Sichere E-Mail an der TUM

Ansätze und Mobile Geräte als Herausforderung

Dr. Matthias Wachs

Technische Universität München

Lehrstuhl für Netzarchitekturen und Netzdienste
TUM IT-Servicezentrum

11. Cyber-Sicherheits-Tag, München
5. November 2015

Die TUM im Überblick

- $\sim$ 38.500 Studierende
- $\sim$ 10.000 Beschäftigte
- 13 Fakultäten an 3 Standorten
- 6 Wissenschaftliche Zentralinstitute

Die TUM im Überblick

- $\sim$ 38.500 Studierende
- $\sim$ 10.000 Beschäftigte
- 13 Fakultäten an 3 Standorten
- 6 Wissenschaftliche Zentralinstitute

- $\sim$ 1.000 Kooperationsverträge
- Max-Planck- & Fraunhofer-Institute,
- Helmholtz-Zentrum
- 166 Partneruniversitäten

E-Mail als zentrales Kommunikationsmedium

- Interne Kommunikation
- Externe Kommunikation
- Geschäftsprozesse

E-Mail als zentrales Kommunikationsmedium

- Interne Kommunikation
- Externe Kommunikation
- Geschäftsprozesse

Herausforderungen:

- Personenbezogene Daten
- Forschungsdaten, Patentanträge, Vertragsdaten
- Einstellung, Immatrikulation, Prüfungsanmeldungen

TUM Secure E-Mail

Ziel des Projekts

Sichere Kommunikation für alle Mitglieder der TUM mit internen und externen Partnern

TUM Secure E-Mail

Ziel des Projekts

Sichere Kommunikation für alle Mitglieder der TUM mit internen und externen Partnern

- **Lehrstuhl für Netzarchitekturen und Netzdienste**
  Wissenschaftliche Grundlagenarbeit
  System- und Softwareentwurf, Evaluation
- **TUM IT-Servicezentrum**
  Prozesse für TUM-weite Einführung

TUM Secure E-Mail

Ansatz

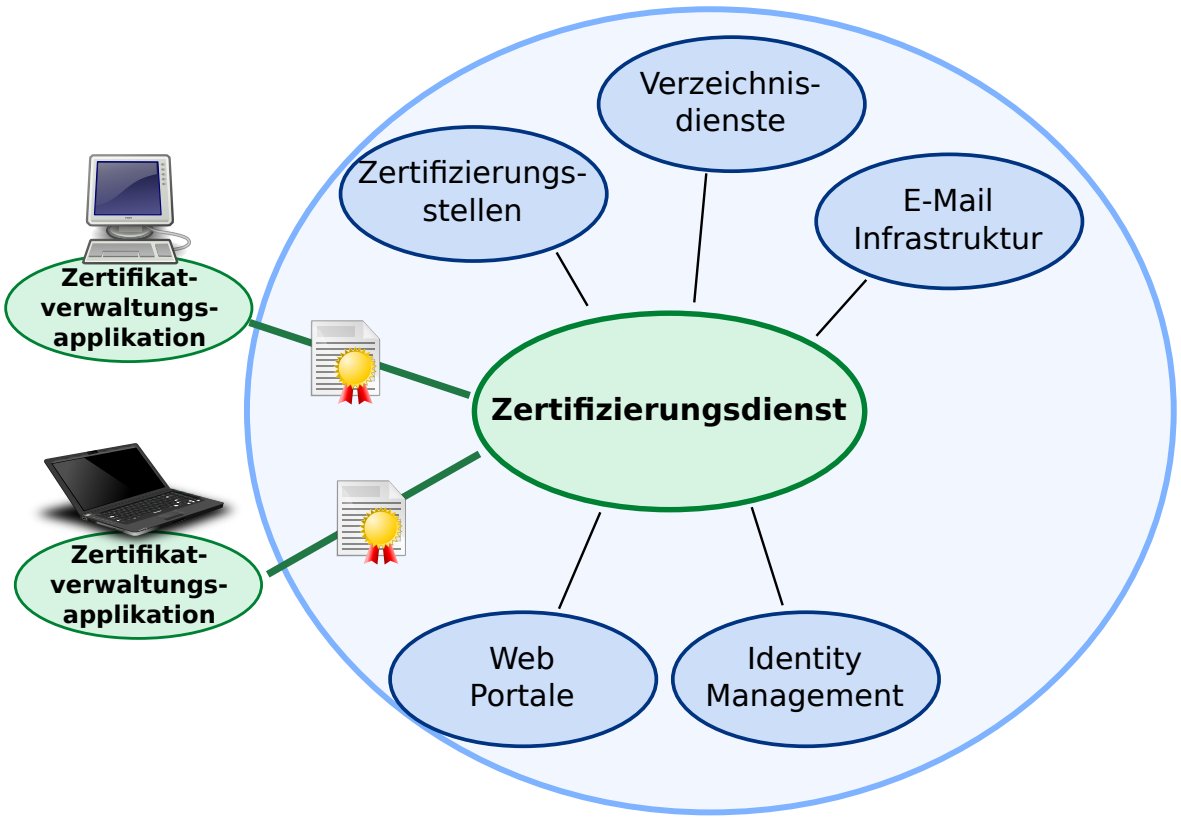
Alle Mitglieder der TUM werden mit digitalen Zertifikaten ausgestattet

- Ende-zu-Ende-Verschlüsselung
- S/MIME & OpenPGP

TUM Secure E-Mail

Ansatz

- Zentraler Zertifizierungsdienst
- Zertifikatsverwaltungsapplikation für Anwender



TUM Secure E-Mail

Anforderungen

- Sicherheit auf dem Stand von Wissenschaft & Technik
- Integration in existierende IT-Infrastruktur
- Effiziente Prozesse
- Nutzerfreundlichkeit

TUM Secure E-Mail

Nutzerfreundlichkeit

Nutzerakzeptanz notwendig!

Sichere Kommunikation jederzeit und überall

- Etablierte Clients
- Mobile Geräte

TUM Secure E-Mail

Herausforderung Mobile Geräte

E2E-Verfahren nicht auf mehrere Geräte ausgelegt

- Private Schlüssel
- Zertifizierungsstellen
- Öffentliche Schlüssel
- Vertrauensstellungen

$\rightarrow$ Synchronisation

TUM Secure E-Mail

Herausforderung Mobile Geräte

Sichere Schlüsselspeicherung

Hardware-Token:

- Heterogenität
- Kosten
- Anbindung

TUM Secure E-Mail

Herausforderung Mobile Geräte

Sichere Schlüsselspeicherung

Hardware-Token:

- Heterogenität
- Kosten
- Anbindung

Mehrere Zertifikate:

- S/MIME & OpenPGP
- Verschlüsselung und Identität
- Personen, Gruppen, Funktionszertifikate

TUM Secure E-Mail

Herausforderung Mobile Geräte

- Device-Management:
  Enrollment, Verlust, Sperrung, Löschung
- Private Geräte & BYOD
- E-Mail-Client-Unterstützung

TUM Secure E-Mail

Zusammenfassung

Unser Fokus:

- Bereitstellung & Verwaltung von Zertifikaten
- Automatisierte Verwendung durch den Nutzer
- Unterstützung mehrerer Endgeräte

TUM Secure E-Mail

Zusammenfassung

Unser Fokus:

- Bereitstellung & Verwaltung von Zertifikaten
- Automatisierte Verwendung durch den Nutzer
- Unterstützung mehrerer Endgeräte

Herausforderungen für uns:

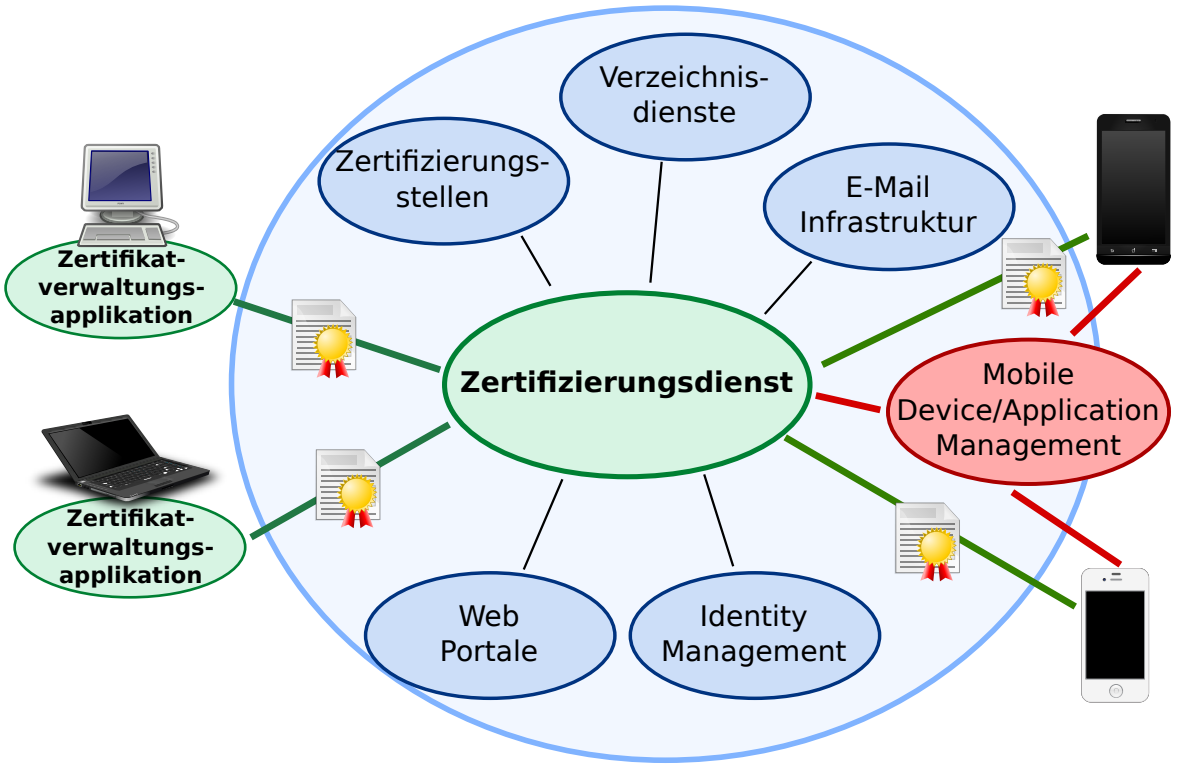
- Mobile Device Management
- Mobile E-Mail-Anwendungen

TUM Secure E-Mail

Zusammenfassung

Ziel:

- Integration Zertifikatsverwaltung und MDM



Danke für die Aufmerksamkeit!

Fragen?

Kontakt:

matthias.wachs@tum.de