SECARDEO

certMode Certificate Distribution

Automatic certificate distribution

- user certificates on iOS & Android
- managed & unmanaged devices
- transparent to the user
- support for native apps
- enable mobile end-to-end encryption

Secardeo GmbH
Hohenadlstr. 4
D-85737 Ismaning
Tel. 089 / 18 93 58 90
Fax 089 / 18 93 58 99
info@secardeo.com
www.secardeo.com

S/MIME certificates for mobile devices

Automated - Secure - MDM integration

Mobile certificates

Digital certificates can be used on mobile devices for authentication, encryption and digital signatures. Native mail apps on iOS and Android devices support S/MIME. Certificates and private keys are stored in the OS certstore/keychain.

Risks

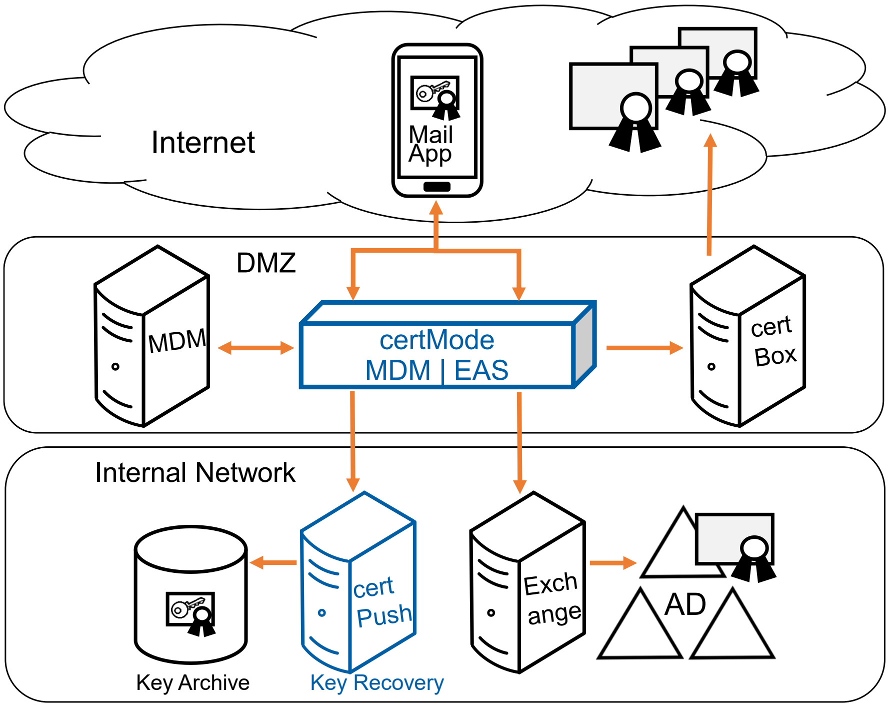
For using cryptographic functions, the user‘s certificates and private keys have to be installed. This can be done manually on unmanaged devices. However, most user‘s will not be able to do this. On managed devices, the certificates and keys can be provided by the MDM. Apple prevents from other ways to import usable keys into managed devices. Storing private keys and passwords of all mobile users in an MDM system that is connected to the internet and provides access on those keys for administrators poses inacceptable risks for an enterprise.

Secure distribution

certMode automatically distributes your user’s private keys and S/MIME certificates to their managed or, using certPush, unmanaged mobile devices in a secure manner. By this, it eliminates conceptual security deficiencies of existing MDM systems and also offers the automated key distribution without an MDM. Furthermore it can perform a global search and retrieval of partner certificates for native mail apps via LDAP services like the Secardeo certBox.

Integration

The certMode MDM proxy integrates with your standard MDM systems and iOS devices. It provides a secure connection to the Secardeo certPush key recovery service. The certMode EAS proxy integrates with your MS Exchange or any other ActiveSync server. It provides a connection to the Secardeo certBox or another LDAP server.



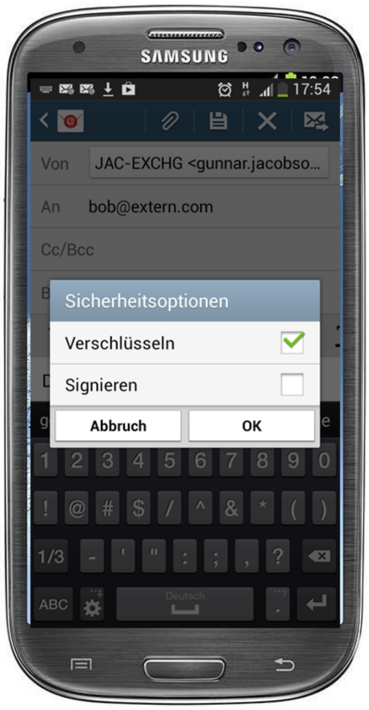
certMode provides an MDM proxy for distributing your user’s private keys and certificates and an Exchange ActiveSync proxy for retrieving external partner’s encryption certificates. This enables transparent end-to-end encryption on mobile devices. certMode is delivered as a virtual machine.

certMode MDM provides the following features:

- secure automated key recovery from a central key archive by certPush service
- supplies managed iOS devices securely with a user‘s private keys via MDM proxy
- supplies unmanaged iOS devices and Androids with a user‘s private keys by certPush
- securely adds PKCS#12 containers to iOS device profiles managed by MDM
- pushes encrypted PKCS#12 to unmanaged devices via e-mail
- recovers keys from certEP or Windows ADCS key archive

certMode EAS provides the following features:

- supplies native mail apps on iOS and Androids with recipient certificates from global directories
- transforms EAS certificate retrieval requests into LDAP search requests
- returns all encryption certificates found in AD and in Internet directories to the device



Von JAC-EXCHG <gunnar.jacobso...

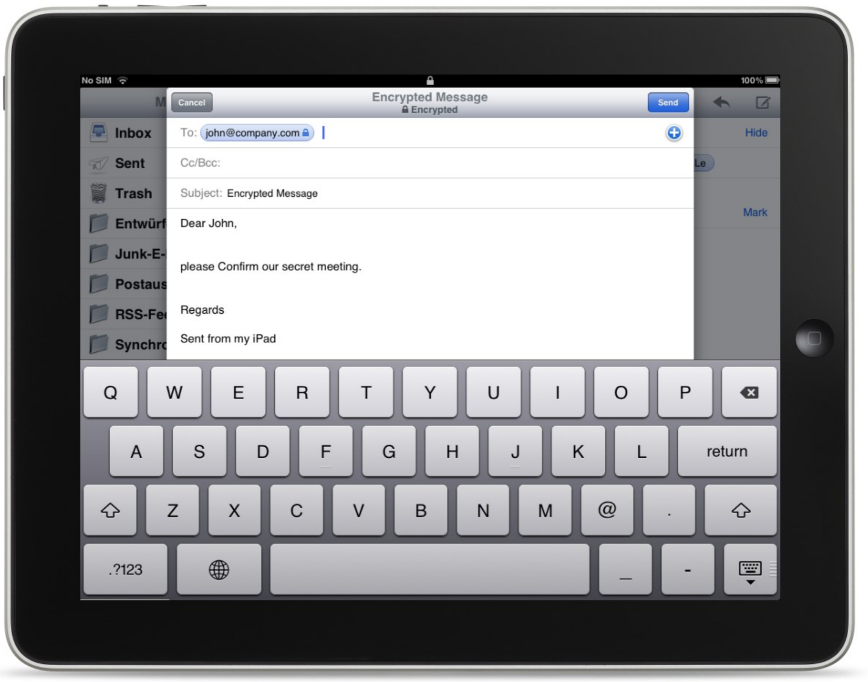
An bob@extern.com

Cc/Bcc

Sicherheitsoptionen

Verschlüsseln ☑

Signieren □



Encrypted Message
🔒 Encrypted

To: john@company.com 🔒

Cc/Bcc:

Subject: Encrypted Message

Dear John,

please Confirm our secret meeting.

Regards

Sent from my iPad

Virtual Appliance:

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

Network: 2x Bridged
HDD: 1 x 20 GB

Supported mobile OS:

- iOS 7 and newer
- Android 4.2 and newer

Supported Standards:

- Apple MDM protocol
- Exchange ActiveSync protocol
- LDAPv3 RFCs 4510 - 4512
- X.509-Certificate and CRL Profile RFC 5280

Key Archives & Formats:

- Secardeo certEP
- AD Certificate Services
- PKCS#12

Supported MDM systems:

- AirWatch
- Citrix XenMobile
- Microsoft Intune
- MobileIron
- SAP Afaria

Further on request.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)