



Certificate Provisioning

Certificate Directory Server

- Secure certificate publishing
- Global certificate retrieval
- Provides global PKI Connectivity
- Supports Standard E-Mail Clients

Certificate searching & publishing

Global end-to-end encryption

Certificate searching...

For end-to-end encryption the recipient's public key is required by a client application like Outlook. The certBox provides your clients automatically with X.509 certificates and PGP keys on the internet. Ca. 170 certificate directories (repositories) are connected. Additionally, an easy to use HTML search GUI is provided.

... and publishing

The certBox Appliance may serve as a public external repository (certificate store) or as a secure ldap proxy to your internal directory. External partners can retrieve your user certificates automatically via LDAP or manually through an intuitive Web GUI with a responsive

design. Automatic certificate synchronization with Active Directory can be accomplished by the optional certSync Windows service. In order to fulfil data protection requirements, the access to your certificates is protected using advanced access control mechanisms.

Validating, uploading or ad-hoc certificates

External certificates may be validated centrally according to your trust policy before they are provided for usage. Partners may seamlessly upload their individual certificates. The certBox ICE service offers end-to-end encryption to external recipients who do not have a certificate by issuing ad-hoc certificates.

Easy to use

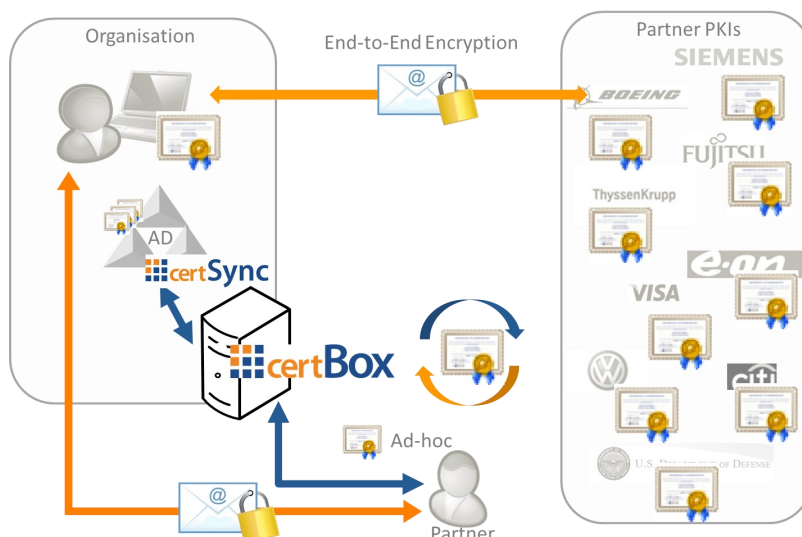
The certBox is a ready to use virtual appliance being installed in your DMZ. At your clients the certBox will be configured as an LDAP search directory. This can be done automatically via Group-Policies. Mobile clients on iOS and Android can be integrated seamlessly via the certMode service. Configuring the certBox is done comfortably via web browser.

Virtual appliance or SaaS?

The certBox is offered as a virtual appliance for VMware or Hyper-V. Clustering is possible for high availability. The certBox Cloud Service is a ready to use SaaS service.



Secardeo GmbH
Hohenadlstr. 4
D-85737 Ismaning
Tel. +49 89 18 93 58 90
Fax +49 89 18 93 58 99
info@secardeo.com
www.secardeo.com

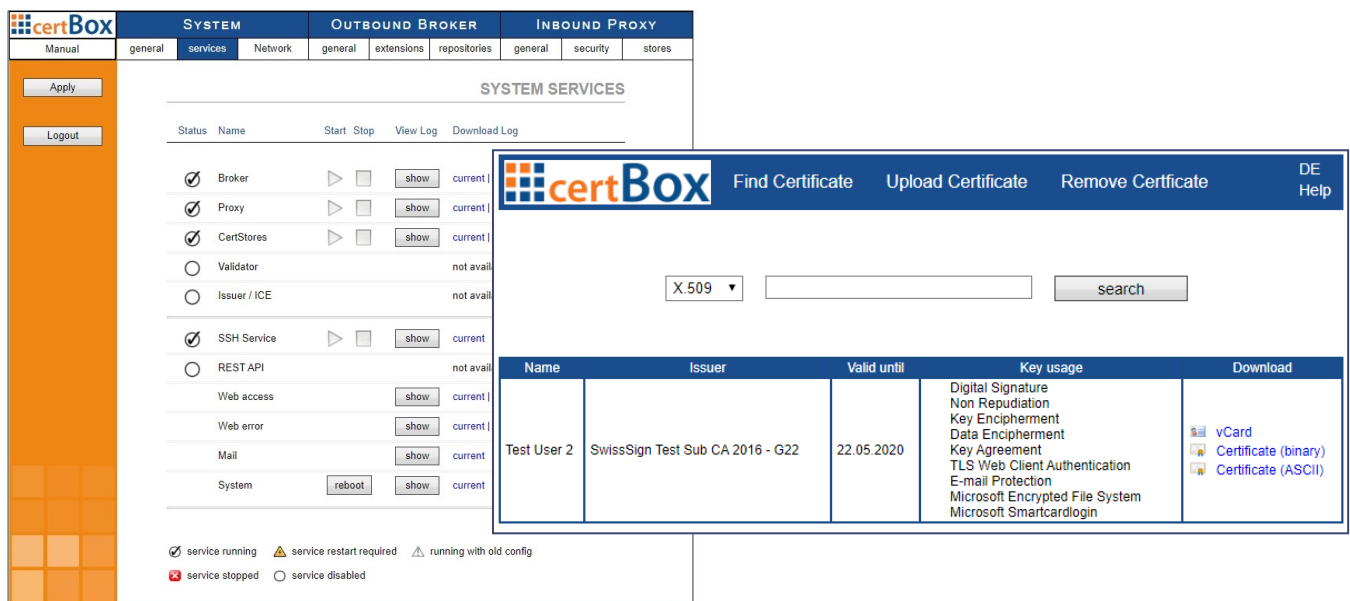


Secardeo certBox Standard Edition offers the following features:

- Publishing and searching for X.509 certificates and PGP keys via LDAP and HTTP
- Rule based localisation of the corresponding certificate repository
- Built-in certificate repository list (~170) and CA certificate trust list
- LDAP filter for popular e-mail clients; HTML search interface protected by CAPTCHA
- Public repository for your organization's certificates (certificate store)
- Comfortable options for import/export and certificate management
- LDAP proxy provides access control and patented DN encryption for search requests from outside
- Local caching of external certificates and business partner store
- High availability using certbox cluster
- Synchronisation with MS Active Directory (using optional Windows service certSync)

The certBox Enterprise Edition additionally provides the following functions:

- Policy based central certificate validation using CRLs and OCSP
- Ad-hoc certification of recipients without a certificate (Identity Certified Encryption - ICE)
- Decryption for recipients without S/MIME client via Web-Decrypter
- Partner certificate upload/removal form and support for organisational certificates
- Authentication for requests from and towards the external and internal network
- Statistics for in- and outbound searches and performance check
- HTTP CRL-Proxy
- REST API



The screenshot displays the certBox web interface. On the left, there's a sidebar with 'Manual', 'general', 'services', 'Network', 'general', 'extensions', 'repositories', 'general', 'security', and 'stores'. The main area is titled 'SYSTEM SERVICES' and lists various services with their status and actions. A search bar at the top right allows finding certificates by X.509 ID. Below the search bar, a table shows search results for 'Test User 2' issued by 'SwissSign Test Sub CA 2016 - G22' on '22.05.2020'. The table includes columns for Name, Issuer, Valid until, Key usage, and Download. The key usage list includes Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement, TLS Web Client Authentication, E-mail Protection, Microsoft Encrypted File System, and Microsoft Smartcardlogin. Download options include vCard, Certificate (binary), and Certificate (ASCII).

Name	Issuer	Valid until	Key usage	Download
Test User 2	SwissSign Test Sub CA 2016 - G22	22.05.2020	Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement TLS Web Client Authentication E-mail Protection Microsoft Encrypted File System Microsoft Smartcardlogin	vCard Certificate (binary) Certificate (ASCII)

Virtual Appliance:

VMware Virtual Hardware 8
Hyper-V Generation 1 (VHD)

Network: 1/2x Bridged
HDD: 1 x 40 GB

Software-as-a-Service:

Operated in German data center

Supported Standards:

- LDAPv3 RFCs 4510 - 4512
- X.509-Certificate and CRL Profile RFC 5280
- X.509 PKI LDAPv2 RFC 4523
- LDAP via TLS RFC 4513
- PKI Repository Locator Service RFC 4386

Further information on request.

Client-Applications:

- MS Outlook 2003-2019
- Mozilla Thunderbird
- Symantec Encryption Desktop

Further information on request.