Release Documentation

Processamento para Emissores

3D Secure para Cartões Reais

Emissores

Versão: 01.00

Data: 2012-12-21

Estado: Final

Classificação: Restrito

Referência: DCSIBS120461

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:	DCSIBS120461
Título do Documento:	3D Secure para Cartões Reais
Versão:	01.00
Estado:	Final
Classificação:	Restrito
Tipo de Documento:	Release Documentation
Área Funcional Responsável:	AF Desenvolvimento de Serviços

Documentos Relacionados

Referência	Título	Origem
DCSIBS110139	Manual do Serviço - Processamento para Emissores V1.10	AF Desenvolvimento de Serviços
DCSIBS100026	Manual de Implementação - Serviços para Emissores – Emissores V02.20	AF Desenvolvimento de Serviços
DCSIBS120049	Formulário de Caracterização do BIN V01.20	AF Desenvolvimento de Serviços

Revisões

Versão	Data	Descrição	Autor
01.00	2012-12-21	Criação do documento	AF Desenvolvimento de Serviços

Índice

Índice de Figuras

Índice de Tabelas

1 Introdução

O Serviço de Processamento para Emissores da SIBS FPS actualmente permite aos Emissores a aceitação e processamento das transacções de pagamento efectuadas com cartão de marca internacional em Comerciantes com *site* na *internet*.

As operações de pagamento na *internet* tratam-se de transacções e-*commerce* em ambiente *card-not-present*, onde são transmitidos dados de cartão ao Comerciante sem um controlo efectivo por parte do Titular do Cartão do tratamento dado a esta informação. Estas operações correspondem a transacções com maior propensão à fraude devido à grande dispersão de dados dos cartões pelos diversos intervenientes nas transacções, e nem sempre com as medidas de segurança adequadas.

De acordo com as estatísticas relativas a comércio electrónico, os pagamentos na *internet* atingem taxas de crescimento na ordem dos 40%[1] principalmente devido à comodidade e simplicidade deste tipo de pagamento mas em grande parte devido ao crescimento do uso de dispositivos móveis ligados à *internet (smartphones, tablets)*. Por este motivo, a definição e implementação de mecanismos que permitam fortalecer a segurança dos pagamentos *online* ganha importância redobrada. Estudos revelam que as preocupações de segurança representam o primeiro entrave às compras *online* para 73% dos detentores de cartão[2].

Acompanhando a evolução dos pagamentos *online* e dando especial enfoco na segurança das transacções, a SIBS FPS passa a disponibilizar aos Emissores um *Access Control Server* (ACS) para cartões reais complementando a actual oferta de soluções 3D Secure já existente com o serviço do MB NET e na vertente de *Acquiring* com o serviço de TPA Virtual.

O protocolo 3D Secure oferece aos intervenientes de um pagamento *online* um nível adicional de segurança, mesmo em cartões de débito, desde que todas as partes – o Cartão, o Titular do Cartão e o Comerciante – sejam aderentes ao protocolo 3D Secure, resultando num acréscimo de confiança dos utilizadores neste tipo de pagamentos e numa diminuição dos custos relativos ao tratamento de situações de fraude e de disputas intimamente relacionadas com situações em que o Titular do Cartão não reconhece a transacção efectuada[3]. A título informativo, uma das marcas internacionais previu com o lançamento do programa a redução em 80%[4] do número de *chargebacks* relativos com operações *e-commerce*.

[1] Informação disponibilizada na documentação da MasterCard (MasterCard SecureCode – *Issuer Implementation Guide* – 01 Dez 2011

[2] MasterCard International Consumer Segmentation Research, Q4 2002

[3] Mais de 70% dos *chargebacks* registados na marca MasterCard relacionados com *e-commerce* resultam dos códigos 4837 (*No cardholder authorization*) ou 4863 (*Cardholder not recognized*)

[4] Benefício para os membros referido no documento 3-D Secure – *Introduction* (70001-01)

A solução 3D Secure para Emissores (ACS de cartões reais), implementada pela SIBS FPS, contempla três *schemes* – VISA, MasterCard e AMEX[5] – e, embora assuma designações diferentes para cada uma das marcas internacionais, o protocolo 3D Secure tem implementações semelhantes:

- Na VISA, o 3D Secure é denominado *Verified by Visa*;
- Na MasterCard, o 3D Secure é denominado *SecureCode*;
- Na AMEX, o 3D Secure é denominado *SafeKey*.

O ACS agora disponibilizado pela SIBS FPS prevê também a aplicação do protocolo 3D Secure a operações *e-commerce* efectuadas com cartões Maestro, cabendo ao Emissor definir se estes cartões são passíveis de aderirem ao protocolo 3D Secure, uma vez que está prevista pela MasterCard[6] a aceitação destes cartões em transacções na *internet*.

Tradicionalmente, no mercado português, os cartões Maestro não eram personalizados com o *card security code*[7] sendo frequente que os Emissores não permitissem a sua utilização em transacções *e-commerce*. Com a certificação dos BINs dos cartões Maestro nos programa SecureCode e com a adesão ao serviço ACS da SIBS FPS, os Emissores destes cartões passam a poder permitir a utilização destes cartões para a realização de pagamentos na *internet*

[5] Em processo de certificação do *Safekey* AMEX. Será comunicada atempadamente a data de entrada em produção.

[6] A MasterCard divulgou, através dos Operation Bulletin nº4 (1 Abril de 2010) e nº 10 (1 Outubro 2010), a obrigatoriedade dos cartões Maestro passarem a ser aceites em transacções e-commerce a partir de 15 de Abril de 2011.

[7] CVC2 – Card Verification code para a MasterCard, CVV2 – Card Verification Value para a VISA

2 Descrição de Evolução

O ACS implementado pela SIBS FPS passa a processar operações de autenticação efectuadas na *internet* com cartões reais aderentes ao protocolo 3D Secure de um dos três Sistemas de Pagamento Internacional (SPI); com garantias acrescidas de segurança para os Titulares do Cartão e para os Emissores. No momento da compra com cartão, e antes de ser autorizada a transacção, são efectuadas duas validações adicionais às verificações[8] já existentes para este tipo de operação:

- Autenticação do Cartão - Esta validação é efectuada pelo SPI que valida se o BIN do cartão está registado nos seus sistemas (Directory Server) como aderente ao protocolo 3D Secure;
- Autenticação do Titular do Cartão – Esta validação é efectuada pela solução de ACS do cartão e permite autenticar o Titular do Cartão através do método de autenticação que o mesmo escolheu no momento da adesão ao protocolo 3D Secure. Desta forma, é assegurado que a compra é efectivamente realizada pelo Titular do Cartão.

Durante o processo de autenticação é gerado, pelo ACS um código de segurança – CAVV/AAV/EAVV[9] que é determinante na decisão da operação no processo de autorização da transacção. O CAVV/AAV/EAVV gerado pelo ACS é enviado ao Comerciante na mensagem de resposta à autenticação, com a indicação do resultado do processo de acordo com a codificação específica de cada uma das marcas internacionais. O Comerciante por sua vez deve interpretar o resultado da autenticação efectuada e decidir sobre o prosseguimento a dar à transacção de acordo com regras de risco por si definidas. Caso o Comerciante decida prosseguir com a compra, deve incluir o CAVV/AAV/EAVV na mensagem de autorização.

Na autorização das operações *e-commerce* efectuadas com cartões 3D Secure, procede-se à validação da integridade e correspondência do CAVV/AAV/EAVV gerado no momento da autenticação e o valor enviado pelo Comerciante na mensagem de pedido de autorização da transacção[10]. É ainda verificada a validade da autenticação efectuada, seguindo-se as recomendações da MasterCard na implementação das melhores práticas do protocolo 3D Secure. Caso o sistema detecte que existe um desfasamento superior a 30 dias decorridos entre a autenticação e a autorização, a operação é rejeitada e o Comerciante deve submeter uma nova autenticação 3D Secure.

A autorização da operação pode depois ser efectuada quer em cenário de real-time (em que o Emissor decide a autorização da operação em tempo real), quer num cenário alternativo em que a decisão é delegada pelo Emissor na SIBS FPS.

---

[8] No processo de autenticação de uma compra é validado se: o cartão existe na base de dados da SIBS FPS, a data de expiração, se o CVV2 está correcto, a situação do cartão, se a operação está autorizada para o cartão, entre outras validações. Para melhor detalhe desta validação consultar o Manual do Serviço do Processamento para Emissores.

[9] VISA – CAVV; MasterCard – AAV; AMEX - EAVV

[10] A SIBS no serviço para Emissores prevê a possibilidade de autorizar transacções com cartões *on-us*, mesmo quando o Emissor utiliza um ACS distinto da solução disponibilizada pela SIBS FPS.

Os Emissores que adiram à solução ACS de cartões reais da SIBS têm os seguintes impactos operacionais e técnicos:

- Aderir ao ACS de cartões reais da SIBS de acordo com o processo de adesão descrito na secção 3.1;
- Efectuar o enroll dos BINs aderentes ao serviço, junto dos Sistemas de Pagamento Internacionais (SPI).
- Informar os Titulares dos Cartões cujo(s) BIN(s) estão registados nos SPIs como 3DS, que devem aderir ao protocolo 3D Secure caso pretendam efectuar compras seguras na *internet* com o seu cartão.
- Implementar um conjunto de mensagens H2H que permitirá efectuar a adesão e a gestão do Titular do Cartão ao serviço 3DS:
    - A adesão do Titular do Cartão pode ser efectuada através dos canais disponibilizados pelo Emissor com a implementação da mensagem H472 – S472 – Adesão 3D Secure. Como alternativa a esta implementação a operação de adesão está também disponível através do Portal de Serviços SIBS (PSS);
    - Para consulta e manutenção da solução 3D Secure, o Emissor deve implementar as seguintes mensagens *Host-to-Host:*
        - H473 – S473 - Consulta 3D Secure;
        - H474 – S474 - Manutenção do 3D Secure.

      Como alternativa à implementação destas mensagens, estas operações estarão também disponíveis através do Portal de Serviços SIBS (PSS);
- Implementar os dados adicionais do registo Tipo 1 do Ficheiro de Destinos (DST5) quando o campo (0699) SIS_OPRTIP ("Código de Transacção Expandido") assume os valores:
    - 1E7 – Adesão ao serviço 3D Secure;
    - 2E7 - Consulta ao serviço 3D Secure;
    - 3E7 - Alteração *Password* ao serviço 3D Secure;
    - 4E7 – *Reset Password* ao serviço 3D Secure;
    - 5E7 - Alteração telemóvel ao serviço 3D Secure;
    - 6E7 - Alteração do cartão e data expiração associada ao serviço 3D Secure;
    - 7E7 - Alteração ao método de autenticação (troca de método);
    - 8E7 - Cancelamento ao serviço 3D Secure;
    - 9E7 – Autenticação.

O Emissor deve ainda ter presente que quando um cartão é aderente ao protocolo 3D Secure:

- Sempre que haja uma renovação, por data de expiração, o novo cartão mantem a adesão ao protocolo 3D Secure.
- No caso de situações de colocação de cartões em lista negra, não será possível efectuar a adesão ao protocolo 3D Secure, e no caso dos cartões que tenham o serviço activo o mesmo será automaticamente cancelado.

2.1 Modelo Operativo

O modelo operativo para a realização de uma transacção e-*commerce* com cartões 3D Secure em Comerciantes 3D Secure, considerando que o portador de cartão aderiu ao serviço, consiste nos seguintes passos:

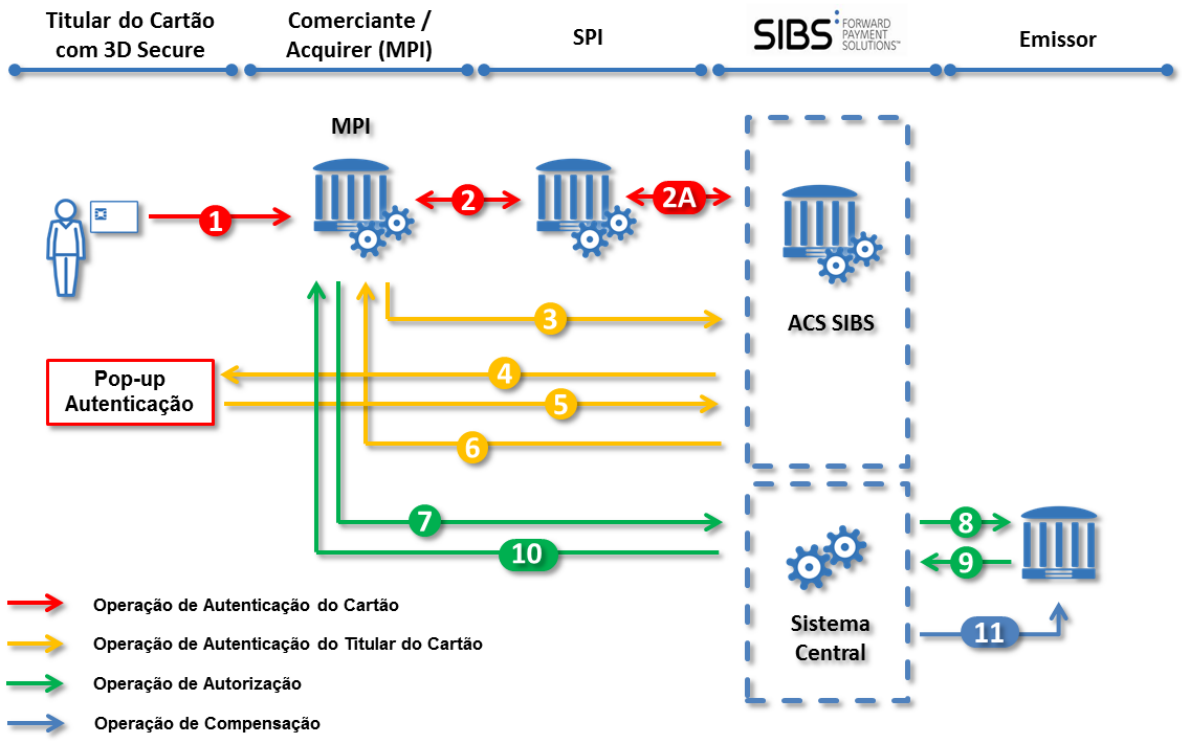

Figura 1 - Processo de compra 3D Secure

1. O Titular do Cartão 3D Secure introduz os dados de cartão (número de cartão, data de expiração e CSC[11]) no *website* do Comerciante 3D Secure;
2. O Comerciante, através da componente da sua solução de e-commerce certificada pelas marcas internacionais (MPI), envia estes dados ao SPI que valida se o BIN do cartão está registado no protocolo 3D Secure. Caso o BIN do cartão esteja registado no protocolo 3D Secure o SPI envia o URL do ACS onde é efectuada a autenticação do Titular do Cartão. Caso o Emissor não tenha efectuado o registo do BIN junto do SPI, o comerciante receberá a indicação que o mesmo não é participante no protocolo;
3. O MPI invoca, através do URL informado pelo SPI, um pedido de autenticação do Titular do Cartão ao ACS da SIBS FPS (que actua em nome do Emissor);

[11] CSC – Card Security Code.

4. O Comerciante apresenta ao Cliente (através de *pop-up* ou *i-frame*) um formulário disponibilizado pelo ACS[12] onde o Titular do Cartão se autentica com as credenciais definidas durante o processo de adesão ao 3D-Secure[13].

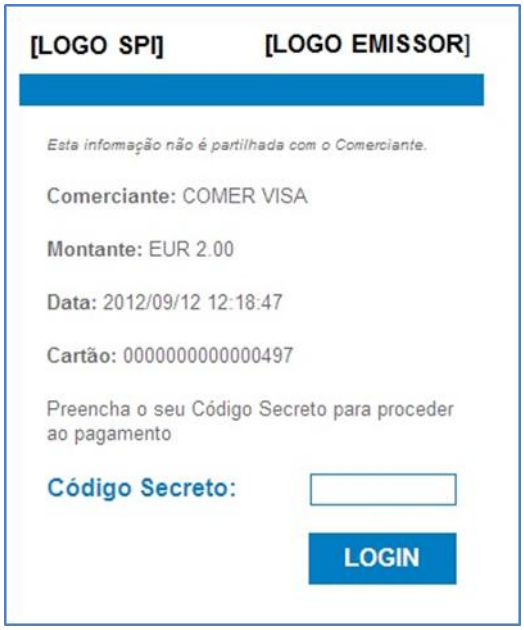

Figura 2 – Exemplo de um formulário de autenticação do Titular do Cartão - *Pop-up* 3D Secure

5. O ACS valida a autenticação do Titular do Cartão de acordo com o método escolhido no momento da adesão;
6. O resultado da autenticação é devolvido ao Comerciante;
7. O Comerciante interpreta o resultado da autenticação e decide sobre o seguimento a dar à transacção de acordo com regras de risco por si definidas, submetendo se assim o entender um pedido de autorização;
8. Caso a transacção seja feita com cartões *on-us* e em *real-time* com o Emissor, a SIBS FPS envia o pedido de autorização ao Emissor. No caso de não existir real-time, é realizada a decisão mediante os parâmetros posicionados pelo Emissor.;
9. A SIBS FPS recebe do Emissor a decisão de autorização se o cenário de autorização seleccionado for *real-time* ou decide mediante os parâmetros posicionados pelo Emissor para o cenário de autorização a utilizar;
10. A SIBS FPS envia decisão da autorização da transacção para o Comerciante/*Acquirer*;
11. Em processo de final de dia, o Emissor recebe, via Ficheiro de Destinos as operações de autenticação e autorização efectuadas para os seus cartões (detalhadas com a indicação do canal em que foram realizadas).

[12] A informação recolhida neste formulário não se encontra disponível para o Comerciante.
[13] Na solução disponibilizada pela SIBS FPS só está disponível a autenticação por *password*;

3 Processo de Adesão

3.1 Adesão do Emissor

Para aderir à solução ACS para cartões reais da SIBS, o Emissor deve efectuar os seguintes passos:

- Abrir um projecto com o SPI para certificar os BINs que serão aderentes ao protocolo 3D Secure. Esta certificação terá que ser efectuada de modo independente para cada um dos SPI (VISA, MasterCard e AMEX) e irá certificar pelo menos um BIN como aderente ao 3DS. A abertura deste projecto junto dos SPI poderá ter custos associados, que terão que ser confirmados pelos Emissores junto das Marcas;
- Solicitar junto da SIBS FPS a abertura de um Projecto de Adesão e Alteração de Serviços (PAAS) contactando para o efeito o respectivo gestor de relação. Com a abertura do PAAS junto da SIBS FPS, são definidos os calendários de implementação e testes;
- Enviar para a Área de Regularização da SIBS FPS (através do e-mail regularizacoes@sibs.pt) o formulário de "Caracterização do BIN" devidamente preenchido com indicação que pretende a a adesão ao serviço 3D Secure para os seus BINs, e definir quais os métodos de autenticação que pretende que estejam associados a esse mesmo BIN;

  Ao preencher o formulário "Caracterização do BIN" deve ter em atenção os seguintes aspectos:
  - O tratamento de transacções com cartões 3D Secure é independente do que está posicionado, na caracterização de BIN para a aceitação de transacções MO/TO, ou seja, se o Emissor posicionar na caracterização de BIN o parâmetro de adesão ao serviço 3D Secure como "SIM", e o parâmetro de "NÃO aceitação de transacções card-not-present (sem pin)", só serão aceites transacções 3DSecure (autenticadas pelo cardholder) na *internet* em Comerciantes 3D Secure.

Acção' (I,A,E)	5. 3D SECURE
(n.a.)	5.1 Aderente ao serviço
(n.a.)	5.2 Tentativas antes do bloqueio (introduza um valor de 1 a 9)
(n.a.)	5.3 Resets ao Código de Acesso (introduza um valor de 1 a 9)
(n.a.)	5.4 Autenticação por *Password*
(n.a.)	5.5 Autenticação por SMS
(n.a.)	5.6 Autenticação por MB CODE

- Implementar as novas mensagens *Host-to-Host*, conforme descrito nas especificações técnicas apresentadas na secção 5.1 **-** Mensagens *Host-to-Host*, caso pretenda a integração da funcionalidade com os seus sistemas. Em alternativa o Emissor pode optar por uma gestão do serviço recorrendo às mesmas funcionalidades que se encontram disponíveis através do Portal de Serviços SIBS (secção 4 - Manual de Utilizador);
- Assegurar a capacidade de processar os dados adicionais no registo do Tipo 1 do Ficheiro de Destinos (DST5), assim como novos códigos de operações descritos em 5.2.1 - Dados Adicionais do Ficheiro de Destinos (DST5).

3.2 Adesão do Titular do Cartão

Os Titulares dos Cartões com BIN 3D Secure devem aderir ao protocolo 3D Secure caso pretendam efectuar compras seguras na *internet* com o seu cartão. Na adesão, o Titular do Cartão deve indicar um dos três métodos de autenticação disponíveis[14]. Este método será utilizado aquando da compra *online* para autenticar o Titular do Cartão.

Existem três métodos de autenticação possíveis: por *password*, por SMS ou por MB CODE. Na primeira fase de disponibilização da Solução 3D Secure da SIBS FPS, o único método de autenticação disponível é a autenticação por *password.*

[14] As formas de adesão e autenticação dos titulares dos cartões são definidas pelos respectivos Emissores, não sendo obrigatório os Emissores disponibilizarem todos os métodos de autenticação identificados pela SIBS FPS.

A adesão do Titular do Cartão é efectuada de acordo com os canais que o Emissor coloca à disposição dos seus Clientes. A SIBS FPS possibilita a integração com os sistemas do Emissor (sistemas internos, *homebanking*, *mobile banking*, etc…) através da implementação da mensagem H472 – S472 – Adesão 3D Secure e disponibiliza a funcionalidade também através do Portal de Serviços SIBS (PSS).

4 Manual de Utilizador

4.1 Descrição das Funcionalidades

As funcionalidades 3D Secure disponíveis no PSS incluem: a adesão ao 3D Secure, a consulta de dados do cartão, a alteração de credenciais de acesso do Titular do Cartão, a alteração do método de autenticação do Titular do Cartão, o *reset* da inibição do cartão e o cancelamento do 3D Secure no cartão.

4.1.1 Adesão 3D Secure

A funcionalidade Adesão ao 3D Secure permite ao Titular de um Cartão aderir com o seu cartão ao protocolo 3D Secure seleccionando um dos três métodos de autenticação. Na primeira fase de disponibilização da Solução 3D Secure, o único método disponível é o de *password,* contudo este documento descreve os outros dois métodos que estão previstos disponibilizar brevemente.

O acesso à funcionalidade "Adesão ao 3D Secure" está disponível através dos seguintes menus do PSS: "Cartões → 3D Secure → Consultar Cartão → Consultar Dados Cartão".

Figura 3 – Consulta Dados do Cartão – botão para acesso ao ecrã de Adesão ao 3D Secure

Carregando no botão "Adesão 3D Secure" é apresentado o seguinte ecrã que permite a adesão.

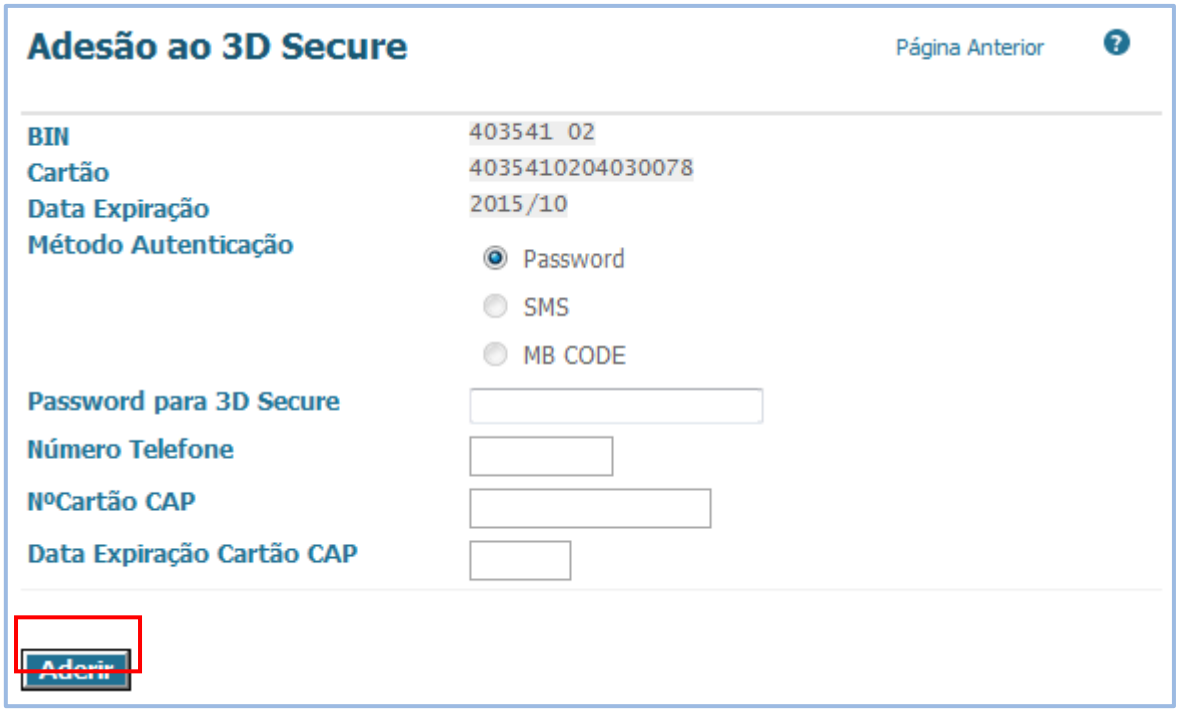

Figura 4 – Adesão ao 3D Secure

Este ecrã é composto pelas seguintes informações ou parâmetros:

- BIN - corresponde ao número do identificativo BIN, mais a sua extensão;
- Cartão - corresponde número completo constante do cartão;
- Data Expiração - corresponde à data de expiração constante no cartão (AAAAMM).
- Método Autenticação - corresponde ao tipo de autenticação pretendido (*Password* ou SMS ou MB CODE);

  Os métodos de autenticação são mutuamente exclusivos, só podendo ser escolhido um.

  - Ao escolher a opção '*Password*', deve preencher o campo '*Password* para 3D Secure' com 6 a 20 caracteres alfanuméricos, enquanto os campos 'Número Telefone', 'Nº Cartão CAP' e 'Data Expiração' devem ficar vazios.
  - Ao escolher a opção 'SMS', deve preencher o campo 'Número Telefone' enquanto os campos '*Password*', 'Nº Cartão CAP' e 'Data Expiração' devem ficar vazios.
  - Ao escolher a opção 'MB CODE', deve preencher os campos 'Nº Cartão CAP' e 'Data Expiração Cartão CAP', enquanto os campos '*Password'* e 'Número Telefone' devem ficar vazios.

Uma vez escolhida a autenticação desejada e preenchidos os campos necessários, prima o botão 'Aderir' para aceder ao ecrã final de adesão.

Após carregar no botão 'Aderir', obtém-se o seguinte ecrã.

Figura 5 – Adesão ao 3D Secure - Operação concluída com sucesso

4.1.2 Consulta 3D Secure

A funcionalidade Consulta 3D Secure permite ao Titular do Cartão o acesso às informações relativas ao serviço de um cartão previamente inscrito no 3D Secure.

Figura 6 – Consulta Dados de Identificação de Cartão - Ecrã de *Input*

Para identificar o cartão cuja informação se pretende consultar, deverão ser indicados:

- BIN - corresponde ao número de identificativo BIN do cartão, mais a sua extensão;
- Cartão - corresponde ao número do cartão, mais a sua extensão;
- Data Expiração - corresponde à data de expiração constante no cartão (AAAAMM).

Após o preenchimento dos campos acima descritos, prima 'Consultar' para aceder aos dados do cartão, sendo gerado o seguinte ecrã de *output*, e permitindo o acesso às funcionalidades identificadas na seguinte figura.

Figura 7 – Consultar 3D Secure

Como resultado da consulta, são apresentadas as seguintes informações:

- Situação - situação do cartão 3D Secure;
- Data Situação – data da última actualização da situação do cartão;
- BIN - identificativo BIN e a sua extensão;
- Cartão - número do cartão;
- Data Expiração - data de expiração do cartão;
- Data Adesão - data de adesão do cartão ao 3D Secure;
- Método Autenticação - método de autenticação escolhido (1 – *Password*, 2 – SMS, 3 – MB CODE);
- Número Telefone - número de telefone de contacto do Titular do Cartão, deve ser "0" caso o método de autenticação escolhido pelo Titular do Cartão não seja SMS;
- Nº Cartão CAP - número de cartão CAP em formato de 16 dígitos. Deve ser "0" caso o método de autenticação escolhido pelo Titular do Cartão não seja o MB CODE;
- Data Expiração Cartão CAP - data de expiração do cartão CAP, em formato AAAA MM. Mostra "0" caso o método de autenticação escolhido pelo Titular do Cartão não seja o MB CODE;
- Número Tentativas Chave Acesso - número de tentativas falhadas de inserção da chave de acesso 3D Secure;
- Nº *Reset* Chave Acesso - número de *resets* feitos à inibição de cartão após atingido o limite de tentativas de uso da chave de acesso;
- Data Última Alteração – apresenta a data da última alteração efectuada aos dados.

4.1.3 Manutenção 3D Secure

A partir do ecrã de Consulta 3D Secure é possível efectuar a gestão e alteração das credenciais de autenticação do cartão aderente ao 3D Secure.

O acesso à funcionalidade "Consulta 3D Secure" está disponível no PSS através dos seguintes menus:

"Cartões → 3D Secure → Consultar Cartão" → Consultar 3D Secure", ou;

"Cartões → 3D Secure → Consultar Cartão" → Consultar Dados Cartão → Consulta 3D Secure".

No ecrã de Consulta 3D Secure são facultadas opções para alterar a palavra-passe, número de telefone, número do cartão CAP, levantar a inibição do 3D Secure no cartão (caso o utilizador tenha excedido o número máximo de tentativas de palavra-passe) e cancelar o serviço.

4.1.3.1 Alterar *Password*

O acesso à funcionalidade de alteração de password está disponível no PSS em "Cartões → 3D Secure → Consultar Cartão → Consultar Dados Cartão → Consulta 3D Secure → Alterar *Password*", conforme apresentado na Figura 7 – Consultar 3D Secure.

Para alterar a *password* 3D Secure do cartão, deve premir o botão "Alterar *Password*".

Figura 8 – Alteração da *Password* do 3D Secure

Na alteração da *password* do 3D Secure é-lhe solicitado uma nova *password*, assim como confirmação da mesma.

Dados de *Input*:

- *Password* para 3D Secure Actual - correspondendo à *password* 3D Secure actual. Este campo não é obrigatório no entanto caso seja preenchido, terá de ser usada a *password* actual correcta;
- *Password* para 3D Secure Nova - correspondendo à nova *password* 3D Secure, introduzindo 6 a 20 caracteres alfanuméricos;
- *Password* para 3D Secure Nova Confirmação - correspondendo à confirmação da nova *password* 3D Secure.

Prima 'Alterar' para completar a alteração de *password.*

4.1.3.2 Alterar Número Telefone

A funcionalidade para autenticação por SMS não se encontra ainda disponível

O acesso à funcionalidade está disponível em *"Cartões → 3D Secure → Consultar Cartão → Consultar Dados Cartão → Consulta 3D Secure → Alterar Telefone"*, conforme apresentado na Figura 7 – Consultar 3D Secure.

4.1.3.3 Alterar Cartão CAP

A funcionalidade para autenticação por número de cartão CAP e data de expiração, não se encontra ainda disponível.

O acesso à funcionalidade está disponível em "Cartões → 3D Secure → Consultar Cartão → Consultar Dados Cartão → Consulta 3D Secure → Alterar Cartão CAP", conforme apresentado na Figura 7 – Consultar 3D Secure.

4.1.3.4 *Reset* Chave Acesso

Esta funcionalidade é executada em exclusivo pelo Emissor a pedido do Titular do Cartão e permite reabilitar a utilização do serviço após a inibição do serviço 3D Secure no cartão por excesso de tentativas de acesso com erro da *password*. A possibilidade de repor o estado do serviço está disponível recorrendo à opção *Reset* Chave Acesso (Figura 7 – Consultar 3D Secure).

O acesso à funcionalidade está disponível em "Cartões → 3D Secure → Consultar Cartão → Consultar Dados Cartão → Consulta 3D Secure → Reset Chave Acesso", conforme apresentado na Figura 7 – Consultar 3D Secure.

Figura 9 – Exemplo: Alteração ao 3D Secure

4.1.3.5 Cancelar

Esta funcionalidade permite o cancelamento do protocolo 3D Secure no cartão. Ao premir este botão, será apresentado um *pop-up* de confirmação da acção. Prima 'OK' para completar a acção, ou 'Cancelar' para anular a operação.

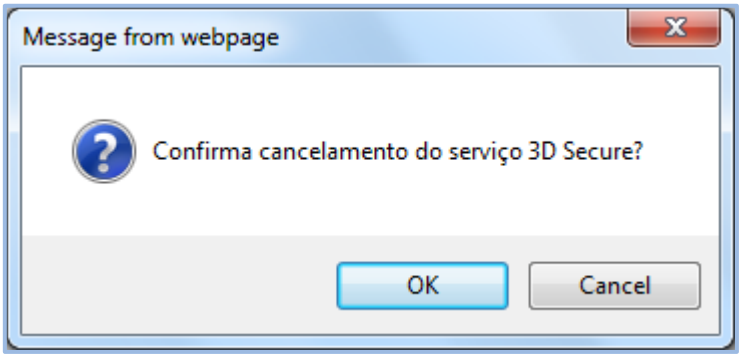

Figura 10 – *Pop-up* de confirmação de cancelamento 3D Secure

O acesso à funcionalidade está disponível em "Cartões → 3D Secure → Consultar Cartão → Consultar Dados Cartão → Consulta 3D Secure → Cancelar", conforme apresentado na Figura 7 – Consultar 3D Secure. O cancelamento do serviço não impede nem restringe que o titular do cartão possa voltar a aderir ao serviço através dos canais disponibilizados pelo Emissor.

5 Especificações Técnicas

5.1 Mensagens *Host-to-Host*

Os Emissores que pretendem integrar o serviço nos seus sistemas têm à sua disposição as seguintes mensagens *Host-to-Host*.

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

5.1.1 H472 - S472: Adesão ao 3D Secure

N.º Campo	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Validações/ Observações
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	
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/Hora da Transmissão	14	N	21	21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N	21	35	35	
0320	LOG_PERN01	Identificação do Período do Log Central	4	N	21	38	38	
0117	LOG_NUMN01	Número de Registo Log Central	8	N	21	42	38	
Detalhe								
1350	CAR_MBNCOD	Código de Cartão Associado ao Serviço	1	N	21	50	38	A)
0505	CAR_PANN03	PAN do Cartão	16	N	22	50	38	
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	38	50	38	
0261	BIN_NUM	BIN	6	N	44	50	38	
0319	BIN_EXN	Extensão de BIN	2	N	50	50	38	
0128	CAR_NUM	Número do Cartão	7	N	52	50	38	
6876	CAR_ATT3DS	Modo de Autenticação 3D Secure	1	N	59	50	38	B)
3974	EXT_TELNUM	Número de Telefone	9	N	60	50	38	C)
3286	CHV_HASRSA	*Hash* da Chave RSA	20	A	69	50	38	D), F)
0505	CAR_PANN03	PAN do Cartão	16	N	89	50	38	E)

N.º Campo	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Validações/ Observações
5325	CAR_EXPDATN01	Data de Expiração do Cartão	6	N	105	50	38	E)
4247	SIS_INIDAT	Data de Início	8	N	111	50	38	
0012	MSG_RESTIPA00	Código de Resposta	1	A	119	50	38	
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem pela SIBS	8	A	119	51	38	
0472	MSG_RESTXT	Texto Resposta	45	A	119	51	46	
0472	MSG_RESTXT	Texto Resposta	45	A	119	51	91	
		Total	**118**		**50**		**135**	

A) Por pré-definição só aceita o valor igual a '2 - cartão *On-Us'*

B) Se o método de autenticação for igual a:

1 – *Password*. O campo D) é obrigatório, mas deve estar cifrado[15]. Os restantes campos C) e E) devem estar a zeros;

2 – SMS. O campo C) é obrigatório. Os restantes campos D) e E) devem estar a zeros;

3 – MB CODE. Os campos E) são obrigatórios, mas o número do cartão CAP deve estar cifrado. Os restantes campos C) e D) devem estar a zeros.

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

5.1.2 H473 - S473: Consulta 3D Secure

N.º Campo	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Validações/ Observações
Header								
0470	CODMSG-BS	Código da Mensagem BS	4	A	1	1	1	
0002	VERMSG	Versão de Mensagem	2	N	5	5	5	
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/Hora da Transmissão	14	N	21	21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N	21	35	35	
1709	LOG_SIS	Sistema do Log Associado à Transacção (Novo Código Expandido)	2	N	21	38	38	

[15] A informação relativa ao algoritmo de cifra é disponibilizada aos Emissores no processo de Adesão e Implementação ao serviço.

N.º Campo	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Validações/ Observações
0320	LOG_PERN01	Identificação do Período do Log Central	4	N	21	40	38	
0117	LOG_NUMN01	Número de registo *log* central	8	N	21	44	38	
Detalhe								
1350	CAR_MBNCOD	Código de Cartão Associado ao Serviço	1	N	21	52	38	A)
0505	CAR_PANN03	PAN do Cartão	16	N	22	52	38	
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	38	52	38	
0261	BIN_NUM	BIN	6	N	44	52	38	
0319	BIN_EXN	Extensão de BIN	2	N	50	52	38	
0128	CAR_NUM	Número do Cartão	7	N	52	52	38	
4247	SIS_INIDAT	Data de Início	8	N	59	52	38	
6876	CAR_ATT3DS	Modo de Autenticação 3D Secure	1	N	59	60	38	
3974	EXT_TELNUM	Número de Telefone	9	N	59	61	38	
0505	CAR_PANN03	PAN do Cartão	16	N	59	70	38	
5325	CAR_EXPDATN01	Data de Expiração do Cartão	6	N	59	86	38	
6799	SIS_SIT3DS	Situação do 3D Secure	1	N	59	92	38	
6800	SIS_SITDAT_3DS	Data Situação do 3D Secure	8	N	59	93	38	
6868	CAR_TENCHV	Indica o Número de Tentativas Falhadas	1	N	59	101	38	
6869	CAR_RETCHV	Número *Reset Password*	1	N	59	102	38	
3257	SIS_TIMSTP	Timestamp Actualização DB2	26	A	59	103	38	
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A	59	129	38	
0472	MSG_RESTXT	Texto Resposta	45	A	59	129	46	
0472	MSG_RESTXT	Texto Resposta	45	A	59	129	91	
		Total	**118**		**50**		**135**	

A) Por pré-definição só aceita o valor igual a 2 - cartão *On-Us*.

5.1.3 H474 – S474: Manutenção do 3D Secure

N.º Campo	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Validações/ Observações
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	
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/Hora da Transmissão	14	N	21	21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N	21	35	35	
1709	LOG_SIS	Sistema do Log Associado à Transacção (Novo Código Expandido)	2	A	21	38	38	
0320	LOG_PERN01	Identificação do Período do Log Central	4	N	21	40	38	
0117	LOG_NUMN01	Número de Registo Log Central	8	N	21	44	38	
Detalhe								
1350	CAR_MBNCOD	Código de Cartão Associado ao Serviço	1	N	21	52	38	A)
0505	CAR_PANN03	PAN do Cartão	16	N	22	52	38	
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	38	52	38	
0261	BIN_NUM	BIN	6	N	44	52	38	
0319	BIN_EXN	Extensão de BIN	2	N	50	52	38	
0128	CAR_NUM	Número do Cartão	7	N	52	52	38	
4247	SIS_INIDAT	Data de Início	8	N	59	52	38	
6876	CAR_ATT3DS	Modo de Autenticação 3D Secure	1	N	67	52	38	B)
6876	CAR_ATT3DS	Modo de Autenticação 3D Secure (Novo)	1	N	68	52	38	H)
2483	MSG_ACCCOD	Código de Gestão da Mensagem	1	A	69	52	38	
6799	SIS_SIT3DS	Situação do 3D Secure	1	N	70	52	38	C)
6800	SIS_SITDAT_3DS	Data Situação do 3D Secure	8	N	71	52	38	C)
4319	CHV_HAS	*Secure Hash*	40	A	79	52	38	G)
4319	CHV_HAS	*Secure Hash (Novo)*	40	A	119	52	38	G)
6803	SIS_RETIND	Indicador *Reset Password*	1	A	159	52	38	D)
3974	EXT_TELNUM	Número de Telefone	9	N	160	52	38	E)
0505	CAR_PANN03	PAN do Cartão	16	N	169	52	38	F)

N.º Campo	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Validações/ Observações
5325	CAR_EXPDATN01	Data de Expiração do Cartão	6	N	185	52	38	F)
3257	SIS_TIMSTP	*Timestamp* Actualização DB2	26	A	191	52	38	
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A	217	52	38	
0472	MSG_RESTXT	Texto Resposta	45	A	217	52	46	
0472	MSG_RESTXT	Texto Resposta	45	A	217	52	91	
		Total	**216**		**51**		**135**	

A) Por pré-definição só aceita o valor igual a 2 - cartão *On-Us*;

B) Se MSG_ACCCOD = 3 (Alteração) e o CAR_ATT3DS = 1 (*Password*) então os campos G) são de preenchimento obrigatório. Os restantes campos F) e E) devem estar a zeros.

Se MSG_ACCCOD = 3 (Alteração) e o CAR_ATT3DS = 2 (SMS) então o campo E) é de preenchimento obrigatório. Os restantes campos F) e G) devem estar a zeros e a espaços de acordo com as suas especificações.

Se MSG_ACCCOD = 3 (Alteração) e o CAR_ATT3DS = 3 (MB CODE) então os campos F) são de preenchimento obrigatório, mas o número do cartão CAP deve estar cifrado. O campo E) e G) deve estar a zeros ou a espaços de acordo com as suas especificações.

C) Se MSG_ACCCOD = 4 (Cancelamento) a situação cartão 3D Secure (SIS_SIT3DS) assume o valor 9 e a data de situação cartão 3D Secure tem de estar preenchida, os restantes campos pertencentes aos métodos de autenticação existentes deverão estar a espaços ou a zeros de acordo com as suas especificações.

D) Se MSG_ACCCOD = 3 (Alteração) e acção = *Reset* chave de acesso, o CAR_INDRST = 1, os restantes campos pertencentes aos métodos de autenticação existentes deverão estar a espaços ou a zeros de acordo com as suas especificações.

H) Se MSG_ACCCOD = 6 (Alteração Método Autenticação) vai preenchido com o código do novo método de autenticação escolhido, caso contrário vai igual a zero.

5.2 Ficheiros

A implementação desenvolvida pela SIBS FPS que suporta esta nova funcionalidade tem impacto nos dados adicionais do registo Tipo 1 do Ficheiro de Destinos (DST5)

5.2.1 Dados Adicionais do Ficheiro de Destinos (DST5)

No Ficheiro de Destinos quando o campo (0699) SIS_OPRTIP ("Código de Transacção Expandido") assume os valores:

- 1E7 – Adesão ao serviço 3D Secure;
- 2E7 - Consulta ao serviço 3D Secure;
- 3E7 - Alteração *Password* ao serviço 3D Secure;
- 4E7 – *Reset Password* ao serviço 3D Secure;
- 5E7 - Alteração telemóvel ao serviço 3D Secure;
- 6E7 - Alteração do cartão e data expiração associada ao serviço 3D Secure;
- 7E7 - Alteração ao método de autenticação (troca de método);
- 8E7 - Cancelamento ao serviço 3D Secure;
- 9E7 – Autenticação.

Tabela 1 - Dados Adicionais do Registo de Tipo 1 do Ficheiro DST5 para processo de adesão / manutenção do serviço 3D Secure

Campo	Sigla	Nome do Campo	Comp.	Pos.	Rep.	Observações
(0699) SIS_OPRTIP = '1E7', '2E7', '3E7', '4E7', '5E7', '6E7', '7E7', '8E7'						
6876	CAR_ATT3DS	MODO DE AUTENTICAÇÃO 3D SECURE	1	312	N	A)
(0699) SIS_OPRTIP = '9E7'						
6876	CAR_ATT3DS	MODO DE AUTENTICAÇÃO 3D SECURE	1	312	N	
1368	SPI_3DSMNT	MONTANTE 3DS	12	313	N	
1369	SPI_DCMMOEN01	CASAS DECIMAIS DA MOEDA	2	315	N	

A) Operação sem impacto contabilístico para o cliente.

5.3 Dicionário de dados

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

N.º	Sigla	Nome Campo	Comp.	Rep.	Formato	Descrição	Valores
0002	MSG_VER	Versão de Mensagem	2	N		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	AAAAMMDD HHMMSS	Campo que contém a data e a hora em que se efectuou a transmissão da mensagem da CPU da SIBS para a 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 - Transacção aprovada 1 - Pedido de degradação de Cenário 4 - Transacção não aprovada por razões várias 5 - Transacção não aprovada; o campo SALDO indica o máximo que poderia ter sido pago na transacção que finda 6 - Erro aplicacional 7 - Captura do cartão"

N.º	Sigla	Nome Campo	Comp.	Rep.	Formato	Descrição	Valores
0117	LOG_NUMN01	Número de Registo Log Central	8	N		Identifica o número do registo no Ficheiro de Log do CPU-SIBS referente à transacção. 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 transacções a SIBS 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 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 usa mais do que um ficheiro de log por dia, pelo que, num mesmo ficheiro da Compensação MB, 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	Nome 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 492 >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		Último mês e ano em que o cartão ainda é válido.	

N.º	Sigla	Nome Campo	Comp.	Rep.	Formato	Descrição	Valores
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. Se = 1 cartão *Not-on-us* Se = 2 cartão *On-Us*	
1368	SPI_3DSMNT	Montante 3DS	12	N	Sem decimais	Montante da compra enviado pelo comerciante no âmbito do sistema 3D Secure da Visa (Purchase Amount). Exemplo: Display amount: €125.45 (atributo 1367) Purchase amount: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 Transacção (Novo Código Expandido)	2	A		Código utilizado nas mensagens e nos registos de detalhe correspondentes a cada operação e que indica ao Banco qual o subsistema transaccional 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.	Valores possíveis para o Centro de Processamento de Dados de Lisboa: 01 - QUE 02 - POS 01 03 - INT. 04 - BX. V. 05 - ATM-OLO 01 06 - PMB 07 - ATM-OLO 02 08 - POS 02 0A - Registos Batch 0C - SIDF 0D - POS 03 0E - POS 04 0F - ATM-OLO 03 10 - ATM-OLO 04

N.º	Sigla	Nome Campo	Comp.	Rep.	Formato	Descrição	Valores
							11 - FEP - ATM 12 - FEP - POS 13 - RECLAMAÇÕES Valores possíveis para o Centro de Processamento de Dados de Viseu (codigos não aplicados com o LOG em DB2): 51 - QUE 52 - POS 01 53 - INT. 54 - BX. V. 55 - ATM-OLO 01 56 - PMB 57 - ATM-OLO 02 58 - POS 02 5A - Registos Batch 5C - SIDF 5D - POS 03 5E - POS 04 5F - ATM-OLO 03 60 - ATM-OLO 04"
2483	MSG_ACCCOD	Código de Gestão da Mensagem	1	A		Código que determina a acção que a mensagem desenvolve.	1 - Inserção 2 - Consulta 3 - Alteração 4 - Abate 5 - Confirmação 6 - Alteração Método Autenticação 7-Insere adiantamento 8-Altera-adiantamento 9-Abate-adiantamento"

N.º	Sigla	Nome Campo	Comp.	Rep.	Formato	Descrição	Valores
3257	SIS_TIMSTP	Timestamp Actualização DB2	26	A	Timestamp	Indica o timestamp de actualização 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	
3286	CHV_HASRSA	*Hash* da Chave RSA	20	A		Valor do Secure Hash da chave RSA.	
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			
5325	CAR_EXPDATN01	Data de Expiração do Cartão	6	N	AAAAMM	Data de expiração do cartão 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.	
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.	
6801	SIS_TENPSW	Número Tentativas *Password*	1	N		Identifica o número de tentativas de *password* possíveis	
6802	SIS_RETPSW	Número *Reset Password*	1	N		Número de *reset* efectuados à *password*	

N.º	Sigla	Nome Campo	Comp.	Rep.	Formato	Descrição	Valores
6803	SIS_RETIND	Indicador *Reset Password*	1	N		Indica se é para efectuar *reset* à *password*	0 - Não 1 - Sim"
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* efectuados ao código acesso	
6876	CAR_ATT3DS	Modo de Autenticação 3D Secure	1	N		Modo de Autenticação 3D Secure (o correspondente ao TRM_ATT3DS).	1 - *Password* 2 - SMS 3 - MB CODE"