WHITEPAPER

Fernzugriff auf zentrale Daten und Anwendungen

- **Sicherheitsanforderungen**
- **Datenschutz**
- **Lösungen**

Stand: 23.02.2015

WHITEPAPER

Inhalt

www.ecos.de

ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

WHITEPAPER

Fernzugriff auf zentrale Daten und Anwendungen

Beim Fernzugriff auf zentrale Daten und Anwendungen werden hohe Anforderungen an Datenschutz und Datensicherheit gestellt. Das Bundesdatenschutzgesetz (BDSG) spricht davon, dass der „Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht“. Dies gilt im Besonderen, wenn von unterwegs oder vom Homeoffice aus auf personenbezogene Daten zugegriffen wird, zumal Vorstände, Geschäftsführer oder Büroleiter in dem Fall für Datenschutzverletzungen persönlich haftbar gemacht werden können.

Die nachfolgende Ausarbeitung gilt für privatwirtschaftliche Unternehmen, öffentliche und kirchliche Einrichtungen in gleichem Maße.

www.ecos.de
ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

► Klassifizierung nach Sicherheitsstufe

Für eine Planung der zu treffenden Sicherheitsmaßnahmen ist es wichtig, eine möglichst realistische, sicherheitsrelevante Einschätzung der zu bearbeitenden Daten und Dokumente vorzunehmen. Die folgende Tabelle soll einen Anhaltspunkt für eine mögliche Einschätzung liefern. Sie stellt jedoch keine juristisch belastbare Klassifizierung dar, da die Einstufung der einzelnen Daten von Unternehmen zu Unternehmen verschieden sein kann.

Es macht auch keinen Unterschied, ob ein Zugriff auf Dateiebene, über eine Terminalserver- oder Virtual-Desktop-Infrastruktur oder über ein Webportal erfolgt.

	Sicherheitsklasse		
	normal	**mittel – hoch**	**hoch – sehr hoch**
IT-Systeme	CMS Intranet	CRM ERP	Interne Verfahren IT-Systeme
Kommunikation	Korrespondenz Marketing & PR	Konstruktionszeichnungen Ausschreibungen Angebote	Patentanträge Finanzberichte E-Akte Prozessakten
Personen-bezogene Daten	Adressdaten Telefonnummern	Einkommen Sozialleistungen Religionszugehörigkeit Schuldnerdaten	Psychologische Gutachten, Prozessakten Meldedaten Patientendaten Strafregister Kontodaten

ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

► Angemessene Schutzmaßnahmen

Schutzklasse: normal

Für den Zugriff auf Daten, die keiner höheren Sicherheitsklasse unterliegen, ist eine reine 2-Faktor-Authentisierung eventuell ausreichend. Nach dem Prinzip Wissen und Besitz, wird für eine erfolgreiche Authentifizierung, neben dem Wissen um das Passwort, auch der Besitz einer weiteren Komponente, wie z.B. ein OTP-Token oder das persönliche Handy vorausgesetzt. Sollten Zugangsdaten in falsche Hände geraten, z.B. über einen Keylogger auf dem genutzten PC oder ein unzureichend komplexes Passwort, so könnte ohne 2-Faktor-Authentisierung ein Fremder Zugang zu den gleichen Daten erlangen, wie der berechtigte Mitarbeiter.

Derzeit wird die Gefahr durch Keylogger oftmals unterschätzt. Dabei kursieren im Internet zahlreiche Anleitungen mit denen sogar minderjährige, sogenannte „Skript-Kiddies“, in der Lage sind einen Trojaner zu erstellen der von aktuellen Virenscannern nicht erfasst wird. Die passenden Test-Plattformen werden praktischerweise auch gleich im Internet angeboten.

Wie wichtig solche Schutzmaßnahmen sind, zeigt die Tatsachen, dass große Portalanbieter wie Google, Facebook oder Apple, für Premium-Zugange bereits eine entsprechende Absicherung anbieten oder vorschreiben.

ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

Schutzklasse: mittel – hoch

Für den Zugriff auf Daten der Schutzklasse mittel – hoch, ist eine reine 2-Faktor-Authentisierung nicht mehr ausreichend. Sie bietet zwar, in Verbindung mit einem Firmen-PC, einen wirkungsvollen Schutz vor einem unberechtigten Zugang zu Daten und Anwendungen. Kommen jedoch private oder Gast-PCs zum Einsatz oder werden Firmen-Notebooks auch privat genutzt, so ist der Schutz nicht mehr ausreichend. Gleiches gilt für die Nutzung eines Firmennotebooks zuhause im (W)LAN, im Hotel oder an einem öffentlichen HotSpot. Hier gilt es zwei Gefahrenquellen abzusichern.

Eine Schadsoftware könnte auf dem genutzten Gerät eine bestehende VPN-Verbindung nutzen, um zentrale Systeme anzugreifen. Selbstverständlich verfügt jeder PC über eine Antivirensoftware und auch auf dem Privat-PC sind stets die aktuellen Updates und Virensignaturen installiert. Bei einer Erkennungsrate von 93,1 – 99,7 %[1)] und 315.000[2)] neuen Bedrohungen pro Tag, ergibt sich jedoch ein erhebliches Restrisiko, ganz zu schweigen von dem Risiko einer Zero-Day Attacke. Im Februar 2013 hatten Häcker es geschafft, einen Trojaner auf der Seite Sparkasse.de zu platzieren. Für das Aufrufen einer Bankseite dürfte einem Mitarbeiter wohl schwerlich ein fahrlässiges Verhalten vorzuwerfen sein. Um diese Gefahr abzuwehren, sollte für den Verbindungsaufbau keine klassische, sondern eine ausschließlich applikationsbasierte VPN-Verbindung zum Einsatz kommen, die exklusiv durch die vorgesehene Client-Software genutzt werden kann. Damit wird zudem eine Man-in-the-Middle Attacke verhindert.

Ein weiteres Gefährdungspotential sind temporäre Dateien, die auf dem genutzten PC hinterlegt werden. Diese können Informationen zu Verbindungsparameter oder Daten der genutzten Anwendungen erhalten, die ein Fremder missbräuchlich nutzen könnte. Als wirksamer Schutz vor verwertbaren Spuren auf den genutzten Privat- oder Gast-PC, empfiehlt sich die Nutzung einer Sandbox für eine sichere Ausführung der Client-Software.

Ein weiteres Risiko besteht darin, dass der verwendete VPN-Client oder auch der auf dem Gast-PC genutzte Browser infiziert sind. Daher sollten sämtliche Anwendungen digital signiert sein, um eine Manipulation der Client-Software selbst auszuschließen. Bei der Nutzung eines Privat- oder Gast-PCs empfiehlt sich die Nutzung eins Sticks, der alle notwendigen signierten Anwendungen Clients und Browser beinhaltet. Das vermeidet bei Webanwendungen zudem einen möglichen Supportaufwand aufgrund Browser-Inkompatibilitäten und fehlender PlugIns.

[1)] Chip Online

[2)] Kaspersky Stand 2013

ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

Schutzklasse: hoch – sehr hoch

Für den Zugriff auf hochsensible Daten im Unternehmen von außerhalb, reichen die zuvor beschriebenen Maßnahmen, wie eine 2-Faktor-Authentisierung, eine applikationsbasierte VPN-Verbindung, digital signierte Anwendungen und eine Sandbox, nicht aus.

Unter laufendem Windows gibt es keinen wirksamen Schutz gegen Trojaner, die Bildschirminhalte protokolieren und weiterleiten. Kommen private PCs zum Einsatz, ist es in dieser Schutzklasse unerlässlich, eine 100%ige Trennung zwischen der beruflichen und privaten Nutzung des PCs sicherzustellen.

Einzig wirksamer Schutz stellt, in dem Fall, das Booten des PCs aus einer gekapselten und gesicherten Umgebung dar, so dass die lokale, möglicherweise mit Malware behaftete Festplatte, physikalisch ausgeschaltet bleibt. Zudem sollte das Betriebssystem der gekapselten Umgebung die Hoheit über die angeschlossene Tastatur, Maus und Grafikkarte übernehmen, so dass eventuelle Schadsoftware im BIOS oder UEFI keinen Einfluss nehmen kann.

Eine Lösung der Schutzklasse *hoch – sehr hoch* muss zudem vor Angriffen im eigenen Netz schützen, also auch zuhause im (W)LAN, im Hotel oder an einem öffentlichen HotSpot. Idealerweise sollte ein entsprechend geschützter PC getarnt und damit für mögliche Angreifer im Netz gar nicht sichtbar sein.

Ebenso muss einem Szenario, in dem der Benutzer selbst der Angreifer ist, Rechnung getragen werden. Firmware und Client-Software aber auch Aktualisierungsprozesse müssen dem hingehend abgesichert sein, dass sie gegen jegliche Manipulation von außen geschützt sind.

Nur so lassen sich alle Anforderungen gemäß Bundesdatenschutzgesetz §9 und Telekommunikationsgesetz § 88 gesetzeskonform erfüllen.

www.ecos.de
ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

► Anforderungen gemäß BDSG

Im Folgenden möchten wir die Anforderungen beleuchten, die seitens des Bundesdatenschutzgesetzes für die Verarbeitung personenbezogener Daten gestellt werden. Die gleichen Maßstäbe sollten auch bei sensiblen, nicht-personenbezogenen Unternehmensdaten zugrunde gelegt werden.

§ 9 BDSG - Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. *Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),*

Bei Heimarbeitsplätzen ist sicherzustellen, dass der genutzte Raum abschließbar und auch von außen gegen Einbruch gesichert ist.

2. *zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),*

Um zu verhindern, dass Unbefugte in den Besitz von Zugangsdaten gelangen, z.B. über einen Trojaner auf dem genutzten PC, und damit Zugang zu Daten und Anwendungen bekommen, ist eine 2-Faktor-Authentisierung (Wissen- und Besitz-Komponente) unerlässlich. Hierzu gibt es unterschiedliche Lösungen, basierend auf OTP-Token (One-Time-Password), SMS-OTP, SmartCard, USB-Token…).

www.ecos.de
ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

3. *zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),*

Es empfiehlt sich der Einsatz einer Terminalserver- oder Virtual-Desktop-Infrastruktur, so dass gar keine Daten lokal verarbeitet und gespeichert werden. Damit können auch Im Servicefall, bei Verlust eines Notebooks oder Ausscheiden eines Mitarbeiters, keine Daten in falsche Hände geraten.

Mit dem Ausführen der Client-Software in einer Sandbox oder gekapselten Umgebung, wird der Zugriff auf verwertbare Spuren verhindert.

Die Zugriffsrechte lassen sich, abhängig von der eingesetzten Technologie, über die Serversysteme oder die eingesetzten Zugangslösungen, über ein zentrales Management auf Benutzer-, Gruppen-, oder Rollen-Ebene festlegen. Dies umfasst auch das Recht, bzw. das Verhindern, Daten aus einer Session heraus lokal abzuspeichern oder lokal zu drucken. Das Erstellen, Abspeichern, Drucken oder Weiterleiten von Bildschirmkopien wird über eine sichere Zugangslösung verhindert.

4. *zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),*

Grundvoraussetzung für einen sicheren Fernzugriff auf Daten und Anwendungen ist eine verschlüsselte Verbindung, idealerweise eine gesicherte VPN-Verbindung.

Weiterhin ist sicherzustellen, dass der eingesetzte PC frei von Schadsoftware ist, z.B. von Trojanern, die Bildschirminhalte und Tastatureingaben protokollieren und weiterleiten. Sicherer als das Arbeiten unter einem Risiko-behafteten Windows System, ist hier das Booten des PCs aus einer gekapselten und gehärteten Umgebung heraus.

Eine weitere Gefahr beim Arbeiten von Zuhause, vom Hotel oder über einem HotSpot, geht von Dritt-PCs im gleichen Netz aus. Ein infiziertes Gerät könnte über das Netzwerk Zugriff auf Daten und Systeme erlangen. Dies ist über eine Client-seitige Firewall zu verhindern.

ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

Über das zentrale Management-System müssen alle Zugriffsberechtigungen jederzeit ersichtlich sein.

5. *zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),*

Eine Protokollierung der erfassten, geänderten und gelöschten Daten, lässt sich, realistisch betrachtet, nur serverseitig realisieren. Auch aus diesem Grund sollten keinerlei Daten und Dokumente lokal gespeichert und verarbeitet werden.

Die Protokollierung der erfassten und geänderten Daten, sollte Teil der Fachanwendung oder – bei einer Nutzung auf Dateiebene – Teil der Serveradministration sein.

6. *zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),*

Auch eine Auftragskontrolle lässt sich, realistisch betrachtet, nur serverseitig realisieren. Ein weiterer Grund keinerlei Daten und Dokumente lokal zu speichern und zu verarbeiten.

Die Kontrolle hierrüber sollte Teil der Fachanwendung sein.

7. *zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),*

Um sicherzustellen, dass auch, im Falle eines abhandengekommenen Laptops, kein Unbefugter auf Daten zugreifen kann, sollte sichergestellt sein, dass keinerlei Daten, Dateien oder auch nur temporäre Dateien auf dem Gerät gespeichert werden. Mit entsprechenden Fachkenntnissen ist es immer nur eine Frage der Zeit, das Windows-Passwort oder sogar eine Festplattenverschlüsselung zu knacken.

Im Falle einer Zerstörung oder eines Verlustes, wären auch lokal gespeicherte Daten, teils unwiederbringlich, verloren. Die Praxis zeigt, dass gerade bei der Heim-Nutzung firmeneigener Laptops oder Privat-PCs, das letzte Backup meist mehr als wenige Stunden zurückliegt. Ein weiterer Grund keine Daten lokal zu halten.

ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine zweckgebundene Trennung hat in der entsprechenden Fachanwendung zu erfolgen oder – bei einem Arbeiten auf Dateiebene – durch getrennte Ablage auf dem jeweiligen Server oder Bereich. Es ist sicherzustellen, dass ausschließlich Personen mit der entsprechenden Zugriffsberechtigung, Zugang zu den Daten erlangen.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

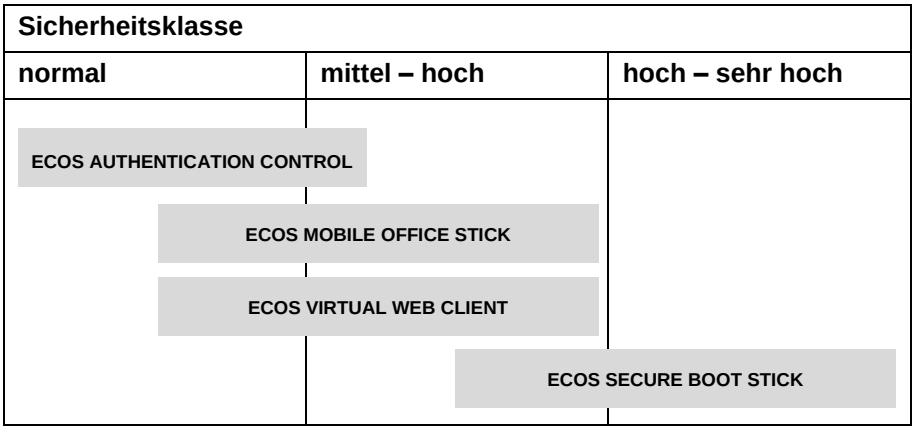
Eine VPN-Verbindung mit 256 Bit AES-Verschlüsselung sollte hier die Grundvoraussetzung sein.

ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

► Lösungen

ECOS bietet verschiedenen Lösungen zur Abdeckung der unterschiedlichen Sicherheitsstufen an. Neben dem kaufmännischen Aspekt, unterscheiden die Lösungen sich auch im Handling, da unterschiedliche Sicherheits-anforderungen auch ein unterschiedliches Mitwirken des Anwenders erwarten.

Das Innovative ist, dass alle ECOS Lösungen sich, innerhalb eines Unternehmens, plattformunabhängig, beliebig kombinieren lassen, um unterschiedliche Anforderungen, je nach Aufgabengebiet, abzudecken. Alle Lösungen verbindet, dass sie über ein gemeinsames Management-Tool verwaltet werden, in dem sich Benutzer- und Zugriffsrechte sehr granular auf Benutzer-, Gruppen,- oder Rollenebene verwalten lassen.



ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

Zugriff auf Daten normaler Sicherheitsstufe

ECOS AUTHENTICATION CONTROL

Mit ECOS AUTHENTICATION CONTROL (ACA) lassen sich passwortgeschützte Zugänge (VPN-Gateway, Web-Anwendung, Windows-Anmeldung…) über einen weiteren Besitz-Faktor absichern. ECOS ACA unterstützt folgende Authentifizierungsverfahren:

- SMS
- E-Mail
- OTP-Token
- USB-Token
- Smart-Card

Technische Details

- Virtuelle Appliance, zur Installation unter VMWare, Citrix XEN Server, Hyper-V, Oracle VirtualBox oder auf freigegebener Hardware
- Authentisierungsserver für SafeNet® eToken PASS, eToken NG-OTP (nur OTP-Teil) und OTP per SMS
- Authentifizierung gegen externen LDAP-Server
- Authentifizierung gegen int. oder ext. RADIUS-Server
- Vollständiger RADIUS-Server integriert
- Umfangreiches Token Life-Cycle Management
- SMS Versand via Internet Dienst oder SMS Gateway über RPC oder per E-Mail, angetriggert durch die RADIUS-Anfrage mittels Username und Passwort
- Unterstützung der SMS-Dienste der Telekom und Fax.de
- Verzeichnis-Synchronisation der Benutzer mit Microsoft® ADS, Novell® eDirectory, CA® eTrust,Siemens® DirX, SUN® Directory, LDAP und weiteren Directories

ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

Zugriff auf Daten mittlerer bis hoher Sicherheitsstufe

I) ECOS MOBILE OFFICE STICK

Der ECOS MOBILE OFFICE STICK (MOS) ermöglicht einen sicheren Zugang zu einer Terminalserver- oder Virtual-Desktop-Infrastruktur, bzw. Webanwendungen. Sämtliche Software für einen verschlüsselten Zugang zu Microsoft Terminalserver, Citrix, VMware View oder Webanwendungen befindet sich auf dem Stick. Die Nutzung ist für den Anwender völlig installations- und konfigurationsfrei. Die Ausführung der digital signierten Anwendungen erfolgt innerhalb einer Sandbox. Eine applikationsbasierte VPN-Verbindung verhindert die Nutzung des Tunnels durch unautorisierte Anwendungen und mögliche Schadsoftware. Der ECOS Mobile Office Stick dient gleichzeitig als 2-Faktor-Authentisierung, zertifikatsbasiert oder mit integrierter Smartcard.

Technische Details

- Installations- und konfigurationsfrei Nutzung, ohne Administratorrechte
- Clients: VPN, Citrix Receiver, VMware Horizon View incl. PCoIP, RDP, VNC
- Integrierter Firefox; optional Firefox oder Internet Explorer in einer bestimmten Version und mit vorinstallierten Plug-Ins
- Starke zertifikatsbasierte 2-Faktor-Authentisierung, gekoppelt an die Hardware-ID des Sticks
- Ausführung sämtlicher Software innerhalb einer Sandbox
- VPN-Verbindung auf Applikationsebene
- Transparenter VPN-Client für einzelne oder alle User freischaltbar (konfigurationsfrei für den Anwender; bei der Erstbenutzung Installation einer Softwarekomponente unter Administratorrechten)
- Nutzung des transparenten VPN-Tunnels auf zentral festgelegte, lokal installierte Applikationen eingrenzbar
- Nutzung des VPN-Tunnels auf digital signierte Applikationen eingrenzbar, inkl. Prüfung der Signatur vor Freigabe des VPN-Tunnels
- Auswahl des Zielsystems, bei verteilten Servern
- Festlegung der Zielserver und Ports auf Benutzer- oder Gruppenebene
- Nutzung lokaler Ressourcen nach Freigabe durch den Admin: lokale Laufwerke, ext. USB-Speicher, lokale Drucker
- Automatischer Zugriff über HTTPS-Proxy, wenn vorhanden
- Verbindung über einen frei wählbaren TCP Port
- Software in Deutsch und in Englisch
- Easy Enrollment
- Zentral festgelegte Password-Policy
- Remote-Aktualisierung der Sticks
- Einbindung kundenspezifischer Applikationen möglich
- Anbindung an ECOS System Management Appliance SMA100 über SSL VPN
- Nutzung unter Windows Vista, 7, 8, 8.1, (32 Bit und 64 Bit), sowie Mac OS X

ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

II) ECOS VIRTUAL WEB CLIENT

Der ECOS VIRTUAL WEB CLIENT (VWC) ermöglicht einen sicheren Ad hoc-Zugang zu einer Terminalserver- oder Virtual-Desktop-Infrastruktur, bzw. Webanwendungen. Er ist von der Software und dem Sicherheitskonzept sehr stark an den ECOS MOBILE OFFICE STICK angelehnt, wobei es sich beim VWC um eine reine Softwarelösung handelt. Über einen Standardbrowser wird sämtliche Software für einen verschlüsselten Zugang zu Microsoft Terminalserver, Citrix, VMware View oder Webanwendungen ad hoc geladen und frei jeglicher Installation oder Konfiguration ausgeführt. Die Ausführung der digital signierten Anwendungen erfolgt innerhalb einer Sandbox. Eine applikationsbasierte VPN-Verbindung verhindert die Nutzung des Tunnels durch unautorisierte Anwendungen und mögliche Schadsoftware. Eine sichere 2-Faktor-Authentisierung wird beim VWC über den Versand eines Einmalpasswortes an die Handynummer des Benutzers realisiert.

Technische Details

- Lizensierung nach Named-User
- Ad-hoc-Zugriff auf eine Terminalserver- oder VD-Infrastruktur über einen Standard-Browser
- Automatischer Download der notwendigen Client-Software
- Installations- und konfigurationsfrei Nutzung, ohne Administratorrechte
- Clients: Citrix Receiver, VMware Horizon View Client incl. PCoIP, Microsoft RDP, VNC
- Integrierter Firefox oder Internet Explorer, optional in einer bestimmten Version und vorinstallierten Plug-Ins
- 2-Faktor-Authentisierung mit Einmalpasswort per SMS oder Token
- VPN-Verbindung auf Applikationsebene
- Ausführung sämtlicher Software innerhalb einer Sandbox
- Auswahl des Zielsystems, bei verteilten Servern
- Nutzung lokaler Ressourcen nach Freigabe durch den Admin:
  lokale Laufwerke, ext. USB-Speicher, lokale Drucker
- Lokale Laufwerke
- Ext. USB-Speicher
- Lokale Drucker
- Zugriff über Proxy konfigurierbar
- Verbindung über einen frei wählbaren TCP Port
- Software in Deutsch und in Englisch (voreinstellbar)
- Einbindung kundenspezifischer Applikationen möglich
- Anbindung an ECOS System Management Appliance SMA100 über SSL VPN
- Nutzung unter Windows Vista, 7, 8, 8.1 (32 Bit und 64 Bit)

ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

Zugriff auf Daten hoher bis höchster Sicherheitsstufe

ECOS SECURE BOOT STICK

Der ECOS SECURE BOOT STICK (SBS) ermöglicht einen hochsicheren Zugang zu einer Terminalserver- oder Virtual-Desktop-Infrastruktur, bzw. Webanwendungen aus einer gekapselten und gesicherten Umgebung heraus. Mit dem Booten des PCs über den ECOS SBS wird die lokale Festplatte nicht aktiviert. Ein speziell gehärtetes ECOS Secure Linux übernimmt die Hoheit über die angeschlossene Hardware. Sämtliche Software für einen verschlüsselten Zugang zu Microsoft Terminalserver, Citrix, VMware View oder Webanwendungen ist digital signiert auf einer schreibgeschützten Partition. Eine integrierte Firewall schütz vor Angriffen im lokalen (W)LAN. Der ECOS Secure Stick dient gleichzeitig als 2-Faktor-Authentisierung, zertifikatsbasiert oder mit integrierter Smartcard.

Technische Details

- Gehärtetes ECOS Secure Linux-Betriebssystem
- Treiber für alle gängige Hardware und einen Verbindungsaufbau per LAN, WLAN, UMST, LTE sowie die Anmeldung an einem HotSpot
- Clients: Citrix Receiver, VMware Horizon View Client incl. PCoIP, Microsoft RDP, VNC, NoMachine
- Firefox inkl. Java-Unterstützung
- Anbindung an beliebiges Gateway über IPSec, oder an ECOS SMA100 über SSL VPN
- Starke zertifikatsbasierte 2-Faktor-Authentisierung, gekoppelt an die Hardware-ID des Sticks
- Auswahl des Zielsystems, bei verteilten Servern
- Nutzung lokaler Ressourcen nach Freigabe durch den Admin: ext. USB-Speicher, lokale Drucker
- Zugriff über Proxy konfigurierbar
- LAN-Forewarding für den Anschluss eines IP-Telefons
- Software in Deutsch und in Englisch (voreinstellbar)
- Tastaturtreiber für >50 Sprachen und Länder
- Multi-Monitor Support
- Remote Aktualisierung der Firmware
- Prüfung auf Integrität und korrekte Update-Server
- Digital signierte Firmware und Client-Software
- Speicherung von Firmware und Client-Software auf einer schreibgeschützten Partition
- Blockieren von TCP/IP- und Ping-Anfragen
- Verhinderung der Nutzung in einer virtuellen Umgebung
- Integrierte Firewall
- Instant Logout

ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

Zentrales Management

ECOS SYSTEM MANAGEMENT APPLIANCE

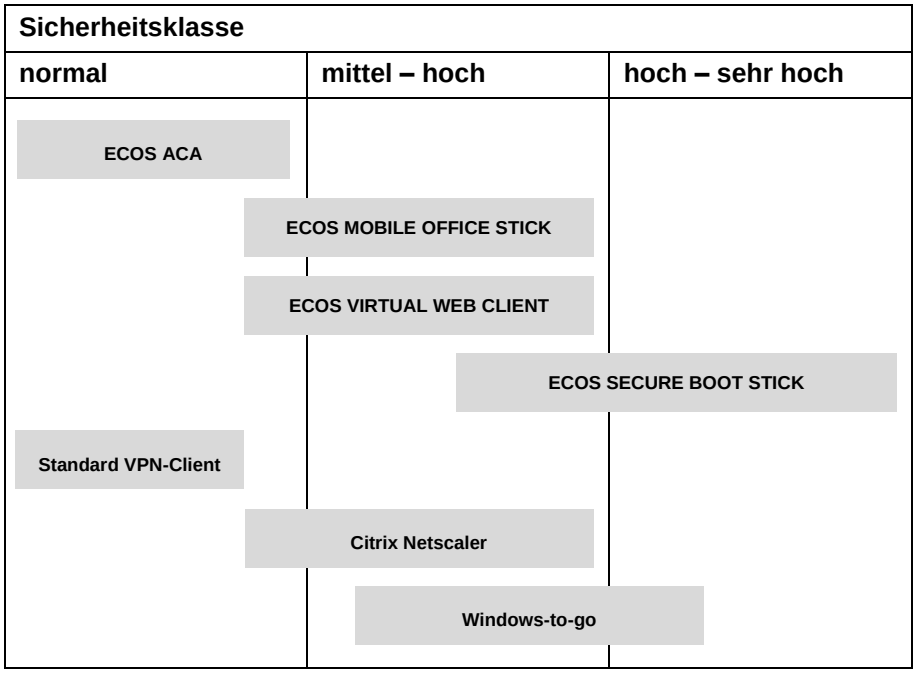
Für die zentrale Verwaltung aller ECOS-Zugangskomponenten dient die virtuelle ECOS SYSTEM MANAGEMENT APPLIANCE (SMA). Über eine webbasierte Oberfläche lassen sich alle Benutzer- und Zugriffsrechte zentral verwalten. Eine Anbindung an AD oder sonstige Verzeichnisdienste erleichtert die Administration erheblich. Die ECOS SMA dient auch gleichzeitig zur remote Aktualisierung aller ECOS Produkte.

Technische Details

- Virtuelle Appliance zum Betrieb unter VMware, Citrix XenServer, Hyper-V, Oracle VirtualBox oder auf einer dedizierten Hardware
- Integriertes VPN-Gateway(IPsec, SSL-VPN) und Authentisierungsserver
- unbegrenzte Anz. VPN-User
- unbegrenzte Anz. VPN-Tunnel
- Zentrales Management aller ECOS-Produkte
- Zentrale Benutzer- und Rechteverwaltung
- Remote Aktualisierung aller ECOS Produkte
- Benutzersynchronisation mit Active Directory oder anderen Verzeichnisdiensten
- Integrierte CA (Certificate Authority)
- Einbinden bestehender CA und Bereitstellen einer eigenständigen CA
- Integriertes Smartcard- und Token-Management
- Tokenlifecycle Management (Personalisieren, Ersetzen, Sperren, etc. von Sticks)
- Gruppen- und Rollenbasierte Zuweisung von Konfigurationen (z.B. Zielsysteme)
- Benutzerdefinierte Reports und LDAP-Schnittstelle
- Mandantenfähig
- Ausbau als Hochverfügbarkeitslösung mittel ECOS HA-Modul

ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

► Technologien im Vergleich



ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333

	VPN-Client	ECOS AUTHENTIVATION CONTROL	Citrix NetScaler®	ECOS MOBILE OFFICE STICK	ECOS VIRTUAL WEB CLIENT	Windows To Go®	ECOS SECURE BOOT STICK
Administration							
Installations- und konfigurationsfreie Nutzung	×	✓	×	✓	✓	✓	✓
Remote-Aktualisierung, interaktionsfrei	~	-	×	✓	✓	×	✓
Zentrale Rechtevergabe	×	-	✓	✓	✓	✓	✓
Synchronisation mit AD	✓	✓	✓	✓	✓	✓	✓
Automatisierter Roll-out-Prozess	~	×	✓	✓	✓	O	✓
Handling							
Plug-n-Play auf PC und Mac	×	-	×	✓	✓	×	✓
Updates automatisch im Hintergrund	×	-	×	✓	✓	×	✓
Keine Veränderungen auf dem Privat-PC	×	-	×	✓	✓	✓	✓
Nutzung unter laufendem Betriebssystem	✓	✓	✓	✓	✓	×	×
Sicherheit							
100%ige Trennung private-/berufliche Nutzung	×	×	×	×	×	✓	✓
Schutz vor unbefugtem Zugriff über eine 2-Faktor-Authentisierung	O	✓	O	✓	✓	O	✓
Schutz vor verwertbaren Spuren auf dem genutzten PC über eine Sandbox oder gekapselte Umgebung	×	×	×	✓	✓	✓	✓
Schutz vor Angriffen der Infrastruktur durch Schadsoftware auf dem genutzten PC	×	×	×	✓	✓	×	✓
Schutz vor Datenspionage über Trojaner auf dem genutzten PC	×	×	×	×	×	✓	✓
Schutz vor Zugriff auf private Fotos und E-Mails	×	×	×	×	×	×	✓

✓ Enthalten, O Zusätzliche Technik erforderlich, × Nicht möglich, - nicht zutreffend, ~ herstellerabhängig

www.ecos.de
ECOS Technology GmbH · Sant-Ambrogio-Ring 13a · D-55276 Oppenheim · Tel.: +49 6133 939- 200 · Fax: +49 6133 939- 333