



Produktpräsentation TeleSec OneTimePass



Telekom Security

Product Cluster Identity Security



Marktführer in ID-Security Services in Deutschland



Hochverfügbarer, skalierbarer Betrieb im Telekom Trust Center



Eigene international anerkannte Root-Schlüssel



Eigene Softwareentwicklung für Krypto-Komponenten



Eigenes Betriebssystem TCOS für Secure-Elements und Chipkarten



Vertrauensdienste Anbieter (VDA) gem. EU-Vertrauensdienste Verordnung eIDAS



Vielfach Zertifizierte Sicherheit (z.B. ETSI, ISO27001)



> 20 Jahre ID-Security Erfahrung



Betrieb nach IT Infrastructure Library (ITIL)



Erfahren in der Umsetzung komplexer und großer Security Projekte



Identity Security

Unsere Produkte im Überblick




Certificate Services & PKI

IoT / M2M PKI-Service P



Hoch automatisierte Ausstellung und Management von Zertifikaten für die „DINGE“ im Netz.

TeleSec Server Pass S



SSL / TLS Web-Server Zertifikate für die sichere Kommunikation im Web. In allen Browsern als sicher eingestuft.

TeleSec Public Key Service S



Qualifizierte elektronische Signatur und Fernsignatur nach eIDAS, als Ersatz für die handschriftliche Signatur.

TeleSec Shared Business CA S




Die Cloud Public Key Infrastructure (PKI) für die flexible und schnelle Einbindung in Ihr Unternehmen.

Smart Meter Energy CA P



Nach BSI (TR3109) zertifizierte Ausgabe und Management von Zertifikaten im Smart-Meter ECO System.

Individual PKI P




Planung, Aufbau und Betrieb von kundenindividuellen PKI Lösungen im Trust Center oder beim Kunden.



Smartcards & Secure Elements

TCOS Smartcards P



Ausweissysteme für elektronische Reisepässe und nationale ID-Karten. Smartcard basierte Projektlösungen.


TCOS Secure Elements P



Sicherer Speicher und Sicherheitsanker für digitale Identitäten von Personen und Geräten.

Access Management

TeleSec One Time Pass S



Die Cloud Authentifizierungslösung ermöglicht starke Zwei-Faktor-Authentifizierung mittels Einmalpasswort.

Professional Services @ ID

Solution Design & Engineering P



Anforderungsmanagement; Techn. Solution- und Prozessdesign; Architektur und Engineering

Trusted IT Operations

TeleSec OneTimePass

Die Herausforderung



Herausforderungen

- Schutz vertraulicher Daten im Unternehmen
- Eliminierung von schwachen und leicht zugänglichen Passwörtern
- Reduzierung von Helpdesk-Aufwänden und Kosten
- Einfache und schlanke Prozesse im Wirkbetrieb / einfache Integration
- Eine vom Nutzer akzeptierte und einfache Lösung
- Erfüllung gesetzlicher Vorgaben (Compliance / DSGVO)

Mögliche Gefahren

- Weitergabe und unberechtigtes Nutzen fremder Passwörter
- Wirtschafts- und Industriespionage
- Wirtschaftsschäden durch Erpressung
- Nicht nutzbare IT-Systeme

Mögliche Risiken

- Datendiebstahl
- Identitätsdiebstahl
- Know-How Verlust
- Produktivitätsverluste
- Imageschäden
- Rechtliche Konsequenzen
- Finanzielle Verluste



TeleSec OneTimePass

Die UseCases



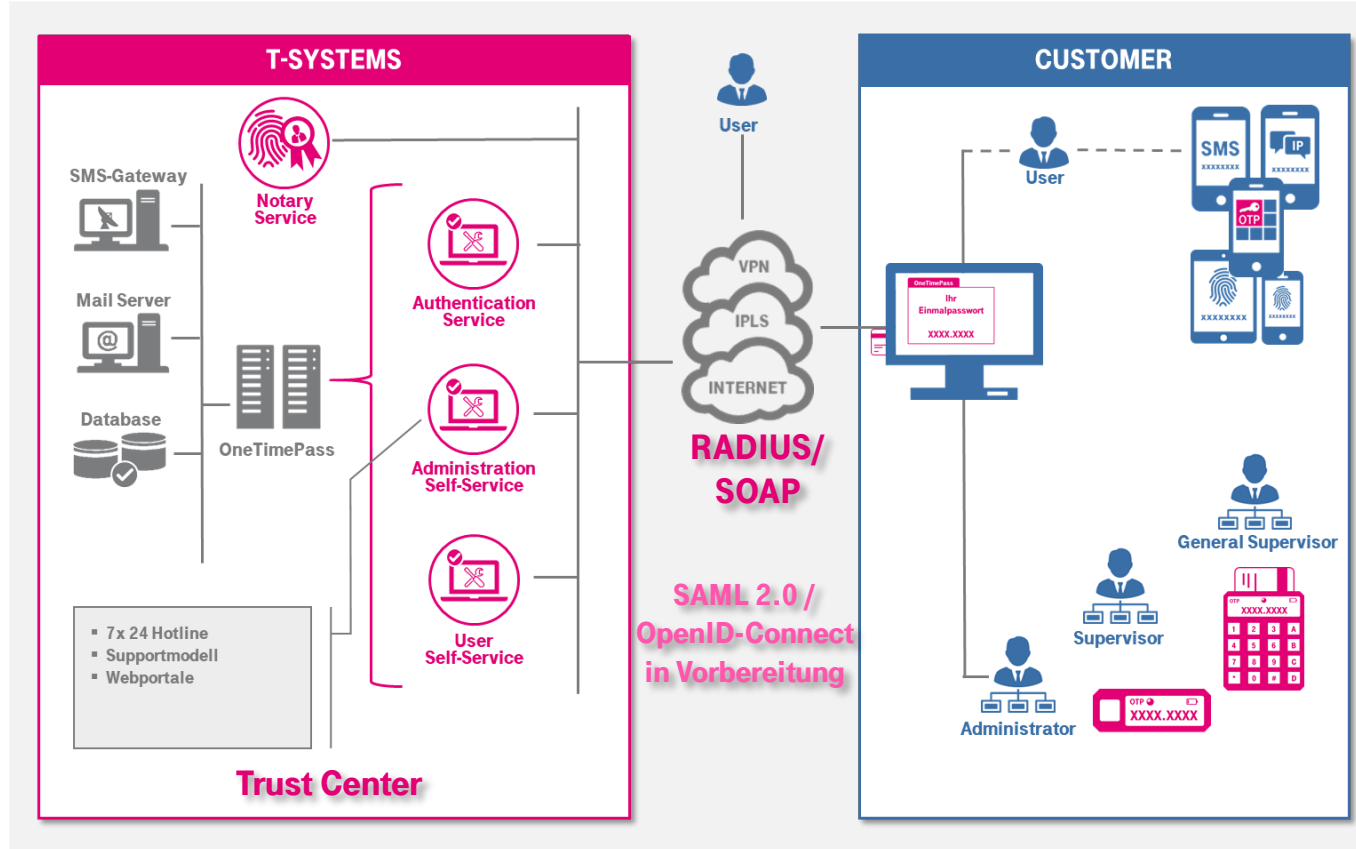
Die UseCases (Auszug)

- **Remote Access**
 - Mobiles Arbeiten ohne Verzicht auf Sicherheit
 - Kurzfristige Umsetzung
 - VPN-Zugang
 - Anbindung an virtuelle Desktop-Infrastruktur (Citrix)
- **M-TAN**
 - Mobile TAN only als zusätzlicher Faktor (MFA)
 - Mobile TAN inkl. Passwort (2FA)
 - Übertragung der generierten OTPs via SMS (IP-Client (verschlüsselt) in Vorbereitung)
- **Geschlossene Benutzergruppen**
 - Schutz von Webseiten / Bereichen oder Anwendungen vor Zugriff Unbefugter
- **Cloud Security**
 - Absicherung von Benutzer- und privilegierten Cloudzugängen



TeleSec OneTimePass

Die Lösung



Daten

- Zentral gehostete Lösung
- Trust Center basiert
- Kundenadministration
- Datenhoheit beim Kunden

Aufwand

- Investitionssicherheit
- Keine Laufzeitbegrenzung der Token
- Kein Eingriff in Clientsoftware
- Skalierbar

Support

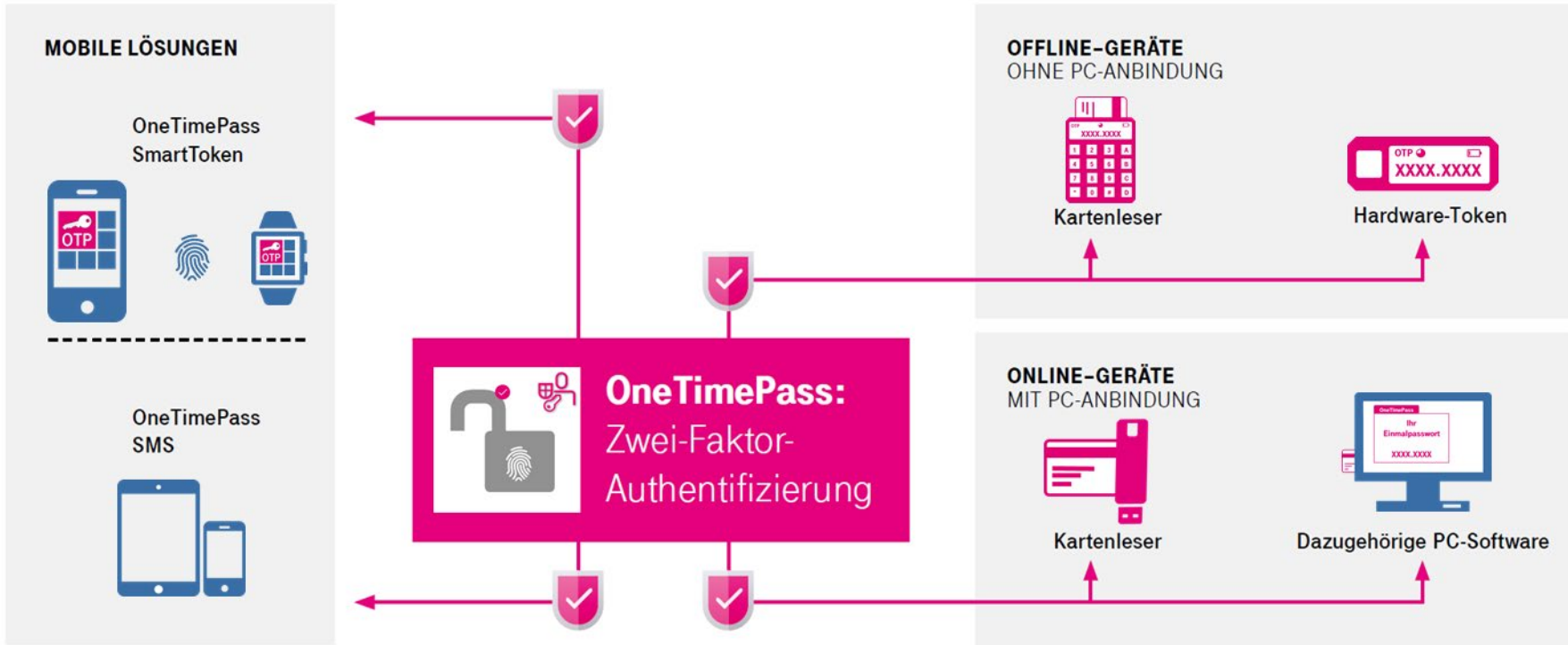
- Support 7x24
- Migrationsunterstützung



TeleSec OneTimePass

Die Token







- Für jeden Anwendungsfall und Kundenwunsch der passende OTP-Generator
- Kategorisierung anhand der Bauart
- Beliebig kombinierbar



TeleSec OneTimePass

Der Nutzen



-  **Erhöhte Netzwerk- und Kommunikationssicherheit**
-  **Flexibilität durch Nutzung von Standards**
-  **Volle Datenhoheit**
-  **Eliminierung schwacher, statischer Passwortsysteme**
-  **Schlanke und günstige Prozesse im Wirkbetrieb**
-  **Kosten- und Investitionssicherheit**



TeleSec OneTimePass Support- & Service-Schnittstellen



Support-Schnittstelle

1st Level

- Montag – Freitag
(außer an Feiertagen)
- 07:00 Uhr bis 19:00 Uhr
- Deutsch / Englisch

2nd Level

- Montag – Freitag
(außer an Feiertagen)
- 08:00 Uhr bis 16:00 Uhr
- Deutsch / Englisch

Service-Schnittstellen

Störungsmeldungen

- Montag - Sonntag
- 00:00 Uhr bis 24:00 Uhr
- Deutsch / Englisch

Service-Portal

- Homepage TrustCenter-Solutions
 - Vorstellung OTP-Service
 - Links zu Webservices
 - Kontakt
 - Download-Bereich

Webservices

- OTP-Nutzerportale
 - User-Selfservice
 - Nutzeradministration
 - Verwaltung OTP-Provider



TeleSec OneTimePass Bereitstellung & Implementierung



Voraussetzungen

Produktvorstellung

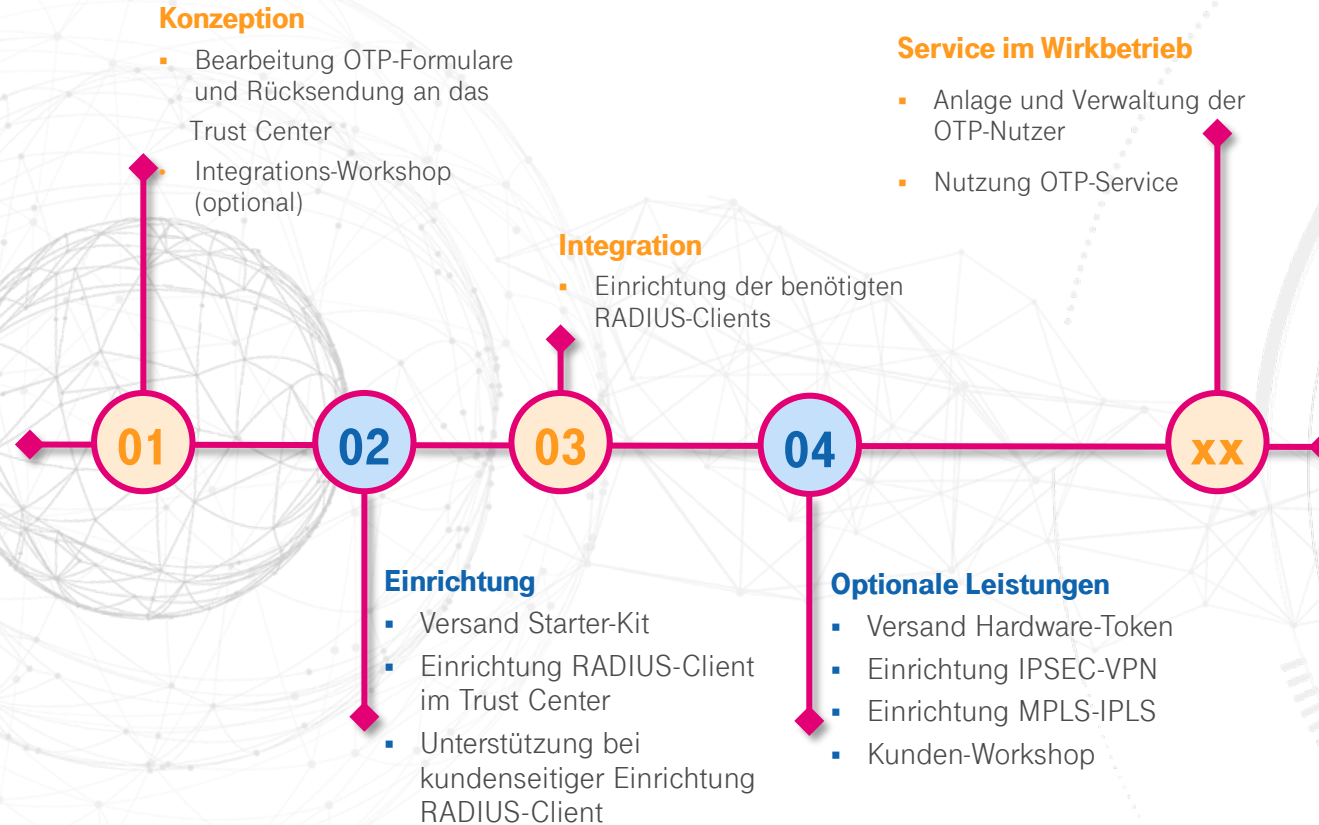
- Nutzungsvoraussetzungen
- Art der Anbindung
- Schnittstellen (RADIUS, SOAP (Automatisation))

Angebotserstellung

- Mengengerüste
- Authentifizierungsmedien
- Art der Anbindung
- Nutzung national / international (Tokenart)

Bereitstellung

- OTP-Formulare
- Handbücher/ Dokumentationen
- Optional: OTP-Teststellung



TeleSec OneTimePass Preismodell



Einmalige Kosten

- Bereitstellung
 - RADIUS-Client
 - optionale Netz-anbindung (z.B. IPLS)
- Authentifikationsmedien
- Ggf. Kunden-Workshop

Laufende Kosten

- Betrieb
 - OTP Plattformbetrieb
 - OTP-Service abhängig von der Nutzerzahl
 - Ggf. optionale Netzanbindung

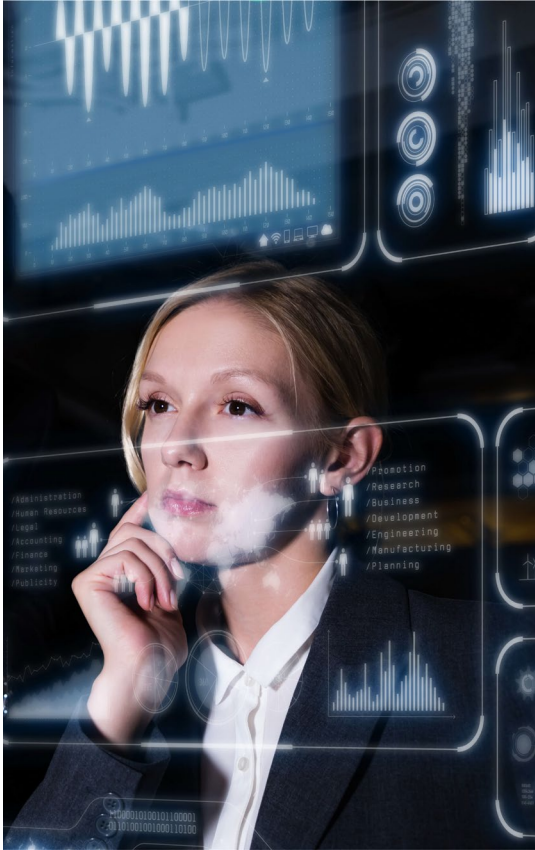
Nutzungsabhängig

- SMS-Token
 - Pauschale pro Nutzer/ pro Monat
 - Ggf. SMS-Einzelabrechnung



TeleSec OneTimePass

Vorteile auf einen Blick



- 1 Starke 2-Faktor-Authentifizierung
- 2 Verschiedene Authentifikationsmedien, beliebig kombinierbar
- 3 Kunde behält die volle Kontrolle, alle administrativen Tätigkeiten bleiben in seiner Hand
- 4 Einfache Integration der Anwendung durch Nutzung des Standard-RADIUS-Protokolls
- 5 Reduzierung der möglichen Angriffsszenarien
- 6 Vermeidung von Folgekosten aufgrund möglicher Attacken
- 7 Betrieb zahlreicher Security Lösungen im hochsicheren Trust Center der Deutschen Telekom
- 8 Security made in Germany





Interesse?

Vertrauen Sie dem führenden Anbieter von Sicherheitslösungen.

Kontakt:

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

Herausgeber:

Deutsche Telekom Security GmbH
Bonner Talweg 100
53113 Bonn
Deutschland

T · · Systems ·

Let's power
higher performance

