safe and smart

ecos

ECOS SecureBootStick®

Highly secure access to data and applications

- Easy
- Flexible
- Highly secure

IT-Security Solutions

Made in Germany

BSI
zugelassen
VS-NfD
EU/NATO RESTRICTED
ECOS TECHNOLOGY

Remote access—easy, flexible, highly secure

Our working world requires a growing flexibilization of working hours and work location, but creating home-based or alternating telecommuting workplaces and mobile workstations often reaches limits. Either there are no budget resources for secure laptops or the administrative effort is too heavy. Private devices cannot be permitted for security concerns.

As the threat situation grows, IT security requirements are rising enormously—not only regarding the use of private devices outside the company, but also when connecting external service providers and customers.

Benefits at a glance:

- Hardened ECOS Secure Linux operating system
- Full separation of professional and private use
- All software on one stick
- Multi-factor authentication per smartcard
- Integrated firewall
- Central management
- Remote updating
- Data safe for document storage*
- Approved for VS-NfD, EU-/NATO RESTRICTED**

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

Companies also need to prepare for real-world threats, such as natural disasters, by deploying emergency workstations. The ECOS SecureBootStick allows for the first time public authorities, companies and other organizations admitting the use of private and third-party computers while observing the highest security requirements, and this even for the processing of documents of confidential documents classified VS-NfD. Compared to other solutions, administration efforts and costs can be cut significantly while user satisfaction and especially the security level are considerably improved.

ECOS SecureBootStick (SBS) product family

The ECOS SecureBootStick provides users with a highly secure access to data and applications of their company or organization from any PC or Mac.

The ECOS SecureBootStick family covers various security requirements.

The ECOS SecureBootStick CL offers a high security level at a particularly attractive price. Since the first version, which was brought to market in 2007, a high level of expertise has shaped the continuous development of this product family to improve its security, its integration into various infrastructures and its hardware compatibility.

The ECOS SecureBootStick HE takes the proven solution to new security level thanks to a custom-designed and hardware-encrypted USB stick equipped with different security features.

The ECOS SecureBootStick FX, just like the HE, provides a range of security features molded into hardware. It is additionally equipped with an integrated smartcard and a PIN pad for direct PIN entry. All encryptions and processes are secured with the smartcard.

The ECOS SecureBootStick SX is the flagship of the product family. Though widely identical to the FX, the SX is BSI-approved and specifically designed to provide access to data and applications classified VS-NfD, EU-/NATO RESTRICTED—even on a private PC or Mac.

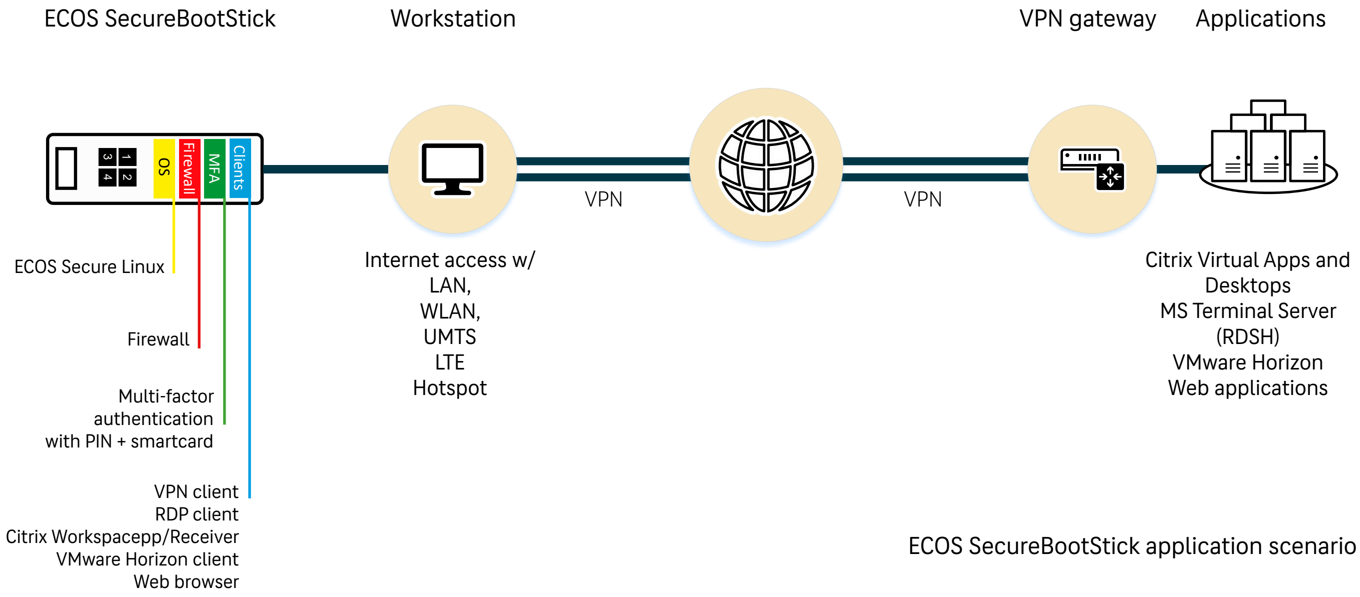
The ECOS SecureBootStick ZX is equipped with an ID-1 card slot and supports PKI and ID cards for user authentication. The ZX is identical to the SX in design and software and BSI-approved for VS-NfD, EU-/NATO RESTRICTED.

ECOS SecureBootStick CL

ECOS SecureBootStick HE

ECOS SecureBootStick FX/SX

ECOS SecureBootStick GX/ZX



ECOS SecureBootStick application scenario

Highly secure access to your organization's network

The Secure Boot Stick family provides high-security access to terminal server/virtual desktop infrastructures and web applications from a secure and encapsulated environment.

Any PC boots the specially hardened ECOS Secure Linux operating system of the stick. The internal hard drive is kept shut down, so potential malware on the hard drive will not get any chance. Disconnecting the internal hard drive ensures an integral separation of professional and private usage of the guest computer. The SBS contains all necessary firmware and applications. The private computer is thus only a private periphery.

All software on one stick

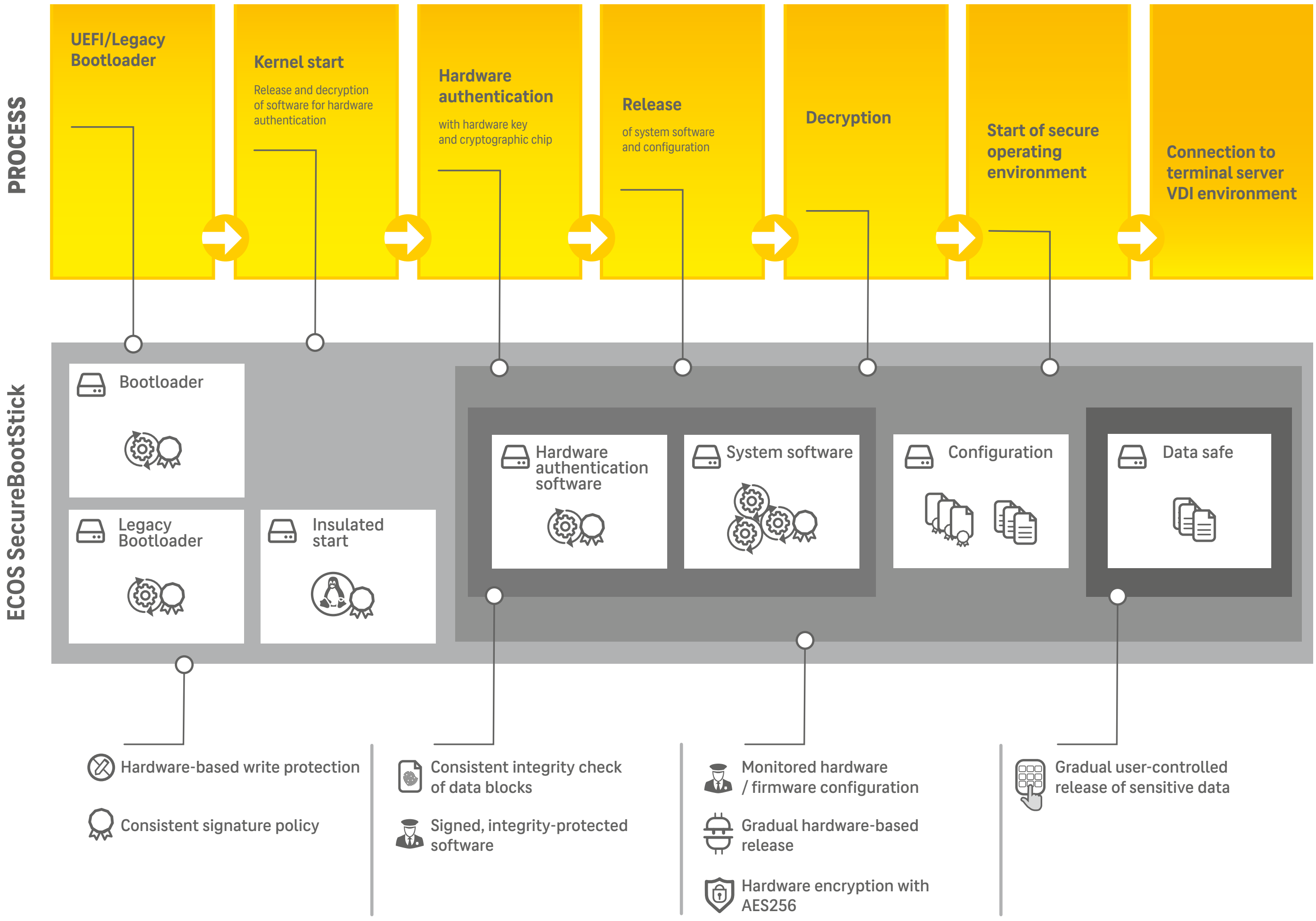
The Secure Boot Stick contains all clients required for a high-security remote access to Microsoft RDSH (formerly Windows Terminal Server), Citrix Virtual Apps & Desktops (formerly XenApp und XenDesktop), VMware Horizon (formerly VMware View) and computers with remote desktop sharing.

The SBS also provides a Firefox and a Chromium browser for access to web applications.

Easy to implement and administrate

The integrated VPN clients interface with any existing VPN gateway using IPsec or OpenVPN. An HTTPS connection is possible in conjunction with Citrix ADC (formerly Citrix NetScaler). As an alternative to the integrated VPN client and taking additional manufacturer licenses into account, a Cisco AnyConnect client (per SSL), a Juniper client and an F5 client are also available. The use of a genua genuscreen VPN gateway is mandatory for the BSI-approved SX/ZX variants in accordance with the security and operating procedures for VS-NfD, EU-/NATO RESTRICTED.

ECOS Easy Enrollment allows rolling out accesses in large numbers and very short time. All users receive identically pre-configured sticks. The central management issues personal activation codes, alternatively personal smartcards for the FX/SX variants, for


PROCESS
UEFI/Legacy Bootloader
Kernel start
Release and decryption of software for hardware authentication
Hardware authentication
with hardware key and cryptographic chip
Release
of system software and configuration
Decryption
Start of secure operating environment
Connection to terminal server VDI environment
ECOS SecureBootStick
Bootloader
Legacy Bootloader
Insulated start
Hardware authentication software
System software
Configuration
Data safe
Hardware-based write protection
Consistent signature policy
Consistent integrity check of data blocks
Signed, integrity-protected software
Monitored hardware / firmware configuration
Gradual hardware-based release
Hardware encryption with AES256
Gradual user-controlled release of sensitive data

Schematic view of the ECOS SecureBootStick HE, FX, SX, ZX

the user-specific configuration. The ZX variant can be coupled with a PKI or personal ID card by synchronizing the public keys. The central management allows administrating and remotely updating all sticks.

Maximum compatibility

The integration of private end devices also increases the compatibility requirements. The SBS therefore contains drivers for all customary PCs, Macs and x86-based tablets, including graphics drivers, LAN/ WLAN/UMTS/LTE drivers as well as a browser for hotspot logon.

An integrated Citrix HDX RealTime Media Engine ensures optimal transmission of audio and video signals, especially with Microsoft Skype for Business and Microsoft Teams. Combined with RDP, Microsoft RemoteFX provides the best possible audio quality. For the use of guest PCs abroad, the stick contains keyboard drivers for more than 90 languages and countries.

Local printers or IP telephony can be connected via USB and LAN port forwarding. The respective rights for document printing are configured in the central

Application scenarios

Customers operate the ECOS SecureBootStick in various areas.

Promoting work and family life balance

For many job applicants considering new career opportunities work and family life balance is more important than the remuneration of their new position. This applies not only to young families who want to gain more time for raising their children; in times of demographic change and in view of the shortage of caregivers, caring for older family members is also playing an increasing role. In addition, active participation in working life is also particularly important for older people or people with restricted mobility.

Career should not fall by the wayside in the process. Considering the much deplored skills shortage, it is not a surprise that flexibilizing the work places largely helps employers to present themselves as attractive. The challenge for IT is now to create home, telework or mobile workstations while meeting the highest security requirements, and this with limited resources and as effortless as possible.

Maximum flexibility in the hectic daily routine

Some things cannot wait until the next workday just because the company notebook is still at the office. Besides, children do not announce diseases 24 hours in advance. Solutions allowing the use of the private PC and meeting the highest security requirements do not only increase employee satisfaction, but also the company's efficiency.

Connecting external employees

Companies and public authorities regularly draw on external consultants or service providers for important tasks. However, processes such as connecting non-business laptops to internal networks or external remote access to databases and specialist applications for third parties place particularly high demands on IT security.

IT and remote IT maintenance

To maintain IT infrastructure and specialist applications, professionals need a 24/7 access to relevant systems. Remote access to critical systems requires particularly high security arrangements.

This applies especially to external service providers who typically use their own laptops and expect a connection to local networks.

Secure access at home and abroad

The vast majority of countries have entry regulations with some kind of restriction on encryption technologies. One of the biggest concerns is the access granted to law enforcement agencies to notebooks and storage media. Some countries place obligations on travelers to hand over encryption keys for law enforcement purposes.

Many companies therefore urge their employees to take only clean devices that do not contain sensitive work-related information. However, the necessity to access important data while on the road remains.

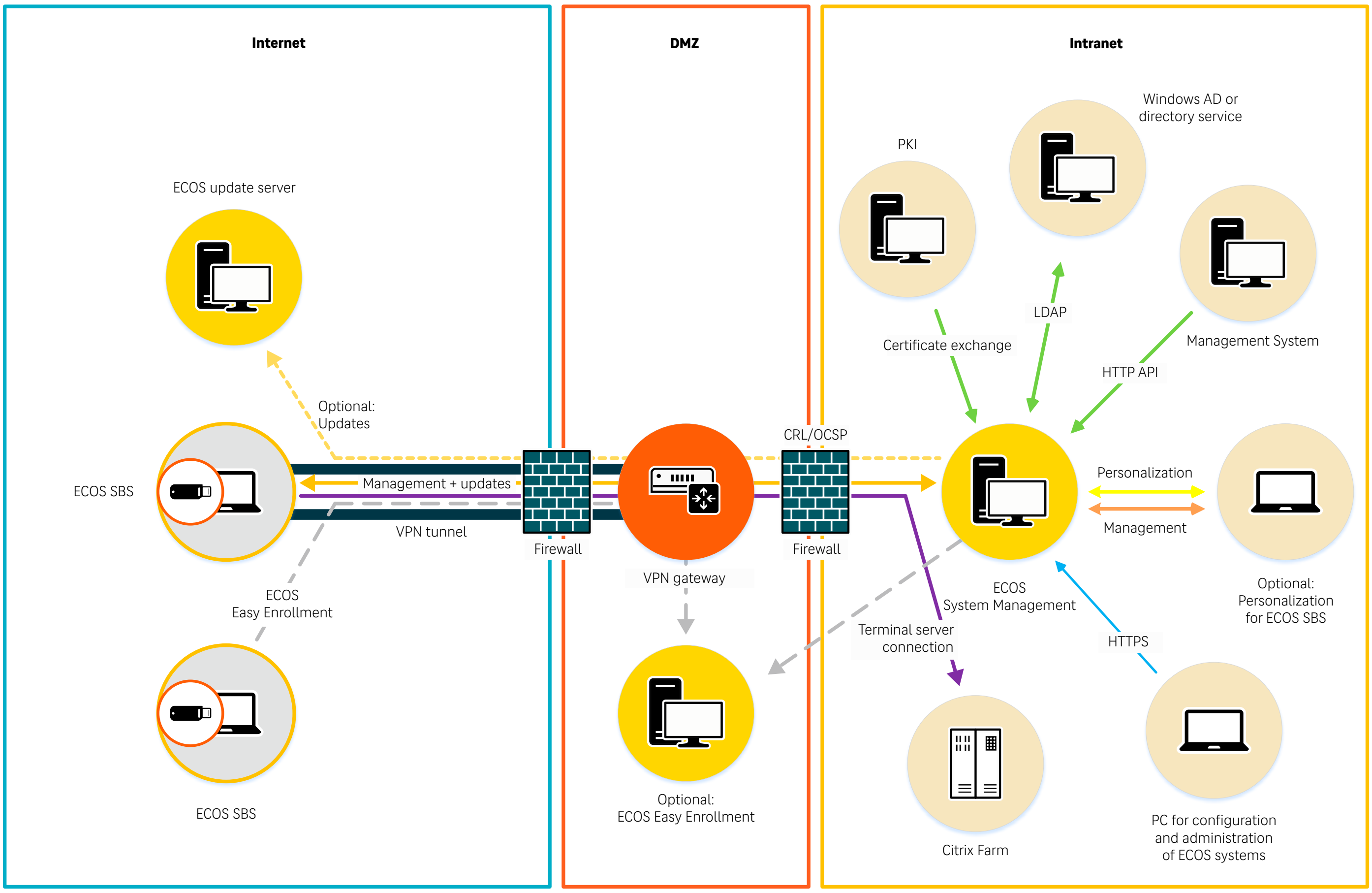
Providing flexible workplaces for emergency

In times of increasing weather events and other unforeseeable occasions, public authorities and companies must take precautions to be able to maintain emergency operation even when the staff's route to work is jammed.

Working with the home PC avoids unnecessary downtimes and expensive emergency offices, provided the relevant IT security and data protection requirements are met.

Confidentiality on a customary PC

Federal agencies, the German Armed Forces, and companies subject to intelligence regulations have long been aware of the requirements that are now progressively introduced in the area of critical infrastructure and other security-related companies: processing documents classified VS-NfD, EU-/NATO RESTRICTED requires BSI-approved end devices, not only in the management, but also for software developers or engineers. Solutions like hardened laptops do not really satisfy users and certainly not financial controlling departments.
The BSI-approved ECOS SecureBootStick SX/ZX allow for the first time the access to VS-NfD, EU-/NATO RESTRICTED from a customary PC.



Example of integration into an existing infrastructure of the ECOS SecureBootStick CL/HE

management. Other USB devices, such as foot pedals for dictation devices, are partly supported.

Design of the ECOS SecureBootStick

Highest security requirements were the top priority in the design of the Secure Boot Stick. The Secure Boot Stick therefore contains different partitions that are successively released during the boot process by respectively the immediately preceding security check or authentication procedure. The partitions for boot loader, firmware and applications are write protected, from the HE variant onwards with a hardware-side write protection.

Starting with the boot loader, all SBS parts are consistently secured by AES 256-bit encryption, which is software-encrypted in the CL variant and hardware-encrypted for all others. For document storage, the FX/SX/ZX variants also offer a data safe designed as hardware-encrypted drive and protected by smartcard with PIN entry.

Multi-factor authentication

The Secure Boot Stick offers not only the safety of a secured and encapsulated environment, but also serves strong multi-factor authentication purposes. The CL variant contains a certificate tied to the SBS hard-

Security concept

The ECOS SecureBootStick cascades various security measures that add up to an extremely high security level. The following safety assessment lists potential threat scenarios and shows how to prevent them.

Protection against infected PC

Since the guest PC boots within an encapsulated and hardened Linux environment, no potential malware can be activated on the internal hard drive. Furthermore, the ECOS Secure Linux operating system takes control of the connected periphery (mouse, keyboard, graphics card, network card), so even BIOS or UEFI malware will pose no threat.

Protection against unauthorized access

A strong multi-factor authentication is the basis of a secure user authentication. The login to the gateway and the access to the data safe therefore not only require the knowledge of the personal password or personal PIN, but also the Secure Boot Stick itself or, depending on the product variant, the corresponding smartcard.

Protection against manipulation

The Secure Boot Stick has various protection measures against possible manipulations. First, firmware and applications are on a write-protected partition, with which boot loader, kernel and all applications are digitally signed. They verify each other in a permanently recurring chain-of-trust process. Any attempt to manipulate the file system or replace parts of the code will immediately render the stick useless and, while in ongoing operation, lead to an immediate shutdown of the computer. Manipulations are thus effectively prevented.

Protection against spying

The end device can only connect to the gateway with a secured VPN connection and only after successful authentication. All relevant parts of the firmware are stored on a write-protected partition to protect the SBS against potential Trojans on websites, for example at hotspot logon. In addition to the abovementioned chain of trust, this prohibits the manipulation of the operating system.

The Secure Boot Stick provides multiple defenses against attacks exploiting the system management mode. In the early boot process, BIOS or UEFI are inspected for potential malware. For particularly security-relevant agencies or companies, a fingerprint of the computer can be created on the first start-up (from version 7 on, available January 2020). Any modification of the PC must thereby be authorized by the administrator. Manipulations of BIOS/UEFI and the hardware are thus both detected. Hardware-based attacks, for example trying to read out key material from the main memory, are thwarted by the encryption at many levels.

Protection against online attacks

The ECOS Secure Linux operating system is a lean system designed to provide only those parts of an operating system that are required to run the solution. Potential security gaps are thus significantly reduced right from the start.
The operation system has also been hardened and compiled to meet the highest security requirements. The Secure Boot Stick provides an own firewall for protection against attacks within the same network – whether from hackers or an infected PC. The firewall blocks all TCP/IP and ping requests. A potential attacker, for example in the same hotel, train or any location where you share a network with unknown people, will not even be able to detect the guest computer.

Protection against unwanted user interventions

The system checks whether the Secure Boot Stick is booting in a virtual machine before executing the firmware. This prevents the circumvention of security measures, for example by a keylogger or a Trojan trying to log screen content or keystrokes on the host system.

Protection against manipulated updates

Every time the Secure Boot Stick connects to the central management, it scans automatically for potential updates and authorized users. If available, a new image is loaded in the background. In this process, the correct origin and the integrity of the update image are verified. Once download and verification have been successfully completed, the new image will be executed the next time the Secure Boot Stick is booted.

ware ID for personalization. From the HE variant on, the SBS is coupled using a cryptographic key in the hardware. For the FX/SX/ZX variants, authentication is additionally supplemented by a smartcard.

Smartcard-based protection

The FX/SX variants have an integrated reader for smartcards in SIM card format ID-000. Smartcard and SBS act as the possession component for a strong multi-factor authentication. The encryption of the SBS and all processes are secured by smartcard, be it the rollout, the login to the gateway or software updates. PC/SC forwarding allows performing additional operations on the smartcard, for example signing, encrypting or Windows smartcard logon. The ZX variant is equipped with a card slot for PKI and ID cards in ID-1 format.

Data safe

The product variants FX/SX/ZX offer authorized users a hardware-encrypted data safe for storing data securely and can be used to store data from a VDI session and edit it offline. The data safe can be used in combination with smartcard and PIN entry like a normal memory stick, while Windows, Mac OS or Linux are running.

Data privacy

An instant logout process prevents unauthorized screen reading. When the Secure Boot Stick is disconnected, the computer shuts down immediately. Depending on timeout settings, users can continue their work right where they left after they reconnect. With its multi-factor authentication, the granular assignment of rights, the avoidance of local data storage, the exclusion of Trojans and the secured VPN connection, the SBS meets all technical requirements according to Art. 32 of the German General Data Protection Regulation and the BSI baseline protection. The protection of personal data is thus ensured for all employees using their own devices for work. As the internal private hard drive stays disconnected, no administrator will be able to access private photos or e-mails on employees‘ private computer.

Easy and flexible for users

The Secure Boot Stick is easy to use. After powering on and entering the PIN, the PC boots up and directs the user to chosen systems or applications. Entering the WLAN key is just as simple as on a smartphone and the key is encrypted and stored for future logins. After selecting the desired system or application, users have access to their accustomed environment.

Cost-benefit analysis

According to ECOS customers, the Secure Boot Stick has a savings potential of up to 80% in the overall cost estimate compared to corporate laptops. This is partly due to the significantly lower investments and operating costs, partly to the distinctly reduced support efforts.

Personalization

The provided templates allow flexibly customizing the user interface of the Secure Boot Stick to your CI. Additionally, SBS and smartcards can be fitted with own logos.

ECOS SystemManagementAppliance (SMA)

The ECOS SystemManagementAppliance allows centrally administrating and remotely updating all ECOS access solutions. It is a virtual appliance, operable under VMware, Microsoft Hyper-V, Citrix Hypervisor, Oracle Virtualbox, and Linux KVM or on dedicated hardware. The appliance is operated in the DMZ or the internal network.

Central user and rights management

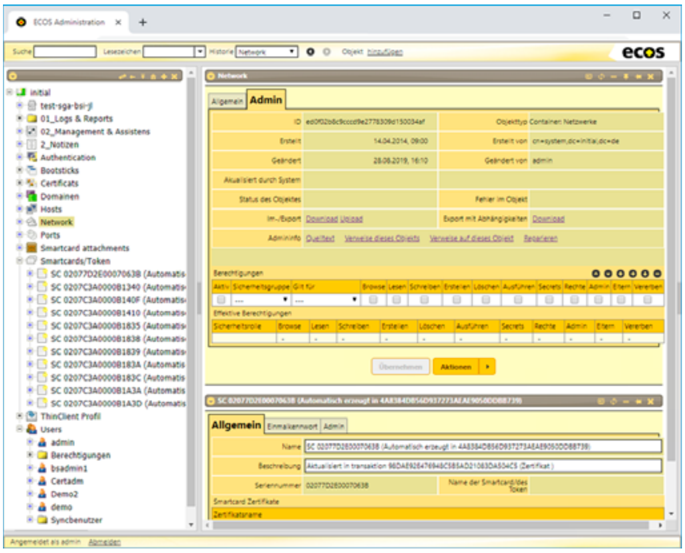
For access to a WTS/VDI environment or web applications, it is possible to create profiles made available to users after application launch. Access rights can be administrated on user, group or role level. A random number of profiles can be created per user and be either remotely shared or revoked. The rights management also allows configuring very granularly the use of local printers or enabling connected USB storage devices for data transfer in a WTS or VDI session. The sharing of external devices can thus be tied to both the vendor ID and the serial number of the device.

Control via AD

The coupling with Active Directory and other directory services allows synchronizing users and rights—even with more than one directory service. It also allows remotely controlling of the SMA from the AD. Assigning a user a particular AD group can thus trigger tasks like issuing an activation code or assigning corresponding rights.

Certificate administration

The System Management Appliance provides its own CA to issue certificates. Alternatively, the SMA allows the usage of existing certificates when coupled to a PKI. Certificates can also be directly generated on smartcards. Certificates can be validated using either a CRL or the integrated OCSP service of the SMA.



Historie: Network

ID	ed0f02b8c9cccd9e2778309d150034af	Objekttyp	Container: Netzwerke
Erstellt	14.04.2014, 09:00	Erstellt von	cn=system,dc=initial,dc=de
Geändert	28.08.2019, 16:10	Geändert von	admin
Akualisiert durch System			
Status des Objektes		Fehler im Objekt	
Im-/Export	Download Upload	Export mit Abhängigkeiten	Download
Admininfo	Quelltext Verweise dieses Objekts Verweise auf dieses Objekt Reparieren		

Berechtigungen

Aktiv	Sicherheitsgruppe	Gilt für	Browse	Lesen	Schreiben	Erstellen	Löschen	Ausführen	Secrets	Rechte	Admin	Eltern	Vererben
□	---	---	□	□	□	□	□	□	□	□	□	□	□

Effektive Berechtigungen

Sicherheitsrolle	Browse	Lesen	Schreiben	Erstellen	Löschen	Ausführen	Secrets	Rechte	Admin	Eltern	Vererben
	-	-	-	-	-	-	-	-	-	-	-

SC 02077D2E00070638 (Automatisch erzeugt in 4A8384D856D937273AEAE9050DD88739)

Name	SC 02077D2E00070638 (Automatisch erzeugt in 4A8384D856D937273AEAE9050DD88739)		
Beschreibung	Aktualisiert in transaktion 98DAE928476948C585AD21083DA534C5 (Zertifikat)		
Seriennummer	02077D2E00070638	Name der Smartcard/des Token	

Smartcard Zertifikate

Zertifikatsname

ECOS system administration interface

Certificate renewal

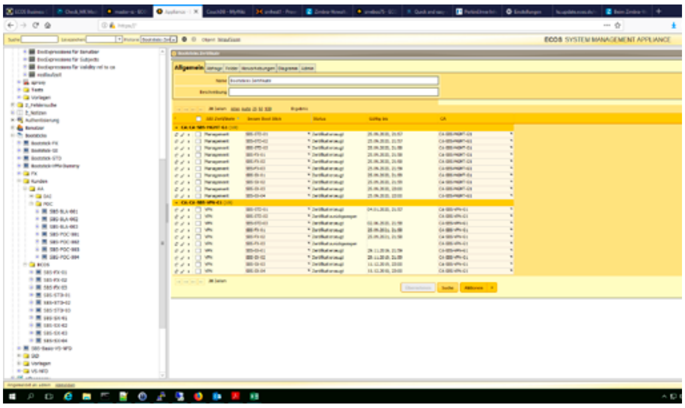
The System Management Appliance renews certificate automatically in the background and requires no administrator or user intervention, regardless whether it is a software certificate or a certificate stored on a smartcard.

Multitenancy capability

The System Management Appliance can map complex multitenancy models and allows configuring separate admin logins, AD connections, PKI connections and CAs for all customers.

Update server

The System Management Appliance serves as central update server for all Secure Boot Sticks. After downloading a new software version, which can be performed with a second evaluation system, the



Certificate renewal

update can be rolled out to chosen users, groups or all users. This makes it easy to model and establish rollout processes on the SMA.

Report editor and active reports

In addition to a range of pre-defined reports, the integrated report editor allows creating various evaluations and storing them for further processing. Active Reports allow the time-controlled dispatch of reports to relevant recipients as well as all users cited by report. Users can thus be notified automatically about pending certificate extensions.

Administration interface

The System Management Appliance possesses a web-based administration interface. The user-specific rights assignment allows modelling administrative roles and respective access rights (e.g. super admin, administrators, helpdesk etc.).

Interfaces

The System Management Appliance can be fully integrated into existing IT infrastructures. All SMA features are remotely controllable with the HTTP interface. An SNMP and a SysLog interface are at disposal for the connection to a monitoring or reporting system. Additionally, the SMA can be connected to AD or other directory services as well as to an existing PKI.

High availability

When combined with the ECOS HA module, the System Management Appliance is operable as high availability solution and supports various internet connections as well as clustering separate sites. This is especially important when the SMA is operated as VPN gateway. If combined with a third-party VPN gateway, it is recommended to operate the SMA redundantly, provided the integrated OCSP service is used for certificate validation, e.g. for gateway login.

ECOS up-to-date service and 3rd level support

ECOS regularly provides updates for the Secure Boot Sticks and System Management Appliance. Updates include compatibility improvements for latest hardware, the update of all applications (including third-party manufacturers) as well as new functions and security features. The up-to-date service also includes a third level support. Our release notes contain detailed information about changes and new features of the respective version.

ECOS 1st level support

ECOS offers a first level support to assist users in the configuration of their ECOS SecureBootStick. This includes changing the boot order to USB, assisting with WLAN configuration, mouse, keyboard or monitor settings and other questions about the use of the Secure Boot Stick and remote access.

Function overview ECOS SecureBootStick	CL	HE	FX	SX	ZX
BSI-approval					
Approved for processing of data with classification level VS-NfD, EU/NATO RESTRICTED				✓	✓
Applications					
RDP client, Citrix Workspace App, VMware Horizon (per RDP, PCoIP, BLAST), Firefox, Chromium, VPN client for IPsec	✓	✓	✓	✓	✓
Citrix HDX RealTime Media Engine for optimizing audio and video transmission for Skype for Business and Microsoft Teams	✓	✓	✓	✓	✓
Microsoft RemoteFX for optimizing the audio quality with RDP	✓	✓	✓	✓	✓
Supported destination systems					
Microsoft RDSH, WTS 2000 and later, RDS, RD sharing, Citrix Virtual Apps & Desktops, VMware Horizon or web server	✓	✓	✓	✓	✓
VPN					
Connection to default gateway via IPsec, OpenVPN or HTTPS | Connection to genua genuscreen via IPsec	✓ | –	✓ | –	✓ | –	– | ✓	– | ✓
Additional VPN clients: Cisco AnyConnect, Juniper, F5 (additional licenses may be required)	✓	✓	✓		
Administration					
Profiles for access to various applications/servers on user, group or role level	✓	✓	✓	✓	✓
Use of local resources after release (external USB storage devices, local printers)	✓	✓	✓	✓	✓
Authorization assignment for external devices tied to manufacturer ID or serial number of the device	✓	✓	✓	✓	✓
Remote update for all applications and firmware	✓	✓	✓	✓	✓
Compatibility					
Integrated smartcard reader for PKI cards with CardOS 5.X in ID-1 format (service ID card, BW military ID card)			✓ | –	✓ | –	– | ✓
Compatible with all customary 64-bit PCs, Macs and tablets with x86 architecture	✓	✓	✓	✓	✓
UEFI Secure Boot support	✓	✓	✓	✓	✓
Keyboard drivers for more than 90 languages and countries	✓	✓	✓	✓	✓
Multi-monitor support	✓	✓	✓	✓	✓
Connection via LAN, WLAN, UMTS, LTE incl. browser for login to hotspot	✓	✓	✓	✓	✓
Software in German and English (pre-configurable)	✓	✓	✓	✓	✓
Data safe					
2 GB, usable to store documents securely (not for VS-NfD)			✓	✓	✓
Hardware encryption with AES256, secured by smartcard + PIN			✓	✓	✓
Installation-free as USB drive under Windows, Linux and macOS			✓	✓	✓
Additional features					
Signing, encrypting or Windows smartcard logon by PC/SC forwarding			✓	✓	✓
Forwarding of external USB and LAN devices, for example to connect IP phones	✓	✓	✓	✓	✓
Automatic reconnect after disconnection or connection change	✓	✓	✓	✓	✓
Multi-factor authentication					
Software certificate, tied to SBS hardware ID | Hardware anchor | Smartcard	✓ | – | –	✓ | ✓ | –	✓ | – | ✓	✓ | – | ✓	✓ | – | ✓
On-screen password entry | Integrated PIN pad for direct PIN entry on SBS	✓ | –	✓ | –	– | ✓	– | ✓	– | ✓
Security					
Read-only partitions | Signed partitions for boot loader and kernel	– | ✓	✓ | ✓	✓ | ✓	✓ | ✓	✓ | ✓
Encryption of all security-related partitions by Software | Hardware	✓ | –	– | ✓	– | ✓	– | ✓	– | ✓
Signed read-only partition for firmware and applications	✓	✓	✓	✓	✓
Writeable partition for storage of user parameters	✓	✓	✓	✓	✓
Hardened ECOS Secure Linux operating system	✓	✓	✓	✓	✓
Digitally signed boot loader, firmware and applications with chain of trust verification	✓	✓	✓	✓	✓
Securing of all processes by smartcard (e.g. Easy Enrollment, gateway login, SBS update)			✓	✓	✓
Integrated firewall for protection against attacks within the same network and blocking of ping requests	✓	✓	✓	✓	✓
Encryption of RAM content except for the executable program code	✓	✓	✓	✓	✓
VM start detection preventing use in virtual environment	✓	✓	✓	✓	✓
Fingerprinting of guest computer incl. periphery (V7 and higher)	✓	✓	✓	✓	✓
Instant logout on SBS disconnection	✓	✓	✓	✓	✓
Secured process for firmware and application update with verifi cation of integrity and correct update servers	✓	✓	✓	✓	✓
Connection, dimensions and scope of delivery					
USB A | C	✓ | – | –	✓ | – | –	✓ | ✓ | ✓	✓ | ✓ | ✓	✓ | ✓ | ✓
Dimensions (W, H, D)	12x22x4	12x41x4	28x85x13	28x85x13	28x85x14
Weight (g)	3	6	68	68	72
Stick | Carry strap | 2 connection cables for USB (A and C)	✓ | ✓ | –	✓ | ✓ | –	✓ | ✓ | ✓	✓ | ✓ | ✓	✓ | ✓ | ✓

Function overview ECOS SystemManagementAppliance (SMA)

Central management of all ECOS products	
User and rights administration on user, group and role level	✓
Rights assignment for destination systems with distributed servers	✓
Sharing of local devices such as storage devices and printers	✓
Remote rights assignment and revocation	✓
Integration into existing infrastructure	
Virtual appliance for operation with VMware, Citrix Hypervisor, Hyper-V, Oracle VM VirtualBox or on a dedicated hardware	✓
Synchronization with AD or other directory services	✓
Control of all system management functions possible via REST API	✓
Certificate management	
Integrated CA (Certificate Authority)	✓
Alternatively: connection to an existing PKI	✓
Certificate rollout on smartcards	✓
Provision of CRL or OCSP server	✓
Central password policy	✓
Smart reports	
Predefined reports	✓
Report editor	✓
Active reports	✓
Token lifecycle management	
Easy Enrollment	✓
Creating and blocking accesses centrally	✓
Distribution to single users, groups or all users	✓
Remote updating of access solutions	
Central update server	✓
Distribution to single users, groups or all users	✓
Multitenancy management	
Separate administrator logins	✓
Separate AD connection	✓
Separate PKI connection	✓
Separate CAs	✓
Administrator interface	
Web-based	✓
User-specific rights assignment (admin, helpdesk, HR etc.)	✓
Interfaces	
HTTP API, LDAP, SysLog, SNMP	✓
Integrated VPN gateway (IPsec, SSL VPN) and authentication server	
unlimited number of VPN users	✓
unlimited number of VPN tunnels	✓
Miscellaneous	
Redundant and highly available in combination with HA module	✓
Scope of Delivery	
ISO image with ECOS Secure Linux and ECOS SystemManagementAppliance	✓
Smartcard reader (Professional-X and Enterprise-X)	✓

Licensing

SMA100 ECOS SystemManagementAppliance [Starter]	up to 99 users
SMA110 ECOS SystemManagementAppliance [Professional]	up to 999 users
SMA120 ECOS SystemManagementAppliance [Enterprise]	1.000 users and more
SMA111 ECOS SystemManagementAppliance [Professional-X] für SBS FX, SX, ZX	up to 999 users
SMA121 ECOS SystemManagementAppliance [Enterprise-X] für SBS FX, SX, ZX	1.000 users and more

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.