vs-top

Security Laptop Approved for Classification Levels
NATO Restricted and EU Restricted

Technical Information
# Table of Contents

1 IT Security for Flexible, Mobile Work 1  
  1.1 The Challenge................................................................. 1  
  1.2 Requirements for a Security Laptop................................. 2  

2 The Solution: The Security Laptop vs-top for Use with Classified Data 2  
  2.1 The Concept........................................................................ 2  
  2.2 Security Architecture Overview........................................... 3  
  2.3 User Compartments.............................................................. 4  
    2.3.1 Primary Compartment.................................................... 4  
    2.3.2 Secondary Compartment............................................... 5  
  2.4 The Firewall/VPN Compartment.......................................... 5  
    2.4.1 Packet Filter.................................................................. 5  
    2.4.2 VPN............................................................................ 6  
  2.5 Connectivity........................................................................ 6  
  2.6 Disc Drive Encryption........................................................ 6  
  2.7 Ease of Operation............................................................... 6  
  2.8 Deployment Scenarios & Access Profiles.............................. 6  
    2.8.1 “At Home or Mobile” Deployment Scenario.................... 7  
    2.8.2 “In the Company Network” Deployment Scenario............ 8  
  2.9 Hardware............................................................................ 9  

3 Approval 9  

4 Infrastructure 10  
  4.1 Smartcard........................................................................... 10  
  4.2 Central Management Station............................................... 10  
  4.3 VPN Gateway...................................................................... 11  
  4.4 Communications Server..................................................... 11  
  4.5 Optional Initialization Station.............................................. 11  
  4.6 Optional Key Server........................................................... 11  
  4.7 Optional Installation Server................................................ 11  
  4.8 Optional FND Server.......................................................... 12  

5 Support 12  
  5.1 Installation and Configuration Service................................. 12  
  5.2 Software Support for Operational Systems.......................... 12  
  5.3 Support from Sales Partners.............................................. 12  

6 Glossary 14
1 IT Security for Flexible, Mobile Work

The information in this brochure is intended for IT security-professionals that are responsible for securing external and mobile IT infrastructure. It provides a compact overview of how the Security Laptop vs-top can be used to allow employees access to company data from both inside and outside the company without endangering the security of the company network. The vs-top provides you with the key advantages listed in the following table:

<table>
<thead>
<tr>
<th>Key advantages of the vs-top</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data processing and transfers for mobile users according to the</td>
</tr>
<tr>
<td>NATO RESTRICTED and EU RESTRICTED classification requirements</td>
</tr>
<tr>
<td>High security through strictly separated working areas on a</td>
</tr>
<tr>
<td>single laptop</td>
</tr>
<tr>
<td>A compact, easy to use laptop with standard applications</td>
</tr>
<tr>
<td>High security disc drive encryption</td>
</tr>
<tr>
<td>Central administration of complete communication infrastructure</td>
</tr>
</tbody>
</table>

The vs-top has been approved by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) as meeting the requirements of the German VS-NfD (classified – for official use only), NATO Restricted, and EU Restricted classifications.

1.1 The Challenge

The number of employees that use their laptops to access business data from outside the company network is continuously increasing in this globalized and digitalized world. Connections are readily made using a variety of possible routes including Ethernet, WLAN and cell/mobile phone networks and, in addition, there is an ever increasing number of persons working from home. If the predictions are to be believed, in the future more and more offices will regularly stand empty and teamwork will increasingly take place using e-mail, groupware and online conferences.

This mobile and decentralized method of working is made possible by technical progress. However, it also brings a number of challenges with it: How can flexibility and usability be combined with reliable 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 also no longer sufficient to secure the LAN with a firewall. External clients must also be protected and data transfer reliably encrypted. If a mobile device is lost then unauthorized third parties cannot be allowed to access confidential data: leakage of such information can result in financial loss, damage to customer trust and legal penalties for neglecting statutory requirements.
1.2 Requirements for a Security Laptop

A mobile device containing confidential company information and which is used to access company networks has to meet significantly higher security requirements than a device that is only used privately. And mobile working with classified information requires a particularly high level of security.

Generally, a number of security components to protect the data come into consideration. For example, a firewall to protect the mobile device from unwanted access and a VPN solution to encrypt the data being transferred. In addition, encryption of the disc drive can prevent access to confidential information if the device should ever be lost. Two-factor authentication should be used to ensure a high level of security for VPN access and for accessing data which has been saved locally.

If the user is allowed to access trusted resources and at the same time less trustworthy ones – for example, having unrestricted access to the Internet for research purposes – then the applications and data for the trusted and untrusted resources must be in working environments that are strictly separated from one another. If this is not the case then there is a danger of that malicious software that has managed to infiltrate via the web browser could access confidential data either on the laptop itself or in the company network.

2 The Solution: The Security Laptop vs-top for Use with Classified Data

2.1 The Concept

The Security Laptop vs-top provides users with an all-round secure mobile working environment and allows access and processing of confidential data in a company network. In addition, it can be used to access a privately used e-mail client or a web browser that allows active content without risk to any confidential information. The necessary security components are integrated in the security laptop. All the user requires for secure two-factor authentication is a smartcard.

![Fig. 1: vs-top: Mobile access to confidential data](image)
To this end, the vs-top has two strictly separated working environments – the so-called user compartments: The vs-top has a primary and a secondary compartment. An operating system such as Windows or Linux can be installed in each compartment and run in parallel but securely separated from each other. A key combination is provided to allow switching between the primary and secondary compartments.

A further compartment contains a firewall to protect the user compartments and a VPN solution to secure network connections that are made with the vs-top.

In addition, protection from unauthorized access is provided by the vs-top’s integrated disc drive encryption. Additional software is not required for this as it is completely transparent for the user compartments.

genua provides the Central Management Station genucenter for the administration of the vs-top. This enables the efficient administration of a full and scalable communication infrastructure.

2.2 Security Architecture Overview

Strict separation of the compartments and reliable security components are the foundation for the high security provided by the vs-top. But how can we be certain that this is the case with a software based product?

**High security separation:** The occurrence of errors – and therefore the danger of security problems – in software has been demonstrated to increase with size and complexity. The L4 microkernel was therefore chosen as the basis for implementing the strict separation of the vs-top. The L4 microkernel comprises circa 60,000
lines of code and therefore presents a very small attack surface. The resources that are available to a compartment and the access permissions it has can be defined in the microkernel.

These features of the L4-separation make the vs-top significantly more secure than conventional virtualization solutions. The way hardware resources are forwarded to the user compartments in the separation also brings advantages in both performance and usability: With the vs-top, a user compartment can, for example, be allowed to access the graphics card hardware acceleration allowing significantly more advanced applications to be executed than would be possible with virtualization solutions.

**Reliable security components:** The firewall/VPN compartment security components are based on a hardened Open Source operating system. They form the basis of numerous certified and approved genua security solutions and therefore have been thoroughly evaluated.

**Trustworthy encryption:** The encryption of the disc drive and the network communication only use components that have been 100 percent developed by genua in Germany or are based on software building blocks that have been thoroughly tested by genua.

**BSI approval:** The system has successfully gone through the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) approval process for NATO RESTRICTED and EU RESTRICTED classification requirements. This approval procedure includes that critical components undergo a rigorous examination and that both functioning and accuracy are tested.

### 2.3 User Compartments

#### 2.3.1 Primary Compartment

The primary compartment of the vs-top provides the high security working environment in which confidential data can be processed. Users can make VPN connections from this compartment – for example, to access resources in company networks.

While working with remote desktop solutions is only possible with an Internet connection, the vs-top also allows the transfer of confidential data into the primary compartment. This means that the user can, for example, access documents that have been saved locally when an Internet connection is not available. From the primary compartment users can also authenticate to a local company network or use a VPN to authenticate to another domain and use resources such as network drives.

Rollout and administration of the operating system used in the primary compartment can be readily carried out from a central location using, for example, System Center Configuration Manager (SCCM).
2.3.2 Secondary Compartment

The secondary compartment is shown in the primary compartment as a separate window: Switching between the user compartments is carried out using a key combination.

This allows the user, for example, to process private documents or use a web browser with active contents such as JavaScript. Classified material may not be processed here.

Connections to the Internet can be made from the secondary compartment over so-called captive portals, at the same time the primary compartment can be connected with a VPN.

2.4 The Firewall/VPN Compartment

The security components in the laptop’s firewall/VPN compartment are set in front of the user compartments and run on a separate, hardened operating system. All data connections from the user compartments are directed through the firewall/VPN compartment via virtual network interfaces. Firewall rule sets and VPN configurations are centrally administered and assigned to the Security Laptop.

![Diagram showing network connections through the firewall/VPN compartment](image)

Fig. 3: All network connections run through the firewall/VPN compartment

2.4.1 Packet Filter

The firewall that is integrated in the vs-top is based on the stateful packet filter used in the Firewall & VPN Appliance genuscreen, which is certified by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) according to CC EAL 4+. All network connections for the primary and secondary compartments are routed through this firewall. Direct external connections avoiding the firewall/VPN compartment and direct network connections between the primary and secondary compartments are not allowed. The use of separate internal network interfaces to the firewall/VPN compartment mean that network traffic from the primary and secondary compartments is processed separately.
2.4.2  VPN

The VPN component functions as a layer 3 based IPsec gateway. This allows secure data transfers to be made over the Internet using VPN connections with only strong encryption algorithms and long encryption keys.

2.5  Connectivity

The vs-top supports 10/100/1000 Mbit/s base-T Ethernet. Wireless network communication is in line with the WLAN 802.11a/b/g standards. The integrated modem is compatible with the LTE, UMTS and GPRS mobile/cell systems.

2.6  Disc Drive Encryption

Disc drive encryption is integrated into the vs-top. This covers all of the primary and secondary compartment partitions as well as the configuration of the firewall/VPN compartment. The complete system including the integrated drive encryption is approved for classification levels NATO Restricted and EU Restricted. There is no need to install an additional drive encryption application. Users are provided with a personal smart card with an individual private key to access the encrypted data.

2.7  Ease of Operation

Use of the vs-top differs little from that of conventional laptops and does not require any special instructions. Conventional operating systems and applications can be used and all important settings are administered centrally, meaning that configuration errors by inexperienced users can be excluded.

A vs-top application for Windows is available for making and terminating connections to the Internet and a VPN. This application comes with a number of connection and access profiles and users are able to configure their own profiles such as a WLAN profile for their home or hotel, or an LTE profile with its own SIM card and PIN.

The access profiles are administered with genua’s Central Management Station. For security reasons only administrators are authorized to create, modify or delete access of the user compartments to VPN or open networks.

2.8  Deployment Scenarios & Access Profiles

The vs-top can be deployed in a number of different scenarios: mobile – i. e. when travelling – at home and at the workplace.

The requirements for each deployment scenario are met by the relevant access profile specifying the configurations for the firewall and VPNs for each user compartment. As already mentioned, the access profiles can be configured in the Central Management Station genucenter and assigned to individual or multiple vs-tops at the same time. This centralized approach ensures that the same network cannot be accessed from the primary and secondary compartments.
2.8.1 “At Home or Mobile” Deployment Scenario

All connections from the primary compartment are encrypted and authenticated using IPsec if the laptop is being used outside the company network, while unencrypted network connections can be made from the secondary compartment to any address.

An alternative access profile could be considered, in which both user compartments can only communicate via VPN tunnel with different networks: The primary compartment could be used to communicate with the company network and the secondary compartment with a network in which confidential information cannot be processed (e.g. the test network within an organization).

Fig. 4: Access profile with a VPN for mobile use

Fig. 5: Access profile with two VPNs for mobile use
2.8.2 “In the Company Network” Deployment Scenario

Access profiles, which allow direct network connections from the primary compartment without a VPN tunnel, can be defined for the situation when the laptop is in the company network. This is made possible by a feature in the firewall/VPN compartment that allows it to determine whether or not the vs-top is directly connected to a trustworthy company network. This is known as Friendly Net Detection (FND) and requires that a FND server can be reached by SSH. In this situation communication for the secondary compartment is completely blocked.

![Diagram of FND](image)

Fig. 6: Access profile for the company network, communication is blocked for the secondary compartment

Alternatively, communication can be configured to use a VPN tunnel out of the company network, ensuring that the access to the company network from the secondary compartment is not possible.

![Diagram of VPN Tunnel](image)

Fig. 7: Access profile for the company network, secondary compartment communication is encrypted
2.9 Hardware

The vs-top is available on the HP EliteBook 830 G6 hardware (Q4/2019).

In addition, genua supports the following hardware:

- Fujitsu Lifebook U748
- Fujitsu Lifebook E744
- Fujitsu Lifebook E746
- HP EliteBook 830 G5
- HP Elitebook 820 G3
- HP Probook 640 G2

The Portfolio of supported hardware is continuously expanded. You will find an overview of the current hardware variants together with technical details on the genua product website.

![Fig. 8: The vs-top is available on a range of hardware](image)

3 Approval

The vs-top has been approved by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) as meeting the requirements of the German VS-NfD (classified – for official use only), NATO RESTRICTED and RESTREINT UE/EU RESTRICTED classifications. Mobile employees of public authorities, the armed forces and companies can therefore use the Security Laptop vs-top to process confidential information.
4 Infrastructure

4.1 Smartcard

User authentication for the disc drive encryption and saving the long-term VPN connection key is by smartcard. This ensures that the key material is not only protected but that it can also be removed from the laptop by the user when they are not using it.

Removal of the smartcard causes the vs-top to enter sleep mode. The smartcard has to be used to decrypt the disc drive once more when the vs-top is wakened from sleep mode.

Each vs-top is assigned only one user smartcard. A replacement smartcard to decrypt the disc drive can be ordered from the vs-top administrator if a user loses their smartcard.

Smartcards already existing in an organization can be used with the vs-top if requested.

4.2 Central Management Station

The genucenter Central Management Station provides user-friendly rollout and administration of any number of security laptops with the genucenter’s convenient grouping function making changes and updates for multiple devices at once.

The genucenter makes the consequent implementation of firewall and VPN connection security guidelines possible for all devices in internal and external use. Additional laptops can be easily integrated in the Central Management Station and provided with a tried and tested configuration.
### 4.3 VPN Gateway

genua offers their Firewall & VPN Appliance genuscreen as a VPN remote peer. The genuscreen has VS-NfD, NATO Restricted, EU Restricted, and OCCAR Restricted classification level approval as well as Common Criteria (CC) EAL 4+ certification by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI). The genuscreen can be administered with the Central Management Station genucenter, similarly to the vs-top.

### 4.4 Communications Server

As the security laptop may only have a temporary IP address or may be unreachable from outside – when, for example, it is behind a NAT gateway – connections have to be established from the laptop itself. So that the Central Management Station does not have to be directly connected to an insecure network such as the Internet, it is necessary in VS-NfD-conform operation that a communications server is installed in a DMZ between the genucenter and the insecure network.

The Firewall & VPN Appliance genuscreen is used as a communications server. This can be reached from outside and makes it possible for the Security Laptop to establish the necessary secure connection to the Central Management Station genucenter.

### 4.5 Optional Initialization Station

New smartcards must be initialized if an organization is not using smartcards of its own. Initialization is carried out with an initialization station and this function can be provided by the Firewall & VPN Appliance genuscreen.

### 4.6 Optional Key Server

Depending in part on user behavior, we recommend the use of a central key server in addition to a central Firewall & VPN Appliance genuscreen when more than around 1,000 security laptops are being administered.

The key server takes over the function provided by the smartcard of the VPN gateway genuscreen and is quicker in larger setups. This means that, for example, a VPN infrastructure with a four-figure number of Security Laptops per VPN gateway genuscreen can readily provide a good response time.

### 4.7 Optional Installation Server

As with the majority of business laptops, the vs-top can be configured according to the requirements of the organization. One such requirement could be that provisioning is carried out from a number of locations. In such cases the devices to be provisioned are connected with an installation server in a network segment intended for his purpose. The initial configuration is then installed on the devices along with individual keys for disc drive encryption and securing network communication.
This requires a stable connection between the genucenter and installation server. On the other hand, it is not necessary that there is a direct connection between the Security Laptop and the genucenter.

4.8 Optional FND Server
Security Laptops can recognize a trustworthy network in order to automatically offer the user an access profile that is only allowed in that environment. This requires a Firewall & VPN Appliance genuscreen that can be reached by SSH and has been configured as an FND server.

5 Support

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

5.2 Software Support for Operational Systems

Hardware guarantee: A standard guarantee following the hardware manufacturer’s conditions is included in the Security Laptop purchase price. The guarantee length for HP is 3 years and for Fujitsu 2 years. In addition we offer an optional guarantee and warranty extension including next business day on-site service in Germany.

Update service: Development of the vs-top is ongoing and our update service ensures that you will have both the newest versions automatically delivered to you and access to our full patch data base.

Hotline: In addition to our update service, we provide e-mail and telephone support in German and English. You can use our hotline for any questions related to the vs-top. If required, we can provide telephone hotline support 24 hours a day, 7 days a week.

5.3 Support from Sales Partners

Support services from sales partners: Many authorized genua sales partners provide extended support options such as an on-site hardware exchange service within a guaranteed time.
Our contact information:

genua GmbH, Domagkstrasse 7, 85551 Kirchheim, Germany
tel +49 89 991950-0, fax +49 89 991950-999, info@genua.eu, www.genua.eu
# 6 Glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSI</td>
<td>The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) is the national German cyber-security organization.</td>
</tr>
<tr>
<td>DMZ</td>
<td>A demilitarized zone is a neutral region between an organization’s internal network and external public networks. It allows controlled access to servers connected to the zone and at the same time protects the internal network from unauthorized external access.</td>
</tr>
<tr>
<td>FND</td>
<td>Friendly net detection is the automatic recognition of so-called “known networks”. The intention is, on the one hand, to guarantee security for the central data network in remote access VPNs and on the other hand to allow the user to work in the company and other trustworthy networks without hindrance.</td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security – a security protocol that provides a high degree of confidentiality, authentication and integrity for communication over IP networks. IPsec can be used to establish virtual private networks (VPNs).</td>
</tr>
<tr>
<td>Microkernel</td>
<td>The near-minimum amount of software that can provide the mechanisms needed to implement an operating system. These mechanisms include low-level address space management, thread management, and inter-process communication.</td>
</tr>
<tr>
<td>Packet Filter</td>
<td>A firewall that applies filter rules based on IP addresses and port numbers. Additional protection can be provided by so-called “stateful inspection”.</td>
</tr>
<tr>
<td>SCCM</td>
<td>A system center configuration manager is a software product from the Microsoft System Center Suite providing functions such as system update management and license monitoring.</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell – a network protocol which can be used to establish an encrypted network connection to a remote computer.</td>
</tr>
<tr>
<td>Smartcard</td>
<td>A hardware component that forms part of a system for identifying and authenticating users.</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network – a technology enabling an external computer to be connected to a local network using the Internet as a transport medium and providing encrypted data transfer.</td>
</tr>
</tbody>
</table>
VS-NiD

VS-NUR FÜR DEN DIENSTGEBRAUCH (confidential – for official use only) is a level of protection for classified information defined in German law.