



GT-SEGURANÇA

**MANUAL DE SEGURANÇA
DA RSFN**

Versão 2.5
Novembro/2009

Histórico de Revisão

Data	Versão	Descrição	Autores	E-mail
22/11/2001		Elaboração	L. Germano Guimarães – ASBACE/ATP Frederico Burgos – Bacen	lgermano@asbace.com.br fburgos@bcb.gov.br
22/11/2001	1.0	1ª Revisão e Aprovação	Grupo Técnico de Segurança SPB Associações, Câmaras e Banco Central	Spb.seguranca@bcb.gov.br
22/02/2002	2.0	2ª Revisão	L. Germano Guimarães – ASBACE/ATP Frederico Burgos - Bacen	lgermano@asbace.com.br fburgos@bcb.gov.br
15/04/2002	2.1	3ª Revisão	L. Germano Guimarães – ASBACE/ATP Frederico Burgos - Bacen	lgermano@asbace.com.br fburgos@bcb.gov.br
20/11/2003	2.2	4ª Revisão	Frederico Burgos – Bacen Paulo Roberto A Carvalho - Bacen	fburgos@bcb.gov.br paulor@bcb.gov.br
14/12/2005	2.3	5ª Revisão	Frederico Burgos – Bacen Paulo Roberto A Carvalho - Bacen	fburgos@bcb.gov.br paulor@bcb.gov.br
18/12/2006	2.4	6ª Revisão	Frederico Burgos – Bacen Paulo Roberto A Carvalho – Bacen Lucas de Carvalho Ferreira - Bacen	fburgos@bcb.gov.br paulor@bcb.gov.br lucas.ferreira@bcb.gov.br
04/11/2009	2.5	7ª Revisão	Frederico Burgos – Bacen Paulo Roberto A Carvalho – Bacen	fburgos@bcb.gov.br paulor@bcb.gov.br

Índice

HISTÓRICO DE REVISÃO.....	1
1 INTRODUÇÃO.....	3
2 ESCOPO.....	3
3 POLÍTICA DE SEGURANÇA DA RSFN	4
3.1 SUMÁRIO.....	4
3.2 ABREVIATURAS.....	4
3.3 CONSCIENTIZAÇÃO.....	4
3.4 OBJETIVO.....	4
3.5 PREMISAS.....	4
3.6 DIRETRIZES	5
4 CERTIFICAÇÃO DIGITAL NA RSFN.....	7
4.1 CREDENCIAMENTO DE AUTORIDADES CERTIFICADORAS.....	7
4.2 ESPECIFICAÇÕES PARA A GERAÇÃO DE CERTIFICADOS DIGITAIS TIPO SPB.....	7
4.3 EXEMPLOS ILUSTRATIVOS DE PREENCHIMENTO DE CSRS.....	8
4.4 PROCESSO DE OBTENÇÃO E HABILITAÇÃO DE CERTIFICADOS.....	9
4.5 PROCESSOS DE ATIVAÇÃO, SUBSTITUIÇÃO E REVOGAÇÃO DE CERTIFICADOS.....	10
5 ESPECIFICAÇÕES PARA SEGURANÇA DE MENSAGENS E ARQUIVOS.....	12
5.1 CABEÇALHO ("HEADER") DE SEGURANÇA DAS MENSAGENS.....	12
5.2 AGREGAÇÃO DA SEGURANÇA NA EMISSÃO DE MENSAGENS.....	13
5.3 VERIFICAÇÃO DA SEGURANÇA PARA A RECEPÇÃO DE MENSAGENS.....	14
5.4 GERAÇÃO DE ARQUIVOS DE AUDITORIA (LOGS) DAS MENSAGENS TRAFEGADAS.....	15
5.5 TRATAMENTOS DE ERROS NA RECEPÇÃO DAS MENSAGENS.....	16
5.6 CÓDIGOS INDICATIVOS DE TRATAMENTOS ESPECIAIS QUANTO À SEGURANÇA.....	17
5.7 TROCA DE ARQUIVOS ATRAVÉS DE SERVIDORES FTP.....	18
6 INFORMAÇÕES PARA OS TESTES DE SEGURANÇA	19
6.1 TESTES DE SEGURANÇA.....	19
6.2 INFORMAÇÕES SOBRE O USO DO APLICATIVO PSTAW10.....	19
7 OUTRAS APLICAÇÕES.....	21
7.1 DOMÍNIOS DE MENSAGERIA.....	21
7.2 WEB SERVICES PROVIDOS PELO BANCO CENTRAL.....	21
8 GLOSSÁRIO DE TERMOS.....	22
ANEXO A (CABEÇALHO DE SEGURANÇA).....	26
.....	26

1 Introdução

Este manual tem por objetivo consolidar os entendimentos contidos nos documentos expedidos pelo GT-Segurança da Rede do Sistema Financeiro Nacional - RSFN, desde a sua organização. O GT-Segurança da RSFN, institucionalizado pela Circular 3.424, de 12/12/2008 e regulamentado pelo Comunicado 18.655, de 02/07/2009, é constituído por representantes do Banco Central do Brasil (Bacen), da Secretaria do Tesouro Nacional, das associações de bancos de âmbito nacional, das câmaras e dos prestadores de serviço de compensação e de liquidação participantes da RSFN.

Os requisitos de segurança são implementados para garantir a integridade, a confidencialidade, a disponibilidade e o não repúdio das informações trafegadas.

A definição dos requisitos de segurança exigidos foi baseada em padrões conhecidos e utilizados no mercado.

Entende-se por Protocolo de Segurança o mecanismo utilizado para troca de informações seguras entre os participantes da RSFN.

O GT-Segurança 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. 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.

Os ambientes de homologação e de produção deverão ser distintos. Primeiramente as aplicações deverão ser homologadas, para posteriormente serem disponibilizadas no ambiente de produção.

2 Escopo

O GT-Segurança tem como missão definir os requisitos de Segurança para a troca eletrônica de informações no âmbito da RSFN, no que tange a Criptografia, Protocolos, Algoritmos e Certificação Digital.

As recomendações e os padrões aqui contidos 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 trafegadas.

3.5 Premissas

3.5.1 Os serviços da RSFN, incluindo a infra-estrutura 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 enviadas à RSFN serão obrigatoriamente assinadas digitalmente pela Instituição Participante emissora, com exceção, caso julgado necessário, das relativas a testes de conectividade;
- 3.5.4 Todas as mensagens enviadas à RSFN serão obrigatoriamente criptografadas com exceção das relativas a testes de conectividade e a comunicação de erros de segurança, além das emitidas sem destinatário específico;
- 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 das mensagens;
- 3.5.8 Toda e qualquer mensagem gerada e enviada à RSFN por um de seus participantes é de exclusiva responsabilidade de quem a originou;
- 3.5.9 As premissas anteriores também se aplicam aos arquivos disponibilizados nos servidores FTP na RSFN;

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 utilizadas para troca de mensagens no SPB não deverão ser utilizados para mensagens ou aplicações 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 Técnico da RSFN **(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 a 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 Infra-estrutura 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 tipo 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 do tipo SPB;
- 4.1.7 Para maiores informações consultar as resoluções da ICP-Brasil.

4.2 Especificações para a geração de Certificados Digitais tipo SPB

- 4.2.1 Campos obrigatórios a serem incluídos no CSR:

C=BR

O=ICP-Brasil

OU=ISPB-cccccccc

OU=SISBACEN-iiii

CN=Identificação única da instituição certificada e do certificado (ex: P ou T + número seqüencial, 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 seqüência "Xnnn",

onde "nnn" é uma numeração seqüencial única de 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;

Obs: Os certificados poderão ser enviados ao Banco Central em qualquer ordem de número sequencial.

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 GT-Segurança, na forma:

OU=CSPB-1 (Serpro); ou

OU=CSPB-2 (Certisign); ou

OU=CSPB-4 (Serasa);

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-1024 bits e um arquivo CSR, no padrão PKCS#10;
- 4.4.2 A solicitação para a emissão de certificado é feita diretamente a uma AC, via Internet;
- 4.4.3 A AC atua como Autoridade Registradora e verifica os dados da solicitação e do preposto da instituição;
- 4.4.4 O Bacen disponibilizará às ACs, para conferência, uma relação das Instituições Participantes, com as codificações ISPB e Sisbacen;
- 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 tipo SPB através do aplicativo PSTAW10;

- 4.4.7 Ao enviar através do PSTAW10, a Instituição deverá informar o código do documento CSPB (Certificados Digitais do SPB) ou CMES (uso para o domínio de mensagem Sisbacen);
- 4.4.8 O aplicativo PSTAW10 é de uso gratuito a todas as Instituições que devam enviar e/ou receber arquivos do Bacen. Está disponível para download através da Internet no *site* www.bcb.gov.br. Seu uso está amparado pela Carta-Circular 2.847, de 13 de abril de 1999.
- 4.4.9 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;
- 4.4.10 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;
- 4.4.11 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;
- 4.4.12 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 assinatura das mensagens em ambientes de homologação distintos. Para cada ambiente, ainda que usando o mesmo certificado, deverá haver um processo de ativação independente;
- 4.4.13 Poderá haver mais de um certificado habilitado a qualquer tempo, mas apenas um estará ativo em cada domínio/ambiente;
- 4.4.14 Cada certificado deverá estar associado a um par de chaves únicas;

4.5 Processos de ativação, substituição e revogação 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 será emitida pelo Bacen mensagem de "broadcast" (GEN0007), onde constam o novo certificado e os dados de identificação do anterior (AC e número de série);
- 4.5.4 Os certificados substituídos deverão ser obrigatoriamente revogados pela Instituição junto à AC, não podendo mais serem utilizadas as chaves a eles correlacionadas;
- 4.5.5 As mensagens de ativação por substituição de certificados deverão ser encaminhadas preferencialmente entre os 60 e 30 minutos anteriores à abertura diária do Sistema de Transferência de Reservas – STR ou até 60 minutos após o fechamento, de modo que todas as mensagens de um mesmo dia possam ser assinadas pela mesma chave;
- 4.5.6 Somente nos casos de revogação por contingência ou suspeita de violação de segurança é que poderão ser enviadas e processadas mensagens de ativação fora do período preferencial;
- 4.5.7 Os certificados ativos estarão disponíveis no *site* www.bcb.rsfn.net.br, no arquivo Ativados.zip, atualizado a cada vinte minutos no período de 6:30h às 21:00h;
- 4.5.8 A substituição dos certificados do Bacen, quando do seu vencimento anual, em qualquer ambiente (produção ou homologação), será previamente comunicada no *site* www.bcb.rsfn.net.br e por meio da mensagem GEN0018, enviada a todas as instituições com certificados ativados, com antecedência de pelo menos 3 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. A efetiva substituição do certificado digital do Bacen se dará na data estabelecida pela GEN0018, no mínimo trinta minutos após o fechamento do STR;
- 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 substituirá o anterior o qual não poderá mais ser usado, de acordo com o item 4.5.4.
- 4.5.11 Todo certificado será automaticamente invalidado para uso no âmbito do SPB 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 revogado às 24 horas do dia 07/11/2006.

5 Especificações para Segurança de Mensagens e Arquivos

5.1 Cabeçalho ("header") de segurança das Mensagens

Todas as mensagens e/ou arquivos eletrônicos trocados no âmbito da RSFN devem iniciar com uma sequência de 332 bytes - o cabeçalho de segurança, responsável pela implementação dos mecanismos de assinatura e criptografia dos mesmos.

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	014CH: Fixo na primeira versão (332 bytes)
C02	003-003	Versão do protocolo	00H: Em claro, 01H: Primeira versão
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
C07	008-008	Algoritmo da chave simétrica	01H: Triple-DES com 168 bits (3 x 56 bits) (Vide 5.1.3)
C08	009-009	Algoritmo da chave assimétrica local da assinatura	01H: RSA com 1024 bits
C09	010-010	Algoritmo de "hash"	01H: MD5 (somente até 30/04/07) 02H: SHA-1
C10	011-011	AC do certificado do destino	Ex. 01H: Serpro 02H: Certisign, 04H: Serasa
C11	012-043	Série do certificado do destino	Identificador único do certificado na AC (Vide 5.1.4)
C12	044-044	AC do certificado da assinatura	Ex. 01H: Serpro, 02H: Certisign, 04H: Serasa
C13	045-076	Série do certificado da assinatura	Identificador único do certificado na AC (Vide 5.1.4)
C14	077-204	Buffer de criptografia da chave simétrica	Chave 3DES (24 bytes) cifrada por PKCS#1v1_5
C15	205-332	Buffer de assinatura da mensagem	Hash (20 bytes) assinado pelo PKCS#1v1_5

5.1.1 As posições 077-204 e 205-332 são cifradas respectivamente com a chave pública do destinatário e a chave privada do emitente, de acordo

- 5.2.4 Calcula-se o "hash", para efeito de assinatura, do XML já em código único (Unicode UTF-16 BE) e com "padding", indicando o algoritmo utilizado (campo C09);
- 5.2.5 Indicam-se os códigos de AC 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 Assina-se a mensagem (anotando o resultado do "hash" do conteúdo em XML, com o padding) com a chave privada correspondente ao certificado da participante emissor, anotando o resultado no campo C15;
- 5.2.8 Sorteia-se chave simétrica (Triple-DES 192 bits) e cifra-se a mensagem que foi objeto de assinatura;
- 5.2.9 Cifra-se a chave simétrica (24 bytes) utilizada na cifragem da mensagem com a chave pública correspondente ao certificado digital do destinatário, com o resultado no campo C14;
- 5.2.10 No caso de arquivos, são válidas todas as regras descritas para as mensagens, exceto, em alguns casos, o padrão XML, que poderá não ser adotado. Em qualquer caso o "padding" também se faz necessário, inclusive para os arquivos não criptografados e/ou compactados.

5.3 Verificação da segurança para a recepção de mensagens

- 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 (campos C12/C13);
- 5.3.2 No caso do Bacen, para as mensagens GEN0001 e GEN0006, 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 com a chave privada correspondente à chave pública do certificado;
- 5.3.4 Decifra-se a parte XML da mensagem (a partir da posição 333), inclusive o "padding";
- 5.3.5 Calcula-se o "hash" da Mensagem XML em código Unicode UTF-16 BE com o "padding", de acordo com o algoritmo indicado em C09;
- 5.3.6 Confere-se a assinatura da mensagem, comparando o "hash" obtido;
- 5.3.7 Se houver qualquer erro no decorrer do processo, 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:

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
065-396	Binário	Cabeçalho de segurança completo
397-TAM	Unicode	Mensagem em claro (Unicode double byte com "padding")

- 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 conseqüente 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:

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 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 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
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 uma mensagem assinada e cifrada.
- 5.6.2 Excepcionalmente nas condições abaixo, poderá assumir os seguintes valores:
 - “1” - Mensagem relativa a segurança ou que utiliza um certificado ainda não ativado (caso da 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 (nos casos das mensagens GEN0004);
 - “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 servidor FTP para que as Instituições enviem ou recebam os arquivos solicitados;
- 5.7.2 Cada provedor (Bacen, Selic e Câmaras) deverá ter o seu próprio servidor FTP;
- 5.7.3 O padrão de nome do servidor será : ftp-p.<instituição>.rsfn.net.br para o servidor de produção e ftp-t.<instituição>.rsfn.net.br para o servidor de homologação;
- 5.7.4 O servidor FTP não terá mecanismo de segurança. A segurança será feita através dos mecanismos de criptografia e assinatura dos arquivos semelhantes aos da Mensageria;
- 5.7.5 O servidor FTP deverá ser configurado para criar logs de acessos totais, contendo usuário, ip, data/hora e atividade realizadas;
- 5.7.6 Cada Instituição terá um único usuário para Logon;
- 5.7.7 O nome de usuário será o ISPB da Instituição;
- 5.7.8 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 5.7.7

- 5.7.9 O provedor de serviço FTP poderá remover o arquivo do diretório após 03 dias úteis da sua data de disponibilização;
- 5.7.10 Arquivos públicos são somente assinados (campo C04 = 6 ou 10);
- 5.7.11 No caso de arquivos compactados deve ser usado o algoritmo ZIP. 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 5.2.3 e 5.2.4 para mensagens. Mesmo após a decifragem (se for o caso) e conferência da assinatura o “padding” não deverá ser removido;
- 5.7.12 A senha FTP inicial gerada para cada usuário será o próprio nome;
- 5.7.13 A troca de senhas para os servidores FTP dar-se-á conforme critérios de cada provedor.

6 Informações para os testes de SEGURANÇA

6.1 Testes de segurança

6.1.1.Os testes de segurança são conduzidos unicamente pelo Bacen e constituem-se de uma única etapa, de ativação, já com o uso de mensagens GEN0006 transmitidas através das filas do software MQ-Series.

6.1.2.O conteúdo detalhado para efeito do preenchimento das mensagens é divulgado no Catálogo de Mensagens e de Arquivos da RSFN.

6.1.3.Todas as Instituições Participantes deverão passar por esta etapa antes de submeter certificados à habilitação no ambiente de produção.

6.1.4.Todos os certificados recebidos pelo Bacen, uma vez verificados, serão arquivados como habilitados, sujeitos à ativação.

6.1.5.A ativação de um certificado consistirá no envio de mensagem assinada pelo mesmo, código GEN0006, onde são indicados o código da certificadora e o número de série. Caso exista outro certificado ativo, este deverá ser também identificado, indicando-se a sua situação após a ativação (habilitado, revogado ou descartado por vencimento).

6.1.6.Após o recebimento de uma mensagem GEN0006 correta, o Bacen gera uma mensagem GEN0007, com o mesmo conteúdo, transmitindo-a a todas as instituições participantes.

6.1.7.Entende-se como certificado ativo o 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 conferência de assinatura digital, só serão consideradas as assinaturas com a identificação dos certificados ativos, exceto nas mensagens de ativação (GEN0006) e teste de eco (GEN0001).

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

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

6.1.10.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 aplicativo PSTAW10

- 6.2.1.O programa pode ser obtido no *site* www.bcb.gov.br, na seção "Sisbacen", item "Transferência de arquivos". O seu uso está amparado pela Carta-Circular 2.847, de 13 de abril de 1999.
- 6.2.2.O aplicativo executa em qualquer ambiente Windows de 32 bits (Windows 95, 98, ME, NT, 2000, XP, 2003, Vista ou Linux com emulação). Para utilizá-lo é necessária a identificação de um usuário cadastrado no Sisbacen autorizado na transação PSTA300.
- 6.2.3.Para o envio do certificado digital, deverá ser informado no PSTAW10 o código de documento CSPB (Certificado Digital da Instituição no SPB) ou CMES (Certificado Digital da Instituição no domínio MES).

7 Outras aplicações

7.1 Domínios de mensageria

- 7.1.1 Com o advento de novas aplicações no âmbito do Bacen, surgiu a necessidade de se diferenciar os respectivos contextos em domínios de mensageria. Assim, as atuais aplicações dos sistemas componentes do SPB (Ex:STR) estão inseridas no domínio SPB01, e foi instituído o domínio MES01 para a mensageria Sisbacen, contemplando mensagens definidas pelo Vol. III do Catálogo de Mensagens e de Arquivos da RSFN;
- 7.1.2 Para o envio do certificado digital da mensageria Sisbacen no domínio MES01, deverá ser informado no PSTAW10 o código de documento CMES (Certificado Digital da Instituição no domínio MES);
- 7.1.3 Os domínios para efeito deste manual de segurança não utilizam os dígitos numéricos finais, sendo identificados apenas pela sigla do sistema (SPB ou MES).
- 7.1.4 Caso seja necessário utilizar o mesmo certificado digital para mais de um domínio, ele deverá ser enviado pelo PSTAW10 para cada um dos domínios separadamente.
- 7.1.5 As regras preconizadas nos capítulos anteriores para manutenção de arquivos de log, horário de substituição de certificados digitais, divulgação dos certificados do Bacen e uso da RSFN não se aplicam obrigatoriamente aos demais domínios.

7.2 Web Services providos pelo Banco Central

- 7.2.1 Os *web services* utilizados pelas instituições financeiras para alimentar o sistema de Autocadastramento de Pessoas Físicas (APF), instituídos pela Carta-Circular 3.205, de 05/09/2005, terão suas comunicações autenticadas pelo lado cliente por meio de certificados digitais no mesmo padrão aqui estabelecido.
- 7.2.2 O envio destes certificados se dará pelo uso do PSTAW10, utilizando o código de documento CAPF (Certificado digital para *web services* APF).

8 Glossário de termos

ABNT: Associação Brasileira de Normas Técnicas.

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. Também conhecido como algoritmo de chave secreta.

ASN.1: Abstract Syntax Notation Number.

Assinatura Digital: Assinatura eletrônica semelhante a assinatura real de um documento. Provê garantia da origem de uma mensagem. A assinatura é feita utilizando a chave privada. É utilizada a chave pública para verificar a origem.

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 uma determinada mensagem transmitida não seja modificada 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

CCS: Cadastro de Clientes do Sistema Financeiro Nacional

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

Chave Pública: Chave de um par de chaves criptográficas que é divulgada pelo seu dono e usada para verificar a assinatura digital criada com a chave privada correspondente ou, dependendo do algoritmo criptográfico assimétrico utilizado, para cifrar e decifrar mensagens.

Chave simétrica: 3DES ou triplo DES tipo EDE (Encrypt-Decrypt-Encrypt) com 3 chaves independentes (k_1, k_2, k_3) e modo CBC (Cipher Block Chaining), sendo o Vetor de Inicialização (IV - Initialization Vector) os 64 bits (8 bytes) iniciais da Chave Simétrica

Chave simétrica cifrada: Chave simétrica criptografada com a chave pública do destinatário.

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

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

Digest: Um resumo de mensagem (message digest) é o resultado obtido com a execução de uma função hash sobre um texto.

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 seqüência de bytes cria um código chamado message digest (resumo de mensagem). O algoritmo utilizado para o SPB é SHA-1.

Geração da chave simétrica: Para cada mensagem enviada, deverá ser criada uma chave simétrica para cifrá-la.

Geração do Cabeçalho de Segurança: Preenchimento dos campos no cabeçalho de segurança que será enviado junto com a mensagem.

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 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 sua respectiva assinatura digital, 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.

PIN: Personal Identification Number - Número de Identificação Pessoal

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

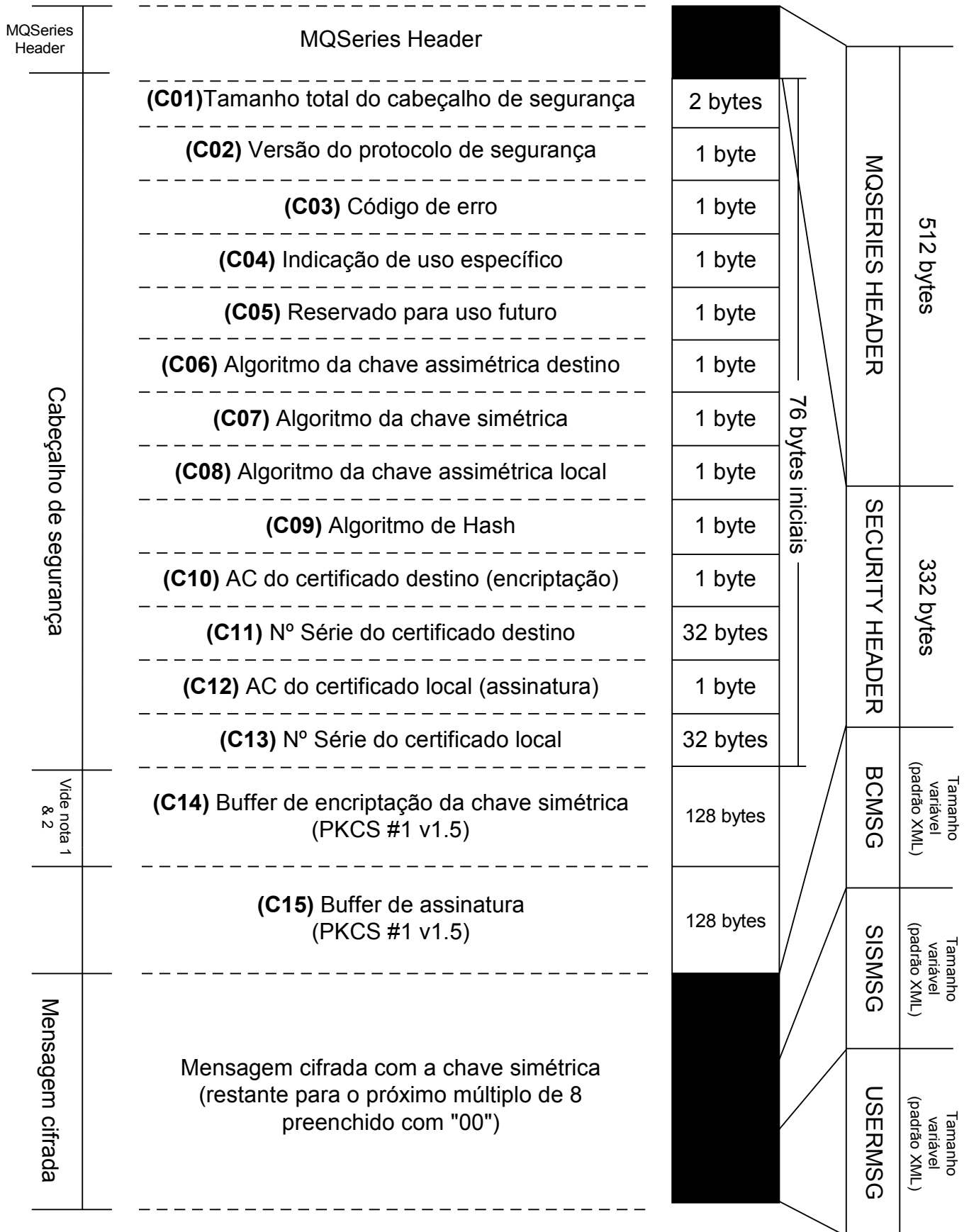
RSFN: Rede do Sistema Financeiro Nacional – Rede de telecomunicações que provê infra-estrutura para troca de informações entre o Banco Central do Brasil e instituições que operam no âmbito do Sistema de Pagamentos Brasileiro (SPB) ou no âmbito da Mensageria do Sisbacen (MES).

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.

Sistemas operacionais ou SO: Programa de computador que diz para a máquina como processar as instruções recebidas dos softwares ou dos periféricos (teclado, modem, etc). Ele gerencia a entrada e saída de dados do computador, isto é, acesso aos discos rígidos, armazenamento de dados na memória e disponibilização da informação na tela ou impressora. Um computador não funciona sem um sistema operacional.

Web Services: Sistemas de troca de informações baseados em XML que usam a Internet para interação direta entre aplicações.

Anexo A (Cabeçalho de Segurança)



Nota 1: A Chave DES consiste de 64 bits binários (= 8 bytes), desses, 8 bits (=1byte) são utilizados para verificação de paridade ímpar. Na implementação TripleDES (3DES), são utilizadas 3 chaves DES, portanto o tamanho total da chave é 192 bits = 24 bytes.

Nota 2: Devido a escolha do algoritmo simétrico 3DES e modo de operação CBC, para o vetor de inicialização devem ser usado os 8 bytes iniciais da chave simétrica.