Serviço Federal de Processamento de Dados SERPRO

e-Financeira

Modelo técnico de criptografia de arquivos e-Financeira.

Versão 1 - 18/07/2016

1 OBJETIVO:

O objetivo deste documento é apresentar uma proposta de solução técnica para criptografia dos dados, a serem enviados para o sistema e-Financeira. Em atendimento da demanda RFB, foi desenvolvido um modelo que possibilite a criptografia dos dados a serem enviado pelas instituições financeiras, para o sistema e-Financeira.

2 MODELO DE CRIPTOGRAFIA PROPOSTO:

A solução técnica proposta, objetiva possibilitar 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 decriptografia 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.

2.1 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-Financeira.	<-->	Estabelecer túnel TLS com o Web Service Cliente 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.

2.2 Modo de Operação dos Algoritmos de Criptografias e-FinanceiraRecepção de arquivos de lote criptografados

2.2.1 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, descriptografá-lo, validá-lo e gerar 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 envioLoteEventos-v1_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 será publicado no site do e-Financeira para download.

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

2.2.2 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

2.2.3 Layout

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

2.2.4 Dados para a Chamada ao Web Service de Envio de Lote Criptografado

2.3

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_1.xsd
***Schema* Retorno**	retornoLoteEventos-v1_0_1.xsd
URL	https://efinanc.receita.fazenda.gov.br/WsEFinanceiraCripto/WsRecepcaoCripto.asmx

2.3.1 Mensagens retornadas pelo web service de envio de lote criptografado

2.4 MS0040 - Informação recebida não é um arquivo XML:

2.5 Ocorre quando não é enviado para o Web Service um arquivo XML

válido.

2.6 MS0041 - Erro na estrutura do xml do lote criptografado.:

2.7 Ocorre quando há erro na validação do xml recebido com o schema definido.

2.8 MS0042 - Não foi possível descriptografar a chave com o identificador (thumbprint) do certificado chave pública do servidor da e-Financeira informado:

2.9 Ocorre quando foi passado um identificado do certificado (thumbprint) que não é referente ao certificado do servidor da e-financeira.

2.10 MS0043 - Não foi possível descriptografar o lote de eventos utilizando a chave informada:

2.11 Ocorre quando o servidor da e-Financeira não consegue descriptografar o lote com a chave que foi informada.