

**MANUAL DE INTEGRAÇÃO COM O
WEBSERVICE DO GVS**

ELABORADOR:
BRUNO BARROS MENDES

CATEGORIA/REGISTRO:
MPO.152
CLASSIFICAÇÃO:
RESERVADO
PROCESSOS:
N/A
ÁREA RESPONSÁVEL:
DESENVOLVIMENTO

VERSÃO:
2.0
FASE:
PRODUÇÃO
DATA VIGÊNCIA:
13/04/2017
DIRETORIA RESPONSÁVEL:
TI



Sumário

| | |
|--|----|
| 1. PROCESSO PARA OBTER VOUCHERS SOLUTI..... | 4 |
| 2. PROTOCOLO DE AUTENTICAÇÃO NO WEBSERVICE – HMAC..... | 4 |
| 3. ENDPOINT..... | 5 |
| 4. SERVIÇO GETVOUCHER..... | 5 |
| 4.1 Requisição..... | 5 |
| 4.2 Código de Exemplo – Getvoucher..... | 8 |
| 5. SERVIÇO SUGESTAODEUSOVOUCHER..... | 9 |
| 5.1 Requisição..... | 9 |
| 5.2 Código de Exemplo – sugestaodeusovoucher..... | 11 |
| 6. SERVIÇO SITUACAOVOUCHER..... | 12 |
| 6.1 Requisição..... | 12 |
| 6.2 Código de Exemplo – situacaovoucher..... | 13 |
| 6.3 Descrição do Status 2 – situacaovoucher..... | 13 |
| 7. SERVIÇO REMOVERSUGESTAODEUSO..... | 14 |
| 7.1 Requisição..... | 14 |
| 7.2 Código de Exemplo – removersugestaodeuso..... | 15 |
| 8. SERVIÇO CANCELARVOUCHER..... | 15 |
| 8.1 Requisição..... | 15 |
| 8.2 Código de Exemplo – cancelarvoucher..... | 17 |
| 9. OBSERVAÇÕES..... | 17 |

GLOSSÁRIO

| SIGLA | DESCRIÇÃO |
|--------------------|---|
| Sistema GVS | Sistema de gerenciamento de Vouchers Soluti |
| SOAP | Simple Object Access Protocol |
| URL | Uniform Resource Locator |
| AC | Autoridade Certificadora |

1. PROCESSO PARA OBTER VOUCHERS SOLUTI

O Sistema GVS da AC Soluti permite via WS SOAP obter vouchers, inserir sugestão de uso, remover sugestão de uso e verificar a situação do voucher a partir da sua base de dados.

Antes de consumir os serviços do Web service do GVS é necessário que você tenha adquirido os vouchers da Soluti. Os serviços atuarão sobre esses vouchers.

2. PROTOCOLO DE AUTENTICAÇÃO NO WEBSERVICE – HMAC

Comunicação HTTP/HTTPS com autenticação HMAC, para comunicação simples, de forma simplificada, o objetivo é permitir a comunicação entre dois sistemas remotos com segurança sem o tráfego da senha nas requisições.

Será necessário calcular um valor HMAC para cada mensagem que será enviada para o servidor, o cálculo HMAC é definido da seguinte forma:

Cliente e servidor devem utilizar a mesma chave “KEY” para cálculo do HMAC. Essa chave deve ter tamanho e entropia suficiente para desestimular ataques de força bruta e de dicionário.

O HMAC de cada mensagem é calculado da seguinte forma:

$$\text{hmac}^i = \text{H}(\text{ H(hkey}^i \text{) } \parallel \text{ H(hkey}^i \parallel m \text{) })$$

Onde “H()” é o algoritmo de hash, “m” é a mensagem, “||” representa concatenação de strings e “hkey” é a chave utilizada para o cálculo. A função de hash - “H()” - utilizada no projeto é a **sha256**.

A chave “hkey” é definida da seguinte forma:

$$\text{hkey}^i = \text{nonce}^i \parallel \text{KEY}$$

Essa forma é utilizada para o cliente enviar a requisição para o servidor e o servidor confiar na mensagem recebida pelo cliente.

A “key” é gerada da seguinte forma:

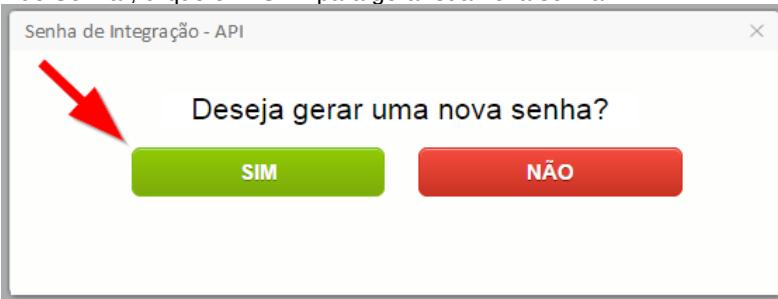
Acesse o sistema e clique em “Gerador de senha” como demonstra a imagem a seguir:



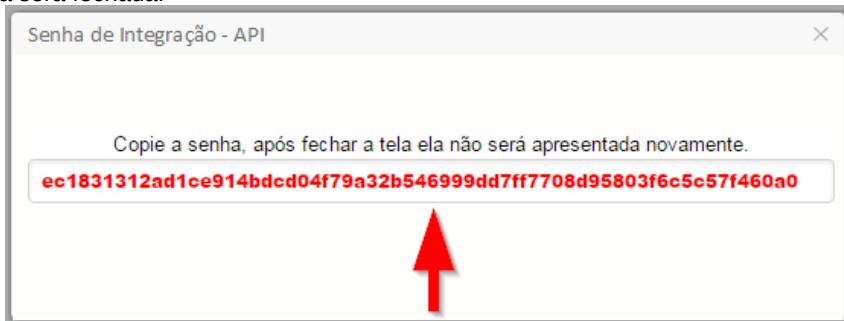
Em seguida será aberta a tela para gerar uma nova senha. Clique na imagem “Gerador de Senha”:



Após clicar em “Gerador de Senha”, clique em “Sim” para gerar sua nova senha:



Nova senha gerada. A senha deve ser COPIADA e inserida no seu código que faz a conexão com nosso Web service na variável “KEY”(ou na variável que vá receber essa chave). Caso na tela anterior você tenha clicando em “NÃO”, a tela de geração de senha será fechada:



3. ENDPOINT

O endpoint de produção será informado pela equipe de desenvolvimento no ato da entrega do sistema homologado pelo cliente.

O endpoint de homologação está disponível em: <https://gvshom.ca.inf.br/GVS/webservices/GVSServices.jws?wsdl>

4. SERVIÇO GETVOUCHER

4.1 Requisição

| DESCRÍÇÃO | O WebService GVS fornece o serviço getvoucher. Esse serviço quando consumido, verifica os parâmetros e fornece um voucher para utilização. | | |
|------------|--|------------|--|
| MÉTODO | getvoucher | | |
| PARÂMETROS | NOME | TIPO | DESCRÍÇÃO |
| | Usuario | xsd:string | É informado seu usuário de acesso ao sistema. |
| | Nonce | xsd:string | Valor aleatório. O nonce recomendado é criado da seguinte forma: timestamp concatenado com um número aleatório de 4 dígitos. |

| | | | |
|--|------------|------------|--|
| | Codproduto | xsd:string | Informe o código do produto referente ao voucher que deseja. |
| | CodVenda | xsd:string | Informe o código da venda do seu ERP. Essa informação é opcional. |
| | Sugestao | xsd:string | Informe o nome do cliente que receberá o voucher. (Opcional) |
| | Cpf-cnpj | xsd:string | Informe o CPF ou CNPJ do cliente que receberá o voucher. (Opcional) |
| | Restrito | xsd:string | Informe true para que o voucher seja de uso restrito para o CPF/CNPJ informado ou informe false para que o voucher não seja de uso restrito. |
| | Hmac | xsd:string | É calculado anteriormente e armazenado em uma variável (HMAC) que será "chamada" aqui. A mensagem "m" é composta pela concatenação de todos os parâmetros anteriores (<i>Usuario, Nonce, Codproduto, Codvenda, Sugestão, Cpf-cnpj, Restrito</i>). Para verificar como é calculado o HMAC, leia o Item 2 . |

RETORNO

| STATUS | DESCRÍÇÃO | EXEMPLO |
|--------|---|--|
| 0 | Retornará esse status quando o usuário informado for inválido ou o cálculo do hmac for inválido. | {"status": "0", "mensagem": "Autenticação inválida/HMAC inválido."} |
| 1 | Retornará esse status quando não existir voucher alocado para seu usuário com o código do produto informado. | {"status": "1", "mensagem": "Nenhum voucher encontrado para esse produto.", "hmac": "76aa1c5d2b08f67fb50fb14dd024a2089b0b6a2e92aceecb01cea0a41a6d222"} |
| 2 | Retornará esse status quando não existir voucher alocado para seu usuário com o código do produto informado, sem código de venda e sem sugestão de uso. | {"status": "2", "mensagem": "Não existem vouchers disponíveis.", "hmac": "b2494653867dc885bf00fdf699f7788a1a2b133d598d679e5d796e80cf7f5dec"} |
| 3 | Retornará esse status quando for retornado um voucher que está alocado para seu usuário com o código do produto informado, sem código de venda e sem sugestão de uso. | {"status": "3", "voucher": "000045000101", "hmac": "6d394393d56663184b13d158aff0e0726cde474e9145742f85b1d643016620a4"} |
| 4 | Retornará esse status quando não tiver sido informado o nome do cliente para a sugestão de uso. | {"status": "4", "mensagem": "Informe a sugestão de uso.", "hmac": "53ebde463806f82215dbb09ba7041b0c5a5483209a05d8a9f13b4052f22c2dbb"} |
| 5 | Retornará esse status quando não tiver sido informado o CPF ou CNPJ do cliente para a sugestão de uso. | {"status": "5", "mensagem": "Informe o CPF/CNPJ da sugestão de uso.", "hmac": "191a54a8c83679112d5176076e7f5dd88b288e015a939ed8c3d475f1ebd2cc2d"} |

| | | |
|----|---|--|
| 6 | Retornará esse status quando não tiver sido informado se o voucher será de uso restrito ou não. | {"status":"6","mensagem":"Informe se o voucher será de uso restrito ou não.", "hmac":"67f97bd72ddb54b1b12aa9d5ae3b8088cda89cbff9799f73315878c4ccbb0681"} |
| 7 | Retornará esse status quando tiver sido informado um valor diferente de true ou false. | {"status":"7","mensagem":"Informe true para voucher restrito ou false para não restrito.", "hmac":"88dc9e37eeeade6ba8e304ddc33d640cf8cd3ca17571bcd4b8a24e2df0b7bda"} |
| 8 | Retornará esse status quando tiver sido informado um CPF inválido. | {"status":"8","mensagem":"O CPF informado é inválido.", "hmac":"ab655bfc9c32117b89ec8db77023664a8304ae7b9cce1ea775c82d07921c2cd"} |
| 9 | Retornará esse status quando tiver sido informado um CNPJ inválido. | {"status":"9","mensagem":"O CNPJ informado é inválido.", "hmac":"f1fcc99abee4614b1311778ae5c39cf2c78f1084658d5fad6e80d772ce7352bf"} |
| 10 | Retornará esse status quando for retornado um voucher disponível para utilização e feito o registro da sugestão de uso. | {"status":"10","voucher":"00004500101","mensagem":"Sugestão de uso informada.", "hmac":"88a48cd7aba4ac3246e28941d6788ba28e0fd8df979c1d39d8a6aa323402a35"} |
| 11 | Retornará esse status quando o voucher solicitado estiver com sugestão de uso para outro CPF/CNPJ. | {"status":"11","mensagem":"Voucher com sugestão de uso para outro cliente.", "hmac":"f96e758aebf8f07fe7d2802a6411352aef06fee60fed473f711333018ea5f031"} |

4.2 Código de Exemplo – Getvoucher

Segue um código em PHP que exemplifica como implementar o serviço:

```
<?php

$usuario = $_POST["usuario"];
$senha = $_POST["senha"];
$codProduto = $_POST["produto"];
$codVenda = $_POST["venda"];
$nome = $_POST["nome"];
$cpfcnpj = $_POST["cpfcnpj"];
$restrito = $_POST["restrito"];

$key = $senha;
$nonce = time() . rand(1000, 9999);
$hkey = $nonce.$key;
$hash_hkey = hash("sha256", $hkey);
$dados = $usuario.$nonce.$codProduto.$codVenda.$nome.$cpfcnpj.$restrito;
$hash_hkey_dados = hash("sha256", $hkey.$dados);
$hmac = hash("sha256", $hash_hkey.$hash_hkey_dados);

try {
    $soap = new SoapClient("http://[REDACTED]/webservices/GVSServices.jws?wsdl", array(
        'trace' => 1,
        'soap_version' => SOAP_1_2,
        'cache_wsdl' => WSDL_CACHE_NONE
    ));

    $jsonReq = array(
        'usuario' => $usuario,
        'nonce' => $nonce,
        'codproduto' => $codProduto,
        'codvenda' => $codVenda,
        'sugestao' => $nome,
        'cpf-cnpj' => $cpfcnpj,
        'restrito' => $restrito,
        'hmac' => $hmac
    );

    $resposta = call_user_func_array(array($soap, 'getvoucher'), $jsonReq);

    echo ($resposta);
} catch (Exception $e) {
    echo $e->getMessage();
}
```

Aconselhamos que seja tratado o hmac de retorno para garantir a integridade da resposta.

Segue código de exemplo em PHP:

```
$resposta_sem_hmac = preg_replace('/(,[\ ]?"hmac"[ ]?:[\ ]?"[\w\d]+")/i', "", $resposta);
$hmacRetorno = hash("sha256", hash("sha256", $hkey) . hash("sha256", $hkey . $resposta_sem_hmac));
```

Na primeira linha é obtido o json sem a chave "hmac". Na segunda linha realizamos o cálculo do hmac com a resposta que recebemos. Assim podemos comparar o hmac que recebemos com o hmac que calculamos.

5. SERVIÇO SUGESTAODEUSOVOUCHER

5.1 Requisição

| | | | |
|------------|--|------------|---|
| DESCRÍÇÃO | O WebService GVS fornece o serviço sugestaodeusovoucher. Esse serviço quando consumido, verifica os parâmetros e insere/altera a sugestão de uso do voucher. | | |
| MÉTODO | sugestaodeusovoucher | | |
| PARÂMETROS | NOME | TIPO | DESCRIÇÃO |
| | Usuario | xsd:string | É informado seu usuário de acesso ao sistema. |
| | Nonce | xsd:string | Valor aleatório. O nonce recomendado é criado da seguinte forma: timestamp concatenado com um número aleatório de 4 dígitos. |
| | Voucher | xsd:string | Informe o voucher que deseja inserir/alterar a sugestão de uso. |
| | Sugestao | xsd:string | Informe o nome do cliente que receberá o voucher. |
| | Cpf-cnpj | xsd:string | Informe o CPF ou CNPJ do cliente que receberá o voucher. |
| | Restrito | xsd:string | Informe true para que o voucher seja de uso restrito para o CPF/CNPJ informado ou informe false para que o voucher não seja de uso restrito. |
| | Hmac | xsd:string | É calculado anteriormente e armazenado em uma variável (HMAC) que será "chamada" aqui. A mensagem "m" é composta pela concatenação de todos os parâmetros anteriores (<i>Usuario</i> , <i>Nonce</i> , <i>Voucher</i> , <i>Sugestão</i> , <i>Cpf-cnpj</i> , <i>Restrito</i>). Para verificar como é calculado o HMAC, leia o Item 2 . |

RETORNO

| STATUS | DESCRIÇÃO | EXEMPLO |
|--------|--|---|
| 0 | Retornará esse status quando o usuário informado for inválido ou o cálculo do hmac for inválido. | {"status":"0","mensagem":"Autenticação inválida/HMAC inválido."} |
| 1 | Retornará esse status quando o voucher não for encontrado. | {"status":"1","mensagem":"Voucher não encontrado.","hmac":"ebda0006f82a31319113cd03458257ace68775a83411f4e7baa251ea0adfdfaf"} |
| 2 | Retornará esse status quando o voucher já estiver sido utilizado na emissão de um Certificado Digital. | {"status":"2","mensagem":"Voucher já utilizado.","hmac":"a9519237abe2895591cb6dac931ed4041cef4b7b8d92ce84cf964c3d82d0613d"} |
| 3 | Retornará esse status quando não tiver sido informado o CPF ou CNPJ do cliente para a sugestão de uso. | {"status":"3","mensagem":"Informe o CPF/CNPJ da sugestão de uso.","hmac":"191a54a8c83679112d5176076e7f5dd88b288e015a939ed8c"} |

| | | |
|----|---|--|
| | | 3d475f1ebd2cc2d"} |
| 4 | Retornará esse status quando tiver sido informado um CNPJ inválido. | {"status":"4","mensagem":"O CNPJ informado é inválido.", "hmac":"f1fcc99abee4614b1311778ae5c39cf2c78f1084658d5fad6e80d772ce7352bf"} |
| 5 | Retornará esse status quando tiver sido informado um CPF inválido. | {"status":"5","mensagem":"O CPF informado é inválido.", "hmac":"ab655bfc9c32117b89ec8db77023664a8304ae7b9cce1ea775c82d07921c2cdd"} |
| 6 | Retornará esse status quando o voucher informado estiver com sugestão de uso para outro CPF/CNPJ. | {"status":"6","mensagem":"Voucher com sugestão de uso para outro cliente.", "hmac":"f96e758aebf8f07fe7d2802a6411352aef06fee60fed473f711333018ea5f031"} |
| 7 | Retornará esse status quando não tiver sido informado o nome do cliente para a sugestão de uso. | {"status":"4","mensagem":"Informe a sugestão de uso.", "hmac":"53ebde463806f82215dbb09ba7041b0c5a5483209a05d8a9f13b4052f22c2dbb"} |
| 8 | Retornará esse status quando não tiver sido informado se o voucher será de uso restrito ou não. | {"status":"8","mensagem":"Informe se o voucher será de uso restrito ou não.", "hmac":"67f97bd72ddb54b1b12aa9d5ae3b8088cda89cbff9799f73315878c4ccb0681"} |
| 9 | Retornará esse status quando tiver sido informado um valor diferente de true ou false. | {"status":"9","mensagem":"Informe true para voucher restrito ou false para não restrito.", "hmac":"88dc9e37eeead6ba8e304ddc33d640cf8cd3ca17571bcdc4b8a24e2df0b7bda"} |
| 10 | Retornará esse status quando a sugestão de uso tiver sido inserida/alterada com sucesso. | {"status":"10","mensagem":"Sugestão de uso atualizada com sucesso.", "hmac":"g45sdaf3a156f88b420eab59b958b356c779c9843e6494d3ada24aad53881a7fd"} |

5.2 Código de Exemplo – sugestaodeusovoucher

Segue um código em PHP que exemplifica como implementar o serviço:

```
<?php

$usuario = $_POST["usuario"];
$senha = $_POST["senha"];
$voucher = $_POST["voucher"];
$nome = $_POST["nome"];
$cpfcnpj = $_POST["cpfcnpj"];
$restrito = $_POST["restrito"];


$key = $senha;
$nonce = time().rand(1000, 9999);
$hkey = $nonce.$key;
$hash_hkey = hash("sha256", $hkey);
$dados = $usuario.$nonce.$voucher.$nome.$cpfcnpj.$restrito;
$hash_hkey_dados = hash("sha256", $hkey.$dados);
$hmact = hash("sha256", $hash_hkey.$hash_hkey_dados);

try {
    $soap = new SoapClient("http://XXXXXXXXXX/webservices/GVSServices.jws?wsdl", array(
        'trace' => 1,
        'soap_version' => SOAP_1_2,
        'cache_wsdl' => WSDL_CACHE_NONE
    ));

    $jsonReq = array(
        'usuario' => $usuario,
        'nonce' => $nonce,
        'voucher' => $voucher,
        'sugestao' => $nome,
        'cpfcnpj' => $cpfcnpj,
        'restrito' => $restrito,
        'hmact' => $hmact
    );

    $resposta = call_user_func_array(array($soap, 'sugestaodeusovoucher'), $jsonReq);

    echo $resposta;

} catch (Exception $e) {
    echo $e->getMessage();
}
}
```

Aconselhamos que seja tratado o hmac de retorno para garantir a integridade da resposta.

Segue código de exemplo em PHP:

```
$resposta_sem_hmac = preg_replace('/(,[ ])?"hmac"[ ]?:[ ]?"[\w\d]+"/i', "", $resposta);
$hmactRetorno = hash("sha256", hash("sha256", $hkey) . hash("sha256", $hkey . $resposta_sem_hmac));
```

Na primeira linha é obtido o json sem a chave "hmac". Na segunda linha realizamos o cálculo do hmac com a resposta que recebemos. Assim podemos comparar o hmac que recebemos com o hmac que calculamos.

6. SERVIÇO SITUACAOVOUCHER

6.1 Requisição

| | | | |
|------------|---|------------|---|
| DESCRÍÇÃO | O WebService GVS fornece o serviço situacaovoucher. Esse serviço quando consumido, verifica os parâmetros e retorna todas as informações referentes ao voucher informado. | | |
| MÉTODO | situacaovoucher | | |
| PARÂMETROS | NOME | TIPO | DESCRÍÇÃO |
| | Usuario | xsd:string | É informado seu usuário de acesso ao sistema. |
| | Nonce | xsd:string | Valor aleatório. O nonce recomendado é criado da seguinte forma: timestamp concatenado com um número aleatório de 4 dígitos. |
| | Voucher | xsd:string | Informe o voucher que deseja obter as informações. |
| | Hmac | xsd:string | É calculado anteriormente e armazenado em uma variável (HMAC) que será "chamada" aqui. A mensagem "m" é composta pela concatenação de todos os parâmetros anteriores (<i>Usuario</i> , <i>Nonce</i> , <i>Voucher</i> , <i>Sugestão</i> , <i>Cpf-cnpj</i> , <i>Restrito</i>). Para verificar como é calculado o HMAC, leia o Item 2 . |

| RETORNO | | |
|---------|--|--|
| STATUS | DESCRÍÇÃO | EXEMPLO |
| 0 | Retornará esse status quando o usuário informado for inválido ou o cálculo do hmac for inválido. | {"status": "0", "mensagem": "Autenticação inválida/HMAC inválido."} |
| 1 | Retornará esse status quando o voucher não for encontrado. | {"status": "1", "mensagem": "Voucher não encontrado.", "hmac": "ebda0006f82a31319113cd03458257ace68775a83411f4e7baa251ea0adfdaf"}} |
| 2 | Retornará esse status quando o voucher for encontrado. Será retornado todas as informações do voucher. | {"status": "2", "voucher": "000037000301", "bloqueado": "0", "situacao": "2", "codVenda": "vd2017-01", "cont": "5", "nomeCliente": "Cliente de teste", "negociacao": "1010", "empenho": "1010", "codProduto": "10", "nomeProduto": "CERTIFICADO PJ A1", "alocado": "Usuário A", "nomeSugestao": "Cliente de teste", "cpfcnpjSugestao": "13096767475", "restrito": "true", "nomeCert": "", "cpfcnpjCert": "", "dataEmissao": "", "dataVencimento": "", "hmac": "9e4fca0f8298b4c42326ab e7187de9f9ce2015eb1d4dd373ebf7b 6a22a72f1de"}} |

6.2 Código de Exemplo – situacaovoucher

Segue um código em PHP que exemplifica como implementar o serviço:

```
<?php

$usuario = $_POST["usuario"];
$senha = $_POST["senha"];
$voucher = $_POST["voucher"];

$key = $senha;
$nonce = time() . rand(1000, 9999);
$hkey = $nonce . $key;
$hash_hkey = hash("sha256", $hkey);
$dados = $usuario . $nonce . $voucher;
$hash_hkey_dados = hash("sha256", $hkey . $dados);
$hmac = hash("sha256", $hash_hkey . $hash_hkey_dados);

try {
    $soap = new SoapClient("http://[REDACTED]/webservices/GVSServices.jws?wsdl", array(
        'trace' => 1,
        'soap_version' => SOAP_1_2,
        'cache_wsdl' => WSDL_CACHE_NONE
    ));

    $jsonReq = array(
        'usuario' => $usuario,
        'nonce' => $nonce,
        'voucher' => $voucher,
        'hmac' => $hmac
    );

    $resposta = call_user_func_array(array($soap, 'situacaovoucher'), $jsonReq);

    echo $resposta;
} catch (Exception $e) {

    echo $e->getMessage();
}
}
```

Aconselhamos que seja tratado o hmac de retorno para garantir a integridade da resposta.

Segue código de exemplo em PHP:

```
$resposta_sem_hmac = preg_replace('/([, ]?)"hmac"[ ]?:[ ]?"[\w\d]+"/i', "", $resposta);
$hmacRetorno = hash("sha256", hash("sha256", $hkey) . hash("sha256", $hkey . $resposta_sem_hmac));
```

Na primeira linha é obtido o json sem a chave "hmac". Na segunda linha realizamos o cálculo do hmac com a resposta que recebemos. Assim podemos comparar o hmac que recebemos com o hmac que calculamos.

6.3 Descrição do Status 2 – situacaovoucher

Segue a descrição de cada chave da resposta com status 2:

voucher = voucher solicitado
blockeadoo = valor 0 (blockeadoo, não sendo possível utilizar), valor 1 (habilitado para uso)
situacao = valor 2 (voucher não utilizado), valor 3 (voucher já utilizado)
codVenda = código da venda (Opcional e enviado pelo seu ERP)
cont = quantidade de vezes que o voucher vou requisitado através do webservice
nomeCliente = cliente que adquiriu os vouchers da Soluti
negociacao = uso interno da Soluti
empenho = uso interno da Soluti
codProduto = código do produto interno da Soluti
nomeProduto = nome do produto
alocado = usuário responsável pelo voucher
nomeSugestao = nome do cliente que está sugerido para a utilização do voucher
cpfcnpjSugestao = cpf ou cnpj da sugestão de uso

restrito = valor true (voucher de uso restrito para o CPF/CNPJ informado na sugestão), valor false (voucher de uso não restrito, podendo qualquer pessoa utilizar o voucher)

nomeCert = titular do Certificado Digital

cpfcnpjCert = CPF ou CNPJ contido no Certificado Digital

dataEmissao = data que o Certificado Digital foi emitido

dataVencimento = data de expiração do Certificado Digital

7. SERVIÇO REMOVERSUGESTAODEUSO

7.1 Requisição

| DESCRÍÇÃO | O WebService GVS fornece o serviço removersugestaodeuso. Esse serviço quando consumido, verifica os parâmetros e remove a sugestão de uso, o código da venda e insere 0 no campo cont do voucher informado. | | |
|------------|---|------------|--|
| MÉTODO | removersugestaodeuso | | |
| PARÂMETROS | NOME | TIPO | DESCRÍÇÃO |
| | Usuario | xsd:string | É informado seu usuário de acesso ao sistema. |
| | Nonce | xsd:string | Valor aleatório. O nonce recomendado é criado da seguinte forma: timestamp concatenado com um número aleatório de 4 dígitos. |
| | Voucher | xsd:string | Informe o voucher que deseja remover a sugestão de uso e o código da venda. |
| | Hmac | xsd:string | É calculado anteriormente e armazenado em uma variável (HMAC) que será “chamada” aqui. A mensagem “m” é composta pela concatenação de todos os parâmetros anteriores (Usuario, Nonce, Voucher, Sugestão, Cpf-cnpj, Restrito). Para verificar como é calculado o HMAC, leia o Item 2 . |

| RETORNO | | |
|---------|--|---|
| STATUS | DESCRÍÇÃO | EXEMPLO |
| 0 | Retornará esse status quando o usuário informado for inválido ou o cálculo do hmac for inválido. | {"status":"0","mensagem":"Autenticação inválida/HMAC inválido."} |
| 1 | Retornará esse status quando o voucher não for encontrado. | {"status":"1","mensagem":"Voucher não encontrado.","hmac":"ebda0006f82a31319113cd03458257ace68775a83411f4e7baa251ea0adfdfaf"} |
| 2 | Retornará esse status quando removido a sugestão de uso, o campo código da venda e inserido 0 no campo cont. | {"status":"2","mensagem":"Sugestão de uso removida.","hmac":"2e717bb85ea576e7e5f947376ae96b547b05c2f90f8fa6651d728881d73f73b3"} |
| 3 | Retornará esse status quando o voucher que deseja remover a sugestão de uso já foi utilizado na emissão de um Certificado Digital. | {"status":"3","mensagem":"Voucher já utilizado. Não é possível remover a sugestão de uso.","hmac":"00c8d00d2373d31b00c21178bf8f49fc74a469f6fed045f725e84d2a7d9e79f0"} |

7.2 Código de Exemplo – removersugestaodeuso

Segue um código em PHP que exemplifica como implementar o serviço:

```
<?php

$usuario = $_POST["usuario"];
$senha = $_POST["senha"];
$voucher = $_POST["voucher"];

$key = $senha;
$nonce = time().rand(1000, 9999);
$hkey = $nonce.$key;
$hash_hkey = hash("sha256",$hkey);
$dados = $usuario.$nonce.$voucher;
$hash_hkey_dados = hash("sha256",$hkey.$dados);
$shmac = hash("sha256",$hash_hkey.$hash_hkey_dados);

try {
    $soap = new SoapClient("http://[REDACTED]/webservices/GVSServices.jws?wsdl", array(
        'trace' => 1,
        'soap_version' => SOAP_1_2,
        'cache_wsdl' => WSDL_CACHE_NONE
    ));

    $jsonReq = array(
        'usuario' => $usuario,
        'nonce' => $nonce,
        'voucher' => $voucher,
        'hmac' => $shmac
    );

    $resposta = call_user_func_array(array($soap, 'removersugestaodeuso'), $jsonReq);

    echo $resposta;
} catch (Exception $e) {
    echo $e->getMessage();
}
}
```

Aconselhamos que seja tratado o hmac de retorno para garantir a integridade da resposta.

Segue código de exemplo em PHP:

```
$resposta_sem_hmac = preg_replace('/(,[ ])?"hmac"[ ]?:[ ]?"[\w\d]+")/i', "", $resposta);
$shmacRetorno = hash("sha256", hash("sha256", $hkey) . hash("sha256", $hkey . $resposta_sem_hmac));
```

Na primeira linha é obtido o json sem a chave "hmac". Na segunda linha realizamos o cálculo do hmac com a resposta que recebemos. Assim podemos comparar o hmac que recebemos com o hmac que calculamos.

8. SERVIÇO CANCELARVOUCHER

8.1 Requisição

| DESCRÍÇÃO | O WebService GVS fornece o serviço cancelarvoucher. Esse serviço quando consumido, verifica os parâmetros e cancela o voucher gerando um novo na sua lista de vouchers disponíveis para o uso. | | |
|------------|--|------------|--|
| MÉTODO | cancelarvoucher | | |
| PARÂMETROS | NOME | TIPO | DESCRÍÇÃO |
| | Usuario | xsd:string | É informado seu usuário de acesso ao sistema. |
| | Nonce | xsd:string | Valor aleatório. O nonce recomendado é criado da seguinte forma: timestamp |

| | | |
|---------|------------|--|
| | | concatenado com um número aleatório de 4 dígitos. |
| Voucher | xsd:string | Informe o voucher que deseja cancelar |
| Hmac | xsd:string | É calculado anteriormente e armazenado em uma variável (HMAC) que será "chamada" aqui. A mensagem "m" é composta pela concatenação de todos os parâmetros anteriores (<i>Usuario</i> , <i>Nonce</i> , <i>Voucher</i>). Para verificar como é calculado o HMAC, leia o Item 2 . |

RETORNO

| STATUS | DESCRÍÇÃO | EXEMPLO |
|--------|---|--|
| 0 | Retornará esse status quando o usuário informado for inválido ou o cálculo do hmac for inválido. | {"status":"0","mensagem":"Autenticação inválida/HMAC inválido."} |
| 1 | Retornará esse status quando o voucher não for encontrado. | {"status":"1","mensagem":"Voucher não encontrado.","hmac":"ebda0006f82a31319113cd03458257ace68775a83411f4e7baa251ea0adfdaf"} |
| 2 | Retornará esse status quando o voucher tiver sido cancelado e gerado um novo voucher. | {"status":"2","mensagem":"Voucher cancelado com sucesso.","hmac":"2e717bb85ea576e7e5f947376ae96b547b05c2f90f8fa6651d728881d73f73b3"} |
| 3 | Retornará esse status quando o voucher que deseja cancelar já foi utilizado na emissão de um Certificado Digital. | {"status":"3","mensagem":"Voucher já utilizado. Não é possível cancelá-lo.","hmac":"00c8d00d2373d31b00c21178bf8f49fc74a4uw736ed045f725e84d2a7d9e79f0"} |

8.2 Código de Exemplo – cancelarvoucher

Segue um código em PHP que exemplifica como implementar o serviço:

```
<?php

$usuario = $_POST["usuario"];
$senha = $_POST["senha"];
$voucher = $_POST["voucher"];

$key = $senha;
$nonce = time().rand(1000, 9999);
$hkey = $nonce.$key;
$hash_hkey = hash("sha256", $hkey);
$dados = $usuario.$nonce.$voucher;
$hash_hkey_dados = hash("sha256", $hkey.$dados);
$shmac = hash("sha256", $hash_hkey.$hash_hkey_dados);

try {
    $soap = new SoapClient("https://gvshom.ca.inf.br/GVS/webservices/GVSServices.jws?wsdl", array(
        'trace' => 1,
        'soap_version' => SOAP_1_2,
        'cache_wsdl' => WSDL_CACHE_NONE
    ));

    $jsonReq = array(
        'usuario' => $usuario,
        'nonce' => $nonce,
        'voucher' => $voucher,
        'hmac' => $shmac
    );

    $resposta = call_user_func_array(array($soap, 'cancelarvoucher'), $jsonReq);

    echo $resposta;

} catch (Exception $e) {

    echo $e->getMessage();
}
}
```

Aconselhamos que seja tratado o hmac de retorno para garantir a integridade da resposta.

Segue código de exemplo em PHP:

```
$resposta_sem_hmac = preg_replace('/([, ])?"hmac"[ ]?:[ ]?"[\w\d]+")/i', "", $resposta);
$hmacRetorno = hash("sha256", hash("sha256", $hkey) . hash("sha256", $hkey . $resposta_sem_hmac));
```

Na primeira linha é obtido o json sem a chave "hmac". Na segunda linha realizamos o cálculo do hmac com a resposta que recebemos. Assim podemos comparar o hmac que recebemos com o hmac que calculamos.

9. OBSERVAÇÕES

Os códigos de exemplo foram desenvolvidos em PHP, porém a implementação é independente de tecnologia pois se trata de webservice.

A resposta enviada para a validação é da seguinte forma(exemplo):

```
{"status":"3","voucher":"000045000101","hmac":"6d394393d56663184b13d158aff0e0726cde474e9145742f85b1d643016620a4"}
```

Porém o atributo "hmac" não fará parte do calculo que será realizado sob a resposta, sendo assim, sugere-se a aplicação de uma expressão regular para extração desse parâmetro. Segue um exemplo de remoção do parâmetro "hmac" feito em PHP:

```
$resposta_sem_hmac = preg_replace('/([, ])?"hmac"[ ]?:[ ]?"[\w\d]+")/i', "", '{"status":"3","voucher":"000045000101","hmac":"6d394393d56663184b13d158aff0e0726cde474e9145742f85b1d643016620a4"}');
```

Observe que o atributo "hmac" já não faz mais parte da resposta. Portanto, após a extração do "hmac", tem-se o seguinte conteúdo JSON:

```
{"status":"3","voucher":"000045000101"}
```

Logo em seguida é calculado o hmac como foi orientado acima no **Item**, onde o hmac enviado pelo sistema deve ser igual ao enviado pelo webservice. Caso o cálculo não encontre a mesma informação é possível que a integridade da mensagem tenha sido comprometida, portanto a mensagem do webservice não é válida. Segue um exemplo do cálculo do "hmac" da mensagem:

```
$resposta_sem_hmac = preg_replace('/,[ ]?"hmac"[ ]?[:]?"[w\ld]+")/i', "", $resposta);
$hmac_retorno = hash("sha256", hash("sha256", $hkey) . hash("sha256", $hkey . resposta_sem_hmac ));
```

Onde: **\$hkey** é a mesma composição explicada anteriormente.

A validação da resposta é **opcional**, porém recomenda-se essa conferência para garantir a integridade da resposta enviada pelo webservice.

HISTÓRICO DE REVISÕES

| VERSÃO | DATA | DESCRIÇÃO DA REVISÃO | RESPONSÁVEL | ÁREA/DPTO |
|--------|------------|----------------------|-------------|-----------|
| 2 | DD/MM/AAAA | | | |
| 3 | DD/MM/AAAA | | | |
| 4 | DD/MM/AAAA | | | |
| 5 | DD/MM/AAAA | | | |
| 6 | DD/MM/AAAA | | | |
| 7 | DD/MM/AAAA | | | |
| 8 | DD/MM/AAAA | | | |
| 9 | DD/MM/AAAA | | | |

| | | |
|---|----------------------------|--|
| <u>REVISOR(ES):</u> JOHNATAN FREIRES DE FARIA | <u>DATA:</u> 13/04/2017 | |
| <u>APROVADOR(ES):</u> GUILHERME PEREIRA DA SILVA ALVES | <u>DATA:</u> 13/04/2017 | |