Release Documentation

Processamento para Emissores

3D Secure para Cartões Reais – Evoluções SecurePay / EBA Emissores

Versão: 01.02

Data: 2015-08-06

Estado: Final

Classificação: Restrito

Referência: DCSIBS150096

SIBS - FORWARD PAYMENT SOLUTIONS, S.A.
Rua Soeiro Pereira Gomes, Lote 1, 1649-031 LISBOA, PORTUGAL
Telefone: +351-217 813 000 / Fax: +351- 217 935 755

Ficha Técnica

Referência:	DCSIBS150096
Título do Documento:	3D Secure para Cartões Reais – Evoluções SecurePay / EBA
Versão:	01.02
Estado:	Final
Classificação:	Restrito
Tipo de Documento:	Release Documentation
Área Funcional Responsável:	AF Desenvolvimento de Serviços

Documentos Relacionados

Referência	Título	Origem
DCSIBS100026	Manual de Implementação - Serviços para Emissores - Emissores	AF Desenvolvimento de Serviços
DCSIBS110139	Manual do Serviço - Processamento para Emissores	AF Desenvolvimento de Serviços
DCSIBS120046	Formulário de Caracterização do Emissor	AF Desenvolvimento de Serviços
DCSIBS120047	Formulário de Caracterização do CPD do Emissor	AF Desenvolvimento de Serviços
DCSIBS120049	Formulário de Caracterização do BIN	AF Desenvolvimento de Serviços
DCSIBS150112	Formulário de Gestão de Templates dos SMS	AF Desenvolvimento de Serviços

Revisões

Versão	Data	Descrição	Autor
01.00	2015-04-14	Criação do documento	AF Desenvolvimento de Serviços
01.01	2015-05-08	Nesta versão foram efetuadas as seguintes alterações face à versão anterior: • Informação sobre o modo de utilização dos Limites para autenticação (secção 2.5) • Alteração na Caracterização de BIN (secção 3.1) do descritivo da obrigatoriedade de *password* associada à autenticação por SMS • Correção de incoerência de valores relativos à dependência da caracterização de BIN das notas relativas às mensagens de Adesão (secção 4.1.2.1) e Manutenção do serviço (secção 4.1.2.3) • Apresentação dos impactos no ficheiro DST5 (secção 4.1.3.1) • Apresentação dos impactos no ficheiro EFAC (secção 4.1.3.2) • Inclusão de 2 novas questões nas Perguntas frequentes (Capítulo 6) Outras alterações editoriais não assinaladas com cor azul e sem impacto na informação técnica.	AF Desenvolvimento de Serviços
01.02	2015-08-06	• Adição do campo 8572-BIN_ATTFRE (Autenticação Forte) e nota correspondente C), na mensagem H473 - S473: Consulta 3D Secure (V02) (secção 4.1.2.2).	AF Desenvolvimento de Serviços

Índice

Índice de Figuras

Índice de Tabelas

1 Introdução

Após um período de consulta pública, a 31 de janeiro de 2013, o Banco Central Europeu (BCE) publicou a versão final de um conjunto de recomendações sobre a segurança dos pagamentos na internet, emanadas do *SecurePay forum*.

Ao longo do ano de 2014, foi identificada a necessidade de se criar uma base legal mais sólida, em linha com as recomendações obtidas, proporcionando-se uma implementação mais consistente por parte das Instituições Financeiras de todos os Estados-Membros do Espaço Económico Europeu (UE, Islândia, Noruega e Liechtenstein), tendo sido divulgado, em dezembro de 2014, um documento da *Euro Banking Association* (EBA) intitulado "*Final guidelines on the security of internet payment"* doravante designado como "*Guidelines"*.

Para além das recomendações relativas a processos internos de cada Instituição Financeira, e das recomendações relacionadas com a necessidade de informação aos detentores de cartão, existem também recomendações relativas à autenticação dos detentores de cartão quando efetuam compras na internet ou quando acedem a informação, que permita a realização desse tipo de transações. Assim sendo, a autenticação dos detentores de cartão deverá ser realizada de acordo com os princípios de autenticação forte.

No âmbito do Serviço de Processamento para Emissores, a SIBS FPS disponibiliza a possibilidade dos cartões com marca internacional (VISA e MasterCard), devidamente registados no *Access Control Server* (ACS) da SIBS FPS, poderem efetuar transações em contexto de *e-commerce,* de acordo com o protocolo 3D Secure.

1.1 Enquadramento

Desde o início de 2013, a SIBS FPS disponibiliza no âmbito do serviço de processamento para Emissores, a funcionalidade 3D Secure para cartões reais. Esta funcionalidade prevê a autenticação das transações em comerciantes 3D Secure, quando os cartões de pagamento se encontram registados no ACS da SIBS FPS.

O mecanismo de autenticação suportado contempla apenas a utilização de *passwords* estáticas.

Com a evolução agora divulgada, a oferta 3D Secure para cartões reais passa a suportar também a autenticação forte baseada numa *One-Time Password* (OTP) a indicar pelo Titular do cartão, no momento da autenticação 3D Secure.

Para permitir a divulgação progressiva desta alteração regulamentar aos detentores de cartão, e simultaneamente diminuir os impactos de uma implementação repentina resultante destas medidas, a SIBS FPS desenvolveu em paralelo a funcionalidade de *"Promotion During Shopping"*, que visa a apresentação, no momento da realização da compra num comerciante 3D Secure, de uma mensagem do Emissor aos Titulares de cartão ainda não aderentes ao serviço 3D Secure. Esta mensagem tem como objetivo

encaminhar o Titular do cartão para os canais do Emissor, para que aí possa realizar a adesão ao ACS Cartões Reais.

Alinhada com o previsto nas *Guidelines* publicadas pela EBA, a SIBS FPS possibilita ainda aos Emissores a dispensa da autenticação de operações em função do valor associado às mesmas. Assim, é possível aos Emissores indicarem limites abaixo dos quais os seus clientes são dispensados os mecanismos de autenticação.

1.2 Âmbito

A presente *Release Documentation* apresenta a descrição das novas funcionalidades da oferta 3D Secure - ACS Cartões Reais e respetivos impactos processuais e técnicos de implementação para os Emissores.

Pretende-se com este documento que os Emissores possam avaliar os impactos inerentes às novas funcionalidades introduzidas e possam simultaneamente planear a respetiva implementação.

2 Descrição da Evolução

A autenticação do Titular do cartão que efetua operações com cartão em ambiente 3D Secure era até agora assegurada pelo recurso a uma *password estática* definida pelo Titular do cartão no momento da adesão ao serviço ou em momento posterior através dos canais do Emissor.

Com a evolução agora divulgada, a oferta 3D Secure - ACS Cartões Reais, passa a suportar também a autenticação baseada também em OTP que o Titular do cartão recebe ou gera no momento da autenticação 3D Secure e que tem de introduzir no formulário de autenticação que surge no seu *browser* de internet, no momento da compra.

A definição dos métodos de autenticação que os Titulares dos cartões poderão adotar para efetuarem a autenticação das transações, é realizada pelos Emissores ao nível da caracterização de BIN e Extensão (EXT).

Assim, ao nível do BIN+EXT os Emissores poderão permitir os seguintes métodos de autenticação:

- *Password* estática;
- Autenticação por SMS (envio de OTP por SMS);
- Autenticação por MB CODE.

Associado à autenticação por SMS, os Emissores poderão manter a obrigatoriedade de definição de uma *password* estática pelos seus clientes. Esta indicação será também posicionada ao nível da caracterização de BIN+EXT.

2.1 Mecanismos de autenticação forte

A autenticação forte, de acordo com as *Guidelines* requer a utilização de dois ou mais fatores de autenticação de entre três categorias:

- *Something you know* (ex.: PIN do telemóvel, PIN do cartão EMV-CAP, credenciais do canal onde é efetuada a adesão ao serviço);
- *Something you have* (ex.: telemóvel, cartão EMV-CAP);
- *Something you are* (ex.: elemento biométrico de autenticação da transação ou desbloqueio do equipamento que gera OTP);

sendo que os fatores adotados deverão ser independentes, de forma a evitar que o comprometimento de um fator comprometa o(s) outro(s), e pelo menos um deles deverá ser dinâmico.

Para assegurar o dinamismo da autenticação das transações realizadas com cartão na internet, a SIBS FPS adotou para a sua solução a utilização de OTP. A disponibilização da OTP ao Titular do cartão é efetuada por um de dois métodos:

- SMS com a *One-Time Password,* enviado para o número de telemóvel associado ao número do cartão;
- *One-Time Password,* gerada com recurso ao serviço MB CODE (baseado na utilização de um cartão com aplicação EMV-CAP, do respetivo PIN e de um *hardware token*).

Estas *passwords* têm como características principais serem dinâmicas (sempre que são geradas, são distintas das anteriores), e no caso das OTP enviadas por SMS tem um período de vida útil reduzido.

2.1.1 SMS com OTP

Quando o método de autenticação associado a um cartão é baseado no envio de um SMS com uma OTP, o Titular do cartão teve de indicar o número de telemóvel "responsável" pela autenticação das transações efetuadas com o cartão em causa.

Quando o Titular do cartão registado no ACS da SIBS FPS indica o número do seu cartão no *website* de um comerciante 3D Secure para efetuar um pagamento, é-lhe apresentada uma página onde vê dados relativos ao pagamento que pretende efetuar (nome do comerciante, montante e data da transação) e também a terminação do número de telemóvel associado ao cartão no ACS. Essa página está também preparada para recolher um código numérico que servirá para autenticar o Titular do cartão.

Simultaneamente à apresentação da página de recolha do código numérico é enviado, para o número de telemóvel associado ao cartão, um SMS com uma OTP. É esta OTP que o Titular do cartão deve introduzir na página que é apresentada no *browser* onde está a efetuar a compra.

No caso de o Emissor obrigar à utilização de uma *password* estática complementarmente ao envio do SMS com a OTP, o Titular do cartão é primeiro confrontado com uma página de recolha da *password* estática, sendo depois solicitada a introdução da OTP recebida por SMS.

A SIBS FPS permite aos Emissores a definição do texto dos SMS enviados aos Titulares de cartão, havendo contudo regras para a sua definição (ver 3.4 - Definição de *templates* para SMS). Os textos dos SMS podem ser definidos para todos os cartões de um Emissor, ou podem ser definidos textos por cada BIN+EXT. Desta forma, os Emissores poderão adaptar a linguagem e o formalismo dos textos enviados de acordo com o BIN+EXT.

2.1.2 MB CODE

À semelhança do descrito quando o método de autenticação associado a um cartão é baseado no envio de um SMS para o Titular do cartão, quando o método de autenticação é o MB CODE, é também apresentada uma página de recolha de um código numérico no momento da compra num comerciante 3D Secure.

O Titular do cartão deve gerar nessa altura uma OTP com o cartão EMV-CAP, recorrendo ao PIN e ao cartão EMV-CAP identificado no momento da adesão ao 3D Secure - ACS Cartões reais e ao *hardware token*. A OTP gerada deve depois ser utilizada como código numérico de autenticação na página apresentada no *browser* onde efetua a compra.

2.2 Alteração do método de autenticação

Se o Emissor pretender disponibilizar o método de autenticação de envio da OTP por SMS inicialmente, e posteriormente se verificar a necessidade de complementar a autenticação com uma *password* (em simultâneo com o SMS), poderá dar essa indicação através da caracterização de BIN+EXT. A alteração da caracterização de BIN+EXT para passar a ter *password* obrigatória adicionalmente ao SMS levará a que o serviço passe a fazer o *Promotion During Shopping* para os cartões para os quais não existe uma *password* definida. Nessa situação o Titular do cartão tem de definir a *password* para o cartão no serviço de ACS Cartões Reais através dos canais do Emissor, para que volte a ser feita a autenticação do Titular do cartão com envio de OTP por SMS e recolha e validação da *password*.

2.3 Adesão dos Titulares de cartão

A adesão dos Titulares de cartão ao 3D Secure - ACS Cartões Reais consiste na criação e registo no ACS da SIBS FPS da relação entre um cartão e um mecanismo de autenticação. No momento da adesão ao serviço, efetuada num canal em que é possível ao Emissor do cartão assegurar que o detentor do cartão é o seu Titular, é efetuada a associação do cartão ao mecanismo de autenticação que o Titular do cartão pretende utilizar para efetuar a autenticação dos pagamentos com cartão na internet, em comerciantes aderentes ao 3D Secure. Assim, dependendo do método de autenticação disponibilizado pelo Emissor ao seu Cliente, serão associados os seguintes elementos:

- *Autenticação por Password* estática: será associada apenas uma *password* definida pelo Titular do cartão nos canais do Emissor;
- Autenticação por SMS: será associado o número de telemóvel indicado pelo Emissor. Se o Emissor obrigar à definição de uma *password* complementarmente ao envio da OTP por SMS, será também efetuada a associação da *password*;
- Autenticação por MB CODE: serão associados o número e data de expiração do cartão com a aplicação CAP indicado pelo Emissor (este cartão pode ser o próprio cartão de pagamento do Titular do cartão ou outro cartão de pagamento com a aplicação EMV CAP registado e ativo no serviço MB CODE).

No caso de o Emissor disponibilizar o envio de SMS com OTP como método de autenticação, os SMS serão sempre enviados a partir da infraestrutura de comunicação da SIBS FPS. Contudo, para além da possibilidade do SMS ser envidado através do operador da SIBS e ser faturado pela SIBS ao Emissor, é também possível, para permitir a integração do custo do envio dos SMS nos tarifários acordados por cada Emissor com os operadores de comunicações, cada Emissor parametrizar junto da SIBS FPS a informação

relativa ao seu contrato de comunicações com os operadores (*large accounts*), sendo assim os SMS enviados em seu nome. Neste último cenário, o Emissor tem de informar o seu operador que autoriza a SIBS FPS a enviar SMS usando a sua *large account* e fornecer à SIBS FPS as credenciais para o acesso à infraestrutura do operador.

2.4 Promotion During Shopping

Para além da definição de prazos para a adoção das *Guidelines* pelos Emissores (e restantes *stakeholders* do *e-commerce*), estas também atribuem aos Emissores responsabilidades na "educação" e informação aos Titulares de cartão. Para esse efeito, a SIBS criou a funcionalidade *Promotion During Shopping*.

Esta funcionalidade permite a adesão gradual dos Titulares de cartão aos novos requisitos para a realização de compras na internet resultantes das *Guidelines*, não só pela informação disponibilizada aos Titulares de cartão, mas também por assegurar a flexibilidade que o Emissor entenda necessária na imposição dos mecanismos de autenticação aos seus Clientes.

O *Promotion During Shopping* permite ao Emissor uma comunicação mais próxima com os Titulares de cartão que realizam efetivamente compras na internet, encaminhando-os para os canais dos Emissores. No momento da compra num comerciante 3D Secure, a SIBS FPS verifica se o número do cartão indicado pelo cliente para o pagamento na internet se encontra registado no ACS da SIBS FPS. Se o cartão estiver registado e com o serviço em estado normal (não cancelado, não expirado ou não bloqueado por número de tentativas de autenticação falhadas), é apresentada uma página de recolha das credenciais de autenticação. No caso de o número de cartão não se encontrar registado no ACS da SIBS FPS, a página de recolha de credenciais de autenticação é substituída por uma página com uma mensagem definida pelo Emissor do cartão a encaminhar o seu Cliente para os canais do Banco e propondo a adesão ao 3D Secure - ACS Cartões Reais.

Sempre que é apresentada a página com a mensagem definida pelo Emissor, a transação é considerada autenticada e é atualizado um contador associado ao cartão. Quando este contador atinge o limite definido pelo Emissor, as compras sem autenticação realizadas com o cartão em causa deixam de ser aceites. Desta forma, o Emissor dá a oportunidade aos seus clientes de continuarem a efetuar compras na internet enquanto não têm a possibilidade de aceder aos canais do Emissor para aderirem ao 3D Secure - ACS Cartões Reais.

A ativação do *Promotion During Shopping* e o número de compras sem autenticação são posicionados ao nível do BIN+EXT, através dos parâmetros: "*Promotion During Shopping"* e "Número de Operações sem Autenticação".

A mensagem apresentada ao Titular do cartão resultante do *Promotion During Shopping* é definida pelo Emissor para todos os seus cartões (ao nível da caracterização de Emissor).

2.5 Limites

Tendo em conta os impactos que a autenticação forte terá na usabilidade e na experiência de compra dos Titulares de cartão, as *Guidelines* permitem a adoção de mecanismos de gestão de risco por parte dos Emissores.

Sendo o montante das transações um dos indicadores de risco, e de modo a não degradar a experiência de utilização dos cartões na internet, a SIBS FPS permite aos Emissores indicarem o montante de transação a partir do qual é requerida a autenticação do Titular do cartão. Os detentores do cartão ficam desta forma dispensados[1] de autenticação nas compras na internet cujos valores estejam abaixo desse determinado montante.

Por outro lado, se o Emissor pretender aumentar a robustez do tipo de autenticação de acordo com o montante da transação a autenticar (apenas aplicável às situações em que o método de autenticação é Autenticação por SMS e a *password* estática é obrigatória), poderá definir um montante adicional que permite a distinção da necessidade de uma autenticação simples apenas com *password*, de uma autenticação forte a que acresce o envio de SMS com a OTP.

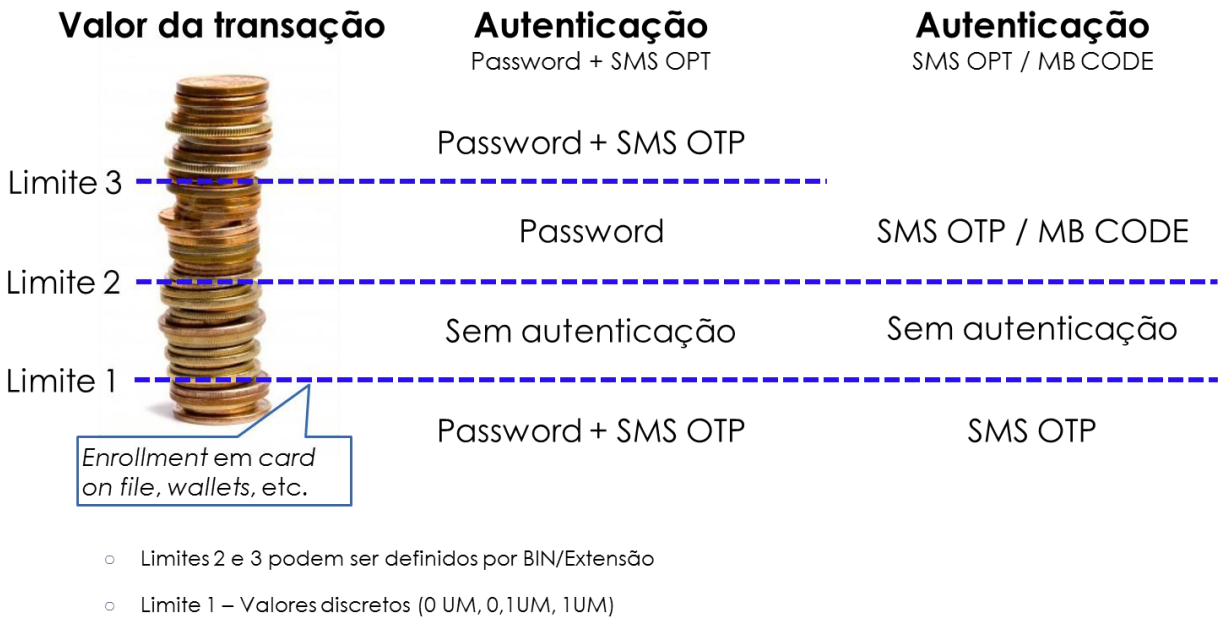
A definição destes montantes é feita para cada BIN+EXT, através dos parâmetros:

- Montante a partir do qual é necessário Autenticação (corresponde ao montante de transação a partir do qual o Titular do cartão é confrontado com um pedido de autenticação de acordo com o método definido na adesão: *Password*, SMS ou MB CODE);
- Montante a partir do qual é necessário Autenticação por SMS e *Password* (aplicável apenas nas situações em que o método de autenticação é SMS com *password* obrigatória e corresponde ao montante a partir do qual é enviado um SMS após a introdução e validação da *password*. Para montantes de transação compreendidos entre o "Montante a partir do qual é necessário Autenticação" e o "Montante a partir do qual é necessário Autenticação por SMS e *Password*", será solicitada apenas a *Password* ao Titular do cartão).

Adicionalmente aos montantes posicionados pelos Emissores, existe também um conjunto de montantes frequentemente utilizados pelos Comerciantes e *providers* de *wallets* nas mensagens de autorização, de modo a validar os cartões e a promover a sua integração com as *wallets*. De acordo com as *Guidelines*, estas transações de associação de cartões a *wallets*, estão também obrigadas à realização de autenticação forte. Para responder a esta obrigatoriedade, a SIBS FPS definiu montantes de sistema para os quais será sempre solicitada autenticação do Titular do cartão. Os montantes definidos neste contexto são: zero unidades monetárias (0,00UM); um cêntimo de unidade monetária (0,01UM) e uma unidade monetária (1,00UM).

[1] A isenção da autenticação da transação por parte do cliente corresponde à assunção do risco da transação por parte do Emissor, uma vez que do ponto de vista do protocolo 3D Secure, é corretamente autenticada.

Na figura abaixo está representado o modelo de funcionamento dos limites.



- Limites 2 e 3 podem ser definidos por BIN/Extensão
- Limite 1 – Valores discretos (0 UM, 0,1UM, 1UM)

Figura 1 - Representação do funcionamento dos limites

Os limites definidos pelos Emissores são posicionados na caracterização de BIN+EXT.

2.6 Protocolo 3D Secure

A evolução à funcionalidade 3D Secure - Serviço de ACS Cartões Reais descrita nesta *Release Documentation* tem o seguinte enquadramento no protocolo 3D Secure:

Se no momento da realização da compra, o Titular do cartão de pagamento tiver efetuado a adesão à funcionalidade 3D Secure - Serviço de ACS Cartões Reais, ser-lhe-á solicitada a informação das credenciais de autenticação de acordo com os métodos de autenticação possíveis definidos pelo Emissor ao nível da caracterização de BIN+EXT, e do método que o Titular definiu no momento da adesão.

Se a autenticação for validada pelo ACS da SIBS FPS, ou o montante da transação estiver incluído no intervalo definido pelo Emissor para dispensar a autenticação, a transação é comunicada ao Comerciante como “Autenticada” de acordo com protocolo 3D Secure. Se a informação indicada pelo Titular do cartão não for validada pelo ACS da SIBS FPS, o comerciante é notificado de que o detentor do cartão não foi autenticado, e segundo o protocolo 3D Secure, não deve prosseguir com a transação.

Se no momento da realização da compra, o Titular do cartão de pagamento ainda não tiver efetuado a adesão à funcionalidade 3D Secure - Serviço de ACS Cartões Reais, e o Emissor tiver solicitado a ativação do *Promotion During Shopping* na caracterização de BIN+EXT, o Titular do cartão é confrontado com a mensagem definida pelo Emissor que o encaminha para os canais do Emissor e indica da necessidade de adesão ao 3D Secure. Se o número de situações em que o Titular do cartão foi confrontado com esta

informação for inferior ao número de transações que o Emissor permite aos seus clientes sem efetuarem a adesão prévia à funcionalidade, o comerciante é informado da tentativa de autenticação do detentor do cartão. Se o número de transações que o Emissor permite sem adesão ao 3D Secure tiver sido igualado ou excedido, o comerciante é informado de que o detentor do cartão não foi autenticado e que por isso não deve prosseguir com a transação.

Em termos genéricos[2], as regras de *liability shift* preveem que o risco das transações seja atribuído aos Emissores sempre que o resultado de uma autenticação 3D Secure é de uma transação autenticada ou tentada.

Tabela 1 - Resultado de autenticação de acordo com o contexto da transação

Contexto da transação		Resultado da autenticação para o comerciante
Cartão aderente ao 3D Secure	Montante dispensa autenticação	Transação autenticada
	Dados de autenticação validados	Transação autenticada
	Dados de autenticação não validados	Transação não autenticada
Cartão não aderente ao 3D Secure	Número de compras sem autenticação inferior ao número autorizado pelo Emissor	Transação com autenticação tentada
	Número de compras sem autenticação igual ou superior ao número autorizado pelo Emissor	Transação não autenticada

EM RESUMO:

- **Evolução à oferta 3D Secure - Serviço de ACS Cartões Reais (VISA, MasterCard).**
- **SMS com OTP e MB CODE como métodos de autenticação de transações na internet.**
- ***Promotion During Shopping* para permitir uma adesão gradual dos Titulares de cartão, sem degradar experiência de compra e sem aumento excessivo de taxas de recusa de transações.**
- **Montantes de transação como elemento de decisão para a necessidade de autenticação.**
- **Envio de SMS com o tarifário da SIBS ou do Emissor**

[2] Podem existir produtos de cartão ou geografias não abrangidos pelas regras de *liability shift*. Os Emissores deverão consultar a aplicabilidade destas regras na documentação dos sistemas de pagamento internacionais.

3 Processo de Adesão

Para permitir a adesão dos seus Clientes ao ACS da SIBS FPS, os Emissores têm de alterar a caracterização de BIN+EXT, definir os parâmetros associados ao *Promotion During Shopping* na caracterização de Emissor e posicionar a informação respeitante ao *template* dos SMS a enviar com as OTP. Os Emissores podem definir o *template* com o texto do SMS por BIN+EXT ou definir um único *template* com o texto a enviar a todos os seus Clientes, independentemente do BIN+EXT. A SIBS definiu também um *template* geral para o serviço que será usado no caso de o Emissor não pretender definir um texto específico próprio.

3.1 Caracterização de BIN

No âmbito da evolução descrita nesta *Release Documentation*, a SIBS FPS procedeu à atualização do formulário de caracterização de BIN. Neste formulário, em particular no bloco de parâmetros correspondente ao 3D Secure, os Emissores podem definir os métodos de autenticação disponíveis para os detentores de cartão adotarem.

Estão disponíveis três métodos de autenticação disponíveis para os Emissores, sendo que o detentor do cartão optará por um dos métodos disponibilizados no momento da adesão do cartão no ACS pelo seu Emissor. Os métodos de autenticação disponíveis são:

- Autenticação por *password*;
- Autenticação por SMS (envio de OTP por SMS);
- Autenticação por MB CODE.

Quando disponibilizado o método de autenticação por SMS, o Emissor pode obrigar simultaneamente à introdução de *password*. Nesse caso, o Emissor deve posicionar na opção[3] sobre o uso simultâneo de *password* com '1 - *Password* Obrigatória'.

Na caracterização de BIN+EXT, são também posicionados os limites que permitem a isenção ou autenticação diferenciada de acordo com o montante das transações. São parametrizáveis:

- Montante a partir do qual é necessária Autenticação;
- Montante a partir do qual é necessária Autenticação por SMS e *Password*[4].

No mesmo bloco de parâmetros, os Emissores indicam se pretendem a ativação do *Promotion During Shopping* e do número compras não presenciais em comerciantes 3D que os seus Clientes podem efetuar antes da adesão ao ACS. Estes indicadores são posicionados respetivamente em:

- *Promotion During Shopping*;
- Número de Operações sem Autenticação.

[3] Esta opção é posicionada no parâmetro 5.5 a) do Formulário de Caracterização de BIN.

[4] Este montante só será usado se o método de autenticação do cartão for SMS e a caracterização de BIN+EXT indicar que é obrigatória a introdução de *password* para o método SMS.

3.2 Caracterização de Emissor

A SIBS FPS procedeu à atualização do formulário de caracterização de Emissor de modo a permitir a definição da mensagem a apresentar aos Titulares de cartão no âmbito da funcionalidade de *Promotion During Shopping*. Esta informação é posicionada em:

- "Texto a apresentar ao cliente para adesão ao serviço 3D Secure" - Mensagem até 160 caracteres, a apresentar, no momento de uma compra 3D Secure, aos detentores de cartão que ainda não efetuaram a adesão do cartão ao ACS da SIBS FPS se o *Promotion During Shopping* estiver ativo para o BIN+EXT do cartão.

3.3 Adesão massiva

A associação do método de autenticação ao cartão é da responsabilidade dos Emissores e/ou dos Clientes detentores de cartão. A SIBS FPS disponibiliza interfaces específicos *host-to-host* (ver 4.1.2 Mensagens *Host-to-Host*) para o registo dos cartões com o respetivo método e credencial de autenticação.

Os Emissores devem analisar a abordagem que considerarem mais adequada para os seus Clientes e disponibilizar a operação de adesão dos cartões ao ACS nos seus canais, ou então proceder à adesão massiva dos seus cartões com recurso ao Ficheiro de Gestão de Dados do Serviço MULTIBANCO - GDSM, descrito no Manual de Implementação do Serviço de Processamento para Emissores (documento SIBS com a referência: DCSIBS100026).

3.4 Definição de *templates* para SMS

Está definido a nível do serviço de ACS da SIBS FPS um *template* com o texto a enviar por SMS para o número de telemóvel associado ao cartão pelo Emissor, para fazer a autenticação do Titular do cartão por SMS.

O texto do *template* definido no serviço é o seguinte:

"Para autorizar a Compra efetuada no <!Nome do Comerciante!> no valor de <!Montante!>, introduza o Código de Autorização <!OTP!>.".

- O serviço de ACS da SIBS FPS substitui o elemento *<!Nome do Comerciante!>* pelo nome do comerciante no momento da transação. Serão utilizados até 25 caracteres da identificação do comerciante indicada nas mensagens técnicas do 3D Secure.
- O serviço de ACS da SIBS FPS substitui o elemento *<!Montante!>* pelo valor da compra no momento da transação. O montante pode ter entre 3 e 12 caracteres.

- A Plataforma Segura de Autenticação da SIBS FPS, usada pelo serviço ACS, substitui o elemento *<!OTP!>* pela OTP gerada aleatoriamente no momento da transação. A dimensão da OTP é de 7 dígitos[5] por omissão. Para a dimensão por omissão, o OTP será enviado no SMS com o seguinte formato "x xxx xxx".

O Emissor pode usar outro texto para os SMS, e nesse caso deve enviar para a área de Regularizações da SIBS FPS o *template*, ou os *templates*, com o(s) texto(s) que pretende através do formulário *"Formulário de Gestão de Templates dos SMS"*, para que seja(m) configurado(s) no serviço. Pode definir apenas um *template* para todos os seus cartões, ou um *template* específico por BIN+EXT. Deve usar a mesma sintaxe indicada acima para o template do serviço, relativamente aos elementos nome do comerciante, montante da transação e OTP, podendo dispô-los como entender no template. A presença do elemento *<!OTP!>* no template é obrigatória. A presença dos elementos *<!Nome do Comerciante!>* e *<!Montante!>* é facultativa.

O processo de decisão do *template* usado pelo serviço para envio da OTP por SMS é o seguinte:

1. Se estiver posicionado no BIN+EXT do cartão usado na transação um *template* específico, usa-se o *template* do BIN+EXT;
2. Se o BIN+EXT do cartão usado na transação não tem um *template* específico definido, e o Emissor tem um *template* próprio posicionado ao nível do Emissor, usa-se o *template* do Emissor;
3. Se não se aplicar nenhumas das situações anteriores usa-se o *template* do serviço.

Os *templates* definidos pelo Emissor, em uso pelo serviço, podem ser consultados no Portal de Serviços SIBS, através da opção de menu Cartões->Cartões Bancários->Caracterização Emissor->Consultar SMS.

3.5 Contactos

Âmbito	Área	Contacto
Adesão ao Serviço	Departamento de Gestão Comercial	Gestor de Relação Telefone: 21 781 30 00
Parametrizações do Serviço	Núcleo de Regularizações	regularizacoes@sibs.pt

[5] Os Emissores que queiram adotar OTP com dimensão diferente de 7 dígitos devem consultar a SIBS FPS.

4 Implementação do Serviço

Os Emissores têm de ter em conta os mecanismos de autenticação disponíveis na oferta ACS e adaptar as suas infraestruturas técnicas de acordo com os requisitos técnicos a seguir detalhados.

4.1 Especificações Técnicas

4.1.1 Mensagens *Real-Time* com Iniciativa na SIBS FPS

A funcionalidade 3D Secure - Serviço de ACS Cartões Reais do serviço de Processamento para Emissores não requer a criação de novas mensagens *real-time*, não havendo consulta ao Emissor no processo de autenticação, uma vez que esta operação é assegurada pelo ACS da SIBS FPS.

Os Emissores aderentes ao serviço devem estar preparados para receber novos valores possíveis no atributo (0005) TRM_ATTCOD, presente nas mensagens de autorização das transações. Os valores possíveis estão descritos no ponto *"Cenários e classificação das operações card not present"* do *Manual de Implementação do Serviço de Processamento para Emissores*. (documento SIBS referência número: DCSIBS100026).

4.1.2 Mensagens *Host-to-Host*

No âmbito da funcionalidade 3D Secure - Serviço de ACS Cartões Reais do serviço de Processamento para Emissores, a SIBS FPS desenvolveu três mensagens que permitem a integração do serviço com os canais dos Emissores:

- H472 - S472: Adesão ao 3D Secure;
- H473 - S473: Consulta 3D Secure;
- H474 - S474: Manutenção do 3D Secure.

Com a evolução descrita nesta *Release Documentation* é divulgada a versão 2 destas mensagens, cujas alterações estão marcadas a azul.

4.1.2.1 H472 - S472: Adesão ao 3D Secure (V02)

N.º	Sigla	Nome	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de mensagem	2	N	5	5	5	'02'
0471	MSG_IDE_H2H	Identificação mensagem do banco	14	A	7	7	7	

N.º	Sigla	Nome	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
0004	MSG_DTH	Data/Hora da transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de resposta da mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do log associado à transação (novo código expandido)	2	N		38		
0320	LOG_PERN01	Identificação do período do log central	4	N		40		
0117	LOG_NUMN01	Número de registo log central	8	N		44		
Detalhe								
1350	CAR_MBNCOD	Código de cartão associado ao serviço	1	N	21			A)
0505	CAR_PANN03	PAN do cartão	16	N	22			
0637	CAR_EXPDAT	Data de expiração do cartão expandida	6	N	38			
0261	BIN_NUM	BIN	6	N	44			
0319	BIN_EXN	Extensão de BIN	2	N	50			
0128	CAR_NUM	Número do cartão	7	N	52			
6876	CAR_ATT3DS	Modo de autenticação 3D secure	1	N	59			C)
4319	CHV_HAS	Secure Hash	40	A	60			B) D)
0505	CAR_PANN03	PAN do cartão	16	N	100			E)
5325	CAR_EXPDATN01	Data de expiração do cartão	6	N	116			E)
4247	SIS_INIDAT	Data de início	8	N	122			F)
8200	EXT_TLMPRX	Prefixo do telemóvel	7	N	130			G)
8106	EXT_TLMNUM03	Número de telemóvel	11	N	137			G)
0012	MSG_RESTIPA00	Código de resposta	1	A		52		
Trailer								
0493	MSG_NOKTIP	Código de recusa da mensagem pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto resposta	45	A			46	
0472	MSG_RESTXT	Texto resposta	45	A			91	
				Total	**147**	**52**	**135**	

A) Por predefinição só aceita o valor igual a '2' - cartão *on-us*.

B) O algoritmo de cálculo do *hash* é efetuado de acordo com o documento fornecido pela SIBS FPS aquando a abertura do PAAS para adesão à solução 3D Secure.

C) O valor posicionado corresponde ao método de autenticação:

- 1 - *Password*;
- 2 - SMS;
- 3 - MB CODE.

D) Preenchimento obrigatório se:

- (6876) CAR_ATT3DS = '1' ou
- (6876) CAR_ATT3DS = '2' e na caracterização de BIN o Emissor estiver posicionado na opção sobre o uso simultâneo de *password* com '1 - *Password* Obrigatória'.

E) Preenchimento obrigatório se (6876) CAR_ATT3DS = '3'.

F) Deve conter a data da adesão ao 3D Secure.

G) Preenchimento obrigatório se (6876) CAR_ATT3DS = '2'.

Se telefone nacional:

- o atributo (8200) EXT_TLMPRX deve ser preenchido com o valor '00351';
- o atributo (8106) EXT_TLMNUM03 deve ser preenchido com os 9 dígitos do telemóvel precedidos de zeros.

4.1.2.2 H473 - S473: Consulta 3D Secure (V02)

N.º	Sigla	Nome	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de mensagem	2	N	5	5	5	'02'
0471	MSG_IDE_H2H	Identificação mensagem do banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de resposta da mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do log associado à transação (novo código expandido)	2	N		38		
0320	LOG_PERN01	Identificação do período do log central	4	N		40		
0117	LOG_NUMN01	Número de registo log central	8	N		44		
Detalhe								
1350	CAR_MBNCOD	Código de cartão associado ao serviço	1	N	21			A)
0505	CAR_PANN03	PAN do cartão	16	N	22			
0637	CAR_EXPDAT	Data de expiração do cartão expandida	6	N	38			
0261	BIN_NUM	BIN	6	N	44			
0319	BIN_EXN	Extensão de BIN	2	N	50			
0128	CAR_NUM	Número do cartão	7	N	52			
4247	SIS_INIDAT	Data de início	8	N		52		
6876	CAR_ATT3DS	Modo de autenticação 3D secure	1	N		60		B)
0505	CAR_PANN03	PAN do cartão	16	N		61		
5325	CAR_EXPDATN01	Data de expiração do cartão	6	N		77		
6799	SIS_SIT3DS	Situação do 3D secure	1	N		83		
6800	SIS_SITDAT_3DS	Data situação do 3D secure	8	N		84		
6868	CAR_TENCHV	Indica o número de tentativas falhadas	1	N		92		
6869	CAR_RETCHV	Número reset password	1	N		93		
3257	SIS_TIMSTP	Timestamp atualização DB2	26	A		94		
8200	EXT_TLMPRX	Prefixo do telemóvel	7	N		120		
8106	EXT_TLMNUM03	Número de telemóvel	11	N		127		

N.º	Sigla	Nome	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
8572	BIN_ATTFRE	Autenticação Forte	1	N		138		C)
Trailer								
0493	MSG_NOKTIP	Código de recusa da mensagem pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto resposta	45	A			46	
0472	MSG_RESTXT	Texto resposta	45	A			91	
				Total	**58**	**138**	**135**	

A) Por predefinição só aceita o valor igual a 2 - cartão *on-us*.

B) O valor posicionado corresponde ao método de autenticação:

- 1 - *Password*;
- 2 - SMS;
- 3 - MB CODE.

C) Apenas tem significado se CAR_ATT3DS = 2 (SMS).

No caso do método de autenticação ser SMS, este atributo indica se, para além do SMS é obrigatória a utilização da password estática para autenticar o cliente.

Valores possíveis:

0 – Sem Password;

1 – Password Obrigatória.

4.1.2.3 H474 - S474: Manutenção do 3D Secure (V02)

N.º	Sigla	Nome	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de mensagem	2	N	5	5	5	'02'
0471	MSG_IDE_H2H	Identificação mensagem do banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de resposta da mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do log associado à transação (novo código expandido)	2	A		38		
0320	LOG_PERN01	Identificação do período do log central	4	N		40		
0117	LOG_NUMN01	Número de registo log central	8	N		44		
Detalhe								
1350	CAR_MBNCOD	Código de cartão associado ao serviço	1	N	21			A)
0505	CAR_PANN03	PAN do cartão	16	N	22			
0637	CAR_EXPDAT	Data de expiração do cartão expandida	6	N	38			
0261	BIN_NUM	BIN	6	N	44			

N.º	Sigla	Nome	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
0319	BIN_EXN	Extensão de BIN	2	N	50			
0128	CAR_NUM	Número do cartão	7	N	52			
4247	SIS_INIDAT	Data de início	8	N	59			
6876	CAR_ATT3DS	Modo de autenticação 3D secure	1	N	67			B)
6876	CAR_ATT3DS	Modo de autenticação 3D secure (novo)	1	N	68			C)
2483	MSG_ACCCOD	Código de gestão da mensagem	1	A	69			D)
6799	SIS_SIT3DS	Situação do 3D secure	1	N	70			
6800	SIS_SITDAT_3DS	Data situação do 3D secure	8	N	71			
4319	CHV_HAS	Secure hash	40	A	79			E)
4319	CHV_HAS	Secure hash (novo)	40	A	119			F)
6803	SIS_RETIND	Indicador reset password	1	A	159			G)
0505	CAR_PANN03	PAN do cartão	16	N	160			H)
5325	CAR_EXPDATN01	Data de expiração do cartão	6	N	176			H)
3257	SIS_TIMSTP	Timestamp atualização DB2	26	A	182			
8200	EXT_TLMPRX	Prefixo do telemóvel	7	N	208			I)
8106	EXT_TLMNUM03	Número de telemóvel com indicativo do país	11	N	215			I)
Trailer								
0493	MSG_NOKTIP	Código de recusa da mensagem pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto resposta	45	A			46	
0472	MSG_RESTXT	Texto Resposta	45	A			91	
		Total			**225**	**51**	**135**	

A) Por predefinição só aceita o valor igual a 2 - cartão *on-us*;

B) O valor posicionado corresponde ao método de autenticação:

- 1 - *Password*;
- 2 - SMS;
- 3 - MB CODE.

C) A funcionalidade de alteração do método de autenticação não se encontra disponível. Este atributo é preenchido a zeros;

D) Pode assumir os valores:

- 3 - Alteração - permite alterar as credenciais associadas ao método de autenticação definido;
- 4 - Cancelamento - permite o cancelamento do serviço 3D Secure.

Se (2483) MSG_ACCCOD = '3' e:

- (6876) CAR_ATT3DS = '1', o atributo F) é de preenchimento obrigatório. O atributo E) é de preenchimento opcional, sendo validado se preenchido. Os atributos relativos a outros métodos de autenticação devem ser posicionados a zeros ou a espaços;

- (6876) CAR_ATT3DS = ‘2’, os atributos I) são de preenchimento obrigatório. Se na caracterização de BIN o Emissor estiver posicionado na opção sobre o uso simultâneo de *password* com ‘1 - *Password* Obrigatória’, o atributo F) é de preenchimento obrigatório se não foi anteriormente definida uma *password* para o cartão e pode ou não ser preenchido caso contrário. Os atributos relativos a outros métodos de autenticação devem ser posicionados a zeros ou a espaços;
- (6876) CAR_ATT3DS = ‘3’, os atributos H) são de preenchimento obrigatório. Os atributos relativos a outros métodos de autenticação devem ser posicionados a zeros ou a espaços.
- (6803) SIS_RETIND = ‘1’, os atributos relativos a outros métodos de autenticação devem ser posicionados a zeros ou a espaços;

Se (2483) MSG_ACCCOD = ‘4’ o serviço é cancelado;

G) Pode assumir os valores:

- 0 - Não;
- 1 - Sim.

4.1.3 Ficheiros com Iniciativa na SIBS FPS

No âmbito da evolução da funcionalidade 3D Secure - Serviço de ACS Cartões Reais do serviço de Processamento para Emissores, a SIBS FPS evoluiu o Ficheiro de Destinos (DST5) para permitir informar os Emissores o tipo e o número de SMS enviados no âmbito da operação de autenticação por SMS.

4.1.3.1 Ficheiro de Destinos - DST5

Os dados adicionais associados ao código de operação (0699) SIS_OPRTIP = ‘9E7’ (Autenticação de uma operação 3D), são alterados para passarem a transportar o código da rubrica de tarifário SIBS FPS aplicado à operação de autenticação resultante dos envios de SMS, e a quantidade de SMS enviados (um utilizador pode solicitar o envio de uma nova OTP por SMS se não receber o SMS quando está a fazer a compra), assim como a indicação da *Large Account* utilizada para o envio de SMS.

De modo a permitir ao Emissor identificar a tipologia de SMS (SMS Nacional ou SMS Internacional) enviada através da sua *Large Account*, é também posicionado o prefixo do telemóvel para onde foi efetuado o envio.

4.1.3.1.1 Registo de tipo 1

N.º	Sigla	Nome	Comp.	Pos.	Rep.	Obs.
(0699) SIS_OPRTIP = ‘9E7’ (Autenticação de uma operação 3D)						
6876	CAR_ATT3DS	Modo de autenticação 3D SECURE/MB NET	1	312	N	
1368	SPI_3DSMNT	Montante da compra enviado pelo comerciante	12	313	N	
1369	SPI_DCMMOEN01	Casas decimais da moeda	2	325	N	
2300	SIS_TARSIB	Código da rubrica do Tarifário da SIBS FPS	6	327	A	A)
8623	SIS_SMSQTD	Quantidade de SMS	2	333	N	

N.º	Sigla	Nome	Comp.	Pos.	Rep.	Obs.
8622	SIS_LRGCTA	"*Large Account*" de envio de SMS	1	335	N	
8200	EXT_TLMPRX	Prefixo de telemóvel	7	336	N	
	Filler		170	343	A	
			Total	512		

A) Preenchido de acordo com o valor do atributo (8622) SIS_LRGCTA:

- se o atributo (8622) SIS_LRGCTA = '1' - *SIBS*, preenchido com a rúbrica de tarifário SIBS correspondente ao tipo de SMS enviado ("Z 8 1 " - SMS Nacional ou "Z 8 2 " - SMS Internacional);
- se o atributo (8622) SIS_LRGCTA = '2' - *Emissor*, preenchido a espaços.

4.1.3.2 Ficheiro de Faturação - EFAC

No Ficheiro de Faturação (EFAC), para além da comunicação da rúbrica de tarifário Z81 relativa ao envio de SMS para números nacionais, passa também a ser informada a nova rúbrica Z82 correspondente ao envio de SMS para números de telemóvel internacionais.

No preenchimento do registo tipo 4 do EFAC, os campos (0408) SIS_REFDAT e (0417) SIS_IDEDAD, são preenchidos de acordo com:

(2300) SIS_TARSIB	(0416) SIS_REFDAT	(0417) SIS_IDEDAD	Descrição
Z81	(0380) SIS_PRCDAT_INS	(0101) FIC_APL_ID1 + (0102) FIC_NOMN01 + (0061) FIC_SEQN01	Data do processamento, nome e identificação do ficheiro
Z82	(0380) SIS_PRCDAT_INS	(0101) FIC_APL_ID1 + (0102) FIC_NOMN01 + (0061) FIC_SEQN01	Data do processamento, nome e identificação do ficheiro

5 Dicionário de dados

A tabela seguinte descreve os atributos utilizados nas mensagens e ficheiros no âmbito deste serviço.

N.º	Sigla do Campo	Nome do campo	Comp.	Rep.	Formato	Descrição	Valores
0002	MSG_VER	Versão mensagem	2	N	AAAAMMDD	Identifica a versão da mensagem indicada no campo (0001) MSG_TIP ou no campo (0470) MSG_TIP_H2H. Identifica a versão da mensagem que está em uso com o Banco; permite que a SIBS possa suportar mensagens com formatos diferentes relativas ao mesmo serviço.	
0004	MSG_DTH	Data/hora da transmissão	14	N	AAAAMMDDHHMMSS	Campo que contém a data e a hora em que se efetuou a transmissão da mensagem do CPU da SIBS para o CPU do Banco. Não aplicável a registos correspondentes a mensagens trocadas no canal *Host-to-Host.*	
0012	MSG_RESTIPA00	Código de resposta	1	A		Campo que informa a resposta do Banco a um pedido de operação.	0 - Transação aprovada; 1 - Pedido de degradação de Cenário; 2 - Transação inválida pelo SPI; 4 - Transação não aprovada por razões várias; 5 - Transação não aprovada; o campo SALDO indica o máximo que poderia ter sido pago na transação que finda; 6 - Erro aplicacional; 7 - Captura do cartão no CA. Códigos válidos apenas nas mensagens de pedido de autorização: 8 - Recusada. Captura cartão. Suspeita fraude;

N.º	Sigla do Campo	Nome do campo	Comp.	Rep.	Formato	Descrição	Valores
							9 - Autorizado com pedido de identificação. Não aplicável a registos correspondentes a mensagens trocadas no canal *Host-to-Host.*
0117	LOG_NUMN01	Número de registo log central	8	N		Identifica o número do registo no Ficheiro de Log do CPU-SIBS FPS referente à transação. Conjugado com os campos (0312) SIS_APLPDD ou (1709) LOG_SIS, e (0320) LOG_PERN01, identifica univocamente um registo no sistema MULTIBANCO. No caso das autorizações, a identificação posicionada para o Acquirer será feita utilizando as 6 posições da direita do registo do log central.	
0128	CAR_NUM	Número do cartão	7	N		Número identificativo do cartão.	
0261	BIN_NUM	BIN	6	N		O emissor (Banco) pode ter vários produtos-cartões, cada um associado a um identificativo ISO (BIN). Nas transações a SIBS FPS envia o BIN do cartão. Na produção de cartões é um campo a preencher pelo Banco, informando qual dos seus BINs, incluídos na caracterização do emissor, pretende usar. Justificado com zeros à direita.	
0319	BIN_EXN	Extensão de BIN	2	N		Campo reservado para a extensão do BIN do cartão do Banco a utilizar em casos especiais. Se não é utilizado está preenchido a espaços.	
0320	LOG_PERN01	Identificação do período do *log* central	4	N		Identificação do número do ficheiro de *log* da SIBS FPS onde foi registada a operação. Este campo combinado com os campos (0117) LOG_NUMN01 e (0320) LOG_PERN01 ou (1709) LOG_SIS constitui uma chave única da operação. A SIBS FPS usa mais do que um ficheiro de log por dia, pelo que, num mesmo ficheiro da Compensação MULTIBANCO, são encaminhadas operações de vários ficheiros de log; os do dia e eventualmente também os de dias precedentes, caso tenha havido algo que impediu a compensação desse *log*.	

N.º	Sigla do Campo	Nome do campo	Comp.	Rep.	Formato	Descrição	Valores
0470	MSG_TIP_H2H	Código da mensagem BS	4	A		Código da mensagem na sessão Banco - SIBS.	
0471	MSG_IDE_H2H	Identificação mensagem do banco	14	A		No caso de a mensagem ser originada do CPD de um Banco, o seu preenchimento tem o formato que este quiser. No caso de a mensagem ser de um terminal bancário: COD.TERMINAL 6 NUM.PERIODO 2 NUM.TRANSACÇÃO 5 COD.OPERADOR 1	
0472	MSG_RESTXT	Texto resposta	45	A		Texto preenchido pela SIBS numa mensagem recusada, com os textos que justificam a recusa para o cliente.	
0492	MSG_RESCOD	Código de resposta da mensagem da SIBS	3	N		Código de resposta da mensagem de sessão Banco ->SIBS. (= 000 - operação aprovada) (> 000 - operação recusada) Normalmente os dois dígitos da direita identificam o código do erro.	
0493	MSG_NOKTIP	Código de recusa da mensagem pela SIBS	8	A		Código da recusa da SIBS a uma mensagem na sessão Banco -> SIBS. (este campo é normalmente preenchido com o modulo do erro, quando existe um erro na mensagem (campo 0492 > 0)).	
0505	CAR_PANN03	PAN do cartão	16	N		Número completo do cartão bancário (*Primary Account Number*), como se apresenta em embossed. (corresponde a parte do atributo A056 dos POS)	
0637	CAR_EXPDAT	Data de expiração do cartão expandida	6	N	AAAAMM	Último mês e ano em que o cartão ainda é válido.	
1350	CAR_MBNCOD	Código de cartão associado ao serviço	1	N		Este campo indica o tipo de cartão utilizado nas operações de adesão, consulta, alterações e cancelamentos para o MB NET.	1 - cartão *not-on-us* 2 - cartão *on-us*

N.º	Sigla do Campo	Nome do campo	Comp.	Rep.	Formato	Descrição	Valores
1368	SPI_3DSMNT	Montante da compra enviado pelo comerciante	12	N	Sem decimais	Montante da compra enviado pelo comerciante no âmbito do sistema 3D Secure.	Exemplo: Montante: €125.45 Representação:12545
1369	SPI_DCMMOEN01	Casas decimais da moeda	2	N		Indicação da unidade mínima aceite por moeda, de acordo com a norma ISO 4217. Por exemplo, o dólar americano tem o valor 2; o iene tem o valor 0.	
1709	LOG_SIS	Sistema do *log* associado à transação	2	A		Código utilizado nas mensagens e nos registos de detalhe correspondentes a cada operação e que indica ao Banco qual o subsistema transacional em que esta se realizou. Corresponde à versão expandida do campo (0312) SIS_APLPDD. Este campo pode não estar preenchido (espaços) em registos gerados na Compensação MULTIBANCO, resultantes do apuramento de valores agregados, para os quais não é criado um registo no ficheiro de log da SIBS FPS.	21 31 22 32 26 36 27 37 28 38 2F 3F 2G 3G 2H 3H
2300	SIS_TARSIB	Código da rubrica do Tarifário da SIBS FPS	2	A		Apresenta o código da rubrica do Tarifário da SIBS FPS. Permite ao Banco atualizar totalizadores para poder auditar a fatura da SIBS FPS no fim do mês.	
2483	MSG_ACCCOD	Código de gestão da mensagem	1	A		Código que determina a ação que a mensagem desenvolve.	1 - Inserção 2 - Consulta 3 - Alteração 4 - Abate 5 - Confirmação 6 - Alteração Método

N.º	Sigla do Campo	Nome do campo	Comp.	Rep.	Formato	Descrição	Valores
							Autenticação 7-Insere adiantamento 8-Altera-adiantamento 9-Abate-adiantamento
3257	SIS_TIMSTP	Timestamp atualização DB2	26	A		Indica o timestamp de atualização do DB2. Formato AAAA-MM-DD-HH.mm.SS.UUUUUU, onde AAAA - ano MM - mês DD - dia HH - hora mm - minuto SS - segundo UUUUUU - microssegundo	
3974	EXT_TELNUM	Número de telefone	9	N		Telefone de contacto do cliente do serviço. Na caracterização *Acquirer* corresponde a telefone de contacto para efeito de fraude/segurança.	
4247	SIS_INIDAT	Data de início	8	N	AAAAMMDD	É a data a partir da qual a informação entra em vigor. No SDD corresponde à data de inscrição da entidade ou ADC no SDD.	
4319	CHV_HAS	*Secure hash*	40	A		*Secure hash.*	
5325	CAR_EXPDATN01	Data de expiração do cartão	6	N	AAAAMM	Último mês e ano em que o cartão ainda é válido (zona 18 - Norma ISO 4909).	
6799	SIS_SIT3DS	Situação do 3D Secure	1	N		Indica a situação do serviço 3D Secure associado ao cartão.	0 - *Promotion*; 1 - Normal; 2 - Inibido por código errado; 9 - Cancelado.
6800	SIS_SITDAT_3DS	Data situação do 3D Secure	8	N		Apresenta a data em que a situação indicada para o 3D Secure foi posicionada.	
6803	SIS_RETIND	Indicador reset password	1	N		Indica se é para efetuar reset à password.	0 - Não 1 - Sim

N.º	Sigla do Campo	Nome do campo	Comp.	Rep.	Formato	Descrição	Valores
6868	CAR_TENCHV	Indica o número de tentativas falhadas	1	N		Indica o número de tentativas falhadas.	
6869	CAR_RETCHV	Número de reset permitidos ao código de acesso	1	N		Indica o número de reset efetuados ao código acesso.	
6876	CAR_ATT3DS	Modo de autenticação 3D Secure/MB NET	1	N		Campo que identifica o modo de autenticação 3D SECURE/MB NET (o correspondente ao TRM_ATT3DS). Nota: No MB NET o SMS pressupõem a existência também da *password*.	1 - SMS; 2 - MB CODE.
8106	EXT_TLMNUMN03	Número de telemóvel	11	N		Identifica o número de telemóvel	
8200	EXT_TLMPRX	Prefixo de telemóvel	7	N		Prefixo de telemóvel para números nacionais e internacionais.	
8572	BIN_ATTFRE	Autenticação Forte	1	N		No caso do método de autenticação ser SMS, este atributo indica se, para além do SMS é obrigatória a utilização da password estática para autenticar o cliente.	0 – Sem Password; 1 – Password Obrigatória.
8622	SIS_LRGCTA	"*Large Account*" de envio de SMS	1	N		Indica qual a *"Large Account"* a usar para o envio de SMS. Permite ao Banco auditar a fatura da SIBS ou do seu Operador de telecomunicações relativamente aos SMS enviados.	0 - Não aplicável 1 - SIBS 2 - Emissor
8623	SIS_SMSQTD	Quantidade de SMS	2	N		Indica a quantidade de SMS enviados. Permite ao Banco atualizar totalizadores para poder auditar a fatura da SIBS FPS ou do seu Operador de telecomunicações.	

6 Perguntas frequentes

1. Qual vai ser o modelo a seguir relativamente ao contacto de telemóvel para uso da OTP?

a) É definido pelo Cliente, somente no momento do *enrollment,* e enviado à SIBS FPS o número do telemóvel, que o guarda (informação estática)?

b) Ou em cada transação 3D Secure os Emissores enviarão o número de telemóvel atual do Cliente, registado na sua base de dados?

Resposta: O serviço está preparado para ser utilizado com o número de telemóvel parqueado na SIBS FPS. O posicionamento do número de telemóvel é assegurado no momento da adesão mas pode ser atualizado através de uma mensagem *Host-to-Host* de gestão do serviço.

2. De que forma o Titular do cartão é informado para que telemóvel está a ser efetuado o envio do SMS no momento da compra? Existe risco de desatualização da base de dados de cartão?

Resposta: Na página de recolha da OTP, é indicado o número de telemóvel para onde é enviado o SMS. Esta indicação é efetuada através dos últimos dígitos do número de telemóvel.

3. O uso do *e-mail* (que também tem certificação por parte do Emissor na sua introdução nas bases de dados) pode ser utilizado para o envio da OTP?

Resposta: O Gabinete de Segurança da SIBS FPS desaconselhou a utilização do *e-mail* para operações relacionadas com a segurança noutras ocasiões. Contudo, fica em aberto a análise desta possibilidade no decorrer da fase 2 do projeto.

4. A generalidade dos Emissores indicou que pondera a autenticação somente com a OTP enviada por SMS. No entanto, existiam algumas dúvidas sobre se o Regulador aceitará a OTP por SMS como autenticação forte. O Regulador já se pronunciou sobre o assunto?

Resposta: A oferta disponível possibilita aos Emissores que assim o entendam, associarem ao envio de OTP por SMS a uma *password* estática definida pelos Titulares de cartão. A SIBS FPS não tem qualquer informação sobre a posição do Regulador nesta matéria.

5. O que acontece ao serviço quando é efetuada a renovação ou substituição de um cartão aderente ao serviço?

Resposta: Nos processos de emissão de um cartão, sempre que há indicação por parte do Emissor do cartão a substituir ou a renovar e esse cartão tem uma adesão com o estado “normal”, o serviço migra para o novo cartão, independentemente de ser uma renovação ou substituição.

Caso o método de autenticação seja o MB CODE deve-se garantir que o novo cartão tem a aplicação SAF ativa no *chip*.

6. Sobre o envio de OTP (SMS) e sobre a utilização de uma *large account number* do Emissor.

a) Qual o custo que a SIBS cobra pelo envio dos SMS?

b) Por outro lado gostaríamos que nos informassem o que será necessário para que a SIBS passe a usar a nossa *large account number*: Alguma autorização expressa da nossa parte junto da operadora?

c) Os Emissores terão de realizar desenvolvimentos para que seja utilizada a sua *large account*?

Resposta: A SIBS tem uma rubrica de tarifário identificada para o envio de SMS (Z 8 1). Está um processo de negociação em curso com os operadores de telecomunicações que visa a redução do valor dos SMS enviados pela SIBS FPS.

Caso seja utilizada a *large account* do Emissor, este terá de autorizar, junto do operador, o envio de SMS por parte da SIBS FPS.

A SIBS FPS aguarda ainda a confirmação dos operadores de comunicações sobre se existe necessidade de adaptação de interfaces técnicos pelos Emissores.

7. Existem requisitos de formato em relação ao SMS a ser enviado?

Resposta: O texto dos SMS pode ser definido por cada Emissor. Esta definição pode ser feita para todos os cartões ou por BIN+EXT. Caso o Emissor não tenha definido o *template* para os SMS a enviar aos seus Clientes, será utilizado um texto "*default*". A composição do texto dos SMS tem um conjunto de 3 *placeholders* que é recomendável colocar no SMS. Um dos *placeholders* diz respeito ao OTP gerado e é por isso obrigatório.

8. O Emissor tem Clientes com números de telemóvel não portugueses. A solução da SIBS FPS está preparada enviar números de telemóvel internacionais?

Resposta: Com a evolução descrita nesta *Release Documentation*, os interfaces técnicos entre a SIBS FPS e os Emissores (mensagens *Host-to-Host*) foram alterados para suportarem números de telefone internacionais.

9. Quando o Cliente define no momento da adesão os dados para o 3D Secure, pode escolher mais do que um cartão para o mesmo serviço?

Resposta: A adesão ao 3D Secure é efetuada para cada cartão de pagamento (cartão cujos dados são indicados ao comerciante para efetuar o pagamento). Assim, se o titular do cartão usar 3 cartões distintos para efetuar pagamentos na internet, deverá aderir com os 3 cartões individualmente.

10. É possível que um cartão aderente ao 3D Secure esteja a transacionar com o método de autenticação MB CODE e a OTP ser gerada com recurso a outro cartão do mesmo titular? A geração do OTP tem que ser efetuada com o cartão que está associado ao 3D Secure?

Resposta: Se o método de autenticação pretendido for o MB CODE, na adesão (nos campos CAR_EXPDATN01 e CAR_PANN03 assinalados com a nota E) na mensagem H472 deverá ser indicada a data de expiração e o número do cartão com a aplicação EMV-CAP/MB CODE que deve ser usado com o *hardware-token* para gerar o OTP (o cartão com a aplicação EMV-CAP, pode ou não corresponder ao cartão de pagamento). O mesmo cartão com a aplicação EMV-CAP para a geração de OTP com o MB CODE pode ser associado a mais do que um cartão de pagamento.

Considerem-se os seguintes exemplos:

Exemplo1:

O cliente tem 2 cartões com os quais pretende fazer pagamentos na internet e aderir ao Serviço 3D Secure com método de autenticação MB CODE para ambos. No entanto apenas um dos dois cartões tem a aplicação EMV-CAP/MB CODE, e pretende usar sempre esse cartão com o *hardware-token* para gerar os OTP de autenticação das compras. Neste caso têm de ser enviadas duas mensagens H472 com os campos (0505) CAR_PANN03, (0637) CAR_EXPDAT, (0261) BIN_NUM, (0319) BIN_EXN e (0128) CAR_NUM preenchidos com os dados de cada um dos cartões e com os campos (0505) CAR_PANN03 E) e (5325) CAR_EXPDATN01 E) de ambas as mensagens preenchidos com os dados do cartão que tem a aplicação EMV-CAP/MB CODE.

Exemplo2:

O cliente tem 2 cartões com os quais pretende fazer pagamentos na internet e aderir ao Serviço 3D Secure com método de autenticação SMS para ambos. Neste caso têm de ser enviadas duas mensagens H472 com os campos (0505) CAR_PANN03, (0637) CAR_EXPDAT, (0261) BIN_NUM, (0319) BIN_EXN e (0128) CAR_NUM preenchidos com os dados de cada um dos cartões de pagamento e com os campos (8200) EXT_TLMPRX e (8106) EXT_TLMNUM03 de ambas as mensagens preenchidos com o número de telemóvel do cliente. Os campos (0505) CAR_PANN03 e (5325) CAR_EXPDATN01 identificados com a nota E) não devem ser posicionados (em conformidade com as regras de preenchimento indicadas na nota E).