung der neuen Position. Dies gilt nicht nur für junge Familien, die mehr Zeit für die Betreuung und Erziehung ihrer Kinder gewinnen möchten. In Zeiten des demografischen Wandels und angesichts des Mangels an Pflegekräften spielt außerdem zunehmend die Betreuung älterer Familienangehöriger eine Rolle. Dabei soll die Karriere jedoch nicht auf der Strecke bleiben. Zusätzlich ist auch für ältere oder eingeschränkt mobile Personen eine aktive Teilhabe am Arbeitsleben besonders wichtig. Vor dem Hintergrund des akuten und vielfach beklagten Fachkräftemangels ist es also nicht verwunderlich, dass eine Flexibilisierung des Arbeitsplatzes in besonderem Maße dazu beiträgt, sich als attraktiver Arbeitgeber zu positionieren. Die Herausforderung für die IT besteht nun darin, Heim-, Tele- oder mobile Arbeitsplätze unter Einhaltung höchster Sicherheitsanforderungen zu realisieren – mit begrenzten Mitteln und möglichst minimalem Aufwand.

Maximale Flexibilität in hektischen Alltag

Manche Tätigkeiten können nicht bis zum nächsten Arbeitstag warten, auch wenn das Firmenotebook gerade im Büro liegt. Ebenso kündigen Kinder Krankheiten meist nicht 24 Stunden im Voraus an. Lösungen, welche eine Nutzung des privaten PC unter Berücksichtigung höchster Sicherheitsanforderungen ermöglichen, steigern nicht nur die Mitarbeiterzufriedenheit, sondern auch die Effizienz des Unternehmens.

Externe Mitarbeiter einbinden

Viele Behörden und Unternehmen greifen für die Erfüllung wichtiger Aufgaben regelmäßig auf die Unterstützung externer Berater und Dienstleister zurück. Vorgänge wie die Einbindung fremder Laptops ins interne Netz oder auch der externe Zugriff auf Datenbanken oder Fachanwendungen durch Dritte stellen jedoch besonders hohe Anforderungen an die IT-Sicherheit.

IT und IT-Fernwartung

Für die Wartung von IT-Infrastruktur und Fachanwendungen benötigen Spezialisten einen 24/7-Zugriff auf entsprechende Systeme. Gerade ein externer Zugriff auf kritische Systeme erfordert höchste Sicherheitsvorkehrungen. Dies gilt im Speziellen auch für externe Dienstleister, die üblicherweise ihr eigenes Notebook einbringen und eine Einbindung in lokale Netze erwarten.

Sicherer Zugriff, auch im Ausland

Die Einreisebestimmungen vieler Länder erlauben den lokalen Sicherheitsbehörden einen uneingeschränkten Zugriff auf mitgeführte Notebooks und Speichermedien. Mögliche Verschlüsselungen müssen auf Verlangen zur Einsicht oder zum Kopieren der Daten offengelegt werden. Daher dürfen in vielen Unternehmen Notebooks nur noch mitgeführt werden, sofern sie frei von jeglichen Daten und Dokumenten sind. Trotz dieser Vorgaben besteht jedoch weiterhin die Notwendigkeit, von unterwegs auf wichtige Daten zugreifen zu können.

Flexible Arbeitsplätze für Notfälle bereithalten

In Zeiten zunehmender Wetterextreme oder für sonstige unvorhersehbare Ereignisse müssen Behörden und Unternehmen Vorkehrungen treffen, um einen Notbetrieb aufrecht zu erhalten, auch wenn für die Mitarbeiter der Weg zum Arbeitsplatz versperrt ist. Statt unnötiger Ausfallzeiten oder kostspieliger Notfallbüros bietet sich ein Arbeiten vom heimischen PC an, sofern entsprechende Anforderungen an IT-Sicherheit und Datenschutz Berücksichtigung finden.

VS-NfD, EU-/NATO restricted am handelsüblichen PC

Bundesbehörden, Bundeswehr und geheimschutzbetreute Unternehmen kennen die Anforderung seit Langem. Im Bereich KRITIS und weiterer sicherheitsrelevanter Unternehmen werden sie zunehmend eingeführt. Die Bearbeitung VS-NfD, EU-/NATO RESTRICTED eingestufter Dokumente erfordert den Einsatz BSI-zugelassener Endgeräte. Das gilt nicht nur für die Verwaltung, sondern auch für die Softwareentwickler oder Ingenieure. Solche Lösungen in Form eines gehärteten Notebooks sind aber nicht immer zur Zufriedenheit der Anwender*innen und selten zur Zufriedenheit des Finanzcontrollings. Mit dem BSI-zugelassenen ECOS SecureBootStick SX/ZX wird es erstmals möglich: ein Zugriff auf VS-NfD, EU-/NATO RESTRICTED von einem handelsüblichen PC.

sich der Stick in mehrere Partitionen, welche im Boot-Prozess sukzessive durch die jeweils vorangehende Sicherheitsprüfung bzw. Authentisierung freigeschaltet werden.
Die Partitionen für Bootloader, Firmware und Applikationen sind schreibgeschützt, was ab der Modellvariante HE über einen hardwareseitigen Schreibschutz realisiert wird. Darüber hinaus sind sämtliche Bereiche des Sticks ab dem Bootloader durchgängig verschlüsselt. Hierbei handelt es sich um eine AES-256-Bit-Verschlüsselung, bei CL ausgelegt als Software-Verschlüsselung, bei allen anderen Produktvarianten als Hardware-Verschlüsselung. Die ECOS SecureBootStick FX/SX/ZX verfügen zudem über einen Datensafe zur Ablage von Dokumenten. Dieser ist als separates Hardware-verschlüsseltes Laufwerk ausgelegt, abgesichert per Smartcard und PIN-Eingabe.

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.

Absicherung per Smartcard

Der ECOS SecureBootStick FX und SX verfügen jeweils über einen integrierten Smartcard-Reader für Smartcards im SIM-Karten-Format ID-000. Smartcard und Stick dienen damit als Besitzkomponente für eine starke Multi-Faktor-Authentisierung. Die Verschlüsselung des Sticks sowie sämtliche Prozesse sind per Smartcard abgesichert: vom Rollout über die Anmeldung am Gateway bis hin zur Aktualisierung des Sticks.

Per PC-/SC-Forwarding lässt sich die Smartcard für weitere Funktionen nutzen, z.B. zum Signieren, Verschlüsseln oder Windows-Smartcard-Logon. In der Ausprägung ZX verfügt der Stick über einen Kartenslot für die Nutzung von PKI-Karten und Ausweisen im Format ID-1.

Datensafe

In den Produktvarianten FX/SX/ZX steht dem Anwender ein hardwareverschlüsselter Datensafe zur Verfügung, welcher für die sichere Ablage von Dateien auf dem Stick genutzt werden kann.
Damit können z.B. Daten aus einer VDI-Session heraus – eine entsprechende Berechtigung vorausgesetzt – auf dem Stick gespeichert werden, um diese offline zu bearbeiten. Unter laufendem Betriebssystem kann der Datensafe, unter Vorhandensein der Smartcard und Eingabe der PIN, wie ein normaler Speicherstick genutzt werden.

Datenschutz

Vor unbefugtem Einsehen des Bildschirms schützt ein spezieller Instant-Logout-Prozess. Mit Abziehen des Sticks fährt der PC in Sekundenschnelle herunter. Abhängig von dem eingestellten Timeout kann der Anwender nach erneutem Aufbau der Verbindung an gleicher Stelle weiterarbeiten. Mit seiner Multi-Faktor-Authentisierung, der granularen Rechtevergabe, der Vermeidung jeglicher lokaler Datenspeicherung, dem Ausschluss von Trojanern und der gesicherten VPN-Verbindung erfüllt der ECOS SecureBootStick alle technischen Anforderungen gemäß Art. 32 DSGVO sowie dem BSI-Grundschutz.
Für Mitarbeiter welche ihr privates Gerät nutzen, ist der Schutz ihrer Daten sichergestellt. Mit dem Abschalten der internen – privaten – Festplatte, wird ein Administrator niemals die Möglichkeit haben, auf private Fotos oder E-Mails auf dem Rechner zuzugreifen.

Einfach und flexibel für Anwender

Die Nutzung des Secure BootS tick ist für die Anwender denk-

Sicherheitskonzept

Der ECOS SecureBootStick zeichnet sich durch eine Kaskadierung zahlreicher Sicherheitsmaßnahmen aus, welche in Summe für ein extrem hohes Sicherheitsniveau sorgen. Die folgende Sicherheitsbetrachtung listet mögliche Bedrohungsszenarien auf und zeigt mit welchen Maßnahmen ein Angriff verhindert wird.

Schutz vor infiziertem PC

Durch das Booten des (Gast-)PC aus einer gekapselten und gehärteten Linux-Umgebung heraus wird eine mögliche Schadsoftware auf der internen Festplatte nicht aktiviert. Zusätzlich übernimmt das ECOS Secure Linux-Betriebssystem die Hoheit über die angeschlossene Peripherie (Maus, Tastatur, Grafikkarte, Netzwerkkarte...), so dass selbst eine Schadsoftware im BIOS oder im UEFI keine Bedrohung darstellt.

Schutz vor unberechtigter Nutzung

Als Grundlage für eine sichere Authentifizierung der Anwender dient eine starke Multi-Faktor-Authentisierung. So erfordern die Anmeldung am Gateway oder der Zugriff auf den Datensafe nicht nur das Wissen um das persönliche Passwort oder die persönliche PIN, sondern auch den zugehörigen ECOS SecureBootStick bzw. je nach Produktvariante, auch die zugehörige Smartcard.

Schutz vor Manipulation

Der ECOS SecureBootStick verfügt über zahlreiche Maßnahmen als Schutz vor einer möglichen Manipulation. Zum einen befinden sich Firmware und Applikationen auf einer schreibgeschützten Partition. Darüber sind der Bootloader, der Kernel und alle Applikationen digital signiert. In einer »Chain of Trust« überprüfen diese sich gegenseitig durch einen sich permanent wiederholenden Prozess. Jegliche Manipulation des Filesystems oder der Austausch von Codeteilen macht den Stick sofort unbrauchbar und führt im laufenden Betrieb zu einem unmittelbaren Shutdown des Rechners. Damit wird jegliche Manipulation wirkungsvoll verhindert.

Schutz vor Spionage

Die Verbindung zwischen dem Endgerät und dem Gateway erfolgt auf Basis einer gesicherten VPN-Verbindung, welche erst nach der erfolgreichen Authentisierung aufgebaut wird. Als Schutz vor möglichen Trojanern auf Websites, z.B. bei der Anmeldung an einem HotSpot, befinden sich sämtliche relevanten Teile der Firmware auf einer schreibgeschützten Partition. Dies verhindert, zusätzlich zu der zuvor aufgeführten »Chain of Trust«, eine Manipulation des Betriebssystems.

Gezielte Angriffe unter Ausnutzung des System Management Modes werden durch den Secure Boot Stick mehrfach abgewehrt. So erfolgt im frühen Boot-Prozess eine Überprüfung des BIOS oder UEFI auf mögliche Schadsoftware . Für besonders sicherheitsrelevante Behörden und Unternehmen lässt sich (ab Version 7, verfügbar ab Januar 2020) bei der ersten Inbetriebnahme ein Fingerprint des Rechners erstellen. Jegliche Veränderung des genutzten PC muss damit vom Administrator autorisiert werden. Damit werden sowohl Manipulationen am BIOS/UEFI wie auch an der Hardware erkannt. Auch hardwareseitige Angriffe, welche z.B. auf das Auslesen von Schlüsselmaterial aus dem Hauptspeicher zielen, werden durch die an vielen Stellen eingesetzte Verschlüsselung verhindert.

Schutz vor Online-Angriffen

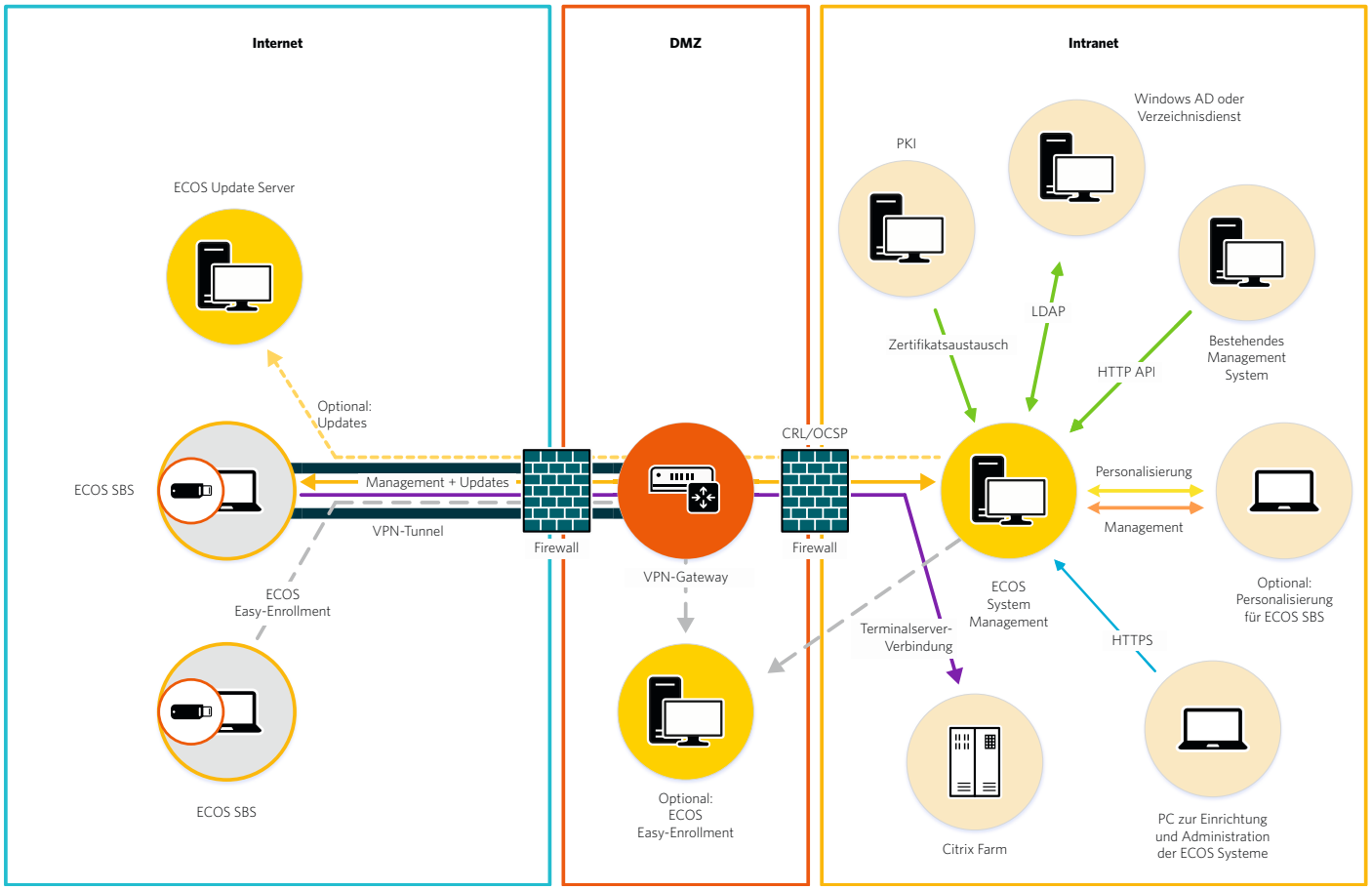
Das ECOS Secure Linux-Betriebssystem stellt ein sehr schlankes System dar, welches nur diejenigen Komponenten umfasst, die zum Betrieb der Lösung benötigt werden. Damit wird das Potential möglicher Sicherheitslücken deutlich reduziert. Zudem wurde das Betriebssystem speziell gehärtet und eigens kompiliert, so dass es höchsten Sicherheitsanforderungen gerecht wird. Der ECOS SecureBootStick verfügt über eine eigene Firewall als Schutz vor Angriffen aus dem gleichen Netz, sei es durch Hacker oder über einen infizierten PC. Diese blockiert zudem sämtliche TCP/IP- und Ping-Anfragen, sodass ein möglicher Angreifer, zum Beispiel im Hotel oder im ICE, wo man sich mit fremden Nutzern im selben Netz befindet, den Rechner erst gar nicht aufspüren kann.

Schutz vor Aushebelung durch Anwender

Vor Ausführung der Firmware erfolgt eine Prüfung, ob der Stick in einer virtuellen Maschine gebootet wurde. Dies verhindert das Untergraben vorhandener Schutzmaßnahmen, beispielsweise einem Keylogger oder Trojaner, welcher auf dem Hostsystem Bildschirminhalte oder Tastaturanschläge protokolliert.

Schutz vor manipulierten Updates

Sobald vom Stick aus eine Verbindung zum zentralen Management besteht, erfolgt eine Prüfung auf mögliche Updates und Berechtigung seitens des Anwenders. Liegen diese vor, so wird im Hintergrund ein neues Image geladen. Dabei wird sowohl der richtige Ursprung als auch die Integrität des Update-Images verifiziert. Nach erfolgreichem Download und Verifikation wird beim nächsten Booten des Sticks das neue Image ausgeführt.



Integration in die vorhandene Infrastruktur am Beispiel des ECOS SecureBootStick CL/HE

bar 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.

Wirtschaftlichkeitsbetrachtung

Gemäß ECOS Kunden ergibt sich in der Gesamtkostenkalkulation mit dem ECOS SecureBootStick ein Einsparungspotential von bis zu 80% im Vergleich zur Ausgabe von entsprechenden Behörden-/Firmennotebooks. Dies beruht zum einen auf den deutlich geringeren Investitionen und den niedrigeren Betriebskosten, zum anderen auf dem deutlich reduzierten Supportaufwand.

Individualisierung

Über die mitgelieferten Vorlagen lässt sich das User-Interface des ECOS SecureBootStick flexibel an das eigene CI anpassen. Darüber hinaus können sowohl die Sticks, als auch die Smartcards mit dem eigenen Logo bestückt werden.

ECOS SystemManagementLAppliance (SMA)

Mit der ECOS SystemManagementAppliance lassen sich alle ECOS Zugangslösungen zentral verwalten und remote aktualisieren. Hierbei handelt es sich um eine virtuelle Appliance, lauffähig unter VMware, Microsoft Hyper-V, Citrix Hypervisor, Oracle Virtualbox, Linux KVM oder auf dedizierter Hardware. Der Betrieb der Appliance erfolgt in der DMZ oder im internen Netz.

Zentrale Benutzer- und Rechteverwaltung

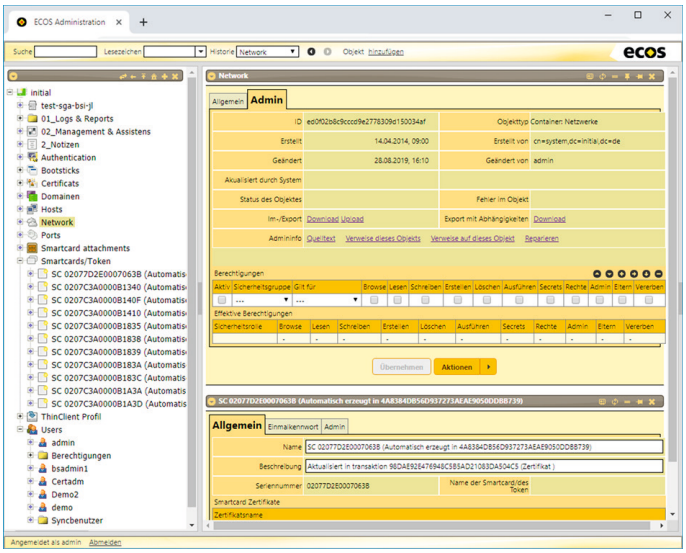
Für den Zugriff auf eine WTS- oder VDI-Umgebung oder auch auf Webanwendungen lassen sich Profile anlegen, welche den Anwender*innen nach dem Starten der Anwendung zur Auswahl stehen. Die Verwaltung der Zugriffsrechte erfolgt auf Benutzer-, Gruppen- und Rollenebene. Es können pro User beliebig viele Profile angelegt werden, welche sich sowohl remote freigeben als auch remote entziehen lassen. Über die Rechteverwaltung lassen sich zudem die Nutzung lokaler Drucker sowie die Freigabe angeschlossener USB-Speichermedien für den Datentransfer mit einer WTS- oder VDI-Session sehr granular festlegen. So kann die Freigabe eines externen Devices sowohl an die Vendor-ID als auch die Seriennummer des Gerätes gekoppelt werden.

Steuerung über AD

Mit der Kopplung an Active Directory oder einen sonstigen Verzeichnisdienst lassen sich Benutzer und Rechte synchronisieren, auch mit mehreren Verzeichnisdiensten. Mit der Kopplung wird sogar eine Fernsteuerung der SMA aus dem AD heraus möglich. So kann z.B. über die Zuordnung eines Nutzers in eine bestimmte Gruppe im AD, das Ausstellen eines Aktivierungscodes angetriggert oder entsprechende Rechte zugewiesen werden.

Zertifikatsverwaltung

Die Appliance beinhaltet eine eigene CA zum Ausstellen von Zertifikaten. Alternativ erlaubt sie auch die Verwendung vorhandener Zertifikate über eine Kopplung an eine bestehende



ECOS System Administration Interface

PKI. Bei der Verwendung von Smartcards lassen sich Zertifikate über die SMA direkt auf der Smartcard generieren. Die Validierung der Zertifikate kann entweder über eine CRL oder den in der SMA integrierten OCSP-Dienst erfolgen.

Zertifikatsverlängerung

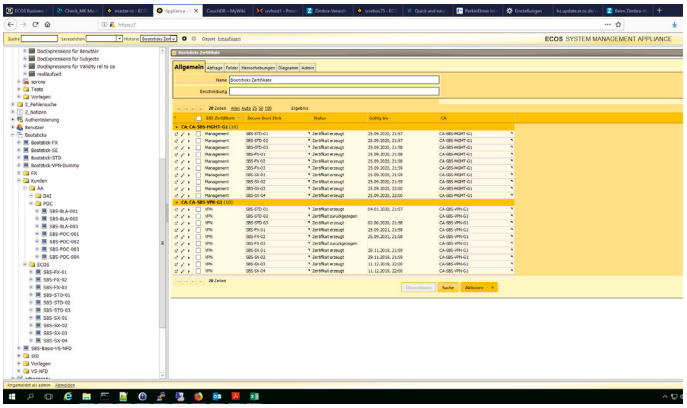
Auch das Verlängern von Zertifikaten wird von der SMA übernommen und kann vollautomatisch ohne Eingriff des Administrators oder Benutzers im Hintergrund erfolgen, gleich ob es sich um ein Softwarezertifikat handelt oder ob das Zertifikat auf der Smartcard gespeichert ist.

Mandantenfähigkeit

Mit der ECOS SystemManagementAppliance lässt sich ein komplexes Mandantenmodell abbilden. So können für sämtliche Mandanten getrennte Admin-Logins, AD-Anbindungen, PKI-Anbindungen und getrennte CAs konfiguriert werden.

Update-Server

Die ECOS SMA dient als zentraler Update-Server für alle ECOS SecureBootStick. Nach dem Download einer neuen Softwarever-



Zertifikatsverlängerung

sion, was ggf. über ein zweites Evaluationssystem erfolgen kann, erfolgt die Bereitstellung an einzelne Personen, Gruppen oder an alle Anwender*innen. Damit lassen sich etablierte Rolloutprozesse in der SMA einfach abbilden.

Report-Editor und Active Reports

Zusätzlich zu einer breiten Auswahl vordefinierter Reports, lassen sich über den integrierten Report-Editor beliebige Auswertungen erstellen und für den weiteren Abruf abspeichern. Darüber hinaus ermöglichen Active Reports einen zeitgesteuerten vollautomatischen Versand erstellter Berichte, sowohl an zuständige Empfänger, als auch an alle im Bericht aufgeführten Anwender*innen. So können z.B. Anwender vollautomatisch über eine anstehende Zertifikatsverlängerung informiert werden.

Admin-Interface

Die Bedienung der SMA erfolgt über eine Web-basierte Oberfläche. Über die User-spezifische Rechtevergabe lassen sich die Rollen und damit verbundenen Zugriffsrechte abbilden.

Schnittstellen

Die Appliance erlaubt eine vollständige Integration in die vorhandene IT-Infrastruktur. So lassen sich über die HTTP-Schnittstelle sämtliche Funktionen der Appliance fernsteuern. Für die Anbindung an ein bestehendes Monitoring- oder Reporting-System stehen eine SNMP- sowie eine SysLog-Schnittstelle zur Verfügung. Darüber hinaus ermöglicht die SMA die Anbindung an das AD oder sonstige Verzeichnisdienste, sowie die Anbindung an eine vorhandene PKI.

Hochverfügbarkeit

In Verbindung mit dem ECOS HA-Modul lässt sich die Appliance als Hochverfügbarkeitslösung auslegen. Diese unterstützt sowohl unterschiedliche Internetanbindungen als auch eine Clusterung getrennter Standorte. Dies ist besonders dann von Wichtigkeit, wenn die SMA als VPN-Gateway betrieben wird. In Verbindung mit einem VPN-Gateway eines Drittherstellers empfiehlt sich eine redundante Auslegung der SMA, sofern der integrierte OCSP-Dienst zur Validierung der Zertifikate genutzt wird, z.B. zur Anmeldung am Gateway.

ECOS Up-to-date Service und 3rd Level Support

ECOS stellt in regelmäßigen Abständen Updates für den Secure Boot Stick und die System Management Appliance bereit.
Dies umfasst aktuelle Hardwaretreiber für neue PCs, die Aktualisierung sämtlicher Applikationen, auch die von Drittherstellern, sowie die Erweiterung um neue Funktionen und Security-Features. In dem Up-to-date-Service ist auch der Zugriff auf den 3rd Level Support bereits enthalten. Die begleitenden Release-Notes enthalten sämtliche Informationen über Änderungen und Features der jeweiligen Version.

ECOS 1st Level Support

Für die Unterstützung der Anwender*innen bei der Einrichtung ihres ECOS SecureBootStick bietet ECOS den 1st Level Support an. Dieser umfasst die Unterstützung bei der Umstellung der Boot-Reihenfolge zum Booten von USB, Fragen zur Konfiguration des WLAN, Einstellungen von Maus, Tastatur oder Monitor sowie mögliche sonstige Fragen in Verbindung mit der Nutzung des Sticks bis zum Zugriff auf die eigene Infrastruktur.

Funktionsübersicht ECOS SecureBootStick	CL	HE	FX	SX	ZX
BSI-Zulassung					
Zugelassen für die Verarbeitung von Daten bis zum Geheimhaltungsgrad VS-NfD, EU-/NATO RESTRICTED				√	√
Applikationen					
RDP-Client, Citrix Workspace App, VMware Horizon (per RDP, PCoIP, BLAST), Firefox, Chromium, VPN-Client für IPsec	√	√	√	√	√
Citrix HDX RealTime Media Engine zur Optimierung der Audio- und Video-Übertragung bei Skype for Business und Microsoft Teams	√	√	√	√	√
Microsoft Remote FX zur Optimierung der Audio-Qualität in Verbindung mit RDP	√	√	√	√	√
Unterstützte Zielsysteme					
Microsoft RDSH, WTS ab 2000, RDS, RD-Freigabe, Citrix Virtual Apps und Desktops, VMware Horizon oder Webserver	√	√	√	√	√
VPN					
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)	√	√	√		
Administration					
Profile zum Zugriff auf unterschiedliche Applikationen/Server auf User-, Gruppen- oder Rollen-Ebene	√	√	√	√	√
Nutzung lokaler Ressourcen nach Freigabe (Datensafe, externe USB-Speicherdevices, lokale Drucker)	√	√	√	√	√
Berechtigungsvergabe für externe Geräte gebunden an die Hersteller-ID oder die Seriennummer des Geräts	√	√	√	√	√
Remote-Aktualisierung sämtlicher Applikationen und Firmware	√	√	√	√	√
Kompatibilität					
Integrierter Smartcard-Reader für PKI-Karten mit CardOS 5.X im Format ID-1 (Dienstausweis, BW-Truppenausweis)			√ | -	√ | -	- | √
Kompatibel mit allen gängigen 64-Bit-PCs, weitgehend mit Intel-basierten Macs und Tablets mit x86 Architektur	√	√	√	√	√
UEFI Secure Boot-Unterstützung	√	√	√	√	√
Tastaturtreiber für mehr als 90 Sprachen und Länder	√	√	√	√	√
Multi-Monitor-Support	√	√	√	√	√
Verbindung per LAN, WLAN, UMTS, LTE inkl. Browser zur Anmeldung am HotSpot	√	√	√	√	√
Software in Deutsch und Englisch (voreinstellbar)	√	√	√	√	√
Datensafe					
2 GB, nutzbar zur Ablage von Dokumenten (nicht für VS-NfD)			√	√	√
Hardwareverschlüsselung mittels AES256, abgesichert per Smartcard plus PIN			√	√	√
Installationsfreie Nutzung als USB-Laufwerk unter Windows, Linux und Mac OS X			√	√	√
Weitere Funktionen					
Signieren, Verschlüsseln oder Windows Smartcard-Logon durch PC-/SC-Forwarding			√	√	√
Forwarding externer USB- und LAN-Devices, z.B. für den Anschluss eines IP-Telefons	√	√	√	√	√
Automatischer Reconnect bei Abbruch oder Wechsel der Verbindung	√	√	√	√	√
Multi-Faktor-Authentisierung					
Software-Zertifikat, gekoppelt an die Hardware-ID des Sticks | Hardware-Anker | Smartcard	√ | - | -	√ | √ | -	√ | - | √	√ | - | √	√ | - | √
Passwort-Eingabe am Bildschirm | Integrierte Tastatur zur PIN-Eingabe am Stick	√ | -	√ | -	- | √	- | √	- | √
Sicherheit					
Schreibgeschützte Partitionen | signierte Partitionen für Bootloader und Kernel	- | √	√ | √	√ | √	√ | √	√ | √
Verschlüsselung sämtlicher sicherheitsrelevanter Partitionen via Software | Hardware	√ | -	- | √	- | √	- | √	- | √
Schreibgeschützte und signierte Partition für Firmware und Applikationen	√	√	√	√	√
Beschreibbare Partition zur Ablage der User-Parameter	√	√	√	√	√
Gehärtetes ECOS Secure Linux-Betriebssystem	√	√	√	√	√
Digital signierte Bootloader, Firmware und Applikationen mit Verifikation im »Chain-of-Trust«-Verfahren	√	√	√	√	√
Absicherung sämtlicher Prozesse per Smartcard wie z.B. Easy-Enrollment, Anmeldung am Gateway, Aktualisierung des Sticks			√	√	√
Integrierte Firewall als Schutz vor Angriffen im gleichen Netz und Blockieren von Ping-Anfragen	√	√	√	√	√
Verschlüsselung der RAM-Inhalte bis auf den auszuführenden Programmcode	√	√	√	√	√
Verhinderung der Nutzung in einer virtuellen Umgebung	√	√	√	√	√
Fingerprinting des Gastrechners inkl. Peripherie (ab V7)	√	√	√	√	√
Instant-Logout beim Abziehen des Sticks	√	√	√	√	√
Abgesicherter Prozess zur Aktualisierung von Firmware und Applikationen mit Prüfung auf Integrität und auf korrekten Update-Server	√	√	√	√	√
Anschluss, Abmessungen und Lieferumfang					
USB-Anschluss A | C	√ | - | -	√ | - | -	√ | √ | √	√ | √ |√	√ | √ | √
Abmessungen (BxHxT)	12x22x4	12x41x4	28x85x13	28x85x13	28x85x14
Gewicht (g)	3	6	68	68	72
Stick | Trageband | 2 Anschlusskabel für USB A und C	√ | √ | -	√ | √ | -	√ | √ | √	√ | √ | √	√ | √ | √

Funktionsübersicht ECOS SystemManagementAppliance (SMA)

Zentrales Management aller ECOS-Produkte	
Benutzer- und Rechteverwaltung auf Benutzer-, Gruppen- und Rollen-Ebene	√
Berechtigungsvergabe auf Zielsysteme bei verteilten Servern	√
Freigabe lokaler Devices wie Speichermedien und Drucker	√
Remote-Vergabe und -Entzug von Rechten	√
Integration in die vorhandene Infrastruktur	
Virtuelle Appliance zum Betrieb unter VMware, Citrix Hypervisor, Microsoft Hyper-V, Oracle VM VirtualBox oder auf einer dedizierten Hardware	√
Synchronisation mit AD oder sonstigen Verzeichnisdiensten	√
Steuerung aller Funktionen des System Management über HTTP-API möglich	√
Zertifikatsverwaltung	
Integrierte CA (Certificate Authority)	√
Alternativ: Anbindung an eine vorhandene PKI	√
Ausrollen von Zertifikaten auf Smartcards	√
Bereitstellung einer CRL oder eines OCSP-Servers	√
Zentrale Passwort-Policy	√
Smart Reports	
Vordefinierte Reports	√
Report-Editor	√
Active Reports	√
Token LifeCycle Management	
Easy-Enrollment	√
Zentrales Erstellen und Sperren von Zugängen	√
Distribution an einzelne User, Gruppen oder alle User	√
Remote-Aktualisierung der Zugangslösungen	
Zentraler Update-Server als Teil der SMA	√
Distribution an einzelne User, Gruppen oder alle User	√
Mandantenverwaltung	
Getrennte Admin-Logins	√
Getrennte AD-Anbindung	√
Getrennte PKI-Anbindung	√
Getrennte CAs	√
Admin-Interface	
Web-basiert	√
User-spezifische Rechtevergabe (Super-Admin, Admin, Helpdesk, Personalverwaltung...)	√
Schnittstellen	
HTTP-API, LDAP, SysLog, SNMP	√
Integriertes VPN-Gateway (IPsec, SSL-VPN) und Authentisierungsserver	
unbegrenzte Anzahl VPN-User	√
unbegrenzte Anzahl VPN-Tunnel	√
Sonstiges	
Redundant und hochverfügbar in Verbindung mit HA-Modul	√
Lieferumfang	
ISO-Image mit vorkonfiguriertem ECOS Secure Linux und ECOS SystemManagementAppliance	√
Smartcard Reader (Professional-X und Enterprise-X)	√

Lizensierung

SMA100 ECOS SystemManagementAppliance [Starter]	bis 99 User
SMA110 ECOS SystemManagementAppliance [Professional]	bis 999 User
SMA120 ECOS SystemManagementAppliance [Enterprise]	ab 1.000 User
SMA111 ECOS SystemManagementAppliance [Professional-X] für SBS FX, SX, ZX	bis 999 User
SMA121 ECOS SystemManagementAppliance [Enterprise-X] für SBS FX, SX, ZX	ab 1.000 User

ecos

safe and smart

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

+49 6133 939 200
info@ecos.de

www.ecos.de

Diese Broschüre wird CO_2-neutral hergestellt.

146.PB_SBS-ALL.2023/02.DE.01.6