Why Secure File Transfer Matters in the Financial Field

The Financial Ecosystem and Community

Financial institutions and all the partners surrounding them, are undergoing massive digital transformation change. In the cyber realm alone, budgets are fast increasing to protect assets, personal information, and critical infrastructure for both software and hardware targets.

We are in the age of customer-centric strategies that produce a competitive edge. That means communication and trust, above all else, is highly valuable and must be protected. When customers feel their security is put before all else, brands earn their trust, which increases loyalty over time. Firms that invest in building trust and their clients' data security build brand awareness and protect their customers.

The financial field represents a multi-trillion-dollar market. So how do small financial players thrive and protect themselves in the market? A solution is to ensure trusted communications at the forefront of their operations. That's where Safety4Data comes in.

How to think about protecting Fintech data in-transit

Successful data sharing focuses on permission-based transfer. In order to create transparent and secure communication, each party must believe in the other – beyond audit of regulation or compliance. Fintech data transfer management often relies on automated governance, but how can just business rules ensure trust in delivery?

One method of ensuring data transfer trust within the financial industry is to improve controls which include securing passwords, data policy, and most importantly, transferring files via highly secure systems.

When people send files filled with data, they must trust a few things – for example:

- Can I trust the person I am transacting with?
- Are the files fully protected from departure to acceptance?
- How do I know someone received the files?

So often emails are sent with precious information for financial transactions, but small companies or individuals don't always have the resources to manage the data.

Secure File Transfer – The Best First Step

Put aside cyber security hype. The most pervasive threat comes from humans and data-in-transit. When employees and partners share information and data, they create a daily interchange for thriving business. Today, this must be secure to ensure trust.

The best first step is to protect the files so securely that it takes away the most vulnerable weak link of data-in-transit. If done easily and automatically, then the path to greater security is assured. Secure file transfer, when done right, dramatically lowers the risk of data breech.

Enter Safety4Data as a solution.

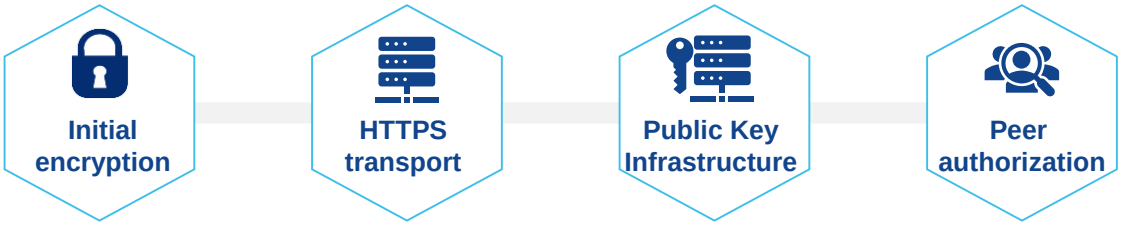
Safety4Data Secure File Transfer

Protecting the Peer to Peer Relationship

The value of a trusted relationship – whether in a private conversation, a critical moment of need, or protecting assets cannot be underestimated. We develop relationships and communicate in a unique way; secure data is very much like that too. When we transfer data, it must be as safe as precious cargo. If we establish a peer to peer relationship, with a toolset that guarantees secure file transfer, we can substantially protect files and data. Imagine a cyber approach where you can increase protection in five minutes - one where you establish a trusted peer relationship and pull files from a trusted place for both parties. Like an armored truck.

Safety4Data is a data encryption and transfer application which relies upon a secured, peer-to-peer virtual network that allows users to confidently exchange data with anyone in their network.

Layers of Security



Every file is secure from the moment of release to the moment of acceptance.

A Bit More about Security

Safety4Data works by assigning a pair of PKI keys – one public and one private. Only the user who owns the keys has the private key, but the user's public key can be given to anyone. When using PKI, the user secures not only the server authentication, but also the Safety4Data user authentication. In addition, users can encrypt/decrypt files using PKI.

During transfer, data is sent via Safety4Data's highly secure, encrypted HTTPS tunnel. The server is then authenticated by a server certificate, verifying the user is communicating with the legitimate Safety4Data application, not an unreliable server.

Files are encrypted and stored on Safety4Data servers until the recipient downloads them, at which time the files on the server is permanently deleted. Encryption certificates are acquired via "Certificate Authorities" and managed to optimize security. Each of these steps occur automatically within the Safety4Data platform.

Data security is created by using the Azure cloud server environment – technology which delivers a superior level of confidentiality, integrity and stored data availability. This is completely managed by the Safety4Data service within the client peer-to-peer realm.

Safety4Data Secure File Transfer

The Safety4 Data Elements

The Service

- Web administration local service is automatically installed in the background for PKI distribution and the files send/download process and the encryption/decryption process.
- Local service setup is done through the web administration and options are available in the notification tray.
- PKI trust is achieved with providers' certificates or optionally with the user's own certificates.

The Administration

- The local administrator creates a virtual user network with either simple (all users can communicate only with local admin) or full (every user can communicate with all users).
- You can also create communication groups.

File size

- As small as 200 MB
- File size can increase to over 1 GB or more if required

User Flexibility

- Users work in their own OS with upload/download folders for drag-and-drop ease
- Optional file sending with a context menu (right-click mouse operation) is available
- Optional direct files upload/download to/from web administration (for one-time communication with client) to provide more comfort for users.

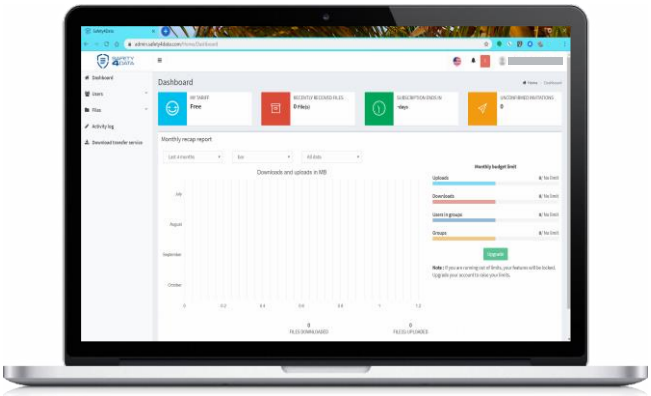
Logging, Audit, Notification

- Every file transfer is registered into the communication log to provide overview for users. An error log is provided if there are errors during the file encryption of transfer.
- A list of downloaded files (simple Download manager) is included in the communications log and includes the name of file, information about sender and option to open a folder where the file is placed.
- Notification of email and system tray about upload/download file is fully configurable..

The Safety4Data Hosted Service

To use Safety4Data, you subscribe on a ser basis and install a light footprint client to ensure secure file transfer. Safety4Data is a set of software and tools on a hosted application, built on a client-server architecture to enable the creation of virtual secured networks.

Administration is an easy-to-use dashboard that manages files, users and subscriber settings for high file security.



Safety4Data Secure File Transfer

Services and Support

Safety4SERVICES represents the program, where file security experts can be engaged for projects and enterprise installations if needed. In addition, the Safety4Data team can create connections to existing data sources, API's and cloud-based systems. The hosted Safety4Data solution is fully supported with software and client upgrades.

We offer personal Cyber Security Consulting services for small to mid-size businesses. We work directly with your business to fill the gaps and find affordable solutions to keeping your information secure and money saved. We understand that cyber security may not be a top priority, however, it is of the utmost importance to prepare, protect and be proactive, as opposed to assume you are safe, then be reactive to a breach that could be easily prevented.

Safety4CARE is Safety4Data's software upgrade program that provides notification of software features and upgrades for the hosted solution.

Get Safety4Data

Start with the trial download HERE

Contact us at sales@it-cns.com