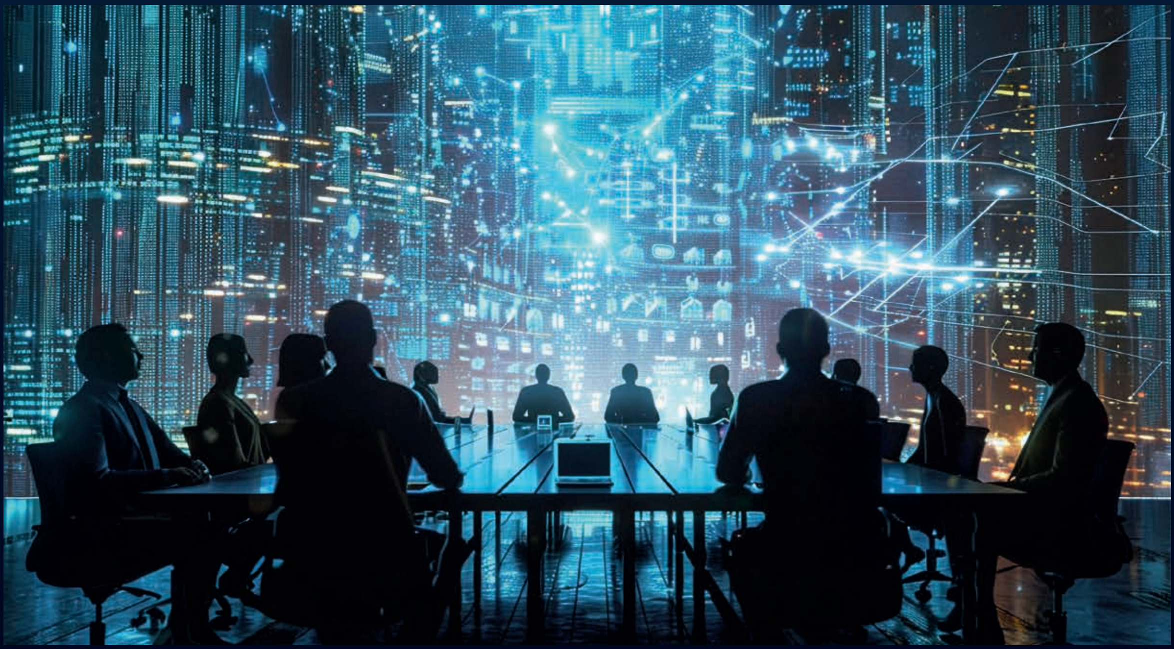
NATIONAL SECURE CLOUD

NSC and VS-Workstation – Your Partner for Maximum IT Security

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

IABG | infodas | KERNKONZEPT | utimaco® | XELERA

TABLE OF CONTENTS



IABG – We Shape IT Security

IABG has been ensuring the safety and security of the state and society for over six decades. Our unwavering goal: to stay one step ahead by anticipating the future. This commitment also extends to Germany's digital sovereignty. In partnership with dedicated German companies, we have therefore established the National Secure Cloud (NSC) programme.

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

Within the NSC programme, IABG defines the overall hardware and software architecture for a secure Infrastructure-as-a-Service (IaaS) and ensures secure management of Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) solutions, including seamless 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 IT Security Without Compromise

Critical IT infrastructure in public authorities and military facilities requires the highest IT security standards. Particularly in times of increased cyber attacks and growing international connectivity, these organisations require secure working environments, cloud solutions that not only meet strict confidentiality and data protection requirements but also align with Germany's digital sovereignty. The foundation for a solution that meets all requirements lies in the National Secure Cloud (NSC) and the VS-Workstation – both developed by a consortium of trusted German IT companies, led by IABG.

Our Solutions: NSC and VS-Workstation

The NSC is a highly secure cloud infrastructure capable of processing data across multiple security levels simultaneously. It meets the stringent requirements of the Classified Information Directive (VSA). A key feature of the NSC is the separation of security domains, allowing several levels of protection to be managed on the same hardware – ensuring high cost-efficiency. The NSC leverages open-source technologies to provide transparency and traceability. This open architecture reduces reliance on proprietary technologies from international providers – the so-called hyperscalers – while enabling simple customisation to meet specific requirements.

The National Secure Cloud

- → Highly secure cloud infrastructure designed to meet the stringent requirements of the German Federal Office for Information Security (BSI).
- → Security domains and secure domain transitions, tailored for public authorities and military applications.
- → High performance, interoperability and scalability.

The VS-Workstation complements the NSC by providing a secure working environment. As with the NSC, the focus is on open-source solutions that support digital sovereignty. These solutions are specially tailored to meet the needs of organisations with high security requirements.

Mechanisms such as access controls and encryption safeguard the confidentiality and integrity of data, while protection against malware and unauthorised access ensures robust security. The VS-Workstation is designed for processing classified information up to the classification level SECRET (DE GEHEIM, EU SECRET, NATO SECRET).

The VS-Workstation Features

→ Modular solution built on European open-source applications.

→ Scalable for large organisations with thousands of users.

→ Capable of processing classified information up to the classification level SECRET.

→ Compatible with ZenDiS openDesk.

Security and Technical Features

The NSC combines software, services and security hardware specifically developed for cloud applications. It utilises a BSI-approved hypervisor to manage multiple security domains on a single piece of hardware. The strict separation of domains ensures maximum security, enabling data to be processed up to classification SECRET.

Special security mechanisms facilitate data exchange between different security domains – also up to classification SECRET – while cryptographic hardware security modules provide robust protection against unauthorised access and usage.

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 users to continue working with their current software. The modularity of these systems also supports the integration of the new technologies, such as artificial intelligence (AI).

In the military sector, the systems can operate autonomously without a network connection if required, even in confined spaces. They also ensure a high level of interoperability with alliance partners, for example, in NATO operations.

The NSC and the VS-Workstation are modular, highly secure and flexible solutions that can be tailored to diverse requirements. This makes them the ideal tools for authorities, military facilities and other security-critical organisations in Germany.

Targeted: Daily Attacks on German Government Networks

- → The BSI detects 250,000 new malware variants every day.
- → The Federal Administration alone receives an average of 775 emails containing malware daily.
- → Each day, the BSI blocks government network users from accessing 370 websites.

Download PDF:
The State of IT Security in
Germany 2024

Examples: Cyber Espionage and Attacks Targeting the Public Sector

- → SolarWinds supply chain attack that affected several US government agencies and other organisations worldwide (2020).
- → Attack on the civilian business operations of the Rheinmetall defence group (2023).
- → Russian military intelligence service attack on Germany's SPD political party headquarters and a defence company (2024).
- → Cyber attack – reportedly originating from China – on the British Ministry of Defence (2024).
- → CDU party central office IT infrastructure taken offline following a cyber attack (2024).

This small selection of global incidents from recent years alone illustrates the ongoing threat of cyber espionage and attacks targeting diplomatic communications and sensitive information. Common attack vectors include phishing, malware and supply chain compromises.

Two Attacks on Public Sector IT

1. **Chambers of Industry and Commerce IT Service Attack (2022):**
   On 3 August 2022, the IT service provider for Germany's chambers of industry and commerce detected unusual activity in its systems and initiated a shutdown to prevent damage. This action disconnected all 79 CCIs in Germany from the internet, taking websites offline and making email communication impossible. Internal applications were also affected. After thorough testing, systems were brought back online, although some chambers remained affected for months.

2. **Ransomware Attacks on Municipal Administrations (2022–2023):**
   Between 2022 and 2023, ransomware attacks targeted 27 municipal administrations and businesses of various sizes. The affected entities ranged from a small community of 2,800 inhabitants to a major city with a population of over 1.8 million. The attacks targeted city and district administrations, local transport providers, energy suppliers, housing associations, city cleaning companies and a school authority.

Digital Sovereignty with the National Secure Cloud

The development of the National Secure Cloud (NSC) addresses the current discussions surrounding digital sovereignty and state IT security. Authorities and armed forces, in particular, handle classified data daily in line with the Classified Information Directive (VSA) and require a high degree of sovereignty. The NSC is a cloud solution specially tailored to these protection needs. 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 central idea was a cloud solution developed in Germany, for Germany, that fulfils two tasks: firstly, to strengthen digital sovereignty and secondly, to be verifiably more secure than conventional cloud solutions.

The well-known international providers often do not fulfil the very high requirements of the VSA beyond RESTRICTED. Due to the complexity and architecture of these solutions, the level of security is only verifiable or measurable to a limited extent. This makes the authorisation/accreditation (e.g. by the BSI) of such solutions extremely difficult.

That's why we have developed our components in such a way that users not only have full control over their data, but that "authorisation capability", for example by the BSI, is also feasible. At the same time, the highest security standards can always be maintained. We rely on open-source software, a comprehensible architecture that is as standardised as possible and a manageable development roadmap to guarantee a high and, above all, measurable level of security and digital sovereignty.

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

The greatest challenge is the protection of classified data in the face of increasing digitalisation, collaboration and networking, including communication between authorities and military institutions (national and international). To this end, IT systems and new technologies must be harmonised with the VSA. However, even here, it is almost impossible to provide 100% protection.

Despite all the challenges, public authorities must ensure that they remain capable of acting and keeping up with technological developments. To this end, it is necessary to efficiently and quickly utilise the advantages of new technologies, such as artificial intelligence or the Internet of Things (IoT).

This will at least mitigate the consequences of demographic developments and the resulting shortage of skilled labour. The aim is to establish stable and secure communication relationships in increasingly complex networks of devices, as well as services and manage the growing volume of data.

Users, whether in administration or processing, require straightforward and user-friendly solutions. The challenges they face are often already complex enough and IT systems or applications must not add unnecessary complications.

At the same time, the solutions offered must remain affordable and feasible within the constraints of state budgets. This is especially critical in the current climate of tight fiscal conditions.

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 demand secure and cost-effective solutions for managing VS data. These systems must facilitate interaction within their own departments, with citizens and with other authorities – all while ensuring compliance with GDPR and VSA regulations. Cross-departmental data exchange, such as between the police and the judiciary, is one example of this need.

Certain state actors, like the Ministry of Foreign Affairs, require the ability to process classified information worldwide. Additionally, their systems must offer spatial flexibility, enabling mobile solutions such as the "Mobile VS-Workstation".

In the military sector, the requirements for security and confidentiality remain consistently high. Functionality is particularly complex due to the wide range of weapons and command and control systems, many of which are proprietary and hardware-based. In these cases, it is essential to gradually decouple software from hardware, with further standardisation being particularly beneficial, especially within the NATO framework. Another critical requirement is the ability to deploy systems quickly in emergencies and ensure autonomous functionality without a network connection. Interoperability with alliance partners, such as during NATO's multi-domain operations, is equally critical.

Nearly all target groups require solutions that save space and resources. The ability to securely transfer data between IT systems with different security classifications is also crucial. It is just as important that the system is highly flexible. After all, new applications or updates must be available in the shortest possible time, not just in response to crises.

Synopsis: State actors need IT systems that are user-friendly, flexible, resource-efficient, scalable, autonomous, interoperable and compliant with all national and international security standards. Certainly not an easy task, but this is precisely where the inherent advantages of cloud technologies prove their worth – provided they are enhanced to meet VS-IT or VSA compliance requirements. This is exactly what we deliver in collaboration 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 harmonise perfectly, offer several distinct advantages over other solutions. Firstly, 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 realistic and secure solution that meets these needs in a relatively straightforward manner.

Ultimately, this is about building an ecosystem: other manufacturers and providers are encouraged to integrate their solutions into the "overall NSC system". This approach enhances both security and sovereignty. Both the NSC and the VS-Workstation are designed from the ground up to meet the highest security standards. This principle is best captured by the phrase "security by design". In practice, this means we prioritise VSA-compliant security before addressing the aspects like "look & feel".

The NSC relies on components that are already approved by the BSI and are continuously being developed further. We are moving forward step by step, balancing performance, security and authorisation capability.

This makes the NSC and VS-Workstation the ideal starting point for implementing diverse user application scenarios and achieving BSI approval.

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 administrations)**
  Digital and data sovereignty are top priorities for governments and their subordinate authorities. Avoiding vendor lock-in is equally critical. 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 is equally critical in a military context. Additionally, international standards, such as those established by NATO, must be strictly adhered to. Consequently, the technical requirements for military organisations are significantly higher than for civilian applications. The NSC technology stack fulfils all these requirements. Current developments show that the German Federal Armed Forces (Bundeswehr) are already using the ZenDiS solution openDesk. The VS-Workstation is the ideal complement, offering full compatibility 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 conception to authorisation – is essential to safeguarding intellectual property and ensuring a return on investment.

Perhaps two more technical examples: our hypervisor enables multiple security domains to run on a single piece of hardware, saving both costs and space. By virtualising security functions, we also allow customers to adapt flexibly to changing requirements. This is because deploying software is much easier than modifying hardware.

Our open secret is a blend of innovative technology, philosophy and structured communication with relevant stakeholders – because success can only be achieved together. As I mentioned earlier: it's 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 focus on open-source software, which offers greater transparency and control. This reduces reliance on proprietary solutions from large international IT companies.

- **Data sovereignty:** Data is stored and managed in national or private data centres rather than foreign cloud services. This protects the data from unauthorised access by third parties.

- **Security standards:** Strict security and data protection standards are implemented to protect IT infrastructure from cyber attacks, including regular security checks and audits.

- **Interoperability: S**ystems and applications are designed for compatibility and seamless data exchange. This fosters efficiency and collaboration between different authorities and departments.

- **Control over software and hardware:** Authorities maintain full control of their software and hardware, enabling them to make adjustments and close security gaps without relying on external providers.

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

  Security: By taking control of their data and IT infrastructures, governments can more effectively manage risks and strengthen their defences against cyber attacks.

  Independence: Reduced reliance on international IT providers gives public authorities more freedom to shape their IT strategies independently.

  Data protection: Compliance with national and European data protection laws is made easier by keeping data stored and processed within the company's own territory.

  Cost control: Open-source solutions often incur fewer licence fees and provide long-term cost savings.

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 users with customised security solutions to meet their individual requirements. Whether for public authorities or the military, each user receives a solution precisely tailored to the specific deployment scenario in terms of functionality and security.

Available modules include a secure cloud management platform, software-as-a-service (SaaS) solutions, cryptographic security solutions and much more – all based on European open-source applications. The modularity of the NSC also enables the integration of new technologies and applications such as AI language models or machine learning. The cloud can be expanded as needed to accommodate 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 offers a minimal attack vector 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 to encrypt data or create certificates, without ever leaving the highly secure environment of the HSM. Moreover, the hardware security modules used are future-proof and can be upgraded to include post-quantum cryptography (PQC) if needed.

Security Domains and Secure Transitions

The NSC enables the creation of security domains where authorities or NATO nations, for example, can maintain control over their data sovereignty, processing and storage independently. In addition, the NSC allows multiple security domains to operate on the same server hardware while keeping them securely separated – up to the classification level SECRET.

Each domain has specific security protocols and access controls designed to prevent information from crossing domain boundaries without proper authorisation. This strict separation ensures that confidential data from military or state organisations remains protected against unauthorised access.

In the past, physically separate systems were required to achieve this level of security. With the new technologies, however, it is possible to operate several security domains in encrypted form on a single hardware platform.

For bidirectional data exchange between different security domains, the NSC employs SDoT (Secure Domain Transition). "This allows structured and unstructured data to be exchanged between the different security domains, even up to the classification level SECRET," explains Benedikt Meng from NSC partner infodas. This capability is particularly important in an international context, such as cooperation between NATO member states. For example, data from a NATO SECRET domain can be securely transmitted to partner countries.

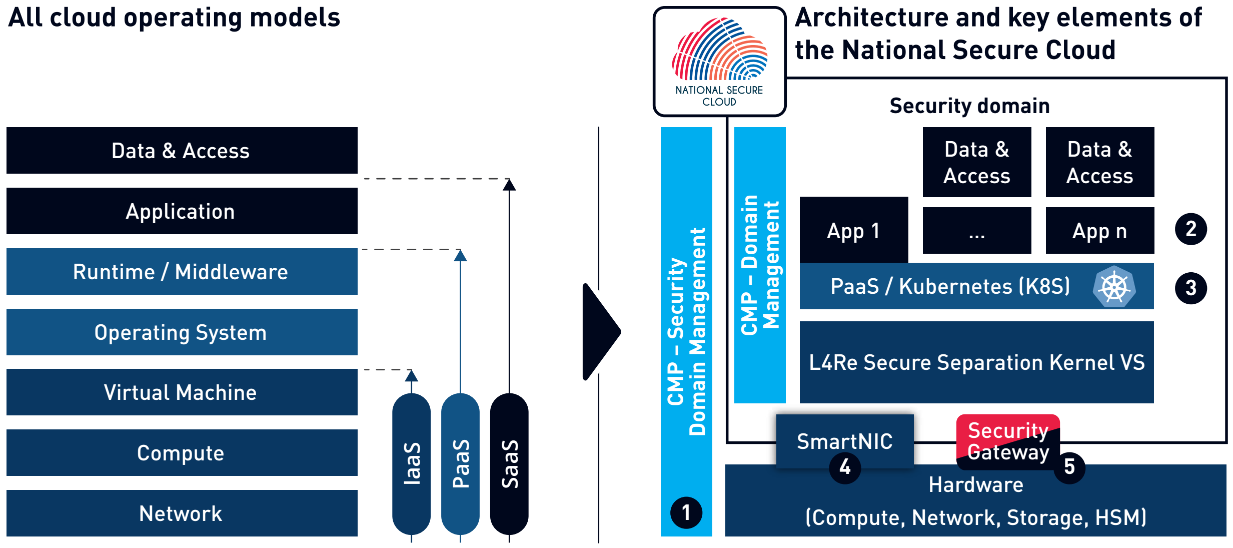
High Interoperability and Scalability

"In addition to the high security standards, the NSC offers interoperability in military and international environments, as it is based on standardised and widely used 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, allowing the cloud system to adapt quickly to different needs and application scenarios – even at short notice during time-sensitive peak loads.

As a cloud platform, the NSC supports applications from various providers. This enables users to continue using their existing, often expensive software, thereby safeguarding their investments. However, it is recommended to transition to the VS-Workstation (see next chapter), which is fully harmonised with the NSC. This transition simplifies the often-confusing variety of software used within organisations, resulting in greater efficiency and enhanced security.

Modular and Highly Secure: The VS-Workstation in Detail



1 Two-level management
2 Basis SaaS catalogue, e.g. VS workstation 3rd party
3 IABG PaaS with Kubernetes
4 SmartNIC for performance and security
5 Security gateway for the domain transition

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). Its range of functions aligns with the standard office products offered by major technology companies. SaaS means that the software is not installed locally on a computer. Instead, it is located in the cloud and 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 generally accessible via the 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.

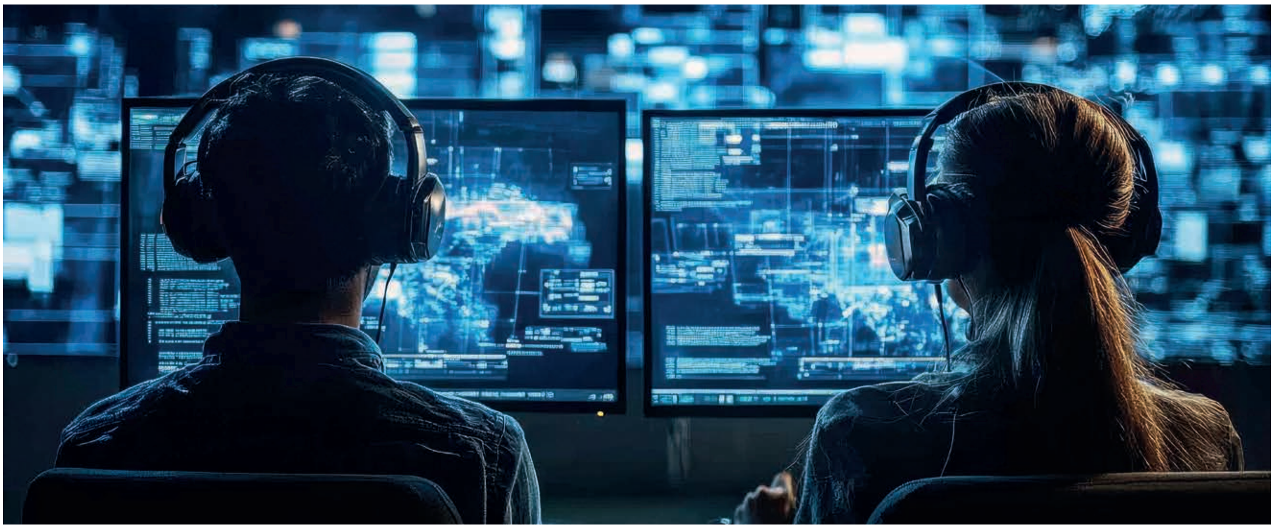
- "Modular" means that the solution integrates well-known European open-source applications (particularly from ownCloud and mspaces) whose functionality aligns with standard solutions available on the market. Where necessary, services from other companies are also integrated.

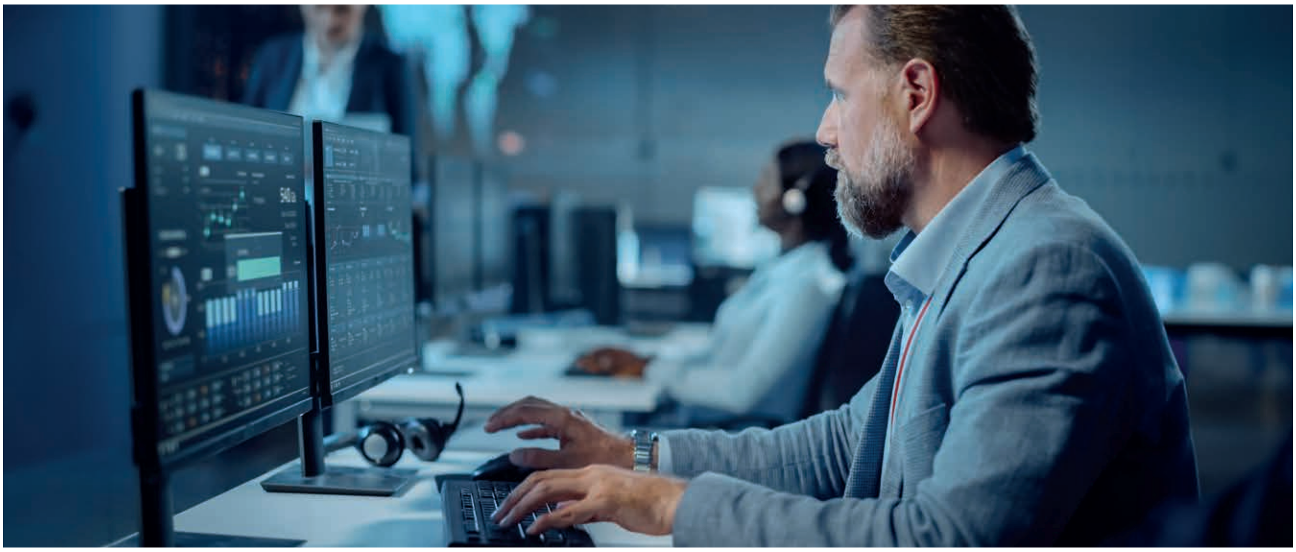
- "Scalable" means that the modules of the VS-Workstation can be deployed individually for virtually any number of users. The VS-Workstation is therefore suitable even for large organisations with many thousands of users.

- "Highly secure" means that the VS-Workstation isdesigned to handle classified information up to classification level SECRET and complies with all corresponding BSI requirements.

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

Synopsis: The VS-Workstation offers all the usual functions of modern office solutions and at the same time guarantees the protection of national interests.





Access to the VS-Workstation

The VS-Workstation is intended for use in a browser running on a BSI-certified, highly secure operating system. This system is hardened with IT security measures, just like the laptops or desktop PCs certified for use in public authorities.

Accessing the VS-Workstation is simple: users can either click on a provided link in their browser or manually enter the URL into the address bar. A central portal then opens, granting access to all functions and modules.

To ensure only authorised users access the portal, it is secured by an Identity and Access Management (IAM) system. This system allows access exclusively to users registered as authorized,based on their login credentials. User rights differ depending on authorisations, ensuring that not everyone can access every module or document area. For example, users who are not authorized to edit classified documents do not have access to the relevant documents nor to the necessary functions.

Users accounts and authorisations are managed within a central directory service, which is an integral part of the VS-Workstation. This service is based on the open-source software Keycloak.

Among its numerous convenience features is single sign-on (SSO), enabling users to log into the VS-Workstation once and automatically gain access to all other applications. There are also integrated user self-services. These allow each user to configure their profile and working environment themselves – independently, without requiring support assistance.

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 files. 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 authorised users, either as read-only or with editing permissions – making it possible to collaboratively work on one document.

For these purposes, the integrated Office solution, detailedin the following pages, is utilised.

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 intended for all users are stored.

The service is built on the modules from the open-source solution ownCloud and includes an integration of the Office solution, which is a core component of the VS-Workstation.

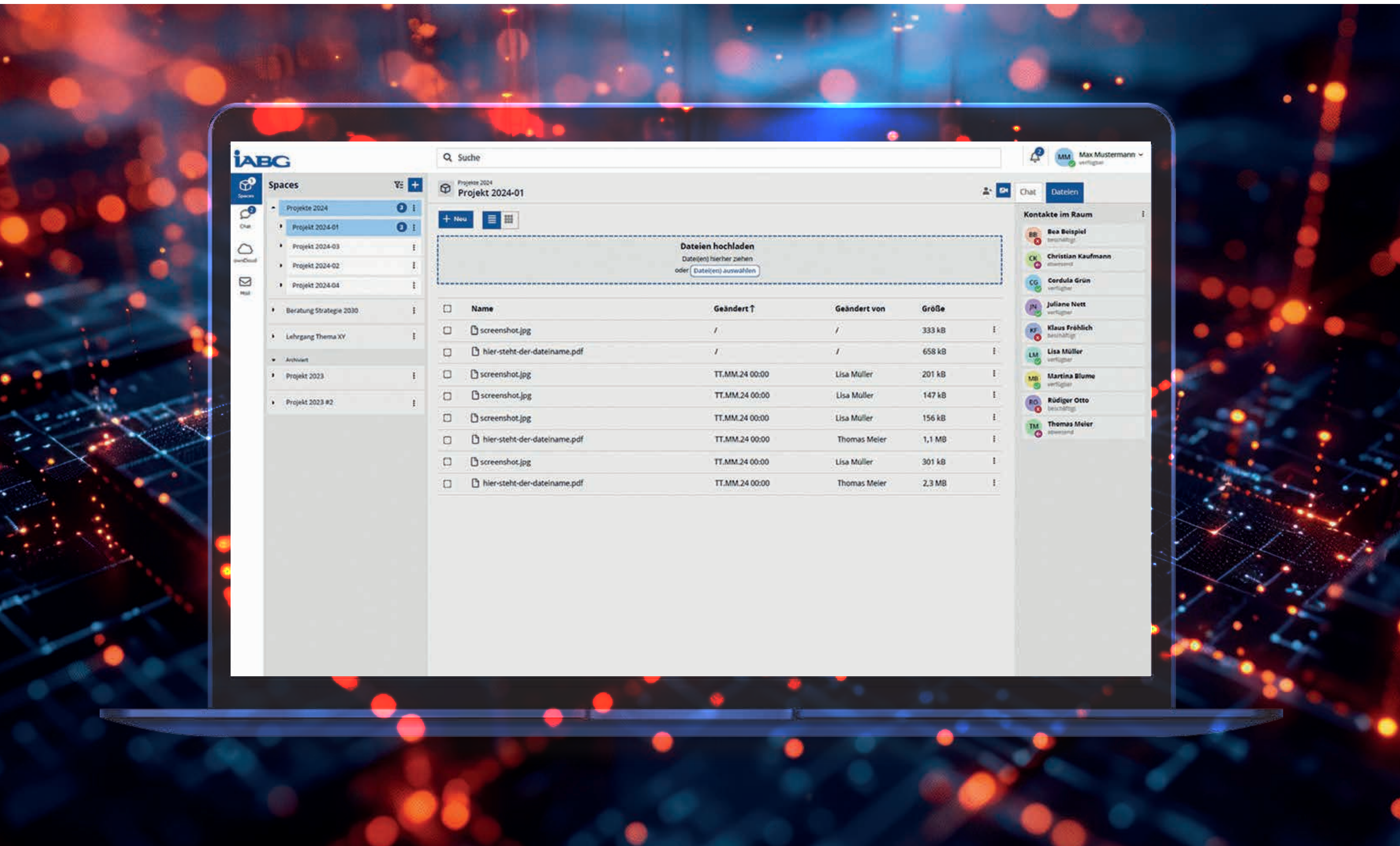
Digital Collaboration with VS Video and Chat

Video conferences and chats are core features of modern office solutions and the VS-Workstation's Collabora Office fully integrates them. Within a domain, users can host video and audio meetings with unlimited participants, including the ability to share their screen. This makes it easy to present slides, review spreadsheets or collaborate on documents in real time.

Additional tools allow users to exchange files and work together on a digital whiteboard. These capabilities are enhanced by an integrated text chat feature that connects all VS-Workstation users, ensuring smooth and efficient communication. This digital collaboration function is located within the VS-Realtime module, accessible exclusively through a secure browser.

The Core of the VS-Workstation: VS Office Collabora

The core module, VS Office Collabora, is a comprehensive office application that uses VS-Drive to store its documents. It includes all the standard tools for text processing,spreadsheets and presentations. These applications are designed to closely resemble familiar standard Office solutions, offering a similar user interface and range of functions to ensure an intuitive user experience.



☐	Name	Geändert ↑	Geändert von	Größe
☐	screenshot.jpg	/	/	333 kB
☐	hier-steht-der-dateiname.pdf	/	/	658 kB
☐	screenshot.jpg	TT.MM.24 00:00	Lisa Müller	201 kB
☐	screenshot.jpg	TT.MM.24 00:00	Lisa Müller	147 kB
☐	screenshot.jpg	TT.MM.24 00:00	Lisa Müller	156 kB
☐	hier-steht-der-dateiname.pdf	TT.MM.24 00:00	Thomas Meier	1,1 MB
☐	screenshot.jpg	TT.MM.24 00:00	Lisa Müller	301 kB
☐	hier-steht-der-dateiname.pdf	TT.MM.24 00:00	Thomas Meier	2,3 MB

BB	Bea Beispiel	beschäftigt
CK	Christian Kaufmann	abwesend
CG	Cordula Grün	verfügbar
JN	Juliane Nett	verfügbar
KF	Klaus Fröhlich	beschäftigt
LM	Lisa Müller	verfügbar
MB	Martina Blume	verfügbar
RO	Rüdiger Otto	beschäftigt
TM	Thomas Meier	abwesend

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-Drive	**Data Platform**	MS oneDrive
VS-ID	**IDM**	AD/LDAP
VS-Base	**Integration Layer**	GraphAPI
NSC (Linux/Windows)	**Platform**	Windows

The Office module of the VS-Workstation supports both the individual document editing and real-time collaboration among multiple users.

Documents can be edited by anyone with write access to the corresponding file. The applications are compatible with Microsoft Office formats (.docx, .xlsx, .pptx) and Open Document Format (ODF). Collabora also supports many other file formats such as .txt, .rtf, .html, .jpg, .png, .gif, .mp4, .webm and .pdf.

The module is based on the open-source cloud solution Collabora Office, which in turn is based on the open-source package LibreOffice, and has been enhanced with collaboration features.

Equipped for the Future: VS-AI

The next version of the VS-Workstation will feature the VS-AI module, which expands its functionality with a locally deployable language model such as the open-source model Mistral. The language model is contextually enriched by an additional local knowledge base while remaining exchangeable. It enables features such as automatic 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 complexity of administrative processes. Overall, the solution creates a robust foundation for the digital transformation of public administrations while fostering opportunities for innovative advancements.

The VS-Workstation is offered as part of the NSC, or as a stand-alone product, available in two subscription variants: on-premises and as SaaS.

- → **Lower initial investment:** No high upfront costs, but manageable monthly or annual payments.
- → **Always the latest software:** Users always have access to the latest features and security updates.
- → **Flexibility:** Subscriptions can be scaled or customised as needed.
- → **Technical support:** Continuous access to technical support and assistance with any 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 examples for various scenarios to minimise the effort required. For a simple cluster, only a few configuration values need to be modified.

How does the NSC ensure federated identity management?

The NSC integrates identity management using Keycloak. As middleware, Keycloak connects multiple identity providers in the background, ensuring a transparent experience behind a unified login interface for all cloud offerings. Combined with a hardware security module (HSM) and smartcards, logins can also be linked to hardware-based solutions.

How is security for cryptographic requirements guaranteed in the NSC?

Comprehensive security solutions are provided, including a BSI-approved hardware security module for all cryptographic requirements. Client-side protection is also available through hard disk encryption and "File and Folder" encryption, meeting standards up to RESTRICTED.

How does the NSC guarantee scalability?

Horizontal stability is achieved using standard Kubernetes techniques, such as the Horizontal Pod Scaler, which enable seamless scaling without manual intervention. Vertical scalability involves expanding resources such as memory, processors or network units.

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

Many components are designed to be crypto-agile and can already be upgraded with post-quantum algorithms. Once these components are approved by the BSI, the NSC is prepared to remain progressive and quantum-safe.

How can you ensure geo-redundancy with the NSC?

For reliable geo-redundancy, three Kubernetes container clusters are required, operated at different locations. This includes a "Watchdog" process that switches the routing of the IP numbers should one of the clusters fail.

The data centres can remain small, as the NSC solution allows multiple security domains to operate on a single server.

This enables rapid deployment of data centres and quick instantiation of SECRET domains.

Why do I need two CMPs to administer the NSCs?

To ensure that the individual domains remain separate, domain administration is conducted within the respective domain for security reasons. Each domain requires its own cloud management platform (CMP). Additionally, a higher-level management system is used to create and manage individual domains.

How do you ensure multi-client capability?

The entire solution is designed with multi-client capability in mind. The logical encapsulation of Kubernetes clusters ensures that applications from different users operate completely independently. This extends to the clients, which are run on encapsulated virtual machines.

How do you achieve homogeneity in operations across multiple locations using the NSC?

across cloud computing, fog computing and edge computing. This standardization simplifies administration regardless of the size or scope of the infrastructure at any location.

What advantages can be achieved by using a SmartNIC at admin level?

SmartNIC technology allows data from multiple security domains, even with different classifications, to be transmitted over a single physical cable. This eliminates the need for a time-consuming physical separation of the entire network infrastructure for different domains, as required with conventional solutions. It also simplifies the creation of new security domains without the need for additional hardware.

What is the multi-security domain cloud?

The NSC is able to run multiple isolated networks or domains for different security levels on a single hardware platform, securely separating them using the L4Re Secure Separation Kernel. This has been approved by the BSI for classification levels up to SECRET.

Can data be exchanged between the security domains?

Yes, structured data can be exchanged between security domains via SDoT Security Gateways. These gateways verify data based on predefined rules. Unstructured data – such as Word, Excel or other files – must be labelled using an SDoT before leaving the security domain. E-mails can also be exchanged securely in this way. These IT security products are approved by the BSI up to the classification level SECRET.

How is the security domain-as-a-service realised?

The NSC achieves physical-equivalent separation primarily through software or flexibly configurable hardware components. This allows for the rapid creation of security domains without the need for additional hardware. Many components are either already approved by the BSI for classification levels up to SECRET or are based on hardware appliances certified to the same level.

To what extent is it NATO-compatible, for example with the Federation Mission Networks?

The NSC's PaaS draws on more than 14 years of experience in developing NATO-compliant cloud applications based on FMN spirals. A notable example is the federated identity management concept, which allows seamless collaboration among NATO partners 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 taking control over their data and IT infrastructures, public authorities can better manage security risks and defend more effectively against cyber attacks.

Independence: Reduced reliance on international IT providers enables public authorities to organise their IT strategies independently.

Data protection: Compliance with national and European data protection regulations is simplified as data is stored and processed within the organisation's own territory.

Cost control: Open-source solutions are often more cost-effective and have lower license fees.

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

Authorities increasingly focus on open-source software due to its transparency and control. This reduces dependence on proprietary solutions from large international IT companies. With open-source, authorities maintain control over the software and hardware components they use. This enables them to make adjustments and address security gaps without relying on external providers.

What does the term "data sovereignty" mean?

Data sovereignty means that all data is stored and managed in national or private data centres rather than in foreign cloud services. This ensures protection against unauthorised access. Furthermore, strict security and data protection safeguard the IT infrastructure from cyber attacks, supported by regular security checks 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 calls, e-mail and file exchange. Additionally, SDoT Security Gateways enable file transfers and e-mail transmission across security domains.

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

Yes, within a domain, standard Office formats (text documents, spreadsheets, presentations) can be edited collaboratively in real time through a web browser. Files can also be securely transferred from one domain to another within the same application.

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

The VS-Workstation is designed to support all security classifications used in Germany (VS-RESTRICTED to SECRET) as well as the equivalent NATO classifications (NATO RESTRICTED to NATO SECRET). Additionally, 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-classified domain to a lower-classified one, it must be appropriately labelled. The creation of this label must always be initiated by an authorized individual who selects the correct classification level. If a documentclassified as SECRET is attempted to be transferred to a lower-classified domain, the SDoT Security Gateway prevents the transfer. Additionally, documents without a label cannot be transferred to lower-classified domains.

Can I connect the VS-Workstation 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 user files managed in the cloud?

File management is based on the well-known open-source product "oCIS" from the company ownCloud. This software is widely supported and used by both industry and the public sector (from Mercedes to Bayercloud to CERN) for enterprise-level file management and scalability. Features such as proven versioning, automatic backups and many other enterprise functions are also automatically available for the VS-Workstation.

Outlook – Shaping IT Security Together

We view the Classified Information Directive (VSA) as a key driver of innovation. For us, this means continuous progress. Our goal is to stay ahead of emerging cyber threats through technical advancements and new developments. We aim not only to meet security standards but also to harden and shape them for the future.

Focusing on User Requirements

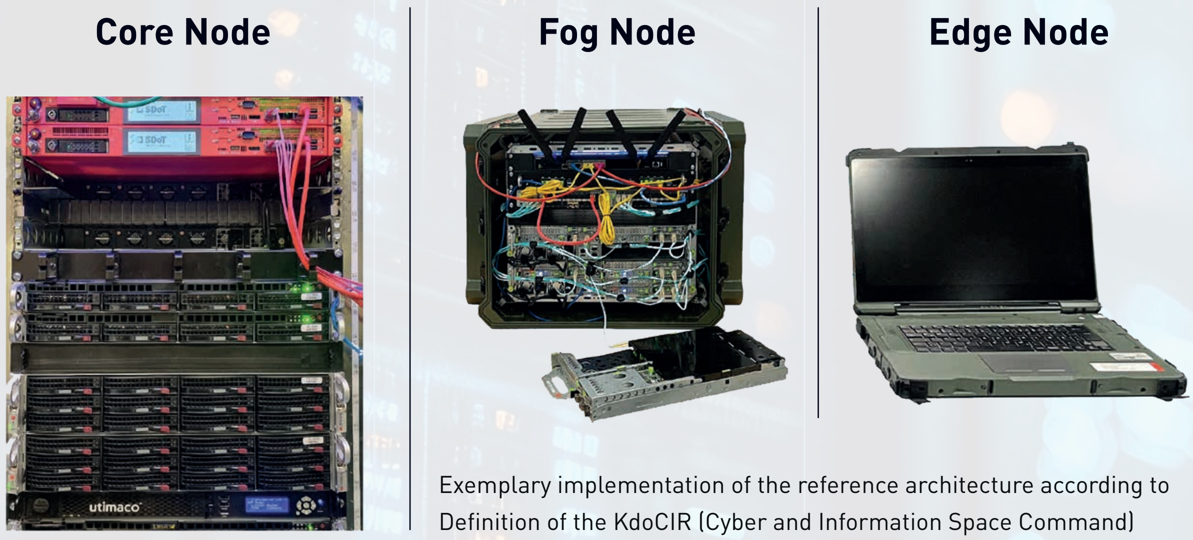
For us, IT security and digital sovereignty – and thereby the state's and society's ability to act – take precedence over "look & feel". With approved components, our network of trustworthy German companies demonstrates how the demanding requirements of the VSA can be met constructively, resource-efficiently, transparently and traceably, even beyond VS-NfD/RESTRICTED.

We also show that a VS-enabled workspace can meet the challenges of modern digital collaboration while facilitating secure exchange, dialogue and communication – all without being dependent on large software providers. This ensures our users do not fall into the trap of vendor lock-in.

We understand that the future lies in separating hardware and software. Our modular approach simplifies the integration of third-party providers. If their software is Kubernetes-capable, much of the groundwork is already laid.

Authorisation procedures place high demands on all stakeholders. Focusing on the triangle of users, authorisation bodies and service providers is essential for achieving and maintaining IT security and digital sovereignty for Germany, with an emphasis on resource-efficient and cost-effective implementation.

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



Exemplary implementation of the reference architecture according to Definition of the KdoCIR (Cyber and Information Space Command)

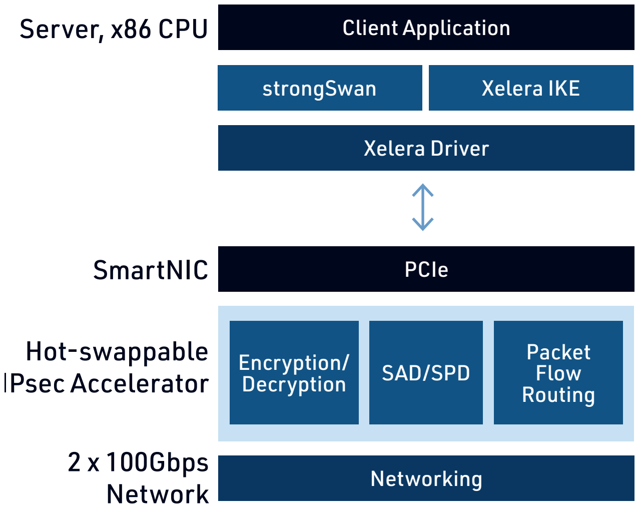
Easy Integration of New Technologies

To continuously enhance the scalability, flexibility and cost-effectiveness of the NSC, development progresses in successive stages, with some already underway.

One example is the integration of SmartNIC technology. Unlike conventional cloud solutions in authorised security contexts, SmartNIC enables physical separation of the network infrastructure across different security domains. This completes the NSC concept of operating multiple security domains on a single piece of hardware.

SmartNIC significantly increases the scalability of the NSC while enabling flexible management of security domains. With a data throughput of 100 Gbps, it delivers network and encryption infrastructure performance comparable to modern commercial cloud infrastructures. Due to its programmability, SmartNIC is an integral part of the future NSC security concept, which maps out future advancements without requiring hardware replacement. SmartNIC 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 forms the foundation of an open and stable ecosystem, built on the principles of modularity, flexibility and interoperability. Over time, authorised IT-security components anchored in hardware will increasingly be replaced by software-based solutions, as reflected in the development roadmaps of our partners.

We are addressing the demand for a genuine, controllable "security domain as a service". This enables dynamic setup and administration in minutes, rather than hours or days.

The Future of NSC is Dynamic

Currently, the NSC is static and functional, meeting eligibility for approval while serving the security-compliant needs of civil and military users. In the future, the NSC will evolve to become dynamic and extend its reach beyond Germany.

This evolution benefits administrators by enabling them to implement increasingly complex requirements efficiently, while maintaining all necessary security standards.

The consistent use of open-source software ensures flexibility and independence. Administrators are equipped to manage operations and defend against cyber attacks, while users, supported by the VS-Workstation, can focus on the growing number of security-related tasks without being burdened by technical complexity.

In short: we design security together – with public agencies and authorising bodies – building trust and acceptance every step of the way.

The Partner Companies of the NSC Programme

The National Secure Cloud (NSC) is being developed by a network of German companies, each taking on specific tasks to meet the stringent requirements of the public sector, the military and regulated industries.

infodas
connect more. be secure.

infodas is one of Germany's leading solution providers for cyber and information security. Since 2024, infodas has been a subsidiary of Airbus. In addition to advising companies, authorities and armed forces, infodas develops high security products for domain transitions and the protection of critical infrastructures. The SDoT (Secure Domain Transition) product family from infodas is approved for the SECRET, EU SECRET and NATO SECRET classification levels. These products are certified according to Common Criteria and hold additional country-specific certifications.

The SDoT product family includes a range of security appliances for controlled unidirectional or bidirectional data exchange between networks or systems of different sensitivity levels. It also provides solutions for creating NATO STANAG 4774/8-compliant and highly secure security labels for data. These functions are essential for data exchange in a cloud with multiple security domains, facilitating collaboration between authorities and nations.

utimaco®

Utimaco plays a key role in meeting cryptographic requirements by providing a BSI-approved hardware security module. This guarantees the physical security of the cryptographic keys used within the NSC. Additionally, Utimaco offers optional client-side protection with hard disk encryption and "File and Folder" encryption, approved up to VS-NfD classification.

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

With over 40 years of experience in IT security, Utimaco is one of the world's leading manufacturers in its key market segments. It is also recognised as a BSI "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 solutions enable organisations to securely operate multiple security domains with different classifications on a single hardware platform.

The L4Re Operating System Framework is based on a microkernel architecture. This means that security-critical applications are strictly separated from standard applications, which significantly reduces the risk of security vulnerabilities. The L4Re technology not only offers maximum flexibility and efficiency but it is also approved by the German Federal Office for Information Security (BSI) for processing of data classified up to SECRET. L4Re is already used in security-critical environments, such as government laptops and network technology, to securely manage information classified as SECRET, NATO SECRET, and EU SECRET.

XELERA

Xelera Technologies GmbH is a software company founded in 2018 and based in Germany. It provides high-performance AI and cybersecurity products for data centres and cloud environments. Serving customers in Europe, the USA and Australia, Xelera's core expertise lies in SmartNIC/DPU and network technologies. Xelera enables next-generation clouds and data centres to meet data rate and security requirements by offering SmartNIC and AI infrastructure technology.

Its SmartNIC/DPU software plays a crucial role in optimising performance, cost efficiency and hardware-level network security in data centres. Additionally, Xelera's technology significantly reduces server power consumption in data centres and cloud infrastructures.

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
Rheinstraße 40-42
64283 Darmstadt

Felix Winterstein
CEO
felix.winterstein@xelera.io
+49 6151 6290901
www.xelera.io

GLOSSARY

Data sovereignty

Control over your own data. The user decides who can access their data, how and for what purpose it is used, and how it is processed.

Hardened system

A specially secured IT system that has been made more resilient through measures such as removing unnecessary functions and closing security gaps.

Hypervisor (microkernel-based operating system)

Software that enables the simultaneous operation of multiple virtual machines on a single physical machine by efficiently allocating hardware resources. A hypervisor also enforces strict separation between domains.

Infrastructure as a Service (IaaS)

A cloud computing model that provides IT resources such as computing power, storage and networks as a service. Users deploy and manage their own applications on these resources.

IoT (Internet of Things)

A network of physical objects equipped with sensors, software and connectivity to collect and exchange data.

Security by design

The integration of security measures into the development process of systems or applications from the outset to minimise vulnerabilities.

Security domain

An isolated area within an IT system designed for a specific security level. Strict access rules govern the processing of data within the domain.

Single-Sign-on (SSO)

An authentication method where users log in once and gain access to various applications or systems without the need to reauthenticate.

SmartNIC

A specialised network interface card that offloads network processing tasks from the server CPU. SmartNICs handle tasks such as network compression and decompression as well as encryption and decryption.

Software as a Service (SaaS)

A cloud computing model that delivers software as a service via the internet. Users access the software through a web browser without the need for local installation.

Classified information (VS)

Matters and objects of all kinds that require special security measures to protect them from unauthorised access. They are classified as TOP SECRET, SECRET, CONFIDENTIAL or FOR OFFICE USE ONLY depending on the required level of protection.

VS data

presented or processed in a specific form for machine processing or originates from such a process (USB sticks, hard drives, etc.).

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

Editorial design
Thöring & Stuhr Kommunikationsberatung GmbH
Mittelweg 144
20148 Hamburg

Design
CC.CONSTRUCT GmbH & Co. KG
Hofaue 21
42103 Wuppertal

Print
Rapp-Druck GmbH
Kufsteiner Straße 101
83126 Flintsbach

IABG | infodas | KERNKONZEPT | utimaco® | XELERA

IT security is non-negotiable.

www.iabg.de