genua.

Remote Service for Classification Level German VS-NfD

Highly Secure Remote Access to Classified Networks

Authorities and companies with an obligation to maintain secrecy increasingly transfer the servicing of systems to the manufacturer, specialized remote maintenance service providers or other locations in order to utilize different benefits. When externally accessing classified networks, however, special precautions need to be taken to avoid cyber risks.

SecurITy made in Germany

SecurITy made in EU

Requirements on Highly Secure Remote Maintenance

Remote maintenance in restricted networks is subject to the rules of the directive for classified information defined by the German Federal Ministry of the Interior and Community (BMI). When restricted data is transferred, these rules stipulate the use of products that have been approved for classification level German VS-NfD by the German Federal Office for Information Security (BSI).

Furthermore, the BSI basic protection catalogs define architecture proposals for the remote maintenance of IT systems. These include the avoidance of a permanent network connection as well as the possibility of monitoring remote maintenance procedures.

The Rendezvous Remote Maintenance Solution

The rendezvous remote maintenance solution for restricted networks can reliably meet these demands:

- Access to the specific target system is fully controlled by the operator and can take place only within an agreed maintenance window.
- To this end, the remote maintenance provider sets up a connection with „Restricted“ level encryption to the remote maintenance platform of genua.
- Secure access is implemented via a rendezvous server that does not permit unilateral maintenance access to the target system.
- A connection to the rendezvous server is now also setup from the customer network, e.g., by an administrator.
- Only when the rendezvous is established the remote maintenance provider can use the now direct connection to the target system.

As the administrator at the authority or at the company with an obligation to maintain secrecy must in all cases authorize access, the administrator always has full control of who accesses the target system in the restricted network and when.

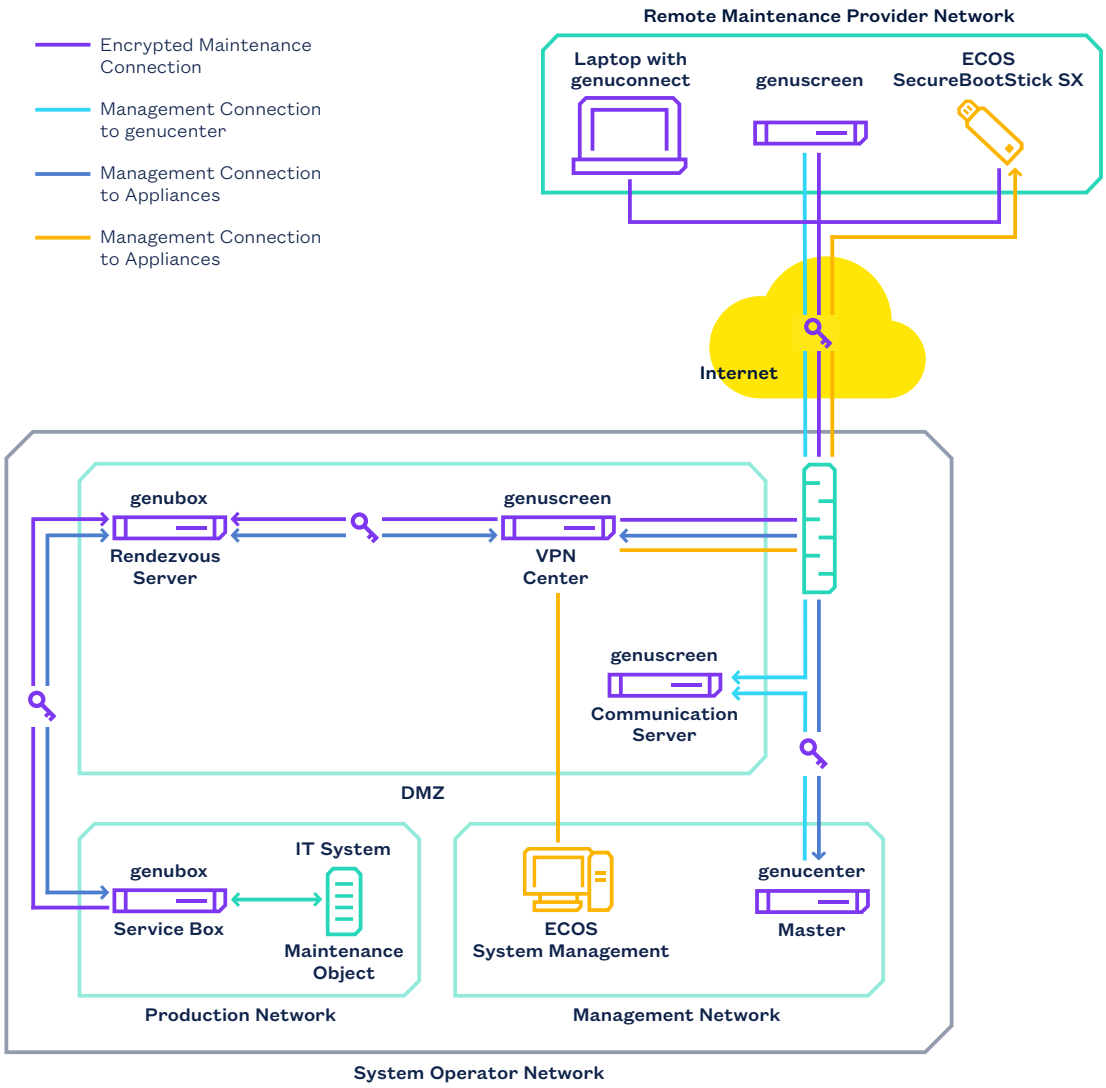
Remote Access – Flexible and Secure

If maintenance is required which for logistical reasons cannot be provided on site, remote maintenance offers a flexible and practical solution for system operators and remote maintenance providers. Depending on the situation and protection needs, however, high requirements on IT security must be met.

Approved Remote Maintenance Clients

For high-security access, the remote maintenance provider has an end device for setting up a restricted-level-compliant IPsec tunnel to the remote peer – the Firewall & VPN appliance genuscreen. genua offers various clients with BSI approval:

- **genuconnect:** VPN software client for protected connections of laptops and tablets with MS Windows
- **genuscreen:** Firewall & VPN appliance for secure connection of properties and mobile locations with multiple workstations
- **ECOS SecureBootStick SX:** Plug & Play security solution for flexible use



Overview: Components and connections for remote maintenance in a restricted network

Overview of Sequence for Secure Remote Maintenance

An SSH VPN is used for directly connecting genuscreen (remote peer to the remote maintenance client) and the rendezvous server. This VPN ensures encryption of the complete path between the remote maintenance client and the rendezvous server. Unlike a conventional VPN which provides site-to-site (network-to-network) or host-to-host connections, an SSH VPN provides access to certain applications/services (ports) only.

The rendezvous server acts as mediator between the remote maintenance provider and the target system. Remote maintenance connections must always be authorized and set up internally. A so-called service box is used for this purpose: It functions as the interface to the target system and, inside the restricted network, also sets up an encrypted connection to the rendezvous server.

The service box additionally serves as a packet filter and protects against unwanted network access to the maintenance objects. The ability to integrate a virus scanner allows the data sent by the remote maintenance provider to be checked and damage caused by malicious software to be avoided.

The maintenance connections are released by an authorized operator, e.g., using the genucenter central management solution or a key switch.

This ensures that remote maintenance providers can access the target system in the sensitive network only when required and only if they have the necessary authorization.

All network access is configured, controlled and monitored using the genucenter central management solution. Since when used for applications for classification level German VS-NfD this solution is not allowed to be directly connected to an insecure network such as the Internet, a communication server needs to be interposed.

Support of Zero Trust Concepts

The remote maintenance solution from genua supports Zero Trust concepts. In this context, the rendezvous server acts as the software-defined perimeter and allows external, authenticated users access to specific services behind the perimeter. Key security functions of the remote maintenance solution from genua:

- Tunnel between the client and the software-defined perimeter, with encryption for classification level German VS-NfD
- Flexible access control at the software-defined perimeter based on identity and the runtime environment
- Privileged access with sophisticated client, role and rights concept

Further Information:

www.genua.eu/genubox

WP-VSFEWA-0423-03-EN

About genua

genua GmbH is an enabler of the digital transformation. We secure sensitive IT networks in the public and enterprise sectors, for critical infrastructure organizations and in industries with an obligation to maintain secrecy with highly secure and scalable cyber security solutions. In doing so, genua GmbH focuses on the comprehensive protection of networks, communication and internal network security for IT and OT. The range of solutions spans from firewalls & gateways, VPNs, remote maintenance systems, internal network security and cloud security to remote access solutions for mobile employees and home offices.

genua GmbH is a subsidiary of the Bundesdruckerei Group. With more than 350 employees, it develops and produces IT security solutions exclusively in Germany. Since the founding of the company in 1992, regular certifications and approvals from the German Federal Office for Information Security (BSI) provide proof of the high security and quality standards of the products. Customers include, among others, Arvato Systems, BMW, the German Armed Services, THW as well as the Würth Group.

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