Manual

MAPX-OP052-2014

Manual de Integração e Segurança SCC

Objetivo: O Manual Técnico do SCC - Webservices tem a finalidade de descrever os procedimentos que os participantes da Financial NET (RTM) devem seguir para configurar e permitir a conexão de seus sistemas com o ambiente Núclea Associação, conectando-se ao sistema que disponibiliza troca de arquivos via Connect Direct, XFB e interface via webservice.

Autor do documento: Infraestrutura e Suporte TI.

Contato: *Infraestrutura e Suporte TI.*

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.

Manual de Integração e Segurança SCC

Denominação: Manual de Integração e Segurança SCC	**Código:** MAPX-OP052-2014	**Folha:** 2/34
Área emitente: Consignado	**Vigência:** 23/10/2025 a 23/10/2027	**Versão:** 11.0

Sumário

Manual de Integração e Segurança SCC

Manual de Integração e Segurança SCC

Denominação: Manual de Integração e Segurança SCC	**Código:** MAPX-OP052-2014	**Folha:** 5/34
Área emitente: Consignado	**Vigência:** 23/10/2025 a 23/10/2027	**Versão:** 11.0

1. Objetivo

Este documento tem como objetivo descrever os padrões, procedimentos e configurações a serem utilizados para a transferência de informações no SCC.

2. Divulgação

Este documento pode ser encontrado:

- Portal Corporativo da Núclea Associação;
- Portal do Participante.

3. Vigência

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

4. Processo de referência

Infraestrutura e Suporte TI – Gerir demandas de soluções e serviços.

5. Disposições gerais

5.1. Premissas e considerações gerais

As regras e padrões deste documento foram concebidos para garantir o intercâmbio de arquivos e Webservices entre o ambiente SCC e os Participantes pela rede privada (RTM Financial NET) para arquivos e rede pública (Internet) para Webservices, de forma segura, controlada, com um uso eficiente dos meios de transmissão e com forte resiliência e suporte a automação.

5.2. Plataformas de transferência suportadas no SCC

O SCC suporta a troca de arquivos pelas plataformas Sterling Connect:Direct e XFB, largamente utilizadas nos meios financeiros em virtude de suas robustez e confiabilidade. O sistema também permite conexão através uma interface via webservice, via Internet.

Observação: As soluções de transferência de arquivos XFB e Connect:Direct não operam em ambientes de rede pública (Internet), sendo restritas a redes privadas ou dedicadas para garantir maior segurança e confiabilidade.

5.2.1. Sterling 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 total 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.

5.2.2. XFB

O Synchrony File Transfer, mais conhecido como XFB (derivado do nome anterior do produto - Axway File Broker) 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.

5.2.3. Integração por webservices

Os principais aspectos do padrão de integração por webservices são:

- Utilização do padrão SOAP 1.1;
- Utiliza-se o padrão WS-Security com certificados digitais X.509 para garantir a assinatura digital e a criptografia de mensagens, tanto nas requisições quanto nas respostas. Essa abordagem assegura as propriedades de não repúdio e confidencialidade, protegendo a integridade das comunicações entre o Participante e a Núclea Associação.
- Disponibilização dos serviços sobre HTTPS em produção e homologação;
- Existência de um método de negócio para cada tipo de transferência de informação;
- Cada método de negócio permitirá, a priori, acesso a uma única informação.

Para cada sistema, a Núclea Associação determinará os endpoints, além da especificação dos serviços propriamente dita, via publicação do WSDL.

5.3. Características dos arquivos no SCC

Os arquivos que trafegam no ambiente SCC, bem como as regras e padrões aplicáveis, estão detalhados no documento "MAPX-OP050-2014 – Manual de Leiautes de Arquivos do SCC", o qual também especifica a estrutura e o conteúdo dos arquivos utilizados.

Como os arquivos que trafegam no SCC já são compactados, assinados digitalmente e criptografados — nessa ordem — no momento de sua geração, não se aplicam mecanismos adicionais de criptografia ou compactação durante a transmissão. Funcionalidades como o Secure+ da plataforma Connect:Direct são desnecessárias e apenas agregariam complexidade e custo à solução, sem oferecer benefícios adicionais.

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

a) Construir uma requisição, em formato definido no documento "MAPX-OP050-2014 - Manual de Leiautes de Arquivos do SCC";

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 utilizando um framework de criptografia padrão SPB;

d) Enviar para a Núclea Associação 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 Associação 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 documento "MAPX-OP050-2014 – Manual de Leiautes de Arquivos do SCC".

5.4. Regras para transferência de arquivos no SCC

a) Os arquivos devem ser compactados utilizando o formato GZIP, conforme especificado na RFC 1952, e em seguida devem ser cifrados e assinados digitalmente — sendo ambos os processos realizados de forma simultânea. No ambiente Unix, o aplicativo "gzip" implementa esse formato. Para compactação em Java, recomenda-se o uso da classe padrão java.util.zip.GZIPOutputStream. Já em C, a biblioteca "zlib" pode ser utilizada, pois também implementa o padrão GZIP sem modificações.

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) A verificação de CRC (Cyclic Redundancy Check) deve ser desabilitada em todas as transferências, uma vez que a integridade dos arquivos já é assegurada pelo protocolo de transporte TCP, além de trafegarem por meios digitais de alta confiabilidade;

f) É obrigatória a habilitação da opção de retomada em caso de falha (checkpoint restart). Caso todas as tentativas de retransmissão sejam esgotadas sem sucesso, a transmissão será considerada mal sucedida, devendo ser adotados os procedimentos operacionais definidos pela Área de Operações da Núclea Associação.

g) Os Participantes podem conectar-se aos servidores de transferência de arquivos da Núclea Associação, utilizando-se de resolução de nomes 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 sitio de contingência do SCC, com respectiva interrupção dos serviços até que esta operação se complete.

h) Os arquivos gerados pela Núclea Associação e destinados aos Participantes podem, opcionalmente, ser transmitidos com o uso do recurso RUN JOB da plataforma

Connect:Direct, desde que a transmissão tenha origem na própria Núclea Associação. Esse recurso não é permitido para transmissões iniciadas pelos Participantes. Após o envio do arquivo, a Núclea Associação executará um comando ou programa por meio de RUN JOB, utilizando o padrão de nome: CIPSCC “nome do arquivo”, onde CIPSCC é o nome do programa a ser executado e "nome do arquivo" corresponde ao nome do arquivo transmitido, passado como parâmetro.

Qualquer parâmetro adicional de configuração solicitado pela Instituição, que não esteja contemplado neste documento, será submetido à análise técnica pela equipe da Núclea Associação. A implementação estará sujeita à viabilidade técnica e operacional, podendo ser recusada caso comprometa a segurança, a padronização ou a estabilidade do ambiente.

5.5. Endereçamento IP dos servidores homologação, produção, contingência e DNS

Abaixo estão descritas as configurações e parâmetros necessários para a configuração das soluções Connect:Direct, XFB e Webservices.

5.5.1. DNS privado

Rede Privada (RTM): SCCCIP.ORG: Utilizado em transferências de arquivos via rede Privada.

5.5.2. Servidores DNS

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

5.5.3. Endereçamento do ambiente

Connect:Direct

Hostname	IP	Porta	Ambiente
cdh.scccip.org	10.200.10.114	1364	Homologação
cdp.scccip.org	10.200.10.115	1364	Produção
cdp.scccip.org	10.200.11.115	1364	Contingência

XFB

Hostname	IP	Porta	Ambiente
xfbh.scccip.org	10.200.10.114	6330	Homologação
xfbp.scccip.org	10.200.10.115	6330	Produção
xfbp.scccip.org	10.200.11.115	6330	Contingência

WebServices (Rede Privada RTM)

URL - Endpoint	IP	Porta	Ambiente
https://www.hext.portaldoconsignado.org.br:8443/ws/[FUNCIONALIDADE]	10.200.10.137	8443	Homologação
https://www.portaldoconsignado.org.br:8443/ws/[FUNCIONALIDADE]	10.200.10.143	8443	Produção

WebServices (Internet. Atenção: Utilizar o DNS para acesso ao serviço)

URL - Endpoint	Porta	Ambiente
https://www.hext.portaldoconsignado.org.br/ws/[FUNCIONALIDADE]	443	Homologação
https://www.portaldoconsignado.org.br/ws/[FUNCIONALIDADE]	443	Produção

Observação: Recomenda-se que os participantes configurem suas aplicações utilizando o hostname dos servidores da Núclea Associação, em vez de endereços IP. Essa prática facilita a gestão de mudanças de infraestrutura e garante maior flexibilidade e confiabilidade na conexão.

O ambiente de Contingência permanecerá inativo e o processo de convergência será transparente para o participante.

[FUNCIONALIDADE] é a operação que o participante deseja acessar. “ASCC005” para Reserva de Averbação e “ASCC013” para Consulta de Margem do Servidor

Para visualizar a interface do serviço, trocar o “A” por “W”, conforme exemplo abaixo:

Exemplo: https://URL/ws/WSCC005.wsdl

5.6. Consifgurações: Connect:Direct, XFB e webservices

Connect:Direct Ambiente Núclea Associação – Ambientes Produção, Contingência e Homologação	
Node	Produção e Contingência: SCCCIPP Homologação: SCCCIPH
DNS Names / IP do servidor Connect:Direct	Produção: cdp.scccip.org / 10.200.10.115 Contingência: cdp.scccip.org / 10.200.11.115 Homologação:cdh.scccip.org / 10.200.10.114
Porta de Comunicação	TCP-1364 (bidirecional)
Usuário de conexão	Ambiente Produção: P02992335 Ambiente Contingência: P02992335 Ambiente Homologação: H02992335
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
Checkpoint Restart	Habilitado a cada 5MB
CRC	Desabilitado
Retries	Short Term: 3 Long Term: 3
Retry Interval	Short Term: 10 Segundos Long Term: 3 Minutos

XFB Ambiente Núclea Associação - Ambientes Produção, Contingência e Homologação	
Site:	Produção e Contingência: STSCCIPP Homologação: STSCCIPH
DNSNames / IP do servidor XFB	Produção: xfbp.scccip.org / 10.200.10.115 Contingência: xfbp.scccip.org / 10.200.11.115 Homologação: xfbh.scccip.org / 10.200.10.114
Portas de Comunicação	TCP-6330 (Bidirecional)
Aplicação	CIPTOIF(aplicação sender Núclea Associação → IF) IFTOCIP (aplicação Receiver IF → Núclea Associação)
Usuário de conexão	Ambiente Produção: P02992335 Ambiente Contingência: P02992335 Ambiente Homologação: H02992335
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

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 SCC.

A definição dos requisitos de segurança exigidos foi baseada em padrões conhecidos, utilizados no mercado e já adotados no âmbito do SPB.

A Núclea Associação 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 SCC.

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 das transferências de informação do SCC adotarão especificações de segurança do SPB (chaves assimétricas) semelhantes.

ii. As transferências de informação transmitidas entre os Participantes do SCC a Núclea Associação são irrevogáveis, incondicionais e finais;

iii. Todas as transferências de informação 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. Todas as transferências de informação devem possuir uma identificação única garantindo sua rastreabilidade e unicidade de processamento; e

vi. Todo e qualquer transferência de informação ao SCC por um de seus Participantes é de exclusiva responsabilidade de quem o originou.

b) Diretrizes:

i. A Núclea Associação utilizará no SCC, certificado digital específico e exclusivo para este sistema conforme as especificações descritas no item 3.2;

ii. A Núclea Associação utilizará mesmo certificado digital em ambos os canais de comunicação, respeitando-se a segregação entre os ambientes de produção e homologação;

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

iv. Será permitido ao participante optar pela utilização do mesmo certificado digital em ambos os canais (Arquivos e Webservices) ou optar por utilizar certificados digitais distintos em cada

canal, cabendo ao participante informar no Termo de Adesão, os dados de cada certificado digital que será utilizado em cada canal;

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

vi. Os Certificados Digitais são do tipo A1 (01 ano de validade) e deverão ser emitidos por uma entidade 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;

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

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

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

x. Apenas para o ambiente de HOMOLOGAÇÃO do SCC poderá ser utilizado, a critério do Participante, certificado digital gerado e assinado por desenvolvimento interno, mantendo-se as especificações e sequenciais (tamanho da chave, algoritmos de criptografia e assinatura, validade e campos);

xi. O certificado desenvolvido internamente deverá ser trocado, no ambiente de HOMOLOGAÇÂO, por certificado emitido por uma entidade certificadora e testado, com o envio de um arquivo, antes do início das operações do participante no ambiente de PRODUÇÃO;

xii. O sistema do SCC, tanto em homologação como em produção, adotará para arquivos apenas o cabeçalho de segurança versão 2 (Header v2) e certificados digitais com chaves criptográficas de 2048 bits. (vide item 3.6). Já para webservices, adotará o padrão WS-Security, conforme detalhado no item 3.7; e

xiii. 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 tipo servidor ICP-Brasil

a) Campos obrigatórios a serem incluídos no CSR:

   i. 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

   ii. OU= Nome da Instituição

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

   iv. OU= SCC Pxxx ou Txxx

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

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

b) Padrão de nomeação de certificados por ambiente:

   i. Os certificados emitidos para os ambientes serão identificados pelo conteúdo do campo "OU"=SCC 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; e

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

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

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

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

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

g) É vedado o reuso, para qualquer finalidade, de CSRs utilizados para a solicitação de certificados a serem utilizados no âmbito da SCC.

6.3. Exemplos ilustrativos de preenchimento de CSRS

a) No caso do primeiro certificado de produção da Núclea Associação (SP):

CN= SCC_p001.cip-bancos.org.br

OU= Camara Interbancaria de Pagamentos – CIP

OU=029922335

OU= SCC P001

L=Sao Paulo

S=SP

O=ICP-Brasil

C=BR

b) No caso do segundo certificado 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=SCC T002

L=Sao Paulo

S=Sao Paulo

O=ICP-Brasil

C=BR

Observação: Não deve ser usado caractere acentuado para atender ao disposto no item 7.1.5 da resolução nº 7 do Comitê Gestor da ICP-Brasil

6.4. Processo de obtenção e habilitação de certificados

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) A solicitação para a emissão de certificado 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 SCC.

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

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

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

f) A Núclea Associação verificará a duplicidade da chave pública e a consistência dos dados registrados e responderá por e-mail a instituição a habilitação do certificado;

g) Cada Instituição terá apenas um certificado ativado por canal de comunicação em cada ambiente de produção ou homologação;

h) Cada certificado deverá estar associado a um par de chaves únicas;

6.5. Processos de ativação, substituição e revogação de certificados

a) Os certificados habilitados, na forma do item 3.4.7, estarão disponíveis para uso, que poderá ser inicial, no caso do primeiro certificado, ou de substituição, pelo encerramento da validade ou revogação de um certificado sendo utilizado;

b) Para ativar certificados, tanto inicialmente como por substituição, a instituição emitirá mensagem por e-mail a Núclea Associação 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 atual, do certificado a ser substituído, a previsão de data, hora, correspondente chave pública do certificado que será ativado e o nº de série do certificado que será desativado.

c) Os certificados substituídos deverão ser obrigatoriamente revogados pelo Participante junto à AC, não podendo mais serem utilizadas as chaves a eles correlacionadas;

d) As ativações ou substituições de certificados deverão ser efetivadas em data e horário que minimizem qualquer impacto operacional;

e) 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;

f) A substituição dos certificados da Núclea Associação, quando do seu vencimento anual, em qualquer ambiente (produção ou homologação), será previamente comunicada aos participantes por e-mail ou INFO-CIP, 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.

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

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

i) Todo certificado será automaticamente invalidado para uso no âmbito do SCC às 24 (vinte e quatro) horas do dia anterior à data especificada em seu campo Válido Até. Por exemplo, um certificado que tenha os dados "07/10/2012 15:34:06" em seu campo Válido Até será desativado às 24 horas do dia 06/10/2012".

6.6. Especificações para a segurança dos arquivos

a) Cabeçalho ("header") de segurança dos Arquivos

Todos os arquivos eletrônicos trocados no âmbito do SCC 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

b) 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".

c) 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.

d) 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.

e) A identificação dos certificados 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 tiver o número de série exibido pelo browser de certificados 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".

f) 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.

g) 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 dos arquivos

a) O cabeçalho de segurança não tem código de página, é sempre binário;

b) O conteúdo que sucede os 588 bytes do cabeçalho de segurança deve estar obrigatoriamente no formato GZIP, conforme especificação da RFC 1952.

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

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

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

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

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

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

i) 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;

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

k) Excepcionalmente nas condições abaixo, poderá assumir os seguintes valores:

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

m) “8” - Indicativo de arquivo compactado;

n) “10” - Indicativo de arquivo compactado, sem cifragem, normalmente de uso público;

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

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

q) 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 recepção de arquivos

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

b) Abre-se a informação da chave simétrica de cifragem do arquivo com a chave privada correspondente à chave pública do certificado;

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

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

e) Confere-se a assinatura do arquivo, comparando o "hash" obtido;

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

6.9. Especificação de segurança para a integração via webservices

A assinatura digital e criptografia adotarão o padrão WS-Security com uso de certificados X509 para assinatura digital e criptografia (chaves assimétricas).

a) Assinatura digital

A assinatura digital deverá ser realizada com:

- Signature Algorithm : RSA-SHA256 (http://www.w3.org/2001/04/xmldsig-more#rsa-sha256)
- Signature Canonicalization: C14N-exc (http://www.w3.org/2001/10/xml-exc-c14n#)
- Digest Algorithm: SHA256 (http://www.w3.org./2001/04/xmlenc#sha256)
- SignatureTarget:
  - Timestamp(Namespace:'http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd')
  - Body (Namespace: http://schemas.xmlsoap.org/soap/envelope/)
- Chave publica do emissor comunicada através do IssuerSerial (issuername e serialnumber) (Namespace: http://www.w3.org/2000/09/xmldsig#)

b) Criptografia

A criptografia deverá ser realizada com:

- Symmetric Encoding Algorithm : 3DES-CBC (http://www.w3.org/2001/04/xmlenc#tripledes-cbc)
- Key Transport Algorithm: RSA-OAEP (http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p)
- Chave publica do receptor identificada pelo IssuerSerial (issuername e serialnumber) (Namespace: http://www.w3.org/2000/09/xmldsig#)
- Encryption Target:
  - Body (Namespace: http://schemas.xmlsoap.org/soap/envelope/)

7. Formato de requisições e respostas

7.1. Conteúdo mínimo da requisição e da resposta

A chamada seguirá o padrão “wrapped document literal”.

Toda requisição conterá pelo menos os seguintes campos:

- IdentEmissor : identificador do Participante Emissor, consistindo de sua identificação enquanto participante na Núclea Associação;
- NUOp (Número Único da Operação): identificador exclusivo da operação, estruturado no formato XXXXXXXXAAAAMMDDSSSSSSS, onde:
  - XXXXXXXX representa o código do Participante;
  - AAAAMMDD corresponde à data da operação (ano, mês e dia);

- SSSSSSS é um número sequencial único.

O valor do NUOp deve ser sempre único dentro do domínio do sistema, não podendo haver repetições, mesmo entre operações distintas.

- DtHrChamada: datahora da chamada, usando o relógio local do Participante
- NumeroControleIF: campo de uso livre do Participante, para estabelecer a relação com seus sistemas internos;
- DataMovimento: data do movimento (data contábil).
- Dominio: indica o domínio ou Aplicação.

Toda resposta conterá pelo menos os seguintes campos:

- DtHrResposta: datahora da resposta
- StatusProcessamento, indicando se o processamento foi realizado com sucesso ou não.

A fig.6.8.1a mostra a estruturação geral:

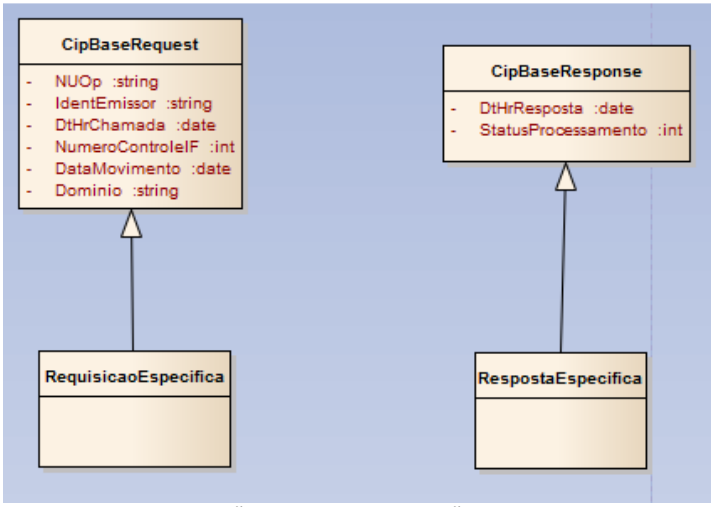

Fig.6.8.1a:Estruturação básica de Requisições e Respostas

O endpoint dos serviços está contido no WSDL, que será fornecido pela Núclea Associação.

7.2. Requisições genéricas

As requisições a seguir devem ser providas, de forma genérica, para finalidades diversas como teste de conectividade e verificação da situação de requisições terminadas por timeout.

7.2.1. Ping

Destina-se ao teste de conectividade entre o Participante e a Núclea Associação. Guarda, neste aspecto, relação com a GEN001.

Deve ser permitido tanto em formato aberto (sem assinatura nem criptografia) quanto com assinatura e criptografia, buscando-se assim ter uma forma básica de teste para o Participante.

A proteção contra-ataques (no caso, “flood”) deve ser provida pela camada de rede e, portanto, está fora do escopo desta especificação.

A fig.6.9.1a mostra os atributos da requisição e da resposta.

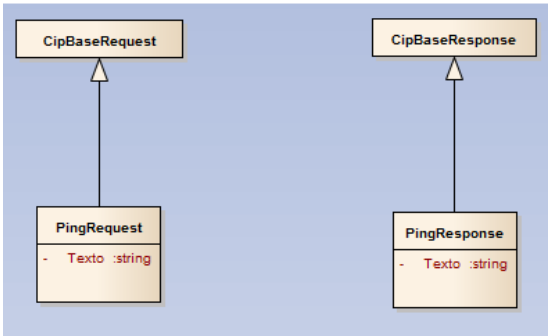

Fig.6.9.1a: Requisição e Reposta da transação PING

7.2.2. Status

Destina-se a recuperar a situação de processamento de uma transação realizada anteriormente, bem como a resposta que foi enviada. Pode ser usada em situações em que houve timeout, para obter o resultado da operação, se ela foi efetivamente realizada. Neste sentido, guarda relação com a GEN012.

Deve ser disponibilizada apenas com assinatura e criptografia, tanto da requisição quanto da resposta.

A fig.6.9.2a mostra os atributos da requisição e da resposta.

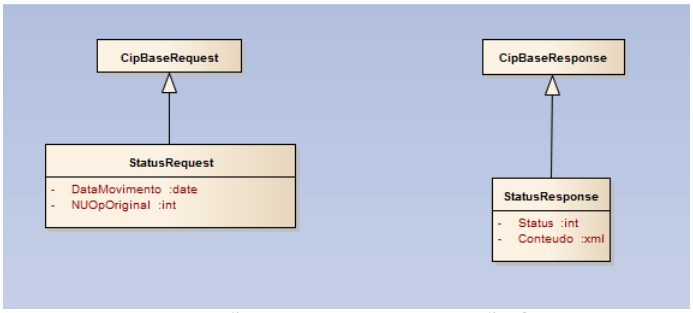

Fig.6.9.2a: Requisição e resposta da transação Status

8. Tratamento de erros

A seguir são relacionados os códigos de erros passíveis de registro em log, a partir da recepção de arquivos inválidos:

Erro	Código	Campo(s)	Causa
00H	-	-	Sem erros, segurança conferida

01H	EGEN9901	C01	Tamanho do cabeçalho de segurança zerado ou incompatível com os possíveis
02H	EGEN9902	C02	Versão inválida ou incompatível com o tamanho e/ou conexão
03H	EGEN9903	C06	Algoritmo da chave do destinatário inválido ou divergente do certificado
04H	EGEN9904	C07	Algoritmo simétrico inválido
05H	EGEN9905	C08	Algoritmo da chave de assinatura inválido ou divergente do certificado
06H	EGEN9906	C09	Algoritmo de "hash" não corresponde ao indicado ou é inválido
07H	EGEN9907	C10	Código da AC do certificado do destinatário inválido
08H	EGEN9908	C11	Número de série do certificado do destinatário inválido (não foi emitido pela AC)
09H	EGEN9909	C12	Código da AC do certificado de assinatura inválido
0AH	EGEN9910	C13	Número de série do certificado de assinatura inválido (não foi emitido pela AC)
0BH	EGEN9911	C15	Assinatura da Mensagem inválida ou com erro
0CH	EGEN9912	C12/13	Certificado não é do emissor do arquivo
0DH	EGEN9913	C14	Erro na extração da chave simétrica
0EH	EGEN9914	C14	Erro gerado pelo algoritmo simétrico
0FH	EGEN9915	arquivo	Tamanho do arquivo não múltiplo de 8 bytes
10H	EGEN9916	C12/13	Certificado usado não está ativado

11H	EGEN9917	C12/13	Certificado usado está vencido ou revogado pela Instituição
12H	EGEN9918	-	Erro genérico de software da camada de segurança
13H	EGEN9919	C04	Indicação de uso específico inválida ou incompatível
14H	EGEN9920	C12/13	Certificado inválido

a vez detectado o erro, é preenchido o campo de código de erro (C03) do cabeçalho conforme a tabela de códigos.

Na hipótese de haver mais de um erro, deve ser reportado o de código menor, que normalmente corresponde à primeira consistência que deve ser feita.

Deve ser gerado um arquivo de log, com o erro EGEN99nn correspondente.

9. Contatos

Núclea Associação			
Assunto	**Contato**	**Telefone**	**E-mail**
SCC	Cde de Clientes	(55 11) 4632-7321	scc@nucleaassociacao.org.br

10. Controle do documento

10.1. Atualização

Manual de Integração e Segurança SCC

Denominação: Manual de Integração e Segurança SCC	**Código:** MAPX-OP052-2014	**Folha:** 32/34
Área emitente: Consignado	**Vigência:** 23/10/2025 a 23/10/2027	**Versão:** 11.0

Versão	Rev.	Data Da Publicação	Motivo/ Descrição	Área Responsável	Data De Vencimento
1	0	12.04.2012	Elaboração Inicial.	Gerencia de Infraestrutura e Suporte de TI RSC	12.04.2013
2	0	31.03.2015	Primeira Revisão Periódica. Inclusão da AC 07H:ImprensaOficiaL.	Segurança	29.07.2015
3	0	26.02.2016	- Acerto de método algoritmo de assinatura HMAC-SHA256 para RSA-SHA256 para o Web Services - Alteração da emissão da chave pública da assinatura e criptografia de BinarySecurityToken para IssuerSerial. - Informações de url, IP, porta e observações do canal web services. - - Ajuste na padronização do leiaute do manual, ajuste no nome do documento no cabeçalho do documento e retirada de quadro redundante sobre informações do web services. - Alterado o contato da área de atendimento.	Gerencia de Infraestrutura e Suporte de TI e Gerência de Arquitetura	26.02.2017
4	1	08.07.2016	Ajustes no capítulo Criptografia e Assinatura Digital: itens 3.1 (diretrizes), 3.4 e 3.5. Para contemplar opção de utilização de certificados digitais distintos por canal de comunicação (Arquivos e/ou Webservices).	Segurança da Informação	26.02.2017

5	0	19.04.2017	Revisão Periódica. Atualização da numeração e correção do layout do documento.	Infraestrutura e Suporte TI	19.04.2018
6	0	24.05.2018	Revisão Periódica do Documento.	Infraestrutura e Suporte TI	24.05.2018
7	0	18.02.2020	Revisão Periódica Atualização da numeração e correção do layout do documento.	Infraestrutura e Suporte TI	18.02.2021
8	0	05.04.2021	Revisão Periódica.	Infraestrutura e Suporte TI	05.04.2022
9	0	18.04.2022	Revisão Periódica.	Infraestrutura e Suporte TI	18.04.2023
10	0	24.03.2023	Revisão Periódica.	Squad Consignado	24.03.2025
11	0	23.10.2025	Atualização do leiaute do documento e revisão de texto	Squad Consignado	23.10.2027

10.2. 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;

- No vencimento, conforme item HISTÓRICO DE ATUALIZAÇÃO deste documento.

10.3. Guarda e retenção

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

10.4. Disponibilidade do documento

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

https://www.nucleaassociacao.org.br/

10.5. Classificação da informação

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

Núclea Associação, São Paulo, 23 de outubro de 2025.