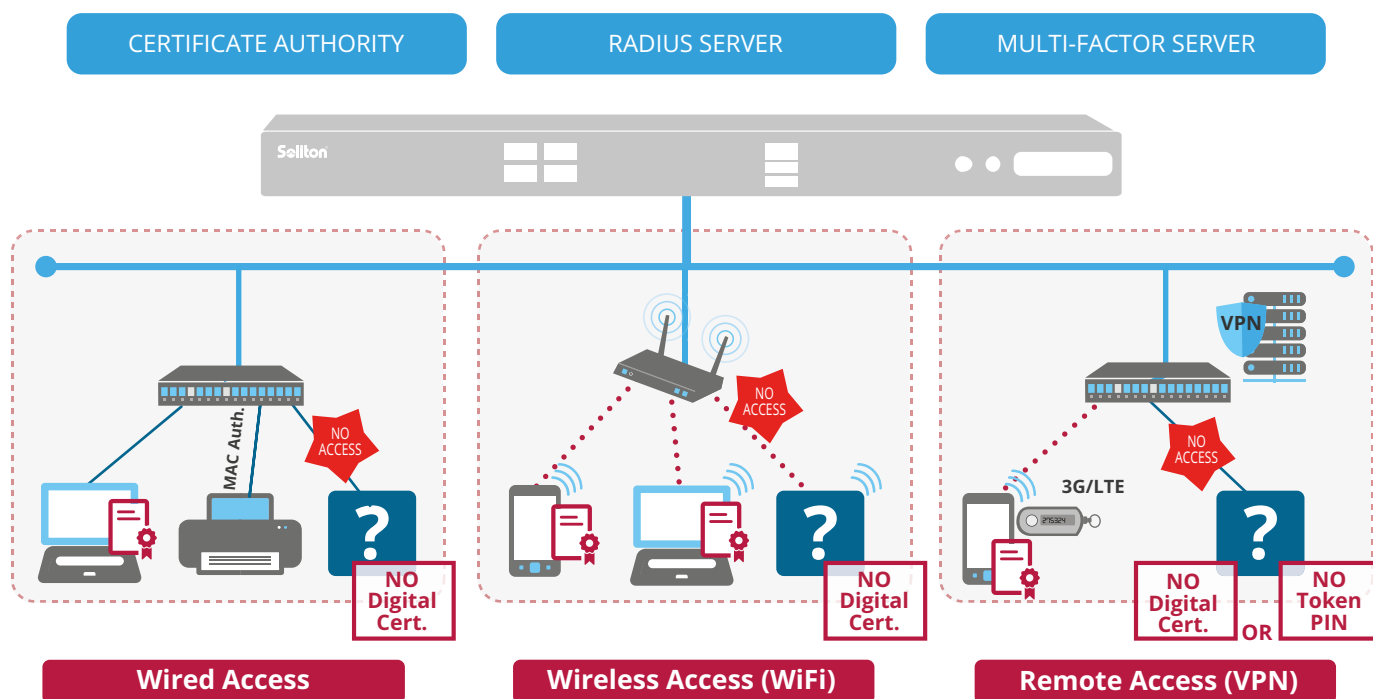


NetAttest EPS Series

With the NetAttest EPS series network administrators can easily implement network access control. Based on the IEEE 802.1X standard the NetAttest EPS series is an all-in-one port-based network access control solution that acts as an authentication and authorization server. It deploys certificates to authenticate users and devices, and to authorize users access to their permitted network resources. The NetAttest EPS series protect the company's network and its elements from unauthorized access and breaches that may lead to the loss of data.



FEATURES AND BENEFITS

The NetAttest EPS series supports a number of key features, including:



ALL-IN-ONE APPLIANCE

The NetAttest EPS embeds features for optimum administering of security functions:

- Conducts user requests to access company's resources and provides authentication, authorization, and accounting (AAA) services.
- The build-in RADIUS server provides multiple EAP authentication methods including MAC address, One-Time Passwords (OTP) or certificate-based authentication, etc.
- Acts as a dedicated certificate authority (CA) issuing and managing certificates. It can also act as a subordinate CA which integrates into an existing Public Key Infrastructure (PKI).



IEEE 802.1X WLAN ACCESS CONTROL

With the NetAttest EPS network administrators can manage the access to the WLAN securely. Guests, temporary employees or contractors can use the self-service portal to request temporary access to the WiFi. When authenticated the guest user is automatically directed to the right network resources. The NetAttest EPS also provides an internal user database for storing temporary employees or contractors.



EASY TO BACK-UP AND RESTORE

Back-up takes less than 20 seconds and a full restore approximately 100 seconds. The full restore includes the CA function and the RADIUS function.



EASY TO MAKE REDUNDANT INSTALLATIONS

In case of a redundant configuration the RADIUS server on both units are active. The network access servers require configuration to use the first NetAttest EPS unit as the primary RADIUS server and the second unit as the secondary RADIUS server. The full configuration, including the CA configuration, is automatically shared daily. In case the master CA crashes, the backup CA will take over.

Options

NetAttest EPS

CA (CERTIFICATE AUTHORITY) EXTENDED OPTION

Key features include:

- **Web-portal:** A self-service portal for end-users to request and download their own user and/or device certificate. Certificates are issued automatically or after approval by the administrator.
- **Online Certificate Status Protocol (OCSP) Responder:** The CA extended option offers OCSP-Responder for easy checking of revocation of certificates.
- **Support of Simple Certificate Enrolment Protocol (SCEP):** The embedded SCEP-server makes the issuing of digital certificates simple and scalable for other IT systems, such as MDM systems or third-party devices, that require a certificate for authentication.
- **Customizable Certificate Signing Request (CSR) templates:** The CSR templates include any kind of data of extended key usage and key generation such as certificate validity period and renewal period.
- **Special-purpose certificates:** The CA extended option allows the administrator to generate special purpose certificates such as Windows SmartCard, Code Signing and Domain Controller certificates.

MAC ADDRESS EXTENDED OPTION

With the MAC address extended option network administrators have a dedicated database available that allows the authentication of MAC addresses of non-802.1X supplicants. The database can store up to 200,000 MAC addresses.

Other features include:

- The MAC address extended option automatically detects the non-IEEE 802.1X supplicants in the network and adds them to the whitelist.
- The dedicated interface for the registration of new MAC-addresses allows the administrator to quickly add new devices to the network.

NETATTEST EPS-*ap*

The NetAttest EPS-*ap* provides a unified deployment process, through the Soliton Key Manager (SKM), for distributing and installing digital certificates on any device and platform. The deployment process is always the same regardless the device and its operating systems.

The NetAttest EPS-*ap* key features:

- Proxy-server: Handles SCEP requests and adds additional security by protecting the internal Certificate Authority (NetAttest EPS) by URL rewriting and forwarding an SSL/TLS encrypted SCEP request to the internal Certificate Authority (NetAttest EPS).
- OTA protocol: Embeds the Apple Over-The-Air (OTA) protocol supporting certificates on Apple devices.

MDM option for NetAttest EPS-*ap*

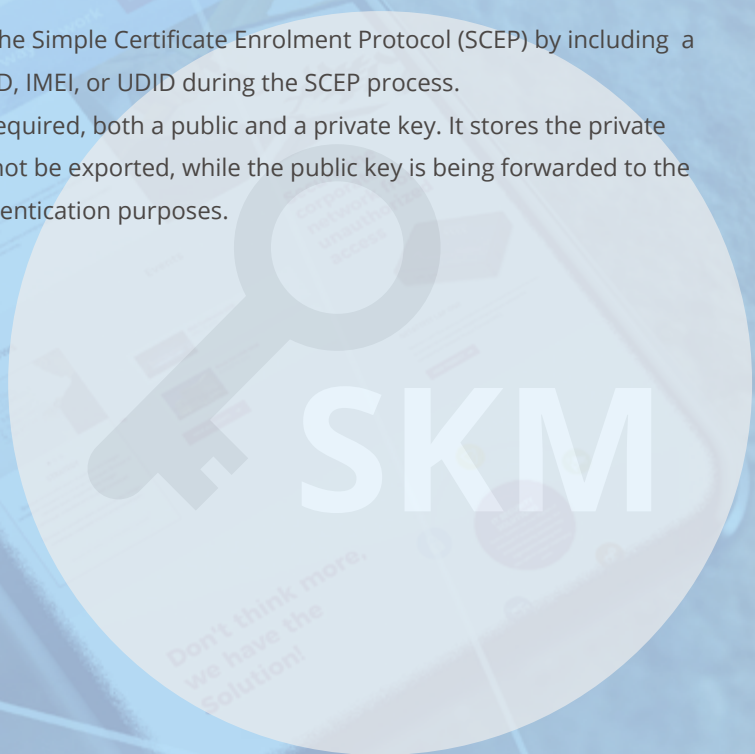
For additional security the NetAttest EPS-*ap* provides a set of Mobile Device Management (MDM) features. It allows to create a profile including several MDM functions such as the automatic locking after a predefined time and the prerequisites of defining the password. Other functions include remote device lock and wipe and the possibility to obtain device information.

SOLITON KEY MANAGER APP

The Soliton Key Manager app makes it easy for network administrators to use short-life certificates for enhanced security. The application offers a user-self-service to automatically request and install user- and device certificates on any device in just 3 steps. The Soliton Key Manager app sends the user a warning to renew the certificates upon users click the link to renew the certificate.

Other key benefits include:

- Soliton Key Manager adds security to the Simple Certificate Enrolment Protocol (SCEP) by including a unique secret per request and e.g. APID, IMEI, or UDID during the SCEP process.
- Soliton Key Manager can generate, if required, both a public and a private key. It stores the private key on the device in a format that cannot be exported, while the public key is being forwarded to the NetAttest EPS where it is used for authentication purposes.



INTEGRATION WITH OTHER SOLITON PRODUCTS

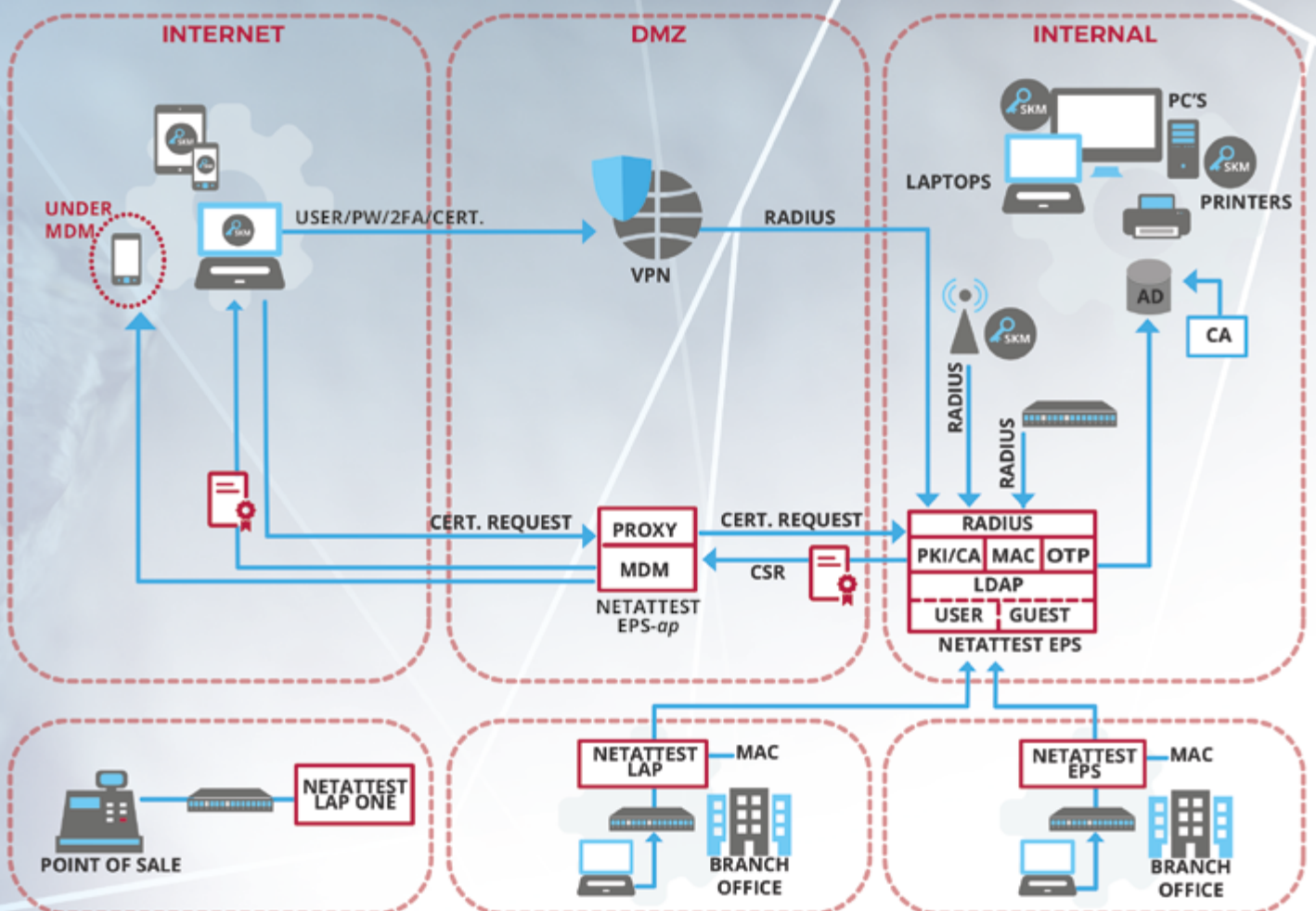
SecureBrowser

SecureBrowser is a remote access solution that establishes connections between a remote device and web servers inside a network. The SecureBrowser can use the digital certificates issued by the NetAttest EPS for strong authentication purposes. Users can now only access the organisation's web servers by using a username, password *and* a valid device certificate.

NetAttest LAP

Not all networks allow the use of IEEE 802.1X network control. Examples are branch offices without managed switches or network environments existing of non-IEEE 802.1X supplicants. Integration with the NetAttest LAP adds an additional layer of security to the network.

NETATTEST EPS INFRASTRUCTURE



SPECIFICATIONS NETATTEST EPS SERIES

SPECIFICATIONS

		EPS-SX15-A & EPS-SX15-V	EPS-ST05-A & EPS-ST05-V	EPS-DX04-A & EPS-DX04-V
	Max. number of user registration	200	200 / 500 / 2,000 / 5,000	100,000
	Max. number of RADIUS clients	20	500	1,000 / 2,2000
	Supporting authentication protocol	EAP-TLS, EAP-MD5, EAP-PEAP (MS-CHAPv2, GTC), EAP TTLS (PAP, CHAP, MS-CHAP, MS-CHAPv2, GTC), Cisco LEAP, EAP-FAST, PAP, CHAP, MS-CHAP, MS-CHAPv2		
	Redundancy	✗	✓	✓
RADIUS EXTENSION	One Time Password	✓	✓	✓
	MAC address authentication option	✓	✓	✓
	Group profile	✗	✓	✓
	Client certificate publish	✓	✓	✓
Certificate Authority (CA)	External server certificate publish	✗	✓	✓
	Max. number of certification	✗	400/1,000/4,000/10,000	200,000
	Extended CA function	✗	✓	✓
External database	Windows Domain	✓	✓	✓
	External LDAP database	✓	✓	✓
	RADIUS proxy	✗	✓	✓
Log management	RADIUS accounting	✓	✓	✓
	RADIUS detail accounting	✗	✗	✓
	Log maintenance	✗	✗	✓
	Other	SNMP (agent), NTP synchronisation, Syslog (TCP/UDP), Support UPS		

PHYSICAL APPLIANCE

	EPS-SX15-A	EPS-ST05-A	EPS-DX04-A
Form Factor	Desktop (option rack mount kit)	EIA19 inch (incl. rack mount kit)	
Dimensions (W x D x H)	165 x 43 x 106 mm	443 x 44 x 407 mm	438 x 44 x 292 mm
Network interface	10/100/1000BASE-T(X) Auto-MDI-X x 4 ports		
Weight	0.65 kg	7.8 kg	4.2 kg
Power supply	90 ~ 264VAC 47 ~ 63Hz (90 ~ 135Vac)		
Max. power consumption	22 VA	121 VA	28 VA
Calorific value	75BTU/h 18.9kcal 22W	412.8BTU/h 104.1kcal 121W	95.5BTU/h 24.1kcal 28W
Operating environment	Temperature 0 ~ 40°C Humidity 20 ~ 90% non-condensing		
Certifications	VCCI (Class B) FCC (Class B) CE, UL, RoHS PSE (power adapter)	VCCI (Class A) FCC (Class A) CE, UL, RoHS PSE (power cable)	

VIRTUAL APPLIANCE

	EPS - SX15 - V	EPS - ST05 - V	EPS-DX04-V
Supporting virtual platform	VMware ESXi 6.5 / 6.0 / 5.5		
VMware virtual machine version	10		
Virtual machine image	OVA		
Number of CPU	2	4	4
Memory size	2,048 MB		8,192 MB
HDD 1	2GB	5GB	96GB
Network adapter	4		
<ul style="list-style-type: none"> • Supports redundancy with virtual and physical appliance. • Support back-up/restore between virtual and physical appliance • No support for displacement by using virtual platform function such as Vmotion and VMwareFT (use the NetAttest EPS redundancy function) 			

OPTIONS

	MODEL	OPTION LICENSE	DESCRIPTION
OP1	EPS-ST05	User extended option (500)	<ul style="list-style-type: none"> ▪ Extend maximum number of user registration
OP2	EPS-ST05	Function extended option (2,000)	<ul style="list-style-type: none"> ▪ Extend maximum number of user registration ▪ Enable Windows Domain authentication ▪ Group Profile
OP3		Function extended option (5,000)	
OP4	EPS-SX15	Windows Domain option	<ul style="list-style-type: none"> ▪ Enable Windows Domain authentication
OP5	EPS-DX04	RADIUS Client extended option	<ul style="list-style-type: none"> ▪ Extend maximum number of RADIUS Client
OP6	EPS-DX04	MAC Address extended option	<ul style="list-style-type: none"> ▪ Enable MAC Address authentication with dedicated DB (maximum 200,000 addresses are registrable)
OP7	EPS-ST05		
OP8	EPS-SX15		
OP9	EPS-DX04	CA Extended option	<ul style="list-style-type: none"> ▪ Enable certificate distribution by Web enroll ▪ Enable certificate distribution by SCEP enroll ▪ Enable publishing Windows Smart Card logon certificate ▪ Execute certification profile
OP10	EPS-ST05	CA Extended option (200)	
OP11		CA Extended option (500) * User extended option (500) is required to be purchased together	
OP12		CA Extended option (2,000) * Function extended option (2,000) is required to be purchased together	
OP13		CA Extended option (5,000) * Function extended option (5,000) is required to be purchased together	
OP14	EPS-DX04 EPS-ST05 EPS-SX15	One-Time Password server option	<ul style="list-style-type: none"> ▪ Enable One-Time Password function

ABOUT SOLITON

Soliton Systems has a strong vision to innovate solutions to logically fulfil the needs of our customers without adding complexity. Soliton support companies with their security management challenges, including network security and remote access to the internal and cloud applications. Soliton's solutions protect the company's resources from unauthorized access and accidental data leakage.

Soliton®



EMEA office

Soliton Systems Europe N.V.

Barbara Strozilaan 364, 1083 HN Amsterdam, The Netherlands

+31 (0)20 896 5841 | emea@solitonsystems.com | www.solitonsystems.com