ECOS SECURE BOOT STICK®

Highly Secure Access to Data and Applications

- Easy
- Flexible
- Highly secure

Security without any compromise

Our working world increasingly demands the flexibilization of working hours and location, but setting up home workstations or alternating teleworking stations frequently reaches limits. There are either no resources for secured notebooks or the administrative effort is too heavy. Private devices can not be permitted for security reasons.

Moreover, IT security requirements rise in a growing threat situation. This applies not only to the use of private devices outside the company, but also to the connection of external service providers and customers. Those responsible also protect themselves against threats from the real world, such as natural disasters. ECOS SECURE BOOT STICK allows for the first time public authorities, companies and other organizations to admit private and non-business PCs while observing the highest security requirements, and this even regarding the editing of confidential documents classified as RESTRICTED. Compared to other solutions, administration efforts and costs can thus be cut significantly while user satisfaction and especially the security level are considerably improved.

Benefits at a Glance:

+ Hardened ECOS Secure Linux operating system
+ 100% separation of company from 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 RESTRICTED**

* SECURE BOOT STICK [FX] [SX] [ZX]
** SECURE BOOT STICK [SX] [ZX]

ECOS SECURE BOOT STICK Product Range

ECOS SECURE BOOT STICK provides users with a highly secure access to the data and applications of their company or organization from any PC or Mac. The security requirements often vary depending on the customer's needs.

The ECOS product family covers various security requirements. The ECOS SECURE BOOT STICK [CL] offers customers a high security level at a particularly attractive price. Since the first version, brought to market in 2007, a high level of expertise in the matter of security, integration into the infrastructure and hardware compatibility has shaped this product and its continuous development.

The ECOS SECURE BOOT STICK [HE] takes the proven solution to new security level with a specially developed, hardware-encrypted USB stick equipped with different security features.

The ECOS SECURE BOOT STICK [FX], just like the [HE], provides a range of security features that have been cast in a hardware mold. In addition to this, it has also an integrated smartcard and an integrated keyboard to enter the PIN directly on the stick, while all encryptions and processes are secured by the smartcard.

The ECOS SECURE BOOT STICK [SX] is the flagship of the product family. Though widely identical to the [FX], the [SX] is BSI-certified to allow the access to data and applications classified confidential RESTRICTED and this even in conjunction with a private PC or Mac.

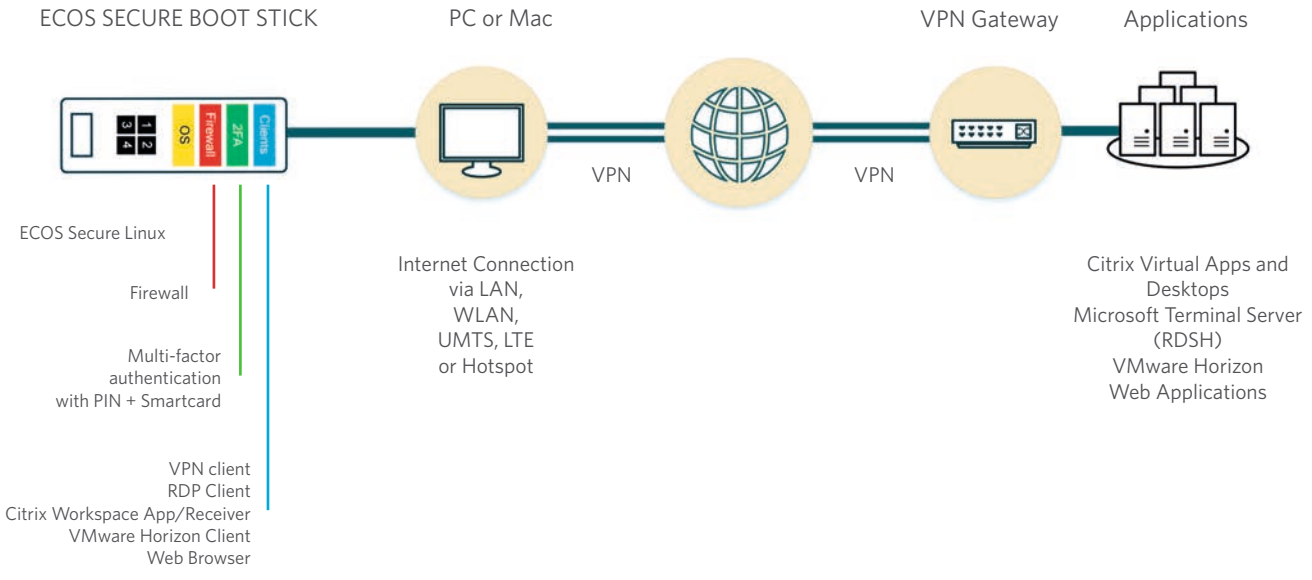
The ECOS SECURE BOOT STICK [ZX], with its card slot in format ID-1, allows the use of PKI cards and identification cards for user authentication. Furthermore, it's identical to the [SX] in structure and software. Like this counterpart, the [ZX] is BSI-certified for level RESTRICTED too.

ECOS SECURE BOOT STICK [CL]

ECOS SECURE BOOT STICK [HE]

ECOS SECURE BOOT STICK [FX] / [SX]

ECOS SECURE BOOT STICK [ZX]



Application Scenario ECOS SECURE BOOT STICK

Highly Secure into Public Authority/Company Networks

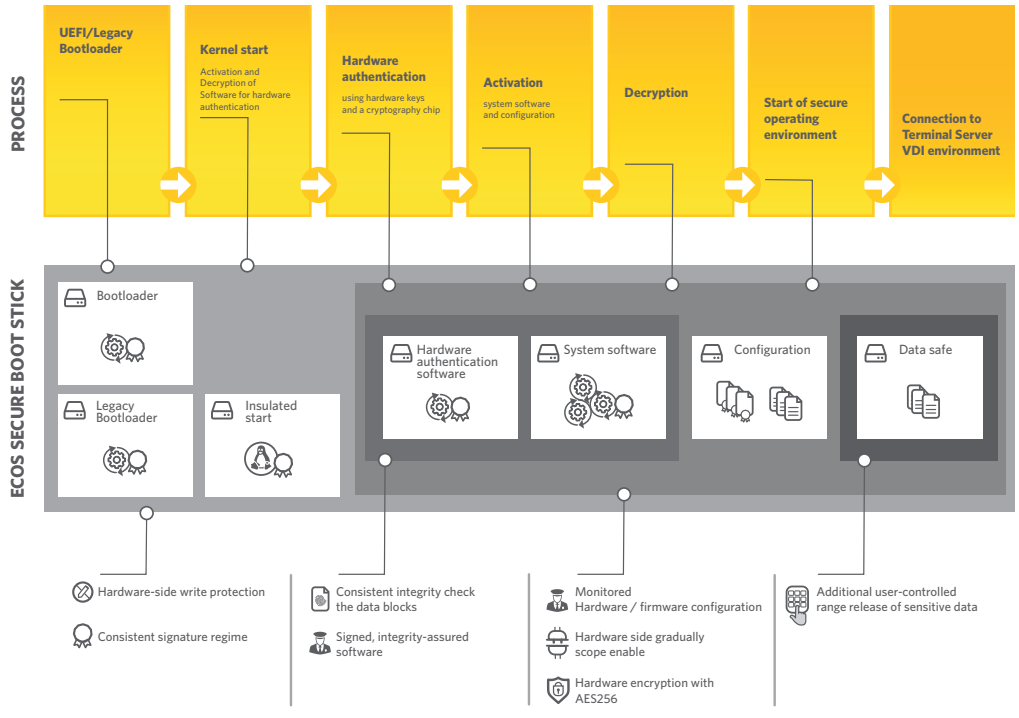
All products of the ECOS SECURE BOOT STICK family provide a highly secure access to a terminal server or virtual desktop infrastructure and web applications within a secure and encapsulated environment. With this stick, any PC or Mac boots up the specially hardened ECOS Secure Linux operating system. The internal hard drive stays deactivated, so potential malware on the hard drive will never get any chance. Disconnecting the internal hard drive ensures 100% separation of corporate and private usage of the PC. The public authority or company stick contains all firmware and applications required. The private PC is thus only a private periphery.

All Software on a Stick

The stick contains the clients required for a highly secure access to Microsoft RDSH (formerly Windows Terminal Server), Citrix Virtual Apps and Desktops (formerly XenApp und XenDesktop), VMware Horizon (formerly VMware View) as well as PCs with remote desktop sharing. The stick 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 through 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, an NCP client, Cisco AnyConnect (per SSL), a Juniper client and F5 are also available. Regarding the BSI-certified [SX]/[ZX], genua genuscreen is mandatory as VPN gateway according to the use and the operating conditions for RESTRICTED.



Schematic view of ECOS SECURE BOOT STICK [HE] [FX], [SX], [ZX]

ECOS Easy Enrollment allows to roll out a large number of accesses in a very short time. All users receive identically pre-configured sticks. The central management generates personal activation codes or, in the case of [FX]/[SX], issues personal smartcards which provide the sticks with the user-specific configuration. The [ZX] variant is coupled to an already existing PKI card or a personal ID card through the synchronization of public keys. The central management, further described below, allows to centrally administrate and remotely update all sticks.

Maximal Compatibility

The implementation of private end devices increases compatibility requirements. The ECOS SECURE BOOT STICK therefore contains drivers for all marketable PCs, Macs and x86-based tablets. This includes graphics drivers, LAN, WLAN, UMTS and LTE drivers as well as a browser for hotspot logon. For an optimal transmission of audio and video signals, especially with Microsoft Skype for Business and Microsoft Teams, the Citrix HDX RealTime Media Engine has been integrated. 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 set through the central management. Further USB devices, such as foot pedals for dictation devices, are supported to a certain extent.

Structure of ECOS SECURE BOOT STICK

During the design of ECOS SECURE BOOT STICK, highest security requirements ranked first. The stick contains different partitions that are successively unlocked during the boot process

Application Scenarios

Customers operate the ECOS SECURE BOOT STICK 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 try to gain more time for the care and education of their children. In times of demographic change and considering the lack of caregivers, caring for elder family members also plays an increasing role.

However, the career shouldn't fall by the wayside. The active participation in working life is also particularly important for elderly persons or persons with restricted mobility. Considering the much deplored and acute skills shortage, it is thus 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 operations can't wait until the next work day just because the company notebook is still at the office. Besides, children don't announce diseases 24 hours in advance. Solutions allowing the use of the private PC while meeting the highest security requirements don't only increase employee satisfaction, but also the company's efficiency.

Connecting External Employees

Many public authorities and companies regularly draw on external consultants and service providers for important tasks. But processes such as connecting non-business laptops to the internal network or enabling the remote access to databases and specialist applications for third parties also place particularly high demands on IT security.

IT and Remote Maintenance

To maintain IT infrastructure and specialist applications, professionals need a 24/7 access to the relevant systems. The remote access to critical systems requires particularly high security arrangements. This applies especially to external service providers who typically use their own notebook and expect a connection to local networks.

Secure Access, Home and Abroad

In many countries, the entry requirements allow local authorities the unrestricted access to notebooks and storage devices. Potential encryptions must be disclosed upon request for inspection or to copy data. Many companies therefore only allow notebooks that are free of any data or documents. Despite these guidelines the necessity to access important data while on the road still 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 from the home PC obviates unnecessary downtimes or expensive emergency offices as long as the relevant IT security and data protection requirements are met.

RESTRICTED on a Customary PC

Federal authorities, the Federal Armed Forces and all companies dealing with classified information have acknowledged the imperatives long ago. These requirements are progressively introduced in the area of critical infrastructure and other security-related companies. The processing of documents classified RESTRICTED requires the use of BSI-certified end devices, not only in the management, but also for software developers or engineers. Solutions in form of a hardened notebook don't really satisfy users and certainly not financial controlling departments. The BSI-certified ECOS SECURE BOOT STICK [SX]/[ZX] allows for the first time the access to RESTRICTED from a customary PC.

by the immediately preceding security check or authentication procedure. Boot loader, firmware and application partitions are respectively write-protected, which is performed through a hardware-side write protection for the [HE] product variant.

Moreover, all areas of the stick, starting with the boot loader, are consistently encrypted by an AES 256-bit encryption which is software-encrypted in the [CL] variant and hardware-encrypted for all others. ECOS SECURE BOOT STICK [FX]/[SX]/[ZX] also provides a data safe for document storage. This data safe is designed as hardware-encrypted drive and protected by smartcard and PIN entry.

Multi-factor Authentication

ECOS SECURE BOOT STICK offers not only the safety of a secured and encapsulated environment, it also serves as strong multi-factor authentication. The [CL] variant contains a certificate tied to the stick's hardware ID for personalization purposes. From [HE] on, the stick is coupled through a cryptographic key in the hardware. For the variants [FX]/[SX]/[ZX], authentication is additionally supplemented by a smartcard.

Protection by Smartcard

ECOS SECURE BOOT STICK [FX] and [SX] respectively contain a smartcard reader for smartcards in SIM card format ID-000. Smartcard and stick act as the possession component for a strong multi-factor authentication. The encryption of the stick and all processes are secured by smartcard, be it the rollout, the login to gateway or the stick's update. PC-/SC- forwarding allows to use the smartcard for additional functions, for example signing, encrypting or Windows smartcard logon. In the [ZX] variant, the stick is equipped with a card slot for PKI cards and IDs in ID-1 format.

»The good thing with this solution is that the user can effectively do nothing wrong.«

Jürgen Berger| Group Leader Systems-Management & Software Distribution | HUK-COBURG

Data Safe

The product variants [FX]/[SX]/[ZX] provide a hardware-encrypted data safe that allows the user to store data securely on the stick. Provided the user is properly authorized, it can, for instance, be used to store data from a VDI session on the stick 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 Security

A special instant logout process prevents unauthorized reading of display content. Once the stick is disconnected, the computer immediately shuts down. Depending on the timeout that has been set, users can continue their work right where they left after reconnecting the stick. With its multi-factor authentication, the granular assignment of rights, the avoidance of any kind of local data storage, the exclusion of Trojans and the secured VPN connection, ECOS SECURE BOOT STICK meets all technical requirements according to Art. 32 of the German General Data Protection Regulation and the BSI basic protection. The protection of their personal data is ensured for staff members who use their own devices. As the internal, private hard drive is disconnected, an administrator will never be able to access private photos or e-mails on the computer.

Security Concept

ECOS SECURE BOOT STICK features the cascading of various security measures which, added together, provide an extremely high security level. The following safety assessment lists potential threat scenarios and shows the measures 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 corresponding ECOS SECURE BOOT STICK or, depending on the product variant, the corresponding smartcard.

Protection Against Manipulation

The ECOS SECURE BOOT STICK presents various protection measures against possible manipulations. First, firmware and applications are on a write-protected partition. Thereover the boot loader 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 is connected to the gateway by a secured VPN connection that will be only be established if the authentication has been successfully completed. All relevant parts of the firmware are stored on a write-protected partition to protect the stick 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.

Targeted attacks exploiting the system management mode are repeatedly parried by the ECOS SECURE BOOT STICK. In the early boot process, BIOS or UEFI are inspected for potential malware. For particularly security-relevant authorities and 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 of the hardware are thus both detected. Hardware-side attacks that, for example, aim at reading out key material from the main memory, are thwarted by the encryption at many points.

Protection Against Online Attacks

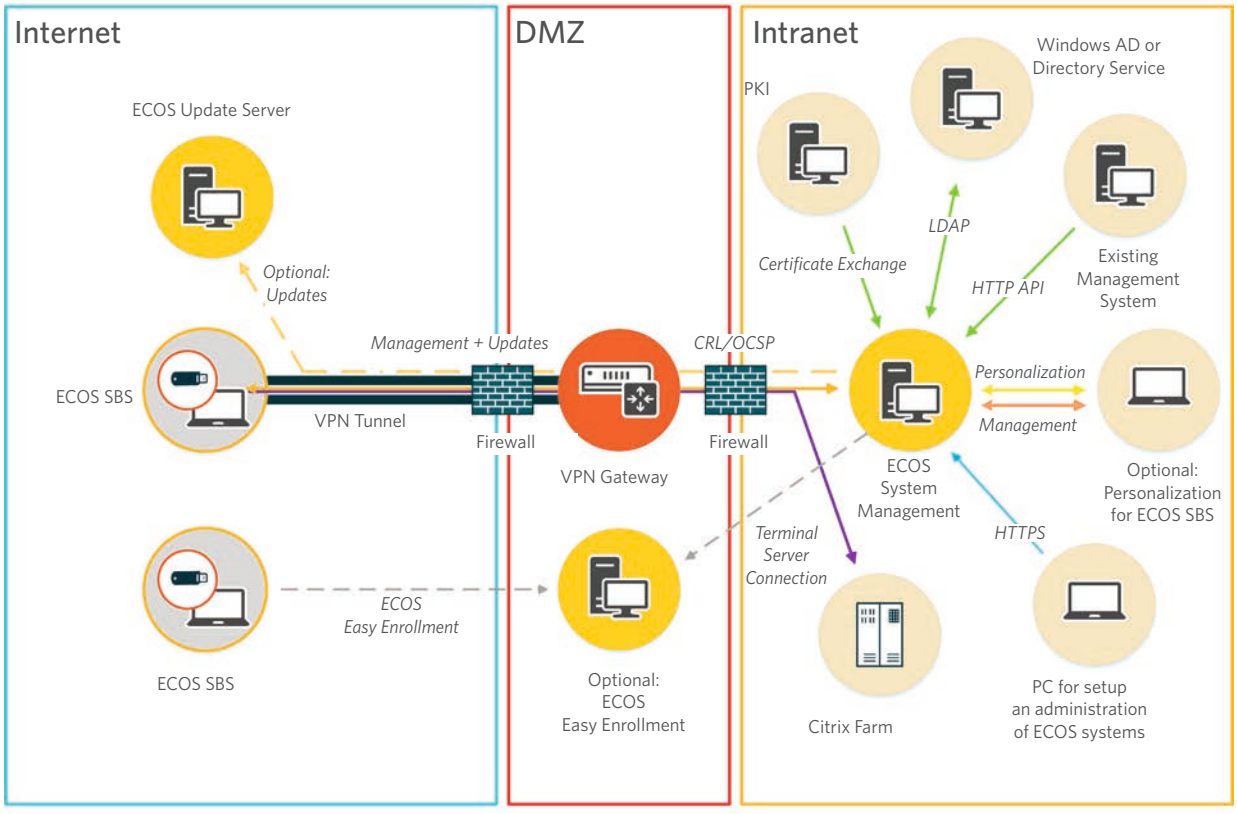
The ECOS Secure Linux operating system is a lean system designed to provide only those parts of an operating system that are required to run the solution. Potential security gaps are thus significantly reduced right from the start. Besides, the operation system has been specially hardened and compiled to meet the highest security requirements. ECOS SECURE BOOT STICK provides its 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 computer.

Protection Against Unwanted User Interventions

The system checks whether the stick is booting in a virtual machine before executing the firmware. This prevents the undermining of the existing 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

As soon as the stick is connected 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 stick is booted.



Example: integration into the existing infrastructure of the ECOS SECURE BOOT STICK [CL]/[HE]

Easy and Flexible for Users

ECOS SECURE BOOT STICK is fairly easy to use. After start-up and PIN entry, the PC or Mac boots up and directs the user to a selection of released systems or applications. For WLAN operation, the key entry is just as simple as on a smartphone and the key is encrypted and stored for future logins. After selection of the desired system or application, users have access to their accustomed environment.

Cost-Benefit Analysis

According to ECOS customers, ECOS SECURE BOOT STICK has a savings potential of up to 80% compared to the usage of public authority/corporate notebooks in the overall cost estimate. This is partly due to the significantly lower investments and operating costs, partly to the distinctly reduced support efforts.

Individualization

The provided templates allow to flexibly customize the user interface of the ECOS SECURE BOOT STICK to the own CI. Additionally, sticks and smartcards can be fitted with own logos.

ECOS SYSTEM MANAGEMENT APPLIANCE

The ECOS SYSTEM MANAGEMENT APPLIANCE allows to centrally administrate and remotely update all ECOS access solutions. It's a virtual appliance, operable under VMware, Microsoft Hyper-V, Citrix Hypervisor, Oracle Virtualbox, 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 that are available to users after starting the application. Access rights can be administrated on user, group or role level. A random number of profiles can be created per user and then be either remotely shared or revoked. The rights management also allows to determine very granularly the use of local printers or to enable connected USB storage devices for the data transfer with a WTS or VDI session. The sharing of external devices can thus be tied both to the vendor ID and the serial number of the device.

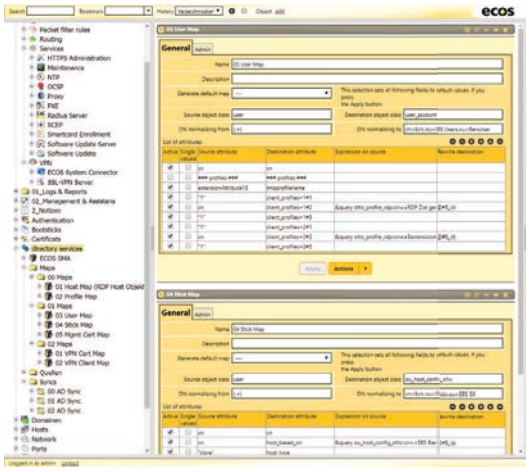
Control via AD

The coupling with Active Directory or other directory services allows to synchronize users and rights, even with more than one directory service. It also allows a remote control of the SMA from within the AD.

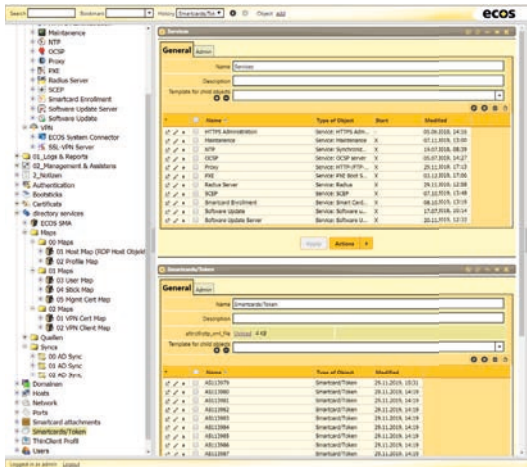
Attributing a user to a particular group in the AD can thus trigger the issuing of an activation code or the assignment of corresponding rights.

Certificate Administration

The ECOS SYSTEM MANAGEMENT APPLIANCE contains its



System Administration Interface: Directory Services



System Administration Interface: Smardcard Management

own CA to issue certificates. Alternatively, it also allows to use existing certificates when coupled to an existing PKI. For the use with smartcards, certificates can be generated directly by the SMA on the smartcard. Certificate validation can be performed either by using a CRL or the OCSP service integrated in the SMA.

Certificate Extension

The SMA also takes over the renewal of certificates and can operate fully automatically in the background without requiring any administrator or user intervention, regardless whether it's a software certificate or a certificate stored on the smartcard.

Multitenancy Capability

The ECOS SYSTEM MANAGEMENT APPLIANCE can map a complex multitenancy model. It is thus possible to configure separate admin logins, AD connections, PKI connections and CAs for all customers.

Update Server

The ECOS SMA serves as central update server for all ECOS SECURE BOOT STICK. After the download of a new software version, which can, if applicable, be performed through a second evaluation system, the update is rolled out to single persons, groups or all users. Established rollout processes are thus easily definable in the SMA.

Report Editor and Active Reports

In addition to a wide range of pre-defined reports, the integrated report editor allows to create various evaluations and store them for further processing. Moreover, Active Reports allow the time-controlled dispatch of reports to relevant recipients as well as all users cited in the report. Users can, for example, be informed automatically about pending certificate extensions.

»The encapsulated, self-contained technology requires no particular update or patches on the computer, which lets me and my IT colleagues sleep far better.«

Florin Comanici
RAS-Service Manager at BayernLB

Admin Interface

The system management appliance is operated through a web-based admin interface. The user-specific rights assignment maps out the roles and the respective access rights, for example for the super admin, administrators, the helpdesk or the personnel management.

Interfaces

The ECOS SYSTEM MANAGEMENT APPLIANCE allows a full integration into the existing IT infrastructure. All of the appliance's features are remotely controllable through the HTTP interface. An SNMP and a SysLog interface are at disposal for the connection to an existing monitoring or reporting system. Additionally, the SMA allows the connection to AD or other directory services and the connection to an existing PKI.

VPN Gateway

In combination with the ECOS MOBILE OFFICE STICK and the ECOS VIRTUAL WEB CLIENT, the ECOS SYSTEM MANAGEMEN APPLIANCE additionally allows to manage the access components, necessarily also as VPN gateway. The ECOS SECURE BOOT STICK interfaces with the gateways of almost all manufacturers or use the SMA as VPN gateway.

»The Secure Boot Stick from ECOS offers our employees the greatest possible flexibility and productivity at work, at home and on the road. In the same time, sensitive data is optimally protected.«

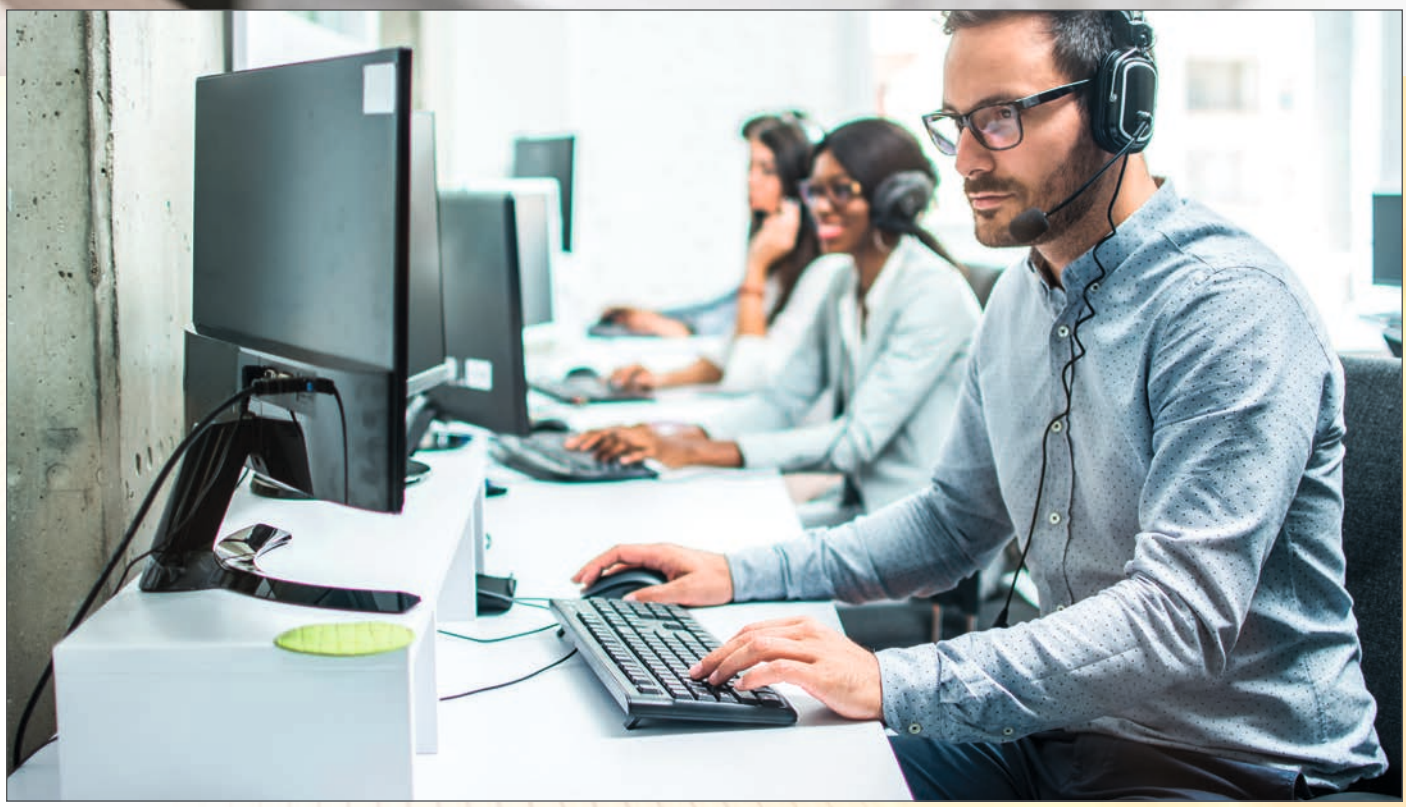
Holger Hofmann | Senior Government Official and Head of Unit Information Technology of Hessian Ministry of Justice

»This is an important step in our HR development concept regarding the reconciliation of work and family life.«

Ulrich Kupczik | Deputy Caritas Director

High Availability

In conjunction with the ECOS HA module, the ECOS SYSTEM MANAGEMENT APPLIANCE can be operated as high availability solution. It supports various internet connections as well as the clustering of separated locations. This is especially important when the SMA is operated as VPN gateway. In combination with a VPN gateway of a third-party manufacturer, it is recommended to operate the SMA redundantly, provided the integrated OCSP service is used to validate the certificates, for example for the login to the gateway.



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

ECOS regularly provides updates for the ECOS SECURE BOOT STICK and the ECOS SYSTEM MANAGEMENT APPLIANCE.This encompasses the latest hardware for new PCs, the update of all applications (including third-party manufacturers) as well as new functions and security features. The up-to-date service also includes the access to the 3rd level support. The accompanying release notes contain all information about the changes and features of the corresponding version.

ECOS 1st Level Support

ECOS offers 1st level support to assist users in the configuration of their ECOS SECURE BOOT STICK. This includes changing the boot order to boot USB, questions about WLAN configuration, mouse, keyboard or monitor settings and other questions about the use of the stick and the access to the own infrastructure.

Function Overview ECOS SECURE BOOT STICK	[CL]	[HE]	[FX]	[SX]	[ZX]
BSI Certification					
Certified for data processing up to classification level RESTRICTED				■	■
Applications					
RDP client, Citrix Workspace App, VMware Horizon (per RDP, PCoIP, BLAST), Firefox, Chromium, VPN client for IPsec	■	■	■	■	■
Citrix HDX RealTime Media Engine to optimize audio and video transmission with Skype for Business and Microsoft Teams	■	■	■	■	■
Microsoft Remote FX for optimization of audio quality in combination with RDP	■	■	■	■	■
Supported Destination Systems					
Microsoft RDSH, WTS 2000 and higher, RDS, RD sharing, Citrix Virtual Apps and Desktops, VMware Horizon or web server	■	■	■	■	■
VPN					
Connection to any gateway via IPsec, OpenVPN or https | Connection to genua genuscreen via IPsec	■ | -	■ | -	■ | -	- | ■	- | ■
Other VPN clients: NCP, 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 (data safe, 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 und firmware	■	■	■	■	■
Compatibility					
Integrated smartcard reader for cards in format ID-000 | PKI cards, IDs in format ID-1			■ | -	■ | -	- | ■
Driver for all current 64-bit PCs, Macs and tablets with x86 architecture	■	■	■	■	■
UEFI secure boot support	■	■	■	■	■
Keyboard drivers for more than 90 languages and countries	■	■	■	■	■
Multi-monitoring support	■	■	■	■	■
Connection by LAN, WLAN, UMTS, LTE incl. browser for login to hotspot	■	■	■	■	■
Software in German and French (pre-configurable)	■	■	■	■	■
Data Safe					
2 GB, usable to store documents securely (not for RESTRICTED)			■	■	■
Hardware encryption by AES256, secured by smartcard plus PIN			■	■	■
Installation-free use as USB drive under Windows, Linux and Mac OS X			■	■	■
Additional Features					
Signing, encrypting or Windows smartcard logon by PC-/SC- forwarding			■	■	■
Forwarding of external USB and LAN devices, for example to connect an IP phone	■	■	■	■	■
Automatic reconnect after disconnection or connection change	■	■	■	■	■
Multi-factor Authentication					
Software certificate, tied to the stick's hardware ID | Hardware anchor | Smartcard	■ | - | -	■ | ■ | -	■ | - | ■	■ | - | ■	■ | - | ■
Password input on screen | Integrated keyboard for PIN entry on stick	■ | -	■ | -	- | ■	- | ■	- | ■
Security					
Write-protected | signed partitions for boot loader and kernel	- | ■	■ | ■	■ | ■	■ | ■	■ | ■
Encryption of all security-related partitions by software | Hardware	■ | -	- | ■	- | ■	- | ■	- | ■
Write-protected, signed 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 verification in »chain of trust« procedure	■	■	■	■	■
Securing of all processes by smartcard such as Easy Enrollment, gateway login, stick 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	■	■	■	■	■
Use in virtual environment forbidden	■	■	■	■	■
Fingerprinting of the guest computer incl. periphery (V7 and higher)	■	■	■	■	■
Instant logout on stick disconnection	■	■	■	■	■
Secured process for firmware and application update with verification of integrity and correct update servers	■	■	■	■	■
Connection, Dimensions and Scope of Delivery					
USB connector A | C | Micro	■ | - | -	■ | - | -	■ | ■ | ■	■ | ■ |■	■ | ■ | ■
Dimensions (W, H, D)	12x22x4	12x41x4	28x85x13	28x85x13	28x85x14
Weight (g)	3	6	68	68	72
Stick | Carry strap | 3 connection cables for USB (A, C and micro)	■ | ■ | -	■ | ■ | -	■ | ■ | ■	■ | ■ | ■	■ | ■ | ■

Function Overview ECOS SYSTEM MANAGEMENT APPLIANCE (SMA)

Central Management of all ECOS Products	
User and rights administration on user, group and role level	■
Authorization assignment for target systems for distributed servers	■
Sharing of local devices such as storage devices and printers	■
Remote assignment and revocation of rights	■
Integration into the Existing Infrastructure	
Virtual appliance for operation under VMware, Citrix Hypervisor, Microsoft Hyper-V, Oracle VM VirtualBox or on certified hardware.	■
Synchronization with AD or other directory services	■
Control of all features of the system management via HTTP-API possible	■
Certificate Administration	
Integrated CA (Certificate Authority)	■
Alternatively: Connection to an existing PKI	■
Rollout of certificates on smartcards	■
Provision of a CRL or an OCSP server	■
Central password policy	■
Smart Reports	
Predefined reports	■
Report editor	■
Active Reports	■
Token LifeCycle Management	
Easy Enrollment	■
Central creation and blocking of accesses	■
Distribution to single users, groups or all users	■
Remote Updating of Access Solutions	
Central update server as part of the SMA	■
Distribution to single users, groups or all users	■
Multitenant Administration	
Separate admin logins	■
Separate AD connection	■
Separate PKI connection	■
Separate CAs	■
Admin Interface	
Web-based	■
User-specific rights assignment (super admin, admin, helpdesk, personnel management...)	■
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 conjunction with HA module	■
Scope of Delivery	
ISO image with ECOS Secure Linux and ECOS SYSTEM MANAGEMENT APPLIANCE	■
Smartcard reader (Professional-X and Enterprise-X)	■

Licensing

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

ECOS TECHNOLOGY GMBH
Sant-Ambrogio-Ring 13a
D-55276 Oppenheim

Phone: +49 (6133) 939-200
E-Mail: info@ecos.de
Internet: www.ecos.de

146.PB.2020/01.EN.01.1