



CompuSec[®] e-Identity[®]

Sicherheit für Notebooks & Desktops PCs

CompuSec[®] ist eine Sicherheitslösung zum Schutz von Notebooks und Desktops, die Zugangsschutz, Festplattenverschlüsselung, E-Mail Verschlüsselung, Dateiverschlüsselung, VPN, Sprachverschlüsselung und Single Sign On bietet. CompuSec[®] nutzt PKI Technologien und beinhaltet eine e-Identity[®] als Sicherheitselement für die Schlüsselspeicherung und den erweiterten Zugangsschutz. Die e-Identity[®] ist entweder als Chipkarte mit USB Chipkartenleser oder als USB Token verfügbar.

CompuSec[®] wurde für Kunden entwickelt, die mehr als nur einen Passwortschutz wünschen. Der hohe Sicherheitsstandard ist kombiniert mit einer flexiblen, für den Nutzer transparenten Funktionsweise. Einzelnutzer, kleine Nutzergruppen sowie auch große Unternehmen und Behörden nutzen CompuSec[®]. CompuSec[®] kombiniert eine Reihe von oft benötigten Sicherheitsfunktionen, die der Nutzer je nach Bedarf bei der Installation oder bei der Personalisierung wählen kann. Große Organisationen und Unternehmen erhalten zudem alle Funktionen für eine effiziente Installation und Nutzung von CompuSec[®], wie z.B. die bedienerlose Installation, das zentralisierte Rollout, die Unterstützung von Festplattenimages, die zentrale Softwareverteilung, zahlreiche Servicefunktionen und das zentrale Nutzermanagement in Form der GlobalAdmin Station.

CompuSec[®] nutzt neue, von CE-Infosys entwickelte Technologien, die bisher unbekannte Funktionen für PC Sicherheitsprodukte realisieren wie die Pre-Boot Authentifizierung mit e-Identity[®], PKI basierte Authentifizierung, die Verschlüsselung von CD's/DVD's und Wechselmedien und die Unterstützung des Hibernation-Mode mit verschlüsselter Hibernationdatei. Die neu entwickelte Zugangstechnologie nutzt nicht die traditionellen PIN Codes. Stattdessen wird eine Challenge/Response Technologie genutzt, um ein Single Sign On für das Betriebssystem auf SmartCard Ebene auszuführen.

Intelligenter Zugang

Immer wenn der PC gestartet wird, erfolgt die Pre-Boot Authentifikation des Benutzers mit einer hochwirksamen 2-Faktoren Authentifizierung. Dazu wird eine SmartCard oder ein USB Token sowie das Passwort benötigt. Der intelligente Zugang gewährt Schutz vor Spionage Technologien, die die Signale des SmartCard Lesers angreifen, um die PIN zu erlangen.



Pre-Boot-PKI

CompuSec® hat eine neu entwickelte Pre-Boot-PKI Technologie, um den Zugang zur Festplatte des Computers zu verwalten. Diese erlaubt Einzelnutzern und Nutzergruppen den Zugang zu einem oder mehreren Computern. Die Benutzer-, Rechner- und Schlüsselverwaltung wird bei großen Organisationen einfach über die GlobalAdmin Station realisiert oder ist bei Einzelinstallationen Bestandteil des Installationsprogramms.



Passwortverwaltung

Der Kunde kann die Passwort-Strategie seinen Bedürfnissen anpassen. Variabel sind die Passwortlebensdauer nach Tagen und/oder Logins, der Passwortwechsel zu jeder Zeit, die Passwortlänge und weitere Einstellungen. In den Fällen wo ein Passwort vergessen wurde, bietet eine Challenge/Response Funktion in Verbindung mit der GlobalAdmin Station eine einfache und sichere Möglichkeit, um dem Benutzer ein neues Passwort zuzuteilen. Bei Einzelinstallationen ist ebenfalls eine Hilfe mittels Passwort- Rücksetzcode möglich.

Bitte Passwort eingeben:

Single Sign On

Zwei Alternativen von Single Sign On werden unterstützt. Erstens: die e-Identity® des Benutzers speichert das System-Anmeldepasswort zusammen mit der Benutzer-ID und dem Domain-Namen. Dies ersetzt die traditionelle Anmeldung am Betriebssystem. Die zweite, fortschrittlichere Methode die CompuSec® bietet, nutzt ein digitales Zertifikat des Nutzers zusammen mit dem privaten Schlüssel in der e-Identity®. Diese zertifikatsbasierte Anmeldung am Domain-Server ist der bevorzugte Weg für Domain-Nutzer und ist voll integriert im Microsoft Betriebssystem. Das zertifikatsbasierte Single Sign On benötigt die GlobalAdmin Station, die als Zertifikatsstelle genutzt wird. Lotus Notes Nutzer speichern ihre ID-Informationen in der e-Identity® und nutzen ebenso die Zertifikate der e-Identity®.



Festplattenvollverschlüsselung

Die Festplattenverschlüsselung von CompuSec® nutzt den schnellen AES Algorithmus. Die Verschlüsselung erfolgt für alle Sektoren der Festplatten, schließt das Betriebssystem mit ein und unterstützt max. 8 Partitionen auf jeweils max. 8 Festplatten. Die Initialverschlüsselung wird direkt nach dem Login des Benutzers gestartet oder nach dem Login unter dem Betriebssystem (Hintergrundverschlüsselung). Die Hintergrundverschlüsselung ermöglicht dem Benutzer den Verschlüsselungsprozess zu unterbrechen und den Computer jederzeit herunterzufahren oder den Hibernation Modus zu nutzen. Sehr wichtig für Nutzer von mobilen Systemen ist die Unterstützung des Hibernation Modus des Windows Betriebssystems. In diesem Modus werden die Inhalte des Arbeitsspeichers (RAM) auf die Festplatte geschrieben und verschlüsselt, bevor der Computer herunterfährt. Beim Neustart werden nach der Pre-Boot Authentifizierung des Benutzers die RAM-Inhalte wieder von der verschlüsselten Hibernation Datei geladen und der Benutzer kann seine Arbeit fortsetzen. Bisher konnten Festplattenverschlüsselungen diesen Modus nicht unterstützen oder keine verschlüsselte Hibernation Datei erzeugen. CE-Infosys war das erste Unternehmen, dass den Hibernation Modus in seinen Produkten unterstützte.



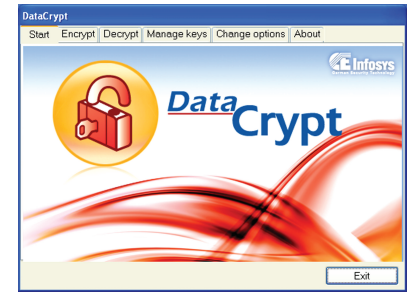
Verschlüsselung von CD's/DVD's und Wechselmedien

CD's/DVD's, Wechselmedien und Wechsellaufwerke wie z.B. USB Speichermodule und externe USB Festplatten können mit CompuSec® e-Identity® verschlüsselt werden. Mit der zentralen Administration über GlobalAdmin ist es möglich die Verschlüsselungsregeln und damit die Modi zu definieren, in welchem diese "Geräte" benutzt werden. Der Nutzer kann das Recht erhalten, den Verschlüsselungsmodus zu verändern. Damit erhält das Unternehmen die Möglichkeit Sicherheitsrichtlinien umzusetzen, z.B. die ausschließliche Nutzung von verschlüsselten CD's/DVD's oder Wechselmedien.



Dateiverschlüsselung für sicheren Austausch

CompuSec® e-Identity® beinhaltet DataCrypt, welches den Nutzern ermöglicht, einzelne Dateien zu verschlüsseln. Mit DataCrypt können die Nutzer verschlüsselte Nachrichten per E-Mail, FTP etc. versenden. Die Daten werden verschlüsselt versendet oder mit einem anderen Medium transportiert. Zusätzlich ist es mit CompuSec® möglich die Dateien auf sicherem Wege auszutauschen. DataCrypt nutzt dazu ein Public-Key Verfahren mit der Schlüsselgenerierung über elliptische Kurven. DataCrypt nutzt die neue "Sealing" Technologie, die alle Strukturen im Header der verschlüsselten Dateien versteckt. Sealing erlaubt den Schutz der verschlüsselten Dateien vor neugierigen Augen bei Ihrer Reise durch das Internet.



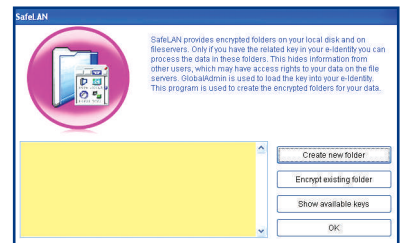
E-Mail Signierung und Verschlüsselung

CompuSec® bietet die erforderlichen Verschlüsselungsmodule, um E-Mails in Microsoft Outlook, Outlook Express oder Lotus Notes zu verschlüsseln und zu signieren. Die benötigten digitalen Zertifikate für die E-Mail Sicherheit sind in der e-Identity® gespeichert. Die kryptografische Software arbeitet mit dem Microsoft signierten CSP (Cryptographic Service Provider). Die E-Mail Sicherheit nutzt den S-MIME Standard, um den Austausch mit anderen Benutzern, die CompuSec® noch nicht verwenden, zu garantieren.



Verschlüsselte Dateien und Verzeichnisse auf Servern

Datei- und Verzeichnisverschlüsselung mit CompuSec® kann auf dem lokalen Rechner oder auf Netzlaufwerken durchgeführt werden. Diese Funktion stellt sicher, dass alle Dateien, die in das Verzeichnis zur Verschlüsselung geschrieben oder kopiert werden, automatisch und absolut transparent für den Benutzer verschlüsselt werden. Dies gewährleistet, dass nur Nutzer die einen autorisierten Zugangsschlüssel besitzen, Zugang zu diesem Verzeichnis haben und somit Dateien entschlüsseln, d.h. lesen können. Diese Funktion wird verwendet um Benutzertrennung auf Unternehmensservern auf kryptografischem Wege zu realisieren. Sicher ist, dass selbst der Server-Administrator die Inhalte der verschlüsselten Dateien nicht lesen kann.



Verschlüsselte Sprachkommunikation

[ClosedTalk]® ist die CompuSec® Komponente für die verschlüsselte Sprachübertragung zwischen zwei CompuSec® Nutzern. [ClosedTalk]® verwendet die Soundkarte des PC's und spart dadurch externe Geräte. Die Sprachdaten werden kostengünstig und sicher über das Internet ausgetauscht. Anstatt mit der Telefonnummer erfolgt die Anwahl des Gesprächspartners mittels der persönlichen E-mail Adresse. [ClosedTalk]® nutzt gesicherte Vermittlungsrechner im Internet zur Vermittlung der Gespräche. Die Verwendung ausgefeilter Sicherheitstechnik garantiert sowohl die Vertraulichkeit der Gesprächsinhalte als auch die der Verbindungsdaten.



Identitätsmanagement

Ein universelles Passwortmanagement unterstützt PC und Internet basierende Anwendungen. Die Identität des Anwenders wird bei der CompuSec® Anmeldung einmalig festgestellt und dann auf Wunsch automatisiert anderen Anwendungen mitgeteilt. Es werden zusätzlich zertifikatsbasierte Anmeldeprozesse an Microsoft Domain Controllern, Lotus Notes, Novell und anderen Netzwerken unterstützt.



Erweiterter VPN Client für sichere Verbindungen zu Firmennetzwerken

CompuSec® bietet IP-Verschlüsselung für WAN- und LAN-Nutzer. Der IPCrypt Client ist eine bei der Installation auswählbare Funktion von CompuSec®. Der IPCrypt Client unterstützt IP Adresspools, Datenkompression, mehrere Einwahlpunkte und weitere Funktionen. Die IP Verschlüsselung von CompuSec® benötigt einen Cryptor als VPN-Gateway im Netzwerk.



Installation und Verwaltung

CompuSec® kann mit oder ohne zentrale Verwaltung installiert werden. Bei der Single-Installation von CompuSec® wird während der Installation eine Sicherheitsdatei mit allen geheimen Schlüsseln erzeugt. Es liegt im Verantwortungsbereich des Benutzers die Datei und die Schlüssel sicher zu verwahren. Beim Einsatz von CompuSec® in größeren Organisationen (z.B. Unternehmen und Behörden) ist eine zentrale Verwaltung mit dem GlobalAdmin Management Programm empfehlenswert. Die GlobalAdmin Station verwaltet alle Rechner, Benutzerprofile, Rechte, Schlüssel, e-Identities® und weitere Daten der CompuSec® Installationen. GlobalAdmin erlaubt bedienerlose Installationen, automatische Softwareverteilung und Software Updates, ein ferngesteuertes Passwortrücksetzen und komplette Verwaltung der VPN-Funktionen. CompuSec® kann als integrierter Teil einer unternehmensweiten PKI-Struktur genutzt werden. Für Unternehmen mit mehreren Standorten ist eine e-Identity® Loading Station verfügbar. Ein automatischer Abgleich mit der Microsoft Nutzerverwaltung und "Active Directory" ist für die CompuSec® Verwaltung gewährleistet.



Systemanforderungen

- Notebook oder Desktop mit Intel Architektur
- Windows 7, Windows Vista und Windows XP (64 & 32 Bit)
- Windows Server 2003, Windows Server 2008 und Windows Server 2008R2
- USB 2.0 Anschluss
- 60 MB freier Festplattenspeicherplatz
- Eingebaute Soundfunktion für [ClosedTalk]®



CE-Infosys GmbH

Am Kümmerling 45
D-55294 Bodenheim
Germany
Tel.: +49 (0) 6135 / 77 0
Fax: +49 (0) 6135 / 77 77

de.sales@ce-infosys.com

CE-Infosys Pte Ltd

12 Tannery Road
#09-01/02 HB Centre 1
Singapore 347722
Tel.: +65 6235 8722
Fax: +65 6235 3164

sg.sales@ce-infosys.com

CompuSec, e-identity und [ClosedTalk] sind registrierte Markenzeichen der CE-Infosys Pte Ltd in Singapur.

Händler: