Safra

Tradição Secular de Segurança

Manual de Integração
Plataforma de Serviços Digitais

Abril 2018 - v 1.2

Sumário

Introdução

O **Banco Safra** disponibiliza aos seus clientes, uma plataforma de serviços, através de uma integração tecnológica de sistemas produtos.

Este documento detalha todos os mecanismos de integração, com seus requisitos, modelo de segurança, acessos e chamadas aos serviços exclusivos contratados.

Confidencialidade

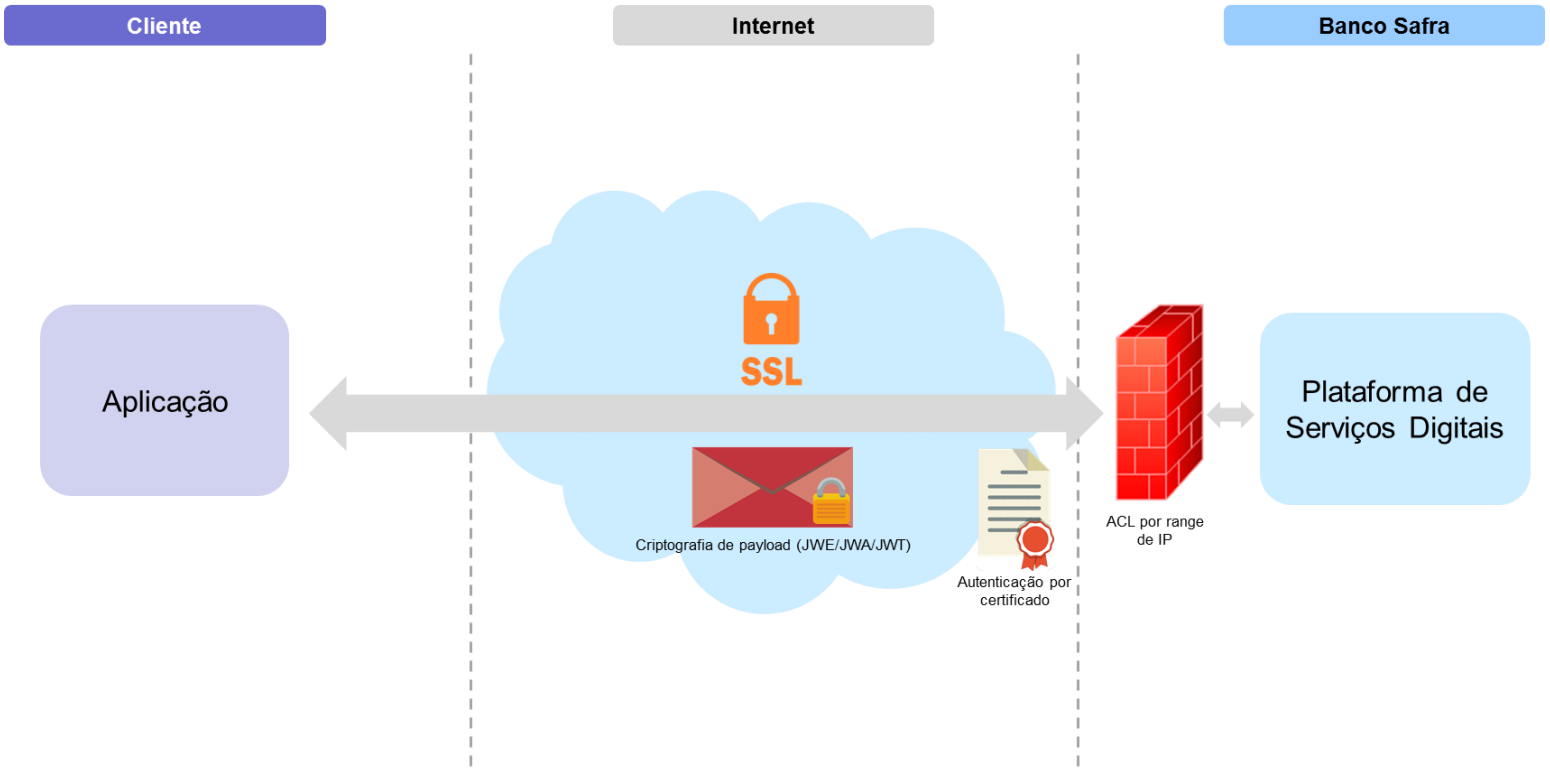
Para manter a integridade e segurança dos serviços, este material é confidencial e de uso exclusivo da equipe de segurança e tecnologia do cliente, devendo ser tratado com total profissionalismo e com divulgação limitada à dependência tecnológica do cliente, sendo proibida a divulgação, cópia e compartilhamento independente do tipo de mídia. O uso não autorizado deste material é proibido e está sujeito às penalidades cabíveis.

Suporte

Central de Suporte Pessoa Jurídica
Grande São Paulo: (11) 3175-8248 - Demais Localidades: 0300 015 7575
Atendimento personalizado de 2ª a 6ª feira, das 8:30 às 19:00 horas, exceto feriados.

Modelo Conceitual

Visando a integração do cliente com o Banco Safra, foi elaborado um modelo conceitual para endereçamento da conectividade:



Requisitos

Para que seja possível a conectividade com a plataforma de serviços digitais do Banco Safra, o cliente deverá realizar as etapas abaixo:

- Solicitar o certificado para conexão segura – TLS, seguindo as orientações do manual "Procedimentos para emissão de Certificado Digital" enviado por email (*);
- Informar os endereços IPs para liberação da conexão – ACL, tanto IP para ambiente de homologação quanto produção;
- Seguir o modelo de comunicação definido com os mecanismos de criptografia (**)
- Acessar os serviços de negócio digitais contratados (**)

* Ambiente de homologação e produção (certificado e endereços IPs específicos)
** Detalhes dos serviços estão definidos neste documento e devem ser seguidos para que o acesso seja permitido.

Serviços

Para viabilizar a comunicação com o Banco Safra, há um conjunto de serviços disponíveis, com suas funções específicas e que devem ser consumidos seguindo uma determinada ordem.

A seguir enumeramos estes serviços, a ordem de invocação e para cada um deles, um detalhamento dos parâmetros e seus requisitos:

- psd001 – Inicialização com troca de chaves (handshake)
- psd005 – Autenticação do cliente com disponibilização de token (JWT) e identificador de sessão de autenticação para utilização nos demais serviços
- psd007 – Renovação da validade do token (JWT)
- psd050 – Inclusão de boletos
- psd052 – Consulta de boletos

Serviço de Inicialização

https://cobranca-**hml**.safranegocios.com.br/psd/psd001

Header:
amc-session-id: GUID que identifica a sessão de comunicação
amc-message-id: GUID que identifica a mensagem enviada
accept-language: pt-BR
Body:
{
jwk: “”
}

A criptografia utilizada para a troca de chaves é a RSA-CTR. Os passos abaixo demonstram o fluxo de troca de chaves entre os sistemas que deverá ser seguido:

-hml = Ambiente de homologação.
Quando iniciar em produção, retirar este **-hml** da URL.

Cliente

1. Emitir o par de chaves Pública e Privada (chaves assimétricas padrão RSA 1024)

2. No header:
   amc-session-id: Gerar um GUID para identificar a sessão de comunicação
   amc-message-id: Gerar um GUID para identificar a mensagem enviada
   amc-aplicacao: "PSD"
   accept-language: Inserir o valor “pt-BR” para identificação do idioma

3. Cifrar e assinar o conteúdo gerado no campo “amc-session-id”
   3.1. Gerar um hash utilizando o algoritmo SHA-256 no conteúdo do Identificador de Sessão de Comunicação (GUID)
   3.2. Cifrar o hash com a chave privada do cliente com o algoritmo RSA-PKCS#1/SHA-256
   3.3. Assinar o valor cifrado do Identificador de Sessão de Comunicação

4. Montar o body **JWK** para a primeira etapa do serviço inicialização:
   Codificar em base64 *a assinatura da Identificação da Sessão* (passo 3) + . +
   Codificar em base64 *o valor "RSA"* + . +
   Codificar em base64 *o valor "enc"* + . +
   Codificar em base64 *o valor "P-256"* + . +
   Codificar em base64 *a chave pública do cliente* (passo 1)

   Importante:
   Utilizar o Dicionário StandardEncoding para codificação em base 64.

5. Etapa 1 (troca de chaves públicas assimétricas):
   Executar a chamada do serviço de inicialização - init

   Header:
   amc-session-id: GUID que identifica a sessão de comunicação
   amc-message-id: GUID que identifica a mensagem enviada
   amc-aplicacao: "PSD"
   accept-language: pt-BR
   Body:
   {
   jwk: "<Representação do Identificador de sessão criptografado com a chave privada do cliente em base 64>.<Representação da sigla ***RSA*** em base 64>.<Representação da sigla ***enc*** em base 64>. <Representação do código ***P-256*** em base 64>.<Representação da chave pública do cliente em base 64>" (passo 4)
   }

   Importante:
   Formato da chave pública: na última parte do payload da primeira chamada do init (jwk em 5 partes base64 separadas por ponto), deve-se enviar PEM? (codificado em base 64).

6. Recebe a chave publica do Banco Safra no retorno da chamada:

   Header:
   amc-session-id: GUID que identifica a sessão de comunicação
   amc-message-id: GUID que identifica a mensagem enviada
   amc-aplicacao: "PSD"
   accept-language: pt-BR
   Body:
   {
   jwk: "<Representação da sigla RSA em base 64>.<Representação da sigla enc em base 64>. <Representação do código P-256 em base 64>.<Representação da chave pública do Safra em base 64>"
   }

7. Decodificar em base64 a quarta posição do JWK (separados por ".") recebido na resposta da requisição, gerando a **chave pública do Banco Safra** que será utilizada nos próximos passos.

   Finalizando assim a etapa 1 de troca de chaves assimétricas.

8. Cifrar o identificador de sessão de comunicação (session-id) com a chave pública do Banco Safra

9. Cifrar e assinar o conteúdo gerado no session-id
   9.1. Gerar um hash utilizando o algoritmo SHA-256 no conteúdo do Identificador de Sessão de Comunicação (GUID)
   9.2. Cifrar o hash com a chave privada do cliente com o algoritmo RSA-PKCS#1/SHA-256
   9.3. Assinar o valor cifrado do Identificador de Sessão de Comunicação

10. Montar o body parametros:
    Codificar em base64 *Identificador de sessão cifrado* (passo 8) + . +
    Codificar em base64 *Assinatura* (passo 9)

11. Etapa 2 (chave simétrica do Banco Safra):
    Executar a chamada do serviço inicialização - init:

    Header:
    amc-session-id: GUID que identifica a sessão de comunicação
    amc-message-id: GUID que identifica a mensagem enviada
    amc-aplicacao: "PSD"
    accept-language: pt-BR
    Body:
    {
    parametros: "<Representação do Identificador de sessão criptografado com a chave pública do Safra em base 64>.<Representação do Identificador de sessão criptografado com a chave privada do cliente em base 64>"
    }

12. Recebe no retorno da chamada com a chave simétrica do Banco Safra:

    Header:
    amc-session-id: GUID que identifica a sessão de comunicação
    amc-message-id: GUID que identifica a mensagem enviada
    amc-aplicacao: "PSD"
    amc-aplicacao: "PSD"

accept-language: pt-BR
Body:
{
"<Representação, em base 64, da estrutura contendo a chave simétrica criptografado com a chave pública do cliente>.<assinatura da chave simétrica, efetuada com a chave privada do Safra>"
}

13. Decifrar o valor da primeira posição da resposta utilizando a chave privada do cliente, obtendo o JWK

14. Decodificar em base64 o campo KID do JWK para obter a **chave simétrica do Banco Safra**, que será utilizada nos demais serviços para cifrar/decifrar as mensagens (payload)

15. Decodificar em base64 a segunda posição da resposta, obtendo a assinatura do Banco Safra

16. Validar a assinatura para garantir a integridade da mensagem
    16.1. Gerar hash do conteúdo da chave simétrica SHA-256 (passo 14)
    16.2. Cifrar o hash gerado utilizando a chave pública do banco Safra (passo 7)
    16.3. Verificar se o resultado cifrado do hash ((passo 16.2) é igual da assinatura do Banco Safra (passo 15)

A chave simétrica tem validade e deve ser testada em todas as chamadas dos serviços. Caso retorne HTTP: 500, verificar se no header existe a chave amc-criptografia com o conteúdo "erro". Nesta situação todo o processo de troca de chaves (handshake) deve ser refeito (passo 1).

Tratamento do Body

Para todas as chamadas dos próximos serviços é necessário tratar o body, codificando/cifrando no envio da mensagem e decodificando/decifrando no retorno da chamada. Segue os passos para estes processos:

Cliente

Montando o Body para envio

17. Codificar em base64 o **Cabeçalho** com o valor { alg: "RSA-AEP", enc: "A256CTR" }
18. Codificar em base64 o **Vetor de inicialização** gerado com 16 caracteres randômicos (para cada requisição)
19. Cifrar a **Mensagem** utilizado o algoritmo AES-CTR com a **chave simétrica** do Banco Safra (passo 14) e o vetor de inicialização (passo 18), e codificar em base64
20. Concatenar com "." a mensagem para envio:

    Cabeçalho (passo 17) + . +
    Vetor de inicialização (passo 18) + . +
    Mensagem cifrada (passo 19)

Tratando o body de retorno

21. Separar o conteúdo da mensagem recebida: Cabeçalho.Vetor de inicialização.Mensagem cifrada
22. Decodificar em base64 o Vetor de inicialização
23. Decifrar a mensagem utilizando o vetor de inicialização (passo 22) com a chave simétrica do Banco Safra (passo 14)

Serviço de Autenticação

https://cobranca-hml.safranegocios.com.br/psd/psd005

Header:
amc-session-id: GUID que identifica a sessão de comunicação
amc-message-id: GUID que identifica a mensagem enviada
accept-language: pt-BR
Body:
{
data:””
}

Para o consumo dos serviços de negócio, é necessária uma autenticação, token valido e um identificador da sessão de autenticação (wokId). Esta autenticação, geração do JSON Web Token (JWT) e do identificador de sessão de autenticação (workId) é realizado neste serviço de autenticação.

-hml = Ambiente de homologação.
Quando iniciar em produção, retirar este **-hml** da URL.

Cliente

24. Montar a mensagem de negócio com as chaves:
{ idEstrategia: "autenticar/psd", versaoAplicacao: 1, credenciais: {}, cliente: "**CLIENTE**" };

25. Tratar o body (passos 17 a 20)

26. Executar o serviço de autenticação - psd005

Header:
amc-session-id: GUID que identifica a sessão de comunicação
amc-message-id: GUID que identifica a mensagem enviada
amc-aplicacao: "PSD"
accept-language: pt-BR
Body:
{
data: “<Representação do cabeçalho JWE* em base 64>.<Representação do vetor de inicialização** em base 64>.<Representação, em base 64, do payload da mensagem de negócio*** criptografado utilizando o vetor de inicialização e a chave simétrica>”
}

27. Recebendo o token (JWT) e o identificador de sessão de autenticação (workId) no retorno da chamada

28. Tratar o retorno do body (passos 21 a 23)

29. Decodificar em base64 o JWT, representado pelo campo “token”

Exemplo de JWT decodificado:

{
"usr": {},
"rol": [],
"apl": “XYZ",
"est": [
“certificado"
],
"exp": 1493556924,
"jti": "5e7a9e6d-99f8-401d-b3e7-a8fdbb0436fb",
"iat": 1493549723
}

30. Recuperar e armazenar o valor do identificador de sessão de autenticação, retornado no campo “workId”

31. Calcular o tempo para expiração do token

Ao decodificar o token, é necessário calcular o tempo de expiração. Deste modo, utilize os campos do JWT da seguinte forma:

Data de expiração: token.exp
Date de emissão: token.iat
Tempo de segurança para renovação antes do JWT expirar: 30 segundos

Calculo de expiração do token (JWT)

Expiração = data de expiração - data de emissão - tempo de segurança para renovação antes do JWT expirar

O token tem validade e deve ser renovado dentro do prazo de segurança (recomendamos iniciar o processo de renovação do token com 1 (um) minuto de antecedência de sua expiração. Caso receba a mensagem HTTP 480, o limite foi excedido e será necessária nova autenticação (serviço: init).

Serviço de Renovação

https://cobranca-**hml**.safranegocios.com.br/psd/psd007

Header:
amc-session-id: GUID que identifica a sessão de comunicação
amc-work-id: GUID que identifica a sessão de autenticação
amc-message-id: GUID que identifica a mensagem enviada
authorization: Bearer <JWT retornado>
amc-aplicacao: "PSD"
accept-language: pt-BR
Body:

```
{
  data:""
}
```

Para manter o acesso aos serviços é necessário manter o token válido, para isso utilize o serviço de renovação.

-hml = Ambiente de homologação.
Quando iniciar em produção, retirar este **-hml** da URL.

Cliente

32. Montar a mensagem de negócio com a chave:
    token:"retornado" (passo 29)

33. Tratar o body (passos 17 a 20)

34. Executar o serviço de renovação - psd007

Header:
amc-session-id: GUID que identifica a sessão de comunicação
amc-work-id: GUID que identifica a sessão de autenticação (passo 30)
amc-message-id: GUID que identifica a mensagem enviada
authorization: Bearer <JWT retornado>
amc-aplicacao: "PSD"
accept-language: pt-BR
Body:
{
data: "<Representação do cabeçalho JWE* em base 64>.<Representação do vetor de inicialização** em base 64>.<Representação, em base 64, do payload da mensagem de negócio*** criptografado utilizando o vetor de inicialização e a chave simétrica>"
}

35. Recebendo o token (JWT) no retorno da chamada

36. Tratar o retorno do body (passos 21 a 23)

37. Decodificar em base 64 o JWT, representado pelo campo "token"

Exemplo de JWT decodificado:

```
{
 "usr": {},
 "rol": [],
 "apl": "XYZ",
 "est": [
  "certificado"
 ],
 "exp": 1493556924,
 "jti": "5e7a9e6d-99f8-401d-b3e7-a8fdbb0436fb",
 "iat": 1493549723
}
```

38. Calcular o tempo para expiração do token

Serviço de Inclusão de Boletos

https://cobranca-hml.safranegocios.com.br/psd/psd050

Header:
amc-session-id: GUID que identifica a sessão de comunicação
amc-work-id: GUID que identifica a sessão de autenticação
amc-message-id: GUID que identifica a mensagem enviada
authorization: Bearer <JWT retornado>
amc-aplicacao: "PSD"
accept-language: pt-BR
Body:
{
data:””
}

Serviço de negócio para a inclusão de boletos.

-hml = Ambiente de homologação.
Quando iniciar em produção, retirar este -hml da URL.

Cliente

39. Montar a mensagem de negócio com os dados específicos:
(ver Tabela 1)

40. Tratar o body (passos 17 a 20)

41. Executar o serviço de inclusão de boletos - psd050

Header:
amc-session-id: GUID que identifica a sessão de comunicação
amc-work-id: GUID que identifica a sessão de autenticação (passo 30)
amc-message-id: GUID que identifica a mensagem enviada
authorization: Bearer <JWT retornado> (passo 29 ou 37)
amc-aplicacao: "PSD"
accept-language: pt-BR
Body:
{
data: “<Representação do cabeçalho JWE* em base 64>.<Representação do vetor de inicialização** em base 64>.<Representação, em base 64, do payload da

mensagem de negócio*** criptografado utilizando o vetor de inicialização e a chave simétrica>”
}

42. Recebendo o retorno da chamada

43. Tratar o retorno do body (passos 21 a 23)

44. Mensagem de negócio:
(ver Tabela 2)

Para todas as chamadas dos serviços é necessário tratar o status HTTP, bem como o conteúdo da mensagem de negócio.

Serviço de Consulta de Boletos

https://cobranca-hml.safranegocios.com.br/psd/psd052

Header:

amc-session-id: GUID que identifica a sessão de comunicação
amc-work-id: GUID que identifica a sessão de autenticação
amc-message-id: GUID que identifica a mensagem enviada
authorization: Bearer <JWT retornado>
amc-aplicacao: "PSD"
accept-language: pt-BR

Body:

```
{
  data:""
}
```

Serviço de negócio para a consulta de boletos.

-hml = Ambiente de homologação.
Quando iniciar em produção, retirar este **-hml** da URL.

Cliente

45. Montar a mensagem de negócio com os dados específicos:
    (ver Tabela 3)

46. Tratar o body (passos 17 a 20)

47. Executar o serviço de consulta de boletos - psd052

Header:
amc-session-id: GUID que identifica a sessão de comunicação
amc-work-id: GUID que identifica a sessão de autenticação (passo 30)
amc-message-id: GUID que identifica a mensagem enviada
authorization: Bearer <JWT retornado> (passo 29 ou 37)
amc-aplicacao: "PSD"
accept-language: pt-BR

Body:

```
{
```

data: "<Representação do cabeçalho JWE* em base 64>.<Representação do vetor de inicialização** em base 64>.<Representação, em base 64, do payload da

mensagem de negócio*** criptografado utilizando o vetor de inicialização e a chave simétrica>”
}

48. Recebendo o retorno da chamada

49. Tratar o retorno do body (passos 21 a 23)

50. Mensagem de negócio:
(ver Tabela 4)

Para todas as chamadas dos serviços é necessário tratar o status HTTP, bem como o conteúdo da mensagem de negócio.

Tabelas de Negócio

Tabela 1 (mensagem de envio)

Campo	Tipo	Descrição
Agencia	Inteiro	Código da agência da carteira do cliente no Safra. Ex.: 200
conta	Inteiro	Código da conta da carteira do cliente no Safra. Ex.: 1234567
documento.nossonumero	Inteiro	Identificação do título no banco. Ex.: 123456789
documento.seunumero	Texto (10)	Identificação do título no cliente. Ex.: 0000004021
documento.especie	Texto(2)	Tipo do documento. Domínio: 01 – Duplicata mercantil 02 – Nota promissória 03 – Nota de seguro 05 – Recibo 09 – Duplicata de serviço
documento.datavencimento	Data	Data prevista para o vencimento do documento. Padrão: yyyy-MM-dd
documento.valor	Long	Valor do documento. Ex.: 1500000 (15.000,00)
documento.codigomoeda	Inteiro	Código da moeda associada ao valor do documento. Domínio: 0 – Real
documento.qtddiasprotesto	Inteiro	Quantidade de dias para protesto do documento. Ex.: 123
documento.identificacaoaceite	Texto (1)	Identificador de aceite do título. Valor fixo: N
documento.desconto.data	Data	Data limite para aplicação do desconto no documento. Padrão: yyyy-MM-dd
documento.desconto.valor	Long	Valor do desconto. Ex.: 12345 (123,45)
documento.multa.juros	Ponto Flutuante	Taxa de juros que será utilizada em caso de atraso no pagamento. Ex.: 12.12345
documento.multa.data	Data	Data de início para aplicação da multa. Padrão: yyyy-MM-dd
documento.multa.taxa	Ponto Flutuante	Taxa da multa que será utilizada em caso de atraso no pagamento à partir da data da multa. Ex.: 12.12345
documento.campolivre	Texto (25)*	Campo livre para descrição no boleto

documento.taxafidc	Ponto Flutuante*	Taxa de FIDC Ex.: 123.123456
documento.danfe	Texto(44)*	Código Nota Fiscal Eletrônica(DANFe)
documento.pagador.nome	Texto (40)	Nome do pagador. Ex.: José da Silva
documento.pagador.tipopessoa	Inteiro	Tipo de pessoa do pagador. Domínio: 1 – PF 2 – PJ
documento.pagador.numerodocumento	Inteiro	CPF ou CNPJ do pagador. Ex.: 12384759392 para CPF ou 192837467000192 para CNPJ
documento.pagador.email	Texto (50)*	E-mail do pagador. Ex.: jose.silva@email.com
documento.pagador.endereco.nome	Texto (40)	Nome do endereço do pagador. Ex.: Av. Paulista, 2000
documento.pagador.endereco.bairro	Texto (10)	Bairro onde o endereço do pagador está situado. Ex.: Cerqueira
documento.pagador.endereco.cidade	Texto (15)	Cidade onde o endereço do pagador está situado. Ex.: São Paulo
documento.pagador.endereco.uf	Texto (2)	Estado onde o endereço do pagador está situado. Ex.: SP
documento.pagador.endereco.cep	Inteiro	CEP associado ao endereço do pagador. Ex.: 94838038
documento.beneficiario.nome	Texto (30) *	Nome do beneficiário do documento. Ex.: Contoso SA
documento.beneficiario.tipopessoa	Inteiro *	Tipo de pessoa do beneficiário. Domínio: 1 – PF 2 – PJ
documento.beneficiario.numerodocumento	Inteiro *	CPF ou CNPJ do beneficiário. Ex.: 12384759392 para CPF ou 192837467000192 para CNPJ
documento.beneficiario.endereco.nome	Texto (40) *	Nome do endereço do beneficiário. Ex.: Av. Paulista, 2000
documento.beneficiario.endereco.bairro	Texto (10) *	Bairro onde o endereço do beneficiário está situado. Ex.: Cerqueira Cesar
documento.beneficiario.endereco.cidade	Texto (15) *	Cidade onde o endereço do beneficiário está situado. Ex.: São Paulo
documento.beneficiario.endereco.uf	Texto (2) *	Estado onde o endereço do beneficiário está situado. Ex.: SP
documento.beneficiario.endereco.cep	Inteiro *	CEP associado ao endereço do beneficiário. Ex.: 94838038
documento.mensagens	Lista (4) *	Agrupador de até quatro (4) mensagens associadas ao documento
documento.mensagens[].posicao	Inteiro *	Posição onde a mensagem será exibida. Dominio: 1 no recibo 2 na ficha

documento.mensagens[].descricao	Texto (72) *	Mensagem associada à posição definida

* Conteúdo não obrigatório

Tabela 2 (mensagem de retorno)

Campo	Tipo	Descrição
statusprocessamento.codigo	Inteiro	Código referente ao resultado da operação
statusprocessamento.mensagem	Texto (400)	Mensagem referente ao resultado da operação
documento.nossonumero	Texto (15)	Identificação do título no Safra. Ex.: 123456789012345
documento.seunumero	Texto (10)	Identificação do título no cliente. Ex.: 0000004021
documento.codigobarras	Texto (44)	Representação numérica do código de barras associado ao documento. Ex.: 42291095230250807293981407750009569690004329 42

Tabela 3 (mensagem de envio)

Campo	Tipo	Descrição
documento.nossonumero	Texto (15)	Identificação do título no Safra. Ex.: 123456789012345
documento.seunumero	Texto (10)	Identificação do título no cliente. Ex.: 0000004021

Tabela 4 (mensagem de retorno)

Campo	Tipo	Descrição
statusprocessamento.codigo	Inteiro	Código referente ao resultado da operação
statusprocessamento.mensagem	Texto (400)	Mensagem referente ao resultado da operação
documento.nossonumero	Texto (15)	Identificação do título no Safra. Ex.: 123456789012345
documento.seunumero	Texto (10)	Identificação do título no cliente. Ex.: 0000004021
documento.registradocip	Texto (1)	Indica registro na CIP. S ou N

Status de Retorno dos Serviços

HTTP Status Code	Descrição
2XX	Sucesso
4XX	Erro de requisição
550	Erro de negócio
5XX	Erro de crítico
500 + header “amc-criptografia”	Expiração da chave de criptografia, necessário refazer o handshake caso o valor seja igual a “erro”