Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2020, 7(10):221-224**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

SFTP Alternatives for Secure File Transfers between Host Server and Clients

Prashanth Kodurupati

Information Technology, Managed File Transfer Engineer, PragmaEdge LLC, Alpharetta, United States of America
Email: prashanth.bachi21@gmail.com

Abstract Secure File Transfer Protocol (SFTP) is a widely used protocol to ensure safe file transfers, but in instances when it's not set up/established on the client end, the host server has to establish an alternative method for secure file transfers. Some commonly used alternatives include setting up an HTTP mailbox, creating an IBM Sterling Mailbox (if the host uses this B2B integrator), using a cloud-storage intermediary, or MFT As A Service (MFTaaS). All these solutions require minimal setup and effort from the client end.

Keywords File transfer, secure file transfer, SFTP, Host Server.

1. Introduction

Data is the lifeblood of most businesses nowadays, and data transfers with a business and between a business (host server) and its clients are a critical operational element. Security of the data (especially in transit) is one of the most significant concerns businesses have nowadays, and there are several ways to achieve that. Some businesses rely upon protocols like Secure File Transfer Protocols (SFTP), while others may employ alternative data security methods. The discrepancy of data security measures and protocols among host servers and clients is a common occurrence, and in order to avoid any operational friction, IT professionals, particularly Managed File Transfer (MFT) engineers, have to rely upon a range of secure file transfer methods to ensure that clients have access to the files they need, even if they *don't* have SFTP setup.

2. Literature Review

The literature on secure file transfer protocols and data security in transit is exhaustive, and it covers a wide range of data/information transfers using a wide range of channels. Secure File Transfer Protocol (SFTP) has been around since 2005 and relies upon an encrypted connection (SSH-Tunnel) for a secure file transfer [1]. While it's available and accessible to a wide range of businesses and one of the most commonly used "routes" for safe file transfers, many businesses opt for Managed File Transfer (MFT) systems. These systems may have their own layer of security and safety and make data transfers relatively easier and automated [2]. In some cases, businesses may rely upon secure HTTP mailboxes for file transfers. This includes publicly accessible mailboxes and mailbox features of specific business integration solutions like IBM Sterling that are purpose-built for safe file transfers [3].

3. Problem Statement: No SFTP Setup on Client Side

The overarching problem many businesses face is that their clients may not follow the data security protocol they are following. For example, a credit bureau may have an SFTP setup on the host side, but the client side doesn't have the requisite configurations and tools on their end, making an SFTP connection impossible between the two. There are several reasons this protocol is widely used in financial institutions where data security is a

significant concern beyond the data security it offers, like resuming interrupted transfers and safe remote transfers [4]. Despite these benefits and strengths, some clients may not have SFTP setup on their end for a number of reasons. This includes (but is not limited to):

- Lack of requisite technical expertise. This is more common with new businesses than established ones that may still be in the process of building or improving their IT infrastructure.
- Legacy systems may prevent a business from setting up an SFTP server or adding SFTP functionalities to their existing servers.
- Compliance and regulatory oversight or conflict. Many businesses (like financial institutions) have to meet rigorous requirements when it comes to safeguarding the data they have (at rest), like consumer financial information and funds data, and securing the data of their customers in transit, as it flows towards and away from their servers. However, the same restrictions may not apply to data they exchange with *their* vendors in their capacity as a client in a B2B interaction. So, an SFTP setup may not have been extended to that front. On the other end of the spectrum, regulatory changes or restrictions may force them to opt for data security measures other than SFTP.
- SFTP may not be part of the data ecosystem in which the businesses operate.

Regardless of *why* a business doesn't have an SFTP setup present, it can lead to two problems for the host server, which needs to ensure a secure file transfer between itself and the businesses (clients). The problem can take two shapes. The client may not have any data security measures in place or none that the host server is capable of dealing with. Or, they have a different data security measure in place instead of SFTP.

Both of these problems can shift the onus of data security towards the host server, as they may have to ensure that the files that need to be transferred to the client reach them in a safe and secure manner and are only accessible to the intended client and cannot be siphoned away during transit.

4. Proposed and Implemented Solutions

The easiest solution would be for the client side to set up SFTP on their end, which may ensure that each instance of data transfer between them and the host servers is safe, secure, and easy. But when it's not an option for any of the reasons mentioned above, the following solutions can be implemented.

4.1 Creating an HTTP Mailbox with Secure Login Credentials

One secure file transfer solution a business can opt for when serving as a host server for clients that do not have an SFTP setup is to set up an HTTP mailbox. They can set it up on their own servers, a cloud service they are using, or a publicly available service, though it's not often recommended because of its security vulnerabilities. The idea is to create an online space that the clients will be able to access if they are just offered the credentials to log in to the mailbox, which requires no setup from the client side. No one else would be able to access the files available on this HTTP mailbox unless they come into possession of login credentials. Therefore, the communication of these credentials is just as critical a security consideration as setting up the mailbox.

Access is another factor to consider in this method of file transfer, so credentials should be ensured for the individuals with the right to access the files. Another important element when it comes to setting up these HTTP mailboxes is their "temporary" nature. Because the longer they are online, the higher the probability of login credentials falling into the wrong hands (accidentally or intentionally). This is one of the reasons why when such mailboxes are established for file transfers among financial institutions, they typically remain live for 24 hours. That's the window through which clients have to access the files.

If it's a frequent practice, a business may create templates or default requests/jobs for the creation of such mailboxes.

4.2 Creating a Mailbox in IBM Sterling

When both a business and its clients have IBM Sterling set up, there are several ways to transfer data securely, including Connect:Direct and IBM Sterling's Global Mailboxes [5]. However, in some cases, the client may be able to access files made available through IBM Sterling's mailbox even when they don't have IBM Sterling, though it may need some setup on their end, like installing client-end software. In limited cases, it may be made available to them with no setup required.

The IBM Sterling Mailboxes are radically different from HTTP mailboxes. Its protection may rely on protocols and safety measures different from those of SFTP. The transfer limits (file sizes) and access control may also differ, though it relies heavily upon how the mailboxes are set up.

4.3 Using a Cloud-Based Intermediary

If the client doesn't have an SFTP setup, the host can also make a file available to them via a cloud-based intermediary. The host business can upload a file using a cloud service and share the link with the client. This default mechanism may not be safe enough, but it can be made safer through access credentials and expiration time. The credentials can be shared with the clients, so even if someone else finds the link, they will be unable to download the file without the requisite credentials. An expiration time after which the file self-deletes adds another layer of safety, similar to an HTTP mailbox.

4.4 Using MFT As a Service (MFTaaS)

Another solution that may help a business safely transfer files to a client that may not have an SFTP setup is leveraging an MFT as a Service or MFTaaS. It's slightly more accessible than using a dedicated on-site MFT solution that might be compatible with the client's MFT or how their transfer requests are configured or processed. MFTaaS are usually cloud-based and may offer a wide range of safe file transfer capabilities, along with how they can be configured for the client. This may include generating credentials for clients, choosing a specific data security protocol, or setting up a time limit for file download access. An MFTaaS use on the host side may require minimal effort and technical expertise on the client side. A simple web interface may allow clients to access the files made available by the host through an MFTaaS.

It's important to understand the solutions presented above lean heavily towards minimal client-side setup and efforts. If we get around this restriction, the range of solutions might increase. Even if an SFTP setup on both ends is not a viable option, an MFT solution used by both client and host or two MFT solutions compatible with each other used by client and host can make the transfers secure, easy, and seamless.

5. Use Cases

Problem	Solutions	Use Case (Financial Sector)	Potential Vulnerabilities
No SFTP on Client Side (or incompatible protocol)	Client implements SFTP (ideal but may not be feasible)	Credit bureau transfers large creditworthiness reports to multiple banks (some with SFTP, some with FTPS).	The client lacks technical expertise or resources for SFTP setup.
	Temporary HTTP Mailbox with Secure Login Credentials	The insurance company needs to send sensitive medical data to a new partner who lacks SFTP or a compatible protocol.	Login credentials intercepted during transmission or storage, data breach if mailbox compromised.
	Mailbox in IBM Sterling (if both have IBM Sterling)	Fintech startup collaborates with a custodian bank (uses FTPS) but doesn't have its own IBM Sterling server.	Client-side software installation is required (may not be feasible), and there are limited data transfer capabilities compared to MFT solutions.
Mismatched Protocols (e.g., Host: SFTP, Client: FTPS)	Cloud-Based Intermediary with Protocol Conversion	Asset manager shares complex investment data with custodians who use a mix of SFTP, FTPS, and secure cloud storage solutions.	Data security during the conversion process (if not transparent) and potential compatibility issues during conversion.
	MFT as a Service (MFTaaS) with Protocol Interoperability	Bank retrieves account data from multiple credit bureaus (varying protocols; some legacy systems may not support modern protocols).	MFTaaS provider security breach, ongoing costs associated with MFTaaS subscription.

	Negotiate a Common Protocol with Trading Partners	Brokerage firms exchange trade confirmations with several hedge funds. Industry-standard protocol (e.g., FIX) is not universally adopted.	A time-consuming negotiation process may require technical upgrades for some partners to comply with the chosen protocol.
Legacy Systems Inhibiting Secure Protocols	MFT as a Service (MFTaaS) with Legacy System Integration	A large insurance company with a mainframe system needs to exchange policyholder data securely with a modern InsurTech startup.	Integration complexity between MFTaaS and legacy systems, potential compatibility issues.
Regulatory Requirements for Data Transfer Security	MFTaaS with Compliance Features and Audit Trails	Wealth management firm transfers customer financial information across borders, complying with international data security regulations.	MFTaaS provider compliance limitations, ensuring MFTaaS features align with specific regulations.

6. Conclusion

SFTP is one of the most widely used protocols for secure file transfers, but it's not universal, and within specific industries like financials and credit, the usage frequency may differ among different stakeholders. This necessitates that MFT engineers and IT professionals should have access to alternative solutions to ensure safe file transfers even when their clients may not have SFTP setup. An HTTP mailbox is a commonly used alternative, but there are others that are as well. Choosing the right solution requires taking into account factors like the amount of data that needs to be transferred, regulatory concerns, and the technical capabilities of clients.

References

[1]. N. N. Mohamed, Y. M. Yussoff, N. H. Kamarudin, and H. Hashim, "New Packet Header Support and Key Exchange Mechanism for Secure Trivial File Transfer Protocol," International Journal Of Electrical And Electronic Systems Research, vol. 11, 2017.

[2]. W. Sardjono and T. Pujadi, "Performance evaluation of systems Managed File Transfer in banking industry using IT Balanced Scorecard," in 2016 International Conference on Information Management and Technology (ICIMTech), 2016.

[3]. IBM, "Understanding IBM Sterling File Gateway," IBM Software Group, 2015.

[4]. M. Kohli and E. Suarez, "Centralized Solution to Securely Transfer Payment Information Electronically to Banks from Multiple Enterprise Resource Planning (ERP) Systems," in 2016 International Conference on Information Technology (ICIT), 2016.

[5]. J. Foley, K. Kido, S. Litzkow, K. Scott and D. Tucker, IBM Sterling Managed File Transfer Integration with WebSphere Connectivity for a Multi-Enterprise Solution, IBM Redbooks, 2011.