

E-Mail, Web, Router

Secure communication in companies

Numerous applications and business processes today require that data be transmitted confidentially and protected against changes. In addition, the clear identification of the communication partners as security for the origin or the addressee of the data. Finally, it is important to use cost-effective communication platforms and to optimize business processes without media breaks. It is therefore uncomplicated to integrate the IT protection goals of integrity, authenticity and confidentiality in the diverse applications and devices; after all, numerous security mechanisms are already supported as standard today.



Experience from > 300 million issued certificates

Potential hazards

- Data theft through unauthorised access to your company.
- Manipulation of documents / projects.
- White-collar crime, competitive espionage, product piracy.



Examples

Risks for Trading

- Reading and/or modifying e-mails.
- No identity of your web portal.
- Insecure identity of the communication partners.

Risks for Produktion

- Loss of know-how due to data theft.
- Manipulation of the supply chain.
- Competitive espionage, product piracy.

Risks for Services

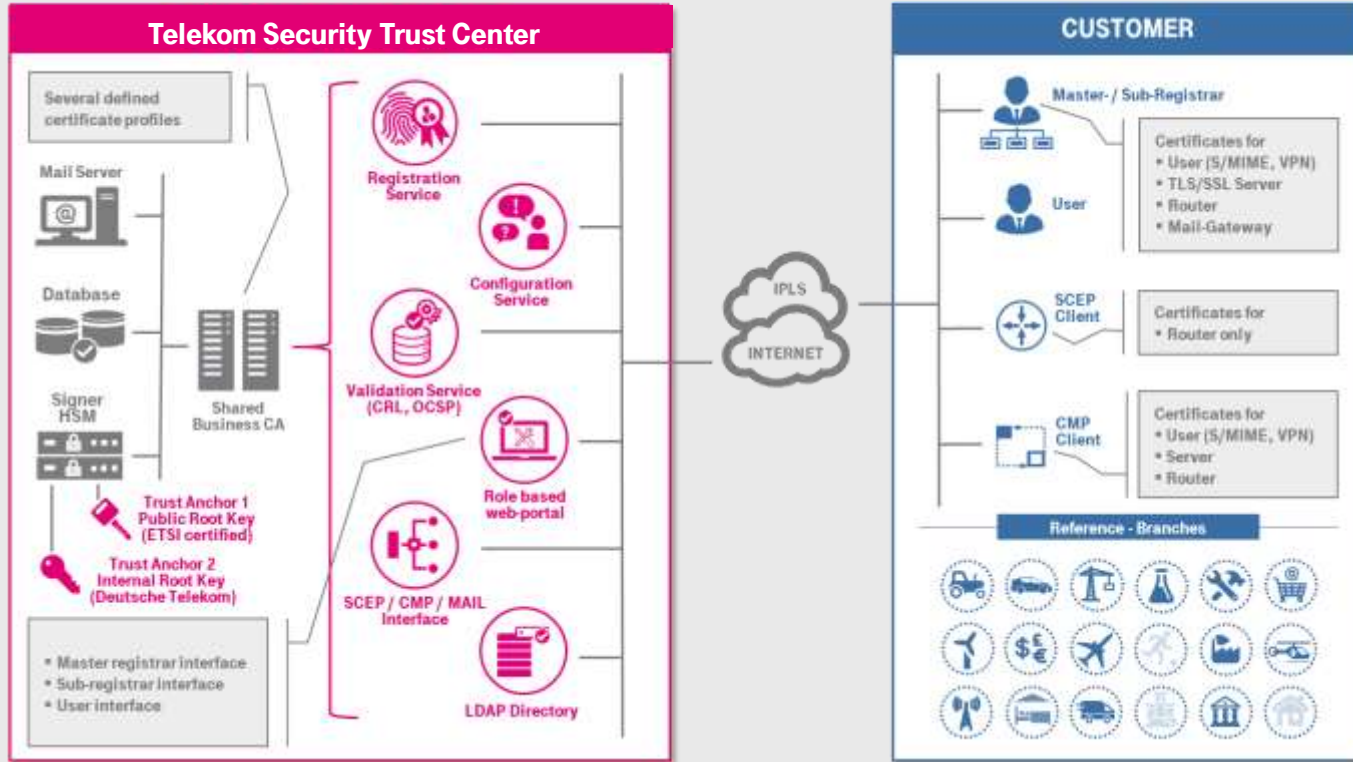
- Impersonation (imitation, identity changes).
- Missed market opportunities.
- Loss of image.



THE SOLUTION

Magenta Security Business.ID the multi-tenant PKI Service (Public Key Infrastructure) from the Telekom Security Trust Center. Easily manage certificates for users, servers, mail gateways and routers.





Magenta Security Business.ID

The advantages at a glance

- Availability: Guaranteed high availability and thus high reliability through a Service Level Agreement (SLA).
- Convenience: Simple provision of a PKI “out of the box”. Complete documentation (e.g. work and installation instructions, role-specific manuals)
- Scalability: Can be flexibly adapted according to certificate requirements (number of employees) and / or applications (e.g. mail, VPN, server).
- Future-proof: Always access to highly qualified trust center staff. Compliance with international standards (ETSI EN 319 411-1). Use of current technologies and mechanisms.

Services:



Operation model

- Multi-tenant PKI service as an ASP model (Application Service Provider).
- PKI operation in the highly secure geo-redundant trust center.

Service

- PKI connection via the Internet
- Provision of different certificate types (e.g. S/MIME, VPN, TLS server, mail gateway)
- Last-Level-Support

Optional

- Individual PKI connection via MPLS (Multiprotocol Label Switching)

Interest?

Trust the leading provider of security solutions.

Contact:

Deutsche Telekom Security GmbH
 security-info@t-systems.com
 www.t-systems.de/security

