

E-MAIL, WEB, ROUTER

SICHERE KOMMUNIKATION IN UNTERNEHMEN

Zahlreiche Anwendungen und Geschäftsprozesse setzen inzwischen voraus, dass Daten vertraulich und vor Veränderungen geschützt übertragen werden. Hinzu kommt die eindeutige Identifizierung der Kommunikationspartner als Sicherheit für die Herkunft bzw. den Adressaten der Daten. Schließlich gilt es, kostengünstige Kommunikationsplattformen zu nutzen und Geschäftsprozesse ohne Medienbrüche zu optimieren. Daher ist es unkompliziert, die IT-Schutzziele Integrität, Authentizität und Vertraulichkeit in den vielfältigen Anwendungen und Geräten zu integrieren; werden doch bereits heute zahlreiche Sicherheitsmechanismen standardmäßig unterstützt.

BEISPIELE

RISIKEN FÜR HANDEL

- Mitlesen und/oder Verändern von E-Mails.
- Keine Identität Ihres Web-Portals.
- Unsichere Identität der Kommunikationspartner.

RISIKEN FÜR FERTIGUNG

- Know-How Verlust durch Datendiebstahl.
- Manipulation der Lieferkette.
- Konkurrenzspionage, Produktpiraterie.

RISIKEN FÜR DIENSTLEISTUNG

- Impersonation (Nachahmung, Identitätswechsel).
- Verpasste Marktchancen.
- Imageverlust.



Erfahrungen aus
> 300 Millionen
ausgestellten
Zertifikaten

MÖGLICHE GEFAHREN

- Datendiebstahl durch unberechtigten Zugriff auf Ihr Unternehmen.
- Manipulation von Dokumenten / Projekten.
- Wirtschaftskriminalität, Konkurrenzspionage, Produktpiraterie.



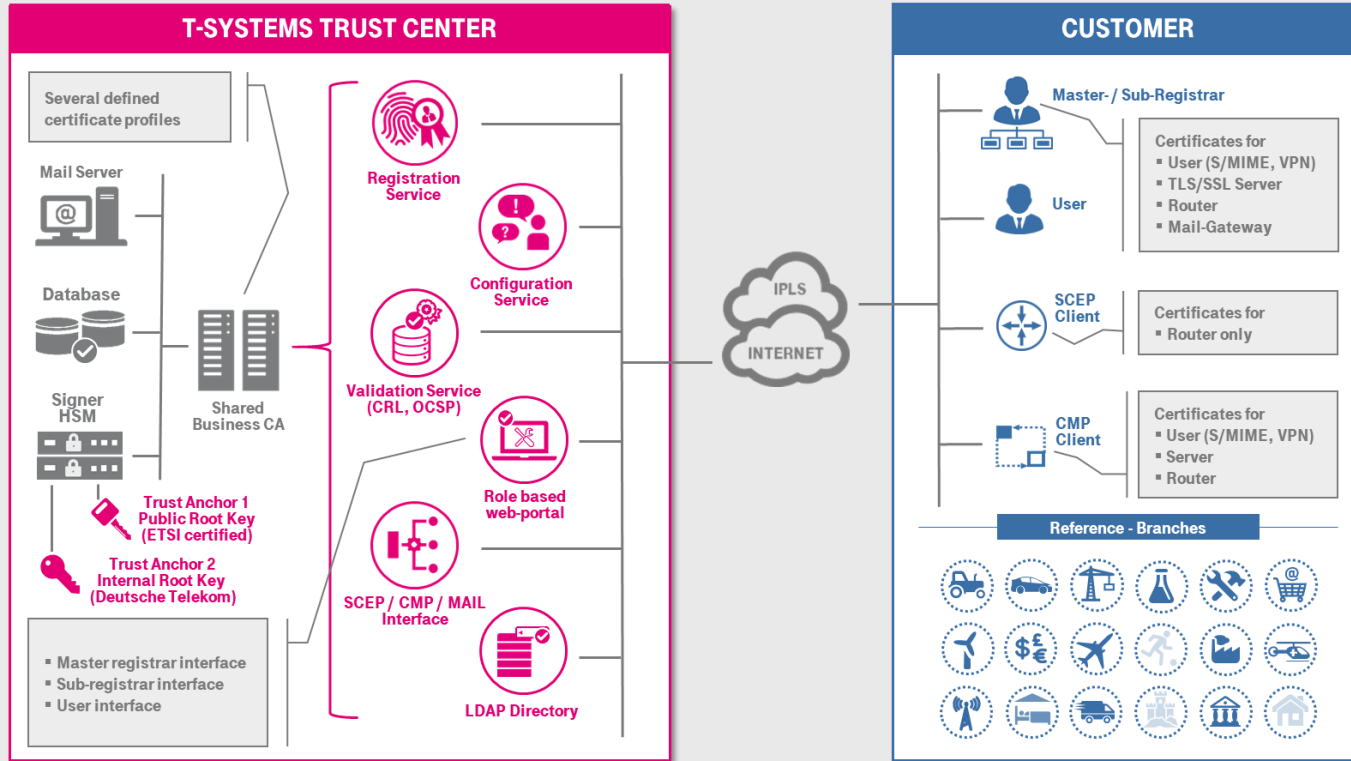
DIE LÖSUNG

TeleSec Shared-Business-CA der mandantenfähige Managed PKI Service (Public Key Infrastruktur) aus dem T-Systems Trust Center. Zertifikate für Benutzer, Server, Mail-Gateway und Router einfach verwalten.



TELESEC SHARED BUSINESS CA

VORTEILE AUF EINEN BLICK



- 🔒 **Verfügbarkeit:** Zugesicherte hohe Verfügbarkeit und damit hohe Ausfallsicherheit durch ein Service Level Agreement (SLA).
- 🔒 **Komfort:** Einfache Bereitstellung einer PKI „out of the box“. Vollständige Dokumentation (z.B. Arbeits- und Installationsanleitung, rollenspezifische Handbücher)
- 🔒 **Skalierbarkeit:** Kann nach Zertifikatsbedarf (Anzahl der Mitarbeiter) und/oder Anwendungen (z.B. Mail, VPN, Server) flexibel angepasst werden.
- 🔒 **Zukunftssicher:** Stets Zugriff auf hochqualifiziertes Trust-Center-Personal. Einhaltung internationaler Standards (ETSI EN 319 411-1). Verwendung aktueller Technologien und Mechanismen.

V01

LEISTUNGEN: Betriebsmodell

- mandantenfähiger PKI-Service als ASP-Modell (Application Service Provider).
- PKI-Betrieb im hochsicheren georedundanten Trust Center.

Service

- PKI-Anbindung via Internet
- Bereitstellung unterschiedlicher Zertifikatstypen (z.B. Mail-Security, VPN, TLS-Server, Mail-Gateway)
- Last-Level-Support

Optionales

- Individuelle PKI-Anbindung via MPLS (Multiprotocol Label Switching)

INTERESSE?

Vertrauen Sie dem führenden Anbieter von Sicherheitslösungen.

Kontakt:

T-Systems International GmbH
 security-info@t-systems.com
 www.t-systems.de/security

