

Sistema de Pagamento Seguro

Introdução ao SPS

Índice

Capítulo 1 – Apresentação

Apresentação do SPS.....	Pág 2
Como Funciona o SPS.....	Pág 4
A comunicação nos sistemas de Comércio Eletrônico.....	Pág 6
Variáveis de Sessão (Revisão).....	Pág 7
Interação entre o consumidor, o servidor Web da loja eo MUP.....	Pág 8
Fluxo de Mensagens para Pagamento Fácil(Importante).....	Pág 10
Antes da Integração.....	Pág 11

Apresentação

O objetivo do SPS é fornecer métodos de pagamento seguro para compras realizadas na Internet.

O SPS procura incorporar os principais métodos de pagamento disponíveis na Internet e fornecer uma interface única para o desenvolvedor da loja. Mas para ser adicionado ao conjunto de opções do SPS, um método de pagamento deve mostrar-se realmente seguro. Assim, consumidor e lojista podem confiar nas transações eletrônicas realizadas através do SPS.

Para cartões de crédito é possível fazer compras parceladas em até 12 vezes.



1. Pagamento Fácil - SPS

Uma maneira mais fácil de iniciar suas compras na Internet. O consumidor deve fornecer os dados de seu cartão em todos os pagamentos. Mesmo fornecendo os dados em todo pagamento, esses dados são criptografados no navegador do consumidor de forma que apenas o banco possa vê-los.



2. Boleto Bancário Bradesco

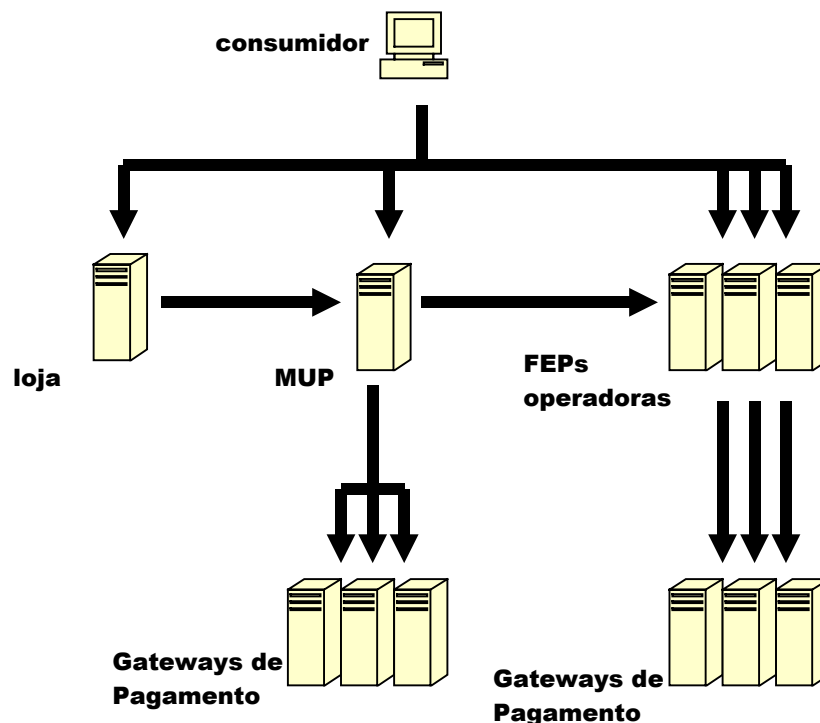
O SPS cria o boleto bancário para que o consumidor imprima e pague. O pagamento pode ser realizado numa agência bancária ou através de home/Internet Banking.

A transação não é on-line.

Como funciona o SPS

Antes de integrar uma loja no Sistema de Pagamento Seguro é preciso primeiro se ambientar com as características deste sistema.

O SPS foi concebido com o principal intuito de prover segurança no processo de pagamento de compras realizadas na Internet. Para atingir esse objetivo o sistema é composto de alguns módulos com funções distintas.



? Figura 1 – Componentes do Sistema de Pagamento Seguro.

O MUP _ módulo único de pagamento _ é a peça central do SPS. Ele representa a loja durante o processo de pagamento. Os gateways de pagamento e os FEPs (front-end processors) das operadoras de métodos de pagamento enxergam a loja através do MUP. O MUP centraliza os certificados das lojas e os comprovantes das transações. O MUP é responsável também por tornar a incorporação de novos métodos de pagamento transparente para o desenvolvedor da loja.

O consumidor deve possuir um navegador web (web browser).

A loja possui uma interface padrão para interagir com o MUP. Essa interface é comum a todos os métodos de pagamento (alguns métodos requerem alguns dados a mais).

Os Gateways de Pagamento representam as operadoras dos métodos de pagamento na Internet. Eles autorizam os pagamentos on-line ou garantem os pagamentos não on-line (caso do pagamento com cheque). Normalmente os Gateways de Pagamento estão

conectados diretamente com os sistemas de processamento da operadora através de redes privadas. Por exemplo, no caso de cartão de débito o Gateway de Pagamento está conectado diretamente no computador do banco emissor do cartão. Desse modo esses Gateways de Pagamento podem verificar a validade, autenticidade e existência de crédito do cartão sendo utilizado no pagamento.

Algumas operadoras de métodos de pagamento possuem servidores de pagamento próprios que aqui chamamos de FEP (front-end processor). Cada um desses servidores de pagamento possui interface própria. O MUP utiliza esses servidores para interagir com os gateways de pagamento dessas operadoras.

A interação entre a loja, o consumidor e o SPS foi projetada de forma que a loja não necessite de sistemas de criptografia ou módulos de segurança proprietários. Isso não exime a loja de zelar pela segurança de seu sistema através da utilização de políticas de segurança adequadas e os recursos normalmente disponíveis para os sites de comércio eletrônico como firewalls e certificados digitais no servidor web entre outros.

A seqüência abaixo dá uma visão geral de como é realizada uma transação de pagamento no SPS.

1. O cliente navega na loja selecionando produtos e inserindo na cesta de compras
2. O cliente informa que quer fechar a compra
3. O cliente fornece os dados de entrega (método de entrega e endereço)
4. O cliente escolhe o método do pagamento.
5. Os dados da compra são transferidos do servidor web da loja para o MUP de forma segura
6. O cliente escolhe detalhes do pagamento (parcelamento)
7. O cliente fornece os dados de pagamento que serão transmitidos de forma segura e autenticada diretamente para a operadora do método de pagamento escolhido
8. A operadora retorna ao SPS o resultado do pagamento
9. O SPS armazena o resultado e o comprovante da transação e o MUP transfere para o servidor web da loja esse resultado
10. A loja apresenta um comprovante de compra para o cliente

Podemos dividir o processo de compra em 3 fases: formação da cesta de compra (passos 1 e 2), seleção do endereço de entrega (passo 3) e autorização (passos 4 a 9).

A seleção do endereço de entrega pode ser realizada de diversas formas como a pergunta direta ao consumidor através de formulário ou a utilização de um cadastro prévio.

A autorização varia de acordo com o método de pagamento utilizado.

Alguns métodos como o boleto bancário não realizam os passos 7 a 10.

Os passos 5 a 9 são discutidos em detalhe nas seções seguintes.

A comunicação nos sistemas de comércio eletrônico seguro

Como as transações de pagamento através do SPS podem ter aprovação on-line, é necessário que a loja interaja com outros sistemas que realizarão essa aprovação.

Os sites WWW tradicionais normalmente interagem somente com o navegador do usuário. Mesmo essa interação é transparente para o desenvolvedor do site uma vez que o Servidor Web realiza todas as funções de comunicação, de controle de seção e autenticação.

Ao utilizar transações on-line com outras instituições inserimos um segundo nível de dificuldade no desenvolvimento pois o site da loja agora precisa se comunicar com outros sites de forma on-line.

A troca de dados entre sites diferentes através do navegador do cliente não é segura.

Uma solução simples e comum utiliza o navegador do consumidor para transmitir os dados entre os sites. O principal problema dessa solução é a segurança. Mesmo utilizando o suporte de criptografia dos Servidores Web, os dados transmitidos são "abertos" no navegador do cliente e portanto estão sujeitos a vários tipos de ataques pois podem ser monitorados, copiados, alterados e até forjados para simular autorizações ou valores de compra falsos por exemplo.

Para solucionar o problema da segurança utiliza-se uma criptografia adicional à fornecida pelos Servidores Web. Esta abordagem requer a instalação de um módulo de criptografia proprietário no Servidor Web da loja. Este fato traz inúmeras consequências: quando a loja utiliza um Servidor Web compartilhado num provedor de *hosting* é preciso pedir para esse provedor instalar o módulo de criptografia (o que nem sempre é possível), é preciso criar um módulo específico para cada plataforma de desenvolvimento de loja (asp, coldfusion, php, java, c, etc.) e para sistemas operacionais diferentes (Windows, Solaris, Linux, etc).

A solução adotada pela Scopus no SPS soluciona o problema de segurança sem a necessidade de instalação de um módulo de criptografia proprietário no servidor web da loja.

A compreensão sobre o esquema de interação entre o servidor web da loja e o MUP é importante para solucionar certos problemas encontrados nesta interação.

Variáveis de sessão (manutenção da cesta de compras e dados do cliente) - revisão

Antes de apresentar o esquema de interação entre o servidor web da loja e o MUP vamos ver como funciona o processo de navegação na loja e manutenção dos dados da cesta de compras e do cliente.

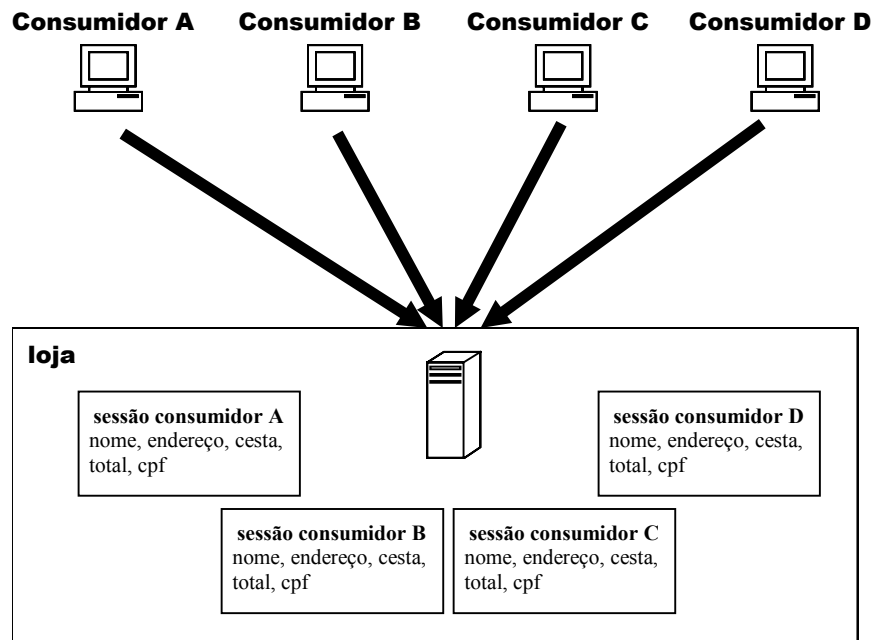


Figura 2 – controle de sessão no servidor web da loja

O servidor web da loja atende a vários consumidores simultaneamente. Para controlar e isolar as operações de cada consumidor o servidor web utiliza o conceito de sessão.

Cada consumidor é associado a uma sessão e cada sessão é associada a um conjunto de variáveis (veja Figura 2). Essas variáveis muitas vezes são chamadas de variáveis de sessão.

As variáveis de sessão são convenientes para o processamento de compras. Pode-se armazenar vários valores nelas para conservar o estado de uma compra e ao mesmo tempo não misturar com o estado da compra de outros consumidores. Quando um consumidor executa uma ação, isto é, quando ele requisita uma página, as variáveis de sessão relativas a esse consumidor são disponibilizadas pelo servidor para o programa da loja.

As variáveis de sessão são recuperadas pelo servidor web da loja de várias formas diferentes dependendo do modo como a loja foi implementada e da plataforma utilizada. Algumas formas comumente utilizadas para recuperação dos dados da sessão são:

- Cookies – um cookie de identificação é criado e enviado para o navegador do consumidor na primeira vez que esse navegador acessa a loja.

Sempre que o consumidor realiza uma ação (inclusão de item na cesta, consulta a cesta, alteração de endereço, etc.) o cookie de identificação é enviado para o servidor web da loja que utiliza esse cookie para identificar a sessão dentro de uma lista de sessões.

Uma vez que a sessão correspondente ao consumidor é identificada, o servidor web pode utilizar as variáveis de sessão correspondentes a essa sessão. Normalmente essas variáveis são armazenadas na memória do servidor ou numa base de dados.

- Identificação na string de requisição – é o texto enviado pelo navegador do consumidor sempre que uma página é executada. Esse texto pode ser visto no campo “Endereço” (“Address”) do navegador. A utilização da string de requisição para identificar sessões é similar ao cookie.

O servidor web da loja cria uma identificação e envia para o navegador. O navegador devolve a identificação nas próximas ações do consumidor.

As variáveis de sessão são armazenadas na memória do servidor ou em uma base de dados e são recuperadas através da associação com a identificação.

- Variáveis de sessão em formulários escondidos ou na string de requisição – nesta forma as variáveis de sessão são enviadas para o navegador e retornadas ao servidor da loja em todas as ações do consumidor.

O servidor não precisa armazenar as variáveis de sessão uma vez que o navegador do consumidor faz este trabalho.

Deve-se notar que, qualquer que seja a forma de recuperar as variáveis de sessão, o servidor web depende do navegador do consumidor. Se o consumidor trocar de navegador (ou computador), as variáveis da sessão original ficarão inacessíveis e a loja estará manipulando um outro conjunto de variáveis de sessão.

Interação entre o Consumidor, o Servidor Web da loja e o MUP

Para que o SPS possa realizar as transações de pagamento, os dados da compra devem ser passados para o MUP de forma segura (passo 5 na lista do início deste capítulo – página 4).

Da mesma forma, nas transações on-line, o resultado do pagamento deve ser retornado para a loja de forma segura (passo 10).

Uma falha de segurança na transação pode causar prejuízos à loja.

O passo 5 (transferência dos dados da compra da loja para o MUP de forma segura) é constituído das seguintes etapas:

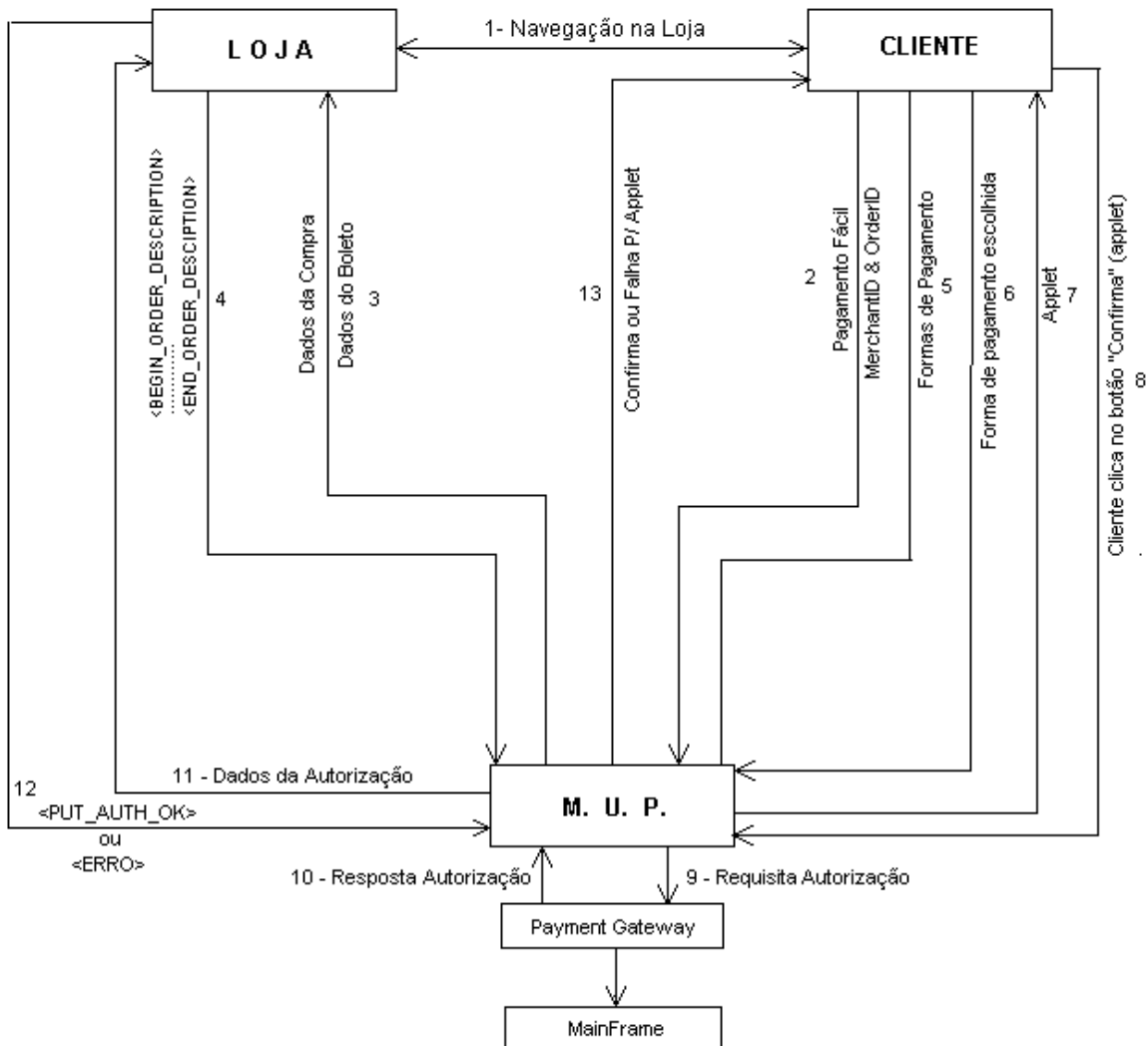
1. A página de escolha do método de pagamento possui *links* para o MUP. Esses *links* apontam para páginas diferentes de acordo com o método de pagamento (por exemplo: pagamento contra-entrega aponta para o arquivo /cheque/redirector.asp). Esses *links* possuem também as identificações da loja e da compra. Ao selecionar uma forma de pagamento o consumidor faz seu navegador requisitar essa página enviando esses dados.
2. A página do MUP que recebe esses dados verifica a existência da loja na base de dados
3. O MUP busca os dados da compra. O MUP simula um navegador requisitando uma página da loja. Ao chamar essa página o MUP fornece algumas variáveis que podem ser configuradas no gerenciador do SPS. A loja deve utilizar esses dados para saber qual compra o MUP está requisitando.

Observe que as variáveis de seção para essa compra não estão disponíveis pois, como foi visto na seção anterior (“Variáveis de sessão”), não é o navegador do consumidor que requisita essa página.

1. A loja monta uma descrição da compra contendo os itens adquiridos, informações de frete e outras taxas e o total da compra. A descrição da compra deve ser formatada conforme descrito no documento de integração de lojas.
2. O MUP recebe essa página e verifica a validade dos dados recebidos. Se os dados recebidos estiverem consistentes ele redireciona o navegador para o processo de pagamento correspondente ao método escolhido.

O processo de pagamento pode pedir mais dados (como por exemplo informações de parcelamento) ou finalizar o pagamento (no caso do boleto e contra-entrega o processo pagamento continua fora do SPS).

Fluxo de Mensagens – Pagamento Fácil



- 1) **Navegação na loja** : O cliente navega na loja normalmente, incluindo e retirando produtos na cesta de compras. Quando o cliente finalizar o processo de escolha, a loja apresenta as formas de pagamento disponíveis para o cliente. Neste momento o cliente escolhe pagar com Pagamento Fácil. O cliente faz, então, uma chamada ao servidor M.U.P. passando como parâmetros o MerchantID, OrderID e Portal (número da loja e número do pedido e identificador do portal de origem respectivamente). Note que esta página é montada pela loja, e é enviada ao cliente.
- 2) **Forma de Pagamento** : Quando o servidor M.U.P. recebe a requisição feita no item anterior, a loja é identificada, suas (da loja) configurações são lidas pelo servidor.
- 3) **Requisição dos dados** : Após lidas as configurações, o servidor abre uma conexão com o servidor da loja requisitando os dados da compra. Esta requisição é feita chamando-se a página que estiver configurada em "URL de notificação", que nos exemplos das lojas de demonstração chama-se DadosCompra.asp.
- 4) **Retorno dos Dados** : A página anterior deverá responder as *Strings* com o descritivo de compra (<BEGIN_ORDER_DESCRIPTION>.....<END_ORDER_DESCRIPTION>) e o descritivo dos dados do boleto (BEGIN_BOLETO_DESCRIPTION>.....<END_BOLETO_DESCRIPTION>). Recebendo estes dados, o servidor faz o *parsing* da string, retirando os dados e dando início ao processo de compra. Se, algum erro existir no envio desta string ou na formatação da mesma, o sistema vai retornar o erro -503.

- 5) **Lista de formas de Pagamento** : Quando o servidor M.U.P. recebe as *strings* com o descritivo da compra, é enviado à máquina do cliente a lista das formas de pagamento disponíveis na loja.
- 6) **Forma de pagamento escolhida** : O cliente escolhe uma forma de pagamento clicando no *link* respectivo.
- 7) **Applet** : Após a escolha da forma de pagamento (à vista, parcelada etc), o servidor do M.U.P. envia ao cliente o *Applet*. Neste applet, o cliente digita os dados do cartão para a efetivação do pagamento.
- 8) **Confirma** : Após a digitação dos dados na Carteira Fácil, o cliente clica no botão “Confirma”. Os dados são criptografados e enviados ao servidor do M.U.P.
- 9) **Requisita Autorização** : O M.U.P. recebe os dados, abre as mensagens e faz a requisição da autorização da transação, enviando os dados para o *Payment Gateway*. Este, envia os dados para a autorização no MainFrame do Banco.
- 10) **Resposta da Autorização** : O sistema recebe a resposta da autorização e repassa para o M.U.P.
- 11) **Dados da autorização** : Os dados da autorização são repassados para a loja. Estes dados são enviados, chamando-se novamente a página configurada na *URL de Notificação*. Mas, nesta segunda chamada, o campo TransId é preenchido com o valor “PutAuth”. Além disso, os campos configurados nos campos post de sucesso ou falha são enviados como parâmetro na chamada da página de acordo com o resultado da transação.
- 12) **Resposta da Loja** : A loja, após receber a resposta da transação deve enviar ao servidor M.U.P. o resultado da atualização dos dados em sua (da loja) base de dados. Assim, se a loja conseguir salvar os dados corretamente, a tag <PUT_AUTH_OK> deverá ser enviada. Caso ocorra algum erro, a tag<ERRO> deverá ser enviada ao servidor como resposta da segunda chamada da página. Vale lembrar aqui, que se algum erro ocorrer antes do envio da tag <PUT_AUTH_OK>, o sistema vai retornar o erro –502.
- 13) **Confirma ou Falha** : De acordo com o resultado do item anterior, é enviada uma url para o applet (Confirma ou Falha), que vai instruir o *browser* do cliente a buscar a página de confirmação de compra ou de falha no pedido diretamente do servidor da loja. No caso de sucesso, a página de confirmação de compra é chamada passando-se o post de sucesso como parâmetro de chamada da mesma. O funcionamento da página de falha é análogo, ou seja, se o processo de autorização falhar, a página de falha da loja será chamada passando-se como parâmetro o post de notificação de falha.

Antes da integração

Antes de iniciar a integração, é preciso considerar alguns aspectos.

Caso a loja já esteja em funcionamento com outras formas de pagamento, é necessário que sejam feitos testes com as formas de pagamento já existentes antes de se realizar a integração. Uma vez realizado estes testes passa-se para a fase seguinte.

Caso seja uma loja nova deve-se saber se a loja aceitará ou não outros métodos de pagamento.

Recomendações

A integração deve ser feita preferencialmente pela mesma equipe que criou a loja, o que contribui para uma adaptação com resultados mais rápidos

A equipe deve ter conhecimento de acesso a base de dados além de conhecer a plataforma de desenvolvimento da loja. Para usar os exemplos é preciso ter conhecimento de ASP.