Journal of Technological Innovations

Est. 2020

# External File Transfers (Incoming) And Importance of Routing Channels

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

**Abstract:**

A server may allow external stakeholders to transfer files following a specific set of requirements. These requirements can be made part of the routing channel a host server opens to its clients for file transfers. It may define several critical components, including the proper destination path for the file, encryption type, transfer protocol, and naming convention. MFT systems and business connectivity solutions like IBM Sterling typically have templates for routing channels to make the creation of these channels easier and seamless.

**Keywords:** Routing channel

## 1. Introduction

Each business has its own set of data streams - both internal and external. Massive data inflow and outflow is the norm for most businesses and critical to a wide range of operational elements. With so much data moving in and out of business, the safety of data at rest, particularly in transit, is a priority for businesses. It's paramount for businesses that have access to sensitive information like consumer financials, credit reports, etc. Those businesses, or, more accurately, professionals overlooking the Managed File Transfers (MFT) within those businesses, strive to ensure that all incoming or outgoing pathways are secure, and routing channels are an important part of the latter.

## 2. Literature Review

The term routing channels applies to a wide range of transfer situations, including ones where transferred media isn't data. However, even if we limit ourselves to file transfers/data transfers, there is some literature that discusses routing channels, often in the context of data fidelity and FPGA. However, we can find ample literature on individual characteristics of routing channels, like safe file transfers, permissions, and safety features like encryption, all of which are elements of defining and creating a routing channel.

When safe file transfers are required, most businesses tend to rely upon standard protocols like Secure File Transfer Protocols (SFTP) that are considered secure enough for sensitive data transfers (like medical reports) [1]. But if a business and its clients/vendors that may wish to send data through and both endpoints use business connectivity solutions like IBM Sterling, they may revert to the solution's/system's own file transfer protocols that may offer more flexibility and security when it comes to managed file transfers [2]. Encryption (and decryption) is another important aspect of safe file transfer and ensures that even if data can be siphoned off in transit, it remains illegible to anyone but the intended recipient and sender [3]. Security has been a concern in managed file transfers since the early days, but it's not the only element to take into account when data transfers, whether or not they are managed through routing channels, are evaluated against safety/security parameters [4].

## 3. Problem Statement: Challenges Faced By External File Transfers

While the security of the data being transferred out or accepted by a business is an important consideration for almost all businesses, some of them have to adopt more stringent measures because of industry practices and regulatory requirements. This includes financial institutions and establishments like credit bureaus, which may receive sensitive data like customers' social security numbers, financial information, etc., from their clients. They also receive critical information about millions of individuals from banks (their loan and repayment information), utility companies, lenders, etc.

External stakeholders and businesses that have to receive this data have to ensure several things to complete a successful transfer, including where the file is supposed to be copied, how it’s encrypted, the right transfer protocol, data validation, and permissions. Challenges can stem from each of these elements, and a single discrepancy may be enough to prevent a successful file transfer. The three most significant problem areas are file transfer destination, file transfer protocol, and encryption.

### Unknown or Improper File Transfer Destination

Any external entity or stakeholder who has to transfer a file to a host server should be aware of the place allocated for them. It may be allocated based on the size and type of the data being transferred, individual stakeholder, their security needs, access levels, or a number of other reasons. The destination may have different titles, depending on the protocol and the exact file transfer instance, including a mailbox or a

virtual directory.

If the sender of the file, i.e., the external stakeholder, is not aware of the right transfer destination, it can lead to a few different problems. The simplest of these is that the file may simply not be transferred. However, in some cases, the file may be transferred to the wrong destination, which may cause problems for both the host and the external vector.

### File Transfer Protocol Mismatch

An external file transfer can be rejected or delayed if there is a file transfer protocol mismatch [5]. If the sender is using a different file transfer protocol than what the sender is equipped to receive or compatible with, the transfer will most likely be denied. Even if the recipient is typically equipped to receive files following different transfer protocols, the exact transfer window (pathway) opened to an external entity may have stricter protocol requirements that the sender has to match. Otherwise, they may not be able to complete the transfer and may lose the transfer window if it was opened for a specific amount of time. Protocol conversion facilities might be available on either end, but again, this is subject to the nature of the transfer itself. If it's set following strict parameters for the external sender, the conversions that may usually facilitate an easier transfer may not be available.

### Encryption Mismatch

The encryption of a file being sent by an external vendor/third party and the recipient server should match. Otherwise, the transfer can either be rejected or, even if it succeeds, the file may not be processed.

### File Structure

The recipient server or MFT system may have its own requirements for file structures, which cover several things, including its extension, file type, folder hierarchy, and naming convention, each of which should be followed to ensure seamless file transfer. If the sender doesn’t follow the naming convention of the recipient, the file name uses special characters that are not recognized by the host server and MFT systems, or the name is too long for the MFT convention, the file transfer may be halted. If the file is transferred, it may be renamed to match the convention (forcefully), which may create confusion on either end of the transfer.

Another problem avenue that may only apply to a specific set of transfers is:

Authorization: In some cases, a routing channel may require special authorization information or permissions to initiate the file transfer, and if it's not present, the transfer may fail.

## 4. Proposed and Implemented Solutions: Establishing Routing Channels

An overarching solution to all these problems is establishing a routing channel to facilitate a file transfer between an external entity (customer, client, etc.) and the host server of a business. A routing channel is essentially an agreement facilitated by an MFT system that allows one entity (sender) to transfer a file to another entity (recipient) based on the terms, naming conventions, and requirements of the recipient, including where the file is supposed to land in their server. It's a general concept used by a variety of MFTs, particularly IBM Sterling, where it facilitates a transfer between a producer and consumer, following their "mailbox" conventions.

It's important to understand that the problems stated above are agnostic to the MFT systems and server conventions and may apply to a wide range of file transfers between external entities and a host server. Each of the problem avenues can be tackled by following the same set of good transfer practices as well, though some business connection systems (with their MFT functionalities) may have their own approach to either preemptively avoiding these solutions or tackling them as needed. In IBM Sterling, a comprehensive solution is to follow routing channel templates [6]. The template may cover all the problem scenarios mentioned above, ensuring a smooth transfer.

### Mailbox Path/Destination Path

Following the predefined templates that may be modified for specific senders, the recipients can share the right destination path or virtual directory path with the sender so they have the right information at hand before initiating the transfer. In IBM Sterling, this is the mailbox element of the MFT system, which focuses on connecting "producers" to "consumers." The mailboxes are generated once new producers are added to the system, but they can also be created if a specific file transfer is needed, which is different from the ones created by default. The same goes for consumers. So, the IBM routing channel template usually includes the right mailbox path that the sender can follow once the template is shared with them.

### Protocol Matching

In some cases, the routing channels also define which file transfer protocols the sender should follow to ensure that the file reaches the desired destination in the host servers. This is moot in cases where IBM Sterling is facilitating the transfer, and their templates are being used since they automatically define the protocols that have to be followed for the transfer. But in cases when it's not mediating a connection and an MFT instance, the protocol may have to not just be defined in the routing channel but also shared with the sender so they follow the right protocol, avoiding a mismatch and potentially failed transfer.

### Encryption Matching

Both the sender (external entity) and host server (recipient) should "agree" on the encryption protocol for a successful file transfer to occur through a routing channel. If the routing channel doesn't account for it, an encryption conversion facility at the recipient end may not be enough to facilitate a transfer between mismatched encryption. So, either the routing channel should be created as an encryption agnostic, and the file transferred to match their native encryption or the right encryption should be communicated to the sender. When an MFT like IBM Sterling is facilitating the transfer, their routing channel template can automatically enforce this convention.

### Naming Conventions and Conversions

The file names, hierarchies, patterns, syntaxes, and, in some cases, even file types have to follow the prerequisites of the routing channels. A routing channel may define some or all of these avenues and have its own naming conventions that the sender has to follow to ensure the file is transferred and accepted at the host end without an incident. However, when the transfer takes place through an MFT system or MFT functionalities of a business connectivity system like IBM Sterling, there might be provisions in place for converting the file name to match the host's naming convention. However, the conversion facilities might have their own limitations, so the best course of action for the sender is to follow the naming conventions enforced by the routing channel or recipient.

## 5. Use Cases

| **Problem** | **Solution (Routing Channel & Templates)** | **Use Case (Credit Bureau)** |
|---|---|---|
| **Unknown or Improper File Transfer** | Mailbox Path: Routing channel templates define the specific mailbox | A bank needs to send a daily report on loan repayments to a specific credit bureau. The routing channel |

| | | |
|---|---|---|
| **Destination** | (destination path) on the credit bureau's server for each sender (bank, utility company, etc.). | template provides the exact mailbox path for the bank to use, ensuring the report lands in the correct location for processing. |
| **File Transfer Protocol Mismatch** | Protocol Definition: Routing channels specify the required file transfer protocol (FTP, SFTP, etc.). Templates pre-configure this in IBM Sterling. | A lender needs to submit credit application data to the credit bureau. The routing channel template ensures they use the SFTP protocol required by the credit bureau, preventing transfer failure due to mismatch. |
| **Encryption Mismatch** | Encryption Agreement: Routing channels can be configured for specific encryption protocols or remain "encryption agnostic" for flexibility. Templates enforce this in IBM Sterling. | A credit card company wants to send sensitive customer information to the credit bureau. The routing channel ensures both parties use the same strong encryption protocol (e.g., AES-256) for secure data transfer. |
| **File Structure Mismatch** | Naming Conventions: Templates define the naming conventions (characters, length) for files accepted by the credit bureau. | A utility company sends monthly customer usage data. The routing channel template dictates the specific naming format for these files (e.g., "Utility_Company_YYYYMMDD.txt") to avoid file renaming or |

| | | |
|---|---|---|
| | | transfer errors. |
| **Authorization Issues (Limited Case)** | Authorization Information: In specific scenarios, routing channels can require additional authorization details for secure transfer initiation. | A new data aggregator wants to start sending consumer credit reports to the credit bureau. The routing channel may require specific authorization credentials for this new sender to be included in the transfer process. |

## 6. Conclusion

Income external file transfers have to be regulated and formatted as per the host server requirements, and routing channels are a key element in this regulation. Routing channel templates offered by business connectivity solutions like IBM Sterling make the process significantly more seamless, but it's imperative that MFT engineers take into account a broader range of factors before developing a routing channel for their clients. The cybersecurity, bandwidth requirement, space requirement, and several other “impacts” a file can have on the host server once a successful transfer is initiated can have significant implications.

## References

1. M. Daniel L. Helsten, D. P. Arbi Ben Abdallah, M. Michael S. Avidan, M. Troy S. Wildes, M. M. Anke Win

ter, B. Sherry McKinnon, R. M. Mara Bollini, B. Penny Candelario and M. C. Beth A. Burnside, "Methodologic Consideration s for Collecting Patient reported Outcomes from Unselected

Surgical Patients," Anesthesiology, vol. 125, no. 3, 2016.

2. B. Zohuri and M. Moghaddam, " Cloud Computing Dri

ven Business Resilience System," in Business Resilience System (BRS): Driven Through Boolean, Fuzzy Logics and Cloud Computation, 2017.

3. Y.-F. Tseng, C.-I. Fan and Y.-F. Cho, "An authenticated re-encryption scheme for secure file transfer in named data networks," Communication Systems, vol. 31, no. 11, 2018.

4. D. Dunford, "Managed file transfer: the next stage for data in motion?," Network Security, vol. 13, no. 9, 2013.

5. R. Goss and R. Botha, "Traffic flow management in next generation service provider networks — Are we there yet?," in 2011 Information Security for South Africa, 2011.

6. I. S. Group, "Understanding IBM Sterling File Gateway," IBM, 2015.