Excellence in Digital Security.

genua.

# genucard

Personal Security Device

Technical Information

# Table of Contents

# 1. genucard: Personal Security Device

The information in this brochure is intended for IT-security professionals who are responsible for securing external and mobile IT infrastructure. It provides you with a compact overview of how, with the help of the Personal Security Device genucard, you can give both on-site and off-site employees access to company networks without endangering the IT security of the network. genucard provides you with the key advantages listed in the following table.

| **Advantages of genucard** | |
|---|---|
| Data processing and transfers compatible with classification levels German VS-NfD, NATO RESTRICTED, RESTREINT UE/EU RESTRICTED, and OCCAR RESTRICTED | ✓ |
| High security, plug & play with every laptop and PC | ✓ |
| Compact easy-to-use device | ✓ |
| Entire infrastructure can be centrally administrated | ✓ |

## 1.1. The Challenge

In a digitized world, the number of employees who need to access company data when on the road or in their home office is increasing. Communications are flexibly established via WiFi and cell/mobile phone networks. If we believe the predictions, in the future, more and more offices will be empty and our collaboration will increasingly take place via e-mail, groupware, and online conferences.

Technical progress makes this decentralized and mobile mode of work possible. But this development also creates challenges: How can flexibility and usability be combined with IT security? Organizations have to ensure that, for example, third parties do not read or manipulate confidential information or infiltrate their company network.

It is thus no longer sufficient to protect the local area network (LAN) with a firewall. External clients also have to be securely protected and data transfers have to be encrypted. If sensitive information leaks, the company runs the risk of financial damages, loss of customer trust, and penalties for neglecting statutory provisions.

## 1.2. Security Software Solutions

In many cases, organizations address this problem by using comprehensive security packages. These are installed on a client and filter incoming and outgoing data traffic. But these solutions do not offer reliable security: On the one hand, they allow the rules for use to be circumvented; on the other hand, on a compromised operating system, a comprehensive security package is no longer able to function properly. Other aspects of “all-around protection” – like, for example, secure data communications – are ignored in these solutions.

### 1.3. Requirements for a Security Package for External Clients

A security solution for clients that allows an organization's network to be externally accessed should fulfill the following requirements:

- The security solution is not an integral part of the computer to be protected. It possesses its own hardened operating system and its own functionality is not impaired by computer malfunctions.
- The security solution is immediately ready-to-go and easy to use.
- Users can unambiguously verify their identities.
- A firewall only allows communications with reliable connections.
- VPN technology ensures encrypted data exchange over public networks.
- Intelligent bandwidth management allows for prioritized uses.
- The company's IT security policy can continuously be centrally administered and enforced vis-à-vis all external clients.
- As an investment with a secure future, the security solution supports the IPv6 standard.

## 2. The Solution: genucard

genua developed the Personal Security Device genucard on the basis of this catalog of requirements. It fulfills all the listed requirements and also offers additional advantages.

### 2.1. An Autarchic Personal Security Device

genucard offers you a physical separation between personal security device and computer: The security applications are not installed on the client that they are supposed to protect, but rather on an autarchic device. genucard remains completely effective, even is the computer to be protected has already been compromised due to careless behavior. As a result, a strong security response is guaranteed for your IT at precisely the decisive moment: in an emergency.

Moreover, an important characteristic of genucard is that all security applications – such as packet filter, encryption functions, and authentication methods – are harmonized with one another. Conflicts to which the use of security software from different manufacturers can give rise are thus avoided.


genucard – the Personal Security Device by genua

Another plus: genucard is an independent computer with its own interfaces. Thanks to the concept of an autarchic system with its own processor and memory, none of the resources of the protected client are used, whereas security software can cause reduced performance.

### 2.2. Easy to Use

As soon as genucard is connected to a computer via USB, it protects the latter from dangers emanating from the internet. The display informs the user of the state of the system and the connection status.

#### 2.2.1. Compatibility

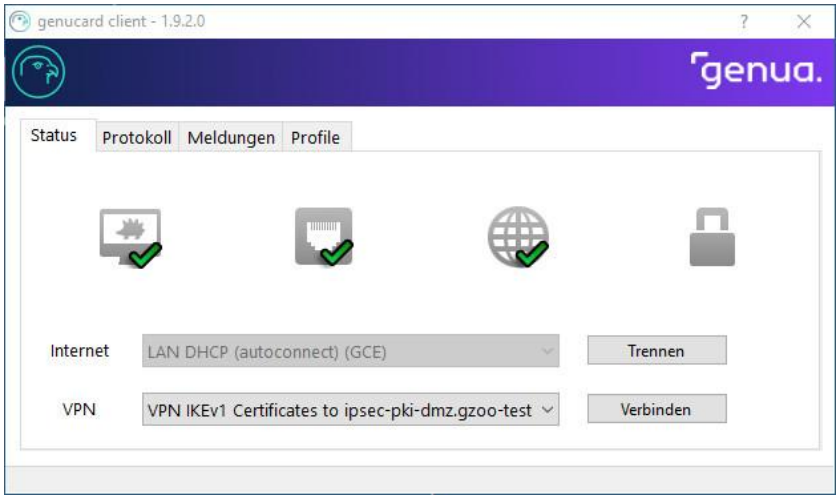
genucard supports the Windows 7, 8, and 10 operating systems, as well as Linux (starting with kernel 2.6).

#### 2.2.2. Windows App

In order to facilitate the use of genucard with Windows, a native Windows application is available. This can be found in the so-called tray (notifications field) and offers the following functions/displays:

- System: Uptime, software version, hardware version
- Internet: Status, joining and separating internet profiles

- VPN: Status, joining and separating VPN profiles
- Host: User, software version, screensaver/sleep-status




Windows app for direct access to important genucard functions

### 2.2.3. User Information

At the Central Management Station genucenter (see chapter 2.6), notifications can be left that are shown to the genucard user. The display takes place both in the Web GUI and by way of the Tray App in a Windows environment. Thus, for example, users can be informed about planned maintenance.

## 2.3. Authentication

### 2.3.1. Smart Card

For purposes of authentication, identity and access rights are verified: Users attach genucard with a smart card to the computer and enter a PIN (Personal Identification Number). A connection in the company network can only be established, if both security features are satisfied.

### 2.3.2. Key Server

Starting with a number of around 1,000 units of genucard and depending on user behavior, we recommend the use of a central key server, along with the central Firewall & VPN Appliance genuscreen, instead of smart cards, in order to avoid user waiting times. The key server assumes the function of the smart card, but is orders of magnitude faster. Using the key server, high-performance VPN infrastructures with a four-figure number of external locations can be created.

### 2.4. Stateful Packet Filter for Firewall Functions

The genucard's integrated firewall is based on the stateful packet filter of the Firewall & VPN Appliance genuscreen that has been certified in accordance with CC EAL 4+ by the German Federal Office for Information Security (BSI).

### 2.5. Secure VPN Data Communications

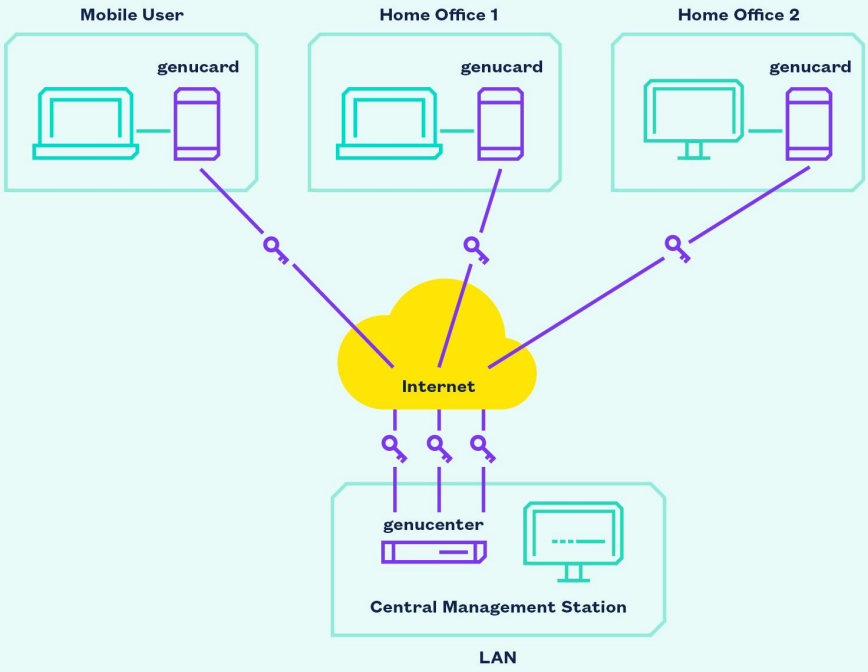
The VPN component of the genucard functions is a layer-3-based IPsec gateway. VPN connections can be established with it, for the purpose of secure data transfer by way of the internet. Only strong encryption algorithms and large key lengths are used.

### 2.6. Convenient Administration

genucard allows for different types of administration:

Users can themselves choose basic genucard settings – like, for example, the configuration of a WiFi connection – on their own computers via a local GUI.

The configuration, administration, and monitoring of multiple genucards is conveniently handled by the Central Management Station genucenter. Changes, updates, and patches can be simultaneously implemented on as many devices as one wants via practical grouping functions.




Central management with genucenter

Using genucenter, it is also possible consistently to enforce security guidelines concerning firewall and VPN dial-in for all clients being used externally. In growing

installations, the additional devices can be easily integrated into the Central Management Station and come equipped with time-tested configurations.

### 2.7. IPv6 Integration for a Future Prove Investment

Given the limitations of IPv4, the rapid growth of the internet leads to bottlenecks, which are supposed to be eliminated by IPv6. Along with the expansion of address capacities, the opportunity is being used to adapt the internet protocol to modern requirements.

The conversion of the internet to IPv6 is already underway and will accelerate in coming years. In the meanwhile, there are already areas that are only reachable using IPv6, other parts that are connected via both protocols, and large parts that are exclusively based on IPv4.

This has consequences for your IT infrastructure: For example, the filter rules for firewalls have to be rewritten for IPv6. A firewall that has not been designed for use with IPv6 will normally not let IPv6 data traffic through.

In light of this development, we are offering you a solution with genucard that can work reliably with both IPv4 and IPv6. You are making an investment in a product that meets both today's and tomorrow's standards.

## 3. Approval

The genucard IPsec VPN solution has the official approval of the German Federal Office for Information Security (BSI) for classification levels German VS-NfD, NATO RESTRICTED, RESTREINT UE/EU RESTRICTED as well as OCCAR RESTRICTED. Official public bodies, military units, and contracting companies with access to classified information therefore can safely use genucard to ensure that employees have secure access to classified data even when working remotely. According to the new directive for classified information (Verschlusssachenanweisung), the approval includes the firewall functions in addition to the VPN component.

## 4. Hardware

### 4.1. Case

genucard is distinguished by an attractive, slim case-design. Connection via USB ensures compatibility with practically all computers.

### 4.2. Connectivity

In order to enable highly secure data communications via all channels, genucard is equipped with the following interfaces:

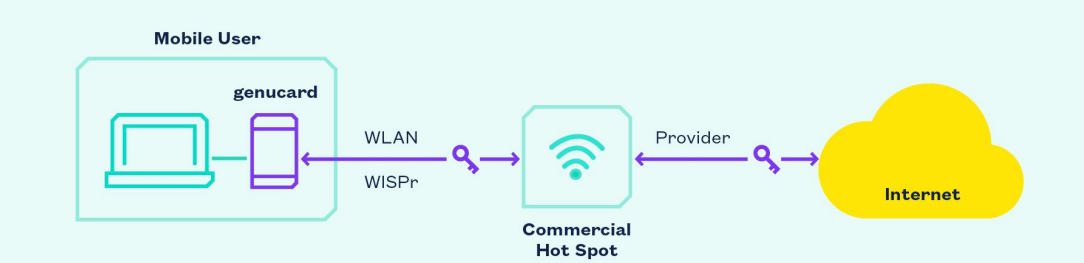
- WLAN Wi-Fi 5, dual-band
- LTE (including SIM card slot)
- USB (for extensions, e.g. Ethernet)
- Smart card

In every imaginable constellation, it thus offers flexible communication and connection possibilities.

## 5. Use Cases

### 5.1. Secure Internet Connection with genucard

This example shows the establishment of an encrypted internet connection with genucard at a commercial hotspot.



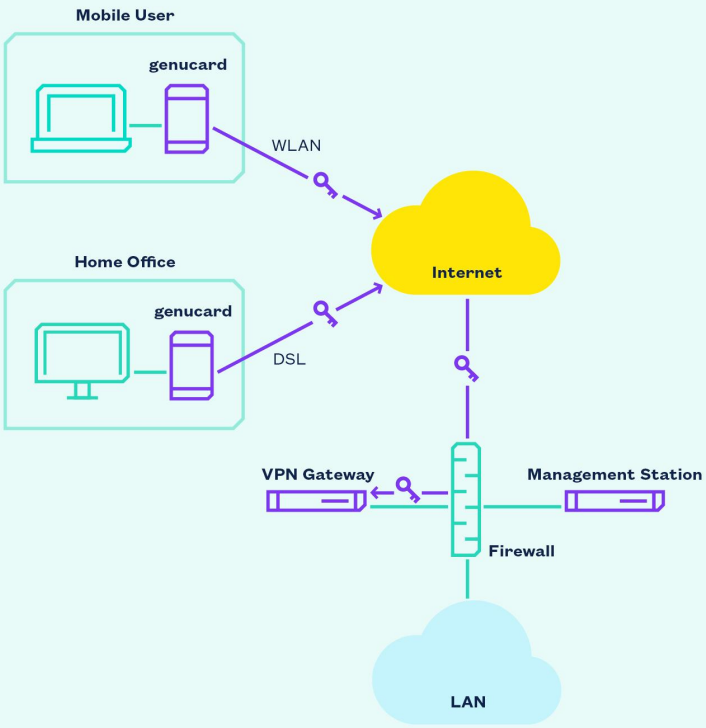

Secure internet connection with genucard

The user verifies his identity and configures a WiFi connection to a commercial hotspot by way of the local GUI. He verifies his identity with the provider using the WISPr protocol. The latter then establishes an internet connection. The genucard's integrated firewall protects the laptop from unauthorized external access.

### 5.2. Remote Access to Company Data via VPN

In the following example, employees who are outside the company network use publicly accessible transmission networks to access data in the protected company network (LAN).

Using genucard, encrypted connections – Virtual Private Networks (VPN) – are established with which public networks are securely bridged. In this way, reliably secured data can be conveniently exchanged via the internet.




Encrypted LAN-access with external devices

genucard is compatible with other genua IT security solutions:

- Firewall & VPN Appliance genuscreen
- VPN Appliance genucrypt

It can be integrated with these products in specific applications.

## 6. Support

### 6.1. Installation and Configuration Service

genua and its specialist sales partners will support you if you wish during the installation, configuration and commissioning of genucard and the Central Management Station genucenter. At the same time your administrators will be given thorough instructions in the use and maintenance of the system.

### 6.2. Ongoing Operation – Software Support

**Update service:** genucard is being constantly developed. New versions are regularly released that incorporate the latest developments and add practical functionality. Additional intermediate versions are released as required.

Our update service ensures automatic delivery of the most current versions, as well as access to our complete patch database.

**Hotline:** In addition to our update service, we provide German and English language support by phone and e-mail. You can use our hotline for all questions regarding your genucard solution. Telephone hotline support is available 24 hours every day on request.

**Security system management:** This service includes ongoing monitoring and maintenance of our solutions, which provide customers with IT security using highly encrypted internet connections.

### 6.3. Sales Partner Support

**Support services from our sales partners:** Many of genua's authorized sales partners offer extended support options such as on-site hardware replacement service within guaranteed maximum times.



genua GmbH

Domagkstrasse 7 | 85551 Kirchheim, Germany

T +49 89 991950-0 | F +49 89 991950-999 | E info@genua.eu | www.genua.eu