

Personal Security Device genucard

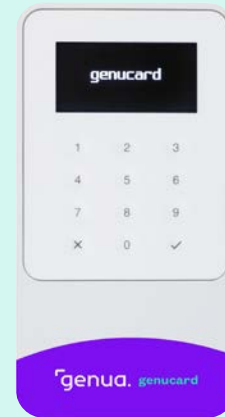
High-security connection to restricted networks



Mobile Work

Flexible portfolio for working remotely

genua.



Personal Security Device for Employees on the Go

Traveling employees, at branch locations or who are working from home need to access the internal networks of their company or their organization via the Internet to access confidential information or use software applications online. With multiple protective components, the Personal Security Device genucard effectively secures this access against cyber attacks:

- A strongly encrypted virtual private network (VPN) ensures smooth data communication of all devices via WLAN, mobile telephony or Ethernet.
- The integrated firewall provides connection monitoring within and outside of the VPN.
- Authentication occurs by means of key handling using a smart card and PIN pad – without this process, no connection to the employer's network is possible.

Interested? Contact us:
sales@genua.de or +49 89 991950-902

All Advantages at a Glance



Self-contained personal security device



Highly secure VPN for data communication



Plug & Play with laptop and PC



Integrated firewall for connection control



Authentication and key handling via PIN pad and smart card



Administration via central management station



Investment security through IPv6 integration



Approved for classification levels German VS-NfD, NATO RESTRICTED, RESTREINT UE/EU RESTRICTED

» The number of new, aggressive hacker attacks on mobile IT users is growing rapidly. Use genucard to protect your company data from unauthorized access.

SecurITy
made
in
Germany

A Self-Contained Device that Guarantees Security

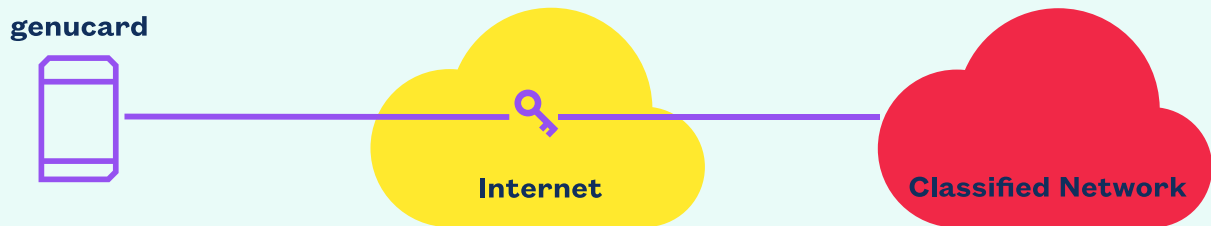
genucard reliably protects your data communication through the combination of multiple security features. Another significant advantage: The security solution is not installed on the computer that it is supposed to protect but rather on an autonomous device with its own operating system. It thereby remains fully effective even if the computer should already be compromised.

The Central Management Station genucenter enables the simple configuration and administration of genucard for all employees from a central control center. This guarantees strong security for your IT – in the event of an emergency, when it really matters.

Approvals for the Restricted Data Sector

genucard has the official approval of the German Federal Office for Information Security (BSI) for classification level RESTRICTED. Whether as an employee of a government authority, of the German Armed Services or in a company with an obligation to maintain secrecy – with the Personal Security Device genucard, you can conveniently access restricted data while traveling, working from home or in branch offices.

According to the new directive for classified information VSA (Verschlusssachenanweisung), the approval includes the firewall in addition to the VPN component. Other approvals exist for NATO RESTRICTED, RESTREINT UE/EU RESTRICTED as well as OCCAR RESTRICTED.



Highly secure connection to a workplace authorized for use with restricted data

Reasons Why

- Experts for the IT security of companies and public organizations
- Offer of a comprehensive, modular IT security portfolio
- Quality without compromise for all products, services, and processes

genua – Excellence in Digital Security

genua develops innovative, reliable as well as market-shaping products and solutions. Whether in the public sector, for the operators of critical infrastructures, in industry or in the protection of classified information: we provide answers to the IT security challenges of today and of tomorrow.

Further information:
www.genua.eu/genucard

More product
information

