Samskip EDI

Connectivity Guide

v 1.0 | 9 January 2023

About This Document

This document provides an overview of connectivity methods between SAMSKIP and its trading partners. Subsequent sections provide specific technical implementation details for each method introduced.

Audience

This document is intended for personnel engaged in establishing an electronic connection with SAMSKIP for the purpose of exchanging business transactions over the Internet.

Document History

Release Date	Document Information
January 9, 2023	Initial document.

Index

1 Introduction

1.1 Samskip Connectivity Policy

SAMSKIP recommends secure connectivity. We do support traditional, less secure file transfer methods; however, these are not encouraged and should, whenever the partner is able to migrate, be switched to a secure connectivity method. We provide a brief overview for connectivity methods. Subsequent sections provide specific technical implementation details for each method introduced. Please note, at the time of writing, we're using Seeburger as our EDI system, capable of providing an even wider range of methods.

1.2 Connectivity Options

SAMSKIP supports several options for connectivity; AS2 (EDIINT), sFTP, FTP, HTTPS, HTTP and SMTP (e-Mail), explained below.

1.2.1 EDIINT (AS2, HTTPs)

AS2 is a "sender transmits" convention whereby the subsystem transmits files to the partner when a file is ready, and vice versa. AS2/EDIINT is the preferred secure and reliable connectivity option. SAMSKIP currently supports EDIINT AS2 which uses a HTTP(s)/WEB transport. The protocol and apparatus take care of all of the following supported optional services:

- Compression
- Encryption
- Failure-recovery/retransmission
- Message disposition notification (MDN)
- Audit trail

1.2.2 SAMSKIP-Mailbox

The Mailbox solution provides EDI trading partners with individual mailboxes. This guide describes the folders/directories per message type and direction and file naming conventions to use, along with a self-service archive repository. Partners simply connect periodically to access their mailbox to pick up and drop off files. This connectivity option is primarily implemented via FTP (and soon Secure FTP or sFTP).

2 Connectivity Methods

2.1 Electronic Data Interchange Internet Integration

Electronic Data Interchange Internet Integration (EDIINT or EDI-INT) protocols provide for secure exchange of business transactions over the Internet. EDIINT represents an upgraded connectivity solution when compared with traditional FTP or even secure FTP. The EDIINT standards contain provisions for increased reliability, better audit trail and error reduction through its recommendations for:

- Reliable delivery – to detect and recover delayed or lost transmission by a specified, configurable, period of time, and to provide remediation, such as retransmission or alert reporting for affected transmission.
- Acknowledgement – message disposition notification requests and responses are processed in accordance with the trading partner profiles.
- Duplicate detection of binary equivalent messages.
- Security – PKI digital signature technology, secure sockets layer (SSL) for communication, and robust encryption, authentication, and authorization.

SAMSKIP's EDIINT Service offers the following EDIINT Applicability Statements or business protocols:

- EDIINT AS2 - communicates data using Hyper Text Transfer Protocol (HTTP) or Hyper Text Transfer Protocol over SSL (HTTPS).

2.2 Secure FTP (sFTP)

SAMSKIP can connect to secure data transfer using Secure FTP (sFTP) based on the SSH2 protocol. The SSH2 protocol provides server authentication, encryption, data integrity verification, and client authentication.

- Server Authentication: is performed using the DSA public key algorithm.
- Encryption and Data Integrity Verification: is supported via algorithms incorporated in every SSH2 product and can be implemented in a modular fashion.
- Client Authentication: can be performed using a password, a public key algorithm such as DSA or RSA, as well as a variety of other methods.

A sFTP session, like the traditional FTP session, involves a dedicated mailbox that is accessed by connecting to and signing on to a sFTP server. It requires the use of an sFTP client that is compatible with the SSH2 protocol. Samskip can connect to but, at the moment of writing, does not, yet, provide a sFTP server.

The sFTP client will facilitate the verification of user password and public key authentication to transfer the data in an encrypted format over the Internet and allow successful decryption of the data once the data transfer completes. Once connected and authenticated using sFTP, partners will have the same functionality offered with a traditional FTP session. SAMSKIP can, still, provide a traditional FTP service.

3 Connectivity Configuration Details

3.1 EDIINT Partner Setup

SAMSKIP's utilizes a product called Seeburger. Seeburger allows SAMSKIP to deploy a test AS2 server in order to provide for pre-production connectivity and transaction testing between SAMSKIP and a new trading partner.

3.1.1 Using AS2 Services

The details for using AS2 services are provided below:

Partner AS2 information for AS2 PRODUCTION	
AS2 Name	SamskipMCL
AS2 URL	https://edi.samskip.eu/as2
AS2 Port	9443
Source AS2 IP Address (IP from which Samskip originates)	145.131.219.66
Destination AS2 IP Address (IP to which partner sends)	145.131.219.81
AS2 Certificate	Will be provided

Partner AS2 information for AS2 TEST	
AS2 Name	SamskipTest
AS2 URL	http://edi.samskip.eu/as2test
AS2 Port	9999
Source AS2 IP Address (IP from which Samskip originates)	145.131.219.66
Destination AS2 IP Address (IP to which partner sends)	145.131.219.81
AS2 Certificate	Will be provided

Please note the AS2 Routing ID is a unique identifier used to facilitate AS2 routing, and should not be confused with the EDI Routing reference that is applicable for EDI ANSI and EDI EDIFACT document flows.

3.1.2 Firewall Configuration

In order to connect to the SAMSKIP PRODUCTION AS2 trading engine the following IPs and port need to be implemented:

- IP Addresses: 145.131.219.81 (from the Trading Partner to SAMSKIP)
- IP Addresses: 145.131.219.66 (from SAMSKIP to the Trading Partner)

- Port: 9443

In order to connect to the SAMSKIP TEST AS2 trading engine the following IPs and port need to be implemented:

- IP Addresses: 145.131.219.81 (from the Trading Partner to SAMSKIP)
- IP Addresses: 145.131.219.66 (from SAMSKIP to the Trading Partner)
- Port: 9999

3.1.3 Defining Trading Partner Preferences

SAMSKIP will provide a trading partner form, Samskip Initiation Document, as Appendix A to this connectivity guide to gather EDIINT preferences prior to setting up the new trading account in Seeburger.

3.1.4 Encryption Requirements

If encryption and signed document exchange is required, SAMSKIP will send a 256 bit VeriSign Certificate with Extended Validation (EV) containing SAMSKIP's public key. The public key is a single key pair with asymmetric key length of 2048. The certificate will be exported in the PKCS #7 format (.p7c / .p7b) and "DER encoded binary X.509 (.cer) " format. If encryption and signed document exchange is required, SAMSKIP will need to receive your certificate to bring your new trading account online. SAMSKIP strongly recommends the use of recognized Certificate Authority (CA) certificates. The certificates should be provided to SAMSKIP in DER encoded binary X.509 format or third party public keys in PKCS #7 (.p7c) format.

3.2 Secure FTP (sFTP) Partner Setup

SAMSKIP can connect to your company's sFTP site. Therefore we need a userid and a password to access an account on the sFTP server.

3.2.1 Firewall Configuration

For SAMSKIP to connect to a sFTP service the following IP need to be whitelisted:

- ip 145.131.219.66

3.2.2 sFTP Authentication Details

A sFTP Server will require Password Authentication AND/OR Public Key Authentication. Please be sure to define the authentication level with SAMSKIP Integration Team. SAMSKIP can connect using encryption algorithms negotiated based on what algorithms are supported by both the client server and SAMSKIP's client. SAMSKIP can at least support those encryption algorithms that are listed below.

Encryption Algorithm	Description
Aes128	Support encryption using AES (Rijndael) with a 128-bit key.
aes256	Support encryption using AES (Rijndael) with a 256-bit key.
blowfish	Support encryption using Blowfish with a 128-bit key.

3des	Support encryption using three-key triple DES with a 168-bit key (192 formally, but 24 are unused). Support for this method is REQUIRED by the SSH2 specification.
arcfour	Support encryption using the Arcfour stream cipher with a 128-bit key. Arcfour is believed to be compatible with RC4, which is a trademark of RSA Security Inc.
cast128	Support encryption using the CAST-128 cipher with a 128-bit key.

MAC

All data transfers must be configured for session information encryption (MAC). A MAC algorithm is what protects session data from tampering by a third-party. During an SSH2 session, a MAC algorithm is negotiated based on what algorithms are supported by both the client and the server. SAMSKIP will support only those MAC algorithms listed below.

MAC Algorithm	Description
hmac-sha1	Support data integrity protection using HMAC-SHA1. Support for this method is REQUIRED by the SSH2 specification.
hmac-md5	Support data integrity protection using HMAC-MD5.

3.3 FTP Partner Setup

SAMSKIP can create a directory for your company on SAMSKIP’s test and production FTP site. (In the near future SAMSKIP will introduce, more secure, sFTP hosting also).

For FTP you will be provided with the exact name of your company’s directory when the account is set up. For security purposes this directory name will be created based on an SAMSKIP naming standard and will not always reflect your company’s name. This directory will be restricted to only your company’s use and will not be visible by other SAMSKIP FTP users.

3.3.1 FTP Login Addresses

SAMSKIP will provide either two distinct FTP addresses for login or create two distinct directories for Test and Production. The ftp credentials will be provided by SAMSKIP’s integration team and will enable a login to: **edi.samskip.com**

3.3.2 FTP Scripting Requirements

Your client FTP scripts will need to do the following:

- initiate sessions with SAMKIP’s FTP server
- put files in the appropriate inbound directories
- get files from the appropriate outbound directories
- delete files from the appropriate outbound directories after successful gets
- manage inadvertent loss of connectivity due to typical public internet latency and other unplanned internet disruptions.

For inbound file transfers, inadvertent loss of connectivity would mean that the FTP script would need to reestablish a session and resend any file that experienced a file transfer disconnect prior to successful completion of the file transfer.

For outbound file transfers, inadvertent loss of connectivity would mean that the FTP script would have to reestablish a session and get the remaining files in the outbound directory tree. In addition, outbound files should not be deleted until the ‘get’ command is completed successfully.

4 Business Continuity & Troubleshooting

Business Continuity is the general reference to business procedures that are put in place to minimize business impact during unexpected service disruption. It is highly recommended that alternative file transfer methods are discussed, and appropriate contingency plans are put in place with SAMSKIP to ensure the appropriate actions are taken such as a viable communications plan with the appropriate contacts information. Please provide business continuity contacts to SAMSKIP Integration Team and note the SAMSKIP customer service contacts in case a need arises to escalate a situation for SAMSKIP to address. The sections below provide high level information on managing file transfer disruptions.

4.1 Primary Site Connectivity

SAMSKIP provides a Portal environment (https://my.Samskip.com/) at the primary processing data center. There are diverse internet access links as well as multiple file transfer servers implemented to ensure a reliable and resilient service. When file transfers are not successfully exchanged with SAMSKIP, please follow the troubleshooting guide to isolate where the service disruption is occurring. For example, the troubleshooting steps will help isolate an internet access issue, a local firewall issue or file transfer server issue.

4.2 Alternate Site Connectivity

To protect your business interest, SAMSKIP provides an alternate processing center that will be brought online in order to service transactions with minimal business disruption. Please contact SAMSKIP Integration Team to get technical details on connecting to the SAMSKIP Portal, including the alternate site location. If there are any issues connecting to the alternate site, please refer to "Appendix B: Troubleshooting Guide" for appropriate diagnostic steps.

If there is a known disruption of file transfer services on the SAMSKIP Portal, please contact SAMSKIP Integration Team (edisupport@samskip.com).

Appendix A: Initiation Document

An organization wishing to establish a trading partnership with SAMSKIP must fill out the SAMSKIP Initiation Document. Please enter all necessary information concerning your trading profile and return this document to SAMSKIP Integration Team (edisupport@samskip.com).

Short Business Case description	
Project description	
Scope	
Current situation	
Future situation\Goal	
Deadline	
Problems identified	
Risks	

Contacts (name, phone and e-mail)	
Client: IT	
Client: operations	
Client: Intermediair	

Connection	
Connection type	
Incoming messages: (Client > Samskip)	
Outgoing messages: (Samskip > Client)	
Additional requirements (if any)	
Requested deployment date	
Comments	

For SFTP	
FTP connection Name	
Agreed inbound server IP/Port	
Agreed outbound server IP/Port	
Inbound directory	
Outbound directory	
Mode (BIN, etc.)	
UID/Pass inbound server	
UID/Pass outbound server	
Customer UID	
Customer PWD	

For AS2	
Outgoing messages: (Samskip > Supplier)	
AS2 Name	
Preferred Mode	
Outbound IP	
Inbound URL	
Certificate	
Message Digest	
Encryptions	
MDN	

Intermediar / Platform	
Booking Flow	○ Alpega - formerTranswide ○ Transporeon ○ Infor Nexus ○ INTTRA ○ Elmica ○ Other: ……
Track and Trace	○ FourKites ○ Sixfold ○ Project44 ○ Shippeo ○ Other: …….

Appendix B: Troubleshooting Guide

AS2

Site Diagnostics

SAMSKIP supports both HTTP and HTTPS for AS2 file transfers. The URLS for each are as follows:

- http://edi.samskip.eu:9999/as2test (AS2 over HTTP)
- https://edi.samskip.eu:9443/as2 (AS2 over HTTPS)

In order to exchanges files over the SAMSKIP AS2 channel the firewall configuration needs to allow for the flow described below:

- files flowing from the trading partner to SAMSKIP needs IP Addresses 145.131.219.66 with ports 9999 (http) or port 9443 (https) open
- files flowing from SAMSKIP to the trading partner needs IP Addresses 145.131.219.66 with ports 9999 (http) or port 9443 (https) open

If you are experiencing issues sending files to SAMSKIP, take the following diagnostic steps below and provide the results when you contact SAMSKIP Helpdesk.

1. Please provide the results of the following diagnostic commands in order to troubleshoot AS2 URL connectivity to the SAMSKIP Primary Data Center.
    a) ping edi.samskip.com
    b) nslookup edi.samskip.com
    c) telnet edi.samskip.com 21
    d) traceroute edi.samskip.com

FTP/sFTP

Site Diagnostics

The troubleshooting steps below will provide a systematic check of the URL that provide FTP access. Provide the results when you contact SAMSKIP Helpdesk.

1. Please provide the results of the following diagnostic commands to troubleshoot FTP URL connectivity to the SAMSKIP Helpdesk.
    a) ping edi.samskip.com
    b) nslookup edi.samskip.com
    c) telnet edi.samskip.com 21
    d) traceroute edi.samskip.com