e-Financeira

Manual para Compactação e Criptografia de dados

Versão 1
08 de maio de 2017
Anexo Único do ADE COFIS Nº 33/2017

Sumário

1. COMPACTAÇÃO DE DADOS

1.1. ORIENTAÇÕES INICIAIS

A solução técnica para a recepção de lotes compactados pelo sistema e-Financeira visa permitir uma melhora de performance na transmissão dos arquivos. O uso dessa solução é opcional por parte das entidades obrigadas à e-Financeira, no entanto recomenda-se sua utilização devido ao ganho potencial de performance nessa transmissão.

1.2. PREMISSAS

O modelo da compactação foi proposto segundo as premissas abaixo:

- A solução adotada utiliza o formato GZIP para comprimir os arquivos do sistema e-Financeira;
- Solução de compactação de padrão aberto e público;
- A solução possibilitará uma troca de arquivos com um fluxo mais ágil, pois a compactação permitirá um menor fluxo de dados transitando na rede;
- Foi priorizada uma rápida implementação com segurança e robustez.

1.3. MODELO DE COMPACTAÇÃO

O modelo utiliza GZIP para compactar os arquivos a serem enviados pelas Instituições Financeiras. O envio será realizado pelos Serviços WEB canal comum não criptografado e outro com canal criptografado SSL.

O GZIP é um mecanismo de compressão público e livre, sendo uma tecnologia aceita no mercado profissional e acadêmico.

Ao utilizar a compactação no envio dos lotes, será estabelecido novas possibilidades para as Instituições Financeiras enviarem os seus respectivos lotes de arquivos, sendo oferecidos novos métodos de recepção.

1.3.1. USO DO MÉTODO GZIP PARA ENVIO DE LOTE NÃO CRIPTOGRAFADO

Foi criado somente um novo método (ReceberLoteEventoGZip) no web service já existente: https://efinanc.receita.fazenda.gov.br/WsEFinanceira/WsRecepcao.asmx

Como utilizar:

Após a geração do arquivo xml de lote, o mesmo deverá:

a) ser compactado utilizando GZIP;

b) transformado em um array de bytes;

c) o array de bytes (base64) passado como parâmetro ao método ReceberLoteEventoGZip do Web Service.

1.3.2. USO DO MÉTODO GZIP PARA ENVIO DE LOTE CRIPTOGRAFADO

Foi criado somente um novo método (ReceberLoteEventoCriptoGZip) no web service já existente:
https://efinanc.receita.fazenda.gov.br/WsEFinanceiraCripto/WsRecepcaoCripto.asmx

Como utilizar:
Após a geração do arquivo xml de lote, o mesmo deverá:
a) ser compactado utilizando GZIP;

b) com o array de bytes do lote compactado, deve ser feito o processo de criptografia padrão da e-Financeira;
c) o array de bytes (base64) criptografado passado como parâmetro ao método ReceberLoteEventoCriptoGZip do Web Service.

1.4. FLUXO PARA O ENVIO DOS ARQUIVOS

1.4.1. FLUXO DE PROCESSOS PARA GERAÇÃO E ENVIO DE ARQUIVOS NÃO CRIPTOGRAFADOS

CLIENTE (Instituição Financeira)			SERVIDOR (e-Financeira)
1	Compactar lote do arquivo XML a ser enviado		
2	Estabelecer túnel SSL com o Web Service do e-Financeira.	**<-->**	Estabelecer túnel SSL com o Web Service Cliente da Instituição Financeira.
3	Enviar esse arquivo compactado como parâmetro (base64)	**-->**	
4		*****	Obter o arquivo compactado e descompactá-lo utilizando a metodologia adotada no GZIP
5			Verificar a estrutura do XML.
6		*****	Processar o arquivo XML e realizar as validações do e-Financeira.
7		*****	Gerar o Recibo do Evento.
8		*****	Assinar o recibo do evento.
9		**<--**	Enviar Recibo do Evento ao Cliente.

1.4.2. FLUXO DE PROCESSOS PARA GERAÇÃO E ENVIO DE ARQUIVOS CRIPTOGRAFADOS

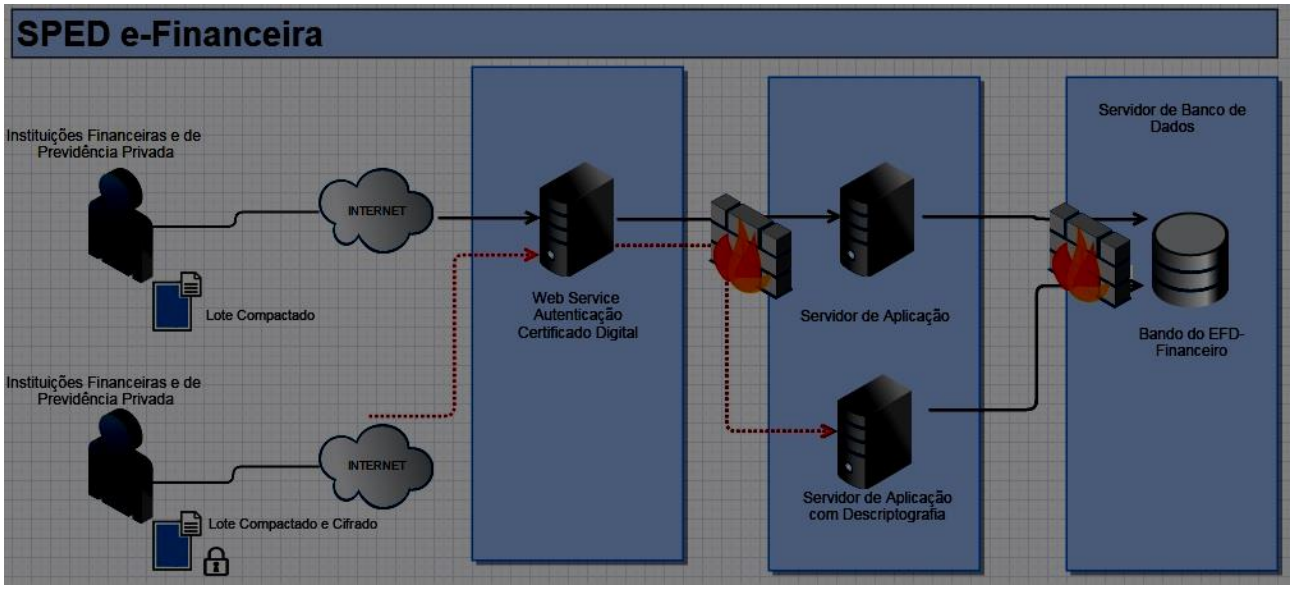
CLIENTE (Instituição Financeira)			SERVIDOR (e-Financeira)
1	Definir uma chave de Criptografia.	*****	
2	Compactar o arquivo XML do lote a ser enviado com GZIP		
3	Criptografar o arquivo compactado a ser enviado (utilizando a Chave de Criptografia, definida no item 1).	*****	
4	Criptografar a Chave de Criptografia, definida no item 1, com a Chave Pública do Certificado Digital ICP Brasil do Servidor e-Financeira.	*****	
5	Gerar um novo arquivo XML do e-Financeira, contendo: • Identificação de Evento de envio de Dados e-Financeira em modo Criptografado. • Chave de Criptografia • Mensagem criptografada	*****	
6	Estabelecer túnel SSL com o Web Service do e-Financeira.	**<-->**	Estabelecer túnel SSL com o Web Service Cliente da Instituição Financeira.
7	Enviar ao servidor e-Financeira, o arquivo XML (gerado no item 5).	**-->**	
8		*****	Descriptografar a Chave Simétrica, com a Chave Privada do Certificado do e-Financeira.
9		*****	Com a Chave Simétrica (obtida no item 8), descriptografar a Mensagem (arquivo xml criptografado).

10		*	Obter o arquivo compactado e descompactá-lo utilizando a metologia adotada no GZIP
11		*	Verificar a estrutura do XML.
12		*	Processar o arquivo XML (obtido na descompactação da mensagem) e realizar as validações do e-Financeira.
13		*	Gerar o Recibo do Evento.
14		*	Assinar o recibo do evento. (Obs.: Recibo não será criptografado).
15		<--	Enviar Recibo do Evento ao Cliente.

1.5. CONSIDERAÇÕES

Serão mantidos os dois Web Services existentes na produção, porém cada serviço terá um método que possibilitará o recebimento dos arquivos compactados. Será mantido o mesmo nível de segurança no transporte dos arquivos, utilizando o canal SSL para fornecer um túnel autenticado, ficando a cargo da Instituição Financeira a forma em que serão transmitidos os arquivos.

1.6. ARQUITETURA DA SOLUÇÃO UTILIZANDO A COMPACTAÇÃO DE ARQUIVOS



2. CRIPTOGRAFIA DE DADOS

2.1. ORIENTAÇÕES INICIAIS

Essa versão do manual traz atualizações referentes aos thumbprints utilizados nos certificados de produção e pré-produção disponíveis para download no Portal SPED. Não houve quaisquer alterações nas demais orientações desse manual anteriormente disponibilizado no respectivo portal.

Conforme artigo 2º do Ato Declaratório Executivo COFIS nºXX, de 05 de maio de 2017, a utilização desse modelo de criptografia de dados da e-Financeira passa a ser obrigatória para quaisquer arquivos transmitidos a partir do primeiro dia útil de março de 2018, inclusive para enviar retificações de arquivos transmitidos/a serem transmitidos sem criptografia até o último dia útil de fevereiro de 2018 (data final para a possibilidade de transmissão de arquivos da e-Financeira sem criptografia dos dados).

2.2. MODELO DE CRIPTOGRAFIA

Esse modelo possibilita que os dados sejam criptografados, ainda no disco da Instituição Financeira, para serem enviados ao servidor do e-Financeira. O envio deste arquivo será realizado sobre o túnel criptografado TLS.

A abordagem de criptografia híbrida foi escolhida para possibilitar que a solução possua performance nas operações de cifragem/decifragem dos arquivos e também possa ser possível compartilhar a chave de criptografia entre o servidor e o cliente de forma segura.

Neste esquema de criptografia utiliza-se um algoritmo de chave simétrica para criptografar a mensagem a ser enviada. Esta chave simétrica será criptografada com um algoritmo de chave assimétrico, possibilitando que apenas o destinatário, detentor da chave privada, possa obter a chave simétrica para descriptografar a mensagem com o algoritmo de chave simétrica. Assim, o arquivo a ser enviado ao e-Financeira conterá uma mensagem criptografada simetricamente e sua chave criptografada assimetricamente com a chave pública do Certificado ICP-Brasil do e-Financeira.

Ao recepcionar o arquivo criptografado, o e-Financeira realizará os procedimentos para descriptografia e obterá o arquivo XML original (anexado na mensagem). Com este XML, o e-Financeira realizará as verificações necessárias e executará os processos do evento solicitado. Por fim, será gerado o Recibo do Evento que será assinado pelo e-Financeira e enviado para a Instituição Financeira declarante. O arquivo de Recibo de Evento não será criptografado, mas sim assinado digitalmente.

2.3. FLUXO DE PROCESSOS PARA GERAÇÃO E ENVIO DE ARQUIVOS CRIPTOGRAFADOS

CLIENTE (Instituição Financeira)			**SERVIDOR (e-Financeira)**
1	Definir uma chave de Criptografia.	*****	
2	Criptografar o arquivo XML a ser enviado ao e-Financeira (utilizando a Chave de Criptografia, definida no item 1).	*****	
3	Criptografar a Chave de Criptografia, definida no item 1, com a Chave Pública do Certificado Digital ICP Brasil do Servidor e-Financeira.	*****	
4	Gerar um novo arquivo XML do e-Financeira, contendo: • Identificação de Evento de envio de Dados e-Financeira em modo Criptografado. • Identificação (thumbprint do certificado do servidor da e-Financeira) • Chave de Criptografia (gerada no item 3). • Mensagem criptografada (gerada no ítem2)	*****	
5	Estabelecer túnel TLS com o Web Service do e-	**<-->**	Estabelecer túnel TLS com o Web Service Cliente

	Financeira.		da Instituição Financeira.
6	Enviar ao servidor e-Financeira, o arquivo XML (gerado no item 4).	**-->**	
7		*****	Verificar a estrutura do XML.
8		*****	Descriptografar a Chave Simétrica, com a Chave Privada do Certificado do e-Financeira.
9		*****	Com a Chave Simétrica (obtida no item 8), decriptografar a Mensagem (arquivo xml criptografado).
10		*****	Processar o arquivo XML (obtido na descriptografia da mensagem) e realizar as validações do e-Financeira.
11		*****	Gerar o Recibo do Evento.
12		*****	Assinar o recibo do evento. (Obs: Recibo não será criptografado).
13		**<--**	Enviar Recibo do Evento ao Cliente.

2.4. ENVIO DE LOTES CRIPTOGRAFADOS

Será disponibilizado no Servidor de Aplicação uma função de Web Service alternativa para recepção de lote de eventos, adicionando mais uma camada de criptografia, além do https já utilizado.

Esse Servidor de Aplicação irá receber um lote de eventos criptografado. Em seguida irá descriptografá-lo, validá-lo e gerará o resultado do processamento do lote que deverá ser armazenado pela empresa declarante para consultas posteriores ao resultado do processamento do lote. Para utilizar este modelo, a empresa declarante deverá seguir os seguintes passos:

1. Gerar uma chave/vetor inicialização AES-CBC 128 randomicamente.

2. Encriptar o arquivo xml de lote original (conforme xsd envioLoteEventosv1_0_1.xsd) com a chave AES-CBC 128 gerada.

3. Encriptar a chave AES-CBC 128 gerada no item 2, com a chave pública do certificado e-Financeira gerado exclusivamente para este fim, utilizando o algoritmo RSA com chave de 2048 bits. Este certificado está disponível no site do Portal SPED na sessão da e-Financeira para download.

4. Gerar o arquivo XML conforme layout de envio de arquivo de lote criptografado

2.5. MODO DE OPERAÇÃO DOS ALGORITMOS DE CRIPTOGRAFIA

- Algoritmo Assimétrico: RSA - 2048 Bits
- Padding para Criptografia Simétrica: PKCS#7
- Padding para Criptografia Assimétrica: PKCS#1 V1.5
- Algoritmo de Criptografia Simétrico: AES - 128 Bits - CBC
- Vetor de Inicialização: Concatenar o Vetor de Inicialização, em Binário. Ao final da Chave Criptográfica (também em binário) encriptar e depois proceder a conversão para Base64.
- Codificação para escrita do XML: Base64

2.6. LEIAUTE

O layout para envio de arquivo de lote criptografado é definido pelo Schema envioLoteCriptografado-v1_0_0.xsd

A estrutura é apresentada abaixo:

tag	eFinanceira			
descrição	Tag raiz do documento			
obrigatório	Sim			
ocorrência	Única			
campo	**obrigatoriedade**	**ocorrência**	**valores válidos**	**descrição**
xmlns	obrigatório	1	http://www.eFinanceira.gov.br/schemas/envioLoteCriptografado/v1_0_0	Namespace do XSD do envio de lote criptografado

tag	loteCriptografado
descrição	Contém as informações necessárias ao envio de um lote criptografado
obrigatório	Sim
ocorrência	Única

tag	id
descrição	Identificador do lote criptografado na empresa declarante
obrigatório	Sim
ocorrência	Única

***OBS: Este campo não é criptografado**

tag	idCertificado
descrição	Identificador (thumbprint) do certificado chave pública do servidor da e-Financeira
obrigatório	Sim
ocorrência	Única

tag	chave
descrição	Contém a chave AES-CBC 128 gerada randomicamente encriptada com o certificado chave pública do servidor da e-Financeira, em Base64.
obrigatório	Sim
ocorrência	Única

tag	lote
descrição	Contém o lote criptografado com a chave AES-CBC 128 gerada randomicamente, em Base64.
obrigatório	Sim
ocorrência	Única

2.7. DADOS PARA A CHAMADA AO WEB SERVICE DE ENVIO DE LOTE CRIPTOGRAFADO

Nome do método	ReceberLoteEventoCripto
Requer Certificado?	Sim. **Observação**: O certificado deve atender a uma das seguintes exigências: • Ser o responsável pela informação. • Ser representante legal do responsável pela informação • Ser procurador do responsável pela informação
***Schema* Parâmetro loteEventos**	envioLoteCriptografado-v1_0_0.xsd
***Schema* Retorno**	retornoLoteEventos-v1_0_1.xsd
URL	Produção: https://efinanc.receita.fazenda.gov.br/WsEFinanceiraCripto/WsRecepcaoCripto.asmx Certificado a ser utilizado para criptografia do lote: efinanc_web.cer idCertificado (thumbprint): 4f96a2a59ef1248411e0ec4b3aed7f3c3e2d6727 Pré-produção: https://preprod-efinanc.receita.fazenda.gov.br/WsEFinanceiraCripto/WsRecepcaoCripto.asmx Certificado a ser utilizado para criptografia do lote: preprod-efinanc.cer idCertificado (thumbprint): 88edffa74bf7984197c1749ba96f56372dc02bac

2.8. MENSAGENS RETORNADAS PELO WEB SERVICE DE ENVIO DE LOTE CRIPTOGRAFADO

MS0040 - Informação recebida não é um arquivo XML:
Ocorre quando não é enviado para o Web Service um arquivo XML

MS0041 - Erro na estrutura do xml do lote criptografado:
Ocorre quando há erro na validação do xml recebido com o Schema definido.

MS0042 - Não foi possível descriptografar a chave com o identificador (thumbprint) do certificado chave pública do servidor da e-Financeira informado:
Ocorre quando foi passado um identificado do certificado (thumbprint) que não é referente ao certificado do servidor da e-Financeira.

MS0043 - Não foi possível descriptografar o lote de eventos utilizando a chave informada:
Ocorre quando o servidor da e-Financeira não consegue descriptografar o lote com a chave que foi informada.

MS0044 - Não foi possível descompactar o lote recebido.