

PKI Automation

Distributing and managing certificates
from any CA for all your devices

Dr. Gunnar Jacobson



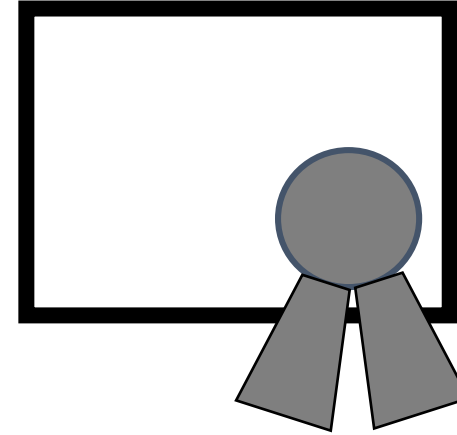
Certificates – for what?

What applications use PKI credentials in your organization?*

81%
SSL/TLS

75%
VPN

54%
S/MIME

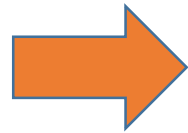


58%
802.1x

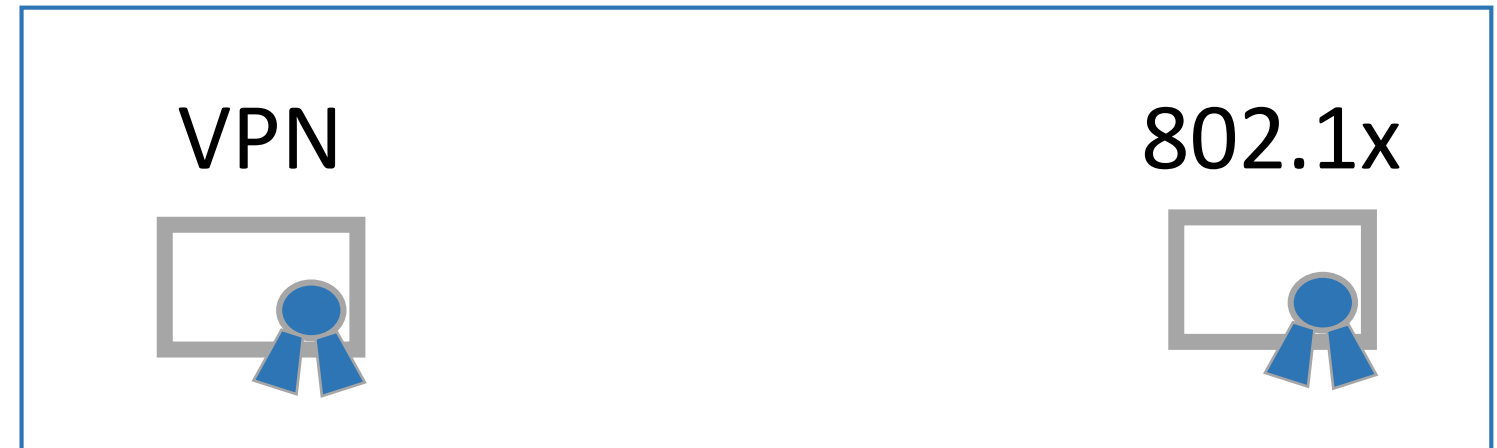
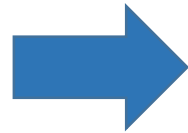
*Ponemon Research 2016

Certificates – from where?

Public CA



Private CA

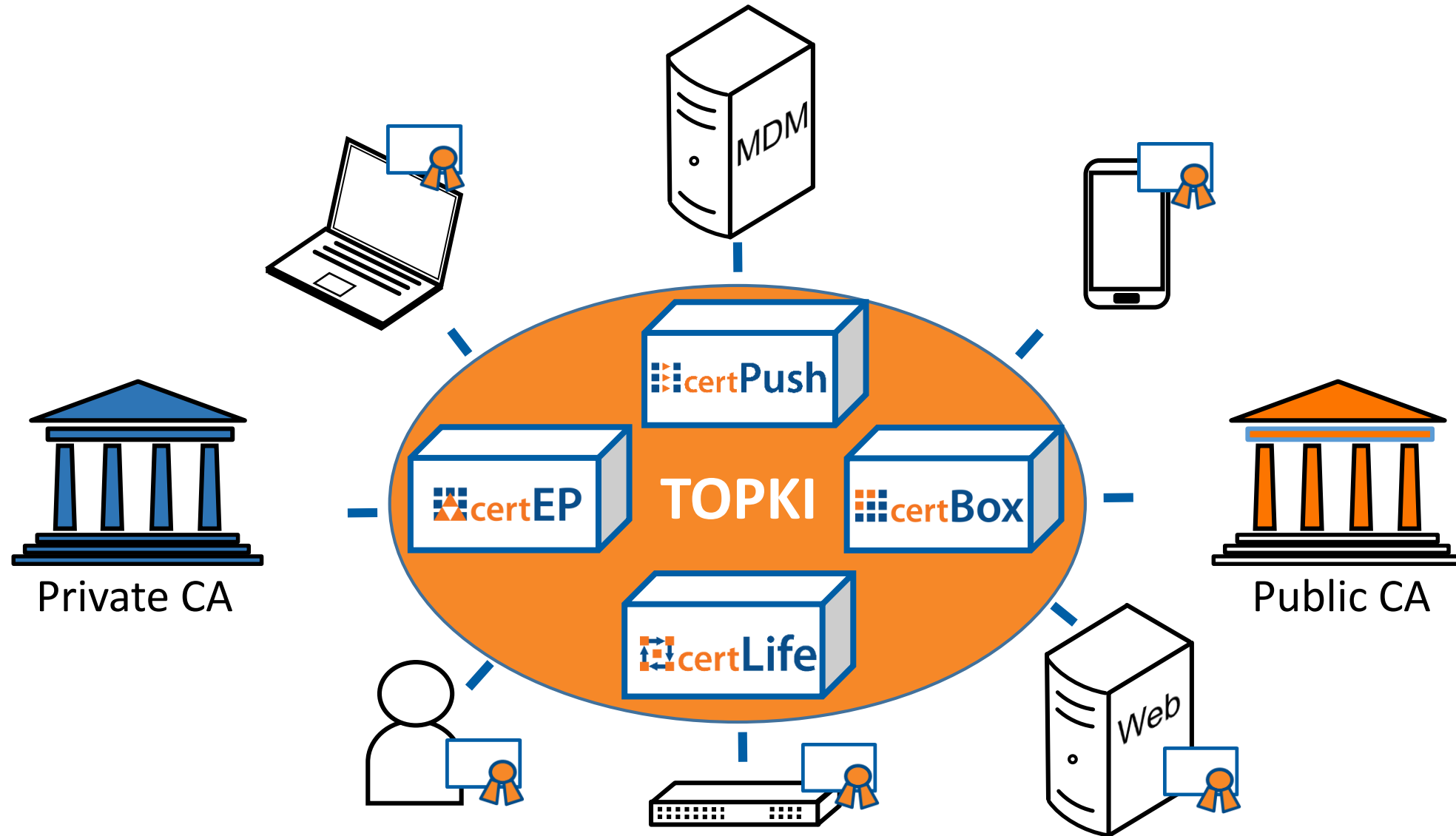


CA Options

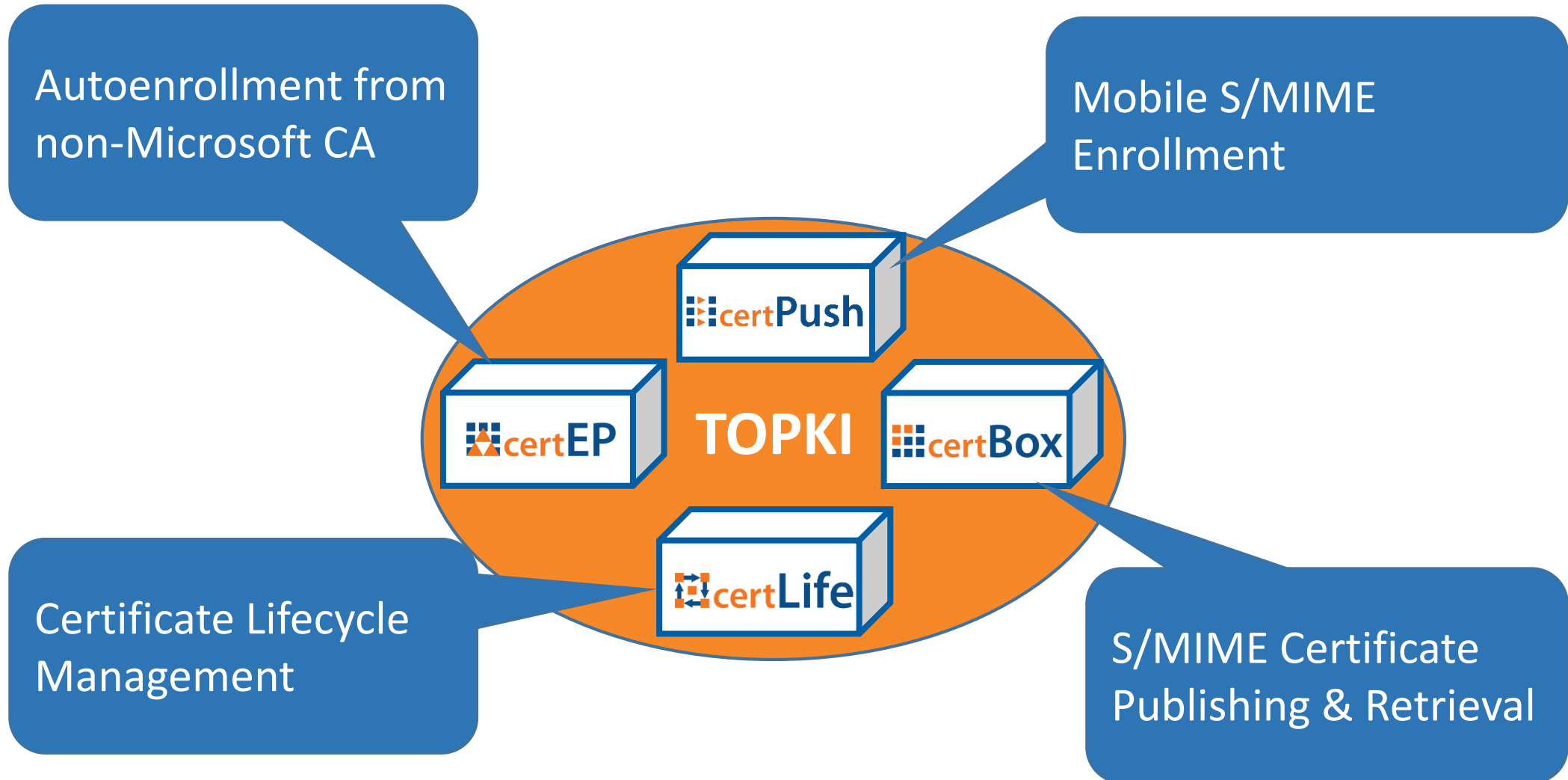
- Microsoft CA (AD CS)
 - Integrated component of Windows Server
 - Autoenrollment
 - Popular & simple
- PKI Products
 - Proprietary, expensive
- Open Source
 - Control over the code
 - No AD integration, no autoenrollment
- Managed PKI
 - Service for a calculable price
 - Trust in CA Provider required
 - AD integration & autoenrollment needed

Distribute & manage certificates

SECARDEO



TOPKI components

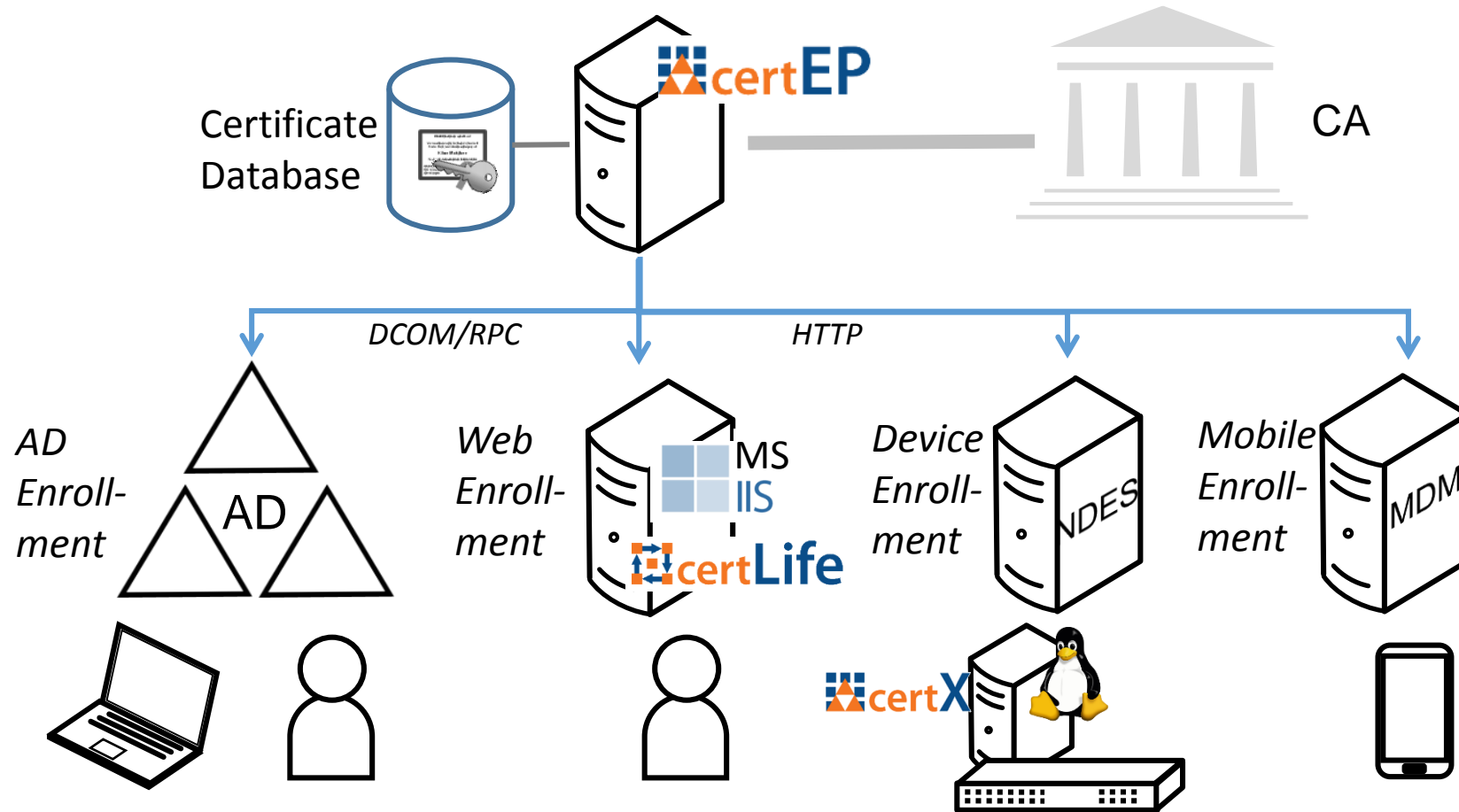


Windows Autoenrollment

- Requirement: Use a non-Microsoft CA for a Windows domain, e.g.
 - Internal OpenSource CA for device certificates
 - Public CA for trusted S/MIME certificates
- Solution: Certificate Enrollment Proxy
- Acts like a Windows Enterprise CA
- Seamless Active Directory integration
- Autoenrollment
- Autorevocation
- Key Archival & Recovery

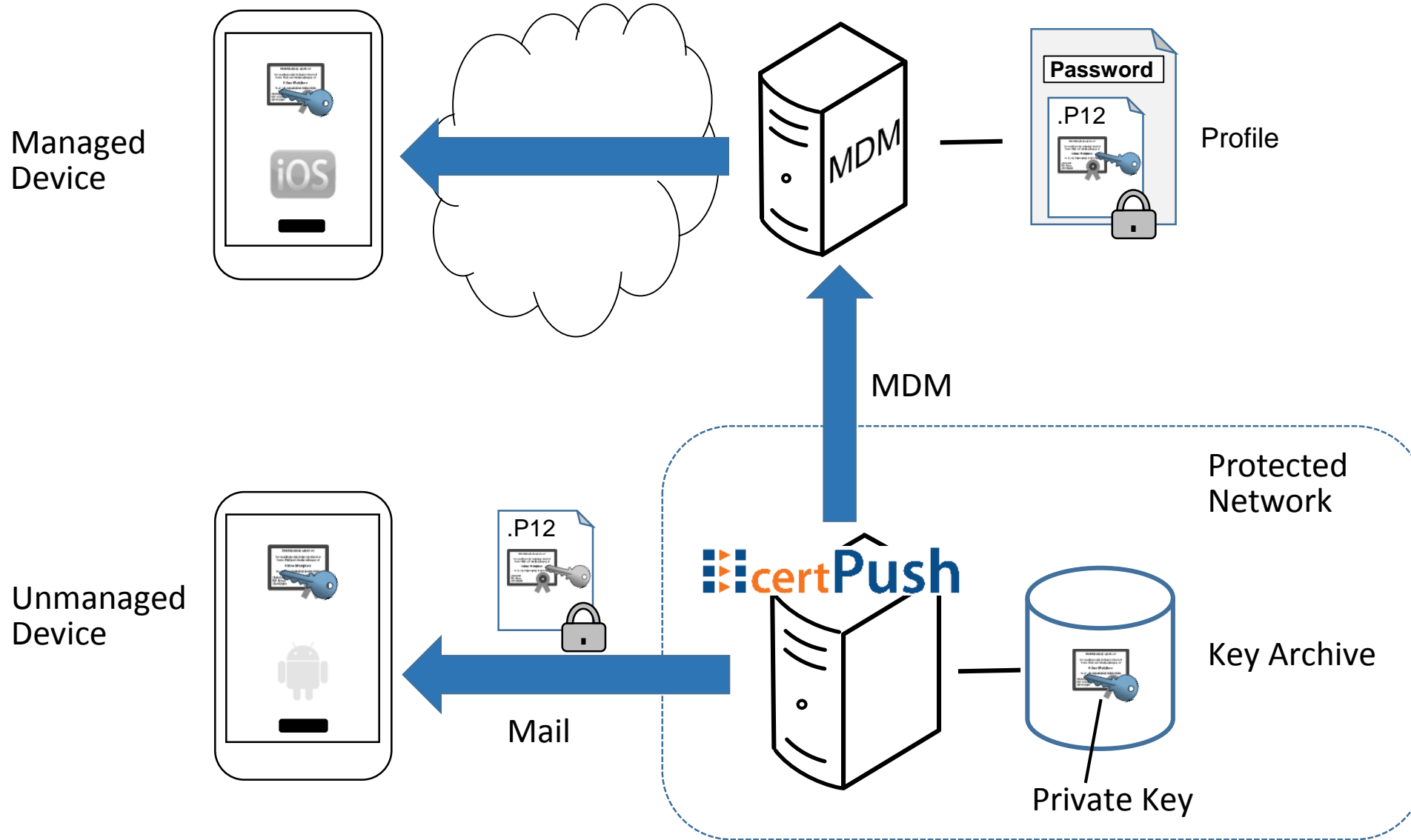


Enrollment scenarios

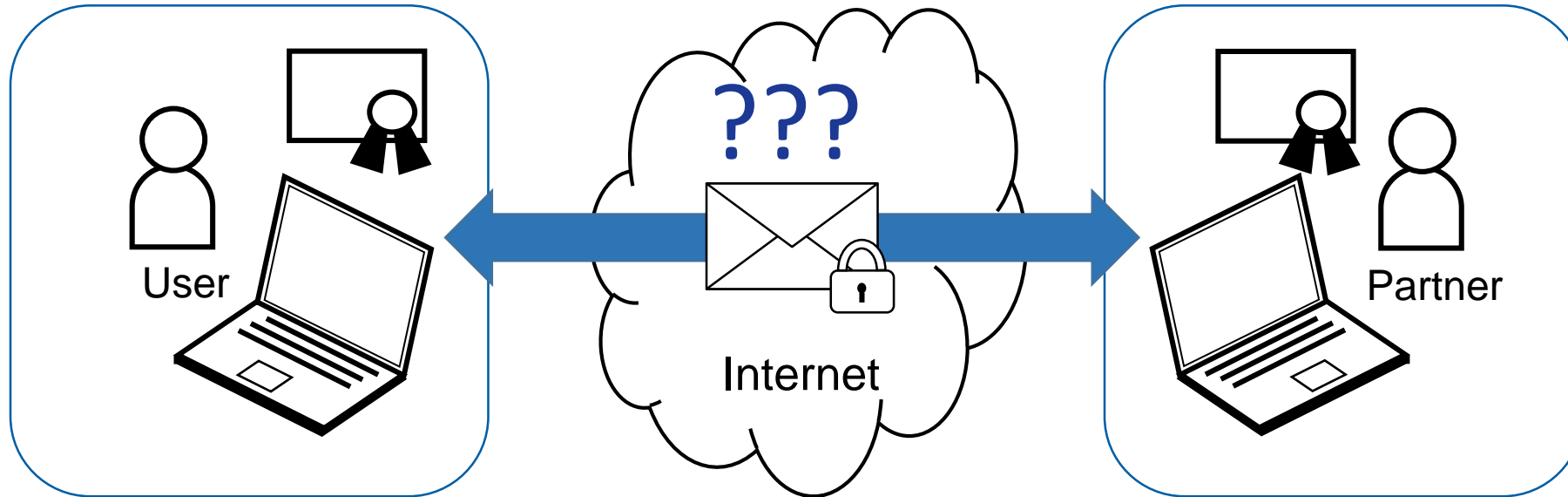


Mobile S/MIME Enrollment

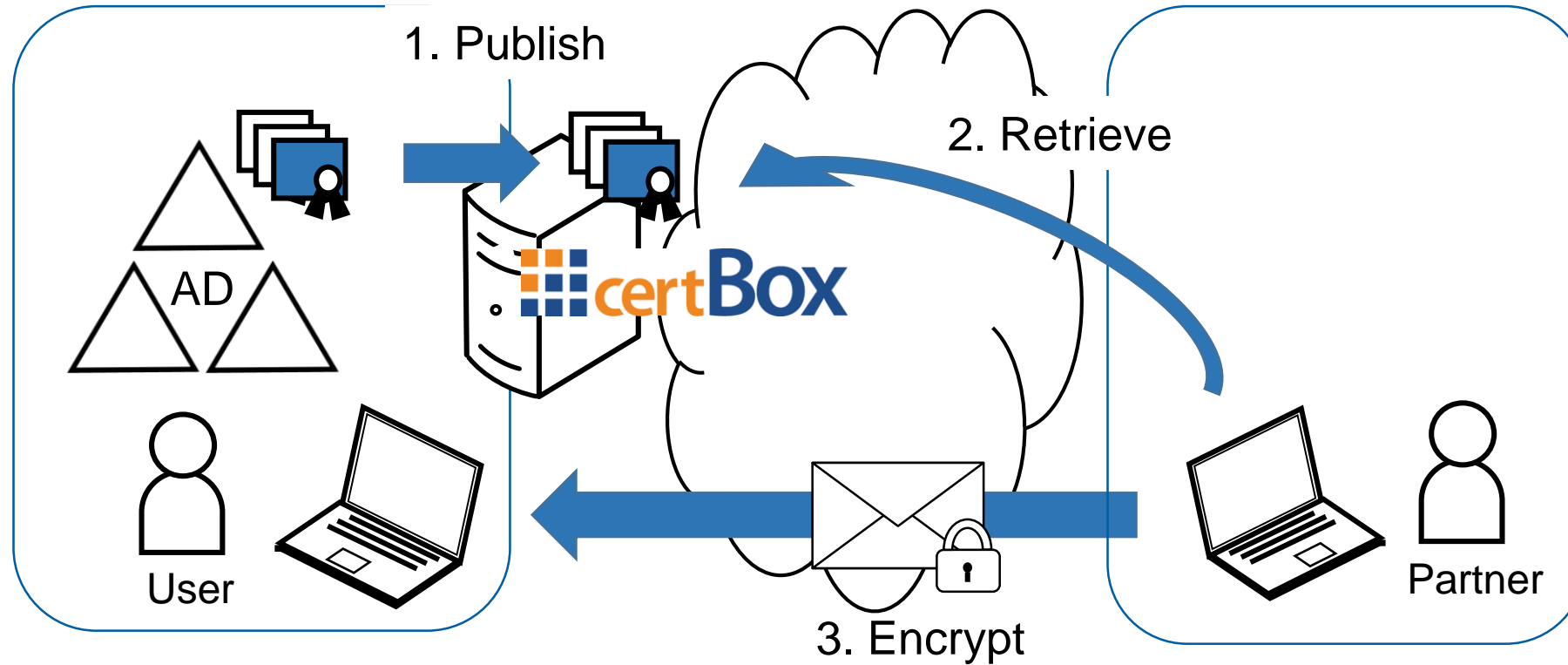
SECARDEO



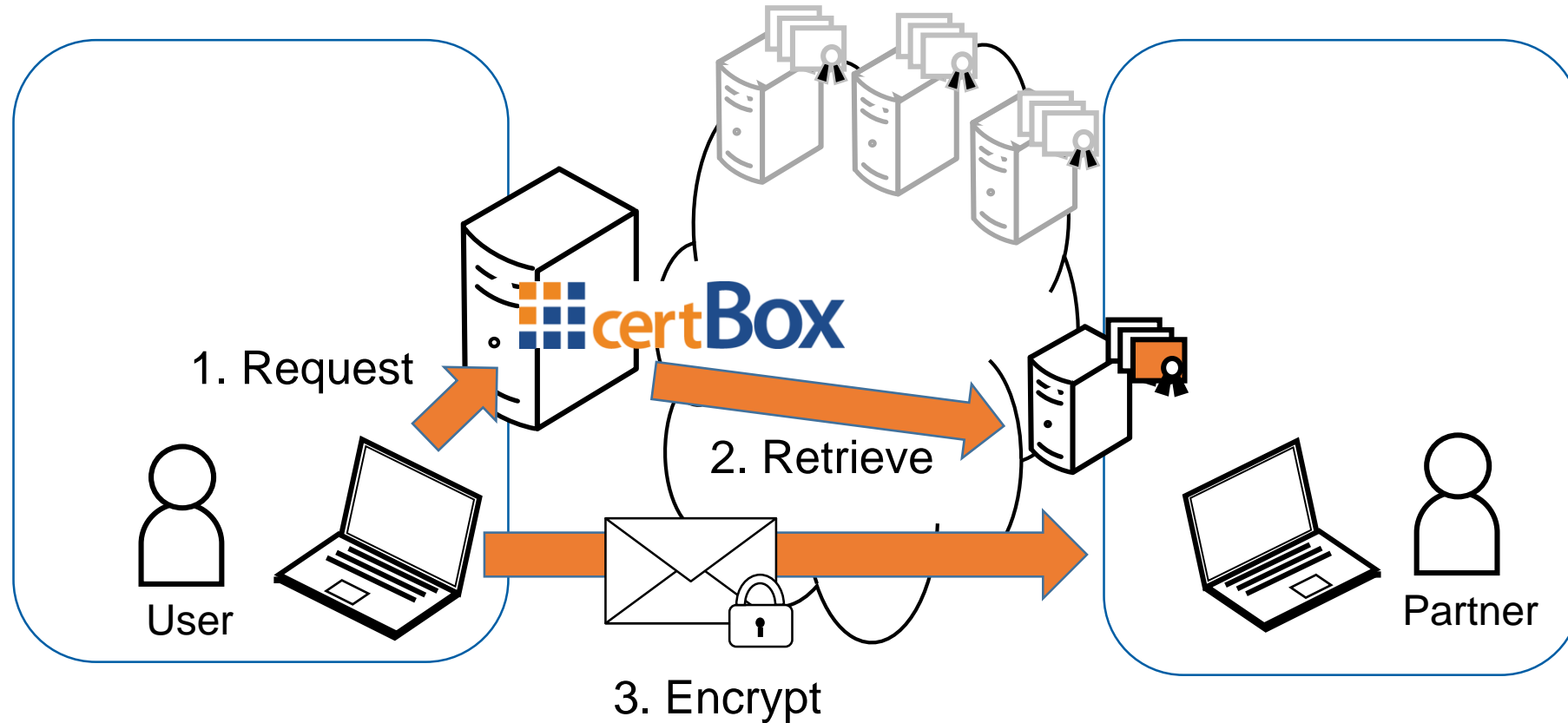
End-to-end encryption



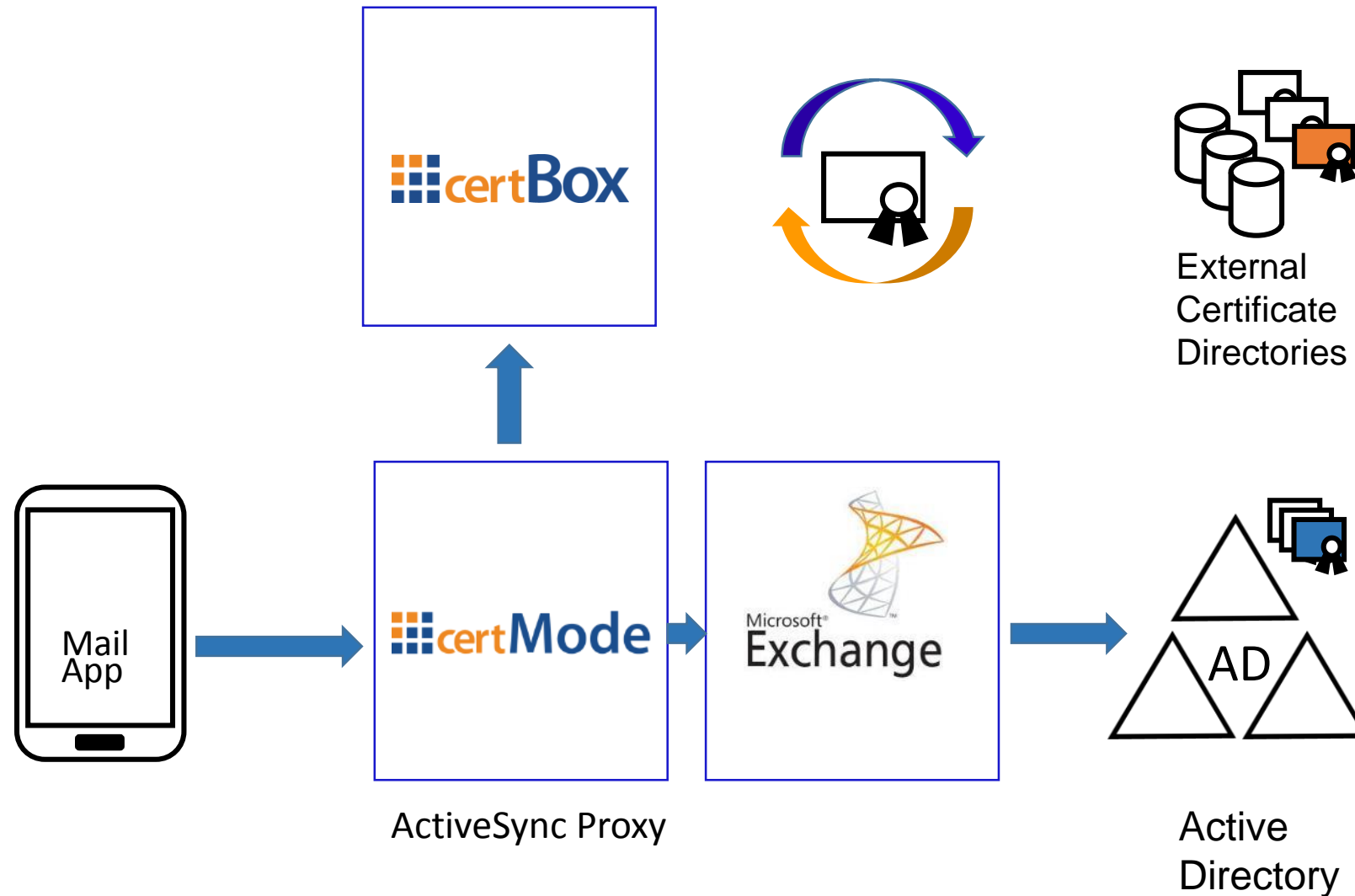
Incoming e2e encryption

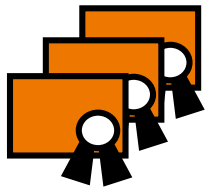
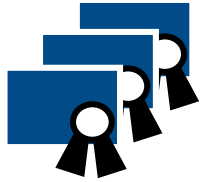


Outgoing e2e encryption



Mobile e2e encryption





Web App for:

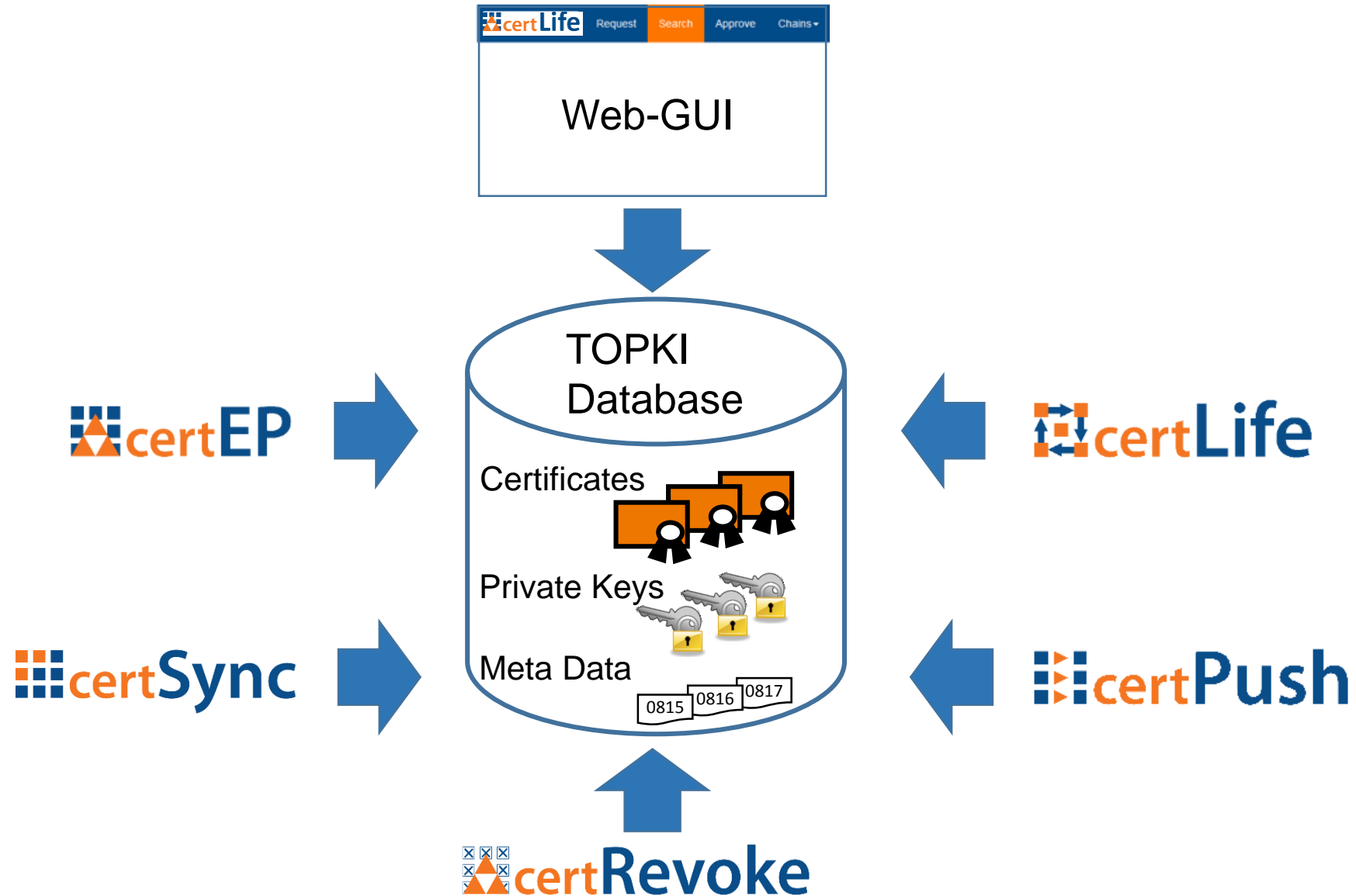
- Role based certificate lifecycle management
- Certificate operations
- Meta data
- User & administrator self-services

Services for:

- Reporting/Statistics
- Notifications
- Central key-pair generation

Certificate database

SECARDEO



Manage certificates with browser

The screenshot shows a web browser window with the URL `www.yourdomain.de/certLife/Search.cshhtml`. The page has a navigation bar with tabs for Request, Search (active), Approve, Chains, and Documentation. A search bar is present at the top. Below it is a table of certificates with columns for Status, Common Name, SAN, Template, Expires, and a menu icon. A context menu is open over the third row, showing options for Revoke, Key Recovery Service (Recover Key, Push Key), and Download (Certificate (PEM), Certificate (DER), Chain (PEM), Chain (DER)).

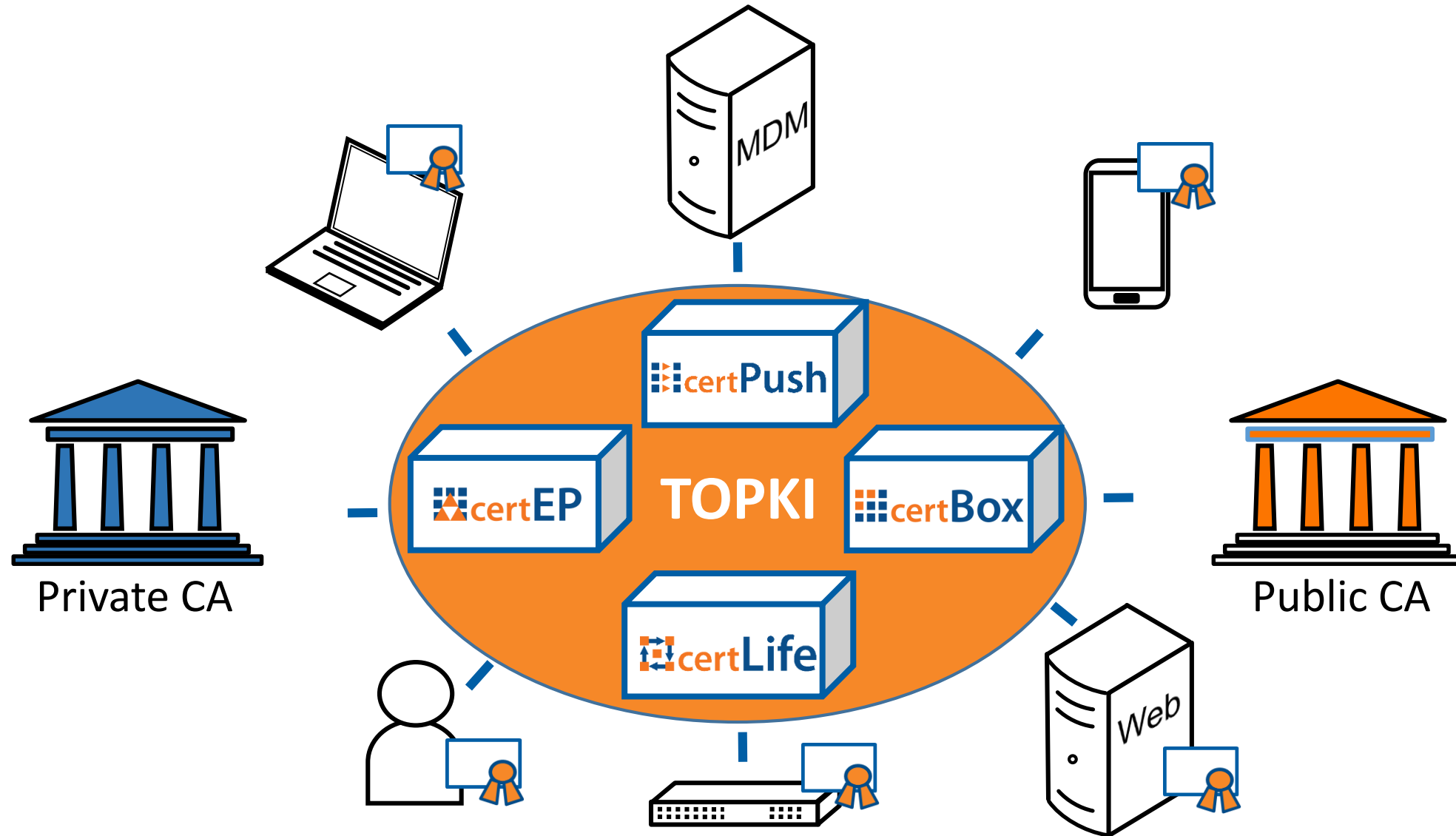
Status	Common Name	SAN	Template	Expires	10 Entries
✓	Mustermann	E: max.muster@exampleDomain.com; R: a...	SMIME	02.08.2017	[Info] [Menu]
✓	Mustermann	E: max.muster@exampleDomain.com; R: a...	SMIME	01.08.2017	[Info] [Menu]
✓	Mustermann	E: max.muster@exampleDomain.com; R: a...	SSL	03.08.2017	[Info] [Menu]

- Revoke
- Key Recovery Service:
 - Recover Key
 - Push Key
- Download:
 - Certificate (PEM)
 - Certificate (DER)
 - Chain (PEM)
 - Chain (DER)



PKI automation with TOPKI

SECARDEO



Thank you for your attention!

Visit us:
Hall 10.1 / 10.1-331