The Data Protection Company

with **Real Life** experience from our SEP Support

protectio**now.**

SEP sesam - Cyber Security

Ransomware protection, compliance and other data security-related benefits with SEP sesam Backup & Recovery

1 Introduction

Cyber attacks not only affect large companies, but recently more and more small and medium-sized businesses. Attackers are always looking for vulnerabilities and entry points in networks and servers in order to infiltrate systems with ransomware or malware. In the process, data is often stolen or the infrastructure is encrypted. The focus of a ransomware attack is always on the backup data. Because if this is also encrypted, the damage of the encryption and by that the demand for a higher ransom increases.

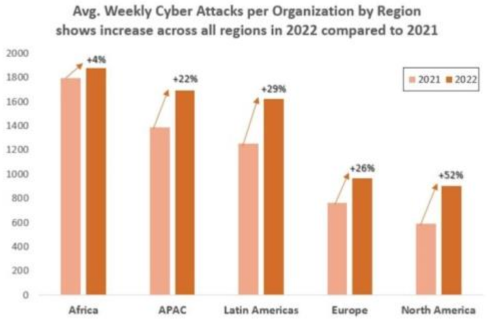
According to data from security researchers at Check Point Research (CPR), the number of cyberattacks in Germany alone increased by 27 percent in 2022 compared to 2021. The statistics were mostly driven by smaller, more agile cybercriminals and ransomware groups focused on exploiting vulnerabilities in collaboration tools used in home office environments. In Germany, the criminals mostly targeted

- Retail/wholesale company (+89 %)
- Public administration facilities (+80 %)
- Educational institutions (+60 %)

Researchers also warn that the maturity of AI technologies like ChatGPT could increase the number of cyberattacks in 2023.

Key statistics on global cyberattack trends in 2022:

- Global cyberattack volume reached an all-time high in Q4, with an average of 1168 weekly attacks per company.
- North America (+52%), Latin America (+29%), and Europe (+26%) regions saw the largest increase in cyberattacks in 2022 compared to 2021.



[Increase in weekly cyberattacks recorded per region in 2022 compared to 2021, Source: Check Point", www.infopoint-security.de/]

www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis

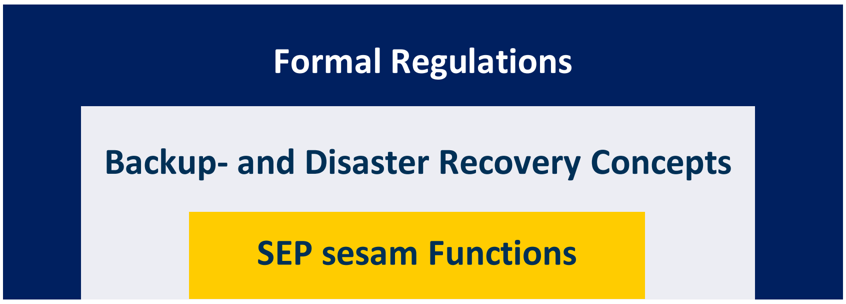
2 Overview

Since the 1990s, there have been efforts in the EU and Germany to standardize protection and security regulations by law. Increasing and global offerings to store or manage data in the cloud is a trend since years. Cybercrime, however, also!

Since then, a large number of regulations relevant to data security have been drafted, revised or replaced by new ones.
Examples are GDPR, KRITIS, NIS2, PATRIOT Act and others.

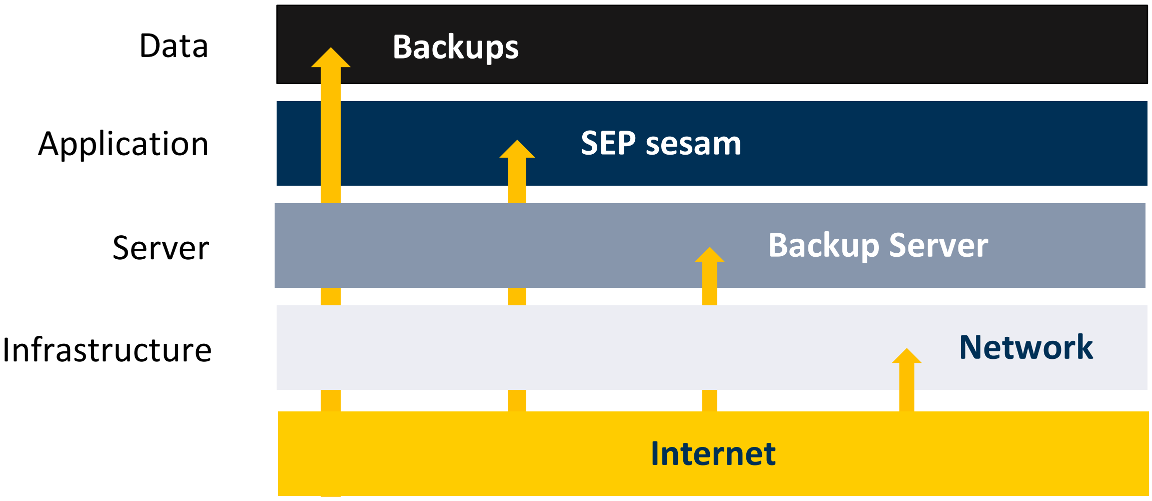
SEP sesam offers good possibilities to meet these requirements and to increase the security in the company enormously. These possibilities are discussed in detail in a separate chapter.

Here are the layers of security that build on each other, as they can also be found in the chapter structure of this document:



Attacks by ransomware viruses are on everyone's lips these days. However, an IT environment is exposed to many different attack vectors, which also operate at different levels. A data center security concept is like a separator made up of a wide variety of different walls increasing safety one after the other. A damaging attack can only be successful if it overcomes all walls.

Possible protection mechanisms of the respective levels are e.g. a firewall on network level, Linux as OS of the backup server, do not keep SEP sesam credentials in the Active Directory and an immutability storage for the backup data.



Here is just a selection of the possible attack vectors:

- Execution or installation of a malware via a manipulated website (link sent via email, messenger or SMS)
- Execution or installation of a malware via a manipulated email attachment or Internet download
- Unauthorized use of access data obtained by phishing
- Installation of unwanted or malicious software via compromised software update procedures (supply chain attack)
- Creating memory overflows and executing unauthorized program code
- Unauthorized access to a system via a zero-day exploit (previously unknown vulnerability)
- Mass testing of user names and passwords (brute force attacks)
- Infiltration of malicious or unwanted software via manipulated storage devices (for example, via USB sticks)
- Exploiting flaws and vulnerabilities in network or authentication protocols to gain unauthorized access to a system
- Obtaining unauthorized physical access to an IT system.
- Spying out access data and other information that can be misused via social engineering
- Redirecting web browser traffic, for example via Cross Site Scripting (XSS)

ⓘ en.wikipedia.org/wiki/Attack_vector

3 SEP sesam Functionalities

3.1 Protecting the Backup Infrastructure

As already indicated in the Overview chapter, protection against attackers takes place at various levels.

Regarding the infrastructure, many general protection mechanisms such as regular updates, frequent backups, virus scanners, firewalls, secure passwords and others must be in place.

But even the multitude of general protection mechanisms cannot provide 100% protection. If viruses are too recent, for example, there are no detection patterns for them yet and the virus scanners are not effective.

Network segmentation

A general division of productive and a separated backup network always represents a higher effort for attackers than a single and flat network structure.

Just as a traffic light regulates road traffic, a segmented IT network also regulates the traffic type, source and destination. Examples of network segmentation are provided by VLAN, Software Defined Network (SDN) and also firewalls.

For this reason, a breach or direct attack to the next level must always be expected. The next step is to secure the backup server. Experience shows that ransomware viruses increasingly try to infiltrate the backup server first (e.g. via Active Directory) and thus get hold of the backup data. Destroying the backup data makes the extortion attempt even more effective.

The following measures have proven to be effective for protecting the backup server:

- Linux instead of Windows as operating system
- Operating system of RDS different to Backup Server
- Activate only absolutely necessary services
- Start services only with the necessary rights and avoid root or administrator as much as possible
- Make use of authentication and authorization
- No integration with Active Directory or other directory services
- Remove the backup server, RDS and other components from the domain
- Multi Factor Authorization (MFA), whenever possible

https://wiki.sepsoftware.com/wiki/index.php/Ransomware_Protection_Best_Practices

3.2 Immutability

The protection of backup data is discussed in detail in this chapter.
In this area especially SEP sesam offers a variety of very effective measures to ensure immutability of the data.

3.2.1 Tape Technology

The most effective protection is known to be the very old WORM technology. Because the media can only be used once, as with a burned CD/DVD, this technology has the not inconsiderable disadvantage of increased media requirements and the associated costs. WORM technology is therefore only useful for archiving purposes, but not for daily backup.

Tape technology, which is also an old technology, offers a solution to this problem. Previously often declared as a discontinued model, it has gained considerable value again, especially due to the strong increase in ransomware viruses. The real physical airgap, which can be easily realized by outsourcing tapes, was the last resort for many SEP customers who were attacked.

Based on our experience with these customer scenarios, we always recommend the use of tape in the backup concept, i.e. to create at least one more copy of the backup data through migration. In fact, there are many customers who previously relied exclusively on disk as a medium who are now returning to the good old tape library.

No virus has yet been found that sets out to retrieve an outsourced tape from a bank or bunker.

SEP sesam has many years of experience with tape technology and supports a wide variety of manufacturers, drive types and tape formats. Additional functions such as readability test, spare pools, recopy (e.g. LTO4 -> LTO8), file search, drive groups, library partitioning, drive sharing, connection protocols, archive synchronization, compression, encryption, multiplexing, and many more are also available. Only the drivers available in the system are used.

ⓘ

wiki.sep.de/wiki/index.php/SEP_sesam_Storage_Hardware_Support_Matrix

https://wiki.sepsoftware.com/wiki/index.php/Tape_Management

3.2.2 SEP Immutable Storage

To prevent attacks on backups, SEP has introduced SEP Immutable Storage (SiS).

The idea behind SiS is that stored data remains completely unchanged in its original and unmodified form for its specified duration (lock time). This means that organizations can quickly recover from a ransomware attack, even if they have lost access to their data and servers, by using stored unmodified data copies to restore the entire operating environment.

The SiS is basically not just a functionality but contains an entire concept with many security recommendations with the goal of achieving maximum security against ransomware. From a functional perspective, the SiS requires Linux as OS, using the immutable flag of the extended file attributes.

Here, the basis for effective protection against ransomware is the interaction of exactly two components:

1. Administration and configuration of the server under root is done under special access protection (console only)
2. The backup server has access only through a dedicated port with very limited permissions. As long as the lock retention is valid, the backup server cannot delete or modify its own written data. Writing new data or reading existing data for the purpose of restore, migration, replication, etc. is possible at any time

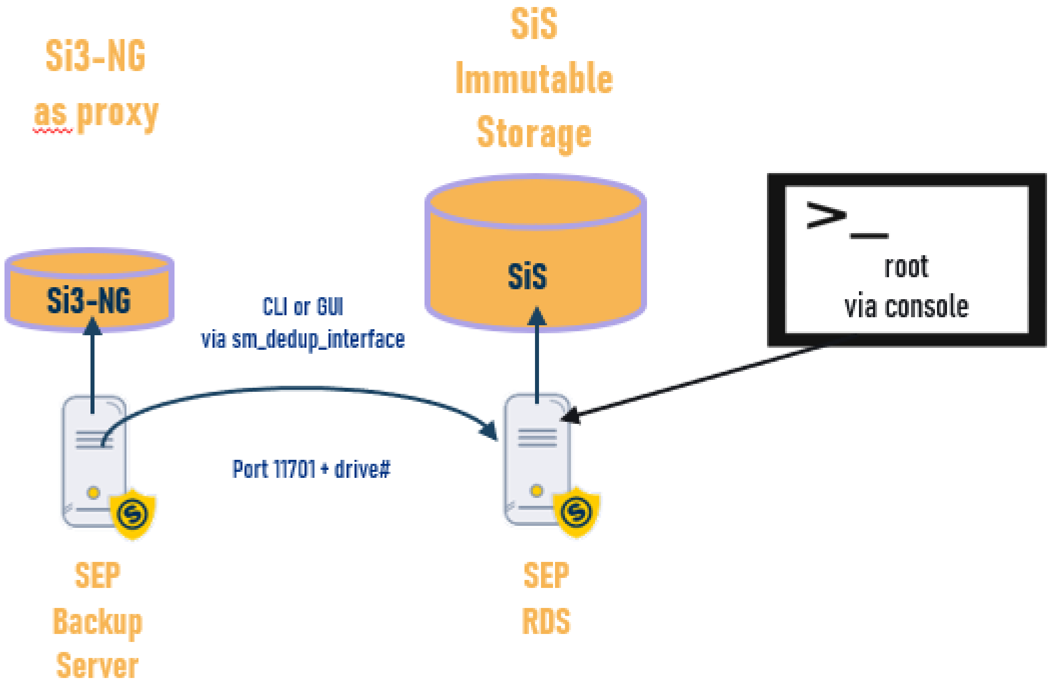
Thus, the SiS also effectively protects against a hostile takeover of the backup server itself.

The following requirements and recommendations:

- Physical Server
- Linux RDS: SLES15, RHEL8, Debian11
- ext4/XFS: Support of the chattr command
- Secured server: no ssh, access only via a local console
- TCP/IP connection
- Retention times: Mediapools > SiS Lock Time
- Correct time synchronisation (ntp)

The SiS requires the use of the SEP sesam integrated software deduplication Si3-NG.

SiS does not require local storage at the backup server. You can either backup directly or replicate your data to SiS.



https://wiki.sepsoftware.com/wiki/index.php/SEP_Immutable_Storage_-_SiS

3.2.3 Blocky4sesam™

Backup is a key area in protecting companies against ransomware, as cyber attacks usually also encrypt or destroy data backups. With Blocky4sesam™ there is a reliable protection for the SEP sesam backup environment against ransomware attacks. It is secure, fully integrated and can be set up without excessive administrative effort for the Windows RDS (Remote Device Server) server.

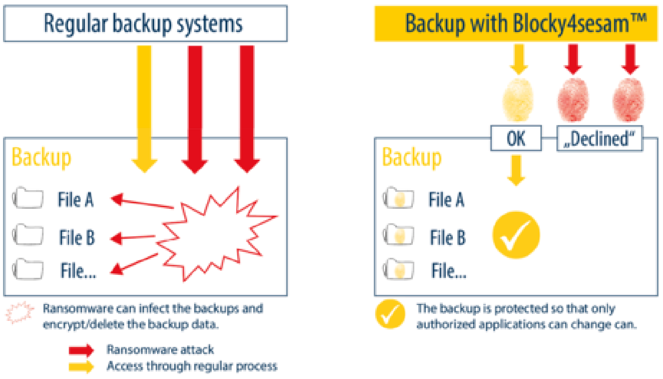
GRAU DATA's ransomware protection is a proven whitelisting technology for applications and as recommended by the BSI (German Federal Office for Security and Information Technology).

The functionality is designed in such a way that it is impossible to change or delete already saved backup data by external processes. To identify authorized accesses, Blocky4sesam™ uses the fingerprint of the application. Unauthorized accesses are immediately logged and reported to the administrator.

After the SEP sesam process has been added to the whitelist, it can write, read and delete at any time, while other applications or processes are denied access.

Features of Blocky4sesam™:

- **Immutability for an SEP RDS**
  ➪ Direct Attached Storage
- **Protects entire Windows volumes/partitions**
  ➪ ReFS, NTFS
- **Application whitelist protected access**
  ➪ check of the fingerprint
- **Write access only for the SEP sesam process**
  ➪ Protection against foreign applications
- **Requires the integrated SEP Software deduplication**
  ➪ Si3-NG
- **Well-known on the market**
  ➪ BlockyForVeeam, BlockyForTSM


Regular backup systems
Backup
File A
File B
File...
Ransomware can infect the backups and encrypt/delete the backup data.
Ransomware attack
Access through regular process
Backup with Blocky4sesam™
OK
„Declined"
Backup
File A
File B
File...
The backup is protected so that only authorized applications can change can.

Further safety measures of the protection of the components as described for SiS, also increase the safety here.

ⓘ https://wiki.sepsoftware.com/wiki/index.php/Blocky4sesam_Configuration

3.2.4 S3 Object Lock

When backing up data to S3 (Amazon Simple Storage Solution) cloud storage, Wasabi cloud storage, or another S3-compatible cloud implementation, you can use the object lock feature to protect data from modification or deletion. Object locking is a data protection feature that can be used to customize the immutability of backup objects. The retention time can be set to a fixed period or indefinitely, and no one can modify, delete, or overwrite a backup object until its retention time expires.

SEP sesam uses object retention in governance mode.
In governance mode, the SEP sesam backup user can add or extend the retention period for an object, but not shorten or remove it. If the retention period is set incorrectly (e.g. 100 years), the user can change this setting with the BypassGovernanceRetention user right.

ⓘ https://wiki.sepsoftware.com/wiki/index.php/Configuring_Si3_NG_Deduplication_Store_with_Object_Lock

3.2.5 Other Options of Immutability

Of course, there are not only the immutability options described in the previous chapters. The range is very wide, whereby not every option also requires a special implementation of the backup software.

Here are a few exemplary examples from real SEP customer projects:

3.2.5.1 Safemode Snapshots

HUAWEI

PURE STORAGE

Many storage types offer the option of generating read-only snapshots. These cannot be modified and the lifetime can also be defined by the customer. Backup software like SEP sesam can use these snapshots as additional restore points or for migration.

Examples are PureStorage FlashBlade or Huawei OceanStor Dorado..

e.huawei.com/eu/products/storage/ransomware

www.purestorage.com/solutions/data-protection/ransomware/safemode.html

3.2.5.2 HPE StoreOnce

Hewlett Packard Enterprise

Many dedup appliances offer the possibility to provide their data with an immutable flag. On the HPE StoreOnce SEP sesam reads this flag with the Catalyst API and considers the status when accessing the data.

support.hpe.com/hpesc/public/docDisplay?docId=sd00001027en_us&docLocale=en_US&page=catalyst_store_screens_properties.html

3.2.5.3 RDX

FAST LTA
We secure Petabytes.

Another possibility with SEP sesam is not only to swap out tapes, but also to create a real airgap with removable disks for the purpose of immutability for disk storage. FAST LTA or other RDX manufacturers are on the market here with the topic of cyber security.

https://wiki.sepsoftware.com/wiki/index.php/Configuring_Removable_Media

3.3 Virus Scanning

It is assumed that the data to be backed up has already been scanned at the source with a current virus scanner installed.

Best practise:

On the backup server the virus scanner often collides with the backup software and must be deactivated.

IKARUS
scan.engine

With the next version of SEP sesam the possibility of a virus check during restore was integrated. Since the time of the restore is typically some time after the backup, it can be assumed that the virus patterns to be applied then are more up-to-date and thus also take effect with more virus types. Infected files that are detected are reported and can be excluded from the restore. Since the scan brings considerable performance losses with it, it is to be activated as an optional function explicitly. The scan can run on both Linux and Windows systems.

The Ikarus Scan Engine uses sophisticated, high-performance scanning technology to analyze threatening content of all kinds. The Austrian product Ikarus serves as the algorithm in many commercial virus scanners as a basis and is thus widely used on the market as a quasi-standard.

ⓘ www.ikarussecurity.com/en/

3.4 Encryption

SEP sesam offers data encryption types on different levels:

Backup job encryption for backup sets (set in the backup job), Si3 encryption for Si3 Deduplication Store, and hardware-based LTO encryption for LTO tape drives (Generation 4 and later), which is done at the media pool level. For each encryption, you must create and store an encryption password.

ⓘ https://wiki.sepsoftware.com/wiki/index.php/Encryption_Support_Matrix

3.4.1 General Notes

An encryption virus encrypts ALL data present, regardless of whether it is already encrypted. Thus follows:

The encryption of backup data by the backup software protects against unauthorized access, but does not provide any protection against the extortion attempts of ransomware.

SEP sesam has integrated the following encryption technologies for its own use. The versions are constantly updated to ensure maximum security of the connections:

- **openSSL 1.1.1**
- **TLS2**

3.4.2 Communication

Various protocols, including encrypted ones, are available for backup server communication with the client:

- **sm_ssh (SEP sesam** SSH **based control communication)**
- **ssh**

ⓘ https://wiki.sepsoftware.com/wiki/index.php/Configuring_Clients

3.4.3 Transport

For the encryption of the data transfer SEP sesam offers the use of the https protocol as well as certificate-based connections.

https://wiki.sepsoftware.com/wiki/index.php/Step_2:_Clients

https://wiki.sepsoftware.com/wiki/index.php/Configuring_SSL_Secured_Communication_for_SEP_sesam_Backup_Network

https://wiki.sepsoftware.com/wiki/index.php/How_to_Replace_the_REST_Server_HTTPS_Certificate_and_Private_Key

3.4.4 Data at rest (SW, HW, Cloud)

3.4.4.1 Software

SEP sesam can encrypt backup data with modern algorithms (e.g. AES256). The password is assigned job-specific and can be stored either - also encrypted - in the SEP sesam database or externally.

For the restore, the password is either read automatically from the database and applied or it must be entered externally in a dialog box.

The password should be kept as secure as possible and not forgotten, otherwise the data can no longer be accessed. It is important to know that even SEP as the manufacturer can no longer read the data, as this would undermine the actual security purpose.

https://wiki.sepsoftware.com/wiki/index.php/4_4_3_Beefalo:Backup#encryption

3.4.4.2 Si3 Deduplication

SEP sesam provides encryption for Si3 deduplication to ensure compliance with data protection laws. It can be activated simply by specifying and confirming the encryption password. Here, each generated block is still encrypted with the IDEA algorithm after compression has taken place.

If an incorrect password is used, the Si3 service (SDS) terminates immediately after the password is checked.

Encryption with Si3 Replication

Si3 encryption is implemented in the read/write procedure of the file system. As a result, internal processing works with the raw data. When replicating an encrypted data store, the data is not transferred to the RDS in the encrypted state. The data is first decrypted on the source Si3 and then re-encrypted on the destination Si3. To ensure absolute security during replication from the source Si3 to the target Si3, a secure VPN connection must be used for the communication.

https://wiki.sepsoftware.com/wiki/index.php/Encrypting_Si3_NG_Deduplication_Store

3.4.4.3 Hardware

SEP sesam provides native support for managing hardware-based LTO encryption by enabling LTO encryption of tape drives at the media pool level.

With LTO encryption, data is transferred from the server to the tape drive via the HBA controller. Then the tape drive encrypts and compresses the data before writing it to or from tape (or decrypts it when it reads data).

The advantage here is the transfer of the load from the backup server / RDS to the LTO drive with integrated dedicated encryption chip, which results in a significant performance gain. In particular, the equivalent also applies to compression, which can still take place before encryption on the drive.

https://wiki.sepsoftware.com/wiki/index.php/LTO_Encryption

3.4.4.4 Cloud

For all cloud types possible with SEP sesam as backend storage of the Si3-NG data store (S3, Azure Blob), an encrypted connection is always established automatically. This is essential, especially for transmission over WAN. The data itself can be optionally encrypted before transmission according to chapter ‘encryption’.

https://wiki.sepsoftware.com/wiki/index.php/Backup_to_S3_Cloud_Storage

3.5 Multi Tenancy

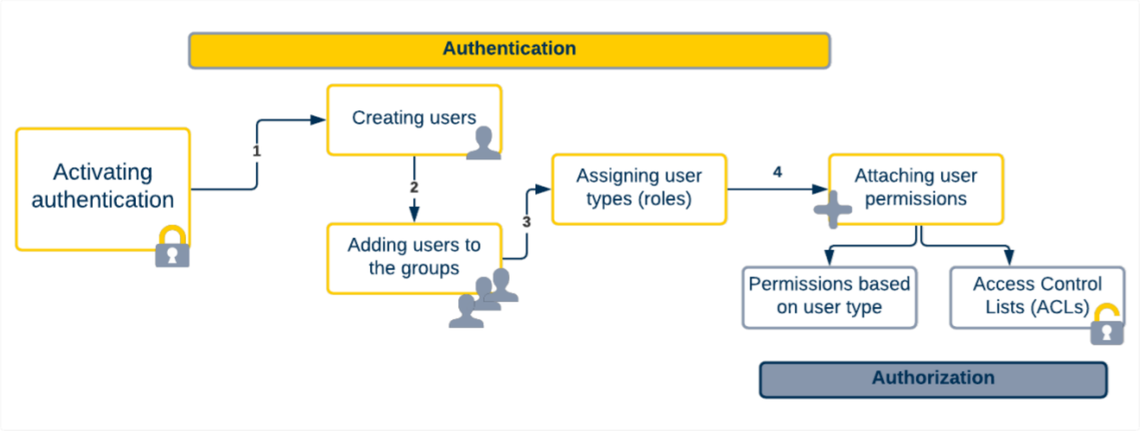
3.5.1 Authentication

SEP sesam offers different methods of authentication to limit the functional usage possibilities of a user:

- Policy-based authentication
- Database-based authentication

The latter can be used in combination with LDAP/AD authentication or to enable certificate-based authentication.

Only one authentication method can be active at a time. In the default case, policy-based authentication is enabled.


Authentication
Activating authentication
1
Creating users
2
Adding users to the groups
3
Assigning user types (roles)
4
Attaching user permissions
Permissions based on user type
Access Control Lists (ACLs)
Authorization

Policy-based authentication uses the sm_java.policy file to set the required user permissions. You can either edit this in the policy file or use the GUI to set the permissions by specifying user types (roles).

SEP sesam currently offers 5 user types. The following list shows the available user types and their corresponding rights.

- **Superuser**
  The only user type with full control over the SEP sesam environment (formerly Admin). This user type with superuser rights is automatically assigned exclusively to the administrator user if database-based authentication is enabled. If policy-based authentication is enabled, this user type with superuser rights is assigned to the Administrator, root and sesam users.
- **Administrator**
  Administrators can administer the SEP sesam system and access the GUI objects (except rights management) if not restricted by ACLs (Access Control Lists).
- **Operator**
  Operators can monitor the entire environment.
- **Backup**
  Backup users can access the GUI objects granted by ACLs. They are also allowed to start backups and restores.
- **Restore**
  Restore users can access the GUI objects granted by ACLs. They are allowed to start only standard restores.

Note that the displayed components and functions in GUI and WebUI depend on the user type.

3.5.2 Authorization

In addition to the default permissions (as described above) based on the selected user type, you can also set custom user roles by configuring ACLs if you have superuser privileges.

ACLs allow you to configure permissions for each user or group with fine-grained access rights for sites, clients, backup jobs (or groups), media pools, and schedules. For example, if you assign the Restore user permission to a specific backup job, that user can start the job-specific backup.

https://wiki.sepsoftware.com/wiki/index.php/About_Authentication_and_Authorization

3.6 HPE Catalyst

If the HPE StoreOnce DedupAppliance is used as a backup target, there are different connection options, depending on whether SAN or LAN are in use. In SAN the connection is possible as VTL, which is mapped in SEP sesam as a physical tape library. In the LAN it can be mounted as nfs storage or via iSCSI. These are all open interfaces and therefore offer potential attack surfaces.

Hewlett Packard
Enterprise

Alternatively, the StoreOnce can be accessed both in the SAN and in the LAN via the Catalyst API. Since Catalyst is a proprietary appliance-specific API, it is much more difficult to attack from the outside, which in fact provides additional protection against unauthorized access.

https://www.hpe.com/psnow/doc/A00042003ENW.pdf?jumpid=in_lit-psnow-getpdf

3.7 Verification of the Backup Data

A verification of the backup data is normally performed automatically by SEP sesam. For backups (also external backups), restores and migrations a checksum verification is applied to ensure proper data integrity.

It is also possible to activate an automatic verification process that starts a restore to a NULL device after a successful backup. It makes sense to configure this as a follow up event after the backup.

https://wiki.sepsoftware.com/wiki/index.php/SBC_CLI

https://wiki.sepsoftware.com/wiki/index.php/Follow-up_Events#Verify_saveset_after_the_backup

3.8 Reduction of the needed Ports

Instead of opening a separate port for each data stream (ftp protocol), by using the **http/https** protocols, data transmission can be restricted to a single port. Your firewall administrator will be happy to have to open only single ports instead of whole port ranges in his sanctuary. Open port ranges undermine the very purpose of firewalls and massively increase insecurity due to their indeterminacy. For this reason SEP sesam defaults the data transfer to http.

Default Ports (can be adapted for a firewall):

http: 11000
https: 11443

https://wiki.sepsoftware.com/wiki/index.php/List_of_Ports_Used_by_SEP_sesam

3.9 Remote Device Server (RDS)

SEP sesam Remote Device Server (RDS) is a storage management component that controls the preparation of data needed to back up a SEP sesam client and writes the backup data to the backup media. During a restore the RDS finds the correct backup sets and sends the data to the client. An RDS acts as a media server in a backup infrastructure.

RDS consists of three components: Sesam Transfer Protocol Server (STPD), Sesam Multiplex Stream Server (SMS) and SEP sesam Client (SBC) including remote access. Control over the jobs is provided by the SEP sesam Server. A separate RDS installation package is available for the installation.

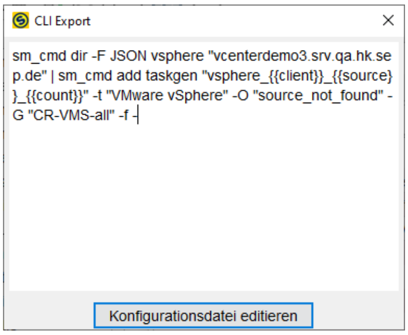
If the network includes multiple sites, you can manage storage devices across sites with a SEP sesam server (e.g. tape libraries or SAN devices located further away). However, if your infrastructure includes multiple sites that do not allow fast data transfer to the central SEP sesam server, a remote device server should be used to back up data to locally attached storage at a remote site. RDS enables efficient data transfer, reduces the load on the primary SEP sesam server and utilizes the storage resources available at the site.

For example, at remote sites, the RDS acts as a backup server and can either serve as a backup proxy to deliver data to the main server or store data on locally attached storage. By using RDS, one can easily and conveniently manage many remote sites from a central console.

In its function, the RDS is thus an important security component for adapting the backup infrastructure to predefined network structures and increases data security if, for example, the backup server and RDS are separated by a firewall and the backup data does not have to be routed through an open port in the firewall.

https://wiki.sepsoftware.com/wiki/index.php/How_to_create_a_Remote_Device_Server_(RDS)

3.10 Automatic Detection of Backup Objects



CLI Export

```
sm_cmd dir -F JSON vsphere "vcenterdemo3.srv.qa.hk.se
p.de" | sm_cmd add taskgen "vsphere_{{client}}_{{source}
}_{{count}}" -t "VMware vSphere" -O "source_not_found" -
G "CR-VMS-all" -f -
```

One experience from support shows that in crisis situations, the problem is often not the actual restore, but that important data was simply not backed up at all. Changes to the data infrastructure were inadvertently not tracked in the backup. And where there is no backup, nothing can be restored either.

Exactly for this situation SEP sesam can provide a remedy.

An algorithm detects new backup objects (VMs or databases) and automatically creates new backup jobs according to predefined rules, so that the new objects are immediately backed up and never forgotten. Since the rules are designed like a programmable interface, it offers a wide range of definition possibilities. For example, new VMs can be classified according to regular expressions of the VM names or filters of the metatags according to productive or test VMs and backup jobs can be created automatically in predefined job groups or schedules.

This powerful tool can be applied not only to all hypervisors supported by SEP sesam, but also to some databases such as MS SQL.

No important VM or DB is ever forgotten again and the completeness of backups is absolutely ensured.

i https://wiki.sepsoftware.com/wiki/index.php/Automating_Backup_Process

3.11 Intentional Deletion of Backup Data

Normally, the deletion of backup data is regulated by the retention periods defined in the media pools and is performed automatically by the backup server.

Intentional deletion of backup data, on the other hand, can be done with malicious intent; in this case, the use of SEP Immutable Storage, for example, can provide protection. However, it may also be necessary due to regulations such as GDPR regarding the deletion of personal data when an employee leaves. This process is known as the "right to be forgotten" (RTBF).

When deleting backup data, it is important to pay very close attention to granularity.

For tape backups the deletion of a complete medium is possible with SEP sesam. Here SEP sesam 'only' deletes the entries in the sesam database. This means that the data itself on the tape is not deleted, but a restore via the backup software is no longer possible. This is sufficient to meet the requirements of the GDPR.

On disk storage, however, the user can cause intentional deletion even of individual backups by setting the EOL of a backup to 'today', for example, and initiating the cleanup manually.

i https://wiki.sepsoftware.com/wiki/index.php/Tape_Management#expire

4 Concept Elements

4.1 Automated Updates and Patches

Often, current updates are ignored or postponed. For attackers, this is the best way to break into a system when security updates are omitted. Keeping systems and software up to date is also a guarantee of value.

SEP sesam offers individually configurable automatic update algorithms, also via GUI.

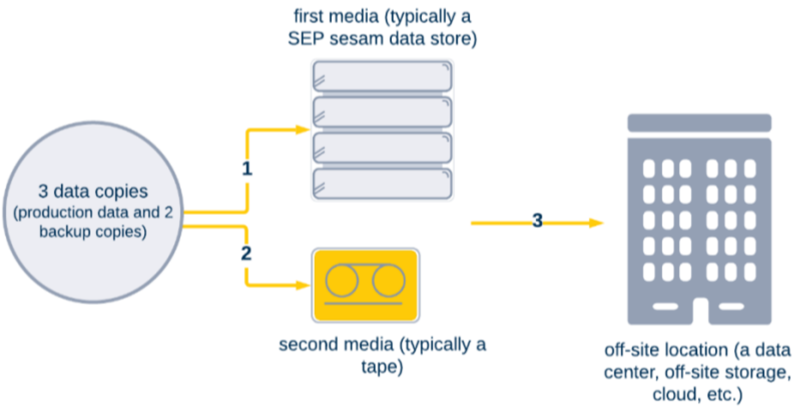
Although an automatic update of all clients is very convenient, it also involves certain risks. Downloading the updates or patches to a repository with subsequent isolated testing and planned rollout in the environment would be the safer option.

https://wiki.sepsoftware.com/wiki/index.php/Updating_SEP_sesam

4.2 3-2-1 Backup Strategy

A backup concept should at least
keep 3 copies of your data at the same time (original + backup + copy),
use 2 different media types (e.g. disk and tape) and
save 1 copy at a remote location.

The 3-2-1 rule is the golden rule of data security. It describes the necessary elements of a backup concept to generate a maximum of security for your backup data, because these are also exposed to multiple attacks from HW defects to failures of entire sites to natural disasters. In fact today the library will often be replaced by the cloud to a 3-1-2 concept.


first media (typically a SEP sesam data store)
3 data copies (production data and 2 backup copies)
1
2
3
second media (typically a tape)
off-site location (a data center, off-site storage, cloud, etc.)

https://wiki.sepsoftware.com/wiki/index.php/Backup_Strategy_Best_Practices

4.3 Disaster Recovery

Disaster Recovery is an important topic to ensure the fast recovery after a total failure of individual clients, the backup server, entire data centers or even entire sites after disasters.

DR is not just a functionality, but always a concept, i.e. an operation description to be tested extensively. Only through intensive multiple testing and documentation can a smooth process be guaranteed in a crisis. Example: You are stuck in the DR process because an important password for the required authorizations is missing.

4.3.1 BMR for Physical Servers

4.3.1.1 Windows

SEP sesam BSR Pro is a fast and efficient disaster recovery solution for Windows systems. It is based on O&O DiskImage. This solution allows you to restore a fully functional Windows system in the shortest possible time. You can easily restore your system to the same or different (dissimilar) hardware using a small GUI. This succeeds, since missing drivers can be reinstalled at restore time.

https://wiki.sepsoftware.com/wiki/index.php/SEP_sesam_BSR_Pro_for_Windows

4.3.1.2 Linux

The SEP Bare Metal Recovery module for Linux is fully integrated into the SEP sesam client installation to ensure fast and complete system recovery. Relax-and-Recover (ReaR) is a Linux BSR recovery solution (based on GPL license) that is easy to set up and requires no maintenance. In case of a disaster, the system can be recovered either on the same hardware or on compatible replacement hardware from an external medium such as USB stick, DVD or netboot of the image.

https://wiki.sepsoftware.com/wiki/index.php/Bare_Metal_Recovery_Linux

4.3.2 Disaster Recovery of the Backup Server

To protect against failures, a daily backup of the backup server is strongly recommended. The possibility of DR of a complete backup server is based on this, because neither BSR Windows nor BSR Linux can be applied for this. It restores itself and its data (DB, Lisfiles, etc.) from the existing backups. This process is documented in detail in the SEP Wiki.

https://wiki.sepsoftware.com/wiki/index.php/SEP_sesam_Disaster_Recovery

4.3.3 DR at a second location

The aim here is to keep backup data from one site (especially VMs) at a second site. In the event of a site failure, the environment can be brought up again at the second site and productive operation can be resumed there. Performance losses in operation are accepted temporarily.

Depending on the requirements and specifications regarding RPO and RTO, DR can become very complex. It is a concept that can be based on a variety of different technical implementations, each with its own advantages and disadvantages. The topic of DR alone would give more than enough content for a separate white paper and can therefore only be briefly touched. Here is a selection of the possibilities:

- The backup data can be moved to the other site. Either by mirroring the storage HW or by using SEP Si3 deduplication or the replication capabilities of a dedup appliance such as HPE StoreOnce Catalyst Copy.
- The secondary site can be a pure failover site (different fire protection zone) or even a productive data center in a branch office.
- It can have there a second productive backup server where the replicated backups are imported, only one failover backup server in standby mode or a RDS that mutates to a backup server in DR case.
- The metadata of the backup server can be transferred with rsync or reside on shared storage.
- The cloud as shared storage for any type of data is now also a real option. Depending on the cloud provider, even the cloud itself can be used as a DR location via IaaS or Paas.
- VMs can either be restored to a second virtualization environment on demand, kept permanently via automated restore or quickly made productive via instant recovery.

Since a mature DR concept with ist many options is based on well-founded experience, we strongly recommend that every customer purchase a paid service here. It is worth it!

i https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery

4.4 Restores

4.4.1 Automated Restores

In SEP sesam, restore jobs can be saved and attached to a schedule as events. This way restores can be automated, e.g. to ensure the restore of critical VMs. Likewise you can restore to a zero device, in order to verify only the readability of a backup.

In our experience, an automated restore can be a requirement of an internal method manual or an external requirement (e.g. BSI).

https://wiki.sepsoftware.com/wiki/index.php/Scheduling_Restore

4.4.2 Ransomware Isolation

To secure the IT environment against infected data, a restore to an isolated environment is recommended in potential cases. Especially with VMware, restoring to a sandbox separate from the network is very easy with the SEP WebUI Restore Assistant or the GUI Restore Wizard.

https://wiki.sepsoftware.com/wiki/index.php/VMware_Sandbox_Restore

4.5 Experiences from SEP Support

? **How customers behave after a virus attack?**

! *In all known cases to date, an investigation and analysis team of external specialists was first engaged to determine the time, extent and course of the infection, among other things. In all infection scenarios, the backup infrastructure was also attacked due to inadequate security measures. In order to restore this, SEP's professional help was therefore called upon as a service - usually at the same time. Since the entire infrastructure at the customer's site had often collapsed, in some cases only on-site deployment was an option.*

? **What were the basics of a successful recovery?**

! *In order to access the backups of the affected systems, the backup infrastructure itself had to be rebuilt first. Unfortunately, it often turned out that the "head" of the backup infrastructure - the SEP sesam server - was inadequately backed up by the user or only on ransomware unprotected backup media. In any case at least a part of the backups of critical systems were on tape, so they could be re-imported with some time effort even without a Sesam self-backup. If a backup of the Sesam server was available, some time could be saved. In none of the cases Backups-on-Disk could be accessed anymore. Extended, unencryptable backup targets (Immutable Storage) were unfortunately not in use in any of the cases.*

? **What was the process of a successful restore?**

! *Once the backup infrastructure had been restored to the best possible state, the procedure was generally always the same: A dedicated, isolated system was restarted as the first restore target ("sandbox" concept). Using the time of infection identified by the analysis team, backup sets written before the infection could now be restored to the "sandbox" system. Once a backup set had been successfully restored to the sandbox, the system was scanned and/or targeted for traces of the identified virus by one - or preferably more - antivirus programs. Only after a* *successful scan was the last step to restore the system to the actual, productive target system.*

? **What are the findings after such a serious incident?**

! *A ransomware virus attack that has been survived practically always creates a dramatically heightened sensitivity to the issue of data protection among customers. New strategic IT projects are launched - usually under the watchful eye of management. IT security and backup concepts are revised. Budgets for new HW (e.g., additional backup storage options) are suddenly no longer an issue and are released immediately. Often, additional external IT security specialists are brought in.*

? **How well you can rely on SEP sesam in case of emergency?**

! *Clear statement: "Never before has a SEP customer had no data available for a successful restore after a ransomware attack! ".*

5 Regulations

5.1 Germany and EU

5.1.1 Legal Storage Requirements

Every company must comply with the generally applicable laws of its state regarding the storage of its data. These laws classify data according to various criteria such as type of data, industry of the company, data format (analog/digital), etc. But not only storage is regulated, in many cases the deletion of data is also prescribed.

ⓘ https://commission.europa.eu/law/law-topic/data-protection_en

5.1.2 General Data Protection Regulation (GDPR)

The General Data Proection Regulation (GDPR), which came into effect in 2016 and was applied in 2018, standardizes the rules for processing personal data by companies, authorities, and associations based in the European Union. The term is "General Data Protection Regulation (GDPR)", the official name "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC". The handling of customer and employee data, data of citizens, etc. is clarified in eleven chapters with a total of 99 articles in connection with data protection.

The regulation applies in all member states and has implications for other countries and their private and public institutions. There are technical, economic, social, and individual aspects involved. Technically neutral regulations exist that can encompass social media and artificial intelligence. The right to be forgotten is formulated, that is, the right to delete (access to) personal information, as well as the right to freedom of information (access to information) and data portability. Principles such as Privacy by Design (data protection is already considered in the design of systems) and Privacy by Default (data protection is the norm, although the user may be able to weaken it themselves by adapting the services or devices) are anchored.

For the particularly serious violations listed in Article 83(5) GDPR, the maximum fine is up to €20 million or, in the case of a company, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

ⓘ https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

5.1.3 No-Spy Rule of the BMI (Federal Ministery of Interior and Community in Germany)

The No-Spy Clause or No-Spy Guarantee is a self-declaration in the procurement process and a contract clause in public contracts in which contracting parties of the public sector assure that they are not legally obliged to disclose confidential information to foreign intelligence or security agencies. Although the self-declaration and contract clause do not prevent data disclosure, they facilitate the burden of proof and the termination of the contract in case of a violation.

Software
Bundesverband IT-Mittelstand
Made in Germany
100%
Service
Qualität
Zukunft

The requirement for the self-declaration and the addition of contract templates for public contracts with the No-Spy Clause was instructed by the Federal Ministry of the Interior in a decree dated April 30, 2014, for federal public contracts. The federal states gradually followed this demand for new contracts with IT companies, which was triggered by the NSA scandal and Edward Snowden's revelations, which made it possible for information to flow out through IT partners of the public sector.

SEP complies with the No-Spy Rule of the BMI.

i https://www.bmi.bund.de/EN/topics/it-internet-policy/data-protection/data-protection-node.html

5.1.4 KRITIS

„Critical infrastructures (KRITIS) are organizations or facilities that are of vital importance to the state community, and whose failure or impairment would result in sustained supply shortages, significant disruptions to public safety, or other dramatic consequences.“
KRITIS definition of the federal ministeries

Sectors and who can be KRITIS:

- Information technology & Telecommunications
- Health
- Energy
- Water
- Nutrition
- Finance and insurance industry
- Transport and traffic
- Municipal waste and disposal
- State/ administration
- Media & culture
- Companies of special public interest
- Digital infrastructure

Bundesamt
für Sicherheit in der
Informationstechnik

All organizations from these sectors, regardless of their size, are counted as critical infrastructures (KRITIS). This entails, among other things, increased requirements for data protection and therefore also for backup software.

SEP has a large number of customers in the KRITIS sector and therefore has extensive experience with the special challenges and necessary concepts of this clientele.

ⓘ https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html

5.1.5 NIS2

EU NIS2 is the European framework for operators of critical infrastructure. This directive sets the minimum cyber security requirements that these companies in one of the 18 sectors will be obligated to follow from 2024. This applies to companies with more than 50 employees and 10 million euros in revenue.

NIS2 replaces the previous NIS directive.

ⓘ https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

5.1.6 Cyber Resilience Act

In September 2022, the European Commission presented a draft of the Cyber Resilience Act (CRA), which aims to improve the cyber security of products that can be connected to each other or to the internet. These products are manufactured by companies and sold to end customers.

ⓘ https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

5.2 Agreements with the USA

5.2.1 SCHREMS 2

Practical effects of the European Court of Justice's jurisprudence on international data transfer (case C-311/18 "Schrems II“):

The European Court of Justice clarified with its ruling that personal data of EU citizens may only be transferred to third countries if they enjoy a level of protection essentially equivalent to that in the EU. For the USA, it denied such an adequate level of protection.

ⓘ https://en.wikipedia.org/wiki/Max_Schrems

5.2.2 Safe Harbour / EU-US Privacy Shield (expired)

For the purpose of data protection at the destination, especially of private data, the exchange of data between states has always been regulated by EU agreements.

In particular, there have been separate agreements with the USA, whose companies and globally offered services and products have been affected. However, especially the access possibilities regulated by law in the USA (PATRIOT Act/CLOUD Act) repeatedly led to the agreements being suspended and unsettled the international IT market.

After the decision in 2015 to declare the Safe Harbour Agreement invalid and the failed EU-US Privacy Shield in 2020, the President of the European Commission Ursula von der Leyen and the President of the USA Joe Biden agreed on a new transatlantic data protection framework (EU-U.S. Data Privacy Framework). On December 13, 2022, the European Commission announced the draft of an adequacy decision for the planned EU-U.S. Data Privacy Framework. This data protection framework should again make it possible to use tracking/analytic and marketing tools from the USA without problems. In addition, the use of standard contractual clauses should be a thing of the past. However, until then, you will transfer personal data illegally to the USA if you use U.S. tools that send such data to the USA.

https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles

https://en.wikipedia.org/wiki/EU%E2%80%93US_Privacy_Shield

5.2.3 PATRIOT Act

The USA PATRIOT Act is a US federal law that was passed by Congress on October 26, 2001, in the context of the war on terrorism. It was a direct response to the terrorist attacks on September 11, 2001.

USA PATRIOT Act stands as backronym for
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

Parts of the law expired on June 1, 2015, and were replaced the next day on June 2, 2015, by the provisions of the USA Freedom Act.

The provisions of the PATRIOT Act allow US authorities such as the FBI, NSA, or CIA not only access to the servers of US companies without a court order but also require foreign subsidiaries to grant access to their servers, even if local laws prohibit this.

https://nl.wikipedia.org/wiki/USA_PATRIOT_Act

5.2.4 CLOUD Act

In 2018, the Patriot Act was expanded by the former US President Donald Trump to include the CLOUD Act (***Clarifying Lawful Overseas Use of Data Act***).

The law requires American internet companies and IT service providers to grant US authorities access to stored data even if the storage does not take place in the US. Conversely, foreign companies can also access data stored abroad by US corporations through this process.

As a result of the law, bilateral agreements are to be worked out that would enable foreign authorities to make their requests directly to the corporations. This would bypass judicial oversight in an inquiry, which has led to criticism by data protection advocates.

The law was introduced after US authorities had problems accessing data stored abroad in various cases. Prior to the passage of the law, companies could rely on the fact that a search warrant only had validity in the US. Under the law, internet companies and IT service providers may be prohibited from informing their users about such covert requests for user data.

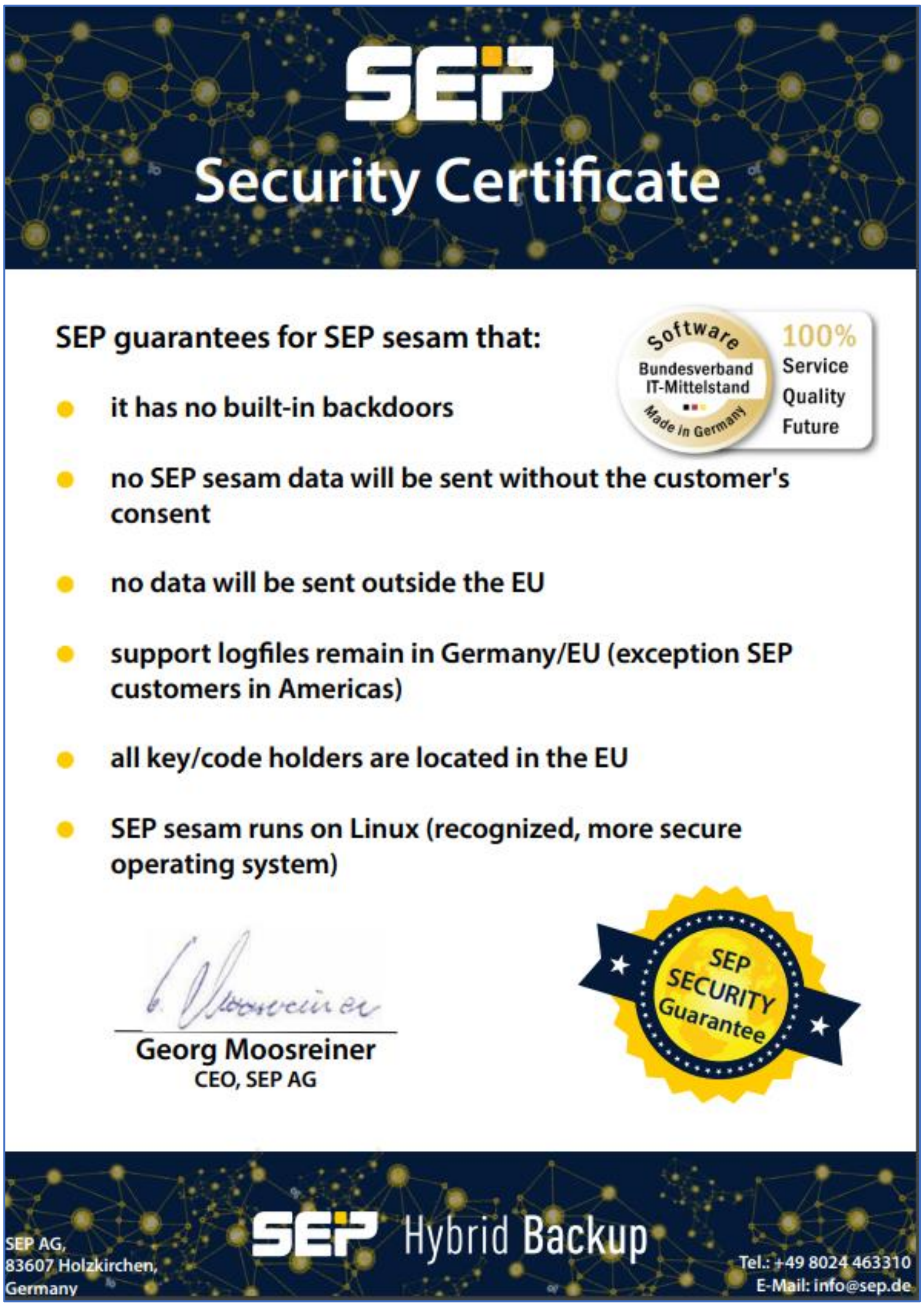
The US privacy organization Electronic Frontier Foundation called the CLOUD Act a "dangerous law". The law is "nothing less than an invasion of privacy and a curtailment of fundamental rights“.

ⓘ https://en.wikipedia.org/wiki/CLOUD_Act

5.3 SEP sesam „Made in Germany“

Not only do EU laws apply in Germany, but also the strictest data protection rules known.

SEP sesam, as a product of a medium-sized German software company, can thus boast several advantages that greatly simplify compliance with legal regulations such as GDPR or the No-Spy Rule. This not only applies to the fact that the state has no access to the data (no backdoors), but also that in the event of support and remote maintenance or sending of log files, the location of the data and information is ensured to remain within the EU. This is confirmed by SEP with a signature on a certificate.



Security Certificate

SEP guarantees for SEP sesam that:

Software
Bundesverband
IT-Mittelstand
Made in Germany
100%
Service
Quality
Future

- it has no built-in backdoors
- no SEP sesam data will be sent without the customer's consent
- no data will be sent outside the EU
- support logfiles remain in Germany/EU (exception SEP customers in Americas)
- all key/code holders are located in the EU
- SEP sesam runs on Linux (recognized, more secure operating system)

Georg Moosreiner
CEO, SEP AG

SEP
SECURITY
Guarantee

SEP Hybrid Backup

SEP AG,
83607 Holzkirchen,
Germany

Tel.: +49 8024 463310
E-Mail: info@sep.de

SEP sesam is optimally suited to fully comply with the regulations of all institutions (such as state of the EU)!

https://www.sepsoftware.com/solutions/sep-security

6 Conclusion

With the extensive protection in SEP sesam, data can be recovered even after undetected cyberattacks.

SEP is one of the most robust and scalable backup solutions on the market today. Centralized management to manage all backup agents and servers, whether local or remote, makes it the perfect solution and can be deployed from small to large enterprise environments.

Many integrated agents and functionalities as well as the large support matrix leave nothing to be desired.

Experience the benefits SEP has to offer. You can find our contact details and a 30-day trial license incl. demo support on our homepage.

ⓘ www.sepsoftware.com

Contact

SEP AG
Konrad-Zuse-Straße 5
83607 Holzkirchen
Germany

+49 8024 46331-0

info@sepsoftware.com

1.

Try the 30-day full version now!

The SEP sesam 30-day full version includes all functions for optimal data backup & recovery, as well as a personal demo support.

2.

SEP sesam Support Matrix

SEP sesam supports a large portfolio of operating systems, databases, virtualization platforms, applications and hardware snapshots.

3.