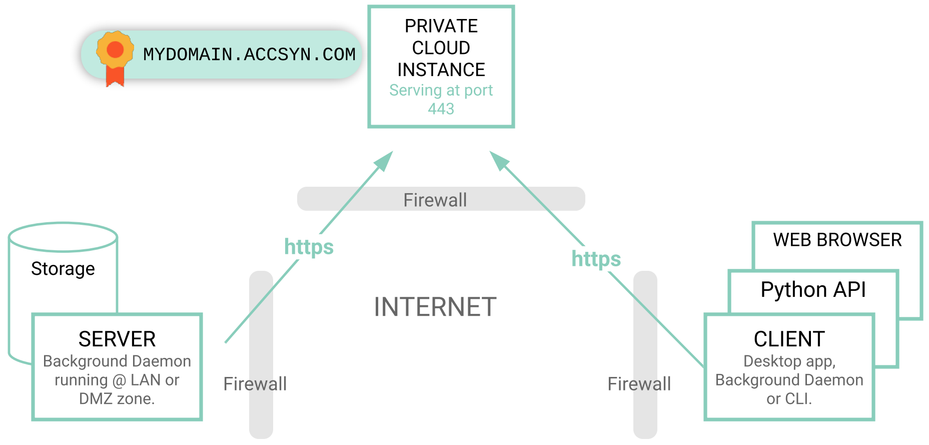
accsyn
- secure data delivery and workflow synchronisation

https://accsyn.com
support@accsyn.com

ACCSYN SECURITY WHITEPAPER

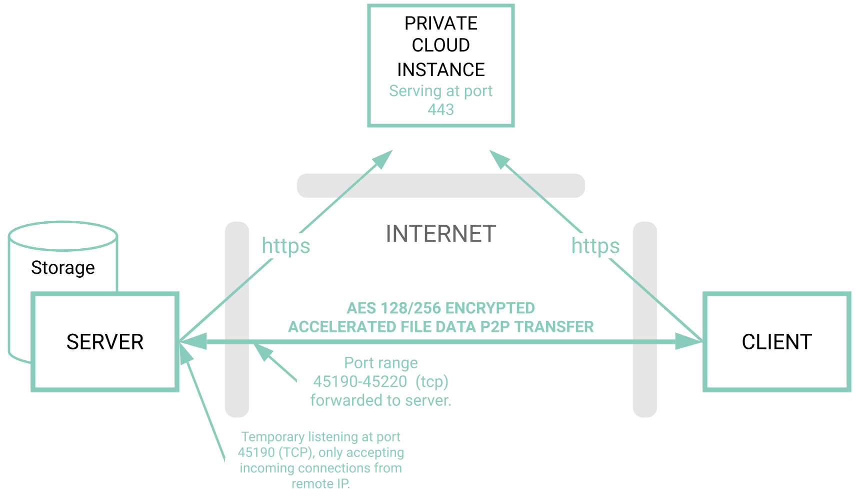
Accsyn is a MFT(Managed File Transfers) software for delivery of file and metadata in workflows, ensuring full encryption of data in transfer.



Schematics 1; Standby operation

In standby mode:

- No services listening on client or server.
- Secure HTTPS cloud communication of metadata, using standard SSL.
- Proper certificates issued by a standard trusted CA (Comodo).
- Dedicated private accsyn cloud instance running in its own VM, no shared database with other clients.


PRIVATE CLOUD INSTANCE
Serving at port 443
INTERNET
https
https
Storage
SERVER
CLIENT
AES 128/256 ENCRYPTED
ACCELERATED FILE DATA P2P TRANSFER
Port range 45190-45220 (tcp) forwarded to server.
Temporary listening at port 45190 (TCP), only accepting incoming connections from remote IP.

Schematics 2; File transfer mode.

In file transfer mode:

- Server process has a built in firewall that accepts connection from client WAN IP only.
- Encryption keys are distributed from the cloud, kept in client memory during session only.
- Data is encrypted using symmetric AES 128/256 over port 45190-45209 (tcp), low port (i.e. 443) options for firewall compability.

Summary:

Accsyn:

- Utilizes industry standard HTTPS (SSL/TLS) protocol.
- All file transfers are encrypted using AES 128/256.
- Package based delivery with E-mail notifications, password chosen by user and stored with SOC2 complient provider. MFA.
- In depth monitoring and audits of transfers.

In comparison to:

FTP:

- Passwords and data are sent unencrypted.

- Vulnerable to brute password attacks on listening service.

- Requires credentials to be generated and sent.

- No E-mail notifications.

SFTP/FTPS:

+ Secure encrypted file transfers.

- Vulnerable to brute password attacks on listening service.

- Requires credentials to be generated and sent.

- No E-mail notifications.

DROPBOX:

WeTransfer, Onedrive

+ Secure encrypted file transfers.

- Your files are stored in the cloud.

ASPERA:

Signiant, Expedat

+ Secure encrypted p2p file transfers based on SSL.

Continued on next page ⟶

ACCSYN SECURITY WHITEPAPER

Private cloud REST server instance

- Each Accsyn customer gets a dedicated Linux cloud virtual machine instance (abbreviated *cloud instance* from here on) having its own database instance, hosted by Glesys (Stockholm, Sweden).

- Running strict IP tables firewall only allowing TCP access on ports 443(https) and admin ssh port (see below).

- A Gunicorn WSGI server acts as web frontend, serving Accsyn python cloud web application over port 443(https).

- Presents a trusted Comodo PositiveSSL certificate.

- Only remote access to virtual machine, besides 443(https), is sshd running at random port allowing only a non-superuser login having a 8 digit randomized hexadecimal username, i.e. "A56FB210". Password authentication disabled.

- Accsyn admin staff is the only users having remote access to customer instance, using public key authentication, with private key stored on a encrypted partition.

- On request Accsyn admin staff can sign required customer NDAs.

Client/server java app

- Communicates with cloud instance using CRUD REST API over https port 443.

- Relies on JSSE standard SSL implementation (Java Secure Socket Extension).

- Installer deploys Java 8 Runtime, currently version u161.

Users and passwords

- No passwords or API credentials are stored at cloud server, Accsyn uses the SOC 2 certified service "Auth0" (auth0.com) as authorization backend.

- The ID token received from auth backend upon successful user+password(/API key) authentication is used by Accsyn client when further communicating REST with the server.

- Accsyn periodically checks the validity of token against Auth0 service, attempts to get a new ID token using the refresh token provided at authentication. If this operation fails, i.e. user is disabled, Accsyn clients will be disconnected accordingly.

- Notifications when a user logs on with a new device, notications when a new file transfer client is spawned.

Data integrity

- No file or metadata is stored in the cloud, files are sent point-to-point only.

- Upon point-to-point file transfer between clients, the cloud generates the AES 128/256 (configurable globally, per user or per work area) encryption key + init vector and distributes it to both parties.

- A separate process is spawned at client side, only accepting connections from remote client WAN IP.

- Data is encrypted using the key supplied by cloud instance, no key exchange between parties over non HTTPS protocols.

-Temporary encryption keys are stored in memory only, per session.

- Web browser download streams the file(s) over HTTPS cloud connection, no intermediate files saved in the cloud.