MAPX

MAPX-OP097-2021

Manual de Integração e Segurança R2C3

Objetivo: O Manual de Integração e Segurança do R2C3 tem a finalidade de descrever os procedimentos que os participantes devem seguir para configurar e permitir a conexão de seus sistemas com o ambiente Núclea. As interfaces de comunicação possíveis são Arquivos, Mensagens e API.

Autor do documento: Squad de Recebíveis.

Contato: Centro de Excelência Clientes.

Público-alvo: Instituições Participantes.

O responsável deve ser contatado nos casos de:

- Dúvidas sobre as informações tratadas neste documento;
- Falhas ou vulnerabilidades encontradas no processo;
- Necessidade de adequação identificada internamente, ou apresentada por auditoria, por órgão regulador, ou por cliente.

SUMÁRIO

1. OBJETIVO

Este documento tem como objetivo descrever os padrões, procedimentos e configurações a serem utilizados pelos participantes para transferência de informações com a R2C3.

2. DIVULGAÇÃO

Este documento pode ser encontrado:

- Portal Corporativo da Núclea;
- Site da Núclea.

3. VIGÊNCIA

Este manual deverá ser revisto quando do vencimento de sua vigência, ou quando necessário.

4. PROCESSO DE REFERÊNCIA

- **Manual de Segurança do SFN versão 4.01**
  https://www.bcb.gov.br/content/estabilidadefinanceira/cedsfn/Manual_Segurança_SFN-v4_01.pdf

- **Catálogo de Serviços do SFN**
  Volume II
  https://www.bcb.gov.br/content/estabilidadefinanceira/cedsfn/Catalogos/Catalogo_de_Servicos_do_SFN_Volume_II_Versao_414.pdf
  Volume V
  https://www.bcb.gov.br/content/estabilidadefinanceira/cedsfn/Catalogos/Catalogo_de_Servicos_do_SFN_Volume_V_Versao_414.pdf

- **ICP-Brasil Resolução 41**
  http://www.iti.gov.br/images/repositorio/legislacao/resolucoes/emvigor/RESOLU__O_41_DE_18_04_2006.PDF

5. DISPOSIÇÕES GERAIS

5.1. PREMISSAS E CONSIDERAÇÕES GERAIS

As regras e padrões deste documento foram concebidos para garantir o intercâmbio de arquivos, mensagens e requisições API entre o ambiente R2C3 e os Participantes de forma segura, controlada, com um uso eficiente dos meios de transmissão, com resiliência e suporte a automação.

5.2. PLATAFORMAS DE TRANSFERÊNCIA DE INFORMAÇÕES SUPORTADAS PELA R2C3

5.2.1. PLATAFORMAS SUPORTADAS

A R2C3 suporta a troca de arquivos pelas plataformas IBM Connect:Direct e Axway CFT (ou XFB), ambas largamente utilizadas nos meios financeiros em virtude de sua robustez e confiabilidade. Os arquivos serão utilizados para operações Batch, onde há maior tolerância a tempos de resposta/retorno. Cabe ressaltar que apenas uma ferramenta será disponibilizada por participante. Portanto, haverá necessidade de opção por

uma das duas ferramentas, o qual deve ser feito pelo documento de adesão ao sistema. O sistema também permite conexão para operações online via Mensagens, utilizando o produto IBM Websphere MQ Series, bem como requisições API Rest. Cabe reforçar que não terá restrições técnicas de escolha nesse caso, portanto no ponto de vista técnico os participantes poderão usar as duas ferramentas concomitantemente.

O tamanho máximo foi considerado devido a característica de negócio das transações. Recomendamos que o participante faça a escolha do canal que melhor se enquadra no seu perfil transacional.

É importante ressaltar que payloads grandes tem um tempo maior de transmissão pela rede, maior possibilidade de retransmissão de pacotes, tempo maior para decriptografia, processamento e geração da resposta e transmissão da resposta quando enquadrada no mesmo cenário, assim como a notificação para terceiros.

5.2.2. REDES SUPORTADAS

- Requisições via arquivos (IBM Connect:Direct/Axway CFT) devem ser feitas via RTM – Financial NET;
- Requisições via mensagens (IBM Websphere MQ) devem ser feitas via RTM – Financial NET;
- Requisições via API devem ser feitas via Internet; e
- As informações do ambiente Núclea estão descritas nos tópicos seguintes.

5.2.3. IBM CONNECT:DIRECT

O Connect:Direct é um software para a transferência de arquivos ponto-a-ponto com arquitetura que permite o envio e recepção automática de arquivos com gerenciamento, garantindo a entrega dos dados, independente da utilização de redes públicas ou privadas. O Connect:Direct oferece funcionalidades de segurança para transferências de dados, independentemente do tipo de informação trafegada. Transmite arquivos contendo todos os tipos de dados, pelas múltiplas plataformas, sistemas de arquivos e mídias distintas.

5.2.4. AXWAY CFT (EX – XFB)

O Axway Transfer CFT também é um software para a transferência de arquivos ponto-a-ponto com arquitetura que permite o envio e recepção automática de arquivos, com total gerenciamento, garantindo a entrega dos dados independentemente da utilização de redes públicas ou privadas. O XFB oferece funcionalidades de segurança para transferências de dados, independentemente do tipo de informação trafegada. Transmite arquivos contendo todos os tipos de dados, pelas múltiplas plataformas, sistemas de arquivos e mídias distintas.

5.2.5. IBM WEBSPHERE MQ

O IBM MQ é um middleware de sistema de mensagens robusto, seguro e confiável. Ele usa mensagens e filas para suportar troca de informações entre aplicativos, sistemas e serviços. Ele simplifica e acelera a integração de diferentes aplicativos e dados de negócios em múltiplas plataformas. Um dos pontos fortes do MQ é sua capacidade de ser altamente configurável e customizável para ambientes distintos e para as diferentes necessidades de transmissão de dados.

5.2.6. API

O protocolo HTTP permite uma grande possibilidade de troca de informações e já é mundialmente utilizado para integração entre sistemas. Por ser um protocolo com tamanha adesão e com infraestrutura simplificada facilita o monitoramento e requer poucos recursos para operação. A característica das aplicações HTTP permite usualmente uma boa escalabilidade. A utilização da arquitetura REST sobre HTTP se ajusta facilmente à modelagem de negócio. Também existem várias vantagens em relação aos testes dos sistemas. É importante observar que a utilização deste protocolo está normalmente ligada a requisições síncronas (também podendo ser assíncronas, com uma requisição de “call-back” ou com um “pooling” de requisições); não considerando as possibilidades advindas do protocolo HTTP2.

A comunicação será feita por meio de protocolo seguro HTTPS tanto para homologação quanto para produção.

A especificação dos métodos estará descrita em um arquivo estruturado na OAS 3.0 (open api specification – V3 – swagger) em formato yaml.

5.3. CARACTERÍSTICAS DOS ARQUIVOS E MENSAGENS DA R2C3

Os arquivos e mensagens trafegados na R2C3, bem como as regras e padrões que a eles se aplicam, estão descritos em detalhe no Manual de Leiautes da R2C3, que também descreve a estrutura e orientações para conteúdo deles.

Como os arquivos e mensagens que trafegam na R2C3 são obrigatoriamente compactados, assinados digitalmente e criptografados (nesta ordem) já na sua geração, não há necessidade de uso de mecanismos adicionais de criptografia ou compactação de dados na transmissão, tais como o Secure+ da plataforma Connect:Direct, que apenas onerariam a solução final, sem benefício correspondente.

Os passos necessários para que um Participante realize troca de arquivos com a Núclea por meio do Connect:Direct ou CFT, são os seguintes:

- **a.** Construir uma requisição, em formato definido no manual de leiautes;
- **b.** Compactar esse posicional usando o algoritmo “gzip” do padrão ZIP (implementado no Unix pelo gzip, em Java pelo java.util.zip, em C pelo zlib, etc).
- **c.** Assinar e encriptar o arquivo e mensagens utilizando um framework de criptografia padrão SPB - “5 Especificações para Segurança de Mensagens e Arquivos” do Manual de Segurança da RSFN.;

d. Enviar para a Núclea esse arquivo da requisição, já em formato SPB encriptado e assinado, utilizando o Connect:Direct ou XFB usando o modo de transferências binário;
e. Após o processamento desse arquivo de requisição, a Núclea enviará de volta um arquivo de resposta, também em formato SPB encriptado e assinado;
f. O arquivo de resposta em formato SPB encriptado e assinado deve ser agora transformado em posicional compactado, utilizando novamente o mesmo framework de criptografia padrão SPB;
g. O posicional compactado deve ser agora descompactado, usando a operação inversa do algoritmo "gzip" do padrão ZIP;
h. A resposta posicional está agora disponível, para ser processada pelo sistema do Participante, de acordo com o formato de resposta definido no manual de leiautes.

Deve ser utilizado o padrão Unicode UTF-8. As codificações estão descritas em http://www.unicode.org.

A definição de caractere, para este Catálogo, é a utilizada no padrão XML 1.0. Trata-se de uma "unidade atômica de texto, como especificado pela norma ISO/IEC 10646:2000. Caracteres legais são a tabulação (tab), o retorno de carro (Carriage Return), a alimentação de linha (Line Feed) e os caracteres legais dos padrões Unicode e ISO/IEC 10646:2000". Exceções à esta regra devem ser notificadas através do Cadastro Técnico.

O subconjunto de caracteres Unicode que são aceitos como texto nas mensagens XML do Catálogo estão compreendidos nas faixas "0000-007F" ("Basic Latin (ASCII) ") e "0080-00FF" ("Latin-1 Supplement"). Em ambas as faixas, os caracteres de controle ("C0" e "C1") que não são aceitos nem recomendados no padrão XML 1.0 também não serão aceitos no conteúdo dos arquivos e mensagens.

Portanto, para os arquivos e mensagens, um caractere válido é definido pela seguinte expressão regular, contendo códigos de caracteres Unicode:

Caractere ::= #x0009 | #x000A | #x000D | [#x0020-#x007E] | #x0085 | [#x00A0-#x00FF]

Opcionalmente, para os dois primeiros bytes das mensagens, poderá ser utilizado o Byte Order Mark (BOM) para o Unicode UTF8, que corresponde a #xEFBBBF.

Os caracteres de padding #x0000, caso existam, deverão ser removidos antes da validação da mensagem pelo parser XML. O padding nas mensagens deste Catálogo está descrito no Manual de Segurança do SFN.

Os arquivos deverão ter o conteúdo com o tamanho máximo de 50 Mbytes após a criptografia e compactação e as mensagens deverão ter o conteúdo com o tamanho máximo de 250 Kbytes após a criptografia e compactação. Vale ressaltar que a mensagem GEN0004 não será compactada e criptografada visando a notificação dos erros de processamento inclusive relacionados ao atendimento dos requisitos (criptografia e compactação). Caso seja necessário enviar uma mensagem com o conteúdo maior que o citado anteriormente, será necessário particionar em múltiplas mensagens, seguindo o padrão de particionamento do SPB. Para compactação é obrigatório preencher o campo C04 do cabeçalho de segurança com o domínio 8 (conforme descrito no item 6.6).

Em complemento, aplicar-se-ão, durante a validação do parser XML, todas as regras descritas no padrão XML 1.0, de modo que todas as mensagens deverão resultar bem-formadas e válidas.

5.4. CARACTERÍSTICAS DAS APIS

Para o projeto R2C3 foi definida a obrigatoriedade de assinatura digital em todas as requisições e respostas (independentemente de qual seja a funcionalidade). Para maiores detalhes em relação à assinatura deve-se consultar a seção ESPECIFICAÇÃO PARA A SEGURANÇA PARA INTEGRAÇÃO VIA API. A validação da assinatura ficará a cargo do consumidor da API.

Em todas as requisições e respostas o body do HTTP deverá ser codificado utilizando o padrão UTF-8.

O protocolo HTTP originalmente é considerado síncrono, mas para atender alguns requisitos funcionais ou não funcionais é necessária a criação de artifícios para realizar um processamento de forma assíncrona. Para o R2C3 seguem alguns critérios para a determinação da comunicação (síncrona/assíncrona):

a. **Tempo de resposta:** para transações que tiverem um tempo de resposta elevado é indicado que o resultado do processamento seja feito através de um call-back (onde cliente disponibiliza um endpoint para receber o resultado do processamento);
b. **Integração com outros participantes:** para transações que necessitarem uma integração com diferentes participantes é aconselhável a definição de um processamento assíncrono pois existe uma dependência da disponibilidade de cada um dos participantes da transação; também sendo indicada a criação de um call-back;
c. **Tamanho do payload:** algumas transações necessitam a transferência de um grande volume de informação mesmo que para uma transação unitária; para estes casos além da indicação da utilização de compactação dos dados também temos algumas opções dependendo do tipo de transação:
d. **Transações de consulta (requisição pequena e grande volume na resposta):** para este tipo de transação indica-se o uso de sucessivas requisições síncronas com respostas paginadas; e
e. **Transações de inclusão (requisição e respostas grandes):** para este tipo de transação indica-se a remodelagem ou criação de novos recursos para tornarem as requisições menores bem como suas respostas; caso isto não seja possível torna-se necessária a quebra da requisição em múltiplas requisições similares ao sequenciamento do protocolo SPB, neste último caso as respostas do processamento serão enviadas através de requisições para um call-back disponibilizado.

Para o R2C3 tem-se imposto um limite de tamanho de payload de 400Kb levando em consideração também a possibilidade de utilização da compactação dos dados. A seguir uma breve tabela indicando o tamanho de payload para transações que envolvam lotes de unidades recebíveis:

Payload	Aberto	Compactado (GZIP)
2 k	≈4 UR	≈30 UR
15 K	≈30 UR	≈220 UR

35 K	≈100 UR	≈750 UR
320 K	≈1.000 UR	≈7.500 UR
400 K	≈1.200 UR	≈9.000 UR

Caso existam transações que necessitem de requisições grandes será disponibilizado um endpoint que aceitará o conteúdo compactado (na requisição).

As transações que tiverem comportamento assíncrono e que necessitarem algum requisito de compactação além do padrão estarão descritas no manual de leiautes.

5.5. REGRAS PARA A TRANSFERÊNCIA DE ARQUIVOS E MENSAGENS NA R2C3

a. Os arquivos devem ser compactados no formato GZIP (conforme especificado na RFC 1952) e posteriormente cifrados e assinados digitalmente, salientando que a cifragem e a assinatura acorrem em um processo simultâneo. No caso do Unix, o aplicativo "gzip" implementa este formato. Se a compactação for feita diretamente em Java, pode-se utilizar a classe standard "java.util.zip.GZIPOutputStream". Caso a compactação seja feita em C, existe a biblioteca “zlib” que também implementa o padrão GZIP sem alterações;

b. Os arquivos devem ser transferidos sempre em modo binário (pois já estão compactados e criptografados);

c. Quaisquer mecanismos adicionais de criptografia ao nível da ferramenta de troca de arquivos, como por exemplo o Secure+, deve estar desabilitado;

d. Todos os arquivos devem ser compactados no formato GZIP, assinados digitalmente e criptografados, nesta ordem, por aplicação específica, antes de serem disponibilizados para as plataformas de transferência de arquivos;

e. Todas as transferências devem desabilitar verificação de CRC – CyclicRedundancy Check, pois a integridade deles já é garantida pelo protocolo de transporte (TCP), além de trafegarem em meios digitais de alta confiabilidade;

f. É obrigatória a habilitação da opção de retomada em caso de falha (checkpoint restart); após esgotarem-se as retentativas de transferência, o processo de transmissão será considerado mal-sucedido e deverão ser adotados os processos operacionais pela área de atendimento IMF.

g. Os Participantes podem conectar-se aos servidores de transferência de arquivos e mensagens da Núclea, utilizando-se de resolução de nomes dos domínios Núclea pelo serviço DNS, ou conectar-se pelo endereçamento IP explicito. Neste caso, é responsabilidade do Participante a alteração de seu ambiente, alterando o endereço IP correspondente, caso seja necessário acessar os servidores no sítio de contingência do R2C3, com respectiva interrupção dos serviços até que esta operação se complete:

i. Recomenda-se que o participante utilize seu próprio domínio via DNS publicado na rede RTM Financial NET (Não obrigatório).

h. Os arquivos gerados pela Núclea, destinados aos Participantes, poderão ser enviados pela Núclea e agregar ao processo de transmissão a utilização do recurso **RUN JOB** do Connect:Direct, caso o Participante faça a opção de receber o arquivo. A utilização deste recurso somente é permitida nas transmissões originadas na Núclea, não sendo permitida a utilização do recurso quando a transmissão iniciar nos Participantes. A Núclea, após o envio do arquivo, executara um comando e ou programa por meio de RUN JOB com o seguinte padrão de nome: CIPR2C3 “nome do arquivo”, onde CIPR2C3 é o programa a ser executado no Participante e “nome do arquivo” entra como parâmetro com o nome do arquivo enviado.

Qualquer parâmetro de configuração adicional na ferramenta de troca de arquivos, solicitado pela Instituição, que não estiver contemplado neste documento será estudado pelo time técnico da Núclea, sob possibilidade de inviabilidade de configuração.

5.6. ENDEREÇAMENTO IP DOS SERVIDORES HOMOLOGAÇÃO, PRODUÇÃO, CONTINGÊNCIA E DNS

Abaixo estão descritas as configurações e parâmetros necessários para a configuração das soluções IBM Websphere MQ, IBM Connect:Direct, Axway Transfer CFT e API.

5.6.1. ZONAS DNS

- (1) Zona Privada (RTM – FINANCIAL NET): CIPR2C3.ORG

(1) Recomenda-se que o participante utilize seu próprio domínio via DNS publicado na rede RTM Financial NET (Não obrigatório).

- (2) Zona Pública (Internet): CIPR2C3.ORG.BR

(2) Apenas para API

5.6.2. SERVIDORES AUTORIATIVOS PARA ZONA PRIVADA

Função	Local	IP
Servidor DNS 1	RTM RJ	10.0.17.2
Servidor DNS 2	RTM SP	10.0.33.2

5.6.3. ENDEREÇOS DO AMBIENTE

Connect:Direct:

Hostname	IP	Porta	Ambiente
cdh.cipr2c3.org	10.200.61.149	1364	Homologação
cdp.cipr2c3.org	10.200.61.21	1364	Produção

Axway CFT:

Hostname	IP	Porta	Ambiente
cfth.cipr2c3.org	10.200.61.149	6330	Homologação
cftp.cipr2c3.org	10.200.61.21	6330	Produção

IBM Websphere MQ:

Hostname	IP	Porta	Ambiente
mqs02.cipr2c3.org	10.200.61.150	1514	Homologação
mqs01.cipr2c3.org	10.200.61.22	1414	Produção

API Gateway (Internet)

Hostname	IP*	Porta	Ambiente
apihext.cipr2c3.org.br	200.185.79.57	443	Homologação
api.cipr2c3.org.br	200.185.79.45 200.185.34.236	443	Produção
api.cipr2c3.org.br	179.190.27.236	443	Contingência

* Os IPs informados trata-se dos IPs de saída para as chamadas API origem Núclea, destino Participante

Obs.: Recomendamos que os participantes não configurem suas aplicações com os IP dos servidores da Núclea, e sim com os hostnames. O ambiente de Contingência permanecerá inativo e o processo de convergência será transparente para o participante diante desta condição.

5.6.4. Configurações: Connect:Direct, CFT, MQ SERIES e API

Abaixo estão descritas as configurações e parâmetros necessários para a configuração da solução Connect:Direct.

Connect:Direct Ambiente Núclea – Ambientes Produção e Homologação	
Node	Produção: R2CDCIPP Homologação: R2CDCIPH
DNS Names / IP do servidor Connect:Direct	Produção: cdp.cipr2c3.org / 10.200.61.21 Homologação: cdh.cipr2c3.org / 10.200.61.149
Porta de Comunicação	TCP-1364
Usuário de conexão	Ambiente Produção: P29011780 Ambiente Homologação: H29011780
Proxy User	Habilitado
Sessões simultâneas (máx)	Envio: 5 (Por Instituição) Recepção: 5 (Por Instituição)
Buffer Size	32k
Protocolo de Transporte	TCP
Tipo de transmissão	Binário
Compressão	Desabilitada
Criptografia (Secure+)	Desabilitada
CRC	Desabilitado

CFT Ambiente Núclea - Ambientes Produção e Homologação	
Site:	Produção: R2CFCIPP Homologação: R2CFCIPH
DNSNames / IP do servidor CFT	Produção: xfbp.cipr2c3.org / 10.200.61.21 Homologação: xfbh.cipr2c3.org / 10.200.61.149
Portas de Comunicação	TCP-6330
Aplicação	CIPTOIF(aplicação Sender Núclea → IF) IFTOCIP (aplicação Receiver IF → Núclea)
Usuário de conexão	Ambiente Produção: P29011780 Ambiente Homologação: H29011780
Proxy User	Habilitado
Sessões simultâneas	Envio: 5 (Por Instituição) Recepção: 5 (Por Instituição)
Buffer Size	32K
Protocolo de Transporte	TCP
Tipo de transmissão	Binário
Blocagem / Tam Reg	Variável (XML)
Compressão	Desabilitada
Criptografia	Desabilitada
Checkpoint Restart	Habilitado
CRC	Desabilitado
Retries	3 a cada 10 minutos
Protocolos	PeSIT

MQ Ambiente Núclea - Ambientes Produção e Homologação	
Cod ISPB	29011780
URL do Servidor MQ	Produção: mqs01.cipr2c3.org - 10.200.61.22 Homologação: mqs02.cipr2c3.org - 10.200.61.150
Domínio	cipr2c3.org
Porta TCP-IP	Produção:1414 • Portas Instituições: 1414 a 1421 Homologação: 1514 • Portas Instituições: 1514 a 1521
Gerenciador de Filas (Queue Manager)	QM.29011780.**C**
Canal Sender	C29011780.**ISPBremoto.C**
Canal Receiver	**CISPBremoto.**29011780.**C**

5.6.5. Definições do MQ

Será ignorada a fila informada no campo ReplyToQ do header do MQ para as respostas geradas pelas aplicações. Será usada a fila de resposta padrão previamente definida.

A fila informada no campo ReplyToQ do header do MQ será usada apenas para as mensagens geradas automaticamente pelo Queue Manager (reports COA e COD). O gerenciador de filas informado no campo ReplyToQMgr deve ser informado no formato QM.ISPBRemoto.seq.

Para as respostas COA/COD se faz necessário configurar QM.ISPBRemoto.C.MSGP e QM.ISPBRemoto.C.HTTP por necessidades específicas do sistema R2C3.

Serão aceitas para processamento apenas as mensagens contidas na(s) fila(s) da respectiva instituição que as gerou.

O tamanho máximo de uma mensagem será 4 MBytes, incluindo o header do MQ, o header de segurança e a codificação do texto XML.

Dessa forma, os campos importantes da mensagem COA (e COD, opcionalmente), que devem ser guardados pelos participantes para fins de comprovação de emissão são:

- MsgId (MQBYTE24);
- AccountingToken (MQBYTE32);
- ApplIdentityData (MQCHAR32);

- PutDate (MQCHAR8);
- PutTime (MQCHAR8).

Padrão de nomes para objetos MQ que será usado no ambiente R2C3, dos prestadores de serviços e das demais instituições participantes:

Filas locais (na IF):

Núclea **requisita** à IF	**QL.REQ.ISPBRemoto.ISPBLocal.seq.**
Núclea **responde** à IF	**QL.RSP.ISPBRemoto.ISPBLocal.seq.**
Núclea **reporta** à IF	**QL.REP.ISPBRemoto.ISPBLocal.seq.**
Núclea envia mensagens de **suporte** à IF	**QL.SUP.ISPBRemoto.ISPBLocal.seq.**

Filas remotas (na IF):

IF **requisita** à Núclea	**QR.REQ.ISPBLocal.ISPBRemoto.seq**
IF **requisita** à Núclea	**QR.RSP.ISPBLocal.ISPBRemoto.seq**
IF **requisita** à Núclea	**QR.REP.ISPBLocal.ISPBRemoto.C** **QR.REP.ISPBLocal.ISPBRemoto.P** **QR.REP.ISPBLocal.ISPBRemoto.H** **Obs.** A fila local requisitada e preenchida no campo *ReplyToQ alias* definido no ambiente da Núclea, que receberá as mensagens geradas ***automaticamente*** pelo *Queue Manager*, tais como COA, COD, *Report Exceptions*.
IF envia mensagens de **suporte** à Núclea	**QR.SUP.ISPBLocal.ISPBRemoto.seq**
IF envia mensagens de COA/COD	**QM.ISPBRemoto.C.MSGP** **Preencher os campos:** **Gerenciador de Fila Remota(RQMNAME): QM.ISPBRemoto.C.MSGP** **Fila de Transmissão(XMITQ): QM.ISPBRemoto.C**
IF envia mensagens de COA/COD	**QM.ISPBRemoto.C.HTTP** **Preencher os campos:**

	Gerenciador de Fila Remota(RQMNAME): QM.ISPBRemoto.C.HTTP **Fila de Transmissão(XMITQ): QM.ISPBRemoto.C**

Filas locais (Núclea):

IF **requisita** à Núclea	**QL.REQ.ISPBRemoto.ISPBLocal.seq**
IF **requisita** à Núclea	**QL.RSP.ISPBRemoto.ISPBLocal.seq**
IF **requisita** à Núclea	**QL.REP.ISPBRemoto.ISPBLocal.C** **QL.REP.ISPBRemoto.ISPBLocal.P** **QL.REP.ISPBRemoto.ISPBLocal.H**
IF envia mensagens de **suporte** ao Núclea	**QL.SUP.ISPBRemoto.ISPBLocal.seq**

Filas remotas (Núclea):

Núclea **requisita** à IF	**QR.REQ.ISPBLocal.ISPBRemoto.seq**
Núclea **responde** à IF	**QR.RSP.ISPBLocal.ISPBRemoto.seq**
Núclea **reporta** à IF	**QR.REP.ISPBLocal.ISPBRemoto.seq**
Núclea envia mensagens de **suporte** à IF	**QR.SUP.ISPBLocal.ISPBRemoto.seq**

Filas de Transmissão: QM.ISPBRemoto.seq.

Queue Manager Alias Name: QM.ISPBLocal.seq.

- seq será igual a **C** para o R2C3

Exemplos: no R2C3 a fila de requisição da instituição 99999999 poderá ser a QL.REQ.99999999.00038166.C e o *queue manager* da instituição 99999999 poderá ser QM. 99999999.C

Canal sender: CISPBLocal.ISPBRemoto.n

Canal receiver: CISPBRemoto.ISPBLocal.n

- n será igual a **C** para o R2C3

Exemplo: no domínio R2C3, no *queue manager* da IF, o canal receptor (*receiver*) poderá ser C29011780.99999999.C (tráfego Núclea à IF 99999999) e o canal emissor (*sender*), C99999999. 29011780.C.

Observações:

- **ISPBRemoto** é o ISPB ou o CNPJ base da instituição a qual pertence o *queue manager* remoto, com 8 dígitos;
- **ISPBLocal** é o ISPB ou o CNPJ base da instituição à qual pertence o *queue manager* local, com 8 dígitos;
- definir todos os objetos MQ usando letras MAIÚSCULAS;
- as filas de suporte são específicas para uso das equipes de suporte ao *queue manager* dos participantes do sistema;

Para se conectar à R2C3, cada instituição deverá definir um Queue Manager Alias Name da seguinte forma:

DEFINE QREMOTE (‘QM.ISPBLocal.seq’);

DESCR('QUEUE MANAGER ALIAS NAME’) RNAME (' ');

RQMNAME ('nome real do queue manager da instituição');

XMITQ (' ')

REPLACE

Atenção:

Para os aglomerados e conglomerados que concentram mais de uma instituição num único *queue manager*, o padrão para o nome da fila de transmissão passa a ser QM.ISPBLocal.ISPBRemoto.seq. Além disso, para esses ambientes e para os que estão conectados a eles (BC e Prestadores), há a inclusão do conceito de *ReplyToQ alias* para permitir o retorno dos *reports* solicitados. O uso do *ReplyToQ alias* permite que as aplicações não precisem colocar o nome do *queue manager* no campo *ReplyToQMgr* do *header* do MQ e retira da aplicação a "decisão" sobre qual *ReplyToQmgr* apontar no MQMD para receber a resposta. Para isso, a aplicação informa o *alias* no *ReplyToQ* e deixa o *ReplyToQmgr* em branco, e deve ser definido o seguinte objeto no MQ para cada instituição à qual se está conectado:

DEFINE QREMOTE (‘nome da reply-to-queue alias à escolha da instituição’)

DESCR('REPLYTOQUEUE ALIAS NAME’)

RNAME (' nome da fila local de report ou QL.REP.ISPBRemoto.ISPBLocal.seq’)

RQMNAME (‘QM.ISPBRemoto.seq ou QM.ISPBRemoto.ISPBLocal.seq’)

XMITQ (' ')

REPLACE

A decisão do nome do RQMNAME é baseada no nome da fila de transmissão do *queue manager* remoto para o *queue manager* local. Ou seja, no ambiente do conglomerado ou aglomerado o RQMNAME é sempre **QM.ISPBRemoto.seq** e, nos ambientes aos quais o conglomerado ou aglomerado está conectado, é **QM.ISPBRemoto.ISPBLocal.seq**.

5.6.6. HEADER DO MQ (MQMD)

Alguns campos do header das mensagens que trafegam no MQ (MQMD) deverão ser formatados de acordo com o definido a seguir:

Report: ativar requisição dos *reports* do tipo COA (*Confirm on Arrival*), COD (*Confirm on Delivery*) e *Report Exception;*

MsgType: usar opção *request* para uma requisição, *reply* para resposta a uma requisição e *report* para um *report;*

Encoding: usar valor nativo da máquina onde está o MQ (opção *native* do MQ);

Persistence: usar opção *Persistence*;

Format: usar opção *NONE*;

CodedCharSetId: usar um dos listados abaixo: 37, 256, 273-275, 277-278, 280, 282, 284-285, 290, 297, 367, 420, 423-424, 437, 500, 813, 819, 833, 836, 838, 850-852, 855-858, 860-866, 869-871, 874-875, 880, 891, 895, 897, 903-905, 912, 915-916, 920, 923-924, 1004, 1009-1021, 1023, 1025-1027, 1040-1043, 1046-1047, 1051, 1088-1089, 1097, 1100-1107, 1114-1115, 1126, 1140, 1148, 1250-1256, 1275, 5348

ReplyToQ: informar o nome da fila, ou o *ReplyToQ alias* definido no ambiente da instituição, que receberá as mensagens geradas automaticamente pelo *Queue Manager*, tais como COA, COD, *Report Exceptions*.

Obs. A Núclea solicitara especificamente os retornos de COA/COD (ReplyToQ) nas filas abaixo, essa configuração será transparente para os participantes uma vez que o próprio MQ responde as mensagens COA/COD.

Exemplo:

QL.REP.999999999. 29011780.C

QL.REP.999999999. 29011780.P

QL.REP.999999999. 29011780.H

ReplyToQMgr: informar o *queue manager alias name*, de acordo com o definido anteriormente (QM.**ISPBLocal**.seq) ou deixar em branco no caso de usar *ReplyToQ alias*.

Atributos para objetos do MQ

Atributos Comuns a Todas as Filas		
ATRIBUTO	***DEFAULT***	***CONSENSO***
ClusterName		na
ClusterNamelist		na
DefBind		na
DefPersistence	NO	YES

DefPriority	0	default
InhibitGet	ENABLED	default
InhibitPut	ENABLED	default
Qdesc		livre
QName		
QType		
Scope	QMGR	livre

Tabela 1 - Atributos Comuns a Todas as Filas

Atributos de Filas Locais		
ATRIBUTO	***DEFAULT***	
Archive		livre
BackoutRequeueQName		livre
BackoutThreshold		livre
CreationDate		livre
CreationTime		livre
CurrentQDepth		livre
DefinitionType	TEMPDYN	livre
DefInputOpenOption		livre
DistLists	NO	livre
HardenGetBackout	NO	HARDENED
IndexType	NONE	livre
InitiationQName		na
MaxMsgLength	4M	4M
MaxQDepth	5000	máximo
MsgDeliverySequence	PRIORITY	FIFO
OpenInputCount		livre

OpenOutputCount		livre
ProcessName		livre
QDepthHighEvent	DISABLED	livre
QDepthHighLimit	80 (%)	livre
QDepthLowEvent	DISABLED	livre
QDepthLowLimit	40(%)	livre
QDepthMaxEvent	ENABLED	livre
QServiceInterval	999999999	livre
QServiceIntervalEvent	NONE	livre
RetentionInterval	999999999	livre
Shareability		livre
StorageClass	DEFAULT'	livre
TriggerControl		Livre
TriggerData		Livre
TriggerDepth	1	Livre
TriggerMsgPriority	0	Livre
TriggerType	FIRST	Livre
Usage	NORMAL	Livre

Tabela 2 - tributos de Filas Locais

Atributos de Filas Remotas		
ATRIBUTO	**DEFAULT**	
RemoteQMgrName		
RemoteQName		
XmitQName		

Tabela 3 - Atributos de Filas Remotas

Atributos de Alias Queues		
ATRIBUTO	***DEFAULT***	
BaseQName		

Tabela 4 - Atributos de Alias Queues

Atributos de NameLists		
ATRIBUTO	***DEFAULT***	
AlterationDate		livre
AlterationTime		livre
NameCount		livre
NamelistDesc		livre
NamelistName		livre
Names		livre

Tabela 5 - Atributos de NameLists

Atributos de Processos		
ATRIBUTO	***DEFAULT***	
AlterationDate		livre
AlterationTime		livre
ApplId		livre
ApplType		livre
EnvData		livre
ProcessDesc		livre
ProcessName		livre
UserData		livre

Tabela 6 - Atributos de Processos

Atributos de Queue Managers		
ATRIBUTO	***DEFAULT***	

AuthorityEvent	DISABLED	livre
ChannelAutoDef	DISABLED	livre
ChannelAutoDefEvent	DISABLED	livre
ChannelAutoDefExit		livre
ClusterWorkloadData		na
ClusterWorkloadExit		na
ClusterWorkloadLength		na
CodedCharSetId		livre
CommandInputQName		livre
CommandLevel		na

DeadLetterQName		livre
DefXmitQName		livre
DistLists		livre
InhibitEvent	DISABLED	livre
LocalEvent	DISABLED	livre
MaxHandles	256	livre
MaxMsgLength	4 Mb	4Mb
MaxPriority	9	livre
MaxUncommittedMsgs	10000	livre
PerformanceEvent	DISABLED	livre
Platform		livre
QmgrDesc		livre
QmgrIdentifier		livre
QmgrName		padrão
RemoteEvent	DISABLED	livre
RepositoryName		livre
RepositoryNamelist	livre	

StartStopEvent	ENABLED	livre
SyncPoint	AVAILABLE	livre
TriggerInterval	999999999	livre

Tabela 7 - Atributos de Queue Managers

Atributos de Canais		
ATRIBUTO	***DEFAULT***	
Auto start (AUTOSTART)	DISABLED	NA
Batch interval (BATCHINT)	0	default
Batch size (BATCHSZ)	50*	default
Channel name (CHANNEL)		padrão
Channel type (CHLTYPE)		padrão
CICS profile name		livre
Cluster (CLUSTER)		
Cluster namelist (CLUSNL)		
Connection name (CONNAME)		DNS(PORTA)
Convert message (CONVERT)	NO	NO
Description (DESCR)		padrão
Disconnect interval (DISCINT)	6000	0
Heartbeat interval (HBINT)	300	default
Long retry count (LONGRTY)	999999999	livre
Long retry interval (LONGTMR)	1200	livre
LU 6.2 mode name (MODENAME)		na
LU 6.2 transaction program name (TPNAME)		na
Maximum message length (MAXMSGL)	4Mb	4Mb
Maximum transmission size		na
Message channel agent name (MCANAME)		na

Message channel agent type (MCATYPE)	PROCESS	livre

Message channel agent user ident(MCAUSER)		livre
Message exit name (MSGEXIT)		livre
Message exit user data (MSGDATA)		livre
Message-retry exit name (MREXIT)		livre
Message-retry exit user data (MRDATA)		livre
Message retry count (MRRTY)	10	livre
Message retry interval (MRTMR)	1000	livre
Nonpersistent message speed (NPMSPEED)	FAST	na
Network-connection priority (NETPRTY)		na
Password (PASSWORD)		na
PUT authority (PUTAUT)	DEFAULT	
Queue manager name (QMNAME)		padrão
Receive exit name (RCVEXIT)		livre
Receive exit user data (RCVDATA)		livre
Security exit name (SCYEXIT)		Livre
Security exit user data (SCYDATA)		Livre
Send exit name (SENDEXIT)		Livre
Send exit user data (SENDDATA)		Livre
Sequence number wrap (SEQWRAP)	999.999.999	99.999.999
Sequential delivery		Livre
Short retry count (SHORTRTY)	10	Livre
Short retry interval (SHORTTMR)	60	Livre
Target system identifier		Livre
Transmission queue name (XMITQ)		Padrão
Transport type (TRPTYPE)		TCP

Tabela 8 - Atributos de Canais

* O valor do parâmetro *Batch size* (BATCHSZ) poderá ser definido entre 25 e 100, mediante acordo entre as partes.

5.6.7. Configuração do Servidor MQ - Opção ADOPTNEWMCA

Foi detectada uma limitação na configuração do MQ que, na ocorrência de falhas de comunicação, pode levar, eventualmente, a uma perda de conectividade entre servidores MQ, que só pode ser solucionada mediante comando STOP FORCE da conexão ou reinicialização do gerenciador de canais.

Para evitar tal falha, o suporte do fabricante do produto (IBM) recomendou a configuração de alguns parâmetros no MQ, com a utilização de atributos, que, por "default", não estão ativados.

Desta forma, considerando-se que tal alteração acarretará melhora na disponibilidade do serviço.

Seguem, abaixo, exemplos com os parâmetros a serem alterados no software, para os sistemas operacionais mais utilizados.

Esclarecemos que eventuais dúvidas acerca dos procedimentos envolvidos na alteração deverão ser sanadas diretamente junto ao suporte do fabricante do produto.

Opção ADOPTNEWMCA

ADOPTNEWMCA do MQ no ambiente Windows:

1. No servidor MQ, abrir MQ Services;
2. Clicar com o botão direito do mouse sobre o Qmgr a ser modificado;
3. Selecionar Properties;
4. Selecionar a pasta Channels;
5. Marcar a opção ALL do parâmetro AdoptNewMCA;
6. Marcar a opção ALL do parâmetro AdoptNewMCACheck;
7. Manter o tempo default dessa opção (60 segundos).

Ativação da opção ADOPTNEWMCA do MQ no ambiente Unix:

Incluir as linhas abaixo no arquivo de configuração do *queue manager* (qm.ini):

CHANNELS:

AdoptNewMCACheck=ALL

AdoptNewMCATimeout=60

AdoptNewMCA=ALL

Ativação da opção ADOPTNEWMCA do MQ no ambiente z/OS:

Incluir os parâmetros abaixo na macro CSQ6CHIP do módulo de parâmetros do channel-initiator:

ADOPTCHK=ALL

ADOPTMCA=YES

Observação: se o MQ for OS/390 V2R1, esses parâmetros são adicionados via PTF que deve ser solicitada ao fabricante.

6. CRIPTOGRAFIA E ASSINATURA DIGITAL

6.1. INTRODUÇÃO

Os requisitos de segurança descritos a seguir visam garantir a integridade, a confidencialidade, a disponibilidade e o não repúdio dos arquivos trafegados no âmbito do R2C3.

A definição dos requisitos de segurança exigidos foi baseada em padrões conhecidos, utilizados no mercado e já adotados no âmbito do SPB - “Manual de Segurança SFN”.

A Núclea procurou não eleger um produto/fornecedor que atenda às especificações de segurança, mas sim especificar os requisitos de segurança.

Os componentes de hardware e software necessários a atender os requisitos de segurança serão avaliados pelos próprios Participantes do R2C3.

Com isso, os Participantes podem avaliar o custo/benefício de desenvolvimento próprio ou das diversas soluções de fornecedores de hardware e software de segurança presentes no mercado e possivelmente utilizar as mesmas soluções já em utilização no SPB.

Os ambientes de testes e produção deverão ser distintos. Primeiramente as transferências de arquivo deverão ser homologadas no ambiente de testes, para posteriormente serem disponibilizadas no ambiente de produção.

a. Premissas:

i. A assinatura digital e criptografia nos arquivos e mensagens do R2C3 adotarão especificações de segurança contidas no Manual de Segurança da RSFN (chaves assimétricas)

ii. Os arquivos e mensagens transmitidos entre os Participantes do R2C3 a Núclea são irrevogáveis, incondicionais e finais;

iii. Os arquivos e mensagens serão obrigatoriamente assinadas digitalmente pelo Participante emissor, com exceção, caso julgado necessário, dos relativos a testes de conectividade;

iv. Todas as transferências de informação serão obrigatoriamente criptografadas com exceção dos relativos a testes de conectividade e a comunicação de erros de segurança.

v. Todos os arquivos e mensagens devem possuir uma identificação única garantindo sua rastreabilidade e unicidade de processamento; e

vi. Todo e qualquer arquivo e mensagem gerada e enviada ao R2C3 por um de seus Participantes é de exclusiva responsabilidade de quem o originou.

b. Diretrizes:

i. A Núclea utilizará no R2C3, certificado digital específico para este sistema conforme as especificações descritas no item 6.2.

ii. A Núclea utilizará o certificado digital, respeitando a segregação entre os ambientes de produção e homologação;

iii. Para os Participantes que são usuários de outros sistemas da Núclea na Financial Net (RTM), será permitida a utilização, em ambiente de Homologação e Produção, dos mesmos certificados digitais utilizados neste sistema. Para os demais participantes será necessária a utilização de certificado digital específico para o R2C3;

iv. O participante pode optar em utilizar diferentes certificados ICP Brasil para utilização via mensageria, por API (assinatura do payload) e ou arquivaria;

v. O participante deverá informar no Termo de Adesão, os dados dos certificados digitais utilizados em cada canal;

vi. É da responsabilidade do participante comunicar a Núclea que um certificado digital está sendo compartilhado em vários sistemas da Núclea, no momento de adesão e no período de troca dele.

vii. Os Certificados Digitais são do tipo A1 (01 ano de validade) e deverão ser emitidos por uma Autoridade Certificadora que atenda aos requisitos estabelecidos pela legislação vigente e que seja devidamente credenciada para tal pelo Comitê Gestor da infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

viii. Quando não for utilizado certificado digital emitido por autoridade certificadora credenciada pela ICP-Brasil, a Núclea e o participante devem estabelecer formalmente no termo de adesão acordo de uso de outros certificados digitais conforme disposto na MP 2.200 de 2001, Art 12. Parágrafo 2º.

ix. Os Participantes serão responsáveis pela segurança física e lógica de acesso a sua chave privada.

x. Os Participantes deverão criar e manter registros (logs) que capacitem a rastreabilidade e/ou a recomposição das transmissões de arquivos geradas no R2C3, garantindo assim sua auditabilidade.

xi. No Ambiente de Homologação, durante o processo de adesão, fica a critério do Participante optar em utilizar o primeiro certificado digital auto assinado, mantendo-se as especificações e sequenciais (tamanho da chave, algoritmos de criptografia e assinatura, validade de 365 dias e campos).

xii. O certificado digital auto assinado deverá ser trocado, no ambiente de HOMOLOGAÇÂO, por um novo certificado digital ICP-Brasil, testado com o envio de um arquivo, antes do início das operações do participante no ambiente de PRODUÇÃO.

xiii. O sistema do R2C3, tanto em homologação como em produção, adotará para arquivos apenas o cabeçalho de segurança versão 3 (Header v3) e certificados digitais com chaves criptográficas de 2048 bits. (vide item 6.4.1). Já para a API, adotará o padrão JWS, conforme detalhado no item 6.9.2.

xiv. Os ambientes de testes e produção deverão ser distintos. Primeiramente, o acesso deverá ser comprovado no ambiente de homologação, para posteriormente ser utilizados no ambiente de produção.

6.2. ESPECIFICAÇÕES PARA A GERAÇÃO DE CERTIFICADOS DIGITAIS TIPO ICP-BRASIL

i. Campos obrigatórios a serem incluídos no CSR:

CN= O common name é composto pelo host+domínio internet registrado pela IF. No exemplo:

srv01.if.com.br, o "srv01 é o host, "if.com.br" é o domínio

OU= Nome da Instituição

OU=cccccccc (onde cccccccc é o número base do CNPJ)

OU= RRC Pxxx ou Txxx

O=ICP-Brasil (campo preenchido automaticamente pela AC emissora do certificado digital)

C=BR (campo preenchido automaticamente pela AC emissora do certificado digital)

ii. Os certificados digitais emitidos para os ambientes serão identificados pelo conteúdo do campo "OU"=RRC seguido de um espaço em branco (“ “), acrescido da seqüência "Xnnn", onde "X" identifica o ambiente (produção=P e homologação=T), e "nnn" é uma numeração seqüencial única de geração do par de chaves, em cada ambiente (produção ou homologação), dentro da instituição.

Caso um certificado digital seja identificado para um ambiente (produção ou homologação), o seu par de chaves correspondente não poderá ser usado no outro;

iii. Poderão ser utilizados opcionalmente os campos "L" (localidade) e/ou "S" (estado);

iv. É vedado o uso do valor 3 (três) como expoente da chave pública gerada para o certificado digital.

v. O bit mais significativo (MSB) da chave pública deverá necessariamente ter valor igual a 1 (um).

vi. É vedado o reuso das chaves públicas utilizadas. Ao solicitar a emissão de um novo certificado digital para uso no R2C3, é imperativo gerar uma nova chave pública. Certificados digitais emitidos para ambientes diferentes (produção e homologação) devem conter chaves públicas diferentes.

vii. É vedado o reuso, para qualquer finalidade, de CSRs utilizados para a solicitação de certificados digitais a serem utilizados no âmbito da R2C3.

viii. A Núclea cadastrará o certificado informado para todos os canais aderidos pelo Participante; exceções a esta regra deverão ser informadas no Cadastro Técnico.

6.3. EXEMPLOS ILUSTRATIVOS DE PREENCHIMENTO DE CSR'S

i. No caso do primeiro certificado digital de produção da Núclea (SP):

CN= RRC_p001.cip-bancos.org.br

OU= Camara Interbancaria de Pagamentos – CIP

OU=29011780

OU= RRC P001

L=Sao Paulo

S=SP

O=ICP-Brasil

C=BR

ii. No caso do segundo certificado digital de homologação para um hipotético Banco XYZ:

CN= srv01.bancoxyz.com.br

OU= Banco XYZ S.A.

OU=31123578 (supondo o número base do CNPJ ser 31123578)

OU=SCG T002

L=Sao Paulo

S=Sao Paulo

O=ICP-Brasil

C=BR

(Obs: Não deve ser usado caractere acentuado para atender ao disposto no item 7.1.5 da resolução nº 41 do Comitê Gestor da ICP-Brasil)

6.4. PROCESSO DE OBTENÇÃO E HABILITAÇÃO DE CERTIFICADOS DIGITAIS

I. Participante, seguindo a orientação dos procedimentos de seu software específico de segurança, gera par de chaves assimétricas RSA-2048 bits e um arquivo CSR, no padrão PKCS#10;

II. A solicitação para a emissão de certificado digital é feita diretamente a uma Autoridade Certificadora, que deve ser consultada previamente para orientar o correto tipo de produto a ser adquirido e que atenda as especificações do R2C3;

III. A AC atua como Autoridade Registradora e verifica os dados da solicitação e do preposto da instituição;

IV. A AC, uma vez validados os dados, emite o certificado digital e envia este à solicitante, sob a forma de arquivo no padrão ASN.1;

V. Participante envia a Núclea, por e-mail, o certificado digital tipo servidor ICP-Brasil (chave pública).

VI. A Núclea verificará a duplicidade da chave pública e a consistência dos dados registrados e responderá por e-mail a instituição a habilitação do certificado digital;

VII. Cada Instituição terá apenas um certificado digital ativo por canal de comunicação em cada ambiente de produção ou homologação; e

VIII. Cada certificado digital deverá estar associado a um par de chaves únicas.

6.5. PROCESSO DE ATIVAÇÃO, SUBSTITUIÇÃO E REVOGAÇÃO DE CERTIFICADOS DIGITAIS

I. Os certificados digitais habilitados, na forma do item 6.2, estarão disponíveis para uso, que poderá ser inicial, no caso do primeiro certificado digital, ou de substituição, pelo encerramento da validade ou revogação de um certificado digital sendo utilizado;

II. Para ativar certificados digitais, tanto inicialmente como por substituição, a instituição emitirá mensagem por e-mail a Núclea com no mínimo 10 dias úteis de antecedência da data pretendida para a ativação ou substituição. Esta mensagem deverá conter os dados do canal de comunicação (Arquivos e/ou Webservices), as informações do certificado digital atual, do certificado digital a ser substituído, a previsão de data, hora, correspondente chave pública do certificado digital que será ativado e o nº de série do certificado digital que será desativado.

III. Recomendamos que os certificados digitais substituídos sejam revogados pelo Participante junto à AC, não podendo mais serem utilizadas as chaves a eles correlacionadas;

IV. As ativações ou substituições de certificados digitais deverão ser efetivadas em data e horário que minimizem qualquer impacto operacional;

V. Somente nos casos de revogação por contingência ou suspeita de violação de segurança é que poderão ser enviadas e processadas substituições de certificado digital fora do período preferencial;

VI. A substituição dos certificados digitais da Núclea, quando do seu vencimento anual, em qualquer ambiente (produção ou homologação), será previamente comunicada aos participantes por e-mail ou INFO-NÚCLEA, com antecedência de pelo menos 10 dias úteis em relação à data estabelecida para a substituição, a qual coincidirá preferencialmente com uma sexta-feira ou com dia útil anterior a um feriado.

VII. Para a habilitação do primeiro certificado digital em um determinado canal de comunicação no ambiente de produção, o Participante já deverá ter ativado pelo menos um certificado digital no mesmo canal de comunicação no ambiente de homologação;

VIII. A ativação de um novo certificado digital pelo Participante automaticamente substituirá o anterior o qual não poderá mais ser usado.

IX. Todo certificado digital para uso no âmbito do R2C3 não será aceito nas 24 (vinte e quatro) horas do dia anterior à data especificada em seu campo "Válido Até". Por exemplo, um certificado digital que tenha os dados "07/01/2020 15:34:06" em seu campo "Válido Até", não será aceito à partir do dia "06/01/2020 15:34:06".

6.6. ESPECIFICAÇÃO PARA A SEGURANÇA DOS ARQUIVOS E MENSAGENS

I. Cabeçalho ("header") de segurança dos Arquivos

Todos os arquivos e mensagens trocados no âmbito do R2C3 devem iniciar com uma sequência de 588 bytes - o cabeçalho de segurança, responsável pela implementação dos mecanismos de assinatura e criptografia deles.

A seguir são enumerados e codificados os campos do cabeçalho, com a sua respectiva localização, descrição e forma de preenchimento:

Campo	Posição	Descrição do Campo	Conteúdos Possíveis
C01	001-002	Tamanho total do Cabeçalho	024CH: Fixo na segunda versão (588 bytes)
C02	003-003	Versão do protocolo	00H: Em claro, 02H: Segunda versão
C03	004-004	Código de erro	Vide tabela de erros no item .0
C04	005-005	Indicação de tratamento especial	Vide item 5.0
C05	006-006	Reservado para uso futuro	00H
C06	007-007	Algoritmo da chave assimétrica do destino	01H: RSA com 1024 bits

			02H: RSA com 2048 bits
C07	008-008	Algoritmo da chave simétrica	01H: Triple-DES com 168 bits (3 x 56 bits) (Vide 3.6.4)
C08	009-009	Algoritmo da chave assimétrica local da assinatura	01H: RSA com 1024 bits 02H: RSA com 2048 bits
C09	010-010	Algoritmo de "hash"	02H: SHA-1 03H: SHA-256
C10	011-011	AC do certificado do destino	Ex. 01H: Serpro 02H: Certisign,03H: Pessoas Físicas, 04H:Serasa, 05H:CAIXA,06H:Valid,07H: Imprensa Oficial,08H: Boa Vista
C11	012-043	Série do certificado do destino	Identificador único do certificado na AC (Vide 3.6.5)
C12	044-044	AC do certificado da assinatura	Ex. 01H: Serpro 02H: Certisign,03H: Pessoas Físicas, 04H:Serasa, 05H:CAIXA,06H:Valid,07H: Imprensa Oficial,08H: Boa Vista
C13	045-076	Série do certificado da assinatura	Identificador único do certificado na AC (Vide 3.6.5)
C14	077-332	Buffer de criptografia da chave simétrica	Chave 3DES (24 bytes) cifrada por PKCS#1v1_5
C15	333-588	Buffer do criptograma de assinatura da mensagem	Hash (20 ou 32 bytes) assinado pelo PKCS#1v1_5

II. As posições 077-332 e 333-588 são cifradas respectivamente com a chave pública do destinatário e a chave privada do emitente, de acordo com as primitivas do PKCS#1 "RSAES-PKCS1-V1_5-ENCRYPT" e "RSASSA-PKCS1-V1_5-SIGN".

III. Algoritmo simétrico 3DES tipo EDE (Encrypt-Decrypt-Encrypt) com 3 chaves independentes (k1,k2,k3) e modo CBC (Cipher Block Chaining), sendo o Vetor de Inicialização (IV - Initialization Vector) os 64 bits (8 bytes) iniciais da Chave Simétrica.

IV. A Chave DES consiste de 64 bits binários (= 8 bytes), dos quais 8 bits (=1byte) são utilizados para verificação de paridade impar, sendo assim o tamanho efetivo da chave é de 56 bits (=7 bytes). Na implementação TripleDES (3DES), são utilizadas 3 chaves DES.

V. A identificação dos certificados digitais é feita por um campo binário (código da AC) e outro com a representação em ASCII do número de série, alinhado à direita, com zeros à esquerda. Assim, se o certificado digital tiver o número de série exibido pelo browser de certificados digitais como "5D77 DA7B 6F02 EFA1 EDDA 741E 78FF 3508", ele deve ser representado como "5D77DA7B6F02EFA1EDDA741E78FF3508", onde cada byte pode apresentar a configuração 0x30 a 0x39 ou 0x41 a 0x46. Se ao contrário for exibido apenas "3B3B C056", será representado por "00000000000000000000000003B3BC056".

VI. Para arquivos com campos C06/C08 configurados com o valor 01H (RSA 1024 bits), deve-se preencher os últimos 1204 bits dos campos C14/C15 com o valor 0.

VII. O algoritmo de hash SHA-1 não pode ser utilizado em criptogramas de autenticação gerados com chaves de 2048 bits. Nesse caso, deve-se utilizar o algoritmo de hash SHA-

Referências:

RSA (ANSI X9.31);

Triple-DES (ANSI X9.52, FIPS 46-3);

MD5, SHA-1 (FIPS 180-1);

CBC (FIPS-81);

Certificado Digital (X.509 v3);

6.7. AGREGAÇÃO DE SEGURANÇA NOS ARQUIVOS E MENSAGENS

i. cabeçalho de segurança não tem código de página, é sempre binário;

ii. O arquivo que sucede os 558 bytes do cabeçalho deve ser apresentado no formato GZIP.

iii. Devido à utilização do algoritmo 3DES, o tamanho do arquivo deve ser tornado múltiplo de 8 bytes, adotando-se, caso necessário, um "padding" de zeros binários;

iv. Calcula-se o "hash", para efeito de assinatura, do arquivo compactado e com "padding", indicando o algoritmo utilizado (campo C09);

v. Indicam-se os códigos de AC e números de série dos certificados digitais do destinatário e do emissor (campo C10 a C13);

vi. O número do certificado digital deve ser ASCII com zeros (0x30) à esquerda, caso necessário (vide item 3.6.5);

vii. Assina-se o arquivo (anotando o resultado do "hash" do arquivo compactado, com o padding) com a chave privada correspondente ao certificado digital do participante emissor, anotando o resultado no campo C15;

viii. Sorteia-se chave simétrica (Triple-DES 192 bits) e cifra-se a mensagem que foi objeto de assinatura;

ix. Cifra-se a chave simétrica (24 bytes) utilizada na cifragem do arquivo com a chave pública correspondente ao certificado digital do destinatário, com o resultado no campo C14;

x. O campo C04 do cabeçalho normalmente será preenchido com zeros binários, indicando tratar-se de uma mensagem assinada e cifrada.

xi. Excepcionalmente nas condições abaixo, poderá assumir os seguintes valores:

xii. “6” - Indicativo de arquivo não compactado, sem cifragem, normalmente de uso público;

xiii. “8” - Indicativo de arquivo ou mensagem compactado;

xiv. “10” - Indicativo de arquivo compactado, sem cifragem, normalmente de uso público;

xv. Arquivos públicos são somente assinados (campo C04 = 6 ou 10);

xvi. No caso de arquivos compactados deve ser usado o formato GZIP.

xvii. Para a assinatura o tamanho do arquivo compactado deverá ser transformado em múltiplo de 08 bytes pelo uso de “padding” de zeros binários, caso necessário, conforme itens 3.7.3 e 3.7.4. Mesmo após a decifragem (se for o caso) e conferência da assinatura o “padding” não deverá ser removido;

6.8. VERIFICAÇÃO DA SEGURANÇA PARA A RECEPÇÃO DE ARQUIVOS E MENSAGENS

i. Verificam-se os certificados digitais envolvidos (se existem e estão habilitados), conferindo se correspondem ao receptor (campos C10/C11) e emissor do arquivo (campos C12/C13);

ii. Abre-se a informação da chave simétrica de cifragem do arquivo com a chave privada correspondente à chave pública do certificado digital;

iii. Decifra-se a parte XML da do arquivo (a partir da posição 589), inclusive o "padding";

iv. Calcula-se o "hash" do arquivo compactado com o "padding", de acordo com o algoritmo indicado em C09;

v. Confere-se a assinatura do arquivo, comparando o "hash" obtido;

vi. Se houver qualquer erro no decorrer do processo, deve ser gerado um log, reportando o código de erro (EGEN99xx);

6.9. ESPECIFICAÇÃO PARA SEGURANÇA PARA INTEGRAÇÃO VIA API

- **Criptografia na Transmissão**

i. A comunicação se dará apenas utilizando o protocolo TLS 1.2 ou mais recente, os serviços não possuem compatibilidade com versões anteriores do TLS ou mesmo SSL
ii. As APIs implementam somente serviços HTTPS.
iii. Características do Certificado Digital:

a. O Participante, seguindo a orientação dos procedimentos de seu software específico de segurança, gera par de chaves assimétricas RSA-2048 bits e um arquivo CSR, no padrão PKCS#10;
b. Para comunicação TLS deve utlizar um certificado digital emitido por uma Autoridade Certificadora emissora de certificados do tipo SSL.
c. A AC atua como Autoridade de Registro e verifica os dados da solicitação e do preposto da instituição.;
d. A AC, uma vez validados os dados, emite o certificado digital e envia este à solicitante, sob a forma de arquivo no padrão ASN.1
e. A comunicação não será estabelecida com um certificado digital auto assinado;
f. Para as requisições feitas pela Núclea para os participantes (Notificações e Callbacks), será considerado as Autoridades Certificadoras (CA´s) que estão presentes no JDK 11.0.5. Abaixo a lista de Common Name (CN) das certificadoras atualmente validas para a versão do JDK citado anteriormente:

- QuoVadis Root CA 1 G3
- DigiCert Assured ID Root CA
- Thawte Premium Server CA
- TeliaSonera Root CA v1
- Thawte Premium Server CA
- Thawte Server CA
- Equifax Secure eBusiness CA-1
- DigiCert Assured ID Root G2
- GDCA TrustAUTH R5 ROOT
- Amazon Root CA 2
- Amazon Root CA 1
- GeoTrust Universal CA
- EE Certification Centre Root CA
- thawte Primary Root CA - G3
- Certigna, O=Dhimyotis
- Class 2 Primary CA
- SZAFIR ROOT CA2
- Certum Trusted Network CA 2

- QuoVadis Root CA 3
- Starfield Services Root Certificate Authority - G2
- QuoVadis Root CA 2
- TrustCor ECA-1
- SecureSign RootCA11
- AffirmTrust Premium
- COMODO RSA Certification Authority
- NetLock Uzleti (Class B) Tanusitvanykiado
- GeoTrust Primary Certification Authority - G3
- Buypass Class 3 Root CA, O=Buypass AS-983163327
- http://www.valicert.com/
- Chambers of Commerce Root - 2008
- OpenTrust Root CA G2
- DigiCert High Assurance EV Root CA
- OpenTrust Root CA G1
- Equifax Secure Global eBusiness CA-1
- Autoridad de Certificacion Firmaprofesional CIF A62634068
- Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc."
- E-Tugra Certification Authority
- EC-ACC
- Actalis Authentication Root CA
- TrustCor RootCert CA-2
- Buypass Class 2 Root CA
- TrustCor RootCert CA-1
- T-TeleSec GlobalRoot Class 3
- T-TeleSec GlobalRoot Class 2
- Global Chambersign Root - 2008
- Certinomis - Root CA
- Baltimore CyberTrust Root
- Atos TrustedRoot 2011
- Microsec e-Szigno Root CA 2009
- Entrust.net Secure Server Certification Authority
- Staat der Nederlanden Root CA - G3
- LuxTrust Global Root 2
- DST Root CA X3
- Staat der Nederlanden Root CA - G2
- Visa eCommerce Root
- NetLock Arany (Class Gold) Főtanúsítvány
- AffirmTrust Commercial
- CFCA EV ROOT
- GeoTrust Primary Certification Authority
- GeoTrust Universal CA 2
- GlobalSign
- NetLock Expressz (Class C) Tanusitvanykiado
- VeriSign Class 3 Public Primary Certification Authority - G3
- OISTE WISeKey Global Root GA CA
- OISTE WISeKey Global Root GB CA
- Certum Trusted Network CA
- IdenTrust Public Sector Root CA 1
- USERTrust RSA Certification Authority
- Staat der Nederlanden EV Root CA
- XRamp Global Certification Authority

- GTE CyberTrust Global Root
- DigiCert Trusted Root G4
- GlobalSign
- Hongkong Post Root CA 1
- DigiCert Global Root CA
- D-TRUST Root Class 3 CA 2 2009
- GlobalSign Root CA, OU=Root CA
- GeoTrust Global CA
- Sonera Class2 CA
- DigiCert Global Root G2
- TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1
- thawte Primary Root CA
- AffirmTrust Networking
- TWCA Global Root CA
- Starfield Root Certificate Authority - G2
- VeriSign Universal Root Certification Authority
- TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H5
- ISRG Root X1
- http://www.valicert.com/
- AAA Certificate Services
- Network Solutions Certificate Authority
- IdenTrust Commercial Root CA 1
- AddTrust External CA Root
- Izenpe.com
- CA Disig Root R2
- SecureTrust CA
- SSL.com EV Root Certification Authority RSA R2
- VeriSign Class 3 Public Primary Certification Authority - G5
- SSL.com Root Certification Authority RSA
- TWCA Root Certification Authority
- Entrust.net Certification Authority (2048)
- Certplus Root CA G1
- SwissSign Silver CA - G2
- ACCVRAIZ1
- http://www.valicert.com/
- QuoVadis Root Certification Authority
- Cybertrust Global Root
- D-TRUST Root Class 3 CA 2 EV 2009
- COMODO Certification Authority
- Hellenic Academic and Research Institutions RootCA 2015
- Hellenic Academic and Research Institutions RootCA 2011
- Secure Global CA, O=SecureTrust Corporation, C=US
- Entrust Root Certification Authority - G2
- QuoVadis Root CA 3 G3
- Deutsche Telekom Root CA 2
- SwissSign Gold CA - G2
- QuoVadis Root CA 2 G3
- Go Daddy Root Certificate Authority - G2

Abaixo a lista de Organization Unit (OU) das certificadoras atualmente validas para a versão do JDK citado anteriormente:

- Trustis FPS Root CA

- certSIGN ROOT CA
- Security Communication RootCA1
- Go Daddy Class 2 Certification Authority
- Equifax Secure Certificate Authority
- Class 3 Public Primary Certification Authority
- ePKI Root Certification Authority
- VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only, Class 3 Public Primary Certification Authority - G2
- Starfield Class 2 Certification Authority
- Class 3 Public Primary Certification Authority
- Security Communication RootCA2
- AC RAIZ FNMT-RCM
- Government Root Certification Authority

- **Assinatura da Requisição**

i. O padrão da assinatura digital para API REST é o JWS (JSON Web Signature).
ii. A assinatura digital deverá ser realizada com RSASSA-PKCS1-v1_5 SHA-256
iii. O JWS deve ser representado no modo compacto e separado (detached). Referência: https://tools.ietf.org/html/rfc7515 (apêndice F)
iv. O header JOSE deverá conter campos públicos e alguns privados:

a. x5t#S256 (campo público correspondente ao thumbprint sha256 em base64url do certificado digital utilizado para assinar a mensagem)
b. kid (campo público contendo o serial id (em hexadecimal) do requisitante com zeros a esquerda; por exemplo: 0000DA7B6F02EFA1EDDA741E78FF3508). 32 caracteres em maiúsculo
c. alg (campo público contendo o valor RS256)
d. http://www.cip-bancos.org.br/identificador-requisicao (campo privado contendo uma identificação única da requisição com até 40 caracteres). Esta identificação deve ser única para o emissor e a data informados.
e. http://www.cip-bancos.org.br/identificador-requisicao-relacionada (campo privado contendo uma identificação única da requisição relacionada, este campo será preenchido pela Núclea quando realizar requisições para os participantes quando relacionadas à uma requisição anterior recebida pela Núclea, o campo terá o tamanho de até 40 caracteres). Campo não obrigatório.
f. http://www.cip-bancos.org.br/data-referencia (campo privado contendo a data de referência da requisição)
g. http://www.cip-bancos.org.br/identificador-emissor-principal (campo privado contendo o identificador do emissor principal da requisição)
h. http://www.cip-bancos.org.br/identificador-emissor-administrado (campo privado contendo o identificador do emissor administrado da requisição)
i. http://www.cip-bancos.org.br/identificador-emissor-principal-relacionado (campo privado contendo a identificação do emissor principal da requisição que originou esta resposta, este campo será preenchido pela Núclea quando realizar requisições para os participantes quando

relacionadas à uma requisição anterior recebida pela Núclea, o campo terá o tamanho de até 8 caracteres). Campo não obrigatório.

j. http://www.cip-bancos.org.br/identificador-emissor-administrado-relacionado (campo privado contendo a identificação do emissor administrado da requisição que originou esta resposta, este campo será preenchido pela Núclea quando realizar requisições para os participantes quando relacionadas à uma requisição anterior recebida pela Núclea, o campo terá o tamanho de até 8 caracteres). Campo não obrigatório.

k. Definição do header JOSE para uma requisição (Participante -> Núclea):

```
JOSEHeaderRequisicao:
      required:
      - alg
      - x5t#S256
      - kid
      - "http://www.cip-bancos.org.br/identificador-requisicao"
      - "http://www.cip-bancos.org.br/data-referencia"
      -          "http://www.cip-bancos.org.br/identificador-emissor-
principal"
      -          "http://www.cip-bancos.org.br/identificador-emissor-
administrado"
      type: object
      properties:
        alg:
          type: string
          description: Algoritmo assinatura
          enum: [RS256]
        x5t#S256:
          type: string
          description: Impressão digital sha256 do certificado em
base64url
          pattern: ^[0-9A-F]+$
          maxLength: 64
        kid:
          type: string
          description: Número de série (em hexadecimal e com zeros a
esquerda) do certificado
          pattern: ^[0-9A-F]{32}$
        "http://www.cip-bancos.org.br/identificador-requisicao":
          type: string
          description: Identificação única da requisição para o
emissor e data de referência
          minLength: 1
          maxLength: 40
        "http://www.cip-bancos.org.br/data-referencia":
          type: string
          description: Data de referência da requisição
          format: date
        "http://www.cip-bancos.org.br/identificador-emissor-
principal":
          type: string
          description: Identificação do emissor principal da
requisição
          pattern: ^\d{8}$
        "http://www.cip-bancos.org.br/identificador-emissor-
administrado":
          type: string
          description: Identificação do emissor administrado da
requisição
          pattern: ^\d{8}$
```

Definição do header JOSE para uma resposta síncrona (Núclea -> Participante):

```
JOSEHeaderRespostaSincrona:
      required:
      - alg
      - x5t#S256
      - kid
      - "http://www.cip-bancos.org.br/identificador-requisicao"
      - "http://www.cip-bancos.org.br/data-referencia"
      -          "http://www.cip-bancos.org.br/identificador-emissor-
principal"
      -          "http://www.cip-bancos.org.br/identificador-emissor-
administrado"
      type: object
      properties:
        alg:
          type: string
          description: Algoritmo assinatura
          enum: [RS256]
        x5t#S256:
          type: string
          description:  Impressão  digital  sha256  do  certificado  em
base64url
          pattern: ^[0-9A-F]+$
          maxLength: 64
        kid:
          type: string
          description: Número de série (em hexadecimal e com zeros a
esquerda) do certificado
          pattern: ^[0-9A-F]{32}$
        "http://www.cip-bancos.org.br/identificador-requisicao":
          type: string
          description:  Identificação  única  da  requisição  para  o
emissor e data de referência
          minLength: 1
          maxLength: 40
        "http://www.cip-bancos.org.br/data-referencia":
          type: string
          description: Data de referência do sistema
          format: date
        "http://www.cip-bancos.org.br/identificador-emissor-
principal":
          type: string
          description: Identificação do emissor principal da resposta
(CIP)
          pattern: ^\d{8}$
        "http://www.cip-bancos.org.br/identificador-emissor-
administrado":
          type: string
          description:  Identificação  do  emissor  administrado  da
resposta (CIP)
          pattern: ^\d{8}$
```

Definição do header JOSE para uma resposta assíncrona (Núclea -> Participante):

```
JOSEHeaderRespostaSincrona:
      required:
      - alg
      - x5t#S256
      - kid
      - "http://www.cip-bancos.org.br/identificador-requisicao"
      - "http://www.cip-bancos.org.br/data-referencia"
```

```
      -         "http://www.cip-bancos.org.br/identificador-emissor-
principal"
      -         "http://www.cip-bancos.org.br/identificador-emissor-
administrado"
      type: object
      properties:
        alg:
          type: string
          description: Algoritmo assinatura
          enum: [RS256]
        x5t#S256:
          type: string
          description: Impressão digital sha256 do certificado em
base64url
          pattern: ^[0-9A-F]+$
          maxLength: 64
        kid:
          type: string
          description: Número de série (em hexadecimal e com zeros a
esquerda) do certificado
          pattern: ^[0-9A-F]{32}$
        "http://www.cip-bancos.org.br/identificador-requisicao":
          type: string
          description: Identificação única da requisição para o
emissor e data de referência
          minLength: 1
          maxLength: 40
        "http://www.cip-bancos.org.br/data-referencia":
          type: string
          description: Data de referência do sistema
          format: date
        "http://www.cip-bancos.org.br/identificador-emissor-
principal":
          type: string
          description: Identificação do emissor principal da resposta
(CIP)
          pattern: ^\d{8}$
        "http://www.cip-bancos.org.br/identificador-emissor-
administrado":
          type: string
          description: Identificação do emissor administrado da
resposta (CIP)
          pattern: ^\d{8}$
```

Definição do header JOSE para uma resposta assíncrona (Núclea -> Participante):

```
JOSEHeaderRespostaAssincrona:
      required:
      - alg
      - x5t#S256
      - kid
      - "http://www.cip-bancos.org.br/identificador-requisicao"
      -       "http://www.cip-bancos.org.br/identificador-requisicao-
relacionada"
      - "http://www.cip-bancos.org.br/data-referencia"
      -         "http://www.cip-bancos.org.br/identificador-emissor-
principal"
      -         "http://www.cip-bancos.org.br/identificador-emissor-
principal-relacionado"
      -         "http://www.cip-bancos.org.br/identificador-emissor-
administrado"
      -         "http://www.cip-bancos.org.br/identificador-emissor-
administrado-relacionado"
      type: object
      properties:
```

```
        alg:
          type: string
          description: Algoritmo assinatura
          enum: [RS256]
        x5t#S256:
          type: string
          description: Impressão digital sha256 do certificado em
base64url
          pattern: ^[0-9A-F]+$
          maxLength: 64
        kid:
          type: string
          description: Número de série (em hexadecimal e com zeros a
esquerda) do certificado
          pattern: ^[0-9A-F]{32}$
        "http://www.cip-bancos.org.br/identificador-requisicao":
          type: string
          description: Identificação única da requisição para o
emissor e data de referência
          minLength: 1
          maxLength: 40
        "http://www.cip-bancos.org.br/identificador-requisicao-
relacionada":
          type: string
          description: Identificação da requisição recebida que
originou esta resposta
          minLength: 1
          maxLength: 40
        "http://www.cip-bancos.org.br/data-referencia":
          type: string
          description: Data de referência do sistema
          format: date
        "http://www.cip-bancos.org.br/identificador-emissor-
principal":
          type: string
          description: Identificação do emissor principal da resposta
(CIP)
          pattern: ^\d{8}$
        "http://www.cip-bancos.org.br/identificador-emissor-
principal-relacionado":
          type: string
          description: Identificação do emissor principal da
requisição recebida que originou esta resposta
          pattern: ^\d{8}$
        "http://www.cip-bancos.org.br/identificador-emissor-
administrado":
          type: string
          description: Identificação do emissor administrado da
resposta (CIP)
          pattern: ^\d{8}$
        "http://www.cip-bancos.org.br/identificador-emissor-
administrado-relacionado":
          type: string
          description: Identificação do emissor administrado da
requisição recebida que originou esta resposta
          pattern: ^\d{8}$
```

exemplo de header JOSE (requisição):

```
{
 "alg": "RS256",
 "x5t#S256": "cTqF4v3fi9iBp2_S4pvJKDbYrlI_mQgivtJIUYN8NUM",
```

"kid": "7269940957DA319805FF0B4A139B956A ",
"http://www.cip-bancos.org.br/identificador-requisicao":
"12345678111111111234567",
"http://www.cip-bancos.org.br/data-referencia": "2020-02-20",
"http://www.cip-bancos.org.br/identificador-emissor-principal": "12345678",
"http://www.cip-bancos.org.br/identificador-emissor-administrado":
"87654321"
}

A requisição HTTP deverá conter o seguinte header:

a. x-jws-signature (campo contendo a serialização compacta e separada do JWS token; por exemplo:

ewogICJhbGciOiAiUlMyNTYiLAogICJ4NXQjUzI1NiI6ICI4OEZGODQ2M0Y4NUZDRUYxQjQ2QUY1RkVGRjQ2N0JFMzUxRTUyOTQyQkQ0Rjc1M0UzQ0Y5NDY2MjA4ODYwRDE1IiwKICAia2lkIjogIjcyNjk5NDA5NTdkYTMxOTgwNWZmMGI0YTEzOWI5NTZhNmIwY2UxM2QiLAogICJodHRwOi8vd3d3LmNpcC1iYW5jb3Mub3JnLmJyL2lkZW50aWZpY2Fkb3ItcmVxdWlzaWNhbyI6ICIxMjM0NTY3ODExMTExMTExMTIzNDU2NyIsCiAgImh0dHA6Ly93d3cuY2lwLWJhbmNvcy5vcmcuYnIvaWRlbnRpZmljYWRvci1lZmV0aXZvLWVtaXNzb3ItcHJpbmNpcGFsIjogIjEyMzQ1Njc4MTExMTExMTExMjM0NTY2IiwKICAiaHR0cDovL3d3dy5jaXAtYmFuY29zLm9yZy5ici9kYXRhLXJlZmVyZW5jaWEiOiAiMjAyMC0wMi0yMCIsCiAgImh0dHA6Ly93d3cuY2lwLWJhbmNvcy5vcmcuYnIvaWRlbnRpZmljYWRvci1lbWlzc29yLXBhcCI6ICIxMjM0NTY3OCIsCiAgImh0dHA6Ly93d3cuY2lwLWJhbmNvcy5vcmcuYnIvaWRlbnRpZmljYWRvci1lbWlzc29yLWFkbWluaXN0cmFkbyI6ICI4NzY1NDMyMSIKfQ..RVfMCxt3cuuThXcQaYUYxXW3g-
2yUHvWY6HkDPs3gaa_lkukeBNwY91anGAIhm2bUmyKihfUXuU2sIBNXAUL107_3o_z9b0Y5go1xDUmd8OkWvGq31vhg2eG9GkaOkUImelvvRX4X8fGTbWsf98ZRBLJojxdxZdOQ6R9z0vV1XrMaIRA1-
j2QntEtn_zJB723_LXYHzNhgEs4RiW1pM1nmp98mKX9CfT1jNDoZrcf0T-
mOqQ44NmGFdvwnkUDcdZlk3wG4TtbPR6hs-
FoVhVQBFiAuX4hdfE6Ae5JdTNp3ofmmZDdMFYzkiJ9lrvBWHGHJf_MDSEmHnfy8egzHMICQ

Todas as requisões deverão ser assinadas, por este motivo não será utilizado nenhum outro método de autenticação (basic-authentication, api key, oauth2 (client-credentials)) e também não será utilizado nenhum token de sessão (oauth2).

Segue uma breve descrição para geração da assinatura:

- **a.** Obter a chave privada do certificado
- **b.** Criar o JOSE Header (item iv.)
- **c.** Criar uma string da seguinte forma: BASE64URL(UTF8(JOSE Header)) + "." + BASE64URL(UTF8(HTTP Payload))
- **d.** Calcular a assinatura da string gerada no passo anterior
- **e.** Criar o http header x-jws-signature com o valor: BASE64URL(UTF8(JOSE Header)) + "." + "." + BASE64URL(assinatura calculada no passo anterior)

Qualquer requisição de "callback" originada pela Núclea também conterá uma assinatura digital conforme os itens anteriores (apenas ressaltando que nestes casos a assinatura utilizará o certificado da Núclea).

Observação: apesar da assinatura descrita poder ser executada em qualquer tipo de payload do body do HTTP, todos os payloads estarão com o conteúdo em JSON.

6.9.1. CONTROLE DE ACESSO

Serão aplicadas regras layer 3 restringindo acesso a requisições API apenas aos participantes do R2C3, desta forma devem ser encaminhados em fase de adesão os endereços IP públicos utilizados durante as requisições API.

7. CONTATOS

Núclea			
Assunto	**Contato**	**Telefone**	**E-mail**
Registradora Núclea. Registro de Recebíveis de Arranjos de Pagamento - R2C3	Centro de Excelência Clientes	(11) 4632-7320	registradora@nuclea.com.br

8. CONTROLE DO DOCUMENTO

8.1. HISTÓRICO DE ATUALIZAÇÃO

Versão	Rev.	Data Da Publicação	Motivo/ Descrição	Área Responsável	Data De Vencimento
1	0	12.02.2020	Elaboração Inicial.	Desenho de Serviços	
1	1	21.02.2020	Especificações de Arquitetura e Segurança.	Arquitetura e Segurança	

1	2	30.03.2020	Características da api.	Arquitetura	
1	3	02.04.2020	Características de arquivos, mensagens e adesão.	Arquitetura	
1	4	02.04.2020	Características das ferramentas.	Arquitetura	
1	5	09.04.2020	Plataformas suportadas – tamanho payload.	Arquitetura	
1	6	29.04.2020	Requisição relacionada (call-back).	Arquitetura	
1	18	17.05.2020	Assinatura jws (retirar payload e acerto descrição campos JOSE header).	Arquitetura	
1	19	25.05.2020	Aumento do tamanho máximo dos campos do JOSE Header (identificação requisição e identificação requisição relacionada) de 23 para 40 caracteres.	Arquitetura	
1	20	03.06.2020	Inclusão dos campos de principal e administrado relacionados no call-back. Detalhamento do campo serial number do JOSE Header. Detalhamento estrutura JOSE Header para requisições, respostas síncronas e assíncronas.	Arquitetura	
1	21	10.06.2020	Inclusão da Autoridades Certificadoras aceitas no jdk 11.0.5 Alteração da descrição do campo `x5t#S256`.	Arquitetura	
1	22	06.07.2020	Revisão dos itens referentes a certificados digitais.	Segurança	
1	23	04.08.2020	Revisão quanto a convenção de nomes dos objetos IBM Webphere MQ.	Centro de Comando	
1	24	02.09.2020	Ajustes na informação referente aos serviços de DNS.	Centro de Comando	
1	25	19.09.2020	Ajustes nos usuários de C:D/CFT, Inclusão de IPs de saída para API.	Centro de Comando	

1	26	24.09.2020	Flexibilização de caracteres TAB e CR (Carriage Return) em arquivos e mensagens. Detalhamento sobre o campo C04 para mensagens. Incluído a característica da mensagem GEN0004. Flexibilização para permitir certificados diferentes por canal.	Arquitetura - Segurança	
1	27	18.11.2020	KID em maiúsculo e exemplo do KID com tamanho de 32 posições.	Arquitetura	
1	28	29.03.2021	API's DMZ do R2C3 em uma nova estrutura de link dedicado.	Redes	
1	29	02.06.2021	Correção do tamanho máximo do arquivo compactado para 50Mbps e ajustes gerais na definição do MQ.	Desenho de Serviços	
3	1	10.04.2023	Alteração da marca CIP para Nuclea e revisão periódica.	Squad de recebíveis	

As 29 alterações acima ocorreram durante o período de homologação do R2C3.

Versão	Rev.	Data de Publicação	Motivo/ Descrição	Área Responsável	Data de Vencimento
1	0	08.06.2021	A partir da entrada em produção do R2C3 - elaboração inicial.	Desenho de Serviços	08.06.2022
2	0	03.06.2022	Revisão Periódica.	Squad de recebíveis	03.06.2023
3	0	25.04.2023	Revisão Periódica.	Squad de recebíveis	25.04.2025
4	0	17.10.2023	Revisão Extraordinária. Retiradas as informações do endereço IP da rede Financial NET de contingência. Ajuste no nome Núclea que passou a ser acentuado. Ajuste do contato de E-mail da área do CdE Clientes.	Squad de recebíveis	17.10.2025
5	0	30.12.2024	Revisão Extraordinária. **5.6.5. Definições do MQ - página 14** Para as respostas COA/COD se faz necessário configurar QM.ISPBRemoto.C.MSGP e QM.ISPBRemoto.C.HTTP por necessidades específicas do sistema R2C3. Na planilha de Filas remotas (na IF): Adicionado a 5ª e 6ª linha **IF envia mensagens de COA/COD:** QM.ISPBRemoto.C.MSGP Preencher os campos: Gerenciador de Fila Remota(RQMNAME): QM.ISPBRemoto.C.MSGP Fila de Transmissão(XMITQ): QM.ISPBRemoto.C **IF envia mensagens de COA/COD** QM.ISPBRemoto.C.HTTP Preencher os campos: Gerenciador de Fila Remota(RQMNAME): QM.ISPBRemoto.C.HTTP Fila de Transmissão(XMITQ): QM.ISPBRemoto.C	Squad de recebíveis	30.12.2026

8.2. CICLO DE REVISÃO

Este documento será revisto e atualizado quando:

- Houver solicitação de atendimento, correção ou adição de informações;
- Existir a necessidade de atender requisitos legais, boas práticas ou recomendações de auditoria;
- Existir mudança na organização que tenha impacto relevante na atividade abordada neste documento;
- Conforme prazo bienal de Revisão Periódica.

8.3. GUARDA E RETENÇÃO

As versões deste documento serão armazenadas por cinco anos, após o vencimento de seu prazo de validade.

8.4. DISPONIBILIDADE DO DOCUMENTO

A última versão deste documento poderá ser obtida no Sítio Eletrônico da Núclea:

https://www.nuclea.com.br/

8.5. CLASSIFICAÇÃO DA INFORMAÇÃO

Podem ser disseminadas dentro e fora da empresa com acesso liberado para leitura. Sua divulgação não causa qualquer dano à Núclea.

NÚCLEA, São Paulo, 30 de dezembro de 2024.