

Projeto de Modernização do Sistema Câmbio Orientação Técnica

Versão 1.0.1

Projeto de Modernização do Sistema Câmbio	
Orientação Técnica	Versão 1.0.1

Histórico de Revisão

Data	Versão	Descrição	Autor
30/09/2010	1.0.0	Versão inicial.	Bacen
03/02/2011	1.0.1	Atualização do item 2.2 - Utilização do PSTA para troca de mensagens do Câmbio	Bacen

Projeto de Modernização do Sistema Câmbio	
Orientação Técnica	Versão 1.0.1

Sumário

1.	Introdução	4
1.1	Definições, Acrônimos, e Abreviações	4
2.	Orientações sobre utilização da Mensageria no Câmbio	4
2.1	Utilização do MQ-Series para troca de mensagens do Câmbio	5
2.2	Utilização do PSTA para troca de mensagens do Câmbio	6

Orientação Técnica

1. Introdução

O propósito desse documento é definir, em alto nível, os requisitos para implantação da infra-estrutura de troca de mensagens para a modernização do sistema Câmbio. As orientações contidas neste documento se aplicam unicamente à versão modernizada do sistema Câmbio, que utiliza as mensagens CAM0005 e posteriores, definidas no volume III do Catálogo de Mensagens e de Arquivos da RSFN. Ou seja, as mensagens CAM0001 a CAM0004, do sistema Câmbio atual, estão fora do escopo deste documento e seu uso atual não será alterado até que sejam desativadas tempestivamente.

1.1 Definições, Acrônimos, e Abreviações

Termo	Definição
Bacen	Banco Central do Brasil
IF	Instituição Financeira
Mensageria	Sistema de transferência de mensagens. Essas mensagens transmitem requisições e respostas de alguma operação ou requisições e respostas de consultas.
PSTA	Sistema de transferência de arquivos, via internet, desenvolvido pelo Bacen. Esse sistema permite uma transferência segura e assinada utilizando a criptografia.
RSFN	Rede do Sistema Financeiro Nacional
SFN	Sistema Financeiro Nacional
SPB	Sistema de Pagamentos Brasileiro
STR	Sistema de Transferência de Reservas do SPB
XML	Documento escrito em texto plano (<i>plain text</i>) desenvolvido para descrever dados ou informações. Utilizado, entre outros, para troca de informações entre sistemas que estão em diferentes plataformas.
XML Schema	O XML Schema é um documento que define a estrutura correta de um documento XML. Informa os elementos e atributos válidos no documento XML, onde eles podem aparecer no mesmo, o domínio de valores permitidos e outras informações. É utilizado para verificar a correção de um documento XML.

2. Orientações sobre utilização da Mensageria no Câmbio

O Banco Central disponibiliza o domínio MES (Mensageria Sisbacen) para serviços não vinculados ao SPB que utilizam a mensageria. Para o envio das mensagens nesse domínio, são utilizados canais, filas, endereços (DNS) e portas específicos, diferentes daqueles utilizados pelo SPB.

As instituições que participam da RSFN poderão utilizar a Mensageria via MQ-Series e, em situações de contingência, utilizar também o PSTA. As instituições que não participam da RSFN utilizarão somente o PSTA. A opção pelo uso do MQ-Series/RSFN ou PSTA/Internet é de responsabilidade da IF, que deve comunicar previamente ao Bacen sobre quaisquer mudanças. Em qualquer caso, o sistema Câmbio aceitará, de uma mesma IF, o envio de mensagens tanto pelo PSTA quanto pelo MQ-Series. As respectivas respostas, quando houver, serão sempre encaminhadas pelo mesmo meio em que foi recebido o estímulo pelo Câmbio, independente do meio de transmissão preferencial da IF. Portanto, o meio preferencial se aplicará nas situações em que a mensagem for originada no Bacen (por exemplo, mensagens R2 e avisos).

Projeto de Modernização do Sistema Câmbio	
Orientação Técnica	Versão 1.0.1

Os arquivos e as mensagens terão, obrigatoriamente, codificação Unicode UTF-16BE. Essa codificação aplica-se aos arquivos e mensagens trocados tanto por meio do aplicativo PSTA quanto por meio do MQ-Series.

2.1 Utilização do MQ-Series para troca de mensagens do Câmbio

O GT-Segurança da RSFN recomenda a utilização de certificados digitais específicos para o domínio MES, mas as IF poderão optar pela utilização do mesmo certificado que hoje é destinado às mensagens no âmbito do SPB (o Banco Central utiliza certificado específico para o domínio MES). As mensagens do grupo GEN, quando relativas ao domínio MES, também deverão ser encaminhadas pelo canal específico e assinadas com o certificado ativado para esse domínio.

A configuração do MQ-Series deve ser feita pela transação PCCS400. Caso o usuário institucional não possua autorização à transação PCCS400, esta deve ser solicitada ao master Sisbacen de sua instituição. Os procedimentos relativos à conexão MQ-Series para o domínio MES que devem ser realizados por intermédio da transação PCCS400 são: Definição de objetos MQ no BC (opção 1), em que deverão ser definidos os objetos MQ equivalentes na instituição; Ativação de canal (opção 3); e Consulta status do canal (opção 4). No caso do ambiente de homologação, antes de acessar a PCCS400, deve ser digitado HOMOLOGA na transação.

Os endereços de MQ no domínio MES obedecem à lei de formação: mqm01.xxxxxx.rsfn.net.br (produção) e mqm02.xxxxxx.rsfn.net.br (homologação), onde xxxxxx é a denominação do participante. São usadas as portas 12422 a 12429. Em homologação, o endereço do Bacen é mqm02.bcb.rsfn.net.br:12422; em produção, o endereço é mqm01.bcb.rsfn.net.br:12422.

O padrão de nome de filas e canais MES obedece a regra vigente, em que o sequencial é 02. Isto é, as filas e canais não têm seus nomes alterados. Os demais sistemas que utilizam o domínio MES compartilham as filas, canais e certificados digitais, que pertencem a todo o domínio.

As IF serão identificadas no Câmbio pelo CNPJ básico de oito posições. No caso das instituições que já participam da Mensageria do SPB, será mantido, portanto, o ISPB. O mesmo é válido para a identificação do Banco Central, que será o ISPB hoje utilizado no STR.

A ativação do certificado digital para envio e recepção de mensagens no domínio MES deve obedecer aos seguintes passos:

1. Caso não utilize o mesmo certificado do SPB, o participante deve obter o certificado de acordo com a seção 4 do Manual de Segurança do SPB, mais especificamente as subseções 4.1 e 4.2. O Certificado utilizado no domínio MES obedece à mesma formatação do utilizado no SPB.
2. Para o certificado do domínio MES, a formação do campo CN obedecerá ao disposto nos itens 4.2.1 a 4.2.4 do Manual de Segurança do SPB, indicando certificado iniciado pela letra "P" para o ambiente de produção, ou "T" para o ambiente de homologação.
3. O participante deve enviar o certificado por meio do PSTA, informando o código de documento CMES (Certificados Digitais da Mensageria Sisbacen). Ainda que opte por utilizar o certificado em uso no domínio SPB, esse certificado deve ser enviado novamente, sob o código CMES.
4. Poderão ser enviados mais de um certificado para o domínio MES, porém apenas um certificado poderá estar ativo por vez.
5. Para ativar o certificado, o participante deverá enviar mensagem GEN0006 no domínio de sistema MES. Mensagens GEN0006 enviadas ao domínio SPB não ativarão certificados do domínio MES e vice-versa. Mesmo que o participante decida utilizar um certificado já ativo no domínio SPB, deverá ativá-lo com nova mensagem GEN0006 no domínio de sistema MES.
6. O formato da mensagem GEN0006 está descrito no volume III do Catálogo de Mensagens.

Projeto de Modernização do Sistema Câmbio	
Orientação Técnica	Versão 1.0.1

Para a ativação inicial do certificado, o participante deve indicar, na mensagem, a “Situação Certificado” igual a 1 (“Ativação do primeiro certificado”).

7. A mensagem GEN0006 será obrigatoriamente assinada com a chave privada correspondente à chave pública veiculada pelo certificado que está sendo ativado. O preenchimento do cabeçalho de segurança obedecerá ao disposto na seção 5 do Manual de Segurança da RSFN, mais especificamente ao disposto nas subseções 5.1 e 5.6. O byte C04 (“Indicação de Tratamento Especial”) deverá ser igual a 1 (“Mensagem relativa à segurança ou que utiliza um certificado ainda não ativado”).
8. A recepção da mensagem GEN0006R1 indicará a ativação bem-sucedida do certificado, habilitando o participante para envio e recepção de todas as mensagens do domínio MES, entre as quais, as do grupo CAM.
9. No domínio de sistema MES, há envio de mensagens GEN0007 após a ativação dos certificados.
10. Os certificados do domínio de sistema MES poderão ser consultados por meio da mensagem GEN0008, que deverá ser preenchida de acordo com o disposto no volume III do Catálogo de Mensagens e de Arquivos da RSFN, e enviada nesse domínio de sistema MES.
11. Mensagens do grupo de serviço CAM deverão sempre estar assinadas e cifradas, utilizando o certificado ativo no domínio de sistema MES. Esse grupo de mensagens obedecerá ao disposto no Manual de Segurança da RSFN e no volume III do Catálogo de Mensagens e de Arquivos da RSFN.

2.2 Utilização do PSTA para troca de mensagens do Câmbio

Não há necessidade de certificado digital para a utilização do PSTA, seja para envio de arquivos ou de mensagens. Para uso do PSTA, o operador deve estar cadastrado na transação PSTA300. Para o envio ou recepção de mensagens relativas ao Câmbio, o operador deve, também, estar cadastrado no serviço SMES001. **(NR)**

Todos os arquivos e mensagens trocados via PSTA devem ser compactados no padrão zip. O PSTA não efetua a compactação, ficando essa, portanto, a cargo da IF emissora do arquivo. O arquivo ou a mensagem devem ser gerados no formato UTF-16BE com a extensão “.XML” e, em seguida, compactados, de modo que o arquivo enviado ao Câmbio é um “.zip”, com um único arquivo XML dentro.

São utilizados os arquivos AMES101 (produção) e AMES111 (homologação), para envio de mensagens ao destinatário Bacen, e arquivos AMES102 (produção) e AMES112 (homologação), para envio de mensagens ao destinatário participante. As mensagens do grupo GEN são exclusivas da mensageria MQ-Series – só são tratados pelo Câmbio arquivos que contenham mensagens do grupo Câmbio, sendo as únicas exceções a GEN0004, utilizada para informar erros de formatação, e as mensagens GEN0001/GEN0001R1, utilizadas para testes de conectividade com a mensageria. **(NR)**

As mensagens enviadas via PSTA devem possuir toda a estrutura XML – *Tags* DOC, BCMSG, SISMSG e USERMSG (opcional) – em formato UTF-16BE, conforme definido no volume III do Catálogo de Mensagens e de Arquivos da RSFN, porém sem o cabeçalho de segurança.

Informações quanto ao uso do PSTA, inclusive relativas à automatização do recebimento e envio de arquivos, podem ser encontradas no arquivo “Leia-me” do próprio aplicativo.