NATIONAL SECURE CLOUD

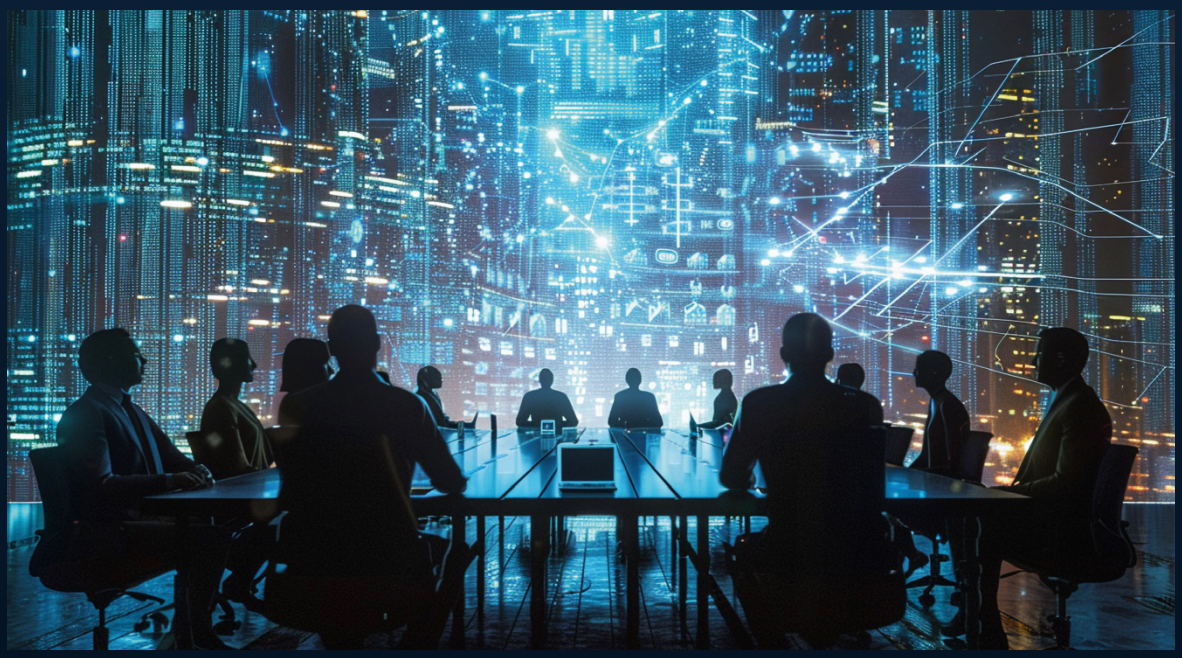
NSC and VS-Workstation – Your Partner for Maximum Security

Development of a Sovereign and Secure Cloud in Germany with Leading Cybersecurity Experts

IABG | infodas | KERNKONZEPT | utimaco®

XELERA | mspaces | INTRE

TABLE OF CONTENTS



IABG – We Design Security

For over six decades, IABG has taken responsibility for the security of state and society. Our unwavering goal: to stay one step ahead by shaping tomorrow today. This commitment also applies to Germany's digital sovereignty. Together with selected German partners, we have therefore launched the National Secure Cloud (NSC) programme.

IABG is a leading European technology company, providing independent and product-neutral advice on the use of security-critical systems. As the coordinator of the NSC programme, we are responsible for its strategic management and further development. This includes meeting the most stringent security requirements for mission owners such as government bodies and the military, while ensuring a secure and sovereign digital infrastructure with full interoperability with international standards.

Within the NSC programme, IABG defines the overall hardware and software architecture and ensures secure management of Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) solutions, including the consistent integration of open-source software.

Industrieanlagen-Betriebsgesellschaft mbH
Einsteinstraße 20
85521 Ottobrunn

Patrick Rund
Senior Manager
Digital Transformation
rund@iabg.de
+49 89 6088 3713
www.iabg.de

Highest Security Without Compromise

Protecting critical IT infrastructure within public authorities and defence institutions requires uncompromising security standards. Given the rise in cyber threats and the growing complexity of international interconnectivity, government and defence stakeholders require sovereign digital infrastructures and secure working environments that not only meet stringent confidentiality and data protection requirements, but also uphold Germany's digital sovereignty. Core components of this architecture are the National Secure Cloud (NSC) and the VS-Workstation – both developed in close collaboration with trusted German IT partners under the leadership of IABG.

Our Solutions: NSC and VS-Workstation

The NSC is a highly secure cloud infrastructure that can process data across multiple security levels simultaneously. It meets the stringent requirements of the German Classified Information Directive (VSA). A central feature of the NSC is the separation of security domains.

This allows multiple protection levels to operate on the same hardware – ensuring high cost-efficiency. The NSC uses open-source technologies to ensure transparency and traceability. Its open architecture reduces dependence on proprietary technologies from international providers – commonly referred to as "hyperscalers" – while enabling straightforward adaptation to specific requirements.

The National Secure Cloud

- A highly secure cloud infrastructure that fulfils the stringent requirements of the German Federal Office for Information Security (BSI).
- Strictly separated security domains and secure domain transitions, tailored to the needs of public authorities and defence operations.
- Robust performance, full interoperability and scalable system architecture.

The VS-Workstation complements the NSC by offering a secure workstation environment. As with the NSC, the focus is on open-source solutions designed to uphold digital sovereignty. These solutions are specifically tailored to the needs of organisations operating under strict security regulations.

Mechanisms such as access controls and encryption ensure the confidentiality and integrity of data. Additional protection against malware and unauthorised access further strengthens the system's security posture. The VS-Workstation is designed for processing classified information up to and including the classification level SECRET.

The VS-Workstation Features

- → Modular solution based on European open-source technologies.
- → Scalable for large organisations with thousands of users.
- → Designed for processing classified information up to the classification level SECRET, including an integrated VS-Registry (classified information registry in accordance with German security regulations).
- → Fully compatible with ZenDiS openDesk.

Security and Technical Features

The NSC combines software, services and security hardware specifically developed for sovereign cloud applications. It uses a BSI-certified hypervisor to manage multiple security domains on a single hardware platform. The strict separation of these domains ensures maximum security and enables the processing of classified information up to the classification level SECRET.

Dedicated security gateways allow controlled data exchange between different security domains – also up to classification level SECRET. Cryptographic hardware security modules provide strong protection against unauthorised access and manipulation.

The NSC and the VS-Workstation meet the highest security standards while remaining user-friendly, scalable and cost-efficient. They integrate seamlessly into existing infrastructures, allowing organisations to continue using their current software environments. The modular design also facilitates the integration of new technologies such as artificial intelligence (AI).

In military contexts, the systems can operate independently of network connectivity if required – even in highly confined or mobile environments. They also offer a high degree of interoperability with allied partners, for example within the framework of NATO operations. As modular, highly secure and flexible systems, the NSC and the VS-Workstation can be tailored to diverse operational requirements. This makes them ideal tools for government authorities, defence institutions and other security-critical organisations in Germany.

In Focus: Daily Cyberattacks on German Government Networks

- The BSI detects around 250,000 new malware variants every single day.
- Germany's federal administration alone receives an average of 775 malware-laden emails each day.
- Every day, the BSI blocks access to 370 websites from within government networks.

Download PDF:
The State of IT Security in Germany 2024

Cyber Espionage: Attacks in Diplomatic and Government Contexts

- Compromise of the SolarWinds supply chain affecting multiple US government agencies and international organisations (2020).
- Disruption of civilian operations at the Rheinmetall defence group through targeted cyber intrusion (2023).
- Targeting of the SPD party headquarters and German defence contractors, attributed to Russian military intelligence (2024).
- Attack on the British Ministry of Defence, reportedly originating from China (2024).
- Takedown of CDU party headquarters IT infrastructure following a targeted cyber incident (2024).

This short selection of global incidents from recent years underscores the persistent threat posed by cyber espionage – particularly against diplomatic channels and sensitive political or strategic information. Common attack vectors include phishing, malware and supply chain compromise.

Two Attacks on Public Sector IT

1. **IT Service Provider Incident Affecting Chambers of Industry and Commerce (2022):**
   On 3 August 2022, the IT service provider for Germany's Chambers of Industry and Commerce detected anomalous activity in its systems and initiated a shutdown to prevent damage. As a result, all 79 chambers (IHKs) in Germany were disconnected from the internet, taking websites offline and rendering email communication impossible. Internal applications were also affected. After extensive analysis, the service provider gradually restored the systems, but some chambers continued to experience disruptions for several months.

2. **Ransomware Attacks on Municipal Authorities and Services (2022–2023):**
   Between 2022 and 2023, ransomware attacks hit 27 municipal administrations and public service providers of various sizes. The affected entities ranged from a small municipality with 2,800 inhabitants to a major city of more than 1.8 million. The attacks affected city and district administrations, local transport companies, energy providers, housing associations, municipal cleaning services and a school authority.

Digital Sovereignty with the National Secure Cloud

The development of the National Secure Cloud (NSC) reflects current discussions on digital sovereignty and state IT security. Public authorities and armed forces, in particular, work daily with classified data in accordance with the Classified Information Directive (VSA) and require a high level of sovereignty. The NSC is a cloud solution specifically tailored to these classification and protection requirements. But what makes it so special? In this interview, Patrick Rund (Senior Manager and Programme Manager Digital Transformation at IABG) explains the advantages of the NSC.

Patrick Rund
Senior Manager
Digital Transformation
IABG

Developing a sovereign cloud and workplace solution suitable for classified information is no easy task. What is the idea behind it?

Our core idea was a cloud solution developed in Germany, for Germany, that fulfils two key objectives: first, to strengthen digital sovereignty, and second, to be demonstrably more secure than conventional cloud solutions.

Well-known international providers often do not meet the stringent requirements of the VSA beyond the RESTRICTED classification level. Due to the complexity and architecture of such solutions, their actual security level can only be verified or measured to a limited extent. This makes approval or accreditation – for example by the BSI – extremely difficult.

That's why we have developed our components in such a way that users not only retain full control over their data, but also ensure that official approval, such as BSI accreditation, is feasible. At the same time, the highest security standards can always be maintained.

We rely on open-source software, a transparent and as-standardised-as-possible system architecture, and a manageable development roadmap to guarantee a high – and above all measurable – level of security and digital sovereignty.

The target groups include public authorities, military organisations and other state actors. What challenges do they face in their work today?

The greatest challenge is the protection of classified information in the face of increasing digitalisation, collaboration and networking – including communication between authorities and military institutions, both nationally and internationally. To this end, IT systems and new technologies must be harmonised with the Classified Information Directive (VSA). However, even then, achieving 100% protection is virtually impossible.

Despite these challenges, public authorities must ensure they remain capable of acting and keeping pace with technological progress. To do so, it is essential to efficiently and quickly harness the benefits of emerging technologies, such as artificial intelligence or the Internet of Things (IoT).

This also helps to mitigate the consequences of demographic change and the resulting shortage of skilled labour. The aim is to establish stable and secure communication channels in increasingly complex networks of interconnected devices and services, to ensure operational continuity and to manage the growing volume of data.

Users – whether in administrative roles or technical operations – require straightforward and easy-to-operate solutions. In many cases, the underlying subject matter is already complex enough. The IT system or application must not add further complications to the solution process.

At the same time, the solutions offered must remain affordable and feasible within the constraints of public sector budgets – especially in the current climate of tight fiscal planning.

The concept of a cloud-based IT system, with its inherent advantages, offers an excellent foundation for addressing these challenges.

What are the different requirements of the target groups?

Public administrations and services require secure and cost-efficient solutions for handling classified (VS) data. These systems must enable interaction within their own departments, with citizens and with other authorities – in full compliance with the GDPR and the Classified Information Directive (VSA). One example of this need is cross-departmental data exchange between the police and the judiciary.

Certain state actors, such as the Ministry of Foreign Affairs, require worldwide availability of systems for processing classified information. These systems must also support flexible deployment locations – for example, through mobile use scenarios such as the Mobile VS-Workstation.

In the military domain, the requirements for security and confidentiality are likewise consistently high. From a functional perspective, military operations involve a wide range of proprietary and hardware-bound weapons and command-and-control systems, resulting in high technical complexity. In such cases, it is essential to gradually decouple software from hardware and advance standardisation – especially in line with NATO standards. Another critical requirement is the ability to quickly deploy systems in the field in emergency situations and ensure full operational capability without network connectivity. Interoperability with allied partners – for instance in the context of NATO's Multi-Domain Operations – is another key requirement.

Nearly all target groups also need compact and resource-efficient solutions. The ability to securely transfer data between IT systems classified at different VS security levels is equally essential. Just as important is the system's flexibility: new applications or updates must be made available at very short notice – especially, but not only, in the event of a crisis.

Synopsis: State actors require IT systems that are user-friendly, flexible, resource-efficient, scalable, deployable without network connectivity, interoperable and compliant with all national and international security standards. Certainly not an easy task – but this is precisely where the classic advantages of cloud technologies come into play, provided that these technologies are adapted for use in classified IT environments (VS-IT) and in compliance with the VSA. That is exactly what we deliver – together with our partners.

Why are NSC and VS-Workstations the best solutions? What sets them apart?

The National Secure Cloud (NSC) and the VS-Workstation, which complement each other perfectly, offer several distinct advantages over other solutions. First and foremost, we follow an open concept, meaning everything is based on open-source technologies. If a customer has specific requirements, we can collaborate with the BSI to deliver a secure and practically feasible solution that fully meets these needs. Ultimately, it's about building an ecosystem: other manufacturers and providers are encouraged to integrate their solutions into the overall NSC system architecture. This increases both security and sovereignty.

Both the NSC and the VS-Workstation are designed from the ground up to meet the highest security standards – a principle best described by "security by design". In practice, this means that VSA-compliant security always comes first – and only then do we address aspects such as usability and look & feel. The NSC is based on components that are already approved by the BSI and are being continuously enhanced. We move forward step by step, maintaining a balanced focus on performance, security and approval readiness. This makes the NSC and the VS-Workstation the ideal foundation for supporting a wide range of operational use cases and for achieving BSI certification.

The National Secure Cloud (NSC) is specifically designed to meet the VS-IT needs of the following users:

- **Government organizations with high IT security requirements (including ministries and affiliated agencies)**
  Digital and data sovereignty are top priorities for governments and their associated public bodies. Avoiding vendor lock-in is equally important. Instead, traditional hyperscaler products should be replaced or complemented with open-source applications such as the VS-Workstation.

- **The German Federal Armed Forces (Bundeswehr) and other military organisations (e.g. NATO or friendly countries)**
  Data sovereignty also plays a central role in the military domain. Additionally, international standards, such as those established by NATO, must be strictly adhered to. As a result, the technical requirements for military organisations are significantly higher than those of civilian government institutions. The NSC technology stack fulfils all these requirements. Recent developments show that the German Federal Armed Forces (Bundeswehr) are aligning their approach with the ZenDiS solution openDesk. The VS-Workstation is the ideal complement and fully compatible with openDesk.

- **Regulated industries**
  Regulated sectors, such as the pharmaceutical industry, allocate substantial financial resources to the development of medical products, which often undergo a highly complex approval process lasting several years. Maintaining confidentiality throughout the entire process – from concept to authorisation – is essential to protect intellectual property and secure return on investment.

Perhaps two more technical examples: Our hypervisor enables multiple security domains to run on a single hardware platform, saving both cost and space. By virtualising security functions, we allow customers to respond flexibly to adaptation needs – since deploying software is much easier than modifying hardware.

Our open secret is a combination of innovative technology, philosophy and structured communication with the relevant stakeholders – because success can only be achieved together. As I mentioned at the beginning: it is a cloud from Germany, for Germany. And anyone who can improve it is welcome to contribute.

The VS-Workstation incorporates the core features of a digitally sovereign workplace designed for government clouds:

- **Use of open-source software:** Public authorities increasingly rely on open-source software, which offers greater transparency and auditability. This reduces dependence on proprietary solutions from major international IT providers.

- **Data sovereignty:** Data is stored and managed in national or agency-owned data centres instead of in foreign cloud infrastructures. This ensures that data remains protected from unauthorised access by foreign jurisdictions or third parties.

- **Security standards:** Strict security and data protection standards are implemented to safeguard IT infrastructures against cyberattacks. These include regular security assessments and audits.

- **Interoperability:** Systems and applications are developed to ensure compatibility and seamless data exchange. This improves efficiency and cooperation across authorities and departments.

- **Control over software and hardware:** Public authorities retain full control over the software and hardware components they use. This enables them to implement modifications and close security gaps independently – without relying on external vendors.

- **Benefits of a digitally sovereign workplace for public authorities:**

  Security: Control over data and IT infrastructures enables authorities to better manage security risks and defend more effectively against cyberattacks.

  Independence: Reduced dependency on international IT service providers allows authorities to shape and implement IT strategies more autonomously.

  Data protection: Storing and processing data within national jurisdiction simplifies compliance with national and European data protection laws.

  Cost control: Open-source solutions are often more cost-effective in the long term, as they reduce licensing fees and vendor lock-in effects.

The National Secure Cloud: Tailored Security for Classified Data (Up to SECRET Level)

Secure and sovereign cloud solutions are essential for modern IT infrastructures, particularly in the public sector. The National Secure Cloud (NSC) addresses this need as a flexible and customisable cloud platform for diverse users. It adapts to specific requirements while meeting the highest security standards.

Modularity and Adaptability

The NSC's modular structure provides user organisations with a toolkit of customised security solutions tailored to their individual requirements. Whether for public authorities or military users, each entity receives a solution precisely adapted to the specific deployment scenario in terms of functionality and security.

Available modules include a secure cloud management platform, software-as-a-service (SaaS) components, cryptographic modules and other security solutions – all based on European open-source applications. The NSC's modularity also enables the integration of new technologies and applications, such as AI technologies including language models or machine learning. The cloud can be flexibly expanded to meet these evolving requirements.

Highest Security Standards According to VSA and VS-IT

Security is the foundation of the NSC. It complies with the strict requirements of the Classified Information Directive (VSA) and its corresponding IT directive (VS-IT). The NSC uses technologies approved by the German Federal Office for Information Security (BSI) up to the classification level SECRET or assessed as approvable. This guarantees the highest levels of data confidentiality, integrity and availability.

"Every cloud requires a hypervisor as the core of virtualisation and resource orchestration," states Dr. Michael Hohmuth, Managing Director of NSC partner Kernkonzept. "Conventional clouds rely on monolithic hypervisors with extensive attack vectors. In contrast, the NSC utilises the modular L4Re Secure Separation Kernel VS, which is authorised up to the 'SECRET' classification level. Its microkernel-based architecture has only a minimal attack surface and forms the foundation for NSC's security-by-design strategy."

Another essential feature is the use of data encryption and digital signatures. The NSC employs BSI-approved hardware security modules (HSMs) to generate, manage and store cryptographic key material. These keys are used in data encryption and certificate generation processes, and never leave the highly secure environment of the HSM. Moreover, the hardware security modules used are future-proof and can be upgraded as required to support post-quantum cryptography (PQC).

Security Domains and Secure Transitions

The NSC enables the creation of security domains in which authorities or NATO nations, for example, can assert and manage full data sovereignty, as well as independently handle data processing and storage. In addition, the NSC can create and securely isolate multiple security domains on the same server hardware – up to the classification level SECRET.

Each domain is equipped with specific security protocols and access controls to ensure that no information crosses domain boundaries without proper authorisation. This strict separation protects confidential data belonging to military or governmental organisations from unauthorised access. In the past, physically separate systems were required to achieve this level of security. With new technologies, however, it is now possible to operate multiple encrypted security domains on a single hardware platform.

For bidirectional data exchange between different security domains, the NSC employs SDoT (Secure Domain Transition) products. "This allows both structured and unstructured data to be exchanged between security domains – up to the classification level SECRET," explains Benedikt Meng from NSC partner infodas. This capability is especially relevant in international contexts, such as cooperation between NATO member states. For example, data from a NATO SECRET domain can be securely transmitted to allied partner nations.

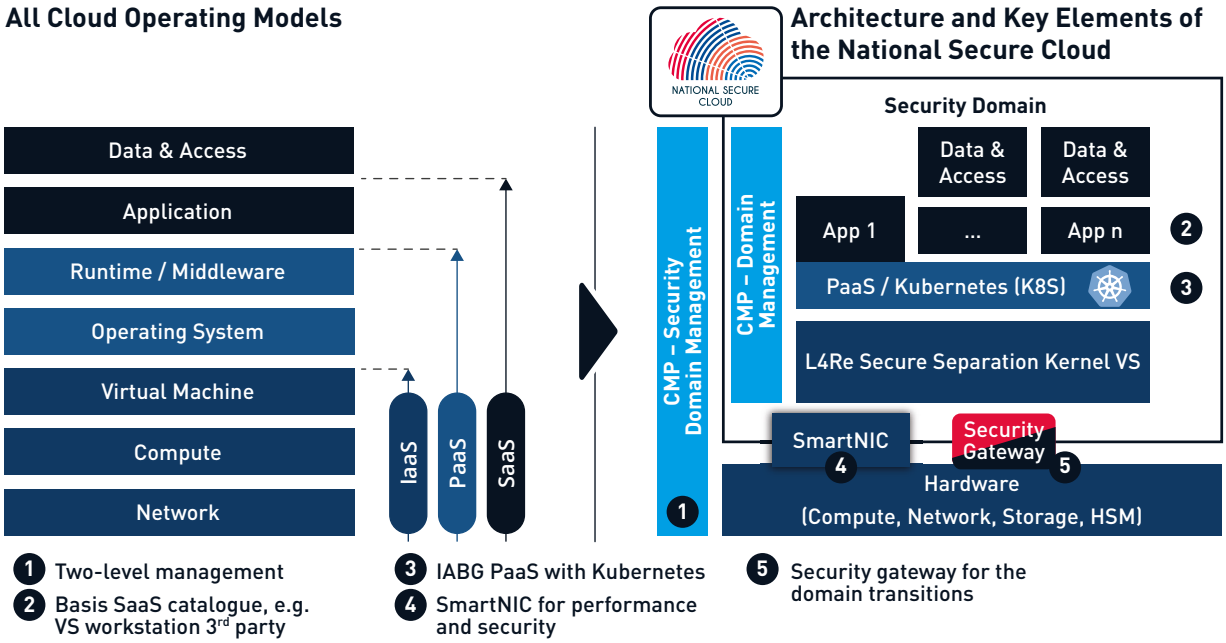
High Interoperability and Scalability

"In addition to its high security standards, the NSC offers interoperability in multinational military environments, as it is based on standardised and widely adopted protocols and open-source components," adds Nils Gerhardt, Chief Technology Officer at NSC partner Utimaco.

The NSC is also designed for seamless integration into existing infrastructures. Its scalability is another key advantage, enabling the cloud system to adapt rapidly to different requirements and operational scenarios – even during deadline-driven peak loads.

As a cloud platform, the NSC supports applications from different vendors, including proprietary solutions. This allows users to continue using their existing – often high-cost – software investments. However, transitioning to the VS-Workstation (see next chapter), which is fully aligned with the NSC, is strongly recommended. This shift reduces the often-complex software landscape within organisations and delivers improved security and greater efficiency.

Modular and Highly Secure: The VS-Workstation in Detail



Modular and Highly Secure: The VS-Workstation in Detail

The VS-Workstation is a modern software solution available both on-premises and as SaaS (Software as a Service). It offers functionality equivalent to standard office products from major technology companies. SaaS means that the software is not installed locally on a computer. Instead, it resides in the cloud and is accessed via a browser such as Firefox or Edge. For public authorities, this means that the VS-Workstation operates within the private cloud of a specialised provider and is not accessible from the public internet. Access is restricted to the internal computer network of the respective authority.

Features of the VS-Workstation

The VS-Workstation is defined by four key features: modularity, scalability, high security and data-sovereignty.

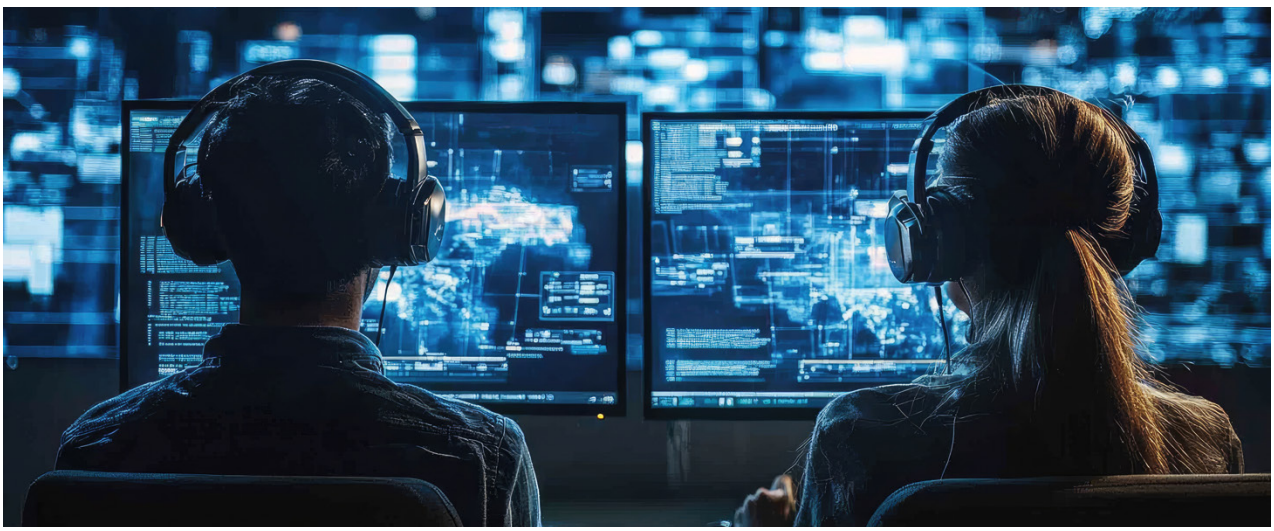
- "Modular" means that the solution integrates well-known European open-source applications (particularly from ownCloud and mspaces), whose functionality is equivalent to that of standard market solutions. Where required, services from other companies are also integrated.

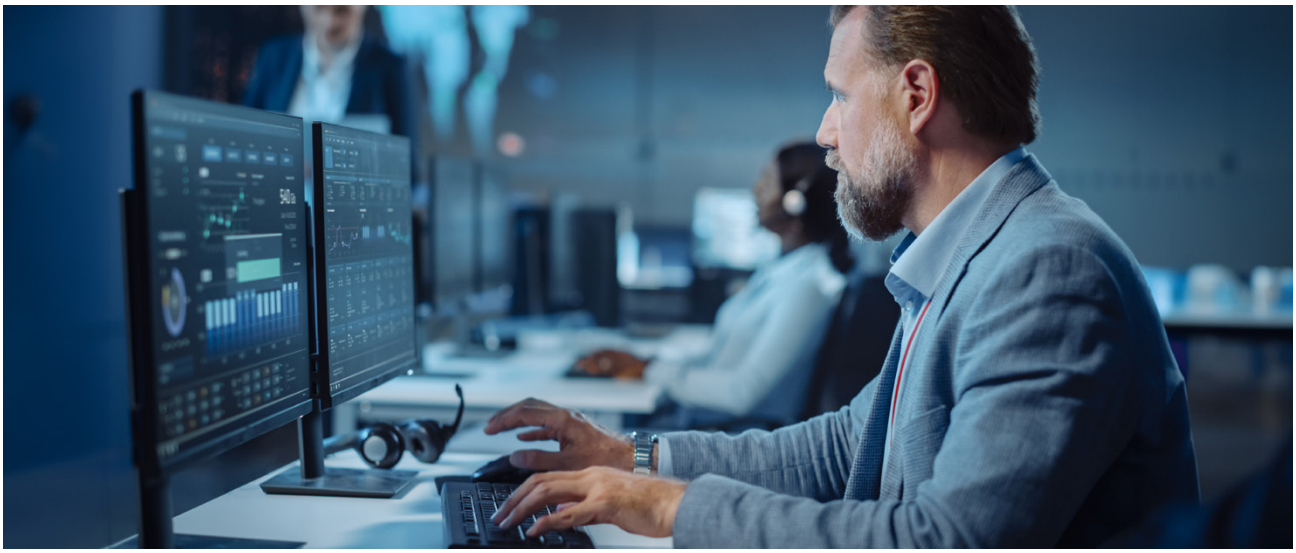
- "Scalable" means that the modules of the VS-Workstation can be deployed independently and scaled for virtually any number of users. The VS-Workstation is therefore suitable even for large organisations with many thousands of users.

- "Highly secure" means that the VS-Workstation is approved for processing classified information up to the classification level SECRET and supports all relevant BSI requirements.

- "Data-sovereign" refers to all cloud solutions and applications that ensure exclusive access to the data for the user, with storage restricted to national infrastructure – in this case, to data centres located in Germany. For European authorities, these are specially certified data centres in various member states.

Synopsis: The VS-Workstation offers the full range of standard functions provided by modern office solutions – while simultaneously safeguarding national interests.





Access to the VS-Workstation

The VS-Workstation is intended for use within a browser environment operating on a BSI-certified, high-security operating system. This system is hardened in line with IT security principles – just like the laptops and desktop PCs certified for use in public authorities.

Accessing the VS-Workstation is straightforward: users can either click a provided browser link or manually enter the address into the browser bar. A central portal then opens, giving access to all available functions and modules.

To ensure that only authorised individuals can use the portal, it is protected by an Identity and Access Management (IAM) system. Only users registered in the system can access the VS-Workstation using their credentials. User access rights are role-based and depend on the assigned authorisations – for example, users who are not authorised to handle classified information have no access to related documents or functions.

User identities and authorisations are managed centrally via a directory service that is an integral part of the VS-Workstation and is based on the open-source software Keycloak. Single Sign-On (SSO) is one of the system's integrated user features – allowing users to log in once and gain access to all connected applications.

The solution also offers integrated user self-services, allowing users to independently configure their profiles and working environments without IT support.

The VS-Drive Cloud Storage

One of the main features of the VS-Workstation is the VS-Drive cloud storage, a file management system similar to Dropbox or OneDrive. The user interface is seamlessly integrated into the VS-Workstation and provides all essential Windows-style file management functions.

Users can view their files, identify file types, rename or delete them. They can also create any number of folders and subfolders to organise their documents. In addition, individual files or folders can be shared with other users – either with read-only access or editing rights – enabling collaborative work on documents.

For these purposes, the integrated Office solution is used, as detailed in the following pages. The reverse is also possible: users can integrate shared files and folders into their own cloud storage. Additionally, there are publicly accessible file areas where documents can be made available to all users.

The service is based on modules from the open-source platform ownCloud and integrates the Office solution, which is a core component of the VS-Workstation.

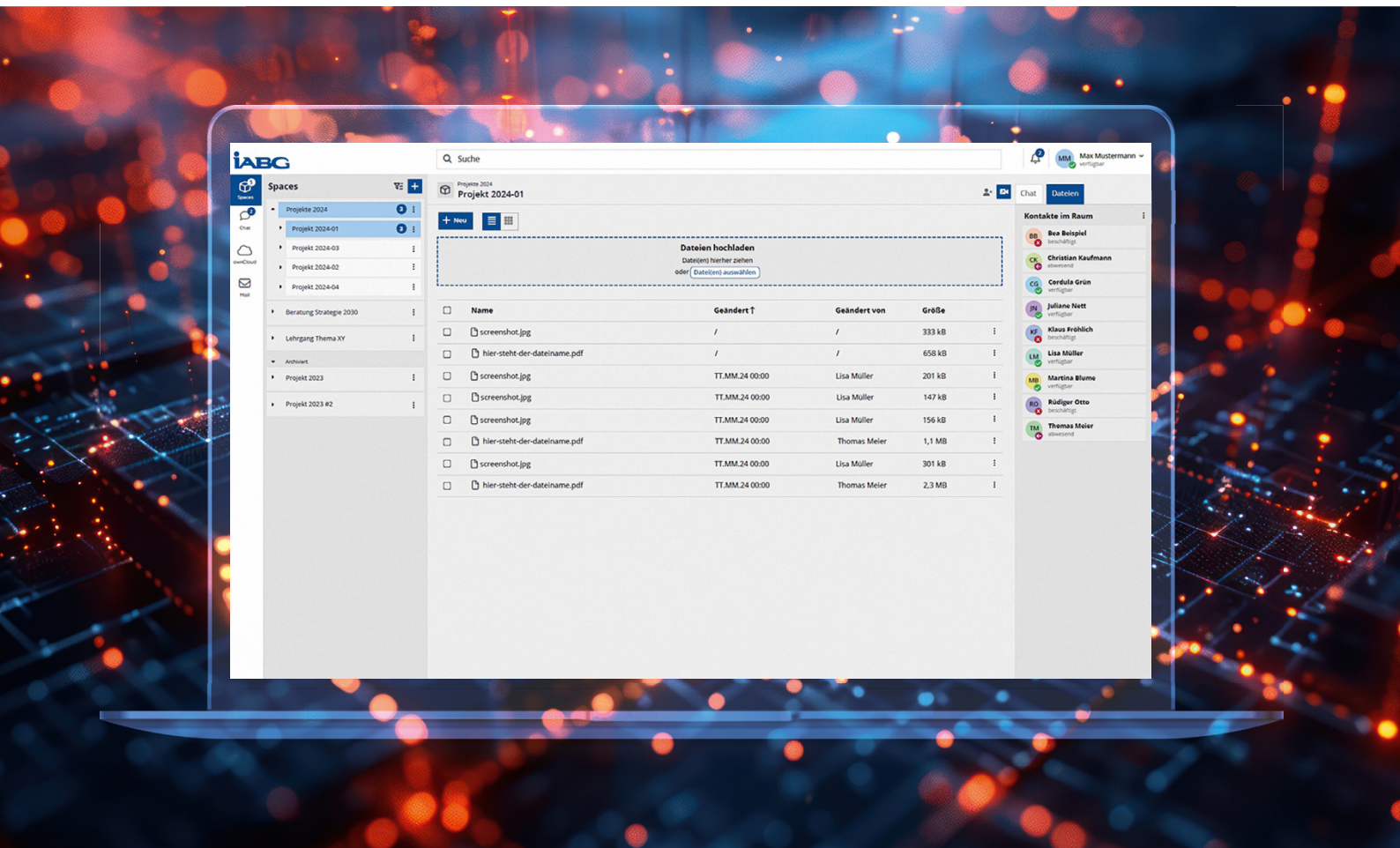
Digital Collaboration with VS Video and Chat

Video conferences and chats are core features of modern office solutions and are also part of Collabora Office within the VS-Workstation. Within a domain, users can host video and audio meetings with as many participants as needed, including the ability to share their screen. This allows for the presentation of slides, spreadsheets or documents in real time.

Additional tools enable file sharing and collaborative work on a digital whiteboard. These functions are complemented by an integrated text chat, which connects all VS-Workstation users in one environment. This digital collaboration capability is part of the VS-Realtime module and is accessible exclusively via browser.

The Core of the VS-Workstation: VS Office Collabora

The core module VS Office Collabora is a full-featured office application that uses VS-Drive as a secure storage location for documents. It includes familiar tools for word processing, spreadsheets and presentations, with a user interface and feature set aligned with common office software standards. The module supports both individual editing and real-time collaboration.



The VS-Workstation compared to the Microsoft Teams Suite

VS-Workstation		MS Teams App
VS-Room	**Workspace**	MS Sharepoint
VS-Chat	**Chat**	MS Teams
VS-Video	**Video**	MS Teams
VS-Docs	**Document Processing**	MS Teams
VS-Registry	**Document Management**	n/a
VS-Drive	**Data Platform**	MS oneDrive
VS-ID	**IDM**	AD/LDAP
VS-Base	**Integration Layer**	GraphAPI
NSC (Linux/Windows)	**Platform**	Windows

Documents can be edited by all users with appropriate write permissions. The application supports Microsoft Office file formats (.docx, .xlsx, .pptx), the Open Document Format (ODF) and a wide range of additional file types.

VS Office Collabora is based on the open-source cloud solution Collabora Office, which itself builds on LibreOffice and has been extended with comprehensive collaboration features.

The integration of a digital VS-Registry (classified document management) ensures that document management processes are fully auditable and compliant with the Classified Information Directive (VSA). This complements the overall system to form a holistic solution for the creation, management, and VSA-compliant collaboration on classified content – traceable, secure, and maintained throughout the entire lifecycle of classified documents.

Equipped for the Future: VS-AI

The next version of the VS-Workstation will include the VS-AI module, which extends its capabilities with a locally deployable language model – for example, the open-source model Mistral. The model is enhanced by an additional local knowledge base that adds contextual relevance, while the model itself remains fully interchangeable.

This enables automated tasks such as document summarisation and text drafting. The integration of cutting-edge technologies like AI modules ensures that the VS-Workstation remains adaptable to increasing data volumes and the growing complexity of administrative processes. As a result, the system provides a robust foundation for the digital transformation of public administration while allowing room for future innovation.

The VS-Workstation is offered within the framework of the NSC and is available in two subscription variants: On-Premises and SaaS.

- **Lower initial investment:** No high upfront costs – instead, manageable monthly or annual payments.
- **Access to the latest software:** Users benefit from up-to-date features and continuous security updates.
- **Flexibility:** Subscriptions can be scaled or adapted to changing requirements.
- **Technical support:** Ongoing access to support services and assistance with operational or configuration issues.

Questions and Answers on the NSC as the Foundation of the VS-Workstation

How much admin work is involved in deploying the NSC?

Deployment follows the industry standard for Kubernetes in enterprise environments. Depending on the size and modules used in the cluster, the so-called "Helm Charts" and associated scripts need to be adjusted.

IABG provides a comprehensive collection of templates and scenario-based examples to minimise the required effort. For simple clusters, only a few configuration parameters need to be adapted.

How does the NSC ensure federated identity management?

The NSC integrates identity management through Keycloak. Acting as middleware, Keycloak connects multiple identity providers in the background and provides a unified login interface across all cloud services. In combination with a hardware security module (HSM) and smartcards, login can also be securely linked to hardware-based authentication.

How is security for cryptographic requirements guaranteed in the NSC?

The NSC offers comprehensive security components, including a BSI-approved hardware security module for all cryptographic requirements. Additionally, client-side protections such as full disk encryption and file/folder encryption are supported – compliant up to the classification level 'VS-NfD' (RESTRICTED).

How does the NSC guarantee scalability?

Horizontal scalability is achieved using standard Kubernetes techniques (e.g. Horizontal Pod Scaler) to enable seamless scaling without manual intervention. Vertical scalability refers to increasing computing resources such as memory, CPUs or network capacity.

Is the NSC already protected against potential attacks from quantum computers?

Many components are crypto-agile and can already be upgraded to support post-quantum algorithms. Once these components receive BSI approval, the NSC is prepared to remain future-proof and quantum-resistant.

How can you ensure geo-redundancy with the NSC?

Reliable geo-redundancy requires three Kubernetes container clusters operated at different locations. This includes a "watchdog" process that dynamically reroutes IP addresses in the event of a cluster failure. Because the NSC supports the operation of multiple security domains on a single server, data centres can remain small. This enables rapid deployment of data centres and quick instantiation of SECRET-level domains.

Reference:
Kubernetes Cluster

Why are two CMPs required to administer the NSC?

To ensure complete separation of security domains, administration takes place within each respective domain. For security reasons, every domain is managed via its own dedicated Cloud Management Platform (CMP). In addition, a higher-level CMP exists to create and coordinate domains independently from within-domain operations.

How is multi-tenancy ensured?

The entire NSC solution is designed as a multi-tenant architecture. Through logical encapsulation of Kubernetes clusters, applications from different clients or organisations are fully isolated. This separation extends all the way to the client level, where applications are operated on encapsulated virtual machines.

How can the NSC ensure operational consistency across multiple sites?

The NSC's technology stack supports the use of uniform technologies across cloud computing, fog computing and edge computing. This standardisation simplifies administration regardless of the size or complexity of the infrastructure at a given location.

What advantages does a SmartNIC offer at the admin level?

SmartNIC technology allows data from multiple security domains – even with different classification levels – to be transmitted over a single physical cable. This eliminates the need for complex physical separation of network infrastructures as typically required in conventional systems. It also simplifies the creation of new domains without the need for additional hardware.

What is the multi-security domain cloud?

The NSC can operate multiple isolated networks or security domains for different classification levels on a single hardware platform. The L4Re Secure Separation Kernel ensures strict separation between domains. This capability has been approved by the German Federal Office for Information Security (BSI) for classification levels up to SECRET.

Can data be exchanged between the security domains?

Yes. Structured data can be exchanged via SDoT (Secure Domain Transition) Gateways. These gateways enforce strict rule-based controls during transmission. Unstructured data – such as Word, Excel or other files – must be pre-labelled in accordance with security policy before being transferred via an SDoT. Email communications can also be securely exchanged in this way. All components are BSI-approved up to the classification level SECRET.

How is the concept of "Security Domain as a Service" implemented in the NSC?

The NSC relies on physical-equivalent separation, which is primarily implemented via software or flexibly configurable hardware components. This makes it possible to create security domains quickly and without the need for additional hardware. Many components are either already approved by the BSI for use up to the classification level SECRET or are based on hardware appliances certified to the same level.

To what extent is the NSC NATO-compatible, for example with Federated Mission Networking (FMN)?
The NSC's Platform as a Service (PaaS) is based on more than 14 years of experience in developing NATO-compliant cloud applications, aligned with the FMN spiral development framework. One example of this is the federated identity management concept, which enables different NATO partners to collaborate securely and efficiently during joint missions.

Can I run my existing applications on the NSC?
The NSC uses Kubernetes, which has become de facto standard for modern applications. Containerised applications can be deployed on the NSC with minimal effort. Additionally, under certain Linux distributions (Ubuntu, Red Hat Enterprise Linux), legacy applications that do not support containerisation can also be provisioned as virtual machines within a domain, if necessary.

How does the architecture of the NSC differ from conventional clouds?
Every cloud requires a hypervisor for virtualisation and resource orchestration. In contrast to conventional clouds, the NSC relies on a modular, microkernel-based hypervisor. The Trusted Computing Base (TCB) – comprising the software and hardware that must be trusted – differs significantly between the NSC and traditional clouds. Conventional clouds rely on monolithic hypervisors with millions of lines of code, whereas the TCB of the NSC's L4Re Hypervisor consists of only around 30,000 lines of code.

This much smaller code base enables complete evaluation and verifiability, while reducing vulnerabilities and susceptibility to errors.

How is BSI-compliant operation possible with Virtual Security Functions (VSF)?
A Virtual Security Function (VSF) is an independent software component that can be instantiated flexibly and dynamically on an NSC system as needed. Examples include secure network transitions with labelling services or cryptographic components. VSFs can be supplied by different providers and are integrated independently.

They operate directly on the L4Re Hypervisor, which guarantees secure isolation. When a security domain is created, VSFs are launched according to its requirements, providing security functions either within the domain or between domains.

How can the NSC be operated securely with regard to hardware risks such as Spectre and Meltdown?
The NSC architecture includes all necessary protective measures to mitigate these hardware vulnerabilities. The domains are structured to minimise the shared utilisation of resources between domains, significantly reducing the risk of attacks such as Spectre or Meltdown.

Q&A: VS-Workstation

What are the advantages of a digitally sovereign workplace for public authorities?

Security: By retaining full control over their data and IT infrastructure, public authorities can better manage security risks and strengthen their defences against cyberattacks.

Independence: Reduced reliance on international IT providers enables public authorities to define and execute their IT strategies independently and in accordance with national priorities.

Data protection: Compliance with national and European data protection laws is simplified, as data is stored and processed exclusively within the organisation's own jurisdiction.

Cost control: Open-source solutions are often more cost-efficient and reduce both licensing fees and long-term operational expenditure.

Why do authorities use open-source software instead of the familiar standard solutions?

Authorities are increasingly adopting open-source software due to its transparency and controllability. This reduces dependence on proprietary solutions from major international IT companies. With open-source software, authorities retain control over both software and hardware components, enabling them to implement changes and close security gaps independently.

What does the term "data sovereignty" mean?

Data sovereignty means that data is stored and managed in national or private data centres instead of foreign cloud services. This ensures protection against unauthorised access. In addition, strict security and data protection standards safeguard the IT infrastructure from cyberattacks, including regular security assessments and audits.

What aspects of a "workplace" are covered by the VS-Workstation software?

The VS-Workstation already supports communication within a domain via chat, video conferencing, e-mail and file sharing. Additionally, SDoT Security Gateways enable file transfers and e-mail communication across security domains.

Can I work on files together with the VS-Workstation?

Yes. Within a domain, common Office file formats (documents, spreadsheets, presentations) can be collaboratively edited in real time via a web browser. Files can then be securely transferred between domains directly within the same application.

What is the purpose of the VS-Registry?

The VS-Registry (classified document registry) is a core component of information security management – especially in environments where sensitive or classified information is processed. It ensures the protection of such information, supports compliance with legal regulations and helps mitigate associated risks.

Can the VS-Workstation be used for collaboration with international partners?

The VS-Workstation is designed to support all classification levels used in Germany (VS-NUR FÜR DEN DIENSTGEBRAUCH to GEHEIM) as well as the corresponding NATO classifications (NATO RESTRICTED to NATO SECRET).

In addition, the "Releasable to" designation allows classified documents to be shared with selected partner organisations, provided that the appropriate domain transition has been configured.

How is it ensured that no SECRET-classified data is transferred to a lower-classified security domain?

Before a document can be transferred from a higher to a lower classification domain, it must be assigned a label. This labelling process must be initiated by an authorised person who selects the appropriate classification level. If a document is labelled as SECRET, the SDoT Security Gateway blocks any transfer to a lower-classified domain. Documents without a label cannot be transferred to lower domains at all.

Can the VS-Workstation be connected to existing identity and access management systems?

Yes, the VS-Workstation applications use Keycloak, an open-source solution for identity management. This allows existing systems to be integrated via LDAP, other identity providers or smart cards.

How are users' files managed in the cloud?

The foundation for file management is the widely adopted open-source product "oCIS" by ownCloud. This software is widely used across industry and public institutions (e.g. Mercedes, Bayercloud, CERN) for enterprise-level file management and scalability. Accordingly, features like versioning, automated backup and other enterprise capabilities are also available in the VS-Workstation.

Outlook – Shaping Security Together

We regard the Classified Information Directive (VSA) as a key driver of innovation. For us, this means continuous advancement. With ongoing technical refinements and new developments, we aim to stay ahead of future cyber threats. Our objective is not only to comply with security standards, but to strengthen and actively shape them.

Focusing on User Requirements

For us, IT security and digital sovereignty – and thus the ability of the state and society to act – clearly take precedence over superficial "look and feel". Our partner network of trusted German companies, using approved components, already demonstrates how the demanding requirements of the VSA can be met constructively, resource-efficiently, transparently and in a verifiable manner – even beyond the VS-NfD/RESTRICTED level.

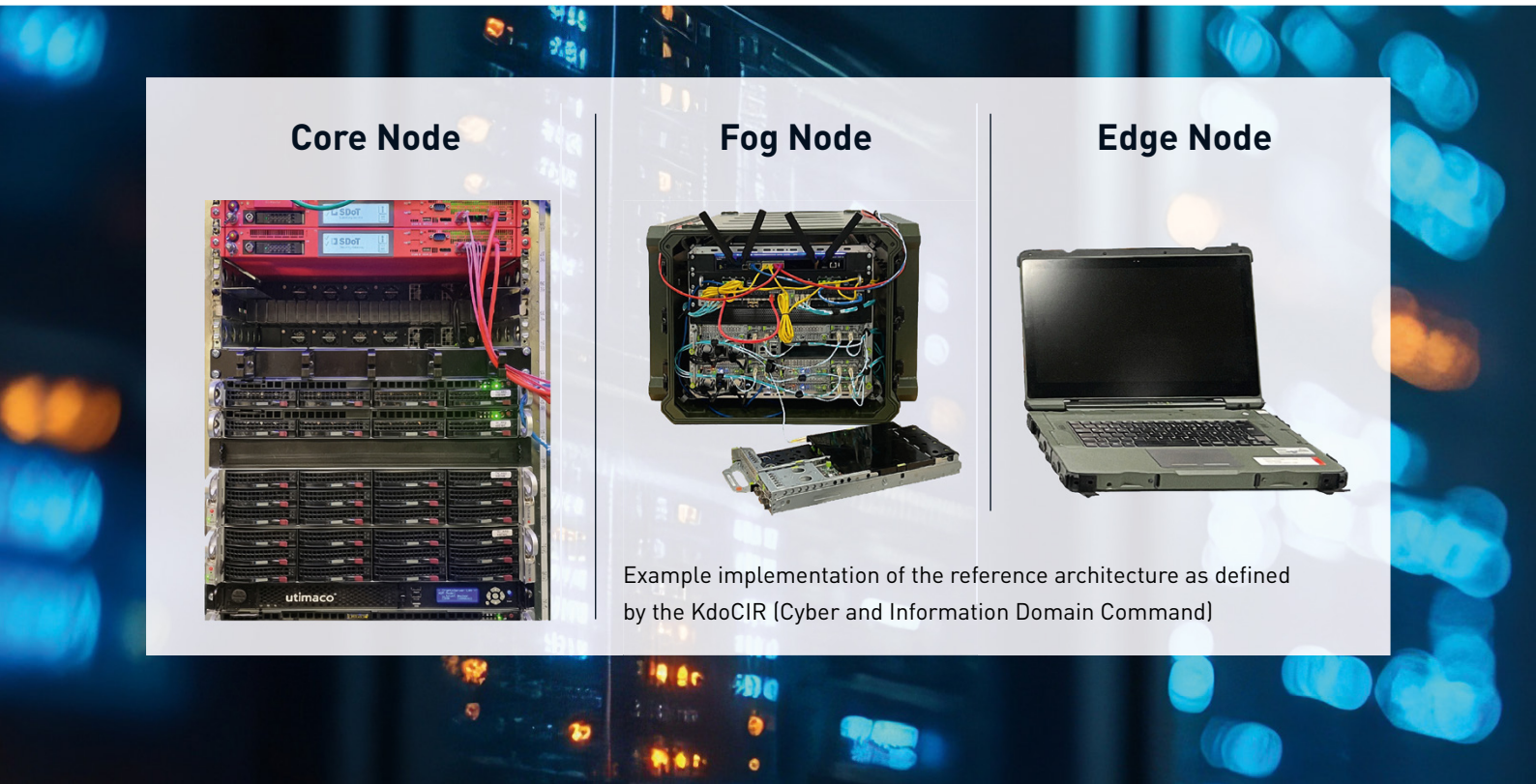
We also show that a VS-enabled workstation can withstand the demands of modern digital collaboration, while enabling secure exchange, dialogue and communication – all without dependency on major software providers.

This ensures that users avoid falling into the trap of vendor lock-in.

We understand that the separation of hardware and software is the path forward. Our modular approach allows for the straightforward integration of third-party solutions. If their software is Kubernetes-compatible, much of the groundwork is already done.

Authorisation procedures place high demands on all stakeholders. Focusing on the triangle of users, approval authorities, and service providers is key to achieving and maintaining IT security and digital sovereignty for Germany, with an emphasis on re-source-efficient and cost-effective implementation.

With the NSC Demonstrator, MDCC scenarios can be trialled today in the context of MDO, demonstrating their added value.



Example implementation of the reference architecture as defined by the KdoCIR (Cyber and Information Domain Command)

Seamless Integration of Emerging Technologies

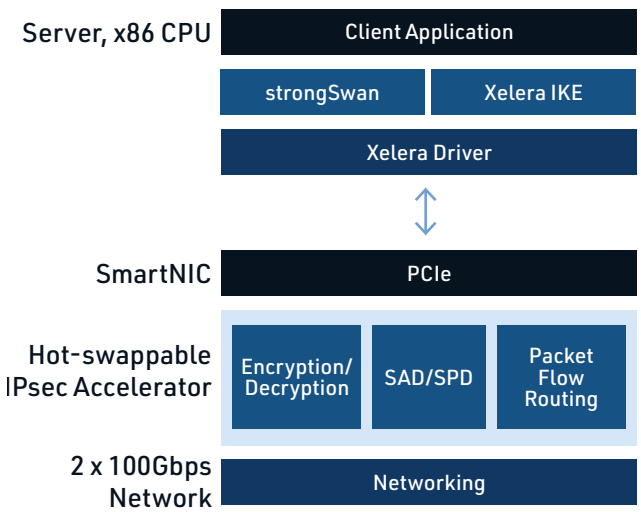
To further strengthen the NSC's scalability, flexibility and cost-efficiency, its development is structured in successive stages – some of which are already in progress.

One such stage is the integration of SmartNIC technology. Unlike conventional cloud solutions in approved security environments, SmartNIC enables logical separation between security domains on a single physical network infrastructure, eliminating the need for physically isolated networks. This completes the NSC's architectural principle of operating multiple security domains on a single hardware platform.

SmartNIC significantly enhances scalability and enables flexible domain management. With a data throughput of 100 Gbps, it delivers network and encryption performance comparable to modern commercial cloud infrastructures.

Thanks to its programmability, SmartNIC is a key component of the NSC's future security architecture – enabling functional upgrades without the need for hardware replacement. The integration is being realised in collaboration with Xelera Technologies GmbH.

SmartNIC structure: Zoom-in from Fig. page 13



Flexibility Through a Strong Partner Network

Our German partner network marks the beginning of an open and robust ecosystem – driven by the principles of modularity, flexibility and interoperability. Over time, certified IT security components that rely on hardware as a trust anchor are increasingly being replaced by software-based alternatives. The development roadmaps of our partners already point in this direction.

We are responding to the demand for a genuine, controllable "Security Domain as a Service". It enables dynamic setup and administration within minutes – instead of hours or days.

The Future of NSC is Dynamic

Today, the NSC is static and functional. It fulfils all certification requirements and forms a solid basis for securely supporting current scenarios in both civilian and military contexts. In the future, the NSC will evolve to become dynamic and extend its reach beyond Germany.

This evolution benefits administrators by allowing them to implement increasingly complex requirements efficiently and in a resource-conscious manner, while ensuring full compliance with all relevant security standards.

The consistent use of open-source software offers both flexibility and independence. Administrators are equipped to manage operations and defend against cyberattacks, while users, supported by the VS-Workstation, can focus on growing number of security-related tasks without being burdened by technical complexity. In short: we design security – together with public sector stakeholders and certifying authorities – building trust and acceptance every step of the way.

The Partner Companies of the NSC Programme

The National Secure Cloud (NSC) is being developed in close collaboration with a group of German companies. Each partner contributes specific capabilities to ensure that the solution meets the demanding requirements of the public sector, the military and regulated industries.

infodas
connect more. be secure.

infodas is one of Germany's leading providers of cyber and information security solutions. Since 2024, the company has been a subsidiary of Airbus. In addition to advising companies, government authorities and the armed forces, infodas develops high-security products for domain transitions and the protection of critical infrastructures. Its SDoT (Secure Domain Transition) product family is approved for handling information classified up to SECRET, EU SECRET and NATO SECRET. The products are certified in accordance with the Common Criteria and hold additional country-specific certifications.

The SDoT portfolio includes a range of security appliances for controlled unidirectional and bidirectional data exchange between networks or systems of varying sensitivity levels. It also supports the creation of NATO STANAG 4774/8-compliant, high-security labels for classified data. These capabilities are essential for secure data exchange in multi-domain cloud environments, enabling trusted collaboration between authorities or allied nations.

utimaco®

Utimaco plays a key role in meeting cryptographic requirements by providing a BSI-approved hardware security module (HSM), ensuring the physical protection of cryptographic keys used within the NSC. Optionally, Utimaco also offers client-side protection through hard disk encryption and "File and Folder" encryption, certified up to the VS-NfD classification level.

Utimaco is a global platform provider of trusted cybersecurity and compliance solutions. The company develops both on-premises and cloud-based hardware security modules, key management systems, data protection solutions and data intelligence tools – tailored for regulated critical infrastructures and public warning systems.

With over 40 years of experience in IT security, Utimaco ranks among the world's leading manufacturers in its core market segments. It is officially recognised by the BSI as a "qualified manufacturer" for hardware security modules.

INFODAS GmbH
Rhonestraße 2
50765 Köln

Benedikt Meng
Business Development
& Public Affairs
b.meng@infodas.de
+49 30 2060 3994 51
www.infodas.com

Utimaco IS GmbH
Germanusstraße 4
52080 Aachen

Nils Gerhardt
Chief Technology Officer
nils.gerhardt@
utimaco.com
+49 241 1696 232
www.utimaco.com

KERNKONZEPT

Kernkonzept specialises in highly secure operating system solutions and develops advanced virtualisation technologies for the NSC, based on the L4Re open-source operating system and the L4Re hypervisor. These technologies enable organisations to securely run multiple security domains with different classification levels on a single hardware platform.

The L4Re Operating System Framework is built on a microkernel architecture. This ensures strict separation between security-critical applications and standard processes, significantly reducing the risk of vulnerabilities. L4Re not only provides maximum flexibility and efficiency, it is also approved by the German Federal Office for Information Security (BSI) for handling data classified up to VS-GEHEIM and NATO SECRET. Additionally, the technology is certified according to Common Criteria EAL4+.

L4Re has been in use for over ten years in both security-critical and mission-critical environments.

FURTHER PARTNERS

XELERA provides high-performance AI and cybersecurity solutions for data centres and cloud environments. The company's core expertise lies in networking technologies and SmartNICs / DPUs, with a focus on optimising performance and cost efficiency. Xelera's innovative SmartNIC technologies are also integrated into the NSC programme.

mspaces has developed a digital workplace that combines office applications, email, video calls, team chats and video conferencing with real-time collaboration and file sharing. Within the NSC programme, this solution has been specifically adapted to meet the heightened security requirements of public-sector organisations.

INXIRE offers a digital VS-Registry for the creation and management of classified content. The software ensures secure collaboration and enables seamless, regulation-compliant handling of classified information – from creation through to processing.

Kernkonzept GmbH
Buchenstraße 16b
01097 Dresden

Dr. Michael Hohmuth
CEO
michael.hohmuth@kernkonzept.com
+49 351 41 888 611
www.kernkonzept.com

Xelera Technologies GmbH
felix.winterstein@xelera.io
www.xelera.io

mspaces
harald.weimer@mspaces.de
www.mspaces.de

inxire GmbH
toni.schnell@inxire.com
www.inxire.com

GLOSSARY

Data sovereignty
The ability to control one's own data. Users decide who may access their data, how it is used, and for what purpose it is processed.

Hardened system
An IT system that has been specifically secured by removing unnecessary functions and closing known vulnerabilities to increase its resilience against attacks.

Hypervisor (microkernel-based operating system)
Software that enables multiple virtual machines to run simultaneously on a single physical device by efficiently managing hardware resources. A hypervisor also enforces strict separation between individual domains.

Infrastructure as a Service (IaaS)
A cloud computing model in which IT resources – such as computing power, storage and networking – are provided as a service. Users are responsible for operating and managing their own applications on this infrastructure.

IoT (Internet of Things)
A network of physical devices embedded with sensors, software and connectivity, enabling them to collect and exchange data.

Security by design
An approach in which security features are built into the system or software from the earliest stages of development, reducing the risk of vulnerabilities.

Security domain
An isolated environment within an IT system that corresponds to a specific security level. Within the domain, strict access rules apply to all data processing activities.

Single-Sign-on (SSO)
An authentication method in which users log in once and subsequently gain access to multiple applications or systems without needing to re-authenticate.

SmartNIC
A specialised network interface card designed to offload network processing tasks from the server's CPU. SmartNICs can perform functions such as network compression and decompression, as well as encryption and decryption.

Software as a Service (SaaS)
A cloud computing model that provides software over the internet as a service. Users access the software via a web browser without the need to install it locally.

Classified information (VS)
Information and materials of any kind that must be protected from unauthorised access through special security measures. Depending on the required level of protection, they are classified by an official authority – or on its behalf – as STRENG GEHEIM (Top Secret), GEHEIM (Secret), VS-VERTRAULICH (Confidential) or VS-NUR FÜR DEN DIENSTGEBRAUCH (RESTRICTED) in accordance with the German Classified Information Directive (VSA).

The designation GEHEIM corresponds to the classification level SECRET and is recognised as the German equivalent of both EU SECRET and NATO SECRET. German SECRET is the foundation for accreditation in both EU and NATO SECRET classification levels.

VS data
Classified information that is presented or processed in a specific format for machine processing or originates from such processing. This includes, for example, data stored on USB sticks, hard drives or similar media.

Further information:
Public sector – IABG

IMPRINT

Responsible
Industrieanlagen-Betriebsgesellschaft mbH
85521 Ottobrunn
Tel.: +49 89 6088 0
info@iabg.de
www.iabg.de

Content
Industrieanlagen-Betriebsgesellschaft mbH
Einsteinstraße 20
85521 Ottobrunn

INFODAS GmbH
Rhonestraße 2
50765 Köln

Kernkonzept GmbH
Buchenstraße 16b
01097 Dresden

Utimaco IS GmbH
Germanusstraße 4
52080 Aachen

Xelera Technologies GmbH
Rheinstraße 40-42
64283 Darmstadt

Security is non-negotiable.

www.iabg.de