Excellence in Digital Security.

genua.

genucard

Personal Security Device

Technische Informationen

Inhalt

1. genucard: Personal Security Device

Diese Informationsbroschüre richtet sich an IT-Sicherheitsverantwortliche, die für die externe bzw. mobile IT-Infrastruktur und deren Absicherung zuständig sind. Sie bietet Ihnen einen kompakten Überblick, wie Sie mit Hilfe des Personal Security Device genucard Mitarbeitern innerhalb und außerhalb des Unternehmens Zugriff auf Firmennetze gewähren können, ohne dass die IT-Sicherheit im Unternehmensnetzwerk gefährdet wird. Dabei bietet Ihnen genucard wesentliche Vorteile.

Vorteile von genucard	
VS-NfD-konforme Datenverarbeitung und -transfers für mobile Anwender	✓
Hohe Sicherheit, Plug & Play mit jedem Laptop und PC	✓
Kompaktes, einfach zu bedienendes Gerät	✓
Vollständige Infrastruktur zentral administrierbar	✓

1.1. Herausforderung

In einer digitalisierten Arbeitswelt steigt der Anteil von Mitarbeitern, die von unterwegs oder im Homeoffice auf Geschäftsdaten zugreifen müssen. Die Verbindungen werden dabei flexibel über WLAN und Mobilfunk aufgebaut. Glaubt man Prognosen, so werden zukünftig immer mehr Büros regelmäßig leer stehen und unsere Zusammenarbeit zunehmend per E-Mail, Groupware und Online-Konferenzen stattfinden.

Der technische Fortschritt ermöglicht diese mobile und dezentralisierte Arbeitsweise. Doch diese Entwicklung bringt auch Herausforderungen mit sich: Wie lassen sich Flexibilität und Usability mit zuverlässiger IT-Sicherheit kombinieren? Organisationen müssen beispielsweise an allen Arbeitsplätzen ausschließen, dass Dritte vertrauliche Daten mitlesen, manipulieren oder das Firmennetz infiltrieren.

Es reicht also nicht mehr aus, das LAN mit einer Firewall abzuschotten. Auch die externen Clients müssen sicher abgeschirmt und Datentransfers zuverlässig verschlüsselt werden. Denn bei Abfluss sensibler Informationen drohen finanzielle Schäden, der Verlust von Kundenvertrauen sowie Strafen wegen Vernachlässigung gesetzlicher Bestimmungen.

1.2. Lösungsansätze

In vielen Fällen begegnen Organisationen diesem Problem mit Security-Komplettpaketen. Diese werden auf einem Client installiert und filtern den ein- und ausgehenden Datenverkehr. Doch diese Lösungen bieten keine zuverlässige Sicherheit: Einerseits lassen sich die Regeln der Anwendung umgehen, anderseits ist das Security-Komplettpaket auf einem kompromittierten Betriebssystem nicht mehr in der Lage, einwandfrei zu funktionieren. Weitere Aspekte eines „Rundum-Schutzes“,

wie z. B. eine sichere Datenkommunikation, bleiben bei diesen Lösungen häufig außen vor.

1.3. Anforderungen an ein Sicherheitspaket für externe Clients

Eine Sicherheitslösung für Clients, mit denen von außen auf das Netzwerk einer Organisation zugegriffen werden kann, sollte folgende Anforderungen erfüllen:

- Die Sicherheitslösung ist kein integraler Bestandteil des zu schützenden Rechners. Sie besitzt ein eigenes, gehärtetes Betriebssystem und ihre Funktionalität wird bei Störungen des Rechners nicht beeinträchtigt.
- Die Sicherheitslösung ist sofort startklar und einfach zu bedienen.
- Anwender können sich eindeutig authentisieren.
- Eine Firewall beschränkt die Kommunikation auf zulässige Verbindungen.
- Ein VPN gewährleistet einen verschlüsselten Datenaustausch über öffentliche Netze.
- Intelligentes Bandbreitenmanagement ermöglicht priorisierte Anwendungen.
- Die IT-Sicherheitsrichtlinie des Unternehmens kann fortlaufend gegenüber allen externen Clients zentral administriert und durchgesetzt werden.
- Als zukunftssichere Investition unterstützt die Sicherheitslösung den Standard IPv6.

2. Die Lösung: genucard

Anhand dieses Anforderungskatalogs hat genua das Personal Security Device genucard entwickelt. Es erfüllt alle aufgeführten Anforderungen und bietet darüber hinaus weitere Vorteile.

2.1. Autarkes, umfassendes Personal Security Device

genucard bietet Ihnen eine physikalische Trennung von Personal Security Device und Computer: Die Sicherheitsanwendungen sind nicht auf dem Client installiert, den sie schützen sollen, sondern auf einem autarken Device. genucard bleibt selbst dann voll wirksam, wenn der zu schützende Rechner durch unvorsichtigen Umgang bereits kompromittiert sein sollte. So ist Ihnen die starke Sicherheitsleistung für Ihre IT genau zum entscheidenden Zeitpunkt garantiert – im Ernstfall.

Ein wichtiges Merkmal von genucard ist zudem, dass alle Sicherheitsanwendungen wie Paketfilter, Verschlüsselungsfunktionen und Authentisierungsmethoden aufeinander abgestimmt sind. Konflikte, die der Einsatz von Sicherheits-Software verschiedener Hersteller verursachen kann, werden vermieden.

genucard – Personal Security Device von genua

Ein weiterer Pluspunkt: genucard ist ein eigenständiger Rechner mit eigenen Interfaces. Durch das Konzept eines autarken Systems mit eigenem Prozessor und Speicher werden keine Ressourcen des geschützten Clients beansprucht, während Sicherheitssoftware Leistungseinschränkungen verursachen kann.

2.2. Einfache Bedienung

Sobald genucard via USB an einen Rechner angeschlossen ist, schützt sie diesen vor Gefahren aus dem Internet. Das Display informiert den Anwender über Systemzustand und Verbindungsstatus.

2.2.1. Kompatibilität

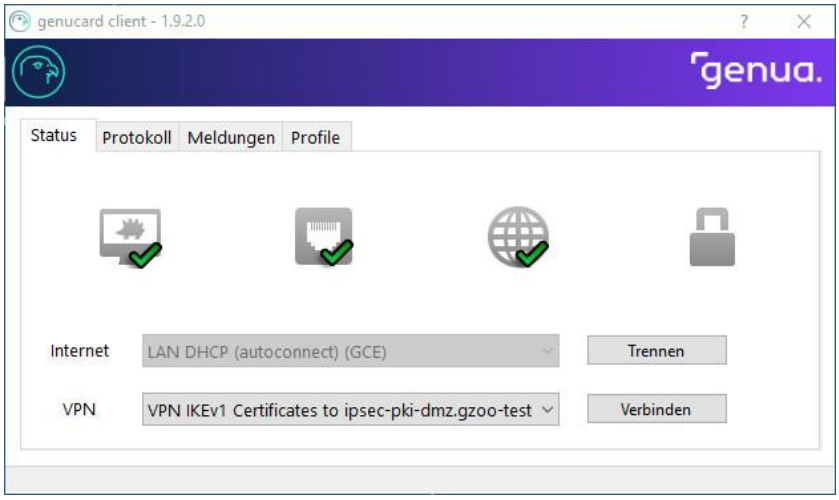
genucard unterstützt die Betriebssysteme Windows 7, 8 und 10 sowie Linux (ab Kernel 2.6).

2.2.2. Windows App

Um die Verwendung von genucard unter Windows zu erleichtern, ist eine native Windows-Applikation erhältlich. Diese ist im sog. Tray (Benachrichtigungsfeld) zu finden und bietet folgende Funktionen/Anzeigen:

- System: Uptime, Software-Version, Hardware-Version
- Internet: Status, Verbinden und Trennen von Internet-Profilen

- VPN: Status, Verbinden und Trennen von VPN-Profilen
- Host: Benutzer, Software-Version, Screensaver/Sleep-Status



Windows App für direkten Zugriff auf wichtige Funktionen von genucard

2.2.3. Anwenderinformation

Auf der Central Management Station genucenter (siehe Kapitel 2.6) lassen sich Meldungen hinterlegen, die dem Anwender von genucard angezeigt werden. Dabei erfolgt die Anzeige sowohl im Web-GUI als auch mittels Tray App unter Windows. So kann z. B. über geplante Wartungen informiert werden.

2.3. Authentisierung

2.3.1. Smartcard

Zur Authentisierung werden Identität und Zugriffsberechtigung überprüft: Anwender stecken genucard mit Smartcard an den Rechner und geben eine PIN (Personal Identification Number) ein. Nur wenn beide Sicherheitsmerkmale erfüllt sind, kann eine Verbindung ins Firmennetz aufgebaut werden.

2.3.2. Keyserver

Ab einer Stückzahl von etwa 1.000 Einheiten von genucard und je nach Nutzerverhalten empfehlen wir den Einsatz eines zentralen Keyservers zusätzlich zur zentralen Firewall & VPN-Appliance genuscreen anstatt von Smartcards, um Wartezeiten der Anwender zu vermeiden. Der Keyserver übernimmt die Funktionalität der Smartcards, ist jedoch um Größenordnungen schneller. Damit können VPN-Infrastrukturen mit einer vierstelligen Anzahl von Außenstellen äußerst performant realisiert werden.

2.4. Stateful Packet Filter für Firewall-Funktionen

Die in genucard integrierte Firewall basiert auf dem vom Bundesamt für Sicherheit in der Informationstechnik nach CC EAL 4+ zertifiziertem Stateful Packet Filter der Firewall & VPN-Appliance genuscreen.

2.5. Sichere VPN-Datenkommunikation

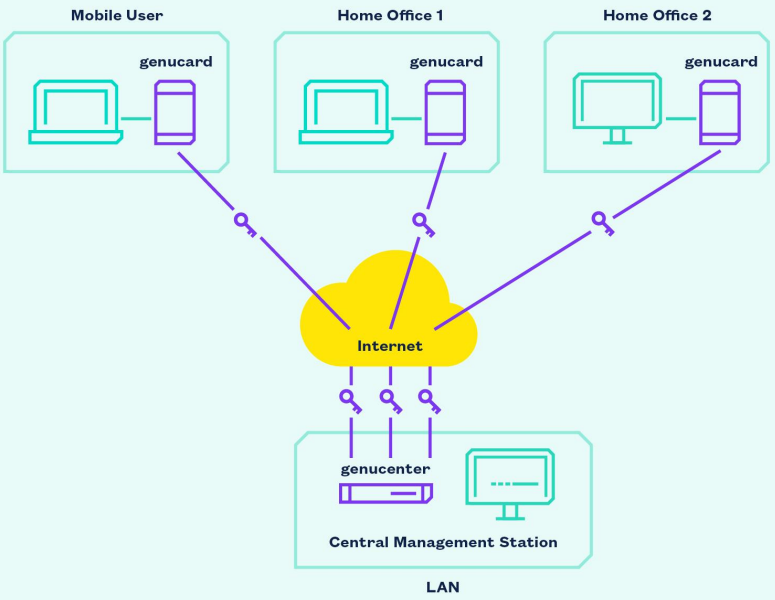
Die VPN-Komponente von genucard fungiert als Layer 3-basiertes IPsec-Gateway. Damit können zur sicheren Datenübertragung über das Internet VPN-Verbindungen aufgebaut werden. Es kommen ausschließlich starke Verschlüsselungsalgorithmen und große Schlüssellängen zum Einsatz.

2.6. Komfortable Administration

genucard bietet verschiedene Möglichkeiten der Administration:

Der Benutzer hat die Möglichkeit, elementare Einstellungen, wie z. B. die Konfiguration einer WLAN-Verbindung, selbstständig am jeweiligen Rechner über ein lokales GUI vorzunehmen.

Die Konfiguration, Administration und Überwachung mehrerer Devices erfolgt komfortabel mit der Central Management Station genucenter. Änderungen, Updates und Patches können über praktische Gruppierungsfunktionen gleichzeitig auf beliebig viele Devices übertragen werden.



Zentrales Management mit genucenter

Mit genucenter ist auch die konsequente Durchsetzung von Sicherheitsrichtlinien bezüglich Firewall und VPN-Einwahl bei allen Clients möglich, die sich im externen Einsatz befinden. In wachsenden Installationen können die zusätzlichen Devices

ganz einfach in die Central Management Station integriert und mit bewährten Konfigurationen ausgestattet werden.

2.7. Investitionssicherheit durch IPv6-Integration

Das rapide Wachstum des Internets führt zusammen mit den Beschränkungen von IPv4 zu Engpässen, die durch IPv6 beseitigt werden sollen. Mit der Erweiterung der Adresskapazitäten wurde auch die Chance genutzt, das Internet Protocol an moderne Erfordernisse anzupassen.

Die Umstellung des Internets auf IPv6 läuft bereits und wird sich in den kommenden Jahren beschleunigen. Inzwischen gibt es bereits Bereiche, die nur mittels IPv6 erreichbar sind, andere Teile, die über beide Protokolle angebunden sind, und große Teile, die ausschließlich auf IPv4 basieren.

Dies hat Konsequenzen für Ihre IT-Infrastruktur: So müssen z. B. für IPv6 die Filterregeln für Firewalls neu erstellt werden. Eine Firewall, die nicht für den Umgang mit IPv6 ausgelegt ist, wird in der Regel IPv6-Datenverkehr nicht durchlassen.

Mit Blick auf diese Entwicklung bieten wir mit genucard eine Lösung, die sicher mit IPv4 und IPv6 umgehen kann – Sie tätigen eine Investition in ein Produkt, das sowohl heutigen als auch zukünftigen Standards entspricht.

3. Zulassung

genucard ist zugelassen für VS-NfD (Verschlusssache – Nur für den Dienstgebrauch), NATO RESTRICTED, RESTREINT UE/EU RESTRICTED sowie OCCAR RESTRICTED beim Bundesamt für Sicherheit in der Informationstechnik (BSI). Behörden, die Bundeswehr und Firmen im Geheimschutzbereich können das Personal Security Device also einsetzen, um Mitarbeitern im Home Office, im Einsatz an Außenstandorten oder auch auf Reisen komfortablen Zugriff auf eingestufte Daten zu gewähren. Die Zulassung umfasst gemäß der neuen Verschlusssachenanweisung (VSA) neben den VPN- auch die Firewall-Funktionen.

4. Hardware

4.1. Gehäuse

genucard zeichnet sich durch ein attraktives, schlankes Gehäusedesign aus. Dabei gewährleistet der Anschluss via USB die Kompatibilität zu praktisch allen Rechnern.

4.2. Konnektivität

Um die hochsichere Datenkommunikation über alle Wege zu ermöglichen, ist genucard mit diesen Schnittstellen ausgestattet:

- WLAN Wi-Fi 5, Dualband
- LTE (inkl. SIM-Karten-Slot)
- USB (für Erweiterungen, z. B. Ethernet)
- Smartcard

Damit bietet sie in jeder denkbaren Konstellation flexible Kommunikations- und Anschlussmöglichkeiten.

5. Einsatzszenarien

5.1. Sichere Internetverbindung mit genucard

Das Beispiel zeigt den Aufbau einer verschlüsselten Verbindung zum Internet mit genucard an einem kommerziellen Hot Spot.

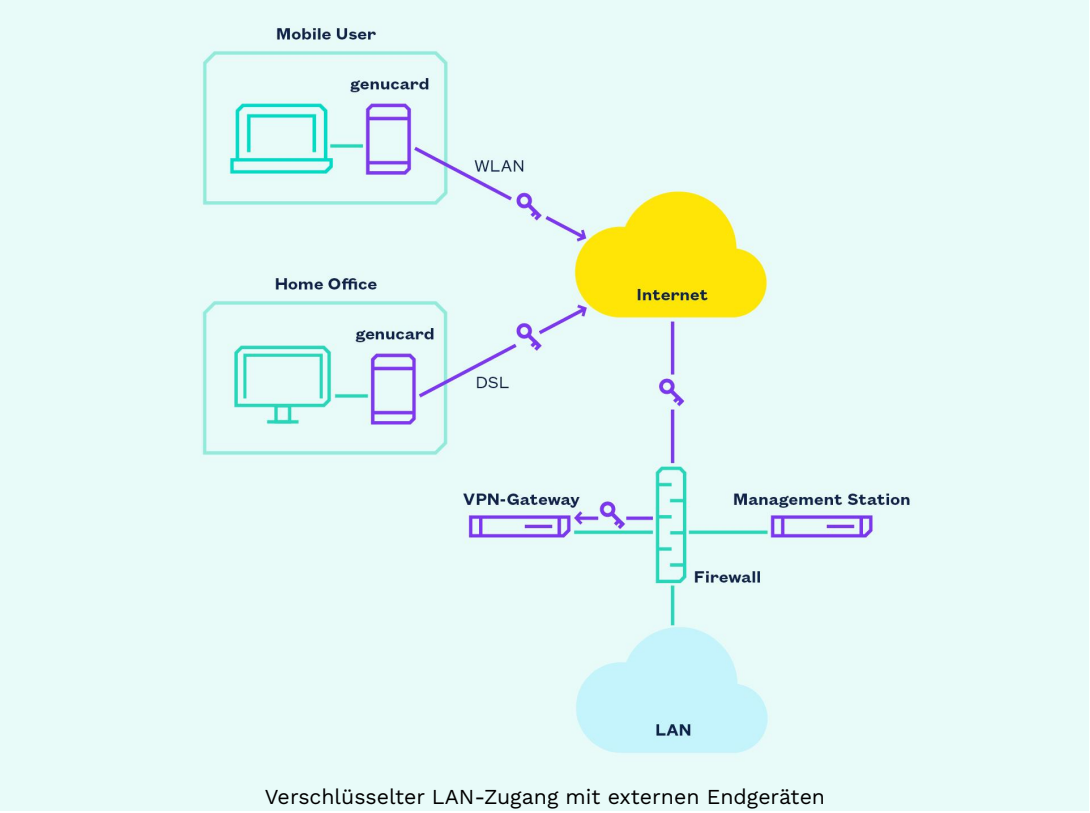
Sichere Internetverbindung mit genucard

Der Anwender authentisiert sich und konfiguriert über das lokale GUI eine WLAN-Verbindung zu einem kommerziellen Hot Spot. Beim Provider authentifiziert er sich über das WISPr-Protokoll. Dieser stellt daraufhin eine Verbindung zum Internet her. Die integrierte Firewall von genucard schützt dabei den Laptop vor unerlaubten Zugriffen von außen.

5.2. Remote-Zugriff auf Unternehmensdaten via VPN

Im Folgenden greifen Mitarbeiter, die sich außerhalb des Firmennetzes befinden, über öffentlich zugängliche Übertragungsnetze auf Daten zu, die sich innerhalb des geschützten Firmennetzes (LAN) befinden.

Dazu werden sowohl die Home Office-Rechner als auch die Laptops mobiler User mit genucards ausgestattet. Zur Authentifizierung erhalten die Mitarbeiter eine Smartcard und eine PIN. Als Übertragungsverfahren kommen DSL, LTE und WLAN zum Einsatz.



Verschlüsselter LAN-Zugang mit externen Endgeräten

Durch genucard werden verschlüsselte Verbindungen – Virtual Private Networks (VPN) – aufgebaut, mit denen der öffentliche Bereich sicher überbrückt wird. Auf diese Weise können Daten komfortabel und zuverlässig abgeschirmt via Internet ausgetauscht werden.

genucard ist kompatibel zu weiteren IT-Sicherheitslösungen von genua:

- Firewall & VPN-Appliance genuscreen
- VPN-Appliance genucrypt

Das Device lässt sich zusammen mit diesen Produkten in spezifische Anwendungen einbinden.

6. Support

6.1. Installations- und Konfigurationsservice

genua und spezialisierte Vertriebspartner unterstützen Sie auf Wunsch bei der Installation, Konfiguration und Inbetriebnahme von genucard und der Management Station genucenter. Dabei werden die Administratoren ausführlich in die Benutzung und Pflege des Systems eingewiesen.

6.2. Laufender Betrieb – Software Support

Update Service: genucard wird ständig weiterentwickelt. Regelmäßig erscheinen neue Versionen, in denen aktuelle Entwicklungen aufgegriffen werden und der Funktionsumfang sinnvoll ergänzt wird. Je nach Bedarf erscheinen zusätzlich Zwischenversionen.

Unser Update-Service sichert Ihnen die automatische Lieferung der neuesten Versionen und Zugriff auf unsere komplette Patch-Datenbank.

Hotline: Zusätzlich zu unserem Update Service bieten wir deutsch- und englischsprachigen Support via Telefon und E-Mail. Sie können unsere Hotline für alle Fragen zu Ihrer Lösung mit genucard nutzen. Der telefonische Hotline Support steht Ihnen auf Wunsch 24 Stunden an allen Tagen zur Verfügung.

Security System Management: Diese Leistung umfasst die ständige Überwachung und Wartung unserer Lösungen, die bei Kunden für IT-Sicherheit sorgen, über stark verschlüsselte Internet-Verbindungen.

6.3. Support von Vertriebspartnern

Support-Leistungen von Vertriebspartnern: Viele autorisierte Vertriebspartner von genua bieten zum Teil erweiterte Support-Optionen an, z. B. Vor-Ort-Austauschservice von Hardware innerhalb garantierter Maximalzeiten.

GC-WP-0921-3-D

genua GmbH

Domagkstraße 7 | 85551 Kirchheim bei München

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