

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 1/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



NUCLEa

Manual

MAPX – XXXX – XXXX

MANUAL DE INTEGRAÇÃO E SEGURANÇA
MÓDULO DE COMPENSAÇÃO DE BOLETOS
DE PAGAMENTO – CMP

Objetivo

Este documento tem a finalidade de descrever os procedimentos que as Instituições Participantes devem seguir para configurar e permitir a conexão de seus sistemas com o sistema da Compensação de Boletos de Pagamento – CMP, para troca de informações entre Nuclea e Instituições, utilizando-se de troca de arquivos.

Autor do documento

Contato: Desenho de Serviços 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 TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 2/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



Sumário

1. OBJETIVO	3
2. PREMISSAS	3
2.1. Redes suportadas	3
2.2. IBM Connect:Direct	3
2.3. Axway Transfer CFT	4
2.4. Características dos arquivos da Compensação de Boletos de Pagamento - CMP	4
3. INSTRUÇÕES DE CONECTIVIDADE	4
3.1. Endereços dos servidores Compensação de Boletos de Pagamento – CMP	4
4. REGRAS TRANSFERÊNCIA DE ARQUIVOS NA COMPENSAÇÃO DE BOLETOS DE PAGAMENTO – CMP	5
5. CONFIGURAÇÃO DOS PRODUTOS COMPENSAÇÃO DE BOLETOS DE PAGAMENTO – CMP	7
5.1. Configurações para o Connect:Direct	7
5.2. Configurações para o CFT	8
6. CRIPTOGRAFIA E ASSINATURA DIGITAL	9
6.1. Introdução	9
6.2. Premissas	9
6.3. Diretrizes	10
6.4. Processos de ativação, substituição e revogação de certificado digital	11
6.5. Especificação para a Segurança dos Arquivos	11
6.6. Certificado Compensação de Boletos de Pagamento - CMP	11
6.7. Exemplo ilustrativos de preenchimento de CSRS	12
6.8. Processo de obtenção de habilitação de certificados	13
7. CONTATOS	13
8. CONTROLE DO DOCUMENTO	13
8.1. HISTÓRICO DE ATUALIZAÇÃO	13
8.2. CICLO DE REVISÃO	15
8.3. GUARDA E RETENÇÃO	15
8.4. DISPONIBILIDADE DO DOCUMENTO	15
8.5. CLASSIFICAÇÃO DA SEGURANÇA	15

MANUAL TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 3/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



1. OBJETIVO

Este documento tem como objetivo descrever os padrões, procedimentos e configurações a serem utilizados para o intercâmbio de arquivos entre instituições e o ambiente da Compensação de Boletos de Pagamento – CMP.

2. PREMISSAS E CONDIÇÕES GERAIS

As regras e padrões deste documento foram concebidos para garantir o intercâmbio de arquivos entre o ambiente da Compensação de Boletos de Pagamento - CMP e Instituições Financeiras de forma segura, controlada, com um uso eficiente dos meios de transmissão, com forte resiliência e suporte a automação. Os vários manuais referentes ao SPB, SFN, Redes e Segurança podem ser encontrados no site do banco central.

2.1. Redes Suportadas

Para a comunicação com a **Compensação de Boletos de Pagamento - CMP** é utilizada a rede Financial NET, fornecida pela operadora RTM. Os parâmetros de configuração de IBM Connect:Direct e Axway CFT estão contidos nos capítulos abaixo.

2.2. Plataformas de transferência suportadas na Compensação de Boletos de Pagamento - CMP

Para troca de arquivos suportamos as plataformas IBM Connect:Direct ou Axway CFT (XFB), ambas largamente utilizadas nos meios financeiros em virtude de suas robustez e confiabilidade. Ficará a critério das Instituições Financeiras a escolha da plataforma que será utilizada, será permitido apenas solicitação de adesão por uma única ferramenta. Desta forma, não será permitida a utilização das duas ferramentas por uma instituição participante.

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 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.

MANUAL TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 4/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



2.4. Axway Transfer CFT

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.

2.5. Características dos arquivos da Compensação de Boletos de Pagamento - CMP

Os arquivos que trafegam na plataforma, bem como as regras e padrões que a eles se aplicam, estão descritos em detalhe no documento “Manual de Leiautes de Arquivos da Compensação de Boletos de Pagamento – CMP”, que também descreve a estrutura do conteúdo dos mesmos.

Como os arquivos que trafegam na Compensação de Boletos de Pagamento - CMP são compactados, assinados digitalmente e criptografados (nesta ordem) já na sua geração, não suportamos mecanismos adicionais de criptografia ou compactação de dados na transmissão, tais como o Secure+.

3. INSTRUÇÕES DE CONECTIVIDADE

Neste capítulo estão descritas as informações de comunicação com a plataforma.

3.1. Endereços dos servidores Compensação de Boletos de Pagamento – CMP

O sistema fará uso de um domínio DNS exclusivo publicado na RTM, conforme abaixo.

Domínio DNS: **cipcmp.com.br**

DNS's RTM:

Função	IP
Name Server RTM RJ	10.0.17.2
Name Server RTM SP	10.0.33.2

MANUAL TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 5/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



Endereços do ambiente:

Hostname RTM	IP RTM	Ambiente Produção
cdp.cipcmp.com.br	10.200.61.50	Connect:Direct
xfbp.cipcmp.com.br	10.200.61.51	Axway CFT (XFB)
Hostname RTM	IP RTM	Ambiente Contingência
cdp.cipcmp.com.br	10.200.62.130	Connect:Direct
xfbp.cipcmp.com.br	10.200.62.131	Axway CFT (XFB)
Hostname RTM	IP RTM	Ambiente Homologação
cdh.cipcmp.com.br	10.200.61.145	Connect:Direct
xfbh.cipcmp.com.br	10.200.61.146	Axway CFT (XFB)

Obs.: É altamente recomendável às instituições que configurem as plataformas de troca de arquivos usando o serviço de resolução de nome (DNS), conforme especificação de endereços acima. A não configuração dos serviços neste formato pode implicar em indisponibilidade dos serviços quando houver comutação para o site contingência da Nuclea.

4. REGRAS TRANSFERÊNCIA DE ARQUIVOS NA COMPENSAÇÃO DE BOLETOS DE PAGAMENTO – CMP

- Todos os arquivos devem ser compactados no formato GZIP, conforme RFC 1952, assinados digitalmente e criptografados, nesta ordem, por aplicação específica antes de serem disponibilizados para as plataformas de transferência de arquivos. Para maiores detalhes vide Manual de Segurança da RSFN em vigência;
- Os arquivos devem ser transferidos sempre em modo binário;
- Qualquer mecanismo adicional de compressão eventualmente habilitado na ferramenta de troca de arquivos deve ser desabilitado para as transferências de arquivos com a Nuclea;
- Todas as transferências devem desabilitar verificação de CRC – Cyclic Redundancy Check, pois a integridade dos mesmos já é garantida pelo protocolo de transporte (TCP), além de trafegarem em meios digitais de alta confiabilidade;
- É obrigatório habilitar a opção de retomada em caso de falha (checkpoint restart); após esgotarem-se as tentativas de transferência, o processo de transmissão será considerado malsucedido e deverão ser adotados os processos operacionais da Nuclea;
- Os arquivos gerados pela Nuclea, destinados as Instituições Participantes, poderão ser enviados agregando ao processo de transmissão a utilização do recurso Run Job do Connect:Direct. A utilização deste recurso somente é permitida nas transmissões originadas na Nuclea, não sendo permitida a utilização do recurso quando a transmissão iniciar nas Instituições Participantes. Ao solicitar a execução do run job, o participante deve informar o caminho do executável bem como qualquer parâmetro adicional necessário;
- Para o caso de instituições que fazem uso de Mainframe, os participantes podem solicitar para à NUCLEA a realização de DE/PARA no arquivo recebido pela própria instituição (quando o envio for

MANUAL TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 6/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



realizado pela Nuclea). As realizações de adequações técnicas para realização dos DE/PARA serão estudadas pelo time técnico da sob possibilidade inviabilidade de configuração. A regra do DE/PARA é aplicável somente ao caso de envio de arquivos a partir da Nuclea; a Nuclea deve receber os arquivos seguindo as especificações definidas no manual dos layouts;

MANUAL

MANUAL TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 7/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



5. CONFIGURAÇÃO DOS PRODUTOS COMPENSAÇÃO DE BOLETOS DE PAGAMENTO – CMP

5.1. Configurações para o Connect:Direct

Abaixo estão descritas as configurações do ambiente correspondendo a Infraestrutura da Nuclea. Os parâmetros precisam ser de conhecimento dos técnicos responsáveis pela configuração da solução Connect:Direct.

Connect:Direct Ambiente Nuclea – Compensação da Cobrança	
Node	Produção e Contingência: CDCIPCMPP Homologação: CDCIPCMPPH
DNS Names / IP do servidor C:D	Produção: cdp.cipcmp.com.br – 10.200.61.50 Contingência: cdp.cipcmp.com.br - 10.200.62.130 Homologação: cdh.cipcmp.com.br - 10.200.61.145
Sistema Operacional	Unix AIX
Porta de Firewall	TCP-1364
Usuário de conexão	Produção e Contingência: P02992335 Homologação: H02992335
Proxy User	Habilitado
Sessões simultâneas (máx.)	Envio: 5 (por IF Remota) Recepção: 5 (por IF Remota)
Buffer Size	32k
Protocolo de Transporte	TCP
Tipo de transmissão	Binário
Compressão	Desabilitada
Criptografia (Secure+)	Desabilitada
Checkpoint Restart	Habilitado a cada 5 MB
CRC	Desabilitado
Retries	Short Term: 3 Long Term: 3
Retry Interval	Short Term: 10 Segundos Long Term: 3 Minutos

MANUAL TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 8/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



5.2. Configurações para o CFT

Abaixo estão descritas as configurações necessárias e parâmetros que precisam ser de conhecimento dos técnicos responsáveis pela configuração da solução CFT.

CFT Ambiente Nucela – Compensação da Cobrança	
Node	Produção e Contingência: STPCMP_CIP Homologação: STHCMP_CIP
DNS Names / IP do servidor C:D	Produção: xfbp.cipcmp.com.br – 10.200.61.51 Contingência: xfbp.cipcmp.com.br - 10.200.62.131 Homologação: xfbh.cipcmp.com.br - 10.200.61.146
Sistema Operacional	Unix AIX
Porta de Firewall	TCP-6330
Aplicação	CIPTOIF (aplicação sender CIP → IF) IFTOCIP (aplicação Receiver IF → CIP)
Usuário de conexão	Produção e Contingência: P02992335 Homologação: H02992335
Proxy User	Habilitado
Sessões simultâneas (máx.)	Envio: 5 (por IF Remota) Recepção: 5 (por IF Remota)
Buffer Size	32k
Protocolo de Transporte	TCP
Tipo de transmissão	Binário
Blocagem / Tam Reg	Variável (XML)
Compressão	Desabilitada
Criptografia (Secure+)	Desabilitada
Checkpoint Restart	Habilitado
CRC	Desabilitado
Retries	3 a cada 10 minutos
Protocolos	PeSIT

MANUAL TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 9/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



5.3. CRIPTOGRAFIA E ASSINATURA DIGITAL

5.4. 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 da Compensação de Boletos de Pagamento – CMP.

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

A Nuclea 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 pelas próprias Instituições Participantes da Compensação de Boletos de Pagamento – CMP.

Com isso, as Instituições 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 na RSFN.

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.

5.5. Premissas

- I. A criptografia e assinatura digital nos arquivos da Compensação da Cobrança adotarão as mesmas especificações de segurança contidas na última publicação do Manual de Segurança da RSFN. A Compensação de Boletos de Pagamento - CMP utilizará a versão 2 do protocolo de criptografia.
- II. Os arquivos transmitidos entre as Instituições Participantes da Compensação de Boletos de Pagamento – CMP à Nuclea são irrevogáveis, incondicionais e finais;
- III. Todos os arquivos enviados serão obrigatoriamente assinados digitalmente pelas Instituições Participantes emissor, com exceção, caso julgado necessário, dos relativos a testes de conectividade;

MANUAL TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 10/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



- IV. Todos os arquivos enviados serão obrigatoriamente criptografados com exceção dos relativos a testes de conectividade e a comunicação de erros de segurança.
- V. Todos os arquivos devem possuir uma identificação única garantindo sua rastreabilidade e unicidade de processamento;
- VI. Todas as Instituições Participantes da Compensação de Boletos de Pagamento - CM devem aderir às especificações de segurança da RSFN, bem como ao Protocolo de Segurança para troca dos arquivos, resguardada a utilização do protocolo 2 para a Compensação de Boletos de Pagamento – CMP;
- VII. Todo e qualquer arquivo gerado e enviado à Compensação de Boletos de Pagamento - CMP por uma de suas Instituições Participantes é de exclusiva responsabilidade de quem a originou;

5.6. Diretrizes

- I. Os participantes deverão utilizar certificado digital para o Compensação de Boletos de Pagamento - CMP, conforme especificações contidas neste manual.
- II. Os Certificados Digitais 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 Brasileiras - ICP-Brasil.
- III. As Instituições Participantes serão responsáveis pela segurança física e lógica de acesso a sua chave privada.
- IV. A configuração dos ambientes de teste e de produção da Compensação de Boletos de Pagamento - CMP nas Instituições Participantes deve obedecer aos padrões estabelecidos no Manual de Segurança da RSFN em vigência.
- V. As Instituições Participantes deverão criar e manter registros (logs) que capacitem a rastreabilidade e/ou a recomposição das transmissões de arquivos gerados na Compensação de Boletos de Pagamento - CMP, garantindo assim sua auditabilidade.
- VI. A Compensação de Boletos de Pagamento - CMP irá utilizar um certificado exclusivo e específico no padrão utilizado na Financial Net (RTM). Para os participantes que são usuários de outros sistemas da Nuclea na Financial Net (RTM), será permitida a utilização, em ambiente de Homologação e Produção, dos mesmos certificados de criptografia de arquivos utilizados nestes sistemas.

MANUAL TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 11/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



Para os demais participantes será necessária a utilização de certificado exclusivo para a Compensação de Boletos de Pagamento - CMP.

- a. É responsabilidade do participante comunicar a Nuclea que um certificado está sendo compartilhado entre mais de um de seus sistemas, no momento da adesão e nos períodos de troca;

5.7. Processos de ativação, substituição e revogação de certificado digital

Os certificados digitais utilizados para a criptografia e assinatura de arquivos no âmbito da Compensação de Boletos de Pagamento - CMP deverão respeitar os mesmos procedimentos e recomendações referentes à ativação, substituição e revogação conforme estabelecido no Manual de Segurança da RSFN em vigência.

5.8. Especificação para a Segurança dos Arquivos

Os arquivos criptografados e assinados no âmbito da Compensação de Boletos de Pagamento - CMP devem seguir as especificações de segurança contidas no Manual de Segurança da RSFN em vigência.

5.9. Certificado Compensação de Boletos de Pagamento - CMP

A Compensação de Boletos de Pagamento - CMP irá utilizar um novo Certificado para troca de arquivos com os Bancos.

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= ccccccc (onde ccccccc é o número base do CNPJ)

OU= CMP Pxxx ou Txxx

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

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

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

MANUAL TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 12/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



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

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

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

É vedado o reuso das chaves públicas utilizadas. Ao solicitar a emissão de um novo certificado para uso, é imperativo gerar uma nova chave pública. Certificados emitidos para ambientes diferentes (produção e homologação) devem conter chaves públicas diferentes.

É vedado o reuso, para qualquer finalidade, de CSR's (Certificate Signing Request) utilizados para a solicitação de certificados a serem utilizados no âmbito da Compensação de Boletos de Pagamento - CMP.

A troca de certificado seguirá os padrões de troca e instalação dos demais sistemas Nuclea que estão na RTM.

5.10. Exemplo ilustrativos de preenchimento de CSRS

Exemplo de primeiro certificado de produção da Nuclea (SP):

CN = cmp_p001.cip-bancos.org.br
OU = Câmara Interbancária de Pagamentos – CIP
OU = 02992335
OU = CMP P001
O = ICP-Brasil
C= BR

Exemplo de segundo certificado de Homologação

No caso do segundo certificado de homologação para um hipotético Banco XYZ com ISPB 12345678: CN = srv01.bancoxyz.com.br OU = Banco XYZ S.A.
OU = 12345678
OU = CMP T002
O = ICP-Brasil
C = BR

Obs.: 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

MANUAL TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 13/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



5.11. Processo de obtenção de habilitação de certificados

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.

A solicitação para a emissão de certificado é feita diretamente a uma Autoridade Certificadora, que deve ser consultada previamente para orientar o tipo de produto a ser adquirido e que atenda as especificações deste manual.

A AC (Autoridade Certificadora) atua como Autoridade Registradora e verifica os dados da solicitação e do preposto da instituição; - A AC, uma vez validados os dados, emite o certificado e envia este à solicitante, sob a forma de arquivo no padrão ASN.1.

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

6. CONTATOS

Nuclea			
Assunto	Contato	Telefone	E-mail
SILOC	CdE Clientes	(11) 4632-7320	siloc@cip-bancos.org.br

7. CONTROLE DO DOCUMENTO

7.1. HISTÓRICO DE ATUALIZAÇÃO

Versão	Rev.	Data de Publicação	Motivo/ Descrição	Responsável	Data de Vencimento
1	0		Versão Inicial	Infraestrutura de TI	Minuta
2	0		Alteração de usuários de conexão C:D e CFT	Infraestrutura de TI	Minuta
2	1		Alteração de do campo "DNS Names / IP do servidor C:D" na tabela do item 5.1	Infraestrutura de TI	Minuta

MANUAL TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 14/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



MINISTÉRIO

MANUAL TÉCNICO DO MÓDULO DE COMPENSAÇÃO DE BOLETOS DE PAGAMENTO - CMP

DENOMINAÇÃO: Manual de Integração e Segurança - Compensação de Boletos de Pagamento - CMP	CÓDIGO: MAPX-OPXXX-2022	FOLHA: 15/15
ÁREA EMITENTE: GERÊNCIA EXECUTIVA DE PROJETOS DE INFRAESTRUTURA	VIGÊNCIA: DD.MM.AAAA a DD.MM.AAAA	VERSÃO: 2.0



7.2. 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 7.1 HISTÓRICO DE ATUALIZAÇÃO deste documento.

7.3. GUARDA E RETENÇÃO

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

7.4. DISPONIBILIDADE DO DOCUMENTO

A última versão deste documento poderá ser obtida pelo site da NUCLEA na Internet no endereço:

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

7.5. CLASSIFICAÇÃO DA SEGURANÇA

Este documento é de caráter corporativo. É permitida a reprodução, cópia ou movimentação para fora das dependências da empresa somente com autorização formal do responsável pelo documento ou pessoa por ele designada.

NUCLEA, São Paulo, 30 de janeiro de 2023.