

Office 365 OME oder S/MIME mit automatisierter Zertifikatsverwaltung

Vergleich von Security, Usability und Management

Dr. Gunnar Jacobson



- CEO Fraud / Business E-Mail Compromise
 - Globaler Schaden: \$1.3 Mrd. p.a.¹
 - Beispiel Pathé NL: \$21.5 Mio.²

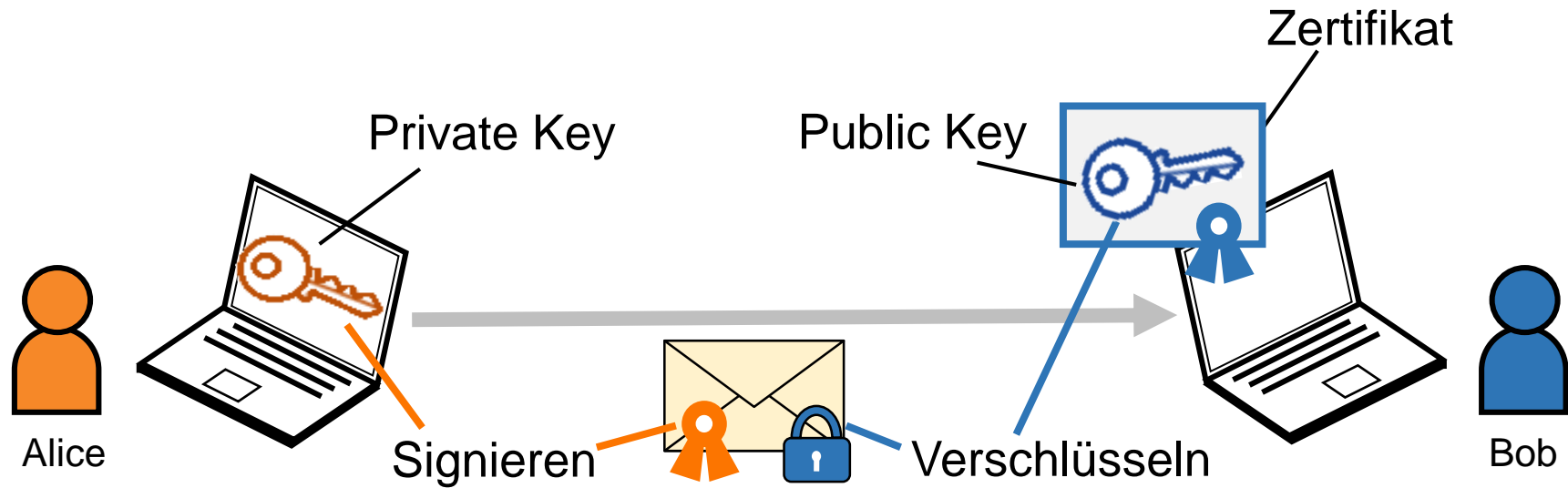
→ Lösung: Digitale Signatur

- Wirtschaftsspionage
 - Schaden in D: €43.4 Mrd. über 2 Jahre³
 - CLOUD Act verpflichtet US-Firmen, den US-Behörden Zugriff auf Daten zu gewährleisten. Auch außerhalb der USA!

→ Lösung: E-Mail Verschlüsselung

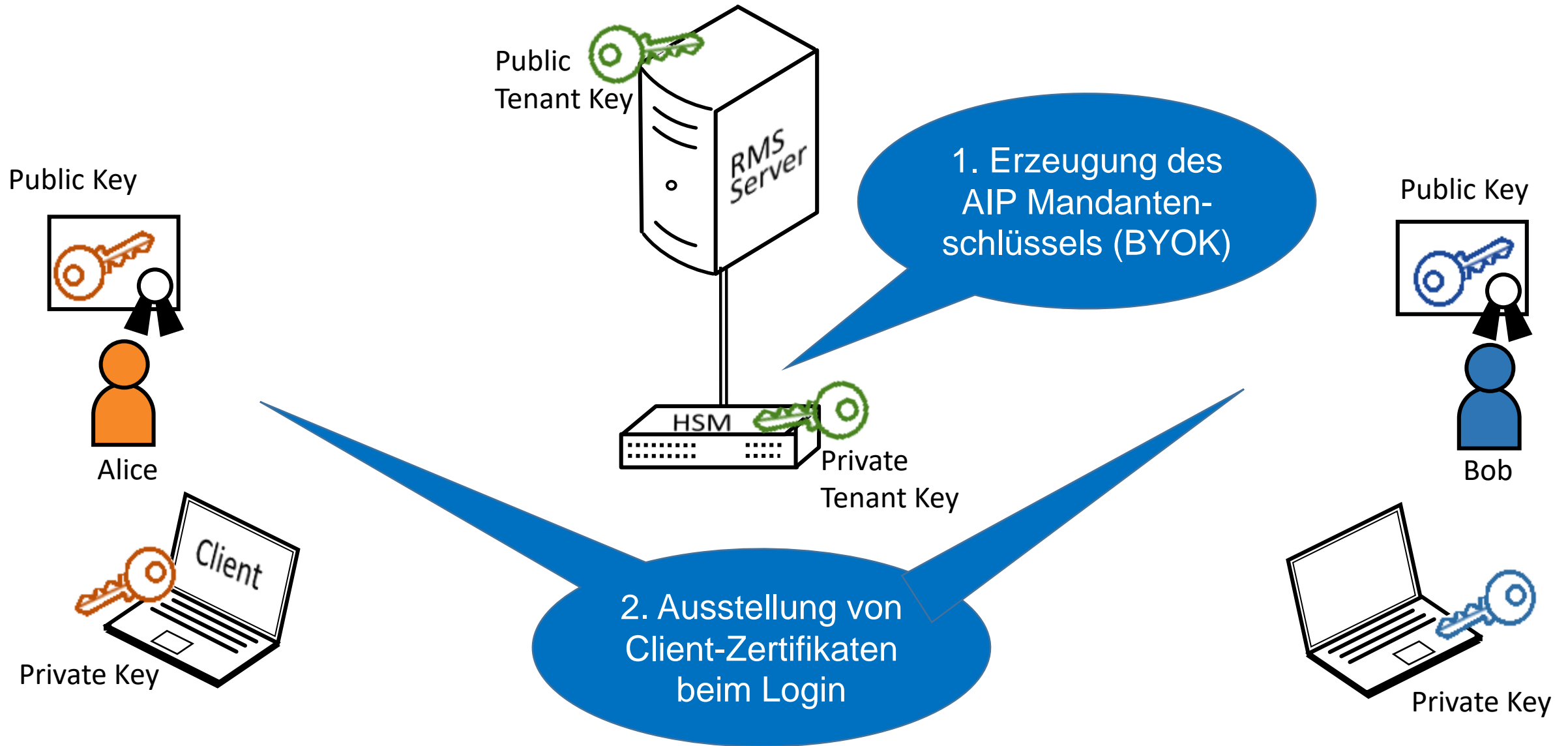
- 1) FBI 2019
- 2) Forbes 2018
- 3) Bitkom 2018

Sichere E-Mail



- OME
 - Online Service zur E-Mailverschlüsselung
 - Nutzt Rights Management Services (Azure RMS) als Verschlüsselungsplattform.
 - Teil von Azure Information Protection (AIP)
- Rechteverwaltung
 - Publishing License
 - AIP Labels

OME Key Management



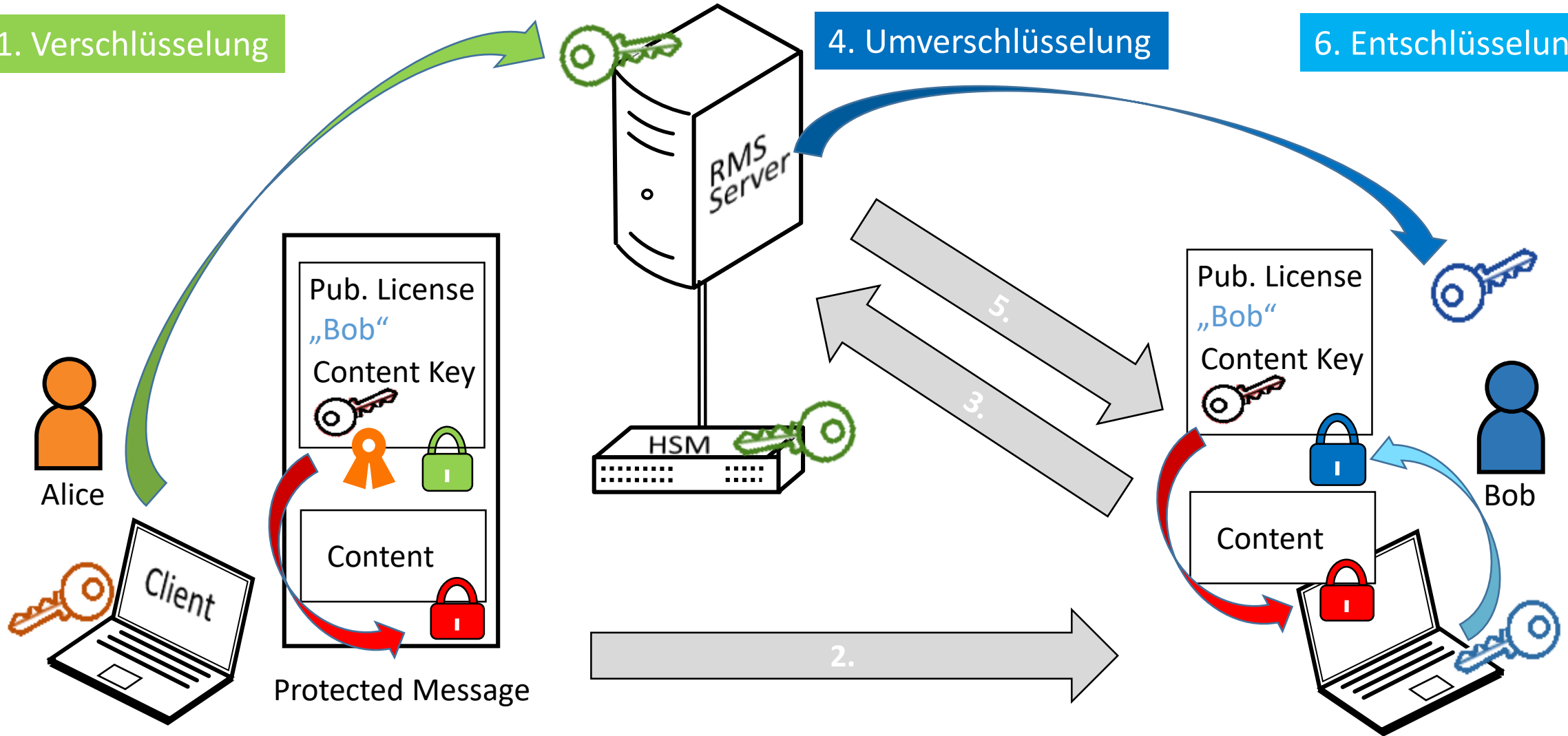
OME/RMS Ablauf

SECARDEO

1. Verschlüsselung

4. Umverschlüsselung

6. Entschlüsselung



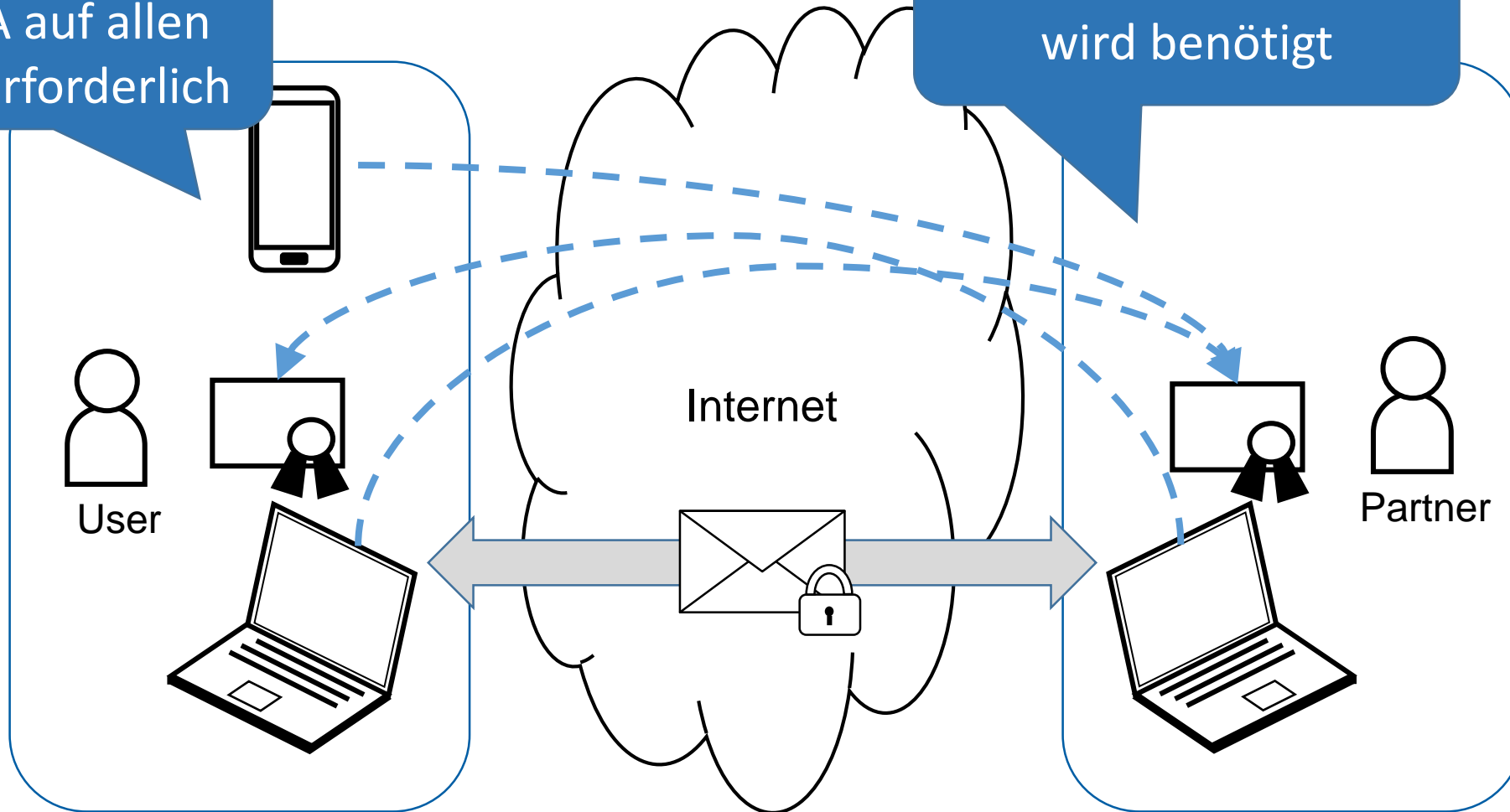
- Vorteile
 - Voll integriert in MS Azure
 - Verschlüsselung mit Externen über Web-Portal
 - Bequem für den Anwender
 - Einfache Realisierung & Verwaltung
- Herausforderungen
 - Proprietäre Lösung, kein Standard
 - RMS & HSM ist unter Kontrolle von Microsoft
 - Keine Ende-zu-Ende Sicherheit da Umverschlüsselung
 - Alle Content Keys sind temporär am RMS verfügbar
 - Der Austausch RMS geschützter Nachrichten zwischen Organisationen ist nur durch Federated Trust möglich
 - Digitale Signatur wird nicht unterstützt

- Secure / Multipurpose Internet Mail Extensions
- S/MIME v3 (1999)
 - Aktuell v3.2: RFC 5751, 2010
- Standard für die Verschlüsselung und Signatur von MIME-gekapselter E-Mail
- Nutzt digitale Zertifikate nach X.509
- Hohe Verbreitung, gute Interoperabilität
 - MS Outlook, Notes, Thunderbird, ...
 - Apple iOS, Android (Samsung,...)
- Wird auch durch Office 365 (OWA) unterstützt!

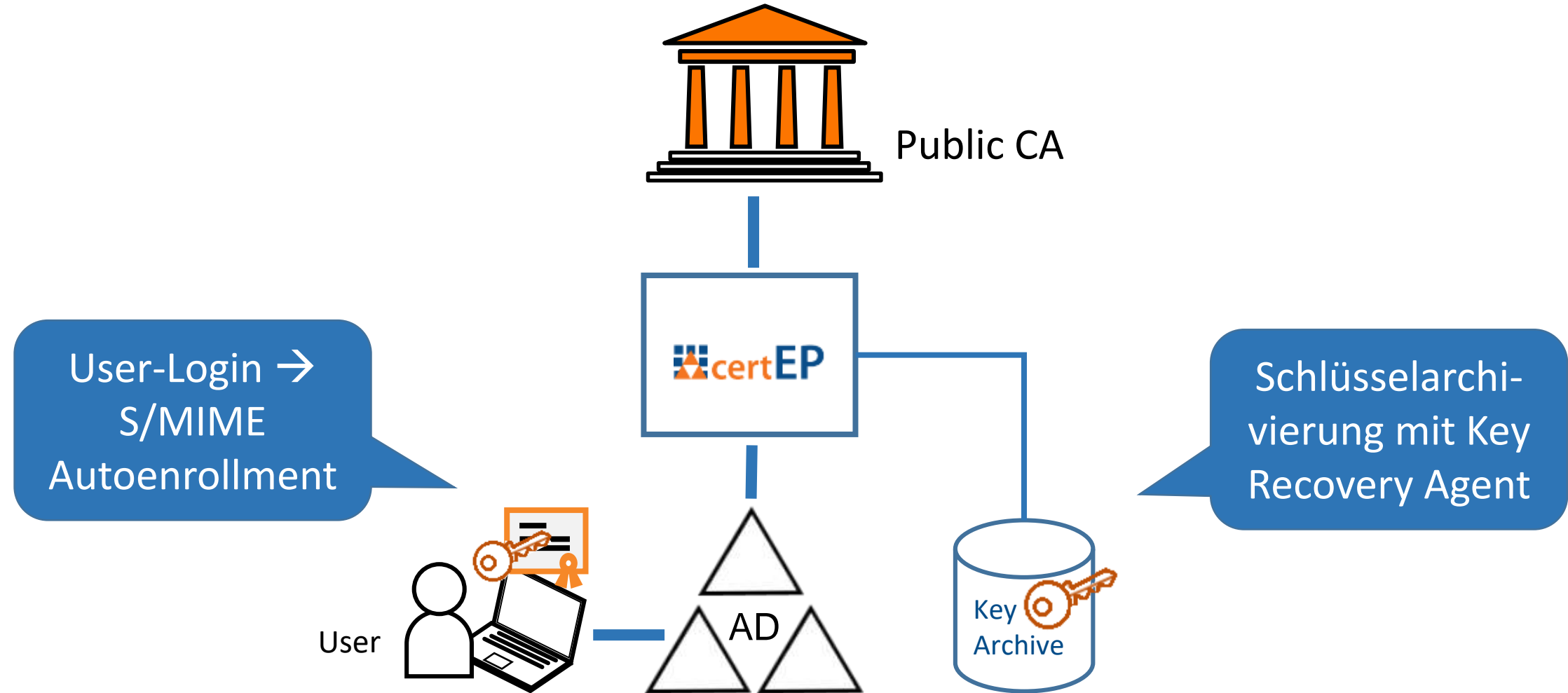
Verteilung von Zertifikaten

Eigenes Zertifikat von Public CA auf allen Geräten erforderlich

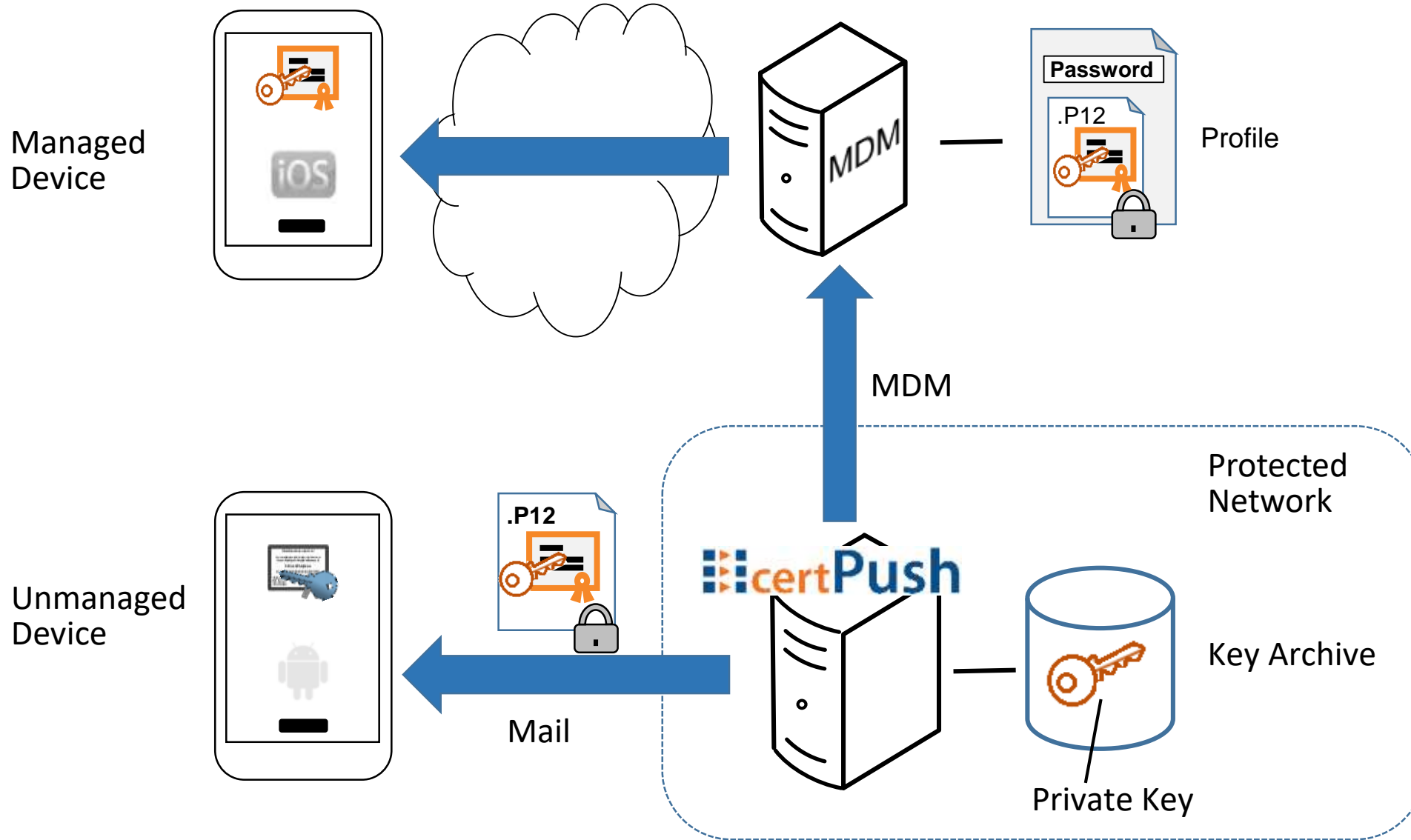
Zertifikat des Partners wird benötigt



Windows S/MIME Enrollment

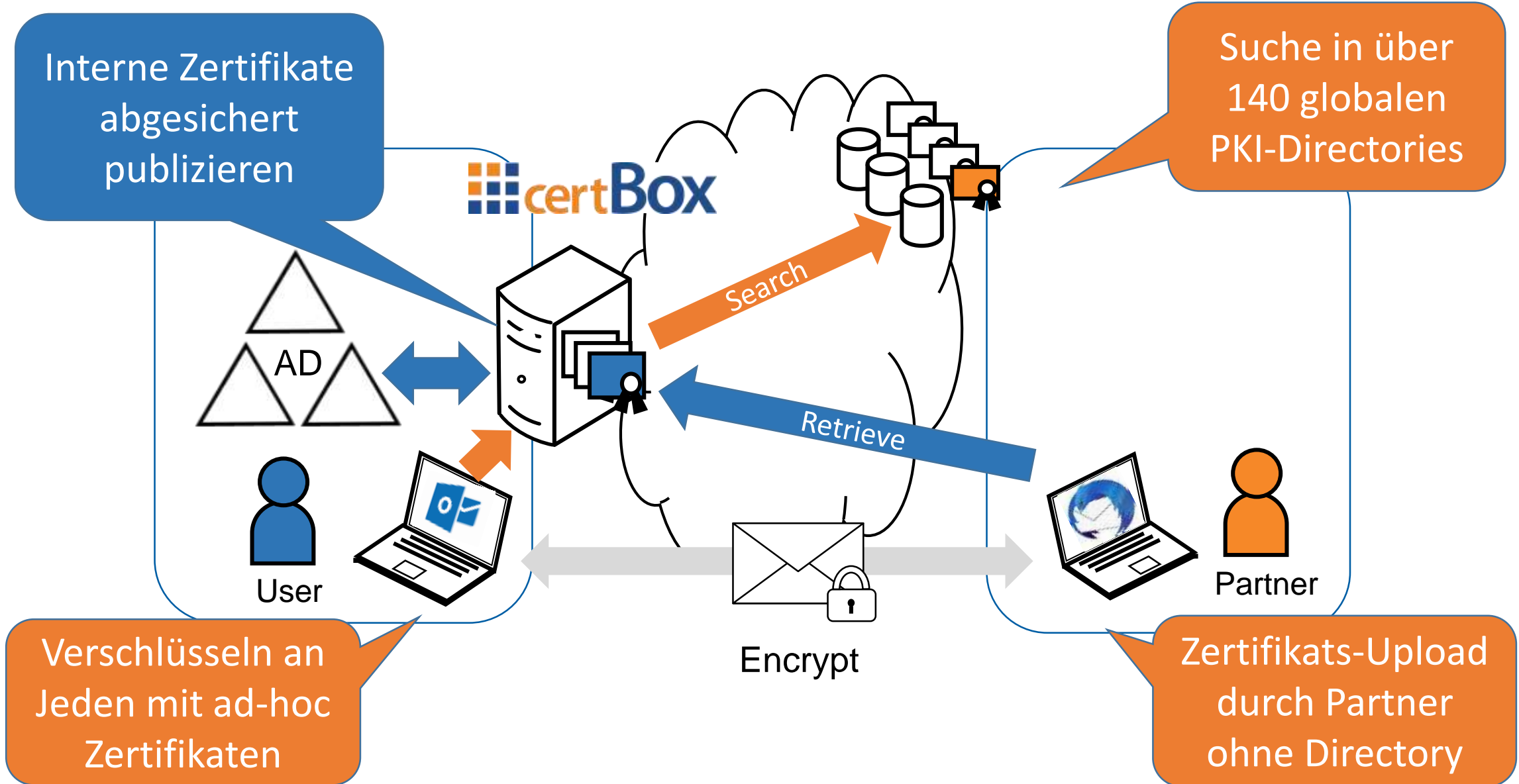


Mobiles S/MIME Enrollment

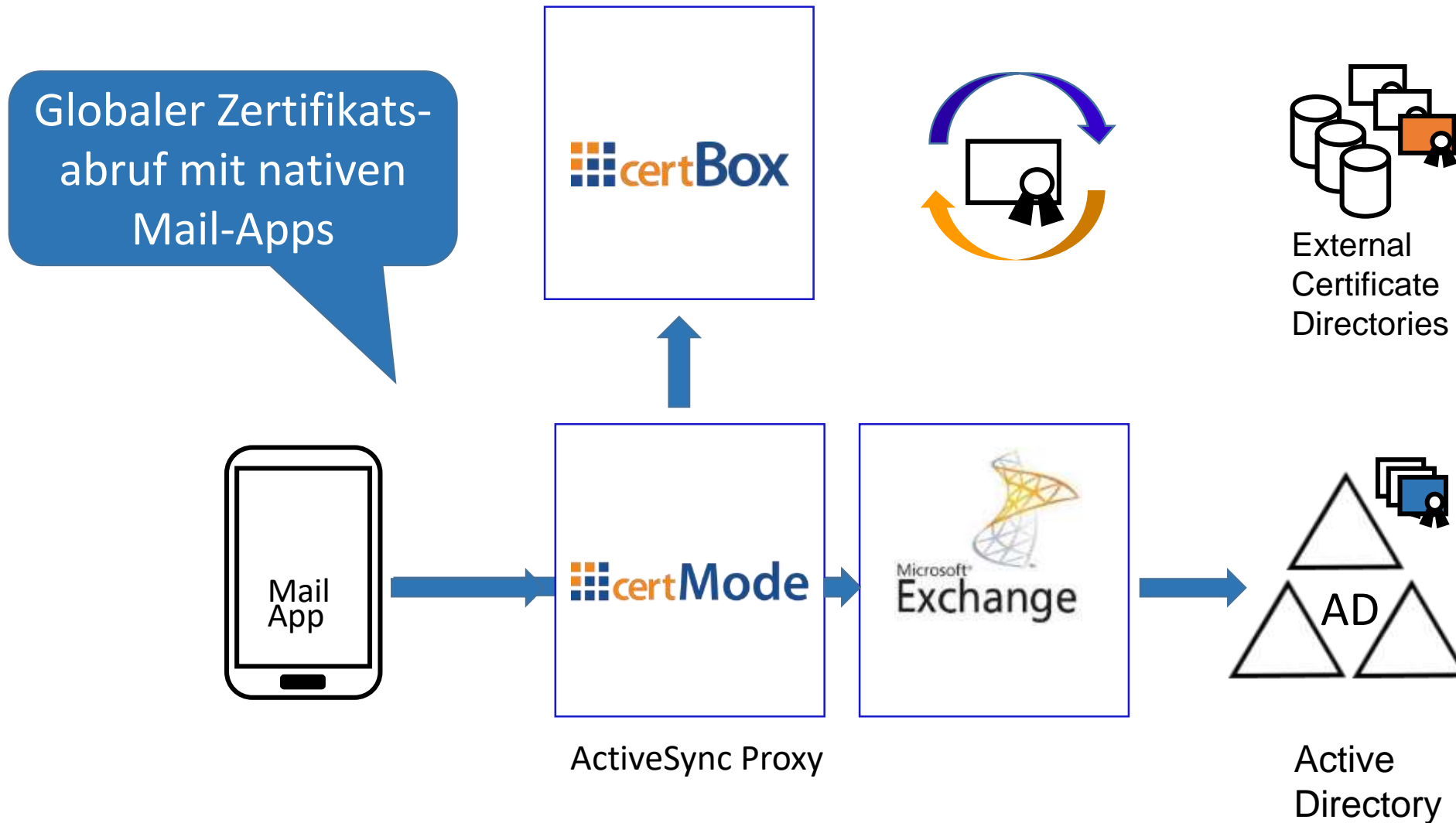


Globaler Zertifikatsabruf

SECARDEO









Mobile E2E Verschlüsselung



Zertifikatsverwaltung

 Administratorzertifikate ▾ Benutzerzertifikate **Suchen** Bestätigen PKI-DEMOAdministrator ▾

Suchen... ▼ 🔍

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	17.05.2021		
✓	srv3.pki-demo.secardeo.com	D: srv3.pki-demo.secardeo.com	SSL	17.05.2021		
✓	srv3.pki-demo.secardeo.com	D: srv3.pki-demo.secardeo.com	SSL	17.05.2021		
✓	Administrator	E: administrator@pki-demo.secardeo.com	SMIME	17.05.2021		
✓	srv4.pki-demo.secardeo.com	D: srv4.pki-demo.secardeo.com	SSL	20.05.2021		
✓	srv5.pki-demo.secardeo.com	D: srv5.pki-demo.secardeo.com	SSL	20.05.2021		
✓	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 ist standardisiert und weit verbreitet
- Unterstützt Verschlüsselung & Signatur
- Benutzerkomfort und einfache Verwaltung durch
 - Automatisiertes Certificate Enrollment & Retrieval
 - Zentrales Certificate Lifecycle Management
- Globale Ende-zu-Ende Verschlüsselung von jedem Gerät mit jedem Partner
- SECARDEO TOPKI
 - PKI Automatisierung für beliebige Zertifikate
 - S/MIME, SSL/TLS, VPN, Computer/Device, ...

Danke für Ihre Aufmerksamkeit!

Besuchen sie uns:
Halle 9 / 9-645