

MANUAL DE CONFIGURAÇÃO DO CONECTA PARA INSURCONNECT

Requisitos para implementar em novos ambientes

SUMÁRIO

1	OBJETIVO	3
2	CONECTA	3
2.1	Envio e recebimento de Arquivos	3
2.2	Formas de comunicação	4
2.3	Protocolos	4
2.3.1	Connect:Direct	4
2.3.2	SFTP/SSH	7
3	PROCESSO DE ATIVAÇÃO, SUBSTITUIÇÃO E REVOGAÇÃO DE CERTIFICADOS E CHAVES.....	9
4	RECOMENDAÇÕES	10
5	CONTATOS ATENDIMENTO SEGUROS.....	11

1 OBJETIVO

Este manual tem o objetivo de consolidar os requisitos técnicos necessários para implementar o Conecta para a plataforma InsurConnect.

2 CONECTA

O conecta funciona 24 horas, porém, se os arquivos forem enviados enquanto a grade de transferência de arquivos estiver fechada, estes ficarão em *standby* até que a próxima grade de processamento esteja disponível novamente.

O Conecta está estruturado para tratar arquivos com alta concentração de registros em processos batch e de forma cíclica e está otimizado para trabalhar com o processamento de arquivos com grande volume de registros em detrimento do envio de muitos arquivos com poucos registros. Por esta razão é recomendado que sejam construídos processos de concentração de registros e posterior criação e envio dos arquivos considerando um intervalo parametrizável de 20 minutos. **Existe no Conecta uma limitação em relação ao tamanho do arquivo. Esse limite é de 1GB para os arquivos de entrada.**

2.1 Envio e recebimento de Arquivos

O nome do arquivo deve seguir o padrão:

[NomeDoArquivo].txt

Exemplo: teste.txt

Para todo arquivo recebido via Conecta e processado no InsurConnect, seu retorno chegará da seguinte forma:

[NomeDoArquivo].txt.S[NúmeroDeSolicitação]

Exemplo: teste.txt.S3123456

2.2 Formas de comunicação

É possível o Cliente comunicar-se via RTM ou via internet.

Para conexões trafegadas via RTM, o Cliente deve entrar em contato com a RTM para definir o melhor modelo de configuração para contingência de rede, considerando questões como NAT e resolução de nomes DNS. Aconselhamos ter apenas um endereço IP para os dois ambientes: Produção e Contingência.

No caso de configuração de conexões via internet, o Cliente deve verificar junto ao seu time de redes, em relação ao endereço IP para entrada e saída nos ambientes de Produção e Contingência.

2.3 Protocolos

O Conecta suporta a transferência de arquivos em duas modalidades: Connect:Direct e SFTP. A escolha da plataforma deve ser feita pela Instituição Financeira cliente.

2.3.1 Connect:Direct

Connect:Direct é um protocolo desenvolvido pela IBM para transferência de arquivos ponto-a-ponto. A arquitetura permite o envio e recebimento automatizado de arquivos, com segurança, gerenciamento e dinâmica entre sistemas operacionais distintos. Mais detalhes sobre o software podem ser consultados no site do fabricante: www.ibm.com.

Nesse modelo, as duas pontas (B3 x Instituição) são servidores e enviam e recebem arquivos.

2.3.1.1 Parâmetros para configuração

Autenticação

A autenticação é feita em 2 passos:

Passo 1. Node + IP + usuário

Passo 2. Validação do certificado digital através do módulo Security+.

Certificado

A B3 enviará o certificado para autenticação dos clientes no CD. O cliente é responsável por fornecer o certificado para autenticação em seu CD. Esse certificado deve atender aos seguintes requisitos:

- Tamanho da chave: 2048 bits
- Algoritmo de hash: SHA 256
- Certificado SSL para servidor
- Emitido por uma CA (Autoridade Certificadora) de raiz confiável.

Importante

Recomendamos que cada ambiente tenha apenas um certificado ativo, para maior transparência no processo de contingência. O certificado de produção deve ser o mesmo em contingência.

É importante que os certificados de Homologação e Produção sejam gerados pela mesma certificadora a fim de validar todo o processo homologatório.

Módulo Secure+

O Módulo Secure+ deverá estar habilitado com o protocolo **TLS 1.2**.

Ativar os padrões de criptografia listados abaixo.

- ECDHE_RSA_WITH_AES_256_GCM_SHA384*
- ECDHE_RSA_WITH_AES_128_GCM_SHA256
- ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Conexões

No Conect:Direct, a comunicação é bidirecional, ou seja: Servidor ⇔ Servidor. Serão necessárias liberações no ambiente da B3 e da Instituição Participante na porta padrão para este protocolo, que está definida pela porta **1364**.

Endereços para Conexão com a B3 via CD

Ambiente	Comunicação	RTM	INTERNET
CERT	Node	B3SEG-RTM-CERT	B3SEG-WEB-CERT
	URL/IP	edi-insurconnect-cert.rtm.netb3.com.br (10.0.48.90)	edi-insurconnect-cert.b3.com.br 177.54.220.148 177.54.222.148
	Alternate Comm Info	N/A	177.54.214.4
PROD	NODE	B3SEG-RTM-PROD	B3SEG-WEB-PROD
	URL	edi-insurconnect-rtm.netb3.com.br (10.0.48.190)	edi-insurconnect.b3.com.br (177.66.125.144)
	Alternate Comm Info	N/A	177.66.125.22 177.54.220.22 177.54.222.22 200.19.56.250 (DR)

Caminho para ser enviado arquivo no Business Process

file=/businessprocess/BP_B3_IN_RECEBE_CD/nomeDoArquivoParaRetorno[.extensão]

Exemplo:

file=/businessprocess/BP_B3_IN_RECEBE_CD/nomeDoArquivoParaRetorno.txt

Os endereços IP e portas para conexão com o ambiente da Instituição Financeira devem ser informados, juntamente com os demais parâmetros, no Formulário termo de adesão enviado separadamente deste documento.

Business Process para Teste de Conexão

Para a realização de testes de conectividade, disponibilizamos a chamada de um BP, onde o participante irá enviar um arquivo e nós faremos uma chamada ao participante, devolvendo o mesmo arquivo recebido.

file=/businessprocess/BP_B3_TESTE_CD/nomeDoArquivoParaRetorno[.extensão]

Exemplo:

file=/businessprocess/BP_B3_TESTE_CD/nomeDoArquivoParaRetorno.txt

Recomendações de Parâmetros Adicionais:

- Sessões simultâneas (pNode e sNode Sessions): 5
- Buffer Size (SSL/TLS): 32K
- Tipo de transmissão: Texto e Binário (para arquivos zipados da transferência de arquivos)
- Retries (Process retry settings): “Short Term e Long Term” = 3 segundos
- Retry Interval: “Short Term” = 10 seg e “Long Term” = 3 min

2.3.2 SFTP/SSH

SFTP (SSH File Transfer Protocol) é um protocolo para transferência de arquivos de forma segura. Por padrão, o SFTP utiliza SSH para autenticação e criptografia da comunicação. Mais informações podem ser consultadas nesse endereço: https://wiki.filezilla-project.org/SFTP_specifications.

Nesse modelo, a B3 é apenas o servidor. O upload e download de arquivos é feito pelo cliente, através de sistemas SFTP *client*. Uma das opções de ferramenta *client* é o Filezilla, mas existem outras opções disponíveis no mercado que podem ser utilizadas pelo cliente.

O SFTP funciona como uma pasta virtual. O cliente tem que implementar um processo cíclico de leitura para verificar o conteúdo disponibilizado na pasta e sensibilização dos seus sistemas internos para processamento dos resultados.

2.3.2.1 Parâmetros para configuração

Autenticação

- Usuário e Par de Chave (SSH Pair Key)
- Par de Chaves

O cliente é responsável por fornecer a Chave pública para autenticação no serviço SFTP.

Obs: Não se trata de um certificado SSL. É necessário gerar o par de chaves SSH

Esse certificado deve atender aos seguintes requisitos:

- Tipo da chave: SSH-RSA
- Tamanho da chave: 2048 bits

Importante:

- Recomendamos que cada ambiente tenha apenas um par de chaves ativo, para maior transparência no processo de contingência. As chaves em produção deve ser as mesmas em contingência.
- Somente chaves assimétricas RSA-2048 bits serão aceitas.
- É vedado o reuso das chaves criptográficas para outras finalidades.
- Os participantes são responsáveis pela segurança, física e lógica, da chave privada criada.
- Do ponto de vista de gerenciamento, SFTP é o modelo com menor recurso de monitoração. Depende muito do sistema interno desenvolvido pela Instituição.

As chaves podem ser geradas tanto em ambiente Windows como Linux.

Conexões

No SFTP, a comunicação é unidirecional. Apenas o cliente conecta na B3.

Serão necessárias liberações no ambiente do Participante para acessar na porta padrão para este protocolo, que está definida pela porta **9039**.

Endereços para Conexão com a B3 via SFTP

Ambiente	RTM	INTERNET
CERT	edi-insurconnect-cert.rtm.netb3.com.br (10.0.48.90)	edi-insurconnect-cert.b3.com.br (177.54.220.148)
PROD	edi-insurconnect-rtm.netb3.com.br (10.0.48.190)	edi-insurconnect.b3.com.br 177.66.125.144 177.54.222.144 (DR)

Após estabelecer a conexão via SFTP aparecerão 3 diretórios principais que são:

IN – Local onde o cliente coloca os arquivos para processamento na B3 (envio);

Obs: Somente é possível enviar arquivos via conecta de até 1 GB, maior que isto o arquivo será rejeitado e retirado da fila de envio.

OUT – Por onde são respondidos os arquivos com informação de retorno e processamento;

OUT_BATCH – Por onde os clientes recebem os arquivos e relatórios disponíveis para o Malote cadastrado;

3 PROCESSO DE ATIVAÇÃO, SUBSTITUIÇÃO E REVOGAÇÃO DE CERTIFICADOS E CHAVES

A B3 não faz a validação dos certificados em qualquer lista de certificados revogados das CAs. Os certificados só serão considerados inválidos após o comunicado formal, via e-mail, pelo Participante.

A Instituição fica responsável por informar a B3 sobre a necessidade de atualizar o certificado. Essa solicitação deve ser enviada com 10 dias úteis antes da ativação. A solicitação deve ser enviada para atendimento.seguros@b3.com.br.

O processo de atualização do certificado deve, primariamente, respeitar os processos de governança das duas Instituições (B3 x Cliente). As alterações de configuração devem, preferencialmente, serem executadas em horário fora das janelas de funcionamento do sistema.

Os certificados substituídos deverão ser revogados, pelo Participante, junto à CA emissora, não podendo serem utilizados futuramente e nem as chaves a eles relacionadas.

A atualização do certificado em Produção não precisa passar por Homologação.

4 RECOMENDAÇÕES

- A Instituição Participante fica responsável por manter os registros de log de seu sistema, que conecta com a B3, permitindo a rastreabilidade e auditoria dos eventos de troca de arquivos.
- Os arquivos transmitidos entre os Participantes e a B3 serão tratados conforme as regras de negócio estabelecidas de forma irrevogável, incondicional e final. É importante considerar as regras do processo de transferência de arquivo existente no InsurConnect.
- As alterações na infraestrutura do cliente, como IP, DNS, certificados etc., devem ser informadas à B3 com pelo **menos 10 dias úteis antes da atividade.**
- O Conecta está estruturado para tratar arquivos com alta concentração de registros em processos *batch* e de forma cíclica, está otimizado para trabalhar com o processamento de arquivos com grande volume de registros em detrimento do envio de muitos arquivos com poucos registros. Por esta razão recomendamos que sejam construídos processos de concentração de registros e posterior criação e envio dos arquivos - ressaltando que o tamanho limite é de 1GB.

5 CONTATOS ATENDIMENTO SEGUROS

A Central de Atendimento da B3 estará disponível de segunda a sexta-feira das 08 às 18h:

- Telefone: 0300-777-1515
- E-mail: atendimento.seguros@b3.com.br
- [Acesse o Portal de Autoatendimento](#)