



## cgTunnel

cgTunnel ensures the worldwide secure deployment of electronic certificates and sensible cryptographic keys from a central server to decentral smartcards. This enables a decentralized fully automated smartcard personalization 24/7, e. g. via corporate self-service portals. The communication and data transfer, regardless of the decentralized Windows clients environment, are end-to-end encrypted from the secure backend (server / certificate authority) directly to the smart card.



## TECHNICAL SPECIFICATION

### Components:

- Server
- Client
- Agent

### Communication:

- APDU Network routing

### Security:

- Enables end-to-end-encryption directly between the secure backend and a smart card through a network

### Standards:

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

### Interfaces:

- PCSC Lite
- Java API

### Scalability:

- Multi-session capable (up to several hundred parallel connections)

### High availability:

- With Load-Balancer\*

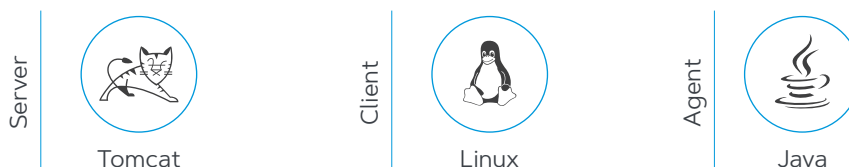
## BENEFITS

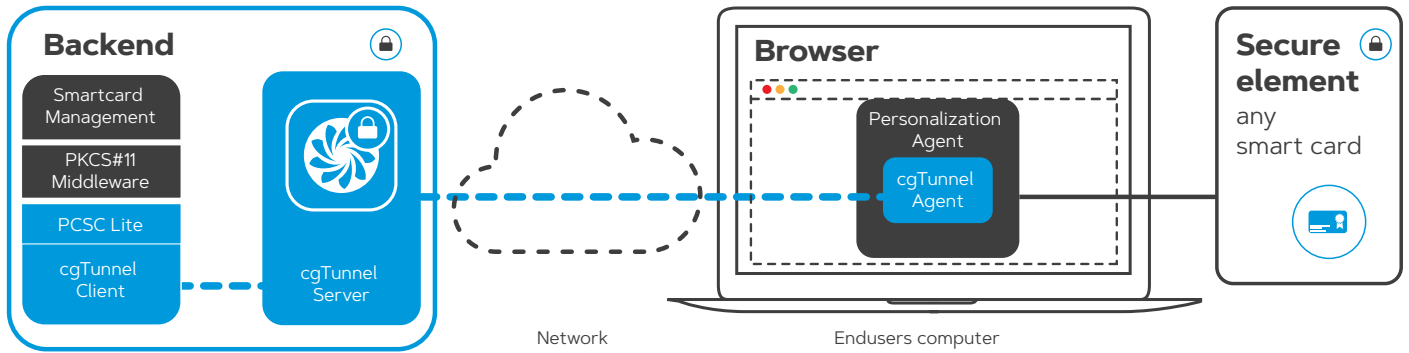
- ✓ Cost savings
- ✓ Improved service flexibility
- ✓ Faster processes throughout the smartcard lifecycle
- ✓ Compliant for the highest security requirements
- ✓ Worldwide availability 24/7

## USE CASE EXAMPLES

- Global and secure certificate deployment
- Initialization and personalization of smart cards with user self-service
- Ideal for decentralized or multinational organizations
- Compatible with all kinds of electronic certificates

## SUPPORTED PLATFORMS





**cgTunnel Client (Backend)**

The cgTunnel Client provides a PCSC Lite standard interface for smart card middleware such as PKCS#11 in the backend. It communicates with the cgTunnel Server and lists all cgTunnel Agents, which are connected to the cgTunnel Server, as virtual smartcard readers in the backend.

**cgTunnel Server**

The cgTunnel Server as the central component is routing smartcard messages, so called Application Protocol Data Units (APDU), between the virtual smartcard readers in the backend and the cgTunnel Agents on the end user workstation via a network in both directions.

**cgTunnel Agent**

The cgTunnel Agent on the end user's workstation connects to the cgTunnel server and receives the APDU commands from the backend PKCS#11 middleware, handing them to a locally connected smartcard reader and sends the APDU responses back to the cgTunnel Server.

**Secure element (smart card)**

The physical smartcard reader locally connected to the end user workstation is passed through a network by cgTunnel as a virtual smartcard reader in the backend. The physical smartcard reader can either be connected by cable or wireless for modern card readers.

**PATENTED TECHNOLOGY**

The international patent pending cgTunnel technology (patent application: : US-15/287,942) enables secure decentralized smartcard personalization and sensible private key transfers, regardless of the client workstations location and environment. With its flexible client server architecture cgTunnel can be individual integrated into existing public key infrastructures.

**REQUIREMENTS**

- **SERVER**  
Apache Tomcat server version 7.0.47 or higher with SSL/TLS certificate (on Windows or Linux); Apache Portable Runtime (APR) recommended for productive environments
- **CLIENT**  
Red Hat Enterprise Linux 6.4 or higher
- **AGENT**  
Java 6 or higher

**cgTunnel  
FITS PERFECTLY TO:**



ONEKEY ID



AirID



cgCard

**DELIVERY**

Server: WAR / JAR files  
Client: RPM Package  
Agent: Java library with API and sample code



certgate GmbH  
Merianstrasse 26  
90409 Nürnberg  
Germany

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

© 2017 certgate. All rights reserved. Reproduction only permitted with the approval of certgate. All brands listed are the brands of the respective owners. Errors, changes, and availability of the listed products, services, characteristics, and possible applications reserved. Products and services will be provided by certgate. certgate makes no guarantee for the information of third parties regarding characteristics, services and availability. certgate reserves the right to make changes to products and services as a result of product development, even without prior notification. None of the statements and depictions represents legal advice or may be interpreted in such a manner. In case of deviations from the contract documents and general terms and conditions of certgate and their affiliated companies and subsidiaries in conjunction with this document, the contract documents and general terms and conditions always have precedent over this document. \*) With 3rd party solution provider