Manual de Segurança do SFN

Versão 5.06

Brasília, 1º de agosto de 2023.

Histórico de Revisão

Data	Versão	Descrição	Autores
22/11/2001		Elaboração	Grupo Técnico de Segurança SPB Associações, Câmaras e Banco Central
22/11/2001	1.0	1ª Revisão e Aprovação	Grupo Técnico de Segurança SPB Associações, Câmaras e Banco Central
22/02/2002	2.0	2ª Revisão	Grupo Técnico de Segurança SPB Associações, Câmaras e Banco Central
15/04/2002	2.1	3ª Revisão	Grupo Técnico de Segurança SPB Associações, Câmaras e Banco Central
20/11/2003	2.2	4ª Revisão	Bacen
14/12/2005	2.3	5ª Revisão	Bacen
18/12/2006	2.4	6ª Revisão	Bacen
04/11/2009	2.5	7ª Revisão	Bacen
01/03/2011	3.0	8ª Revisão	Bacen
25/03/2013	3.1	9ª Revisão	Bacen
08/04/2013	3.2	10ª Revisão	Bacen
23/03/2018	4.0	Ajustes gerais no leiaute do documento. Atualização da descrição do fluxo de mensagens de segurança.	Bacen
14/09/2018	4.01	Substituição das referências ao padrão Unicode UTF-16BE – a padronização de código encontra-se no Catálogo de Serviços do SFN.	Bacen
31/03/2020	4.02	Atualização para a Circular 3.970 e alteração da introdução para atualização do Manual.	Bacen
21/07/2020	4.03	Inclusão de referência para o Manual de Segurança do Pix.	Bacen
25/06/2021	5.00	Definição da terceira versão do Protocolo de Segurança; Alterações referentes ao número sequencial (agora número de controle) dos certificados digitais tipo SPB; Revisão geral do documento.	Bacen
23/12/2021	5.01	Alteração do item 5.1.3.2 e da Nota 2 da tabela do Anexo A – alteração do tamanho do IV do algoritmo AES	Bacen
29/03/2022	5.02	Alteração do item 5.1.8, após suspensão da implantação em produção da terceira versão do protocolo de segurança.	Bacen
27/04/2022	5.03	Inclusão da AC Soluti SPB na lista de ACs autorizadas a emitirem certificados no padrão SPB.	Bacen
15/07/2022	5.04	Alteração do item 5.1.8, para a implantação em produção da terceira versão do protocolo de segurança.	Bacen
23/05/2023	5.05	Alteração no escopo e introdução para incluir informações sobre o Pix nesta seção e alteração do protocolo de transferência de arquivos para o SFTP	Bacen
01/08/2023	5.06	Adiamento de prazos de implantação do SFTP.	Bacen

Este manual foi publicado pelo Departamento de Tecnologia da Informação do Banco Central do Brasil – Deinf, conforme competência expressa na Circular 3.970, de 28 de novembro de 2019.

Índice

1 Introdução

1.1 Objetivo

Este manual tem por objetivo estabelecer os requisitos e recomendações de segurança para os serviços de transferência de mensagens e arquivos no âmbito do SFN, incluindo definições sobre criptografia, protocolos, algoritmos e certificação digital. Os requisitos de segurança aqui definidos são implementados para garantir a integridade, a confidencialidade, a disponibilidade e o não repúdio das informações trafegadas.

1.2 Processo de alteração do manual

O requerimento para alterações deste manual deverá ser encaminhado ao Gestor do Manual de Segurança, no Banco Central do Brasil (Bacen), por meio de Documento de Requisitos Técnicos (DRT), cujo modelo para preenchimento está disponível para download no site do Bacen. Durante o processo de avaliação do DRT, o Gestor do Manual poderá solicitar complementações ou alterações no documento encaminhado pelo requisitante ou ainda consultar os gestores de serviços, participantes da RSFN e as unidades de negócio do Bacen. O Gestor do Manual de Segurança efetuará as devidas adequações e publicará uma nova versão deste Manual no site do Bacen.

São gestores de serviços na Rede do Sistema Financeiro Nacional (RSFN) o Bacen, a Secretaria do Tesouro Nacional, Brasil, Bolsa, Balcão – B3 e Câmara Interbancária de Pagamentos – CIP.

A definição dos requisitos de segurança deve ser baseada em padrões conhecidos e utilizados no mercado, sem eleger um produto/fornecedor, de modo que os participantes possam avaliar o custo/benefício de desenvolvimento próprio ou das diversas soluções de fornecedores de hardware e software de segurança presentes no mercado.

1.3 Sobre o Pix

Este manual é parte integrante da regulamentação do ecossistema tecnológico de pagamentos instantâneos brasileiro – Pix, Todavia, o Pix possui requisitos de segurança específicos que estão estabelecidos no Manual de Segurança do Pix, disponível na página da Comunicação Eletrônica de Dados no âmbito do SFN.

No contexto deste manual, não são aplicáveis ao Pix o processo de habilitação e ativação de certificados dos participantes e as especificações de segurança para mensagens e arquivos que se referem aos domínios de mensageria do SPB e MES

2 Escopo

As recomendações e os padrões aqui contidos serão utilizados na Rede do Sistema Financeiro Nacional (RSFN), e poderão ser utilizados em outras aplicações relacionadas aos mesmos participantes.

3 Política de Segurança da RSFN

3.1 Sumário

A Política de Segurança é um capítulo que contém as regras de conduta para acesso ao ambiente da RSFN e administração da estrutura de segurança. Este capítulo define qual a abrangência da atuação dessa estrutura, bem como os métodos necessários para minimizar as possibilidades de sua violação.

A estrutura de segurança compreende todos os mecanismos de proteção necessários para fortalecer os sistemas de defesa dos ativos computacionais contra ações indesejáveis. Os mecanismos são compostos por software, hardware e procedimentos específicos para segurança.

3.2 Abreviaturas

No final de cada Diretriz se encontram as seguintes abreviações:

(OB) Obrigatório: Item de implementação obrigatória.

(RE) Recomendado: Item de implementação recomendada.

3.3 Conscientização

Os fornecedores, usuários da RSFN e demais pessoas ou empresas relacionadas devem ser informados (ou ter meios para tomar ciência) sobre a existência e a extensão de medidas, práticas, procedimentos e órgãos responsáveis para a segurança dos sistemas de informação na RSFN.

As medidas e os procedimentos para a segurança dos sistemas de informação devem ser coordenados e integrados entre si e com outros princípios e procedimentos adotados pela Instituição Participante, de modo a criar um sistema coerente de segurança passível de avaliações periódicas.

3.4 Objetivo

Definir uma Política de Segurança visando estabelecer diretrizes para as Instituições participantes da RSFN sobre a segurança da informação, para garantir a integridade, a confidencialidade, a disponibilidade e o não repúdio das mensagens e dos arquivos trafegados.

3.5 Premissas

3.5.1 Os serviços da RSFN, incluindo a infraestrutura de rede, roteamento de mensagens e aplicações em geral, devem estar disponíveis pelo período estabelecido no regulamento do Bacen.

3.5.2 As mensagens transmitidas entre os participantes e o Bacen são irrevogáveis, incondicionais e finais.

3.5.3 Todas as mensagens e os arquivos enviados à RSFN serão obrigatoriamente autenticados por meio de criptograma (assinados digitalmente) pela Instituição Participante emissora, com exceção, caso julgado necessário, das mensagens relativas

a testes de conectividade, das relativas a consulta de certificados digitais e das relativas a comunicação de erros de segurança.

3.5.4 Todas as mensagens enviadas à RSFN serão obrigatoriamente criptografadas com exceção das relativas a testes de conectividade, das relativas a consulta de certificados digitais e das relativas a comunicação de erros de segurança, além das emitidas sem destinatário específico (ver item 5.6.2).

3.5.5 Todas as mensagens devem possuir uma identificação única garantindo sua rastreabilidade e unicidade de processamento.

3.5.6 Todas as aplicações devem ser testadas e homologadas junto ao ambiente de homologação do Bacen, quanto às suas funcionalidades, antes de disponibilizadas ao ambiente de produção.

3.5.7 Todas as Instituições devem aderir às especificações de segurança do SPB, bem como ao Protocolo de Segurança para troca de mensagens e arquivos.

3.5.8 Toda e qualquer mensagem ou arquivo gerado e enviado à RSFN por um de seus participantes é de exclusiva responsabilidade de quem o originou.

3.6 Diretrizes

3.6.1 Todas as conexões da RSFN deverão estar configuradas de acordo com as normas de segurança da(s) concessionária(s) fornecedora(s) da infra-estrutura de telecomunicação **(OB)**.

3.6.2 O participante deverá criar e manter Plano de Contingência adequado para suportar sinistros **(RE)**.

3.6.3 O Plano de Contingência deve ser mantido atualizado e ter mecanismos de validação que garantam sua eficácia **(RE)**.

3.6.4 Os participantes devem possuir, preferencialmente, ambiente redundante, incluindo elementos de rede e de processamento, para garantia de disponibilidade do serviço **(RE)**.

3.6.5 As Câmaras, Aglomerados e Conglomerados devem possuir ambiente redundante, incluindo elementos de rede e de processamento, para garantia de disponibilidade do serviço **(OB)**.

3.6.6 As Instituições serão responsáveis pela segurança física e lógica de acesso a sua chave privada **(OB)**.

3.6.7 A Instituição deve armazenar a chave privada num dispositivo especializado para o gerenciamento de chaves criptográficas, visando diminuir a exposição do sistema a falhas e outros tipos de vulnerabilidades do ambiente **(RE)**.

3.6.8 A Instituição deve proteger o acesso físico e lógico às rotinas e recursos geradores de mensagens para o SPB **(RE)**.

3.6.9 Os certificados digitais e seus correspondentes pares de chaves criptográficas utilizados no SPB não deverão ser utilizados em outros domínios (Ex.: MES – Mensageria Sisbacen) **(RE)**.

3.6.10 As Instituições deverão criar e manter sistemática de Segurança da Informação visando assegurar a confidencialidade, a integridade, a autenticidade, o não repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis **(OB)**.

3.6.11 A configuração dos ambientes de homologação e de produção da RSFN nas Instituições deve obedecer aos padrões estabelecidos no Manual de Redes do SFN **(OB)**.

3.6.12 As Instituições deverão criar e manter procedimentos de backup que garantam a recuperação do ambiente e dos dados trafegados **(RE)**.

3.6.13 As Câmaras, Aglomerados e Conglomerados deverão criar e manter procedimentos de backup que garantam a recuperação do ambiente e dados trafegados **(OB)**.

3.6.14 As Instituições deverão criar e manter mecanismos de controle do ambiente quanto a alterações no mesmo, visando à identificação e rastreabilidade das intervenções executadas **(OB)**.

3.6.15 As Instituições deverão criar e manter registros que capacitem a rastreabilidade e/ou a recomposição das transações geradas no SPB, garantindo assim sua auditabilidade **(OB)**.

3.6.16 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 Brasileira - ICP-Brasil **(OB)**.

3.6.17 As Instituições, visando a melhoria da segurança, devem seguir a norma NBR ISO/IEC 27002:2005 editada pela ABNT **(RE)**.

4 Certificação digital na RSFN

4.1 Credenciamento de Autoridades Certificadoras

4.1.1 A Autoridade Certificadora (AC) interessada em fornecer Certificados Digitais às Instituições participantes do SPB, deverá estar devidamente credenciada junto a ICP-Brasil.

4.1.2 O credenciamento da AC se dará segundo os procedimentos da resolução nº 6 do Comitê Gestor da ICP-Brasil, de 22 de novembro de 2001 e normativos posteriores.

4.1.3 A AC deverá ter uma PC (Política de Certificação) específica para emissão de Certificados Digitais para o SPB.

4.1.4 Os Certificados padrão SPB emitidos para as Instituições participantes da RSFN serão tipo A1, (OID=2.16.76.1.2.1.n), com pequenas alterações descritas no item 4.2.

4.1.5 O bit DataEncipherment estará desativado em certificados de assinatura digital, na extensão "Key Usage".

4.1.6 A frequência de emissão de LCR será de uma hora, e nesta deverão constar apenas os Certificados revogados padrão SPB.

4.1.7 Para mais informações, consultar as resoluções da ICP-Brasil.

4.2 Especificações para a geração de Certificados Digitais padrão SPB

4.2.1 Campos obrigatórios a serem incluídos no CSR:

C=BR
O=ICP-Brasil
OU=ISPB-cccccccc
OU=SISBACEN-iiiii
CN=Identificação única da instituição certificada e do certificado (ex: P ou T + número de controle, segundo informação da IF)

4.2.2 Os certificados emitidos para o ambiente de produção serão identificados pelo conteúdo do campo "CN", com a letra "P". Os certificados emitidos para o ambiente de homologação deverão conter a letra "T". Caso um certificado seja identificado para um ambiente (produção ou homologação), o seu par de chaves correspondente não poderá ser usado no outro.

4.2.3 O campo CN deverá ser constituído pela razão social da instituição, seguida de um espaço em branco (“ “), acrescido da sequência "Xnnn", em que "nnn" é um número de controle da geração do par de chaves, em cada ambiente (produção ou homologação), dentro da instituição. No caso de instituições com mais de uma entidade certificada, deverá ser acrescido à sua razão social o departamento, sistema ou identificação da atividade.

i. Para o ambiente de Homologação, o número de controle não precisará mais ser único a partir de 8/9/21.

ii. Para o ambiente de Produção, o número de controle não precisará mais ser único a partir de 2/10/21.

4.2.4 Exemplos ilustrativos de preenchimento do campo CN:

CN=Banco Central do Brasil P001
CN=Banco Central do Brasil - SELIC P001
CN=Banco do Brasil T001
CN=Bolsa de Mercadoria e Futuros - Cambio T002
(Obs: a palavra Câmbio foi propositadamente grafada sem acentuação para atender ao disposto no item 7.1.5 da resolução nº 7 do Comitê Gestor da ICP-Brasil)

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

4.2.6 No bloco de identificação da entidade emissora (ISSUER) do certificado, deverá ser incluído pela AC o código que lhe for atribuído pelo Banco Central do Brasil, na forma:

OU=CSPB-1 (Serpro); ou
OU=CSPB-2 (Certisign); ou
OU=CSPB-4 (Serasa); ou
OU=CSPB-5 (CAIXA); ou
OU=CSPB-6 (Valid); ou
OU=CSPB-7 (Soluti).

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

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

4.2.9 É vedado o reuso das chaves públicas utilizadas no âmbito da RSFN em quaisquer outros certificados digitais. Ao solicitar a emissão de um novo certificado para uso nos ambientes da RSFN, é imperativo gerar uma nova chave pública. Certificados emitidos para ambientes diferentes (produção e homologação) devem conter chaves públicas diferentes.

4.2.10 É vedado o reuso, para qualquer finalidade, de CSRs utilizados para a solicitação de certificados a serem utilizados no âmbito da RSFN.

4.3 Exemplos ilustrativos de preenchimento de CSRs

4.3.1 No caso do primeiro certificado de produção do Bacen (Brasília):

C=BR
O=ICP-Brasil
OU=ISPB-00038166
OU=SISBACEN-DEINF
CN=Banco Central do Brasil P001
L=Brasilia
S=Distrito Federal

4.3.2 No caso do segundo certificado de homologação para um hipotético Banco XYZ:

C=BR
O=ICP-Brasil
OU=ISPB-31123578 (supondo o número base do CNPJ ser 31123578)
OU=SISBACEN-04123 (supondo o código do Sisbacen ser 04123)
CN=Banco XYZ S.A. T002
L=Sao Paulo
S=Sao Paulo

4.3.3 No caso do terceiro certificado de produção do Bacen - SELIC (RJ):

C=BR
O=ICP-Brasil
OU=ISPB-00038121
OU=SISBACEN-DEMAB
CN=Banco Central do Brasil - Selic P003
L=Rio de Janeiro
S=Rio de Janeiro

4.4 Processo de obtenção e habilitação de certificados

4.4.1 A Instituição, seguindo a orientação dos procedimentos de seu software específico de segurança, gera par de chaves assimétricas RSA e um arquivo CSR, no padrão PKCS#10.

4.4.2 A solicitação para a emissão de certificado é feita diretamente a uma AC.

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

4.4.4 A Instituição que solicita o certificado digital é responsável por informar corretamente à Autoridade Certificadora seu código ISPB e Sisbacen. Também é responsável por verificar a sua habilitação junto ao Bacen para uso dos sistemas de mensageria, não sendo esta uma atribuição da AC.

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

4.4.6 A Instituição envia ao Bacen o certificado padrão SPB através do Sistema de Transferência de Arquivos do Banco Central (STA).

4.4.7 Ao enviar através do STA, a Instituição deverá informar o código do arquivo CERTSPB (documento CSPB - Certificado Digital da Instituição no SPB) ou CERTMES (documento CMES - Certificado Digital da Mensageria Sisbacen).

4.4.8 O Bacen verifica a duplicidade da chave pública e a consistência dos dados registrados e confirma a habilitação do certificado no próprio registro de protocolo de envio.

4.4.9 Os certificados habilitados serão arquivados em bases de dados do Bacen, onde, além do seu conteúdo integral, constarão os seguintes dados: AC, série, instituição, validade, situação e chave pública.

4.4.10 Os certificados habilitados só poderão ser efetivamente utilizados no âmbito do SPB ou do MES após a sua ativação. Cada Instituição terá apenas um certificado ativado por vez em cada domínio e ambiente de produção ou homologação.

4.4.11 O certificado habilitado para o SPB deverá ser ativado, com envio de mensagem GEN0006 ao Bacen, somente no domínio SPB01. Após o envio e processamento da mensagem, este certificado estará ativo para os domínios SPB01 e SPB02, simultaneamente.

4.4.12 O certificado habilitado para o MES deverá ser ativado, com envio de mensagem GEN0006 ao Bacen, somente no domínio MES01. Após o envio e processamento da mensagem, este certificado estará ativo para os domínios MES01, MES02 e MES03, simultaneamente.

4.4.13 No caso da existência de mais de um ambiente de homologação em um mesmo domínio (por exemplo, ambiente de pré-produção), poderão ser usados certificados diferentes para a geração de criptogramas de autenticação de mensagens e arquivos em

ambientes de homologação distintos. Para cada ambiente, ainda que usando o mesmo certificado, deverá haver um processo de ativação independente.

4.4.14 Poderá haver mais de um certificado habilitado a qualquer tempo, mas apenas um estará ativo em cada domínio/ambiente.

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

4.4.16 Só poderão ser habilitados e ativados os certificados com chave RSA de 2048 bits.

4.5 Processos de ativação, substituição e desativação de certificados

4.5.1 Os certificados habilitados, na forma do item 4.4, estarão disponíveis para ativação, que poderá ser inicial, no caso do primeiro certificado, ou de substituição, pelo encerramento da validade ou revogação de um certificado ativado.

4.5.2 Para ativar certificados, tanto inicialmente como por substituição, a instituição emitirá mensagem específica (GEN0006). Esta mensagem será obrigatoriamente assinada pela chave privada correspondente à chave pública veiculada pelo certificado que está sendo ativado. Será enviada uma mensagem de confirmação ou de erro, informando o resultado da operação.

4.5.3 Na ativação de cada certificado das Instituições Participantes, o Bacen emitirá mensagem de "broadcast" (GEN0007), em que constam os dados de identificação do novo certificado.

4.5.4 As mensagens de ativação de certificado deverão ser encaminhadas, preferencialmente, em momento posterior ao fechamento dos sistemas que utilizam o certificado, ou em momento em que não haja processamento de mensagens.

4.5.5 A Instituição deve evitar ativar os seus certificados em dia coincidente ao da ativação do certificado do Bacen.

4.5.6 Os certificados ativos estarão disponíveis no site www.bcb.rsfn.net.br, no arquivo Ativados.zip.

4.5.7 A substituição dos certificados do Bacen, quando do seu vencimento, em qualquer ambiente (produção ou homologação) e domínio (SPB ou MES), será previamente comunicada no site www.bcb.rsfn.net.br e por meio da mensagem GEN0018, nos domínios SPB01 ou MES01, conforme o caso, enviada a todas as instituições com certificados ativados. O envio da mensagem ocorrerá com antecedência de pelo menos 3 dias úteis em relação à data estabelecida para a substituição, a qual coincidirá preferencialmente, com uma sexta-feira, em ambiente de homologação, e com um sábado, em ambiente de produção. A efetiva substituição do certificado digital do Bacen se dará na data estabelecida pela GEN0018. O Bacen (ISPB “00038166”) não envia mensagens GEN0007 após a troca do seu certificado.

4.5.8 Os certificado ativos da Instituição e do Bacen para o domínio MES01 são os mesmos certificados ativos para os domínios MES02 e MES03. Os certificado ativos da Instituição e do Bacen para o domínio SPB01 são os mesmos certificados ativos para o domínio SPB02.

4.5.9 Para a habilitação do primeiro certificado no ambiente de produção, a Instituição já deverá ter ativado pelo menos um certificado no ambiente de homologação.

4.5.10 A ativação de um novo certificado pela Instituição automaticamente desativará o anterior.

4.5.11 Todo certificado será automaticamente invalidado para uso no âmbito da mensageria 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 “08/11/2006 15:34:06” em seu campo Válido Até será desativado às 24 horas do dia 07/11/2006.

5 Especificações para Segurança de Mensagens e Arquivos

5.1 Cabeçalho ("header") de segurança

Todas as mensagens e arquivos eletrônicos trocados no âmbito da RSFN devem iniciar com uma sequência de 588 bytes - o cabeçalho de segurança, responsável pela implementação dos mecanismos de geração de criptogramas de autenticação e criptografia dos mesmos.

A seguir são enumerados e codificados os campos do cabeçalho, com a sua respectiva localização, descrição e forma de preenchimento, referente à segunda e à terceira versões do Protocolo de Segurança. Para informações sobre a primeira versão do Protocolo, consultar as versões do Manual de Segurança anteriores à 3.0.

Tabela 1 - Cabeçalho de segurança

Campo	Posição	Descrição do Campo	Conteúdos Possíveis
C01	001-002	Tamanho total do Cabeçalho	024CH: Fixo (588 bytes)
C02	003-003	Versão do Protocolo de Segurança	00H: Em claro 02H: Segunda versão 03H: Terceira versão (vide item 5.1.8)
C03	004-004	Código de erro	Vide tabela de erros no item 5.5
C04	005-005	Indicação de tratamento especial	Vide item 5.6
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) – aceito apenas na segunda versão do Protocolo de Segurança (vide item 5.1.2) 02H: AES com chave de 256 bits – aceito apenas na terceira versão do Protocolo de Segurança (vide item 5.1.3)
C08	009-009	Algoritmo da chave assimétrica local	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	PC do certificado digital do destino	01H: SPB-Serpro 02H: SPB-Certisign 03H: Pessoas Físicas 04H: SPB-Serasa 05H: SPB-CAIXA 06H: SPB-Valid 07H: SPB-Soluti
C11	012-043	Série do certificado digital do destino	Identificador único do certificado na AC (vide item 5.1.4)
C12	044-044	PC do certificado digital da Instituição	01H: SPB-Serpro 02H: SPB-Certisign 03H: Pessoas Físicas 04H: SPB-Serasa 05H: SPB-CAIXA 06H: SPB-Valid 07H: SPB-Soluti
C13	045-076	Série do certificado digital da Instituição	Identificador único do certificado na AC (vide item 5.1.4)

C14	077-332	Buffer de criptografia da chave simétrica	Chave de criptografia simétrica 3DES – segunda versão do Protocolo de Segurança – ou chave de criptografia simétrica AES-256 concatenada com o IV (Initialization Vector) – terceira versão do Protocolo de Segurança – cifrada por PKCS#1v1_5
C15	333-588	Buffer do criptograma de autenticação	Hash (20 ou 32 bytes) assinado pelo PKCS#1v1_5

5.1.1 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".

5.1.2 Na segunda versão do Protocolo de Segurança, a ser descontinuada conforme cronograma previsto no item 5.1.8, deve ser utilizado o 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.

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

5.1.3 Na terceira versão do Protocolo de Segurança, instituída a partir das datas previstas no item 5.1.8, deve ser utilizado o algoritmo de criptografia simétrica AES, com chave de 256 bits, no modo de operação GCM (Galois/Counter Mode).

5.1.3.1 A operação de criptografia deve seguir o padrão AEAD_AES_256_GCM, previsto na RFC 5116.

5.1.3.2 O Vetor de Inicialização (IV – “Initialization Vector” – ou “nonce”) deve ser composto de 96 bits (12 bytes) gerados aleatoriamente.

5.1.3.3 A entrada “Associated Data” (AD) da operação criptográfica deve ser vazia, contendo 0 (zero) bytes.

5.1.3.4 A tag de autenticação deve ter 128 bits (16 bytes), e deve ser apensada ao final do criptograma gerado pela operação de criptografia. A tag não precisa constar no cabeçalho de segurança.

5.1.4 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".

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

5.1.6 O valor 03H do campo C12 do cabeçalho de segurança (PC do certificado digital da Instituição) está reservado para o sistema STR-WEB. A autenticação das mensagens nesse caso é feita utilizando-se certificado digital A3 de Pessoa Física emitido na ICP-Brasil. A aplicação é responsável por gerar o cabeçalho de segurança.

5.1.7 Deve-se utilizar o algoritmo de hash SHA-256 em criptogramas de autenticação gerados com chaves de 2048 bits.

5.1.8 A terceira versão do Protocolo de Segurança está implantada, no ambiente de homologação dos domínios da mensageria, desde 7/3/22. A implantação no ambiente de produção será realizada conforme cronograma abaixo.

I – Para o ambiente de Produção dos domínios de mensageria SPB01, MES01, MES02 e MES03:

a) A partir de 27/8/22, às 9h, todas as mensagens e arquivos desses domínios deverão utilizar somente a versão 3 do Protocolo de Segurança.

II – Para o ambiente de Produção do domínio de mensageria SPB02 (somente mensagens e arquivos do grupo de serviços DDA):

a) A partir de 27/8/22, às 9h, todas as mensagens e arquivos desse domínio poderão utilizar as versões 2 e 3 do Protocolo de Segurança.
b) A partir de 11/9/22, às 9h, todas as mensagens e arquivos desse domínio deverão utilizar somente a versão 3 do Protocolo de Segurança.

5.1.9 Conforme cronograma descrito no item 5.1.8, o Bacen passará a utilizar a terceira versão do Protocolo de Segurança, deixando de utilizar o algoritmo de criptografia simétrica 3DES e passando a utilizar o AES, com chaves de 256 bits, no modo de operação GCM e, portanto, todas as Instituições deverão estar aptas a utilizá-lo para comunicação com o Bacen.

5.1.10 Referências:

RSA (ANSI X9.31);
Triple-DES (ANSI X9.52, FIPS 46-3);
AES (FIPS 197);
GCM (NIST Special Publication 800-38D);
MD5, SHA-1, SHA-256 (FIPS 180-1);
CBC (FIPS-81);
Certificado Digital (X.509 v3).

5.2 Agregação da segurança na emissão de mensagens e arquivos

5.2.1 O cabeçalho de segurança não tem código de página, é sempre binário.

5.2.2 A mensagem que sucede os 588 bytes do cabeçalho deve ser apresentada em XML, nas codificações previstas no Catálogo de Serviços do SFN.

5.2.3 Na segunda versão do Protocolo de Segurança, devido à utilização do algoritmo 3DES, o tamanho da mensagem deve ser tornado múltiplo de 8 bytes, adotando-se, caso necessário, um "padding" de zeros binários. Na terceira versão do Protocolo, onde se utiliza o algoritmo AES, o “padding” não deve ser realizado.

5.2.4 Calcula-se o "hash" do conteúdo da mensagem ou arquivo, com o “padding” (se houver), na codificação prevista no Catálogo de Serviços do SFN, indicando o algoritmo utilizado (campo C09).

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

5.2.6 O número do certificado deve ser ASCII com zeros (0x30) à esquerda, caso necessário (vide item 5.1.4).

5.2.7 Gera-se o criptograma de autenticação (anotando o resultado do "hash" do conteúdo – incluindo o “padding”, se houver) com a chave privada correspondente ao certificado do participante emissor, anotando o resultado no campo C15.

5.2.8 Sorteia-se chave simétrica (Triple-DES 192 bits – no caso da segunda versão do Protocolo de Segurança – ou AES 256 bits – no caso da terceira versão do Protocolo) e cifra-se a mensagem ou o arquivo. Deve ser gerada uma nova chave simétrica para cada mensagem ou arquivo a ser cifrado.

5.2.9 Cifra-se a chave simétrica utilizada na cifragem com a chave pública correspondente ao certificado digital do destinatário, com o resultado no campo C14.

5.3 Verificação da segurança para a recepção de mensagens e arquivos

5.3.1 Verificam-se os certificados envolvidos (se existem e estão habilitados), conferindo se correspondem ao receptor (campos C10/C11) e emissor da mensagem ou arquivo (campos C12/C13).

5.3.2 No caso do Bacen, para as mensagens GEN0001, GEN0006 e GEN0008, o certificado correspondente ao emissor pode não ter sido ativado. Nos demais casos, deve ter sido previamente ativado.

5.3.3 Abre-se a informação da chave simétrica de cifragem da mensagem ou arquivo com a chave privada correspondente à chave pública do certificado.

5.3.4 Decifra-se o conteúdo da mensagem ou arquivo (a partir da posição 589) – inclusive o "padding", se houver.

5.3.5 Calcula-se o "hash" do conteúdo da mensagem ou arquivo, na codificação prevista no Catálogo de Serviços do SFN, com o "padding", se houver, de acordo com o algoritmo indicado em C09.

5.3.6 Confere-se o criptograma de autenticação, comparando o "hash" obtido.

5.3.7 Se houver qualquer erro no decorrer do processo de recepção da mensagem, deve ser emitida uma mensagem GEN0004, reportando o código de erro (EGEN99xx).

5.4 Geração de arquivos de auditoria (logs) das mensagens trafegadas

5.4.1 As mensagens enviadas e as recebidas de forma correta deverão ser gravadas em arquivos de “log”, contendo os seguintes campos, conforme tabela abaixo:

Tabela 2 - Arquivo de auditoria de mensagens

Posição	Formato	Descrição
001-010	ASCII	Tamanho do registro (cabeçalho + mensagem XML=TAM)
011-024	ASCII	Timestamp da mensagem no formato AAAAMMDDHHMMSS
025-032	ASCII	Código ISPB Origem
033-040	ASCII	Código ISPB Destino
041-064	Binário	Identificador da mensagem no MQ-Series
065-652	Binário	Cabeçalho de segurança completo
653-TAM	Unicode	Mensagem em claro (codificação original da mensagem – incluindo o “padding”, se houver)

5.4.2 O arquivo de log deverá ser gerado com periodicidade diária, recomendando-se a identificação da data em seu nome.

5.4.3 O arquivo de log deverá ser constituído de uma sequência contínua de registros de tamanho variável.

5.4.4 O aplicativo V_LogSPB, elaborado apenas para ambiente Windows, será disponibilizado pelo Bacen no site www.bcb.rsfn.net.br, para validação dos arquivos de log.

5.4.5 O prazo de retenção e de consequente possibilidade de recuperação de registros nos arquivos de "log" é de 10 (dez) anos, contados a partir da emissão de cada registro.

5.4.6 As mensagens recebidas com erros na camada de segurança ou no bloco de controle (BCMSG), deverão ser gravadas em arquivos distintos, com retenção de 5 dias, para eventual facilidade de correção.

5.4.7 As Instituições Financeiras devem apresentar seus arquivos de log no padrão especificado no item 5.4.1 acima, ou alternativamente utilizar aplicativo conversor para o padrão especificado, a ser usado sob demanda da fiscalização do Banco Central do Brasil.

5.5 Tratamentos de erros na recepção das mensagens

5.5.1 A seguir são relacionados os códigos de erros passíveis de anotação, a partir da recepção de mensagens inválidas:

Tabela 3 - Erros de segurança na recepção de mensagens

Erro	GEN0004	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 do certificado digital da Instituição inválido ou divergente do certificado
06H	EGEN9906	C09	Algoritmo de "hash" não corresponde ao indicado ou é inválido
07H	EGEN9907	C10	Código da PC 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 PC do certificado inválido
0AH	EGEN9910	C13	Número de série do certificado digital da Instituição inválido (não foi emitido pela AC)
0BH	EGEN9911	C15	Criptograma de autenticação da Mensagem inválido ou com erro
0CH	EGEN9912	C12/13	Certificado não é do emissor da mensagem (titular da fila no MQ)
0DH	EGEN9913	C14	Erro na extração da chave simétrica
0EH	EGEN9914	C14	Erro gerado pelo algoritmo simétrico
0FH	EGEN9915	mensagem	Tamanho da mensagem não múltiplo de 8 bytes (específico para a segunda versão do Protocolo de Segurança)
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 (Usar certificado “a ativar” na GEN0006)

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

5.5.3 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.

5.5.4 Deve ser enviada uma mensagem GEN0004, com o erro EGEN99nn correspondente, onde o cabeçalho de segurança indicará o erro.

5.5.5 As mensagens recebidas com o campo "C03" não deverão ser respondidas, servindo apenas como base para identificação de erros apontados.

5.5.6 A mensagem GEN0004 faz referência à identificação do MQ da mensagem inválida detectada.

5.5.7 De modo a evitar a proliferação de erros, as mensagens GEN0004 são apenas assinadas, com o seu campo C04 apresentando o valor 3.

5.5.8 Quando se referir a erros fora do escopo de segurança, tais como a identificação do bloco BCMSG e/ou de "parsing" deste, o cabeçalho das mensagens GEN0004 deverá conter o erro FFH (hexadecimal "FF").

5.6 Códigos Indicativos de Tratamentos especiais quanto à segurança

5.6.1 O campo C04 do cabeçalho normalmente será preenchido com zeros binários, indicando tratar-se de mensagem ou arquivo assinado e cifrado.

5.6.2 Excepcionalmente nas condições abaixo, poderá assumir os seguintes valores:

"1" - Mensagem que utiliza um certificado digital ainda não ativado (opcionalmente nas mensagens dos eventos GEN0001 e GEN0008, obrigatoriamente na mensagem GEN0006);

"2" - Mensagem não cifrada para o destinatário (somente nos casos de "broadcast" público, isto é, mensagens sem destinatário específico);

"3" - Mensagem não cifrada que pode ser relativa à segurança (opcionalmente nas mensagens dos eventos GEN0001, GEN0004 e GEN0008, obrigatoriamente na mensagem de erro GEN0006E – a partir da versão 4.11 do Catálogo de Serviços do SFN);

"4" - Indicativo de arquivo não compactado, normalmente gerado como resposta a uma mensagem;

"6" - Indicativo de arquivo não compactado, sem cifragem, normalmente de uso público;

"8" - Indicativo de arquivo compactado segundo o padrão Zip.

"10" - Indicativo de arquivo compactado segundo o padrão Zip, sem cifragem, normalmente de uso público.

5.6.3 A mensagem GEN0001 (ECO) pode ser usada para testes em geral, podendo ser emitida com qualquer valor de 0 a 3, ou ainda com todos os campos do cabeçalho zerados, exceto o primeiro (tamanho).

5.7 Troca de arquivos através de servidores FTP

5.7.1 Haverá servidores FTP distintos, no domínio SPB e no domínio MES, para que as instituições enviem ou recebam os arquivos solicitados.

5.7.2 O servidor de FTP será obrigatório apenas na situação em que haja tráfego de arquivos no respectivo domínio de sistema (MES e/ou SPB).

5.7.3 Cada provedor (Bacen, Selic e Câmaras) deverá ter o seu próprio servidor FTP, observado o domínio a que pertencem os arquivos trafegados. Arquivos destinados ao SPB não poderão ser armazenados no servidor FTP do domínio MES e vice-versa.

5.7.4 O padrão de nome dos servidores do domínio SPB será: ftp-p.<instituição>.rsfn.net.br para o servidor de produção e ftp-t.<instituição>.rsfn.net.br para o servidor de homologação.

5.7.5 O padrão de nomes dos servidores do domínio MES será: ftp-p.mes.<instituição>.rsfn.net.br para o servidor de produção e ftp-t.mes.<instituição>.rsfn.net.br para o servidor de homologação.

5.7.6 Para o ambiente PPRO, quando disponível, serão considerados, para o tráfego de arquivos, os servidores de homologação do respectivo domínio de sistema.

5.7.7 O servidor FTP não terá mecanismo de segurança próprio. A segurança será feita através dos mecanismos de criptografia e geração de criptograma de autenticação dos arquivos semelhantes aos da Mensageria. A partir das datas definidas no item 5.1.8, o algoritmo de criptografia simétrica utilizado para cifrar os arquivos será o AES-256.

5.7.8 O servidor FTP deverá ser configurado para criar logs de acessos totais, contendo usuário, endereço IP, data/hora e atividade realizadas.

5.7.9 Cada Instituição terá um único usuário para Logon.

5.7.10 O nome de usuário será o ISPB da Instituição.

5.7.11 Cada Instituição terá acesso aos seguintes diretórios:

/publico (acesso de leitura para todos os usuários)

/nnnnnnnn/download (acesso de leitura do usuário nnnnnnnn)

/nnnnnnnn/upload (acesso de gravação do usuário nnnnnnnn)

Obs. nnnnnnnn é o nome do usuário, conforme especificado no item 5.7.10.

5.7.12 O provedor de serviço FTP poderá remover o arquivo do diretório após 03 dias úteis da sua data de disponibilização.

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

5.7.14 No caso de arquivos compactados deve ser usado o algoritmo ZIP. Para a geração de criptograma de autenticação o tamanho do arquivo compactado deverá ser transformado em múltiplo de 08 bytes pelo uso de “padding” de zeros binários, caso necessário, conforme itens 5.2.3 e 5.2.4. Mesmo após a decifragem (se for o caso) e conferência do criptograma de autenticação o “padding” não deverá ser removido.

OBS: A partir das datas definidas no item 5.1.8, o algoritmo de criptografia simétrica utilizado para cifrar os arquivos será o AES-256, no modo de operação GCM, sem “padding”.

5.7.15 A senha FTP inicial gerada para cada usuário será o próprio nome.

5.7.16 A troca de senhas para os servidores FTP dar-se-á conforme critérios de cada provedor.

5.7.17 Os servidores FTP serão desativados no ambiente de homologação e no ambiente de produção em datas a serem definidas, por comunicado, pelo Bacen. Nessas datas, serão implantados os servidores SFTP nesses ambientes, conforme detalhamento na seção 5.8.

5.7.18 Todos os prestadores de serviço FTP deverão seguir as mesmas datas acima para efetivar a migração do serviço para SFTP.

5.8 Troca de arquivos através de servidores SFTP

5.8.1 O serviço SFTP (Secure File Transfer Protocol) será implantado no ambiente de homologação e em produção em datas a serem definidas, por comunicado, pelo Bacen. As datas valem para todos os prestadores de serviço de transferência de arquivos.

5.8.2 Haverá servidores SFTP distintos, no domínio SPB e no domínio MES, para que as instituições enviem ou recebam os arquivos solicitados.

5.8.3 O servidor SFTP será obrigatório apenas na situação em que haja tráfego de arquivos no respectivo domínio de sistema (MES e/ou SPB).

5.8.4 Cada prestador deverá ter o seu próprio servidor SFTP, observado o domínio a que pertencem os arquivos trafegados. Arquivos destinados ao SPB não poderão ser armazenados no servidor SFTP do domínio MES e vice-versa.

5.8.5 O padrão de nome dos servidores do domínio SPB será: sftp-p.spb.<instituição>.rsfn.net.br para o servidor de produção e sftp-h.spb.<instituição>.rsfn.net.br para o servidor de homologação.

5.8.6 O padrão de nomes dos servidores do domínio MES será: sftp-p.mes.<instituição>.rsfn.net.br para o servidor de produção e sftp-h.mes.<instituição>.rsfn.net.br para o servidor de homologação.

5.8.7 Para o ambiente PPRO, quando disponível, serão considerados, para o tráfego de arquivos, os servidores de homologação do respectivo domínio de sistema.

5.8.8 Os servidores SFTP devem operar sobre a versão 2 do protocolo "Secure Shell" (SSH), na porta 22.

5.8.9 A autenticação nos servidores SFTP se dará por meio de certificados digitais do tipo OpenSSH. Serão aceitos apenas certificados gerados pela AC OpenSSH interna do Bacen, conforme processo descrito no item 5.8.11.

5.8.10 Para cada ambiente (homologação ou produção), poderão existir até dois usuários por instituição, um com permissão apenas de leitura e outro com permissão de leitura e escrita no SFTP. Os nomes dos usuários serão baseados no ISPB da instituição, no ambiente (homologação ou produção) e nas suas permissões, seguindo o formato u<ISPB>.(hro|hrw|pro|prw). Por exemplo, o usuário no ambiente de homologação com permissão de leitura e escrita da instituição com ISPB 11222333 terá o nome “u11222333.hrw”.

5.8.11 Processo de geração de certificados de usuário para acesso aos serviços SFTP:

a. Instituição gera, no seu ambiente, os pares de chaves que serão associados aos certificados OpenSSH a serem utilizados para acesso aos serviços SFTP de cada prestador. Serão admitidas chaves geradas com os algoritmos ed25519, RSA (2048 bits ou superior) e ECDSA (P-256 ou superior). O algoritmo DSA não deverá ser utilizado. Exemplos de comandos para geração das chaves utilizando diferentes algoritmos:

ssh-keygen -t ed25519

ssh-keygen -t rsa -b 4096

ssh-keygen -t ecdsa -b 521

b. Instituição envia a chave pública gerada ao Bacen via STA. Para gerar um certificado para uso no SFTP do ambiente de produção, deve ser utilizado o STA de produção. Alternativamente, para obter um certificado para uso no SFTP de homologação, deve ser utilizado o STA de homologação. Para gerar certificados para usuários com permissão apenas de leitura, deve-se utilizar o código de arquivo CPUBSUR. Para gerar certificados para usuários com permissão de leitura e escrita, deve-se utilizar o código de arquivo CPUBSUW.

c. Bacen emite o certificado OpenSSH associado à chave pública enviada, ao ISPB da instituição e ao tipo de usuário (conforme o tipo de arquivo escolhido no passo anterior), incluindo o certificado como resposta no próprio protocolo do STA. Para usuários com permissão apenas de leitura, o nome do arquivo do certificado será CERTSUR. Para usuários com permissão de leitura e escrita, o nome do arquivo será CERTSUW. O nome do usuário associado ao certificado constará no parâmetro “Principals” do certificado. No parâmetro “Key ID”, serão inseridos o ISPB da instituição, o código sisbacen do usuário e o protocolo no STA, no formato "<ISPB>-<Cód_Sisbacen>-<Protocolo STA>".

Os passos acima deverão ser repetidos para geração do certificado a ser utilizado para acesso ao serviço SFTP do outro ambiente (homologação ou produção).

5.8.12 É recomendado que cada instituição gere pares de chaves distintos para os certificados a serem utilizados no acesso ao serviço SFTP de diferentes prestadores.

5.8.13 Os certificados OpenSSH terão validade de 1 ano.

5.8.14 Após gerados os certificados, eles estarão automaticamente habilitados para uso pelas instituições nos seus clientes SFTP, juntamente com a chave privada associada, no momento do login.

5.8.15 Certificados cuja data de expiração for ultrapassada deixarão de ser aceitos automaticamente. Caso deseje revogar determinado certificado antes de sua expiração, a instituição deve enviar via STA um arquivo de texto contendo o “Key ID” do certificado a ser revogado. O código de arquivo a ser utilizado nesse caso é REVCERT. A partir daí, o Bacen adicionará o certificado relacionado na lista de revogação do SFTP do Bacen. Também será mantida a lista de certificados revogados no site do BCB na RSFN. Os demais prestadores de serviço SFTP devem verificar a lista periodicamente e refleti-la localmente nos seus servidores SFTP.

5.8.16 Cada instituição é responsável por gerar novo par de chaves e refazer o processo de geração do certificado OpenSSH a cada ano, antes da expiração do certificado vigente. Não é permitido utilizar o mesmo par de chaves para gerar um novo certificado.

5.8.17 O Bacen e os demais prestadores de serviço devem configurar seus servidores SFTP para confiarem apenas em logins com certificados emitidos pela AC OpenSSH do Bacen, cuja chave pública associada ficará disponível no site do BCB na RSFN.

5.8.18 Os usuários nos servidores SFTP devem ser criados sem shell e sem senha, de forma que tentativas de login dessas contas por meio de usuário e senha devem sempre falhar.

5.8.19 O Bacen e demais prestadores devem gerar certificados OpenSSH específicos para seus hosts SFTP. O processo de geração de tais certificados de host é igual ao que consta no item 5.8.11, porém, os códigos de arquivo no STA a serem utilizados são CPUBSHS (para hosts SPB) e CPUBSHM (para hosts MES). O nome (FQDN) do servidor SFTP associado ao certificado deve ser previamente informado ao Bacen pelo prestador de serviço. O nome do arquivo do certificado retornado pelo Bacen será CERTSHS, para servidores SPB, e CERTSHM, para servidores MES, e o nome do servidor SFTP constará no parâmetro “Principals” do certificado.

5.8.20 As chaves públicas das ACs OpenSSH do Bacen, de homologação e produção, serão publicadas no site do BCB na RSFN e poderão ser configuradas nos aplicativos clientes para aceite automático dos certificados utilizados nos servidores SFTP do Bacen e demais prestadores.

5.8.21 Os servidores SFTP devem ser configurados para gerar logs de auditoria completos, contendo no mínimo as seguintes informações: usuário, identificador da chave pública, endereço IP, data/hora e atividade realizada.

5.8.22 Cada Instituição terá acesso aos seguintes diretórios:

Em homologação:

/publico (acesso de leitura para todos os usuários de homologação)

/<ISPB>/download (acesso de leitura para os usuários u<ISPB>.hro e u<ISPB>.hrw)

/<ISPB>/upload (acesso de leitura para o usuário u<ISPB>.hro e acesso de gravação para o usuário u<ISPB>.hrw)

Em produção:

/publico (acesso de leitura para todos os usuários de produção)

/<ISPB>/download (acesso de leitura para os usuários u<ISPB>.pro e u<ISPB>.prw)

/<ISPB>/upload (acesso de leitura para o usuário u<ISPB>.pro e acesso de gravação para o usuário u<ISPB>.prw)

5.8.23 O provedor de serviço SFTP poderá remover o arquivo do diretório após 7 dias corridos da sua data de disponibilização.

5.8.24 Arquivos no diretório “publico” devem ser somente assinados (campo C04 = 6 ou 10) pelo prestador e não deverão ter seu conteúdo criptografado.

5.8.25 Arquivos nos diretórios “download” e “upload” sempre devem ser assinados e criptografados pelo emissor.

5.8.26 O algoritmo de criptografia simétrica utilizado para cifrar os arquivos deve ser o AES-256, no modo de operação GCM.

5.8.27 No caso de arquivos compactados, deve ser utilizado o padrão ZIP com o método de compressão “DEFLATE”.

6 Informações para a ativação de certificado

6.1 Ativação de certificado

6.1.1 A ativação de certificado digital constitui-se em uma única etapa, com o envio de mensagem GEN0006 ao Bacen, pela RSFN.

6.1.2 O conteúdo detalhado para efeito do preenchimento das mensagens é descrito no Catálogo de Serviços do SFN.

6.1.3 Todas as Instituições Participantes deverão submeter e ativar certificados no ambiente de Homologação antes de submeter e ativar certificados no ambiente de Produção.

6.1.4 Todos os certificados recebidos pelo Bacen, por meio do STA, uma vez validados, serão arquivados como habilitados, sujeitos à ativação.

6.1.5 Após a validação, se bem-sucedida, o STA informará que o arquivo está aceito. No ambiente de Homologação, complementará com a mensagem “Certificado digital aceito para testes”; no ambiente de Produção, a descrição complementar será “Certificado digital aceito para produção”.

6.1.6 A mensagem GEN0006 deverá ser assinada pelo certificado a ativar, indicados também, no cabeçalho de segurança, o seu código da certificadora e o seu número de série.

6.1.7 Após o recebimento de uma mensagem GEN0006 correta, o Bacen enviará uma mensagem GEN0007 para todas as instituições participantes do domínio em que o certificado foi ativado, conforme descrito no Catálogo de Serviços do SFN.

6.1.8 Entende-se como certificado digital ativo aquele que apresenta a chave pública que deve ser utilizada para cifrar a chave de criptografia simétrica 3DES usada para cifrar a mensagem destinada à Instituição. Para efeito de validação do criptograma de autenticação, só serão considerados os criptogramas de autenticação com a identificação dos certificados ativos, exceto nas situações descritas no item 5.6.2.

6.1.9 Todas as mensagens emitidas pelo Bacen serão assinadas digitalmente e cifradas, salvo as exceções relacionadas no item 3.5.4.

6.1.10 Caso a Instituição queira testar o envio de mensagens não cifradas ou não assinadas, poderá enviar mensagens GEN0001 (eco) antes de solicitar a ativação.

6.1.11 Para a realização dos testes com mensagens as Instituições deverão usar os certificados do Bacen disponibilizados no site www.bcb.rsfn.net.br.

6.2 Informações sobre o uso do Sistema de Transferência de Arquivos - STA

6.2.1 Informações e orientações sobre o uso do STA estão disponíveis no site www.bcb.gov.br.

6.2.2 Para utilizar o STA é necessária a identificação de um usuário cadastrado no Sisbacen autorizado na transação PSTA300. Autorizações adicionais podem ser necessárias para a transmissão de alguns códigos de documento.

6.2.3 Para o envio do certificado digital através do STA, deverá ser informado o código de arquivo CERTSPB (documento CSPB) - Certificado Digital da Instituição no SPB, ou CERTMES (documento CMES) - Certificado Digital da Instituição no domínio MES.

6.2.4 Para envio de certificados digitais do ambiente de homologação, deverá ser usado o STA de homologação; para envio de certificados digitais do ambiente de Produção, deverá ser usado o STA de Produção.

7 Glossário de termos

ABNT: Associação Brasileira de Normas Técnicas.

AES (Advanced Encryption Standard): algoritmo de criptografia simétrica criado em 2001 pelo NIST, por meio da publicação FIPS 197.

Algoritmo assimétrico: É um algoritmo de criptografia que usa duas chaves: uma chave pública e uma chave privada, onde a chave pública pode ser distribuída abertamente, enquanto a chave privada é mantida secreta. Os algoritmos assimétricos são capazes de muitas operações, incluindo criptografia, assinaturas digitais e acordo de chave. Também conhecido como algoritmo de chave pública.

Algoritmo simétrico: Algoritmo de criptografia que usa somente uma chave, tanto para criptografar como para descriptografar. Esta chave deve ser mantida secreta para garantir a confidencialidade da mensagem ou arquivo. Também conhecido como algoritmo de chave secreta.

ASN.1: Abstract Syntax Notation Number.

Auditabilidade: Registro do processamento de transações significativas e/ou críticas para permitir a reconstituição e análise dos eventos ocorridos durante o processamento.

***Autenticação*:** Verificação reivindicada de uma identidade. O processo de determinar a identidade de um usuário que esteja tentando alcançar um sistema.

***Autenticidade*:** Garantir que as mensagens e arquivos transmitidos não sejam modificados por entidades não autorizadas.

AC: Autoridade Certificadora - Entidade que emite certificados digitais. Todos os certificados são assinados digitalmente com a chave privativa da Autoridade Certificadora.

Bacen: Banco Central do Brasil.

***Chave Privada*:** Chave de um par de chaves mantida secreta pelo seu dono e usada no sentido de criar criptogramas para cifrar e decifrar mensagens e arquivos com as chaves públicas correspondentes.

***Chave Pública*:** Chave de um par de chaves criptográficas que é divulgada pelo seu dono e usada para verificar o criptograma de autenticação criado com a chave privada correspondente ou, dependendo do algoritmo criptográfico assimétrico utilizado, para cifrar e decifrar mensagens e arquivos.

Chave simétrica: chave utilizada no algoritmo de criptografia simétrica. A mesma chave é utilizada tanto para cifrar como para decifrar a mensagem ou o arquivo.

***Confidencialidade ou sigilo*:** Condição na qual dados sensíveis são mantidos secretos e divulgados apenas para as partes autorizadas.

Criptograma de autenticação: Conjunto de bytes obtidos através da cifragem do hash da mensagem ou do arquivo com a chave privada do emissor. Provê garantia da origem e da integridade da mensagem ou do arquivo.

CSR: Certificate Signature Request – Arquivo com pedido de assinatura de um certificado digital enviado à Autoridade Certificadora pelo solicitante do certificado.

Disaster recovery: Recuperação de sistemas e das bases de dados e, geralmente após a ocorrência de emergência.

Disponibilidade**:** Garantir que determinado recurso esteja disponível para entidades autorizadas.

Domínio de Mensageria: Contexto específico onde é executada uma determinada aplicação de Mensageria na RSFN.

FIPS: Federal Information Processing Standards - Norma Federal Americana de Processamento de Informações publicada pelo NIST.

FTP: File Transfer Protocol – Protocolo de transferência de arquivos mais utilizado na Internet.

Função Hash: é uma equação matemática que aplicada sobre uma sequência de bytes cria um código chamado message digest (resumo de mensagem).

GCM: modo de operação Galois/Counter Mode para algoritmos de criptografia simétrica, definido em 2007 pelo NIST, por meio da Special Publication 800-38D***.***

Header do MQSeries: Cabeçalho de 512 bytes criado pelo MQSeries onde constam várias informações de controle da mensagem.

ICP-Brasil: Infra-estrutura de Chaves Públicas Brasileira, instituída pela Medida Provisória Nº 2.200-2, de 24 de agosto de 2001;

Integridade**:** A condição na qual a informação ou os recursos de informação são protegidos contra modificações não autorizadas.

Instituição(ões) ou Instituição(ões) Participante(s): Toda e qualquer entidade participante da Rede do Sistema Financeiro Nacional - RSFN habilitada a enviar e receber mensagens e arquivos por meio da referida Rede.

LCR: Lista de Certificados Revogados – Lista cumulativa de todos os certificados digitais revogados, emitidos pela Autoridade Certificadora para uma determinada Política de Certificação (PC).

Log: Arquivo que registra todas as mensagens enviadas e recebidas com seu respectivo criptograma de autenticação, visando permitir a rastreabilidade.

Mensagem cifrada: Mensagem cifrada com a chave simétrica criada exclusivamente para cada mensagem.

Mensagem de "broadcast": Mensagem enviada para todos os integrantes de uma rede, tem por finalidade a propagação de informações de cunho genérico e amplo;

Mensagem padrão XML: Padrão flexível, reconhecido internacionalmente para formatação do conteúdo de mensagens, XML (eXtensible Markup Language).

MQSeries: Software de gerenciamento para envio e recebimento de mensagens.

Não repúdio**:** Garantir que uma determinada entidade originária da mensagem não possa negar sua transmissão.

NIST - National Institute of Standards and Technology – Instituto Americano de Tecnologia e Padrões o qual produz padrões relacionados a segurança e criptografia que são publicados como documentos FIPS.

Participante(s): Vide Instituição.

PC: Política de Certificação - Documento emitido por uma AC que descreve os requisitos, procedimentos e nível de segurança adotados para a emissão, revogação e gerenciamento do ciclo de vida de um Certificado Digital. Para efeito desse documento a PC 3 (Pessoas Físicas) se refere às diversas PCs de certificados digitais de pessoas físicas tipo A3 no âmbito da ICP-Brasil.

PIN: Personal Identification Number - Número de Identificação Pessoal

Protocolo de Segurança**:** o mecanismo utilizado para troca de informações seguras entre os participantes da RSFN.

Rastreabilidade**:** Capacidade ou a possibilidade de ser rastreado, isto é, "investigado, procurado, inquirido".

RSFN: Rede do Sistema Financeiro Nacional – Rede de telecomunicações que provê infraestrutura para troca de informações entre o Banco Central do Brasil e instituições que operam no âmbito do Sistema de Pagamentos Brasileiro (SPB),da Mensageria do Sisbacen (MES) e do Pix.

Segurança da Informação**:** proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

STA: Sistema de Transferência de Arquivos do Banco Central, que tem por objetivo permitir o intercâmbio de arquivos digitais entre o Banco Central do Brasil e outras instituições cadastradas no Sisbacen, de forma padronizada e segura, por meio de conexões de dados protegidas.

Anexo A (Cabeçalho de Segurança)

MQSeries Header		512 Bytes	MQSeries Header
(C01) Tamanho total do Cabeçalho de Segurança	2 Bytes	588 Bytes	Security Header
(C02) Versão do Protocolo de Segurança	1 Byte		
(C03) Código de erro	1 Byte		
(C04) Indicação de uso especifico	1 Byte		
(C05) Reservado para uso futuro	1 Byte		
(C06) Algoritmo da chave assimétrica destino	1 Byte		
(C07) Algoritmo da chave simétrica	1 Byte		
(C08) Algoritmo da chave assimétrica Local	1 Byte		
(C09) Algoritmo de Hash	1 Byte		
(C10) PC do certificado destino (cifragem)	1 Byte		
(C11) Nº de serie do certificado destino	32 Bytes		
(C12) PC do certificado local (Assinatura)	1 Byte		
(C13) Nº de serie do certificado local	32 Bytes		
(C14)[1] [2] Buffer de cifragem da chave simétrica (PKCS #1 v1.5)	256 Bytes		
(C15) Criptograma de autenticação (PKCS #1 v1.5)	256 Bytes		
Mensagem ou arquivo cifrado com a chave simétrica (no caso da segunda versão do Protocolo de Segurança, preencher os bytes restantes para o próximo múltiplo de 8 com "00")		Tamanho Variável (Padrão XML)	BCMSG
		Tamanho Variável (Padrão XML)	SISMSG
		Tamanho Variável (Padrão XML)	UserMSG

Nota 1
Na segunda versão do Protocolo de Segurança, a chave DES consiste de 64 bits binários (8 bytes), desses, 8 bits (1 byte) são utilizados para a verificação de paridade ímpar. Na implementação TripleDES (3DES), são utilizadas 3 chaves DES, portanto o tamanho total da chave é 192 bits = 24 bytes.
Na terceira versão do Protocolo, a chave AES possui 256 bits (32 bytes).

Nota 2
Na segunda versão do Protocolo de Segurança, devido à escolha do algoritmo simétrico 3DES e modo de operação CBC, para o vetor de inicialização devem ser usados os 8 Bytes iniciais da chave simétrica.
Na terceira versão, o algoritmo é o AES no modo de operação GCM. Nesse caso, o vetor de inicialização deve ser composto de 96 bits (12 bytes) gerados aleatoriamente. Já a tag de autenticação deve ter 128 bits (16 bytes) e deve ser apensada ao final do criptograma.