SECARDEO

certPort

Machine Identity Certificates

Machine Certificate Enrollment

- Automated device & server certificates
- For strong authentication & VPN
- For TLS server, client & IoT certificates
- Enable Zero Trust Network Access
- Operate on-premises or in the Azure cloud
- Connect with ADCS, Cloud CA & others
- Supports classical & PQC algorithms



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

Autoenrollment for machine authentication

Integrated with AD/ADCS or Azure/Intune

Device certificates

For a secure network access strong authentication using client certificates according to IEEE 802.1x is best practice. These certificates can also be used for protected VPN connections.

Server certificates

Server certificates are required for authentication and establishment of a secure TLS channel with the client or even a VPN server.

IoT & OT certificates

Authentication of a huge number of IoT devices can only be handled efficiently using certificate based protocols like mTLS. This applies also to Operational Technology (OT) devices or Industry 4.0 environments.

Autoenrollment

All these types of machine certificates need to be enrolled automatically. certPort supports standard protocols for certificate autoenrollment in the Azure cloud or on-premises.

SCEP

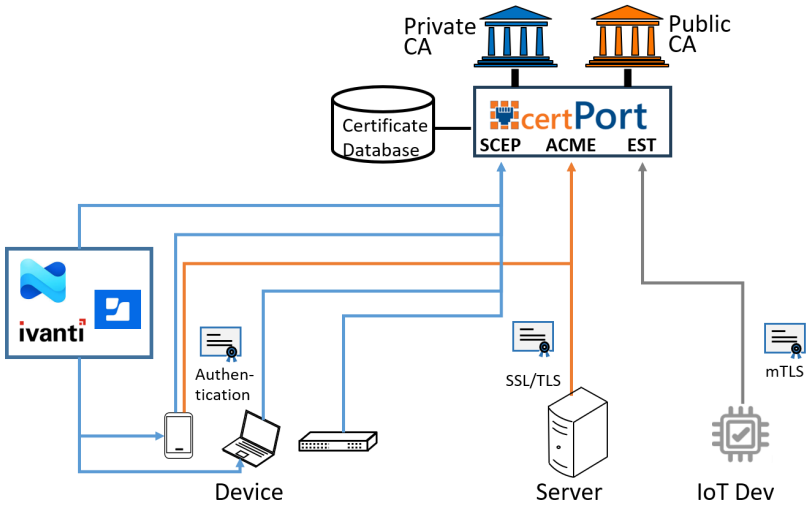
The Simple Certificate Enrollment Protocol is widely used for network devices, computers and mobile devices. Microsoft NDES is an outdated and inflexible example for SCEP enrollment.
certPort is a modern and secure alternative for NDES with ADCS and it can also be used in cloud scenarios with a strong MDM/Intune integration and SECARDEO certVault cloud CA

ACME

The Automatic Certificate Management Environment (ACME) protocol is used for the enrollment of TLS certificates from a CA to a server. It can also be used to autoenroll certificates to client computers and mobile devices.
certPort supports ACME with extended security mechanisms for internal or external servers from private CAs in the cloud like the SECARDEO certCAST cloud CA or on-premises with ADCS or from a series of public CAs and Let's Encrypt.

EST

Enrollment over Secure Transport is a modern, secure successor to SCEP. It serves to automatically assign and renew X.509 certificates to machines & IoT devices.
certPort supports EST with standard and extended features like server-side key-gen or CoAPS.

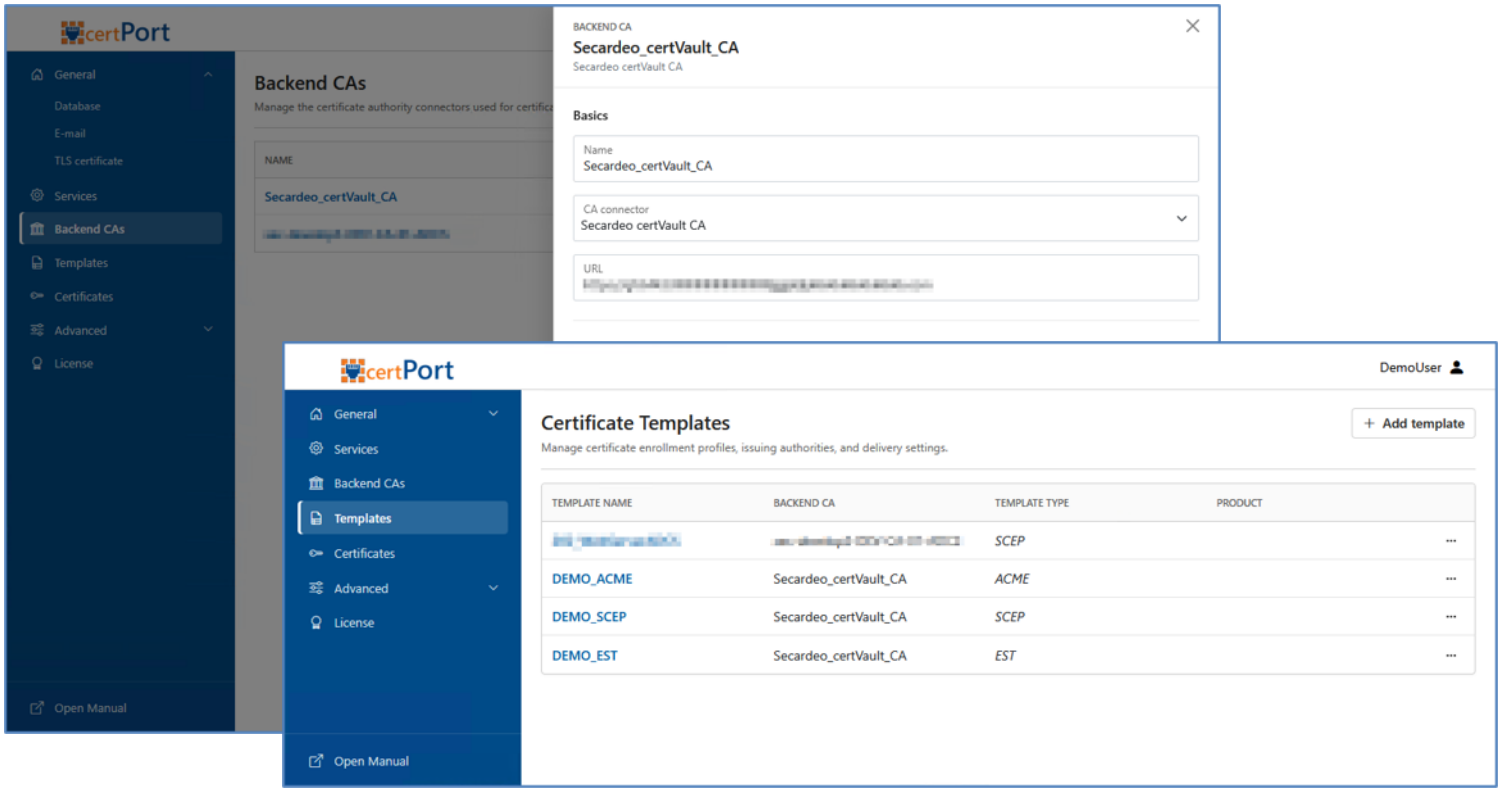


certPort is deployed as a Web App in Azure or on a Virtual Machine on-premises and

- Autoenrolls/-renews machine authentication certificates via SCEP, ACME or EST from your CA
- Automatically revokes Intune SCEP certificates or ACME certificates on request
- Validation of algorithm and key parameters, key usage and EKU based on certificate templates
- ACME support for HTTP, DNS, TLS-ALPN and Device Attestation challenges
- SCEP request validation with Intune, static or dynamic password (NDES mode) or existing certificate
- EST request validation with vendor certificate, basic authentication or existing certificate
- Advanced EST features for server-side key generation and enrollment over CoAPS
- Provides customizable e-mail notifications

certPort Enterprise Edition additionally provides

- Support of multiple public or private backend CAs
- Basic certificate management functions
- Enhanced ACME security features for ACME acceptance and External Account Binding
- Management of ACME accounts and EAB tokens
- Integration with Application Insights and immutable audit log in Azure
- Integration with Azure IoT Hub and Device Provisioning Service



Deployment options:

- Azure Web App via ARMv2 template, Azure Marketplace or Terraform
- Virtual Machine (Windows Server 2022/2025) as an IIS Web Application

Databases:

- Azure SQL
- Azure database for MySQL
- Self-hosted MSSQL
- Self-hosted MySQL
- 100 KB per certificate

Standards:

- RFC 5280 X.509-Certificates and CRLs
- RFC 8894 Simple Certificate Enrolment Protocol (SCEP)
- RFC 8295: Enrollment over Secure Transport (EST)
- RFC 8555 Automatic Certificate Management Environment (ACME)

Supported Clients:

- Android. iOS/iPadOS
- Windows, macOS, Linux
- Various ACME clients
- Various EST clients

Supported CA Backends:

- ACME CAs
- AWS ACM-PCA
- DigiCert CertCentral
- DogTag CA
- D-Trust
- EJBCA
- GlobalTrust SOAP
- GlobalSign Atlas
- OpenXPKI
- Secardeo certVault CA
- Sectigo Certificate Manager
- SwissSign CMC
- Windows CA HTTP
- TOPKI REST

For further CAs, please ask us.

SECARDEO