



Private key distribution

Push S/MIME certificates

- Managed & unmanaged devices
- Manual or automatic push
- Push by e-mail
- Push through MDM
- From Microsoft CA or
- Any CA via certEP



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

Recover keys and push to mobile devices

Automated, securely, standardized

Mobile e-mail encryption

A mobile PKI user needs to be able to encrypt, sign or decrypt his e-mails on his smartphone. For this, he needs the same keys installed on his desktop.

Key recovery and distribution

Standard PKIs like Microsoft ADCS or Secardeo TOPKI provide a central key archive. Private keys are stored here encrypted. Recovery is possible only for authorized instances. Microsoft ADCS makes use of Key Recovery Agents (KRA). With certPush, X.509 user certificates and PKI private keys can be simply recovered from such a central key archive and securely be distributed to all devices of a user in a protected PFX (.P12) container. The user certificates or SMIME certificates may stem from an internal Microsoft CA or a public CA using certEP. Key archival and recovery is done using standard Microsoft mechanisms based on Key Recovery Agents (KRA). The following key archives are supported:

- Microsoft ADCS
- Secardeo TOPKI
- PFX Folder

Distribution scenarios

certPush enables the recovery and the distribution of private keys to mobile devices in an enterprise running iOS or Android.

The following distribution scenarios are possible:

- Distribution via secure e-mail (certPush Mail)
- Distribution via Mobile Device Management (certPush MDM)
- Distribution by certLife user self-service via web browser (certPush KRS)

Push by e-mail

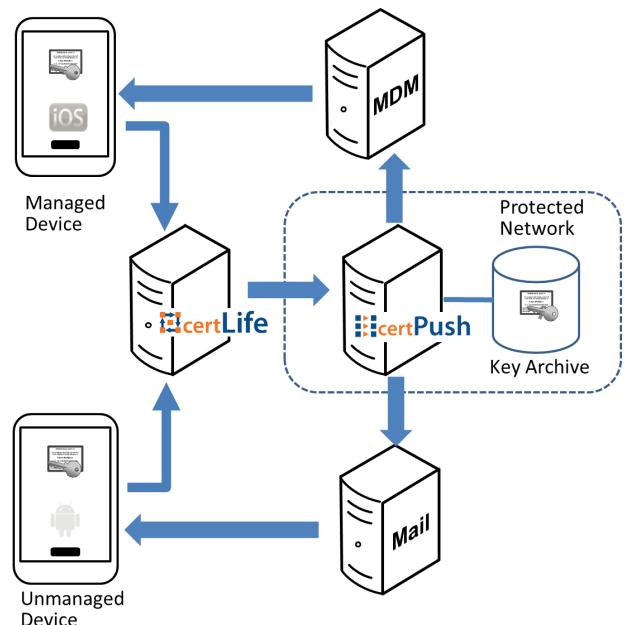
certPush mail distributes the private key in a PKCS#12 encrypted container as a .pfx attachment to the certificate owner. The password to decrypt and import the key on the device is transferred end-to-end encrypted. With this, many e-mail apps that support S/MIME can simply be provided with a certificate and private key.

Push by MDM

certPush MDM uploads a user's certificate and private key to his configured profile on Mobile Device Management (MDM) system. This is done over a secure channel via the MDM API. The PKCS#12 container and password can then be pushed to the mobile device in a mail or exchange profile.

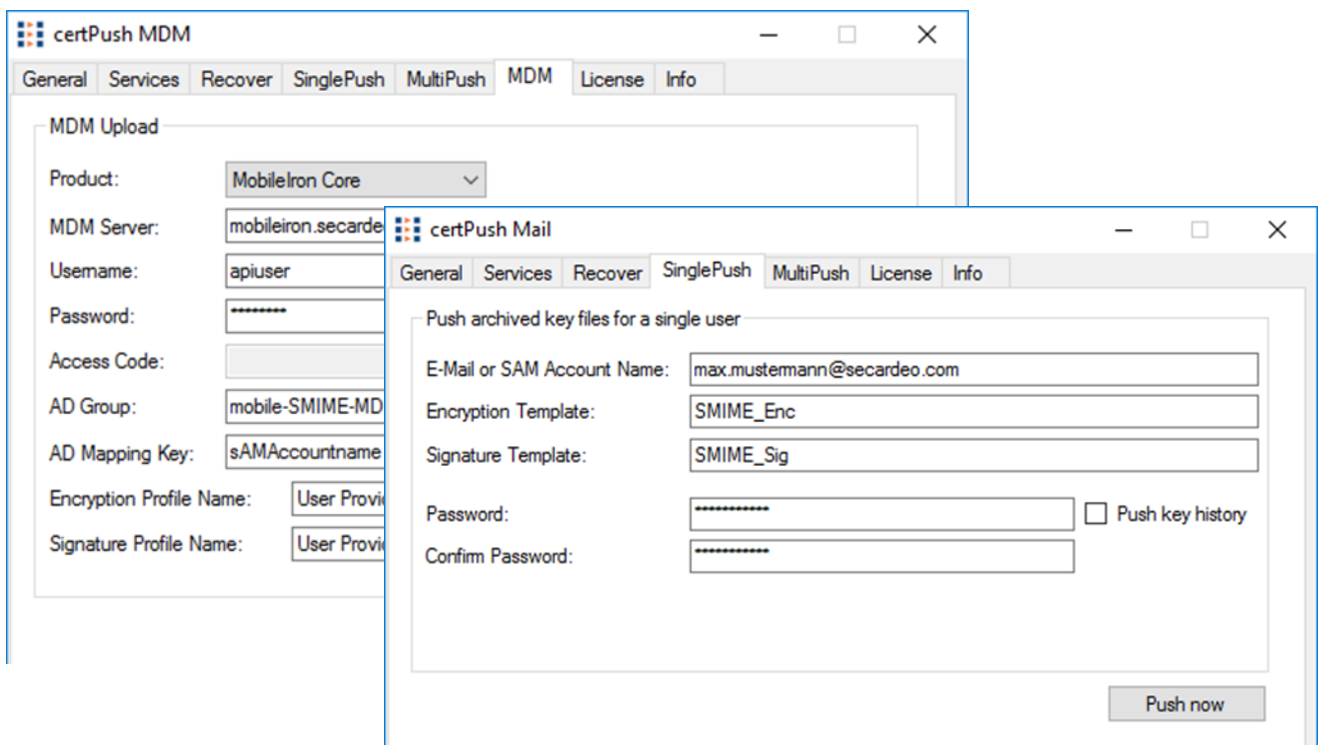
Key Recovery Service

The certPush Key Recovery Service (KRS) provides recovered private keys to authorized applications like certLife based on a strong authentication. By this, a user may import his certificates and keys to his device via a web based self-service.



Secardeo certPush is a key recovery and distribution service for private user keys from a central key archive. With this private user keys can be pushed to the mobile devices of a user. certPush offers the following features:

- Support of Microsoft CA (ADCS) and Secardeo TOPKI
- Reliable recovery process based on Key Recovery Agent certificates
- Recovery and distribution of single private keys
- Batch recovery and distribution of private keys for multiple users
- Recovery of current certificate and private key of a user or the whole key history
- Encrypted distribution to managed and unmanaged devices via e-mail push
- Secure distribution to managed devices by MDM upload
- Automatic key distribution based on an Active Directory group or a list of e-mail addresses
- Periodic background distribution (certPush service)



Operating System:

- Windows Server 2012 R2 - 2019
- Microsoft® .NET Framework 4.6 or higher

HD Requirements:

- Disk Space: 50 MB

Supported Databases:

- MySQL Server v5.7 or higher
- Microsoft SQL Server 2016 - 2017
- SQLite3

Supported Key Archives:

- Secardeo TOPKI
- Microsoft® ADCS
- PFX folder

Standards:

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

Supported MDM Systems:

- VMware AirWatch v8
- MobileIron Core v9-v10
- Microsoft Intune 2002 or higher

Supported Clients:

- Apple iOS 7 or higher (not with MDM Exchange profile)
- Google Android (Samsung Galaxy Sx with Exchange account)
- Microsoft® Windows® 10 (MS Outlook and many more)
- Apple Mac OS X (Apple Mail and more)
- Symantec TouchDown (for iOS and Android)
- Mozilla Thunderbird

For further clients, please ask.