



cgTunnel

cgTunnel sorgt für eine sichere, weltweite Verteilung von elektronischen Zertifikaten und vertraulichem Schlüsselmaterial von einem zentralen Server auf dezentrale Smartcards. Damit wird eine dezentrale, vollautomatische 24/7 Personalisierung von Smartcards, z.B. über Corporate Self-Service Portale, ermöglicht. Bei der Kommunikation und Übertragung werden alle Daten, unabhängig von der dezentralen Einsatzumgebung des Windows Clients, vom sicheren Backend (Server / Certificate Authority) direkt bis zur Smartcard Ende-zu-Ende verschlüsselt.



TECHNISCHE SPEZIFIKATION

Komponenten

- Server
- Client
- Agent

Kommunikation:

- APDU Netzwerk-Routing

Sicherheit:

- Ermöglicht Ende-zu-Ende-Verschlüsselung direkt zwischen dem sicheren Backend und der Smartcard über ein Netzwerk

Standards:

- PC/SC
- HTTPS (TLS/SSL)
- Java

Schnittstellen:

- PCSC Lite
- Java API

Skalierbarkeit:

- Multi-Session-fähig
(mehrere hundert gleichzeitigen Verbindungen)

Hochverfügbarkeit:

- Durch Load-Balancer*

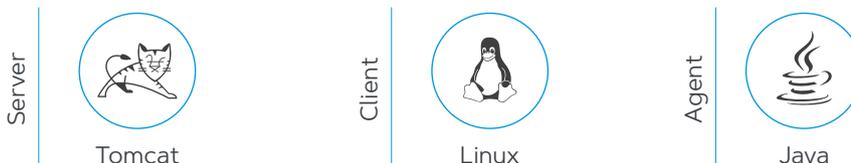
IHRE VORTEILE

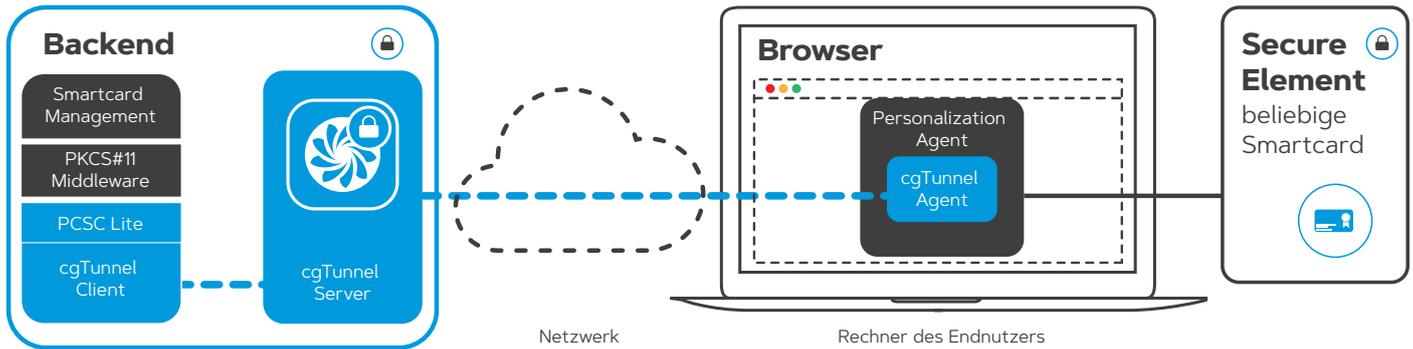
- ✓ Kostensenkung
- ✓ Verbesserte Flexibilität
- ✓ Beschleunigung von Prozessen im Smartcard-Lebenszyklus
- ✓ Compliant für maximale Sicherheitsansprüche
- ✓ Weltweite Verfügbarkeit 24/7

EINSATZMÖGLICHKEITEN

- Globale und sichere Zertifikatsverteilung
- Initialisierung und Personalisierung von Smartcards im User-Self-Service
- Ideal für verteilte oder multinationale Organisation
- Für alle Arten von Zertifikaten geeignet

UNTERSTÜTZTE PLATTFORMEN





cgTunnel Client (Backend)

Über den cgTunnel Client wird ein PCSC Lite Standardinterface für eine Smartcard Middleware wie PKCS#11 im Backend bereitgestellt. Er verbindet sich mit dem cgTunnel Server und stellt alle dort angemeldeten cgTunnel Agents als virtuelle Smartcard Leser im Backend zur Verfügung.

cgTunnel Server

Der cgTunnel Server sorgt als zentrale Komponente für das Routing der Smartcard Nachrichten, sogenannten Application Protocol Data Units (APDU), zwischen den virtuellen Smartcard Lesern im Backend und den cgTunnel Agents auf dem Rechner der Endnutzer über ein Netzwerk in beide Richtungen.

cgTunnel Agent

Der cgTunnel Agent auf dem Rechner des Endnutzers erhält nach Verbindung mit dem cgTunnel Server die APDU Kommandos von der backendseitigen PKCS#11 Middleware, reichen sie an einen lokal über einen Kartenleser angeschlossene Smartcard weiter und senden die APDU Antworten wieder zurück an den cgTunnel Server.

Secure Element (Smartcard)

Die lokal am Rechner des Endnutzers über einen Kartenleser angeschlossene persönliche Smartcard wird mit cgTunnel über ein Netzwerk als virtueller Smartcard Leser im Backend zur Verfügung gestellt. Als Kartenleser können herkömmliche Kartenleser mit Kabel oder moderne drahtlose Kartenleser eingesetzt werden.

PATENTIERTE TECHNOLOGIE

Die international zum Patent angemeldete cgTunnel Technologie (Patent Application: US-15/287,942) stellt die sichere, dezentrale Personalisierung von Smartcards und Übertragung von vertraulichem Schlüsselmaterial, unabhängig von der lokalen Clientumgebung, sicher. Durch die flexible Client-Server Architektur ist cgTunnel individuell in bestehende Public Key Infrastrukturen zu integrieren.

ANFORDERUNGEN

- **SERVER**
Apache Tomcat Server Version 7.0.47 oder höher mit SSL/TLS Zertifikat (auf Windows oder Linux); Apache Portable Runtime (APR) empfohlen für produktive Umgebungen
- **CLIENT**
Red Hat Enterprise Linux 6.4 oder höher
- **AGENT**
Java 6 oder höher

cgTunnel PASST PERFEKT ZU:



ONEKEY ID



AirID



cgCard

AUSLIEFERUNG

Server: WAR / JAR Dateien
Client: RPM Package
Agent: Java Bibliothek mit API und Samplecode



certgate GmbH
Merianstrasse 26
90409 Nürnberg
Germany

Phone: + 49 (0) 911 93 523-0
E-Mail: info@certgate.com
Web: www.certgate.com

© 2018 certgate. Alle Rechte vorbehalten. Das Vervielfältigen ist nur nach vorheriger Genehmigung durch certgate gestattet. Alle Rechte der dargestellten Marken liegen bei dem jeweiligen Markeninhaber. Fehler, Änderungen und Verfügbarkeit der dargestellten Produkte, Services, Eigenschaften und möglichen Anwendungen sind vorbehalten. Produkte und Services werden von certgate ausgeliefert. certgate übernimmt keine Haftung für Informationen von Dritten, welche Eigenschaften, Services und Verfügbarkeit betreffen. certgate macht von dem Recht Gebrauch, Änderungen zu Produkten und Services im Rahmen der Produktentwicklung zu machen, ohne dies vorher anzukündigen. Keine der angegebenen Informationen und Entscheidungen sind rechtlich bindend oder als solche zu interpretieren. Im Falle einer Abweichung zu Verträgen oder den allgemeinen Geschäftsbedingungen von certgate oder deren Partnern oder Zulieferern, welche mit certgate in Verbindung stehen, gelten immer die jeweiligen Verträge oder allgemeinen Geschäftsbedingungen.
*) Durch Drittanbieter-Lösung