genusecure Suite

Mobile Work

Facts and Features

Definition

genusecure Suite safeguards connections, applications, and data of mobile devices running Windows 11. It is designed for any organization that requires the classification levels German VS-NfD, NATO RESTRICTED, and RESTREINT UE/EU RESTRICTED. The security solution comprises a VPN software client, a hard drive encryption as well as a smart card middleware and meets all requirements of the German Federal Office for Information Security (BSI) for secure teleworking while providing the performance of advanced IT tools for effortless collaboration.

Components of genusecure Suite[1]

- VPN Software Client genuconnect
- Full-Drive Encryption Utimaco DiskEncrypt
- Smart Card Middleware Nexus Personal Desktop Client

Typical Use

- VS-NfD-compliant processing of classified information in government agencies or in industries with an obligation to maintain secrecy
- Enabling secure, scalable, and flexible workplaces in home offices or at multiple locations[2]
- Highly secure mobile working with laptops and tablets running Microsoft Windows

Reasons to choose genusecure Suite

- All-in-one security for organizations with German VS-NfD requirements
- Approved by the BSI: The VPN software client and the full-drive encryption meet the highest security requirements and are approved by the BSI
- Simple and convenient: Users work via the familiar Windows interface without any additional layers
- Seamless integration into public key infrastructures (PKI) through a fully PKI-compatible platform

Service

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

SecurITy made in Germany

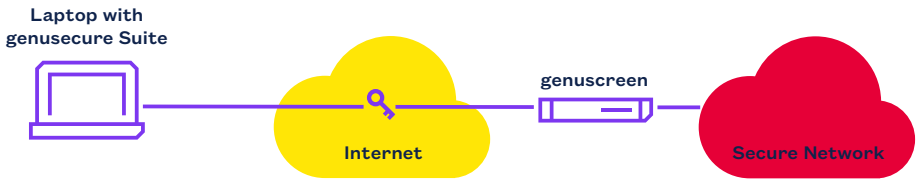
[1] Customers receive one-stop service and support directly from the provider genua GmbH.

[2] Project-specific assurance of hardware support

System Requirements	
Hardware	Processor: Intel: at least Intel 3rd generation core (Ivy Bridge or better, as of 2014); AMD: at least AMD Zen Architecture (Ryzen, as of Feb. 2017); free disk space on UEFI partition (≥ 200 MB); free disk space on Windows partition (≥ 600 MB)
Supported OS	genusecure Suite 2.0: Windows Professional or Enterprise 11 24H2 or 24H4 genusecure Suite 2.1: Windows Professional or Enterprise 11 24H2 LTSC or 25H2
Smart card	CardOS 5.3; ≥ 1 card per endpoint (≥ 2 certificates per card)
PKI	BSI-certified (ECOS TMA or genutrust/D-Trust)
Encryption algorithm	AES-XTS (DiskEncrypt)
VPN protocol	IKEv2/IPsec-ESP, UDP 4500
Default UDP port	4500
Certificate key size	RSA 4096 bits (both user and CA certificates)
Device-health forwarding	Optional; enabled via a single registry flag
Trusted-Network Detection	Optional; enabled via a single registry flag
Automatic authentication	Optional; enabled via a single registry flag
HA capability	Active-active genuscreen clusters (load balancing)
Monitoring	Prometheus & Zabbix exporters; Windows Event Log (Ids 1000-1002)
Installation package	Signed MSI (SHA-256 checksum provided on the customer portal)
Maximum DHCP-offered gateways	4 IPv4 addresses (used by genuconnect)
Maximum number of profiles (genuconnect)	Unlimited – user-selectable
Maximum CPB start-page size	2 MiB

Bundle Features	
Compliance	German VS-NfD (approved-operation) ready, VPN and disk encryption components are BSI-approved and can be used in classified “Verschlusssache – Nur für den Dienstgebrauch” environments when a BSI-certified PKI is in place
Smart-card centric	Single card stores ≥ 2 certificates, one certificate is used for data-at-rest encryption (DiskEncrypt) and another for network authentication (genuconnect)
PKI compatability	ECOS TMA/genutrust (D-Trust), both solutions provide a BSI-approved PKI capable of issuing 4096-bit RSA certificates with the required key-usages (dataEncipherment, keyEncipherment)
Zero trust/micro perimeter	Fine-grained access rules in genuconnect, controls based on user, group, OS, browser, IP range, country, time window, etc.; enforced by genuscreen appliances (which have to be procured separately)
Device health & quarantine	Integrated with genuconnect: Windows Security Center health data can be forwarded to the VPN gateway to automatically place non-compliant endpoints into a quarantine zone
Central management	DiskEncrypt Management Center and genuscreen: Policies for full-disk encryption and VPN/TND are defined centrally and pushed to endpoints via standard deployment tools (e.g., MECM/SCCM)
High availability	Active-active genuscreen clusters as VPN gateways and encryption services can be load-balanced and fail-over without user impact
Monitoring & auditing	Prometheus/Zabbix exporters and Windows Event Log for real-time health, performance, and connection metrics; event IDs 1000-1002 for VPN/TND status changes
Deployment	MSI packages (signed, SHA-256 verified) delivered as MSI installers; can be deployed silently with administrator rights
Supported hardware	Smart-card reader and TPM-enabled endpoint (recommended) required for secure private-key storage and entropy generation

Use Case



Convenient and Needs-Based Provision of Mobile, German VS-NfD-Complient Workplaces

With genusecure Suite, organizations with high-security requirements can easily implement VS-NfD-compliant mobile working – without compromising usability and flexibility. Using the comprehensive security solution and a smart card, employees connect to their organization's secure network via a Virtual Private Network (VPN) and are allowed to process classified information. Thanks to the approved full-drive encryption of genusecure Suite, all data stored on the device is securely protected at all times.

0326-01E

Further Information:

www.genua.eu/genusecure-suite

genua GmbH
Domagkstrasse 7 | 85551 Kirchheim | Germany
+49 89 991950-0 | info@genua.eu | www.genua.eu