ECOS Secure Boot Stick

– Höchste Ansprüche an den Schutz von zentralen Datenbeständen –

Wenn beim Fernzugriff (Remote Access) auf Ihr Netzwerk der kompromisslose Schutz der Datenbestände in Ihrer Zentrale an oberster Stelle steht, dann ist der ECOS Secure Boot Stick das einzig richtige Zugriffsmedium für Sie. Die Benutzer können hierbei Ihre Mitarbeiter sein, die mit Rechnern Ihrer Organisation oder alternativ mit deren privaten, also Fremd-PCs bzw. -Notebooks ausgestattet sind. Oder auch externe Personenkreise wie Agenten, Dienstleister, Freelancer etc., die auf Basis von Fremd-PC/-Notebooks auf Ihr Netzwerk zugreifen dürfen.

Höchste Sicherheits-Anforderungen

Der ECOS Secure Boot Stick ermöglicht hochsichere Fernverbindungen zu zentralen Terminalservern (Citrix® , MS Windows® usw.) oder Webservern über das Internet bzw. WLAN, wobei der bestmögliche Schutz Ihrer zentralen Datenbestände dadurch realisiert wird, dass eben diese von den lokalen Daten/Anwendungen auf den Rechnern der Benutzer strikt getrennt bleiben. Optional bietet Ihnen der Einsatz unserer Smartcard-Variante die ultimative Sicherheit. Das Bootdevice (Flashspeicher) und die Smartcard (Kryptochip) sind bei dieser Variante vereint.

Für den Benutzer installationslos

Der Benutzer startet seinen USB-bootfähigen PC/Notebook einfach mit eingestecktem ECOS Secure Boot Stick, der dabei direkt bootet - ohne dass es jeglicher Installation seitens des Benutzers bedarf. Das auf der Festplatte installierte Windows® wird nicht angesprochen und stellt kein Sicherheitsrisiko dar, selbst wenn dies durch Viren oder Trojaner verseucht wäre. Der ECOS Secure Boot Stick stellt danach eine komplette und sichere, zertifikatsauthentisierte Thin Client-Umgebung zur Verfügung und gewährleistet damit eine strikte Trennung zwischen Daten auf dem PC/Notebook des Zugriffsberechtigten und den Daten Ihrer Organisation, die über den ECOS Secure Boot Stick bearbeitet werden.

Funktionalität

Der ECOS Secure Boot Stick unterstützt standardmäßig verschiedene Terminalserver-Clients, z.B. Microsoft RDP und Citrix ICA.

Für den Internetzugang stehen unterschiedliche Möglichkeiten zur Verfügung, jeweils abhängig von den vorhandenen Schnittstellen des PC/Notebook. Unterstützt werden Ethernet, DSL, WLAN und UMTS.

Die im ECOS Secure Boot Stick enthaltenen VPN Clients ermöglichen sichere und verschlüsselte Verbindungen mit dem Firmennetzwerk über VPN-Tunnel (SSL VPN oder IPsec). Die ECOS Secure Boot Sticks können sich über IPsec auf VPN-Gateways diverser Hersteller konnektieren. Alternativ kann das ECOS SSL VPN-Gateway eingesetzt werden, welches nahtlos in die zentrale Administrations-Komponente integriert ist.

Grundsätzlich findet immer eine sichere 2-Faktor-Authentisierung statt. Dies bedeutet, dass der Benutzer sich nur anmelden kann, falls er über den ECOS Secure Boot Stick verfügt sowie Kennwort bzw. PIN kennt.

Bei Nutzung der Smartcard Variante als ECOS Secure Boot Stick Plus erfolgt die eindeutige Benutzer-Identifikation via eines im integrierten Smartcard-Chip gespeicherten asymmetrischen RSA-Kryptoschlüssels, der durch eine PIN geschützt ist.

Komfortable Administration bei minimalen Kosten

Ihre ECOS Secure Boot Sticks konfigurieren und verwalten Sie komfortabel mit unserer übersichtlichen Administrations-Oberfläche. Eine Zusammenarbeit mit bestehenden Systemen wie Microsoft ADS ist selbstverständlich.

Das zentrale Management vereinfacht die Konfiguration bzw. System-Wartung deutlich und senkt den Administrationsaufwand und damit die Kosten gegenüber herkömmlichen Systemen beträchtlich.

Abb: links: ECOS Secure Boot Stick (Art. Nr. STU400), rechts: ECOS Secure Boot Stick Plus – inkl. Smartcard (Art.Nr. STU410)

Übersicht Leistungsdaten

- Bootet eigenständigen Thin Client
- Clients: ICA, RDP, VNC, NoMachine, XDMCP
- Browser: Firefox mit Java
- Integr. IPsec- und SSL VPN Client, unterstützt auch XAUTH (z.B. für Cisco® VPN-Gateways)
- Zertifikatsbasierte Anmeldung am VPN-Server, sichere 2-Faktor-Authentisierung mit PIN
- Signieren und Verschlüsseln, sowie Windows Smartcard Logon, mit dem STU410 oder anderen Smartcards/USB-Token durch PC/SC Forwarding
- Universelle Druckerunterstützung (USB- und Parallel-Schnittstelle, je nach Hardware)
- Freigabe von autorisierten USB-Speichergeräten (USB-Stick, Digitalkamera usw.) möglich
- Zentrales Management für Tokens und Zertifikate
- Optional in zentrales Management integriertes SSL-VPN Gateway
- Benutzersynchronisation mit Active Directory oder anderen Verzeichnisdiensten möglich