

## CARTA-CIRCULAR 3134 – Banco Central do Brasil

### **Divulga os procedimentos e padrões técnicos para uso de a assinatura digital em contratos de câmbio.**

**1)** Tendo em vista o disposto na Circular 3.234, de 15 de abril de 2004, informamos que os agentes autorizados ou credenciados a operar em câmbio, que façam uso de assinatura digital em contratos de câmbio, devem adotar os seguintes procedimentos:

**I)** os certificados digitais utilizados na assinatura de contratos de câmbio devem ser emitidos por Autoridades Certificadoras no âmbito da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, instituída pela Medida Provisória MP 2.200-2, de 24 de agosto de 2001, e podem ser do tipo A1, A2, A3 ou A4, a critério da parte contratante autorizada ou credenciada a operar em câmbio, com chaves assimétricas de no mínimo 1024 bits;

**II)** o texto do contrato de câmbio deve ser armazenado exclusivamente em código ASCII (formato texto) devendo refletir o conteúdo do contrato registrado no Sisbacen, incluindo a sua numeração.

**2.** Devem ser observados, pela parte contratante autorizada ou credenciada a operar em câmbio, os seguintes padrões técnicos:

**I)** o formato do arquivo contendo o contrato de câmbio assinado digitalmente deve adotar o padrão Public-Key Cryptography Standard nº 7 (PKCS#7), versão 1.5, conforme detalhado no "Request for Comments" (RFC) 2315, do Internet Engineering Task Force - IETF, com a estrutura "ContentType" igual a "SignedData" e com o conteúdo do contrato de câmbio presente no campo "content" da estrutura "contentInfo";

**II)** para geração do "digest" (resumo do documento) deve ser utilizado o algoritmo de "hashing" SHA-1 (RFC 3174);

**III)** na assinatura digital deve ser utilizado o algoritmo assimétrico RSA, com uso das respectivas chaves privadas das partes para cifragem do "digest" do documento, no padrão PKCS#1 (RFC 2313);

**IV)** cada assinatura deve ser executada considerando o atributo "signingTime" no campo "authenticatedAttributes" da estrutura "SignerInfo", refletindo a data-hora de sua efetivação, sendo que todas as assinaturas assim obtidas devem estar no mesmo nível na estrutura do PKCS#7, pela repetição do campo "SignerInfo" da estrutura "SignedData", tantas vezes quantas forem o número de assinaturas digitais apostas. A data-hora de efetivação deve ser controlada pela contratante;

**V)** o pacote PKCS#7 resultante, contendo o contrato de câmbio, as assinaturas digitais geradas e os respectivos certificados digitais utilizados, deve ser armazenado em claro, conforme definido no inciso I, pelo prazo que a regulamentação cambial determinar, sendo opcional o armazenamento dos certificados digitais das Autoridades Certificadoras participantes da cadeia de confiança, bem como das respectivas Listas de Certificados Revogados (LCRs);

**VI)** para efeito de apresentação ao Banco Central do Brasil, quando solicitado, contratante deve manter cópia em claro do pacote PKCS#7, sem envelopamento para cifragem, conforme descrito no inciso V acima;

**VII)** a contratante que tiver a necessidade de cifrar os dados para segurança adicional na transmissão pode, para tal, fazer uso de qualquer padrão.

**Brasília, 27 de abril de 2004.**

**Departamento de Tecnologia da Informação  
Fernando de Abreu Faria Chefe**

**Fonte:**

<http://www5.bcb.gov.br/normativos/detalhamentocorreio.asp?N=104062827&C=3134&ASS=CARTA-CIRCULAR+3.134>