SAYTEC

Juli 2023

sayFUSE HCI

The symmetric hyperconverged infrastructure

WHITEPAPER: THE HOLISTICALLY DESIGNED INFRASTRUCTURE

Table of contents

1. SAYFUSE HCI INFRASTRUCTURE:

The sayFUSE hyperconverged infrastructure (**sayFUSE HCI**) consists of at least three sayFUSE All-in-One Infrastructure Nodes **(sayFUSE HCI Node**), which provide the server storage network infrastructure, and a **sayFUSE Backup Appliance**, which acts as a backup restore platform for archiving, data backup and offsite storage. The integrated **sayTRUST VPSC - Zero Trust** solution enables highly secure communication between the client and the infrastructure.

In this hyperconverged infrastructure, CPU, RAM, storage, and network resources are combined into a single software-defined system and can be managed across nodes. It is fault-tolerant to complete failures of one or more nodes and enables uninterrupted uninterrupted operation. Future expansions by adding additional nodes are easily and without migration effort.

The individual sayFUSE HCI Nodes are identical in hardware and software. Each sayFUSE HCI node contains all necessary hardware and software components, so that in the future no additional licenses for clustering, computing, storage, Kubernetes, monitoring, zero trust, personal key identification, single sign-on, billing and multi-tenancy, ... will be required. In case of a failure of one of the nodes, all computing, storage, networking tasks of the failed node will be taken over by the other nodes and a trouble-free business continuity will be ensured.

The products sayFUSE HCI (all-in-one node for hyperconverged infrastructure), sayFUSE Backup (all-in-one appliance for backup, restore and outsourcing) and sayTRUST VPSC (all-in-one client access solution for zero trust, SSO, PKI, ...) can also be operated on their own and each represents a high-quality solution in its respective field of application.
In interaction within the HCI infrastructure, they mutually reinforce each other and together form a holistic solution for the requirements of today and the future.

1.1. Outline of the project:

The hyperconverged infrastructure consists of N sayFUSE HCI nodes and the sayFUSE backup appliance. The structure is ideally symmetrical over two fire compartments and a backup appliance in each fire compartment. The HCI set up in this way forms the interconnected storage, computing and networking that is used as an "**as a service**" and offers the possibility of providing **completely isolated infrastructures as a service (IaaS)** for sites.

The sayFUSE Backup provides **up to 12 TB/hour of live backup** for high-speed backup. Within the backup appliance, data can be migrated and offloaded from **backup storage** to the integrated **backup library system**. Each appliance contains **six backup drives** with 24 TB capacity each.

The sayTRUST VPSC as Zero Trust Client Access enables communication independent of location and device and a secure working environment.

1.1.1. Main objective of the sayFUSE HCI technology

is the provision of a highly secure infrastructure for business continuity that can be scaled flexibly. It can, for example, provide other sites or clients with complete network infrastructures, so that in future no additional investment will be required on site for e.g., servers, storage, load balancers, etc.

The integrated hypervisor provides cohesive storage, computing and networking across nodes and delivers all infrastructure components as a multi-tenant service. The sites/clients that receive their infrastructure as a service will not need to purchase

additional servers and storage in the future and will be able to use all the services provided.

For example, a site or client receives an isolated infrastructure as a service that is provided by the main administration and can be managed by the respective site or client. It may contain the following infrastructure components as a service:

- Router,
- Load Balancer,
- Firewall,
- Single Sign On,
- Personal Key Identification,
- Zero Trust Access,
- VPN,
- NFS-, iSCSI-, S3- backup- storage,
- Server,
- Virtual Client-PC,
- Backup (multilevel with migration, Media discontinuity and outsourcing)

The individual IaaS are isolated from each other and from the insecure Internet as well as from the in-house network. The access of the users to the individual applications, services, networks or their own virtual PC can be controlled via sayTRUST VPSC Zero Trust Technology, after checking the identity "**Personal Key Identification** (PKI)" via **multi-level Defence in Depth security procedures**.

1.1.2. Main objective of sayTRUST VPSC (Virtual Private Secure Communication)

is to achieve the highest level of communication security by **detecting and eliminating the most critical vulnerabilities** in a communication **between user and the network to be protected**. Users can work securely within their own network as well as from other locations, home offices or mobile hotspots via 8-level "Defence in Depth" Zero Trust technology.

1.1.3. Main goal of the sayFUSE Backup

is to eliminate the typical backup vulnerabilities of tape and storage-based systems and increase the security and speed for data backup.
The sayFUSE Backup combines all five essential backup components, backup server, backup storage backup library, backup drives, flexible choice of backup media, media break and swap. It provides high backup quality and ensures the recoverability of data and systems.

The holistically designed sayFUSE HCI concept ensures high-cost savings and maximum security for the headquarters and for all locations.

1.2. Schematic representation of the sayFUSE hyperconverged infrastructure:

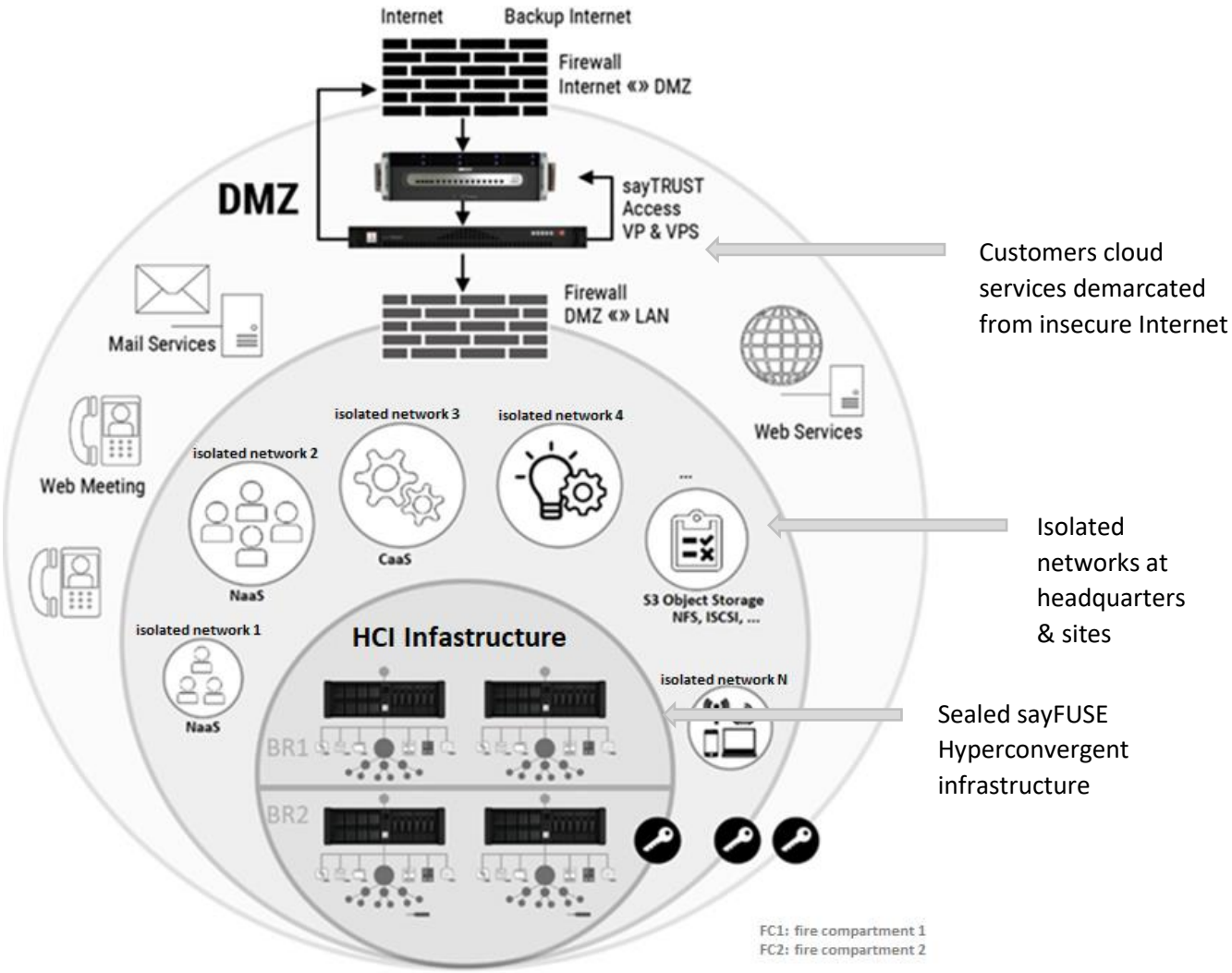
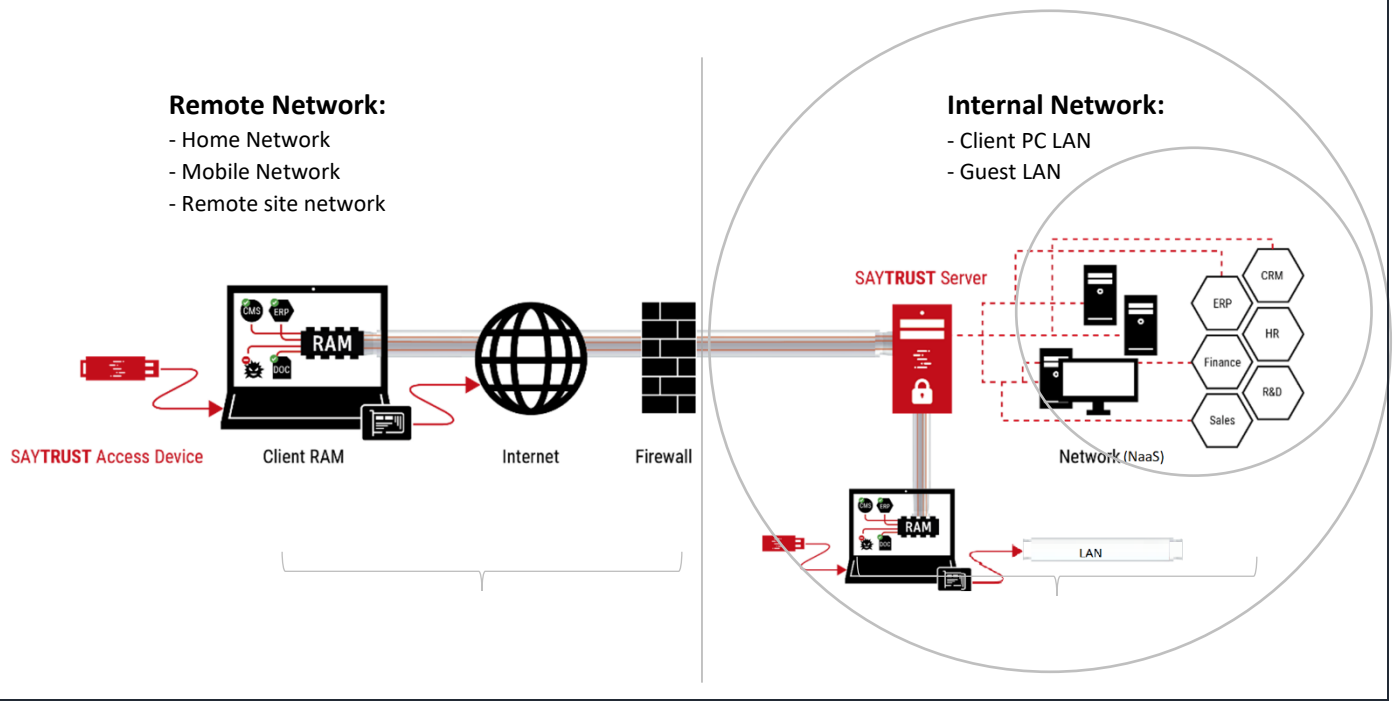


Figure: Representation of overall infrastructure

1.3. Schematic diagram for client access security:



High-security communication requires the **interlocking of all security elements at the most critical interfaces** over the entire communication path. It detects and eliminates these vulnerabilities, both within the in-house network and for remote access. With the sayTRUST VPSC Zero Trust technology, the highest level of security is achieved by **detecting and eliminating the critical vulnerabilities** in a communication.

2. CHARACTERISTICS OF THE TECHNOLOGIES INCLUDED IN SAYFUSE HCI:

This chapter presents the functional scope and features for the holistically designed IT infrastructure. In the sayFUSE HCI Infrastructure Bundle, which is provided as a holistic infrastructure bundle, three elementary technologies are combined.

- Hyper-converged infrastructure for uninterrupted business operations, maximum scalability and high flexibility.
- Backup-restore platform for data archiving, backup and offloading.
- Personalized Zero Trust for client access security.

The objectives of the bundle are availability, scalability of the IT infrastructure and achievement of the highest security level for client access, both within the network and for remote access. Furthermore, the focus is on reducing the complexity of the overall system.

Starting with three devices as a sayFUSE All-in-One Infrastructure Appliance (Nodes), the overall system can be scaled as required with additional devices without migration effort and is suitable from medium-sized companies to large corporate structures.

The use of the sayFUSE HCI infrastructure minimizes current and future hardware and software requirements (Chapter 1. sayFUSE HCI Infrastructure). Even the smallest bundle contains all the features listed below.

In the following, the properties are listed according to the technologies.

2.1. Scope of services of sayFUSE hyperconvergent infrastructure

2.1.1. General properties of the sayFUSE HCI system

1. Each device in a sayFUSE HCI infrastructure is an **all-in-one infrastructure appliance** (node). All hardware and software components are included in each node.
2. The overall system contains several nodes for the HCI infrastructure and a sayFUSE backup appliance (appliance) for the **backup-restore platform**.
3. Each sayFUSE HCI Node contains all necessary hardware components for computing, storage, networking and the software licenses for the hyperconverged infrastructure.
4. Each appliance contains all necessary hardware components for computing, backup storage, backup library system, backup storage-to-disk with media break and offloading.
5. The nodes are identical and each node is able to automatically take over the role and tasks of any node from the federation in case of failure or scheduled maintenance.
6. The nodes that make up the system communicate with each other via an Ethernet-based network infrastructure. No other type of network or connection between servers or between servers and disk systems is required.
7. The system contains **compute, software-based storage** (SDS) and **software-based networking** (SDN) components that form the cluster between the nodes. Each of these components can be managed from a single point in full compatibility with each other.
8. The system is able to add more nodes and can thus be scaled linearly without migration effort.

9. The system forms **high security cloud cluster** that starts with a single node and can grow by adding nodes. There is no limit to the growth of the cluster or to the number of nodes in the cluster.
10. The server storage cluster is designed to tolerate the failure of at least one node at a time. If desired, the configuration option can be extended to tolerate a complete failure of two or more nodes.
11. All management of the system is possible via a web-based interface, a command line and an API interface.
12. The system is able to over-commit CPU and RAM resources. The **over-commit multiplier** can be set by the system administrator.
13. For all virtual disks, only as much data can be written to the disk as is being used (thin provisioning).
14. Virtual machine creation process can be done quickly with pre-built hardware templates. New machines can be added to the templates and the CPU and RAM resources can be specified.
15. The system has an "**Image Service**". Through this image service, which copies ready disk images or ISO files, it is possible to create a virtual machine with a ready disk image or with an ISO installation file.
16. **Security policies** can be created in the system, which can be assigned on virtual machines or groups of virtual machines.
17. Security policies can allow setting access rules from the outside to the virtual machine (inbound) and from the virtual machine to the outside (outbound), and these rules can be changed flexibly..
18. Operations such as listing the virtual machines with a security policy, assigning a policy to a virtual machine, and editing the access rules of a policy can be performed through the web panel.
19. Alerts, **audit logs and detailed performance graphs** of the system can be monitored via the web panel.
20. The system is able to send error, warning and alarm messages by e-mail via SMTP protocol to the desired persons.
21. The system is **multi-tenant** and can provide a site or tenant with a fully independent implementation and administration for its own management if required. The IaaS provided can include all services such as S3, iSCSI, NFS storage, virtual servers and client PC, routing, load balancer, zero trust, VPN, ...
22. The system can be managed via the administration from the central office if required or if a site has no administration.
23. **SSD or hard disk units with different access formats such as NVMe, SAS, SATA** can be used in parallel on the servers. Although it is natural to specify the required minimum number of these units, there is no rule that prevents the simultaneous use of different hard disk capacities and formats in the desired combination.
24. There is **no limit to the number of discs** that can be installed on a node.
25. Software or hardware based RAID1 structure (mirroring) is supported for M2 NVMe to be used for **OS hypervisor**.
26. Each node has a BMC module for **remote management**.

2.1.2. Specifications of the sayFUSE HCI disk subsystem

1. The disk subsystem supports the definition of different tiers for disk clusters with Different physical properties. For example, NVMe tier, SSD tier, HDD tier, etc.
2. **Writes to the HDD tier can be accelerated by an SSD or NVMe disk** that is used as a buffer (cache). This acceleration process is optional when a diskset is created and an acceleration process is not required for every diskset.

3. Data written on data carriers can be encrypted if desired. The encryption process is performed software-based by the system and it is possible to select the encryption on the disk for each tier separately.
4. When creating a virtual machine, it is possible to make an optional selection from different tiers such as HDD, Accelerated HDD, SSD, NVMe, e.g., the operating system disk can be selected from the Accelerated HDD, the data recording disk from the SSD and a disk to be used for backup and archiving can be selected from the HDD tier.
5. For each virtual disk it is possible to specify redundancy options in addition to the tier. It is possible to choose between true copies (2 or 3) or **space-saving redundancy schemes with erasure coding** algorithms.
6. Erasure coding reduces the choice of schemes such as (3+2, 5+2, ..., 17+3) and the additional disk space required for redundancy (**disk space efficiency**). Furthermore, **uninterrupted operation is enabled, even if 1 up to 3 nodes are lost at the same time.**
7. The sayFUSE HCI system can be designed to tolerate the simultaneous **failure of multiple nodes**.
8. Virtual disks can be added and removed and their size can be increased without shutting down virtual machines.
9. For virtual disks, "**storage policy**" templates can be created, which include both tier and redundancy selection

2.1.3. Specification of the control panel of the sayFUSE HCI infrastructure

1. The **system control panel is isolated** to allow site system administrators, rather than users, to manage it themselves.
2. Operations such as defining a new client/location on the system control panel, setting the client's user name and password, and **determining the client's resource usage quotas** can be performed via the web interface.
3. The control panel provides the ability to intervene in the virtual machines, projects and networks of the client/site. The operator in the central office **is able to enable managed services to a site if required**.

2.1.4. The site administration control panel

1. For each site/client using the sayFUSE HCI infrastructure, **their own access panel** is available. The respective site/client is able to access this panel with its own username and password and perform its own daily operations.
2. By accessing this panel, the respective site/client is able to perform operations such as creating and deleting virtual machines, accessing the console, and powering on/off its own machines.
3. The site/client is able to create different operation zones and projects on its panel and allow different users to perform operations on different zones. The site is able to determine which user can perform operations on which project.
4. The resource usage of the site/client can be limited based on CPU, RAM, disk space, disk access frequency (IOPS) and number of load balancers. **This limit is set by the system administrator** and it is ensured that the site does not exceed these limits.
5. The site is able to view the **usage status of its own resources** via the access panel.
6. The site is able to create virtual networks belonging to its system and determine the IP address range that these virtual networks will have.
7. The site is able to define a virtual router that performs routing between the virtual networks it creates and is able to create the necessary routes for this router.
8. The site is able to enable the DHCP service in its virtual network structure. The IP address pool to be used by the DHCP service is defined by the site.

9. The **virtual networks created by the site are independent of the physical network structure.** The system has an SDN (software-defined networking) structure within itself.
10. Virtual networks **are independent of the physical network structure by using technologies such as VxLAN (Virtual Extensible LAN)** and **Geneve technology.**
11. The site is able to create a virtual machine on the open shared network (Internet) or set up virtual networks and access the open Internet through a virtual router using NAT.
12. The site is able to assign an IP address to the virtual machine created in the virtual network to enable access from outside (e.g., from the Internet). This address is defined as a **floating IP address** and its number can be limited for the client/site.
13. With the approval of the site system administrator, the site is able to import its own virtual machine images into the system for use in creating virtual machines.
14. A "**shelving**" function exists for an unused virtual machine. The shelved machine remains in a non-operational state, is not counted in the HCI user's resource usage, and is not included in quota usage. When the swapped-out virtual machine is taken off the shelf and brought to life, it is again counted as usage within the quota.
15. The site is able to set up an **IPSec-based encrypted VPN** to connect the virtual networks within its own structure to another data center configuration outside the cloud structure. This VPN definition is an integral part of the system and requires no additional software or installation.
16. The system administrator is able to limit the number of VPN definitions that the customer can make.
17. The site/client is able to implement and manage its own sayTRUST VPSC Zero Trust in its SDN. The licenses for **the sayTRUST Zero Trust server operating system** are included for each site/client.
18. The site is able to roll out PKI (**Personal Key Identification**), SSO (**Single Sign-on**), **application and desktop publishing** for its users with its sayTRUST VPSC Zero Trust as well.
19. The system administrator is able to enable and manage **backup and restore** for the site's SDN.

2.1.5. Scope of services of the Backup Restore Platform

1. sayFUSE Backup Restore Platform is an all-in-one backup appliance and works **completely autonomously**. It does not require any additional hardware and software for media handling.
2. The backup system includes backup/dedup backup storage for the entire backup dataset and six backup drives that operate autonomously or as a pool.
3. The backup drives turn on with the job before the backup, turn off after the backup is completed, and enable the **media abort and swap**.
4. Each backup drive can be configured, controlled and monitored independently.
5. Each backup drive can be configured for parallel backups and restores.
6. 6 backup drives of the backup system can optionally use backup media for swapping with a capacity of 1 TB up to 24 TB.
7. The integrated backup drives can manage the use of uniform and different media capacities.
8. All-in-one backup system enables backup-to-dedup, backup-to-disk, migration-storage-to-disk, media dropout, and offsite storage.
9. The backup system is equipped with two 2x50 Gbit/s and 2x10 Gbit/s Ethernet ports for backup and restore as standard. Expansion with additional 2x100 Gbit/s ports are possible.
10. The system contains a BMC module for remote management.
11. The control software (**media handling**) of the backup drives and backup media is integrated into the backup system.
12. **A spare backup drive is integrated** into the backup system so that drive and media errors are caught. When such errors occur, the backup is written to the spare backup drive.
13. Both the backup drives and the backup media are uniquely configurable and controlled by the control software.
14. The backup drives and backup media can be clearly controlled via backup jobs.

15. Backup drives **are powered on with the job** and **powered off after the job is completed**. This significantly reduces energy consumption and significantly increases the life of the media and significantly reduces misuse**.**
16. The site is able to manage its own data backup including media break and outsourcing.
17. The backup media are located behind lockable flaps to protect them from unauthorized access.
18. Daily, weekly, monthly, yearly backups are configurable and are performed fully automatically.
19. The backup media can be replaced during operation and removed for swapping.
20. Backup offloading up to **144/288 TB** (native/ compressed) is included in the standard scope of delivery of the backup system. The capacity can be extended if required.
21. **Cleaning cartridges are not required** for the backup library system.
22. The backup library system **has no mechanical wear parts** and has no start-stop behavior for the backup media.
23. The backup media are **electromagnetically encapsulated**.
24. The backup media **can be encrypted for offsite storage**.
25. The backup system allows **duplication of backups before outsourcing**.
26. The Backup system supports dedup backup to reduce network load and time window.
27. The backup system enables **life backup at a speed of up to 12 TB per hour**.

2.1.6. Scope of services of the sayTRUST VPSC Zero Trust

1. sayTRUST VPSC (Virtual Private Secure Communication) is a **personalized Zero-TRUST multi factor communication solution** for user communication from any location and via any client computer using Defence-Depth technology.
2. sayTRUST technology enables a secure connection via multi-level authentication and without complex, rigid and time-consuming installation and configuration on the respective user PC
3. Communication between the client computer and the remote network is performed **without network-to-network coupling**.
4. The **client computer has no information about the remote network**.
5. Access to applications and resources is **certificate-based after unique identification** (PKI) of the user according to his authorizations.
6. One license for the server operating system is included for sayTRUST VPSC technology for each site/client.
7. sayTRUST VPSC Server operating system contains its own integrated, **independent Certificate Authority** (CA) and a PKI is supported.
8. sayTRUST VPSC generates and manages its own Certificate-Authority based, independent, forgery-proof and protected certificates.
9. The **user's identity is checked on the client computer before use**.
10. Configuration of user certificates is possible with S-LDAP and manually.
11. sayTRUST VPSC enables tunneled communication for **local as well as remote and mobile applications** that may reside on the user token.
12. Server-side generated user certificates **control the allowing, blocking and isolating** of **remote and/or local and or mobile applications and resources.**
13. Encrypted communication takes place **within the application layer from the working memory (RAM) of the client PCs**, instead of via network-network coupling of the network card.
14. Encrypted communication is performed via **multi-level defense-in-depth communication security**.
15. During the connection of the user via the remote client computer, foreign computer from the home or foreign network, there is **no possibility for scanning the remote network.**

16. The user computer is decoupled from the remote network even during VPSC communication with it. There is **no possibility to draw conclusions about the network to be protected via the user computer**.
17. Central administration is available for creating and rolling out **permissions for applications, devices, network resources and directories**.
18. A **central distribution system** is included for rolling out user access regardless of location and PC for the initial implementation and through this, subsequent customizations, updates and changes can also be rolled out automatically.
19. It is possible to provide **shares** from the protected network to the client PC **without coupling the client PC and the network** and without using virtual network cards.
20. Technology enables network shares to be deployed **with or without drive mapping** and with network information obfuscation.
21. sayTRUST technology enables the use as **Internal Network Protection** (INP) to maximize internal network security.
22. **Access to applications and resources is certificate-based** and after unique identification (PKI) of the user and his authorizations. The user can only work with the assigned resources.
23. User tokens are AES encrypted USB tokens and client software or app for mobile devices.
24. sayTRUST user token versions are available for AES encrypted tokens with PIN pad, biometric flash disk or microprocessor based.
25. The tokens have AES256 bit encryption.
26. sayTRUST technology enables parallel use of different sayTRUST client tokens, such as:
    - Client Software
    - Mobile App
    - Secure SSD (AES256)
    - Secure USB token with 3-factor authentication (**AES 256 bit microprocessor based** + certificate + password + biometrics)
    - Secure USB stick with 3-factor authentication (**AES 256 bit flash disk based** + certificate + password + biometrics)
    - Secure USB stick (**AES 256 bit flash disk based** + certificate + password + **PIN pad**).

2.1.7. Functionality of Virtual Private Secure Communication (VPSC)

1. User computer recognizes the microprocessor-based sayTRUST Access Stick only after biometric identification of the user (**PKI**).
2. 8-level Defence-in-Depth access security (**DiD**) starts before use at the client PC.
3. Communication security starts in the origin **from the encrypted RAM** of the client PC through Perfect Forward Secrecy (**PFS**).
4. Connection establishment without installation from any computer by means of remote access device.
5. Password manager for single sign on (**SSO**) is integrated.
6. File transfer for interruption-independent **file transfer and synchronization** is included. This resumes a copy/synchronization process at the last position even after a connection loss.
7. **Portable app management** for mobile applications like mail, phone client or office applications is integrated.
8. sayTRUST technology integrates an application gateway for **application farms and/or virtual applications** for Citrix, Microsoft, Linux and web applications without port sharing to the outside or installation of receivers on the user PC.
9. Secure Wake on LAN (**sWo**L) also over multiple gateways and networks is integrated.
10. An Encryption Tool (**ET**) is integrated in the system for users to create personal encrypted containers within the AES encrypted micro/flash chip.
11. Browser function for independence from installed web browsers is integrated.
12. User verification takes place on the client PC before use. The sayTRUST token can only be used after the user has been uniquely identified.

13. Checking of user authorizations starts before tunnel construction begins.

Characteristics of the Client Token

1. Start of policy monitoring before the tunnel.
2. No dependence on the client PC.
3. No software installation on the client PC.
4. No network-network coupling with the remote network.
5. Connection at the application level.
6. Connection from the RAM of the client PC.
7. No remaining traces on the client machine.
8. Client device has and knows no network information from the remote network to be protected.
9. No remaining traces of the connection path.
10. Communication only for certificates that have not been tampered with.
11. Application-level connection, i.e., the terminal device does not receive an IP address from the remote network and does not know it.
12. Communication within application level instead of network-network coupling.
13. Client PC does not become a member of the remote network and does not know it.
14. Tunneling of applications from the client PC's memory.
15. Unauthorized applications cannot establish connections.
16. Targeted blocking of communication for unwanted applications.
17. A new key, previously unknown to the parties, is generated in the process memory for communication depending on the client certificate according to Diffie-Hellman.
18. No installation of a virtual network card on the end device.
19. No installation of client software (optional if stick not desired).
20. Protection against man-in-the-middle attacks.