

Security and Privacy at SYNCING.NET



"Your privacy and safety come first SYNCING.NET. One of the foundations of our file and Outlook synchronization product is that no data content is ever permanently stored on our servers. We have taken comprehensive measures to ensure the security and privacy of your data."

Our customers deserve the highest level of safety when sharing their valuable data using SYNCING.NET. Our security policy includes the following components:

- Data center security
- Network security
- Application security
- Privacy Policy

Data center security

Our data center is located in Berlin, Germany. It is a safe place for mission-critical applications, operated by T-Systems, a subsidiary of Deutsche Telekom AG. Our servers are fully redundant and use highly reliable MySQL database replication.

Performance Data:

- 100% UPS-backed power supply
- Redundant gigabit connectivity to 3 different carriers
- Redundant diesel generators
- Redundant database
- 24 / 7 video monitoring

Network Security

Encryption

All data transfer is secured using industry standard 1024-bit RSA and 256-bit AES end-to-end encryption. Each computer is assigned a unique public and private key for both user and message authentication.

Authentication and Encryption Details

At the beginning of each session, the sending peer (peer A) signs the header of a special communication packet with its private 1024-bit RSA key, encrypts it with the public key of destination peer, and sends this authentication packet to the destination peer (or to the server). The destination peer (peer B) can decrypt the header with its private key, and verify the RSA header came from the right peer (and was not modified in transit) using the sending peer's public key. The public keys are stored on the server and accessible by all peers in the same network.

After verifying the connection came from the right peer (messages from unknown peers are just ignored), peer B sends a 256-bit AES session key to peer A. This session key is also RSA encrypted using peer's A public key. If a wrong peer (e.g. a middle man attack) receives the data, it can't decrypt the RSA data containing the session key without the private key of the destination peer.

All data transmitted between both peers during this session is encrypted and decrypted using the 256-bit AES session key (end-to-end encryption). The key expires when the session ends. Each following session uses another key generated as described above.

Neither SYNCING.NET Technologies nor other peers that are not in the same network are able to decrypt the data, as they don't know the secret session key!

The reason for this double keying (AES + RSA) is that AES symmetric encryption/decryption is fast, so it is used for the bulk of the transfer. However, the same (symmetric) key needs to be known to both peers exchanging the data. RSA 1024-bit encryption/decryption algorithm uses a public/private key pair and it is very strong/secure but also slow and CPU-intensive, so SYNCING.NET only sends a small amount of data - the 32-byte AES session key (32 bytes = 256 bits) and the peer unique ID - using RSA-1024.

Store and Forward

Store and Forward allows two computers that normally are not online at the same time to synchronize their Sync Folders or Outlook Groups. If the option "Store and Forward" is activated (default setting since version 2.0.3082), files and Outlook data will be temporarily cached on our servers when only one computer of the group is online. The data is compressed and encrypted in such a way that only the destination computers can decrypt it. As soon as the destination computer has downloaded a stored file, it is permanently deleted. Temporary cached files are also deleted if not downloaded within 14 days.

Application security

Your Sync Folders and Outlook Groups are closed invitation-only private networks; they differ from the other popular file-sharing applications used for public exchange. Nobody except the people you specifically invite to a Sync Folder or Outlook Group has access to your data.

In addition, each computer has a unique public and private 1024-bit RSA key, used for securely transmitting messages and user authentication. No transfer of data occurs unless a computer has been successfully authenticated.

Privacy Policy

We at SYNCING.NET respect and value the privacy of our users and do everything to ensure your personal privacy. We have developed a comprehensive Privacy Statement in order to protect our customers and to inform everyone how we handle personal information. Our current privacy policy can be found at <http://www.syncing.net/en/meta/privacy-policy.html>.