

# Office 365 OME or S/MIME with an automated certificate management

A comparison of security, usability and management

Dr. Gunnar Jacobson



# Need for secure E-Mail

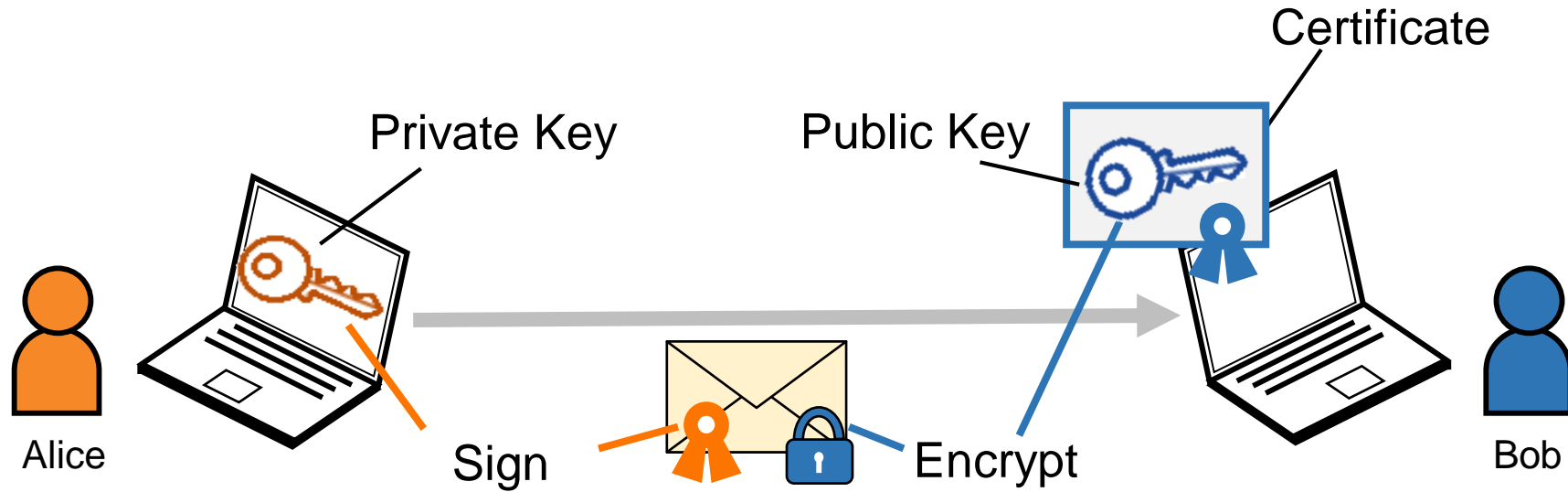
- CEO Fraud / Business E-Mail Compromise
    - Global damage: \$1.3 Bn. p.a.<sup>1</sup>
    - Example Pathé NL: \$21.5 Mio.<sup>2</sup>
- Solution: Digital Signature

- Economic Espionage
    - Damage in D: €43.4 Bn. over 2 years<sup>3</sup>
    - CLOUD Act obliges US companies to grant data access for US administrations. Even outside of the USA!
- Solution: E-Mail Encryption

1) FBI 2019  
2) Forbes 2018  
3) Bitkom 2018

# Secure E-Mail

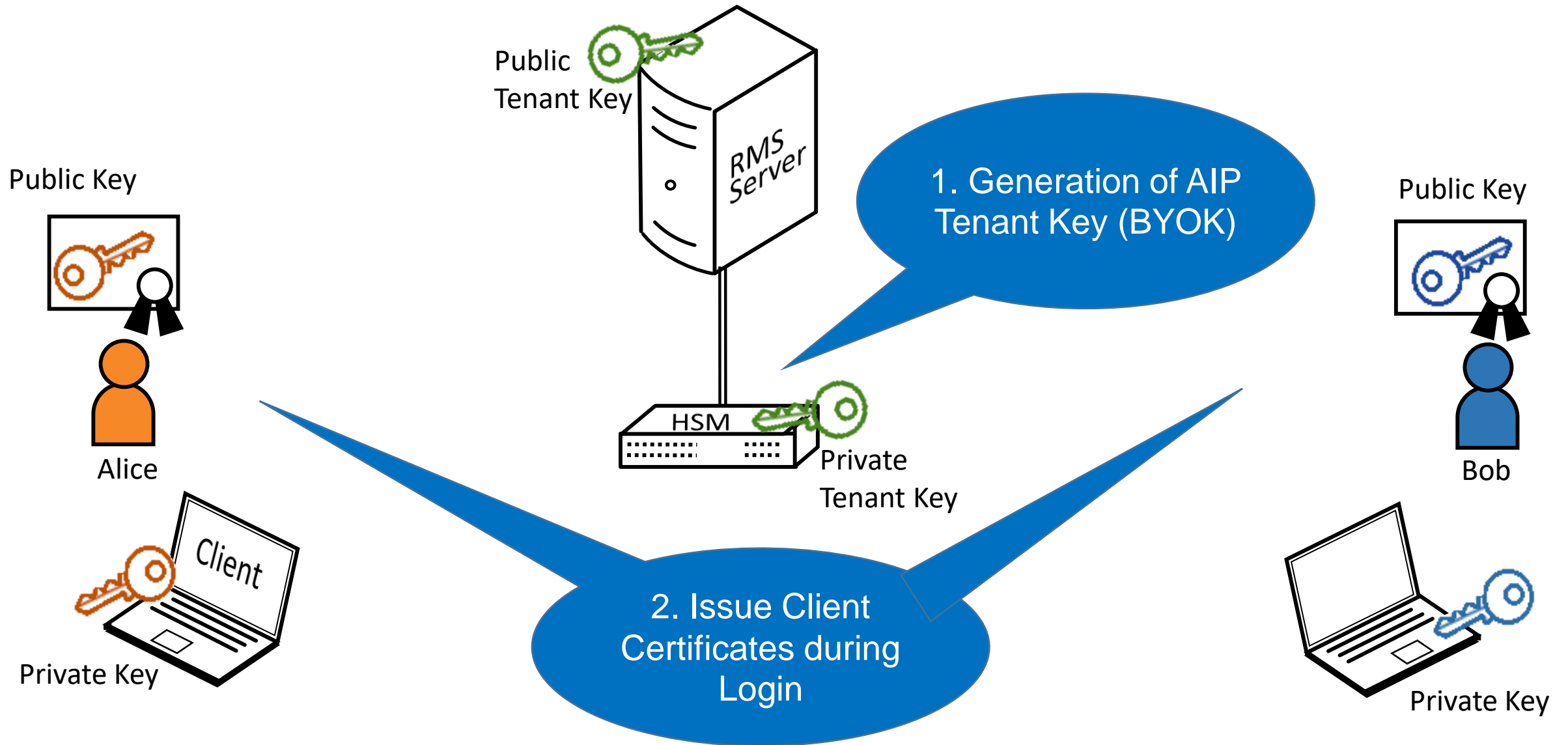
SECARDEO



- OME
  - Online service for e-mail encryption
  - Uses Rights Management Services (Azure RMS) as an encryption platform.
  - Part of Azure Information Protection (AIP)
- Rights management
  - Publishing License
  - AIP Labels

# OME Key Management

SECARDEO



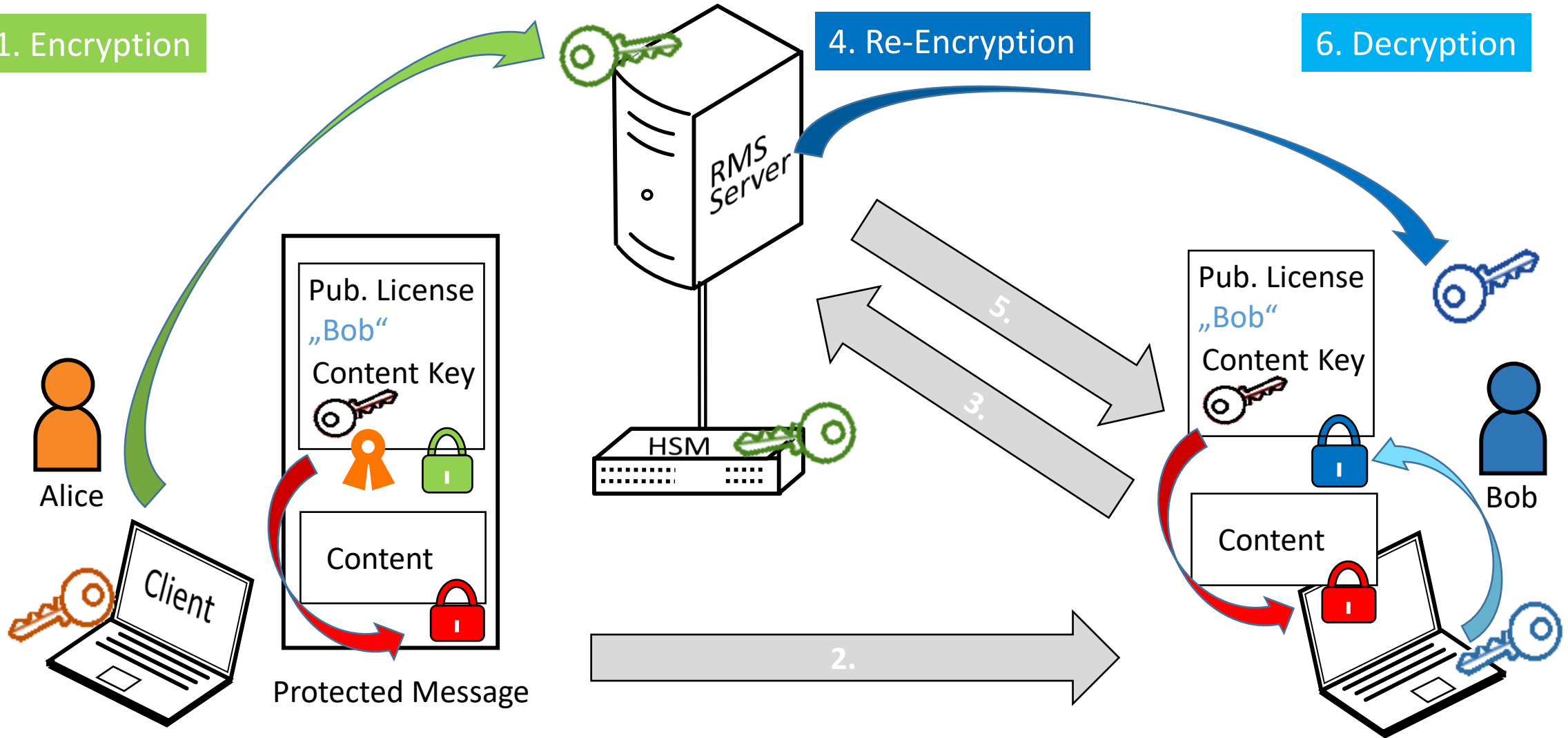
# OME/RMS Process

SECARDEO

1. Encryption

4. Re-Encryption

6. Decryption



- Advantages
  - Fully integrated with MS Azure
  - Encryption for external users via web portal
  - Comfortable for a user
  - Easy implementation & management
- Challenges
  - Proprietary solution, no standard
  - RMS & HSM is under control of Microsoft
  - No end-to-end security due to re-encryption
  - All content keys are temporarily available on RMS
  - The exchange of RMS protected messages between organisations is only possible with Federated Trust
  - Digital signature is not supported

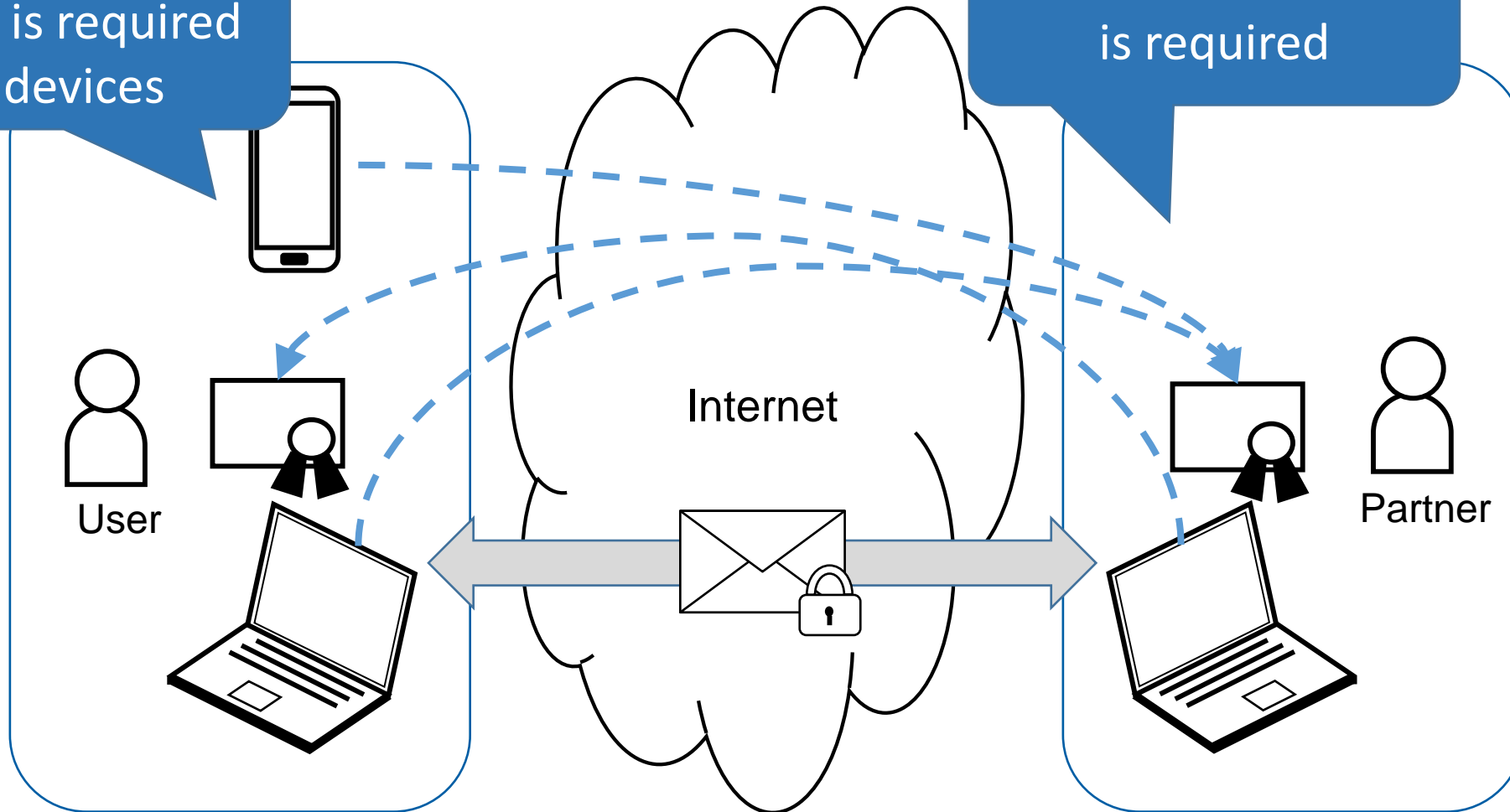
- Secure / Multipurpose Internet Mail Extensions
- S/MIME v3 (1999)
  - Current v3.2: RFC 5751, 2010
- Standard for the encryption and signature of MIME-encapsulated e-mail
- Makes use of digital certificates (X.509)
- High distribution, good interoperability
  - MS Outlook, Notes, Thunderbird, ...
  - Apple iOS, Android (Samsung,...)
- Is also supported by Office 365 (OWA)!



# Verteilung von Zertifikaten

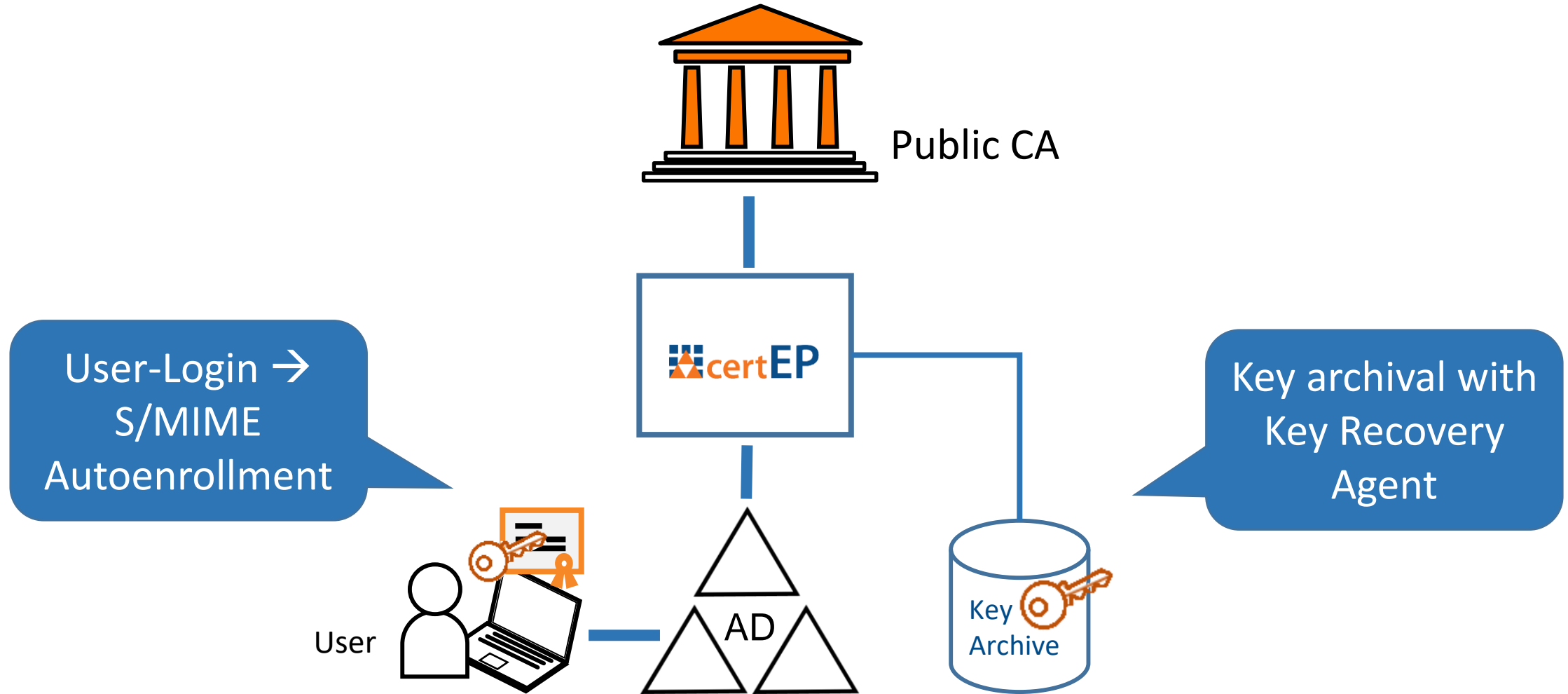
Own certificate from a public CA is required on all devices

Partner's certificate is required

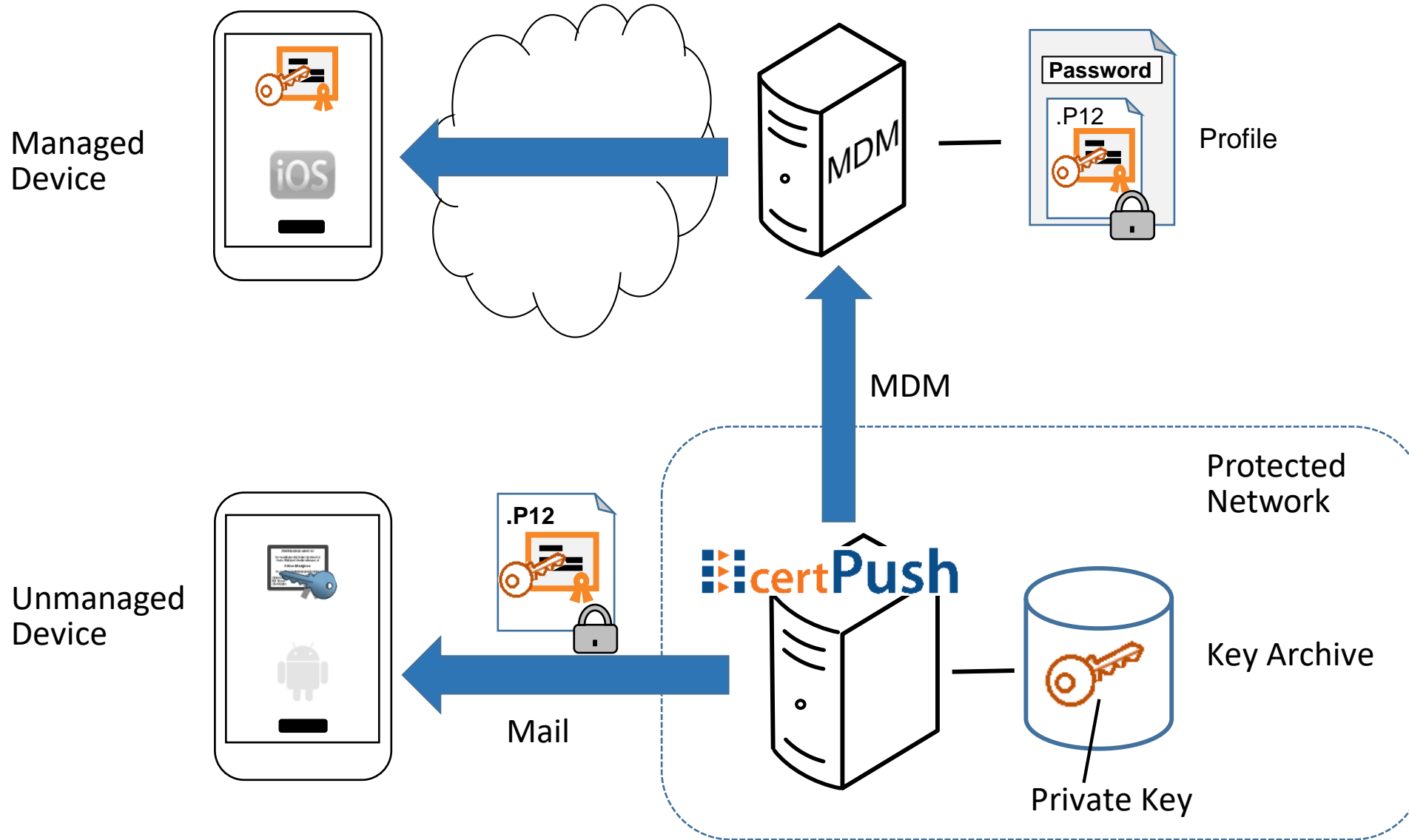


# Windows S/MIME Enrollment

SECARDEO

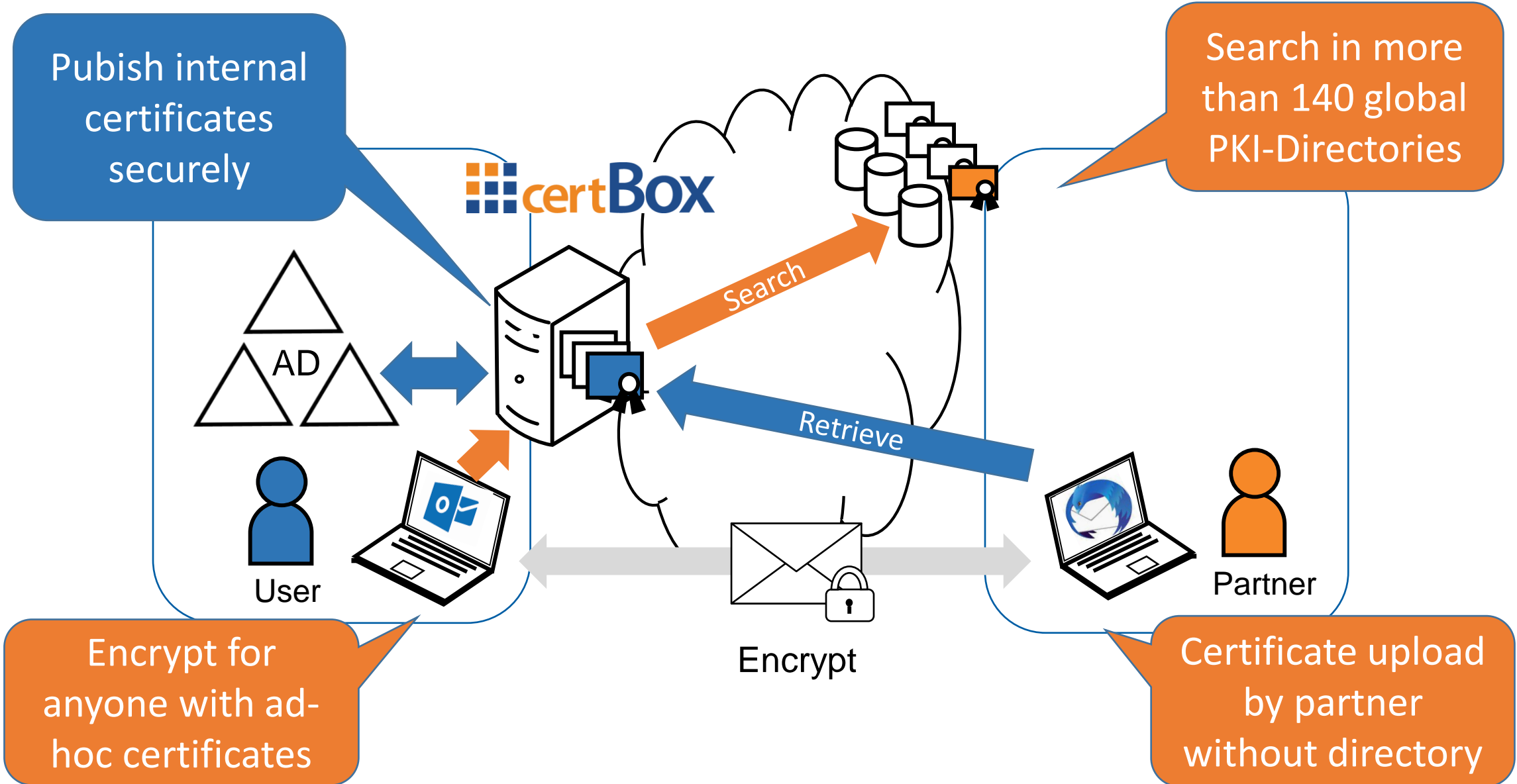


# Mobile S/MIME Enrollment



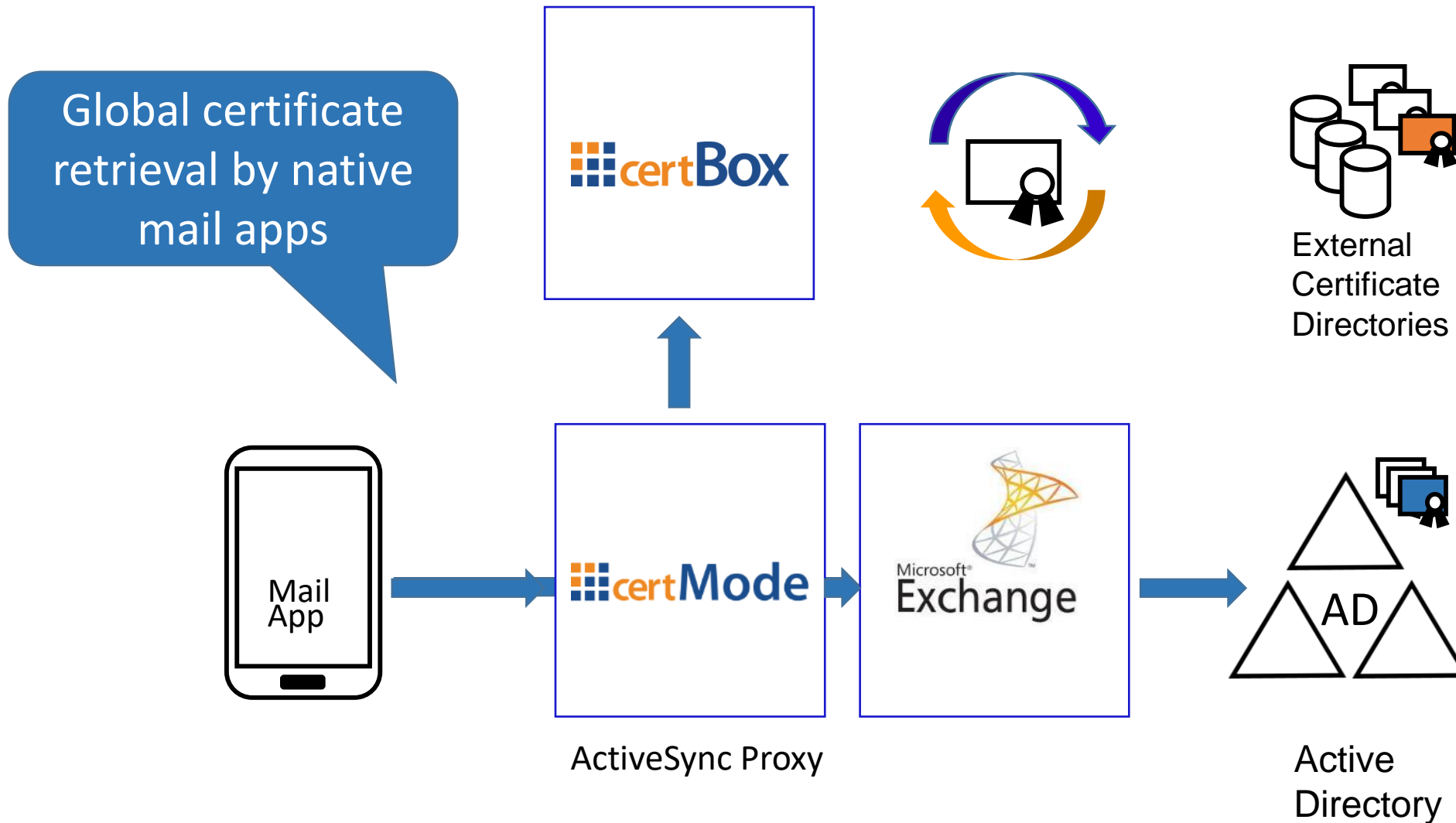
# Global Certificate Retrieval

SECARDEO



# Mobile End-to-End Encryption

SECARDEO



# Certificate Management

 Administratorzertifikate ▾ Benutzerzertifikate **Suchen** Bestätigen PKI-DEMO\Administrator ▾



| Status | Common Name                 | SAN                                    | Template | Expires    | 10 ▾ | Einträge |
|--------|-----------------------------|--|----------|------------|------|----------|
| ✓      | Administrator               | U: administrator@pki-demo.secardeo.com | KRA3     | 12.05.2021 |      |          |
| ✓      | Administrator               | E: administrator@pki-demo.secardeo.com | SMIME    | 13.05.2020 |      |          |
| ✓      | srv.pki-demo.secardeo.com   | D: srv.pki-demo.secardeo.com           | SSL      | 17.05.2020 |      |          |
| ✓      | srv3.pki-demo.secardeo.com  | D: srv3.pki-demo.secardeo.com          | SSL      | 17.05.2020 |      |          |
| ✓      | srv3.pki-demo.secardeo.com  | D: srv3.pki-demo.secardeo.com          | SSL      | 17.05.2020 |      |          |
| ✓      | Administrator               | E: administrator@pki-demo.secardeo.com | SMIME    | 17.05.2020 |      |          |
| ✓      | srv4.pki-demo.secardeo.com  | D: srv4.pki-demo.secardeo.com          | SSL      | 20.05.2020 |      |          |
| ✓      | srv5.pki-demo.secardeo.com  | D: srv5.pki-demo.secardeo.com          | SSL      | 20.05.2020 |      |          |
| ✓      | srv11.pki-demo.secardeo.com | D: srv11.pki-demo.secardeo.com         | SSL      | 08.07.2021 |      |          |
| ✓      | srv13.pki-demo.secardeo.com | D: srv13.pki-demo.secardeo.com         | SSL      | 08.07.2021 |      |          |

- Revoke
- Key Recovery Service:
  - Recover P12
  - Recover JKS
  - Push Key
- Herunterladen:
  - Zertifikat (PEM)
  - Zertifikat (DER)
  - Zertifikatskette (PEM)
  - Zertifikatskette (DER)



- S/MIME is standardised and widely distributed
- Supports encryption & signature
- User comfort and easy management by
  - Automated certificate enrollment & retrieval
  - Central certificate lifecycle management
- Global end-to-end encryption from any device to any partner
- SECARDEO TOPKI
  - PKI automation for arbitrary certificates
  - S/MIME, SSL/TLS, VPN, Computer/Device, ...



Thank you for your attention!

Visit us:  
Hall 9 / 9-645

