SECARDEO

certEntra

Entra ID User Certificates

Cloud User Certificate Enrollment

- Automated user certificates
- For S/MIME end-to.end security
- For certificate based user authentication
- Central key archive
- Connect with private or public CAs
-
- Use Azure Entra ID, Intune & Key Vault

Autoenrollment for S/MIME & CBA

Automated - Azure-integrated - convenient

S/MIME certificates

For seamless end-to-end encryption and e-mail signatures, S/MIME certificates from a public CA and private keys are required on each device of a user. Then Outlook, Apple mail or other e-mail clients can use it.

CBA

For certificate based user authentication (CBA) with a service appropriate certificates from a private or public CA are needed on user devices.

Azure users & devices

In the Microsoft Azure cloud users are managed in Entra ID and devices are managed in Intune. All certificates and private keys of an Entra ID user have to be deployed to all his devices in Intune. There the certificate can be used by standard apps like Outlook, Outlook mobile or native iOS mail.

Autoenrollment

For each user in an Entra ID enrollment group certEntra automatically generates key pair, requests a certificate from the CA and pushes the private key and certificate to the user's devices via Intune. Renewal is done automatically before the certificate expires. Certificates for shared mailboxes are supported. Certificates can automatically be published in Exchange Online GAL for internal encryption or in the Secardeo certBox for spontaneous encryption with external partners.

Secure key archival

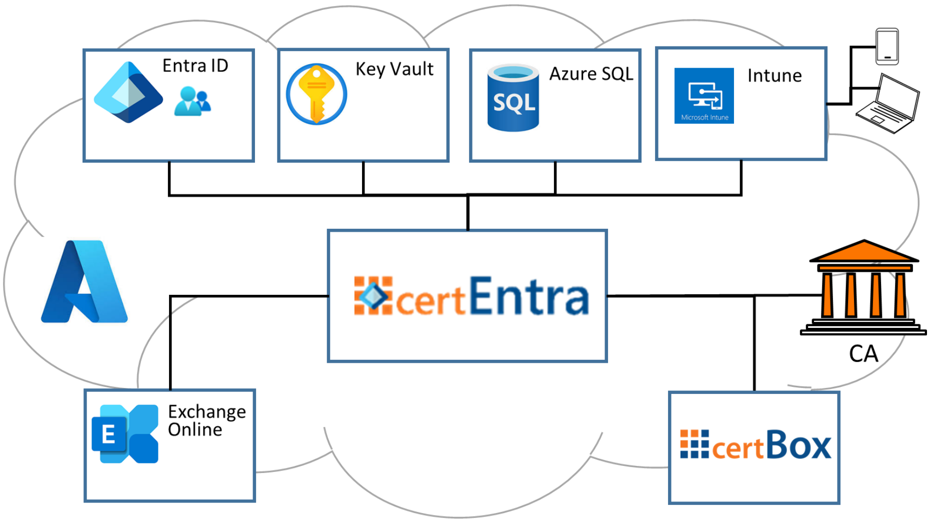
Certificates and optionally private keys are stored in a cloud database. Private keys are archived encrypted with a Key Recovery Agent certificate. They can be recovered by their owners via user self service or by a KRA. KRA keys can reside locally or in the customer's key vault.

Revocation

User certificates can be revoked manually by their owners or the certEntra administrator or they will automatically revoked, when the user leaves the organization or when attributes like name or e-amil address have changed.

Backend CAs

certEntra provides connectors for a series of popular public CAs and also for Microsoft ADCS.



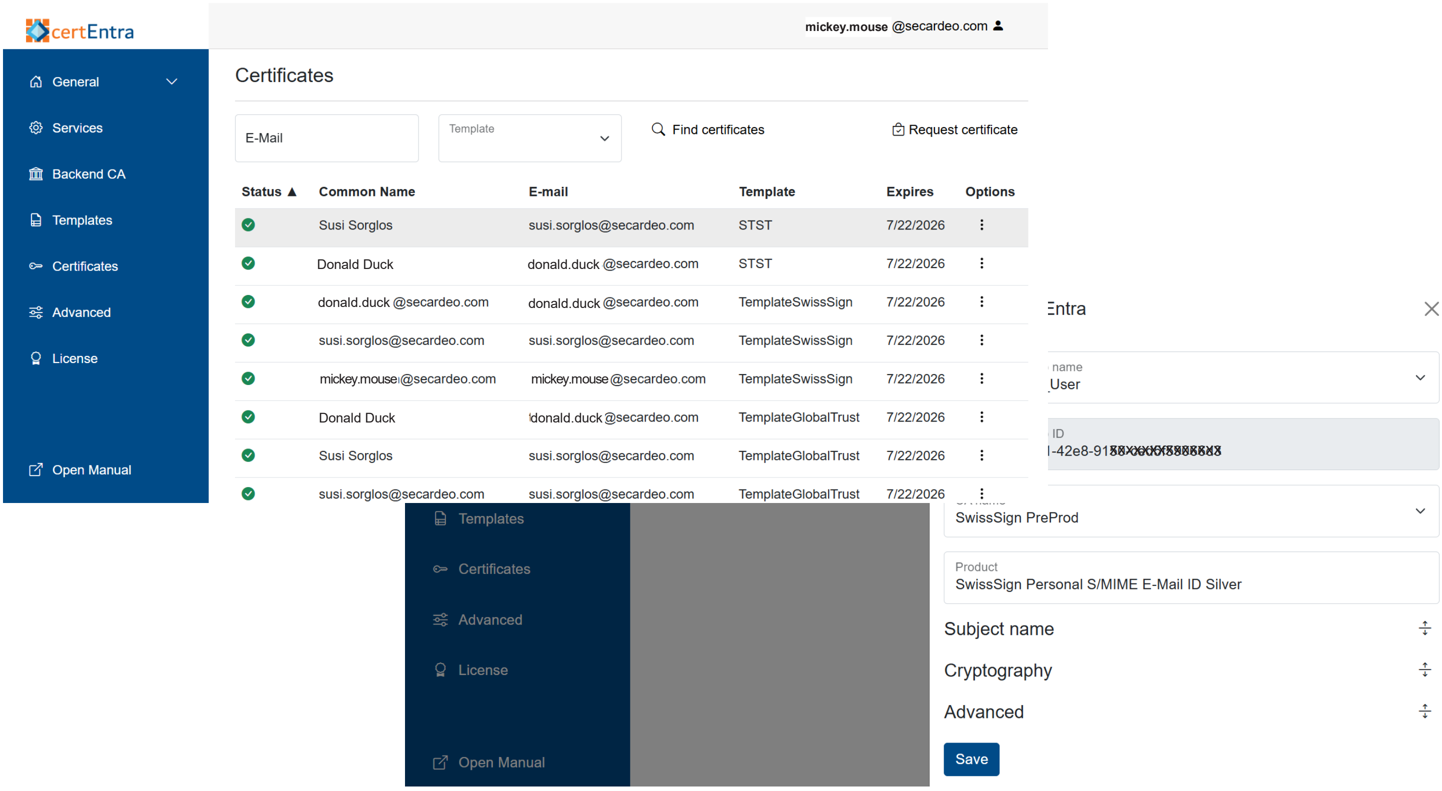
Secardeo GmbH
Hohenadlstr. 4
D-85737 Ismaning
Tel. +49 89 18 93 58 90
Fax +49 89 18 93 58 99
info@secardeo.com
www.secardeo.com

certEntra is deployed as a Windows Virtual machine in Azure or on-premises and

- Autoenrolls/-renews S/MIME or authentication certificates for Entra ID users from public or private Cas
- Archives private decryption keys encrypted with Key Recovery Agent (KRA) certificates
- Automatically revokes certificates of changed or removed users
- Publishes certificates for end-to-end encryption with partners to GAL and Secardeo certBox
- Provides Shared Mailbox certificates to authorized users
- Provides basic certificate management functions for administrators and KRAs
- Provides customizable e-mail notifications

certEntra Enterprise Edition additionally provides

- Support of multiple backend CAs
- KRA certificates in your Key Vault
- User self-services



Certificates

E-Mail | Template | Find certificates | Request certificate

Status ▲	Common Name	E-mail	Template	Expires	Options
✓	Susi Sorglos	susi.sorglos@secardeo.com	STST	7/22/2026	⋮
✓	Donald Duck	donald.duck @secardeo.com	STST	7/22/2026	⋮
✓	donald.duck @secardeo.com	donald.duck @secardeo.com	TemplateSwissSign	7/22/2026	⋮
✓	susi.sorglos@secardeo.com	susi.sorglos@secardeo.com	TemplateSwissSign	7/22/2026	⋮
✓	mickey.mouse @secardeo.com	mickey.mouse @secardeo.com	TemplateSwissSign	7/22/2026	⋮
✓	Donald Duck	donald.duck @secardeo.com	TemplateGlobalTrust	7/22/2026	⋮
✓	Susi Sorglos	susi.sorglos@secardeo.com	TemplateGlobalTrust	7/22/2026	⋮
✓	susi.sorglos@secardeo.com	susi.sorglos@secardeo.com	TemplateGlobalTrust	7/22/2026	⋮

Entra

name: User

ID: -42e8-91[redacted]

SwissSign PreProd

Product: SwissSign Personal S/MIME E-Mail ID Silver

Subject name

Cryptography

Advanced

Save

System Requirements:

- Windows Server 2022-2025
- Disk Space: 1 GB
- Minimum Memory 4GB
- Minimum Cores 2

Databases:

- Self-hosted MSSQL
- Self-hosted MySQL
- Managed Azure SQL
- Managed MySQL
- 100 KB per certificate

Standards:

- X.509-Certificates and CRLs RFC 5280
- PKCS#12: Personal Information Exchange, RFC 7292
- PKCS#7: Cryptographic Message Syntax (CMS),RFC 5652

Supported Clients:

- Android
- iOS/iPadOS 7 or newer
- macOS
- Windows 10/11

Supported CA Backends:

- DigiCert CertCentral
- GlobalTrust SOAP
- GlobalSign Atlas
- Sectigo Certificate Manager (SCM) REST
- SwissSign CMC
- Windows CA HTTP
-

For further CAs, please ask us.

SECARDEO