Índice

1. Certificado Digital

O certificado digital é um documento eletrônico que garante proteção às transações online e a troca virtual de documentos, mensagens e dados, com validade jurídica.
Com este dispositivo, os sistemas de informação podem validar e reforçar os mecanismos de segurança online, utilizando a tecnologia para garantir a privacidade e confirmar a autenticidade das informações dos usuários, empresas e instituições na rede.

2. A anatomia do certificado utilizado para a assinatura de remessas financeiras do Banco do Brasil

O certificado padrão X.509 contém os seguintes campos:

- Versão - Contem a versão do certificado;
- Número serial - Todo certificado possui um, não é globalmente único, mas único no âmbito de uma AC (Autoridade Certificadora). AC LCRs usam o serial para apontar quais certificados se encontram revogados;
- Tipo de algoritmo - Contém um identificador do algoritmo criptográfico usado pela AC para assinar o certificado juntamente com o tipo de função de hash criptográfica usada no certificado;
- Nome do titular - Nome da entidade (Jurídica ou Física) para o qual o certificado foi emitido;
- Nome do emitente - Autoridade Certificadora que emitiu/assinou o certificado;
- Período de validade - Mostra o período de validade do certificado;
- Informações de chave pública da entidade;
- Algoritmo de chave pública;
- Chave pública;
- Assinatura da AC - A garantia que a AC provê sobre a veracidade das informações contidas neste certificado de acordo com as políticas da AC;
- Identificador da chave do titular - É uma extensão do X.509 que possui um identificador numérico para a chave pública contida neste certificado, especialmente útil para que programas de computador possam se referir a ela;

- Identificador da chave do emitente - A mesma ideia mencionada anteriormente, só que se referindo à chave pública da AC que emitiu o certificado;
- Atributos ou extensões - A vasta maioria dos certificados X.509 possui campos chamados extensões (OID) que proveem algumas informações extras, como cadastros adicionais do titular e do emitente, especificações de propósito do certificado e etc.

3. Assinatura Digital – Certificação A1 – Banco do Brasil

O processo de assinatura digital do arquivo financeiro do Banco do Brasil foi construído através da biblioteca System.Security da Framework 4.0 do .NET
Esta biblioteca trata dados criptografados e assinados digitalmente conforme Padrão CADES e Política AD-RB.
A aplicação em resumo realiza a assinatura e co-assinatura de arquivos bancários emitidos pelo sistema RM Nucleus através de um certificado digital e os envia ao Banco do Brasil que realiza um "severa" validação quanto as assinaturas existentes neste arquivo e regras de negócio definidas por esta entidade.

4. Segurança - Assinatura do Arquivo

Segurança quanto à aplicação

O arquivo financeiro (remessa financeira) criado para pagamento realizado pelo Banco do Brasil deverá ser gerado através do sistema "TOTVS Gestão de Estoque, Compras e Faturamento" e somente através dele. Qualquer outra tentativa de criação de um arquivo de pagamento que seja realizado fora do sistema "TOTVS Gestão de Estoque, Compras e Faturamento" não será validado pelo Portal SGO, responsável pela assinatura e envio do arquivo ao Banco do Brasil.
Ao gerar uma remessa de pagamento o sistema realiza diversos processos internos nos quais registros são inseridos na base de dados do SEBRAE que serão reconhecidos pelo Portal SGO responsável pela assinatura digital do arquivo.

A geração da remessa financeira é realizada somente por pessoas autorizadas, definidas pelo SEBRAE através de definições de perfis existentes no "TOTVS Gestão de Estoque, Compras e Faturamento". Lembramos que para realizar a geração deste arquivo é necessário que o

usuário responsável efetue um Login no sistema através de um usuário e senha que são únicos e intransferíveis.

Após a realização do processo descrito a remessa financeira deverá passar por um procedimento de assinatura, co-assinatura e envio ao banco do Brasil.

A assinatura da remessa financeira deverá ser realizada por Diretores e Procuradores do SEBRAE, qualquer outro "tipo de usuário" não será aceito como assinante do arquivo.

Para que um Diretor/Procurador possa assinar um arquivo de remessa financeira o mesmo deverá ser definido como tal. Pra isso a customização trabalha com o sistema de perfis, onde usuários do sistema "TOTVS Gestão de Estoque, Compras e Faturamento" são classificados como Diretores/Procuradores. Para a definição destes perfis o usuário Diretor/Procurador deverá obrigatoriamente informar o seu certificado digital bem como digitar o PIN (senha) deste certificado garantido que o mesmo é o proprietário do certificado informado.

A senha informada neste processo é criptografa pelo sistema garantindo a segurança dos dados informados. Além da segurança quanto a definição de perfis Diretor/Procurador o sistema exige a definição de quais usuários possuem permissão de acesso ao menu de "Aprovação do Pagamento Eletrônico". Os usuários Diretores/Procuradores deverão ter associados ao seu usuário o perfil com permissão de acesso ao menu de "Aprovação da Remessa Financeira", permitindo assinar e co-assinar a remessa financeira.

Obs.: Somente usuários permitidos pelo SEBRAE possuem a permissão para definir perfis de acesso ao sistema "TOTVS Gestão de Estoque, Compras e Faturamento" e Portal SGO.

Após a definição de perfis referentes ao papel Diretor/Procurador e acesso a menus, o sistema permitirá aos usuários devidamente autorizados realizar a assinatura e co-assinatura dos arquivos. No próximo tópico demonstrarei a segurança destes arquivos assinados digitalmente.

Qualquer assinatura realizada através do portal SGO será gravado em banco guardando data, usuário e papel do assinante (Diretor/Procurador), dessa forma remessas que não passarem por este ciclo não serão reconhecidos como arquivos válidos e assinados, sendo informados ao usuário pelo sistema quanto a inconsistência deste ciclo.

Ao realizar a assinatura (aprovação) da remessa financeira através do Portal SGO o sistema irá exigir a digitação da senha (PIN) referente ao certificado digital do Diretor/Procurado garantindo a identidade do usuário assinante. Vale lembrar que o usuário Diretor/Procurador necessita efetuar um Login no Portal SGO através de um usuário e senha que são únicos e intransferíveis.

Após o processo de assinatura e co-assinatura o sistema será o responsável pelo envio desta remessa ao banco do Brasil. O envio é realizado através de uma VPN e um FTP onde usuários e senhas são necessários para acesso ao caminho definido pelo banco do Brasil. O usuário e senha para estes acessos estão registrados em banco e devidamente criptografados. A transmissão dos arquivos texto (base64) via VPN, utiliza o comando ASCII (Configura o tipo de transferência de arquivos para ASCII) no script de FTP.

Após o envio da remessa financeira o banco do Brasil irá realizar “severas” validações quanto à assinatura e co-assinatura, algumas das validações realizadas:

- Verifica se a remessa foi assinada;
- Realiza toda a validação do certificado (se certificado confiável, se certificado revogado, validade quanto à data, agência certificadora confiável, cadeia de certificação, etc.);
- Realiza toda a validação da assinatura (se assinatura válida, faz a conferência do hash utilizado para a assinatura do pacote, validade quanto à data da assinatura, etc.).
- Certificado inválido.
- Assinatura inválida.
- Sequencia de assinaturas (Diretor/Procurador)
- Ao menos duas assinaturas realizadas
- Se o usuário assinante é o mesmo co-assinante, o que não é permitido.
- Validação dos atributos obrigatórios existentes no arquivo após a assinatura do arquivo. Os atributos são: Content Type, Message Digest, Signing Time.
- Cada linha do arquivo deverá conter no máximo 76 caracteres e com CR+LF ao final de cada linha

Segurança quanto a Assinatura

O tráfego de arquivos assinados e enviados ao banco do Brasil é todo realizado na Base 64.

BASE 64 é um método de codificação de dados que permite transformar dados binários (seqüência de bytes) em dados no formato American Standard Code for Information Interchange (ASCII), que é imprimível (texto). Assim, possibilita que dados originalmente no formato binário, após a transformação, possam ser transmitidos através de meios que não permitem dados binários. O conjunto de caracteres ASCII é constituído por 64 caracteres ([A-Za-z0-9], "/" e "+").
Arquivos em Base 64 garante que não será perdido qualquer dado durante a transmissão destes arquivos. Vale ressaltar também que a transformação do arquivo original em BASE 64 segue um padrão definido pelo Banco do Brasil que só o sistema da TOTVS conhece. Quanto ao padrão me refiro à quantidade de caracteres permitidos por cada linha do arquivo e caracteres especiais que definem o final de cada linha existente no arquivo.

O resultado da assinatura e co-assinatura digital da remessa financeira é chamado de pacote PKCS#7. Estes pacotes contêm além do arquivo original codificado, o certificado digital correspondente à chave privativa utilizada para criptografar o arquivo (hash) mais o próprio hash criptografado.
Na verificação da assinatura, a aplicação recebe o arquivo original e gera seu
hash (h1). A seguir, o sistema verificador abre o pacote PKCS#7, retira dele o certificado e de dentro do certificado obtém a chave pública do mesmo. Ainda desse pacote, retira o hash criptografado nele armazenado. Decriptografa o hash utilizando a chave pública que leu do certificado contido no PKCS#7. Essa decriptografia gera um segundo hash (h2). Se o h1 = h2, o arquivo original (que deu origem ao primeiro hash) está íntegro, ou seja, não sofreu qualquer alteração desde o momento em que foi assinado.

O arquivo PKCS#7 fornece a capacidade para implementar vários serviços de segurança. Um serviço de segurança é um tipo de proteção de dados e é independente do mecanismo ou algoritmo de criptografia pelo qual ele é implementado.
A criptografia de dados é fornecida através de envelopes digitais. Este sistema de segurança fornece uma alta probabilidade de que apenas **um destinatário** (Banco do Brasil) pretendido possa ler essa mensagem. O envelope digital criptografa uma mensagem para um conjunto de destinatários.
A autenticação de entidades e integridade de dados é fornecida através de assinaturas digitais. Esses serviços de segurança fornecem a garantia de que uma entidade que alega ser o autor

ou remetente de uma mensagem (SEBRAE) seja realmente essa entidade, e que os dados não foram modificados desde que ela foi assinada.

Um conjunto de signatários pode assinar digitalmente uma mensagem (Diretor/Procurador). Além disso, cada assinatura possui um conjunto de atributos.

Os serviços de segurança mencionado anteriormente são combinados para fornecer autenticação de entidade, a integridade dos dados e a confidencialidade dos dados.

Este pacote é enviado ao Banco do Brasil que após as validações necessárias fornece um feedback ao SEBRAE quanto a aprovação das assinaturas.

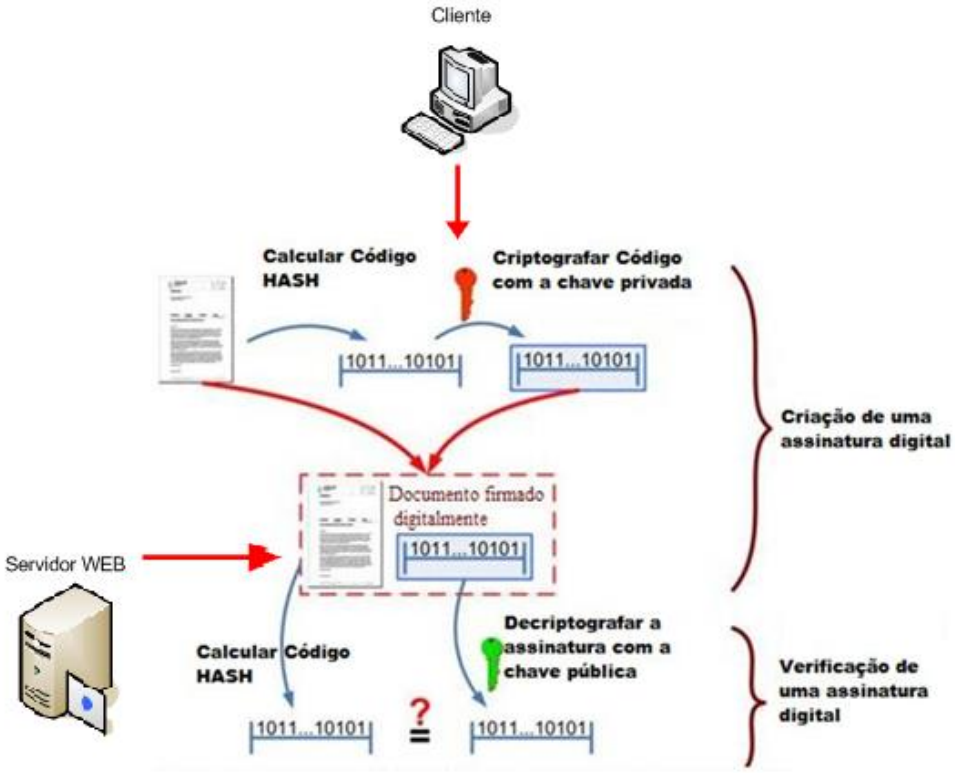

Figura 01 - Fluxo da certificação digital que ocorrerá na autorização se dará da seguinte forma:

O Banco do Brasil é responsável por todas as validações do pacote enviado. Algumas dessas validações são realizadas pelo sistema TOTVS antes da geração deste pacote como exemplificado anteriormente.

Lembramos que qualquer alteração realizada neste pacote que não seja realizada pelo sistema TOTVS será recusado no momento das validações realizadas pelo Banco do Brasil.

Em resumo quanto à segurança temos:

- Usuários definidos com perfil “Financeiro” para a geração dos arquivos de remessa financeira que são gerados somente pela aplicação TOTVS. Estes usuários necessitam de usuário e senha para acesso a aplicação TOTVS;

- Usuário definidos com o perfil de Diretores/Procuradores para assinatura e co-assinatura da remessa financeira. Além da definição dos “papeis” (Diretor/Procurador) destes usuários os mesmos necessitam de um perfil quando a permissão de acesso a menu associados ao seu usuário. A definição do papel de Diretor/Procurador necessita da informação do certificado bem como a senha deste certificado garantindo que o mesmo é o proprietário do certificado.

- Todo o tráfego dos arquivos assinados é realizado na BASE 64 seguindo regras definidas pelo Banco do Brasil que somente o sistema TOTVS os possui.

- O resultado da remessa assinada é um arquivo no formato PKCS#7. Arquivo que segue regras de segurança e autenticações necessárias para a sua geração. Arquivos gerados fora do padrão não são aceitos.

- O envio do pacote assinado é realizado através de uma VPN e FTP definidos pelo Banco do Brasil necessitando de usuário e senha para acesso ao caminho definido pelo Banco do Brasil. Usuários e senhas são armazenados na base do SEBRAE devidamente criptografados.

- A remessa financeira enviada ao Banco do Brasil “sofre” severas validações quanto a assinaturas e regras de negocio que somente sistema TOTVS pertence.

5. Cadeia de Certificação

Uma entre as várias validações da assinatura digital refere-se à Cadeia de Certificação.
A cadeia de certificação é uma série hierárquica de certificados assinados por sucessivas autoridades certificadoras. A cadeia de certificação compreende o certificado da entidade final,

assinado por uma Autoridade Certificados (AC), e zero ou mais certificados de Autoridades Certificadoras assinados por outras ACs, até o certificado de confiança. A Figura 01 ilustra um exemplo de uma cadeia de certificação de um certificado ICP-Brasil.

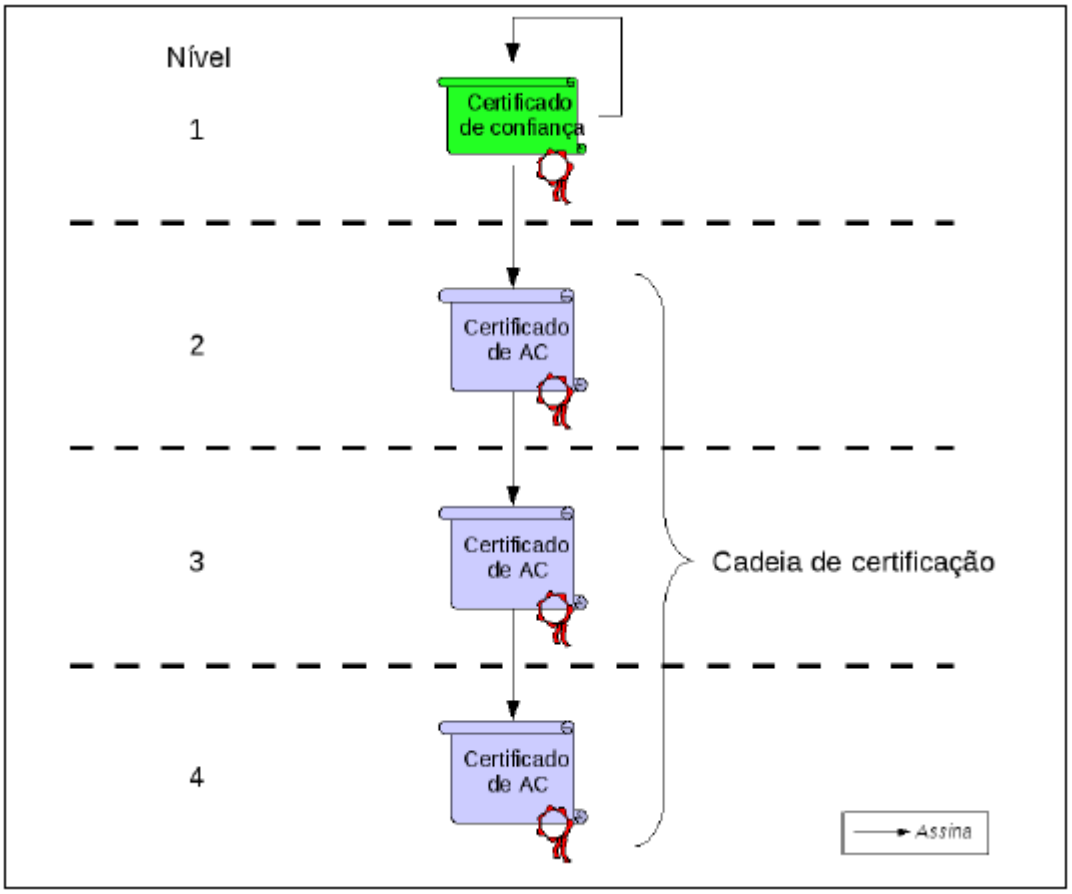

Figura 02 - Exemplo de uma cadeia de certificação da ICP-Brasil

6. Autoridades Certificadoras (AC)

As Autoridades Certificadoras são entidades credenciadas para emitir certificados digitais. É de sua competência: emitir, expedir, distribuir, revogar e gerenciar os certificados digitais das ACs de nível imediatamente subsequente ao seu, assim como colocar à disposição dos usuários listas de certificados digitais revogados e outras informações pertinentes, além de manter o registro de suas operações.

7. Política Padrão AD-RB Baseada em Cades

Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA

Campo de Aplicação

Este tipo de assinatura deve ser utilizado em aplicações ou processos de negócio nos quais a assinatura digital agrega segurança à autenticação de entidades e verificação de integridade, permitindo sua validação durante o prazo de validade dos certificados dos signatários.

Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo **A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100)**, tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

8. Atributos exigidos pelo Banco do Brasil para o arquivo assinado

O processo de assinatura digital das remessas financeiras geradas pelo sistema “TOTVS Gestão de Estoque, Compras e Faturamento” incluem os atributos listados abaixo.

Estes atributos são incluídos em cada remessa financeira no momento da assinatura digital (aprovação da remessa pelo Diretor/Procurador) através de processos e regras de negocio existentes na Customização. Remessas Financeiras que não possuírem estes atributos serão recusadas pela entidade “Banco do Brasil”.

Identificadores de objeto usados

Tipo de dado	OID
Tipo Data (eContentType)	1.2.840.113549.1.7.1
Tipo SignedData	1.2.840.113549.1.7.2
Atributo Content Type	1.2.840.113549.1.9.3
Atributo Message Digest	1.2.840.113549.1.9.4
Atributo Signing Time	1.2.840.113549.1.9.5
Atributo ESS Signing Certificate v2	1.2.840.113549.1.9.16.2.47
Atributo Commitment-type-indication	1.2.840.113549.1.9.16.2.16
Atributo SignaturePolicy	1.2.840.113549.1.9.16.2.15
Atributo SignatureTimeStamp	1.2.840.113549.1.9.16.2.
Atributo CompleteCertificateReferences	1.2.840.113549.1.9.16.2.21
Atributo CompleteRevocationReferences	1.2.840.113549.1.9.16.2.22
Atributo CertificateValues	1.2.840.113549.1.9.16.2.23
Atributo RevocationValues	1.2.840.113549.1.9.16.2.24
Atributo ESCTimeStampToken	1.2.840.113549.1.9.16.2.25
Atributo TimestampedCertsCRLs	1.2.840.113549.1.9.16.2.26
ATributo ArchiveTimeStampToken	1.2.840.113549.1.9.16.2.48

Figura 03 – Atributos exigidos pelo Banco do Brasil

- Content Type - Tipo do conteúdo.
  (OBJECT IDENTIFIER) id-contentType OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 3 }
  (ATTRIBUTE VALUE) ContentType ::= OBJECT IDENTIFIER

- Message digest - O Hash do conteúdo.
  (OBJECT IDENTIFIER) id-messageDigest OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 4 }
  (ATTRIBUTE VALUE) MessageDigest ::= OCTET STRING

- Signing time - Momento da assinatura. O mais praticado é o UTCTime no formato AAMMDDHHMMSSZ
  (OBJECT IDENTIFIER) id-signingTime OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 5 }