



Personal Security Device genucard

Facts & Features

Definition:

The genucard is an autonomous mobile security device for laptops or workstations at home offices. Based on its own processor, memory, and operating system, it features a firewall and VPN gateway, and creates encrypted connections for data transfer via Internet to a remote LAN. The genucard is connected to the laptop or computer via USB and works with Windows XP (from SP3), Windows 7, Linux (from Kernel 2.6), and OpenBSD.

Typical Use:

With genucard, mobile users or colleagues at home office can securely exchange data via VPN with the LAN, e.g. of a public authority or company.

Throughput Volume:

- Firewall: 100 MBit/s
- VPN: 12 MBit/s

Customer Service:

- Customer service directly from the manufacturer genua
- Hotline service / update service
- Comprehensive training courses



Reasons to Choose genucard:

- Autonomous computer with its own processor, memory, and hardened operating system
- Easy to use via USB
- Plug & play with every laptop or workstation
- Fully featured Windows App
- Flexible connection options via Ethernet (LAN/DSL), WLAN, UMTS or USB (e.g. Bluetooth)
- Communication is restricted to permitted connections
- Encrypted data exchange over public networks
- Authentication and key handling via smart card
- Approval for German, NATO and EU classification level "Restricted"
- Full IPv6 support
- Central management of numerous devices by IT department

Reasons to Choose genua:

- Leading German specialist for IT security
- Founded in 1992 – implementation of numerous major projects for industrial, government, and military organizations



Firewall

| | |
|---------------------------|---|
| Stateful packet filtering | State of the art firewall for manageable rulesets |
| Quality of service (QoS) | Guarantee service priorities |
| Queuing (traffic shaping) | Bandwidth management to control traffic volume |
| Filter criteria | Filtering decision can be based on IP address, network protocol, port, interface, flags and state |
| Filter action | Choice of packet handling: pass, block or drop |
| DDoS protection | Proxy for the TCP handshake to protect against TCP SYN floods often used by distributed denial-of-service attacks |
| Spoofing protection | Block forged packets |
| Packet normalisation | Reassemble fragmented packets, generate random IP identification, enforce IP header settings such as TTL and MSS |

Virtual Private Network

| | |
|-----------------------|--|
| General | |
| IPsec | Network layer VPN |
| NAT-Traversal (NAT-T) | Supports connections between NATed devices |
| Authentication | |
| RSA | De facto public-key standard for easy key exchange |
| Smart card | For secure key storage (optional) |
| Algorithms | |
| Encryption | AES-128, AES-192, AES-256, 3DES, (Blowfish, CAST) |
| Hashes | SHA2, SHA1, MD5 |

Networking

| | |
|-------------|---|
| General | |
| NTP client | Obtain time from NTP servers |
| DHCP server | Automatically assign IP address to client |
| Uplinks | |
| Ethernet | 10/100 Mbit/s Base-T |
| WLAN | 802.11b/g (optional) |
| UMTS/GPRS | Integrated UMTS modem (optional) |
| PPPoE | For DSL |
| Bluetooth | For cell phone or satellite uplink (optional) |
| Satellite | Performance boost for satellite uplinks |
| Proxies | |
| SIP | Leading signaling protocol for Voice over IP |
| FTP | Support for File Transfer Protocol |
| DNS | Local DNS resolver |



Monitoring

| | |
|--------|---------------------------------|
| System | System status (memory, load) |
| VPN | Supervise VPN connection status |

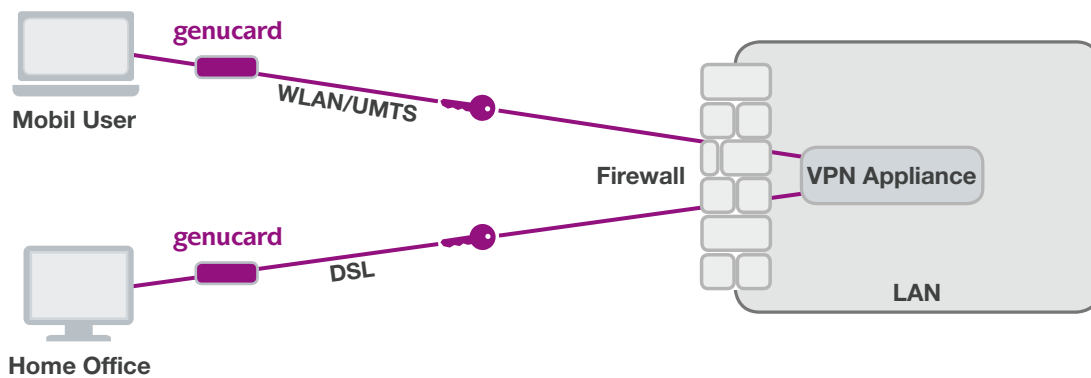
Central Management with genucenter

| | |
|---------------------------|--|
| General | |
| Configuration | Easy management of several (thousand) systems |
| Monitoring | See the health of your systems at a glance |
| Logging | Easily collect and analyse logs |
| Software (patches/update) | Distribute the latest software revision |
| Rollout management | Freely define when to update/upgrade which system |
| Web GUI | Powerful web-based user interface secured with TLS/SSL (HTTPS) |
| Online help | Instant help in the user interface |
| Patch Management | |
| GUI | Get and install patches via GUI |
| Automatic updates | Automate the process of fetching updates for the appliance |
| Patch rollback | Return to previous patch level |
| Logging | |
| Syslog | Use a third party syslog server to store logs |
| Local cache | For short term logs |
| Central | Use genucenter to concentrate the logs on one system |
| Debugging | |
| Network | Powerful commandline tools: tcpdump, traceroute, ping etc. |
| Firewall | Monitor firewall state, rules and logs |
| VPN | VPN connection status overview and problem analysis |



Application Example

Field staff need to access data in the protected LAN via the Internet. Therefore laptops of mobile users as well as the workstations at home offices are outfitted with genucards. Employees receive a smart card and PIN for authentication. For authorized connections, the genucard creates a strongly encrypted Virtual Private Network (VPN) using DSL, UMTS, LAN or WLAN as transfer technologies.



Further information:
www.genua.eu/genucard