



netfiles

Security Concept

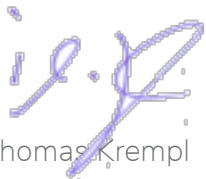
Focus on Security

netfiles is a virtual data room for secure online collaboration and the secure exchange of files and documents beyond company boundaries.

In order to provide these services, the most important aspects are service availability and data security. Our main objective is to ensure that all actions carried out by authorized users in the virtual data room remain confidential, and that your data is reliably protected from unauthorized access.

To achieve this, netfiles uses the most modern software, encryption and security technology and invests in the continuous development and improvement of application and system security, and of internal processes.

The purpose of this document is to give you an overview of netfiles security features, so that you can see in detail what security measures we undertake, and to further underline our company's commitment to your data security.

A handwritten signature in blue ink, appearing to read 'i. Kremp', with a stylized flourish.

Thomas Kremp
Managing Director

User Authentication and Document Access

Authentication

Access to a netfiles data room is possible only with a valid combination of user name and password. Users define their own password the first time they log in, so no one but users themselves know their password. netfiles screens the quality of each password and does not permit unsafe passwords. In addition, data room administrators can define password guidelines to also accommodate company-specific requirements regarding password quality.

netfiles never stores any passwords in plain text. Users' passwords are stored exclusively as what are known as hash values, the result of a special encryption method.

Two-Factor-Authentication

Starting with netfiles Professional, netfiles offers you an additional security option for the login with the Two-Factor-Authentication. Two-Factor-Authentication, which is well known from online banking, offers security on top of your username and password, protecting against unauthorized or inadvertent sharing of the password. In order to log in to the system, the user must enter a security code that is sent to his mobile phone by text message or generated by an Authenticator/OTP app (One Time Password) on a smartphone.

Access Rights

A flexible permissions system with read and write access allows you to define and monitor exactly the access rights that are assigned to each member of the data room. Only project members that have been personally invited to the data room by an administrator can access project data. netfiles is designed in such a way that a user only ever has access to the documents and folders to which he has the appropriate access rights, assigned to him by the data room administrator. All other documents remain invisible and inaccessible to him. Particularly confidential documents can be additionally protected by preventing downloading or printing. Starting with netfiles Professional, extended document protection with a personalized watermark is also possible.

Data Encryption

SSL/TLS Encryption

After login, all data communication between the user's web browser and the netfiles application servers is 256-bit SSL-encrypted (or TLS 1.2 where this is supported by the browser). This method reliably prevents third parties from intercepting or compromising data communication via the Internet. The method – the same one that is used for Internet banking – guarantees that both the login data passed between your computer and netfiles and any documents you upload to or download from netfiles are securely encrypted. The possibility that data might be spied on during transmission can therefore be virtually ruled out. The TLS certificate used for the netfiles servers is from the German trust center TeleSec of Deutsche Telekom AG.

The security of the SSL/TLS encryption of the netfiles server can be checked at any time via the well-known Qualys SSLlabs test:

<https://www.ssllabs.com/ssltest/analyze.html?d=www.netfiles.de&hideResults=on>

Perfect Forward Secrecy

netfiles uses the Perfect Forward Secrecy method for SSL/TLS key exchange. The protection given to SSL connections is such that even recorded copies of encrypted data transactions cannot be decrypted retroactively with the methods available today.

Document Encryption

All files in a netfiles data room are stored in encrypted form on the application servers. Uploaded files are encrypted with a 256-bit Advanced Encryption Standard (AES) key that is valid only for the data room in question. This encryption method is designed to ensure that no one apart from authorized data room users – not even the personnel who oversee netfiles GmbH's data center operations – can access unencrypted documents.

The strict legal requirements for professional secrecy holders (§203 StGB) are met when using netfiles.

netfiles Mobile App

Depending on the user's access rights, the netfiles mobile app stores files for offline use in the mobile device file system. These files are encrypted by an encryption mechanism of the netfiles mobile app with a newly generated AES 256-bit key in addition to the operating system encryption every time the app is set up.

The document contents are encrypted in the same way as information about the documents. Internal operating system caching is deactivated in the netfiles mobile app. This means that, with the exception of files stored in encrypted form for offline access, no readable data remains on the mobile device.

Virus Protection

netfiles reliably checks every uploaded document for computer viruses, ransomware and other malware, thus preventing the spread of infected data via the data room. This protection is always activated and cannot be switched off by data room administrators.

The virus definitions used are updated hourly. This ensures that new threats are detected promptly and reliably. The scan also includes MS Office files including macros. The netfiles server hardware is dimensioned in such a way that even under full load no bottlenecks can occur and all uploaded files are scanned for viruses without exception.

Audit Trail

As administrator of a netfiles data room, you have access to an extensive log of all time-stamped actions and user events.

You can use this log to prove exactly who uploaded, viewed, modified, downloaded or deleted which document and at what time. You can also see when a user logged into or out of the data room.

netfiles ensures that this protocol cannot be changed afterwards. This means that the log can also be used in legal disputes.

High-security data centers in Germany

For the provision of its services, netfiles GmbH uses the data centers of noris network AG in Germany, which are designed according to the highest security standards. Like netfiles GmbH, noris network AG is a German company.

The ISO/IEC 27001 and ISO 9001 certified data centers of noris network AG ensure "365 days/24 hours" monitoring, multi-level access control, video surveillance, automatic fire protection systems, redundant climate monitoring and uninterruptible power supply. The servers and storage systems of netfiles GmbH are located in separate server cabinets within the data center. These are secured in such a way that only employees of netfiles GmbH or persons authorized by netfiles GmbH have access.

netfiles uses two geo-redundant data centers (Munich and Nuremberg) of noris network AG to provide its netfiles service.

Availability

The netfiles service is available via the URL netfiles.de 365 days a year from 00:00 to 24:00. netfiles GmbH guarantees an average monthly availability of 99.9%. Several times a year, netfiles GmbH performs updates to its systems. This requires maintenance windows of up to 4 hours each up to four times a year.

Downtime due to this maintenance work does not count towards the guaranteed availability mentioned above. Maintenance windows will be announced to all users at least three business days in advance via a notification displayed when logging into the netfiles application. Scheduled maintenance usually takes place outside normal working hours, i.e. between 22:00 and 06:00 or on weekends.

Availability is measured by an external service provider and can be viewed at any time via the Internet (<https://secure-stats.pingdom.com/jlwrhmwhbzoe/512122>).

To ensure the availability of the application, netfiles works with the following components.

Redundant hardware

All hardware systems used by netfiles are equipped in such a way that all components, which can usually fail, are designed redundantly. This means that all server components, such as power supplies, hard drives, Ethernet ports, etc. are designed redundantly and a failure of these components will not result in the failure of the server.

netfiles keeps all necessary spare parts of the most important components in stock in order to be able to replace them as soon as possible in case of a defect. There are maintenance contracts with the manufacturers, which guarantee a complete hardware replacement within 24 hours.

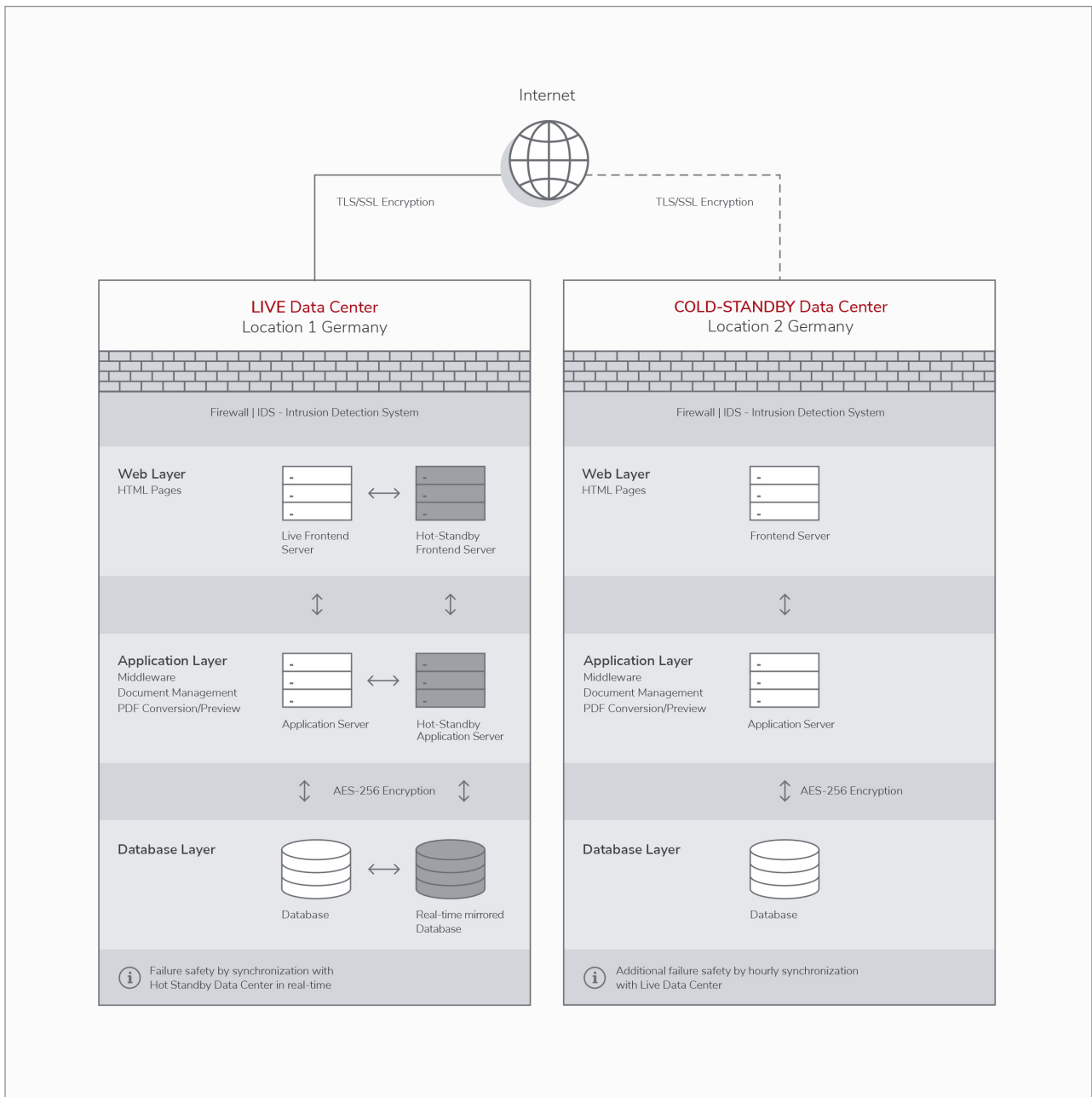
Hot-Stand-By Systems

All netfiles software components run on virtualized servers. This has the advantage that in the event of a hardware failure, any virtual server running on it can be started on another hardware at any time.

In the productive data center, at least two instances of each required virtual server are always running. Thus, in the event of a hardware failure, all functions of the virtual server instances running on it can be immediately taken over by another instance running on different hardware without failure.

All netfiles data is stored in a redundant storage system. All data is stored exclusively on Raid (1 or 6) mirrored disks. Both storage systems are automatically synchronized in real time via the network. This means that in the event of a storage system failure, the hot standby system can immediately take over operation of the netfiles application without any data loss.

Security architecture of netfiles data centers



Redundant Internet Connection

The data centers are redundantly connected to the German Internet backbone via several connections. All routers, switches and Internet access points are fully redundant. This ensures an uninterrupted connection to the Internet.

Desaster Recovery

The geo-redundant cold-standby data center can take over all tasks of the primary data center within a very short time using identical infrastructure and hardware, as well as mirrored data. The disaster recovery is certified according to ISO 22301.

Thus, even in the event of an extraordinary disaster, for example the complete, permanent failure of the main data center, continued operation with minimal downtime and data loss is guaranteed to the same extent and quality.

Backup

In addition to the copies on the productive storage, the hot-standby storage and the cold-standby storage, all data is completely backed up to the backup storage once a day. Snapshots of the last 30 days are stored there. This means that it would be possible to restore a status up to 30 days back if necessary. All backups older than 30 days are automatically deleted.

A full backup is restored once a day in the primary data center on a separate netfiles test system. The backup is tested for usability. This ensures that the data is not only backed up to the backup server, but can also be restored and used in an emergency.

Protection Against Outside Access

Security measures against cybercrime (hacker attacks) are of particular importance for netfiles and are continually being further developed.

Firewall Systems

netfiles uses a multilevel security system with double firewall protection. This guarantees highest levels of security and optimal protection against third party attacks. We use leading and proven security software, such as high-availability firewall clusters from the market leader Checkpoint.

Intrusion Detection System

All systems are continuously automatically monitored for any possible attacks over the Internet. If any suspicious activity is noticed, necessary steps can be taken by the system administrators, who are available 24/7.

Security Audit

The netfiles application and the protection mechanisms described herein are regularly tested by extensive security and penetration tests. The tests are performed by recognized service providers who specialize in security testing and penetration testing.

Data Protection

Strict Data Protection

netfiles GmbH is a German business with its registered office, development and hosting all located in Germany. netfiles GmbH works according to the strict EU data protection guidelines (GDPR) and the legal requirements of the Federal Republic of Germany, in particular the Federal Data Protection Law ("BDSG") and the Telemedia Act ("TMG"). Contrary to the provisions of the US American Patriot Act, for example, which are valid for the European subsidiaries of US companies, German law places no obligation on companies to disclose customer data to foreign security authorities.

Access to user data and documents in the data room is even not possible for employees of netfiles GmbH.

GDPR Compliance

In accordance with legal requirements, netfiles GmbH concludes an order processing contract with its customers in accordance with § 28 GDPR, which regulates the obligations of netfiles GmbH with regard to the processing of personal data.

The corresponding extensive technical and organizational measures (TOM) of netfiles GmbH for data protection are regulated in the separate document "Technical and organizational measures according to DSGVO" (<https://www.netfiles.de/downloads/Technical-and-organisational-measures-netfiles.pdf>).

The data protection officer of netfiles GmbH continuously supports and monitors compliance with all relevant data protection regulations. In addition, he sensitizes and trains all employees involved.

netfiles GmbH assures you that all requirements of the GDPR are met.

ISO/IEC 27001:2013 Certification



The certification unit of TÜV SÜD Management Service GmbH certifies that netfiles GmbH complies with the requirements of ISO/IEC 27001:2013, attesting that netfiles GmbH has introduced and uses a documented information security management system which covers its "marketing, operational and support activities for the netfiles application for virtual project and data rooms". This management system also meets the requirements of ISO 27017:2015 for the implementation of cloud services and ISO 27018:2014 for the protection of personal data in public cloud services.

The process of acquiring ISO 27001 certification involves auditing IT security procedures and validating data protection and information security.

ISO 22301:2019 Certification



The Business Continuity Management System of netfiles GmbH has been certified by TÜV Rheinland according to ISO 22301:2019.

BSI C5 Compliance



netfiles meets the requirements for the security of cloud services defined by the German Federal Office for Information Security (BSI) in the Cloud Computing Compliance Criteria Catalogue (C5).

SOC 2 Certification



netfiles GmbH has been successfully audited by an independent auditing firm for compliance with the "Trusted Criteria" on data security and data protection according to the internationally recognized SOC standard (System and Organization Controls).

IT Security made in Germany



netfiles GmbH is a member of TeleTrusT - Bundesverband IT-Sicherheit e.V. and bearer of the TeleTrusT quality seal "IT Security made in Germany".

Trusted Cloud



netfiles is recognized by the German Trusted Cloud Network (Kompetenznetzwerk Trusted Cloud e.V) as a trusted secure cloud service and hold the "Trusted Cloud" seal of approval.

The Trusted Cloud Project is funded by the German Ministry of Economic Affairs and Energy.

Alliance for Cyber Security



netfiles GmbH is a participant in the Alliance for Cyber Security. With the Alliance for Cyber Security, the BSI has been pursuing the goal of strengthening Germany's resilience to cyber attacks since 2012.

netfiles GmbH
Marktler Strasse 2b
D-84489 Burghausen
Phone +49 8677 91596-10

www.netfiles.com
sales@netfiles.com