Manual do Serviço

Processamento para Emissores

Emissores

Versão: 01.10

Data: 2012-05-24

Estado: Final

Classificação: Restrito

Referência: DCSIBS110139

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:	DCSIBS110139
Título do Documento:	Manual do Serviço - Processamento para Emissores
Versão:	01.10
Estado:	Final
Classificação:	Restrito
Tipo de Documento:	Manual do Serviço
Área Funcional Responsável:	AF Desenvolvimento de Serviços

Documentos Relacionados

Referência	Título	Origem
DCSIBS100026	Manual de Implementação Serviços para Emissores V02.10	AF Desenvolvimento de Serviços
DCSIBS120135	Formulário - Verified by Visa - Acção sobre resultado da validação do CAVV V01.00	AF Desenvolvimento de Serviços
DCSIBS120049	Formulário – Caracterização de BIN V01.10	AF Desenvolvimento de Serviços
n.a.	Formulário – Caracterização de Emissor	AF Desenvolvimento de Serviços
n.a.	Formulário – Caracterização de CPD	AF Desenvolvimento de Serviços
n.a.	Formulário – Caracterização de Padrão EMV	AF Desenvolvimento de Serviços
Memo 2012-030	Acção sobre o resultado da validação CAVV em autorizações e-commerce com autenticação Verified by Visa	AF Desenvolvimento de Serviços

Revisões

Versão	Data	Descrição	Autor
01.00	30-12-2011	Criação do documento	AF Desenvolvimento de Serviços
01.10	24-05-2012	• Novas secções 4.1.6 - Cartões multi-aplicação e 4.5.1 - Ciclo de vida dos cartões multi-aplicação. Alterações de conteúdo inseridas neste âmbito nas seguintes secções 3.4.3, 4.1.1. • Nova secção 4.7 – Autenticação. O conteúdo desta secção constava na secção 4.8 - Autorização, por questão de organização separou-se o processo de autenticação do processo de autorização. • Actualização de data de expiração de chave nas secções 4.4.4.2 e 4.4.4.3. • Alteração do fluxo de estado de um cartão Capturado a Devolver Após Fecho CA e de um cartão Capturado e em Lista Negra, secção 4.5. • Na secção 4.6.1.2 Serviços especiais de marca MB SPOT a apresentação do Serviço Via Verde passou a estar na área de serviços não bancários. • Na secção 8 Anexos, inclusão do anexo Acção sobre a validação do CAVV. • Actualizada a tabela de documentos relacionados. • Substituição de terminologia, de forma a adequá-la à realidade actual do Grupo SIBS e suas marcas (CA-MB por CA MULTIBANCO, TPA-MB por TPA MULTIBANCO, SIDEF por PAYWATCH, sistema MB por sistema da SIBS FPS). • Outras alterações editoriais, não assinaladas, e sem impacto no conteúdo da informação.	AF Desenvolvimento de Serviços

Índice

Índice de Figuras

Índice de Tabelas

Índice de Quadros

1 Introdução

Os Serviços para Emissores contemplam um conjunto de processos e funcionalidades que visam a simplificação e máxima eficiência para o bom funcionamento dos meios de pagamento. O serviço de emissão de cartões é constituído por uma alargada cadeia de valor que poderá ser executada na totalidade pela SIBS: Forward Payment Solutions (SIBS FPS) como entidade processadora.

Os serviços prestados pela SIBS FPS vão desde a emissão lógica de cartões e respectivos PIN (*Personal Identification Numbers*), o processamento de operações e/ou autorização das mesmas, a prestação de serviços de segurança, a aceitação / encaminhamento de operações realizadas em terminais da Rede MULTIBANCO, nas redes de Sistemas de Pagamento Internacionais (SPI) ou em canais como a Internet e rede móvel, até à gestão da compensação e gestão de disputas.

1.1 Enquadramento

No início da década de 80, a comunidade bancária portuguesa criou um modelo de cooperação interbancária que visava responder aos desafios de modernização que se colocavam ao sector. Como consequência desta necessidade e da prevalência de uma visão de longo prazo, foi desenhada uma rede de serviços interbancários, universal e aberta a todos os Bancos, permitindo a modernização dos meios de pagamento, a expansão da componente electrónica desses meios e uma redução substancial nos custos operacionais das entidades intervenientes.

Com a missão de desenvolver e gerir uma rede de serviços interbancários em colaboração com os Bancos e o Banco de Portugal, a SIBS iniciou a execução de um projecto de automatização das operações bancárias de rotina recorrendo às novas tecnologias de informação para a transmissão e processamento de dados. É neste contexto que surge a SIBS FPS como entidade processadora e a Rede MULTIBANCO, concebida com base nos princípios de funcionamento de uma rede cooperativa partilhada por diversos Bancos.

O sistema da SIBS FPS, suportado na capacidade de processamento da SIBS FPS, em múltiplas aplicações desenvolvidas ao longo dos anos para satisfazer um número crescente de necessidades do Sistema de Pagamentos português e na rede de terminais que constituem a Rede MULTIBANCO, é utilizado por um conjunto muito diverso de entidades, de que apenas referimos, a título de exemplo:

- Os Bancos accionistas da SIBS, detentores da marca MB e MB SPOT e Emissores de cartões com essa marca (de forma isolada ou associada a marcas internacionais);
- Emissores ou representantes de vários tipos de cartões (gasolineiras, redes de lojas, etc.);
- Empresas que disponibilizam aos seus clientes a possibilidade de pagamento com cartões, quer nas suas lojas através da rede de terminais de pagamento automático - TPA MULTIBANCO, quer

através das operações de compra, pagamento de serviços ou mesmo de serviços específicos na rede de Caixas Automáticos - CA MULTIBANCO;

- Os Titulares de Cartões que acedem aos serviços disponibilizados para o cartão que contrataram com o Emissor do mesmo.

1.2 Âmbito

O presente documento descreve as principais características dos Serviços de Processamento para Emissores MB e SPI, nomeadamente os processos da cadeia de valor do negócio de emissão, os serviços de emissão lógica de cartões e respectivos PIN, os cenários de decisão de transacções e o processamento e compensação de operações na Rede MULTIBANCO e noutras redes. São igualmente referidas as responsabilidades que cada interveniente deve assumir no âmbito dos Serviços para Emissores, bem como as vantagens proporcionadas por todas as funcionalidades associadas a este serviço.

2 Processamento para Emissores

2.1 Intervenientes

A disponibilização dos Serviços para Emissores envolve as seguintes entidades:

- **Emissores ou Emitentes**

Entidades que contratam com os seus clientes a emissão de cartões bancários e não bancários e que são responsáveis, no âmbito das regras do Sistema de Pagamento a que reportam esses cartões, pelas transacções por eles realizadas.

- **SIBS FPS**

Entidade que realiza a gestão do serviço de pagamento automático e da Rede CA e TPA MULTIBANCO, garantindo a integridade e segurança dos dados transmitidos entre os diversos intervenientes e o sistema central da SIBS FPS.

- **Titulares de Cartões**

Clientes dos Emissores que detêm cartões de pagamento e utilizam os CA e TPA para realizar as operações disponibilizadas.

- ***Acquirers* ou Aceitantes**

Entidades responsáveis pela contratação de Comerciantes para a aceitação de cartões de marcas MB, MB SPOT, SPI ou redes privadas e pelo pagamento de transacções dos cartões que representam aos Comerciantes.

- **Comerciantes**

Entidades que contratam junto dos *Acquirers* a aceitação de cartões de diferentes marcas e que disponibilizam, através dos TPA instalados nos seus estabelecimentos, o serviço de Pagamento Automático aos Titulares de Cartão.

- **Entidades de Apoio ao Terminal (EAT)**

Entidades responsáveis pela relação com os Comerciantes na componente de contratação do serviço de Pagamento Automático, bem como pela matrícula de TPA no sistema da SIBS FPS, pelo pedido de produção de cartões de supervisor e pela garantia do bom funcionamento dos terminais ligados à Rede MULTIBANCO.

A EAT pode ser um Banco membro do sistema ou um *Acquirer* que tenha contratado com a SIBS FPS a utilização da sua rede TPA. Neste caso, o *Acquirer* assume também as funções de EAT.

- **Bancos de Apoio aos Comerciantes (BAC)**

Instituições de crédito nas quais residem as contas bancárias dos Comerciantes. Os BAC disponibilizam o seu sistema de informação para acolher a movimentação financeira nas contas dos Comerciantes decorrentes da utilização dos TPA.

O BAC coincide com a EAT quando esta é um Banco. Se o proprietário do TPA for o Comerciante, o BAC e a EAT podem ser Instituições diferentes.

- **Personalizadores**

Entidades a quem compete a produção física de cartões bancários ou não bancários, no âmbito de um contrato de produção de cartões previamente estabelecido com os Emissores.

- **Sistemas de Pagamento**

Instituições proprietárias de uma marca de cartão de pagamento que contratam com os Emissores e *Acquirers* a utilização e representação dessa marca. No caso de não serem nacionais, denomina-se, no âmbito deste serviço, Sistema de Pagamento Internacional (SPI).

2.2 Apresentação do Serviço

Os Serviços para Emissores englobam um vasto leque de processos e funcionalidades que visam auxiliar os Emissores no processo de comercialização de cartões bancários e não bancários junto dos Titulares de Cartões.

Figura 1 - Cadeia de valor dos Serviços para Emissores

Este serviço foca-se nos processos da cadeia de valor do negócio de emissão, nomeadamente:

1. **Emissão de Cartões**
   Cálculo lógico dos dados dos cartões e emissão dos respectivos PIN.
2. **Gestão de Cartões**
   Parqueamento dos cartões na base de dados da SIBS FPS, bem como a gestão dos estados operacionais que um cartão pode assumir ao longo do seu ciclo de vida.
3. **Autorização**
   Validação dos elementos de segurança dos cartões e verificação (se transacção com cartão) do código secreto (PIN) introduzido pelo titular. Contempla igualmente o encaminhamento do pedido de autorização para o Emissor ou a decisão da SIBS FPS, mediante delegação prévia nesse sentido.

4. **Compensação e Liquidação**

   Envio, a cada Emissor, de informação detalhada sobre todas as operações realizadas na Rede MULTIBANCO ou outras redes com os cartões por si emitidos, assim como os totais apurados. Inclui ainda o apuramento de saldos para liquidação entre todos os participantes no sistema da SIBS FPS.

5. **Gestão de Disputas**

   Serviço disponibilizado no Portal de Serviços SIBS ou via mensagens *Host-to-Host* que permite a gestão das reclamações derivadas da utilização de cartões das marcas MB e de SPI, de acordo com as regras dos Sistemas de Pagamento nacional (MB) e internacionais (VISA, MasterCard e Amex).

6. **Gestão de Fraude - Paywatch**

   Serviços prestado pela PAYWATCH, uma empresa participada pelo Grupo SIBS, que garante a monitorização das transacções realizadas na Rede MULTIBANCO e fora desta, mas com cartões *on us*, numa óptica de prevenção e detecção de fraude e intervenção para bloqueio dos pontos de venda comprometidos.

Cada Emissor define quais os serviços que pretende contratar dentro da cadeia de valor e, para cada um desses elementos, parametriza um conjunto de informação junto da SIBS FPS, devendo estar preparado para o envio e recepção de um conjunto de ficheiros e mensagens (ver Manual de Implementação - Serviços para Emissores).

Caso o Emissor pretenda que a SIBS FPS execute o processamento das operações efectuadas pelos seus cartões, os dados do cálculo lógico dos respectivos cartões ficam parqueados na SIBS FPS (carregamento na base de dados SIBS). Para este cenário é também necessária a parametrização de um conjunto de informações e o envio, pelo Emissor, dos ficheiros definidos para o efeito.

O Emissor pode ainda pretender que a SIBS FPS execute o processamento de transacções efectuadas por cartões cujo cálculo lógico foi realizado por uma outra entidade. Neste caso, é necessário garantir que não existem incompatibilidades com as normas de segurança da SIBS FPS.

2.3 Vantagens do Serviço

Os Serviços para Emissores proporcionam as seguintes vantagens aos **Emissores**:

1. Redução dos pagamentos em numerário a favor de meios de pagamento electrónicos mais cómodos e eficientes;
2. Redução de custos de processamento e telecomunicações nas operações de pagamento;
3. Redução dos tempos de processamento da transacção;
4. Garantia de um nível de segurança na realização das operações comuns para qualquer cartão emitido;
5. Uniformização da informação associada a qualquer transacção efectuada com um cartão do Emissor;

6. Garantia de recepção da informação específica para cada transacção efectuada com um cartão do Emissor;
7. Possibilidade de disponibilização por parte do Emissor, de um conjunto de serviços de valor acrescentado aos seus Titulares de Cartões.

Os Serviços para Emissores proporcionam as seguintes vantagens aos **Titulares de Cartões**:

1. Uniformização do serviço em qualquer Emissor;
2. Disponibilização de um conjunto de operações comuns em qualquer Emissor;

2.4 Responsabilidades

Os principais intervenientes nos Serviços de Processamento para Emissores MB e SPI têm as seguintes responsabilidades na disponibilização do serviço:

Emissores

1. Definir as características do seu portfólio de produtos e gerir o processo de adesão de novos clientes;
2. Parametrizar na SIBS FPS as características dos seus produtos para a respectiva emissão de cartões;
3. Solicitar a emissão de cartões e respectivos PIN;
4. Definir os cenários de autorização de operações realizadas na Rede CA e TPA MULTIBANCO;
5. Executar o tratamento de disputas relativas a operações executadas pelos seus cartões;
6. Receber a informação relativa à compensação e liquidação das transacções efectuadas com os seus cartões.

SIBS FPS

1. Emitir logicamente os cartões com as características parametrizadas pelo Emissor;
2. Assegurar a gestão técnica da base de dados dos cartões;
3. Processar as operações executadas na Rede CA e TPA MULTIBANCO;
4. Enviar ficheiros e mensagens aos Emissores para controlo de gestão das operações;
5. Assegurar a autenticação dos cartões;
6. Executar os processos de validação dos cartões e das operações efectuadas com cartões *on us* na Rede CA e TPA MULTIBANCO e noutras redes;
7. Realizar a compensação e liquidação das operações entre os diferentes intervenientes do sistema da SIBS FPS.

Personalizador

1. Emitir fisicamente os cartões com a informação logica produzida pela SIBS FPS;
2. Garantir que o *layout* dos cartões físicos respeita as regras dos Sistemas de Pagamento incluídos logicamente nos cartões e as escolhas de imagem definidas pelos Emissores;
3. Emitir cartas PIN (associadas ou não a um cartão emitido fisicamente);
4. Envio dos cartões emitidos fisicamente para o destino acordado como o Emissor.

2.5 Contactos

Tabela 1 - Contactos dos Serviços para Emissores na SIBS FPS

Âmbito	Área	Contacto
Pedidos de evolução de serviço	Departamento Gestão Comercial	Gestor de Relação
Dúvidas e comunicação de anomalias	Departamento Gestão Operações e Redes	sac.suporte@sibs.pt

Quadro 1 - Apresentação dos Serviços para Emissores

- Os Serviços para Emissores englobam um vasto leque de processos e funcionalidades que visam auxiliar os Emissores no processo de comercialização de cartões bancários e não bancários junto dos seus clientes.
- A operacionalização do serviço é executada pelas seguintes entidades:
  - Emissores;
  - SIBS FPS;
  - Titulares de Cartões;
  - *Acquirers*;
  - Comerciantes;
  - Entidades de Apoio aos Terminais;
  - Bancos de Apoios aos Proprietários;
  - Personalizadores;
  - Sistemas de Pagamento.
- Este serviço foca-se nos seguintes processos da cadeia de valor do negócio de emissão:
  - Emissão;
  - Gestão de Cartões;
  - Autorização;
  - Compensação e Liquidação;
  - Gestão de Disputas.
- O Emissor pode decidir contratar qualquer um dos serviços apresentados na cadeia de valor, desde que esteja preparado para o envio e recepção de um conjunto de informações no formato definido pela SIBS FPS.
- Cada interveniente nos serviços de processamento para Emissores da SIBS FPS tem um conjunto de responsabilidades fundamentais para o bom funcionamento do serviço e para a correcta troca de informação entre os diversos intervenientes

3 Conceitos

3.1 Cálculo Lógico

O cálculo lógico de cartões consiste na geração dos dados que permitem o funcionamento do cartão e dados de segurança que garantem aos detentores dos cartões a sua fiável utilização na Rede CA e TPA MULTIBANCO e outras redes.

O cálculo lógico é efectuado automaticamente mediante a validação da recepção de todos os ficheiros necessários à produção de cartões enviados pelo Emissor. Se não estiverem presentes todos os ficheiros necessários à produção em causa, os ficheiros são colocados em espera durante um determinado período, consoante se trate ou não de uma produção urgente.

Estando presentes todos os ficheiros necessários à produção, verifica-se se existe infra-estrutura de segurança disponível. Se não existirem módulos de segurança disponíveis para o cálculo lógico, os ficheiros ficam em espera até ser possível o respectivo acesso.

Se as validações descritas forem concluídas com sucesso, e se estiverem satisfeitas as condições necessárias, dá-se início ao processo de cálculo lógico.

3.2 Parqueamento de Cartões (Carregamento na Base de Dados SIBS)

O parqueamento de cartões na SIBS FPS consiste no carregamento pelo Emissor dos cartões na base de dados da SIBS FPS através dos ficheiros definidos para o efeito. Os cartões a carregar no sistema central da SIBS FPS têm de ter um PAN (*Primary Account Number*) com o comprimento máximo de dezasseis dígitos. Com o parqueamento dos cartões, a SIBS FPS está em condições de efectuar todas as validações de segurança anteriores à apresentação de uma operação para autorização e necessárias à execução das operações: a autenticação do Titular do Cartão.

O parqueamento de cartões é assegurado pela SIBS FPS até ao mês de expiração do cartão, inclusive. Após expirado, o cartão deixa de estar parqueado, apesar de permanecer na base de dados por um período adicional de seis meses.

3.3 Dados de Emissor

Antes de proceder à emissão lógica de cartões, o Emissor tem de registar na SIBS FPS um conjunto de elementos – apelidados de Caracterizações - necessários para a parametrização dos cartões a emitir. As caracterizações base para que uma entidade possa emitir cartões são as seguintes:

- Caracterização do Emissor;
- Caracterização do Centro de Processamento de Dados (CPD) do Emissor;
- Caracterização do Padrão EMV (Europay, MasterCard e VISA);
- Caracterização do BIN (*Bank Identifier Number*).

Ao registar os diferentes elementos no sistema da SIBS FPS, o Emissor tem de seleccionar o tipo de caracterização pretendido e preencher o respectivo formulário. Sempre que surja a necessidade de se proceder a actualizações de parametrização no ambiente de Produção, a SIBS FPS requer ao Emissor a execução prévia de testes às alterações que se pretenda implementar.

3.3.1 Caracterização do Emissor

O Emissor preenche e envia à SIBS FPS o formulário “Caracterização do Emissor” no momento da adesão aos Serviços para Emissores ou sempre que pretenda alterar uma das parametrizações em uso.

Nesta configuração, são seleccionados e fornecidos os seguintes dados indispensáveis à troca de ficheiros com a SIBS FPS:

- Elementos genéricos sobre o Emissor;
- Chaves de acesso à base de dados de cartões do sistema da SIBS FPS a partir de uma das seguintes alternativas:
  - Número de cartão único por Emissor (cenário base);
  - Número de cartão único por BIN identificado pelo número de cartão (PAN);
  - Número de cartão único composto por PAN e data de expiração.
- Destinos de ficheiros e processamentos opcionais;
- Definição de envio de dados estatísticos;
- Definição de textos a apresentar em talões de terminais;
- Definição de opções sobre emissão e funcionamento de cartões, que inclui a definição do envio dos ficheiro de *incoming* dos SPIs.

3.3.2 Caracterização do CPD do Emissor

O Emissor preenche e envia à SIBS FPS o formulário “Caracterização do Centro de Processamento de Dados (CPD) do Emissor” aquando do início de funcionamento de um novo CPD. A parametrização de vários CPD permite a parametrização de vários cenários de autorização de operações para o mesmo Emissor. O preenchimento deste conjunto tem como base as características de funcionamento do CPD do Emissor, devendo ser preenchido um impresso por cada CPD no caso de múltiplos centros.

Neste formulário, o Emissor indica um conjunto de informações relativas a:

- Endereço dos ficheiros respeitantes ao CPD em causa;
- Definição dos cenários de funcionamento associados ao CPD;
- Definição de parametrizações em sessões de *real-time* com a SIBS FPS;
- Definição das características do serviço MB PHONE;
- Definição de parâmetros de pedidos de cheques personalizados;
- Definição das operações por cenários de funcionamento (ver capítulo 4).

3.3.3 Caracterização do Padrão EMV

O Padrão EMV possibilita a definição pelo Emissor de diferentes perfis para os cartões EMV. Estes perfis consubstanciam-se na definição de duas ordens de parâmetros:

- Selecção da aplicação EMV a associar ao padrão, tanto ao nível de aplicação de pagamento (por exemplo, MB, VISA, MasterCard, American Express, entre outros) como aplicação de autenticação (por exemplo VISA - DAP, MasterCard - CAP, MB – MB CODE);
- Selecção das línguas suportadas pela aplicação EMV.

Para possibilitar a emissão lógica de cartões EMV, é necessária uma parametrização prévia de um ou vários Padrões EMV. O Emissor preenche e envia à SIBS FPS o formulário “Caracterização do Padrão EMV” aquando da definição de um novo Padrão EMV ou a alteração de parâmetros de um Padrão EMV já existente.

3.3.4 Caracterização do BIN

No formulário “Caracterização do BIN”, o Emissor define um vasto conjunto de parâmetros que condicionam o funcionamento dos cartões a serem emitidos com base nessa caracterização. O Emissor parametriza os seguintes elementos:

- Âmbito de utilização - Serviços permitidos, por tipo de terminal e por área geográfica;
- Parâmetros de gestão de risco para transacções *offline*, em número de operações permitidas e valor;
- Lista de métodos de autenticação do Titular de Cartão;
- Parâmetros de *fallback* para pista / banda magnética.

O Emissor, no momento em que caracteriza, pela primeira vez para um BIN qualquer, os elementos supracitados, desencadeia um processo de preparação do BIN. Este processo inclui a geração e carregamento de chaves públicas de Emissor, não sendo possível a emissão de cartões até que estas chaves existam no sistema da SIBS FPS.

Um BIN (*Bank Identifier Number*) é identificado no sistema da SIBS FPS por oito dígitos. Os primeiros seis correspondem ao BIN atribuído pelo SPI. Os dois seguintes (7º e 8º) designam-se por extensão de BIN,

constituem um sufixo do BIN e são necessários para que a SIBS FPS diferencie vários produtos associados ao mesmo BIN.

O Emissor preenche e envia à SIBS FPS o formulário "Caracterização do BIN" aquando do início de funcionamento de um novo BIN ou extensão de BIN, ou sempre que se pretenda alterar uma das parametrizações em uso. No caso de produtos de marca internacional, o Emissor tem igualmente de caracterizar o BIN junto dos respectivos SPI.

As alterações no formulário "Caracterização do BIN" (mesmo que seja apenas ao nível de extensão de BIN) podem ser alvo de certificação junto das respectivas marcas (ver secção 3.3.4.2).

3.3.4.1 Limites de autorização por BIN

Para as operações realizadas na Rede MULTIBANCO, em situações específicas que apresentam maior risco, o Emissor pode posicionar limites por BIN que funcionam como um limite máximo na aceitação de operações. Os limites aplicam-se a:

- Operações na Rede TPA MULTIBANCO e algumas na Rede CA MULTIBANCO, em cenário de degradação (ver capítulo 4);
- Pagamentos de baixo valor com cartão em portagens e telefones;
- Compras de baixo valor com cartão na Rede TPA MULTIBANCO;
- Operações na Rede CA e TPA MULTIBANCO com recurso a *fallback* de *chip* para pista / banda magnética.

No caso de operações realizadas noutras redes, os limites de autorização por BIN aplicam-se a:

- Operações de pedido de autorização;
- Operações na Rede CA e TPA MULTIBANCO, com recurso a *fallback* de *chip* para pista / banda magnética.

3.3.4.2 Certificação de cartões

A emissão lógica de cartões de um SPI pressupõe um processo de certificação junto do respectivo sistema, seguindo um conjunto de regras e passos específicos. Este processo de certificação garante a conformidade do cartão ao nível dos dados gravados no cartão e da sua usabilidade (transaccional).

Cada SPI tem o seu próprio processo de certificação definido sendo que, tipicamente, o Emissor tem de cumprir esta etapa previamente à emissão lógica de cartões. O processo de certificação junto dos SPI é iniciado por cada Emissor.

Os SPI certificam um conjunto de características que o cartão apresenta tais como: aplicações presentes no cartão (ex: *contactless* - ver secção 3.4.4.3); produto de crédito ou débito; aplicação CAP; tipo de autenticação do portador do cartão (PIN, assinatura, outros - ver secção 3.4.6); marca / modelo de *chip*; Personalizador; e aplicabilidade do logótipo do SPI, entre outros elementos.

Consoante as características do cartão, a sua certificação terá um determinado período temporal.

3.4 Cartões

No início do processamento de uma operação na Rede CA e TPA MULTIBANCO, o sistema da SIBS FPS verifica se tem ou não conhecimento do cartão utilizado para a operação na sua base de dados.

Dependendo do parqueamento ou não de um cartão na sua base de dados, a SIBS FPS distingue os cartões entre:

- **Cartões *on-us*** - Cartões que se encontram parqueados na base de dados da SIBS FPS e para cujos Emissores a SIBS FPS disponibiliza um serviço de processamento com um leque abrangente de funcionalidades;
- **Cartões *not-on-us*** - Cartões não parqueados na base de dados da SIBS FPS dos quais apenas se dispõe de um conjunto base de informações que permitem garantir a aceitação de operações realizadas com esses cartões na Rede CA e TPA MULTIBANCO.

Caso o cartão que vai realizar a operação seja um cartão *on-us*, a SIBS FPS procede de acordo com o cenário de autorização parametrizado pelo Emissor para o BIN e respectiva extensão (ver capítulo 4). Os cartões *on-us* podem transaccionar tanto na Rede MULTIBANCO como em qualquer outra rede. Contudo, os cenários de funcionamento consoante a rede apresentam algumas diferenças:

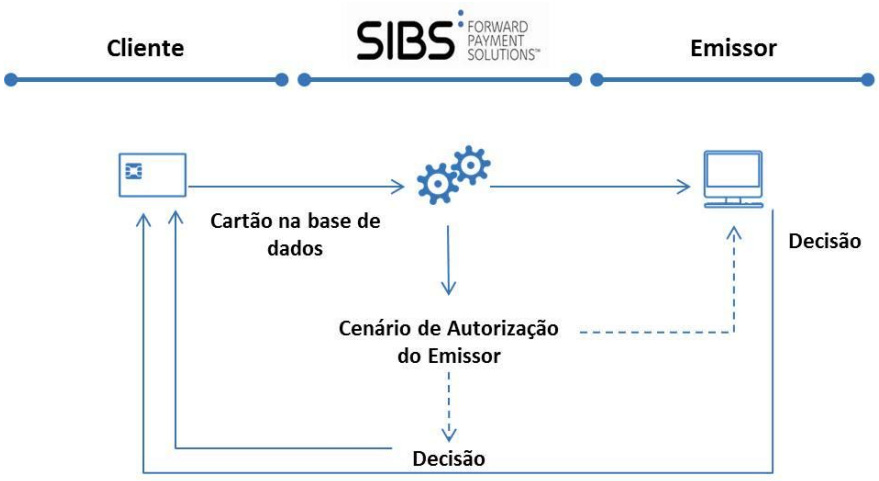

Figura 2 - Funcionamento de um cartão *on-us* na Rede CA e TPA MULTIBANCO

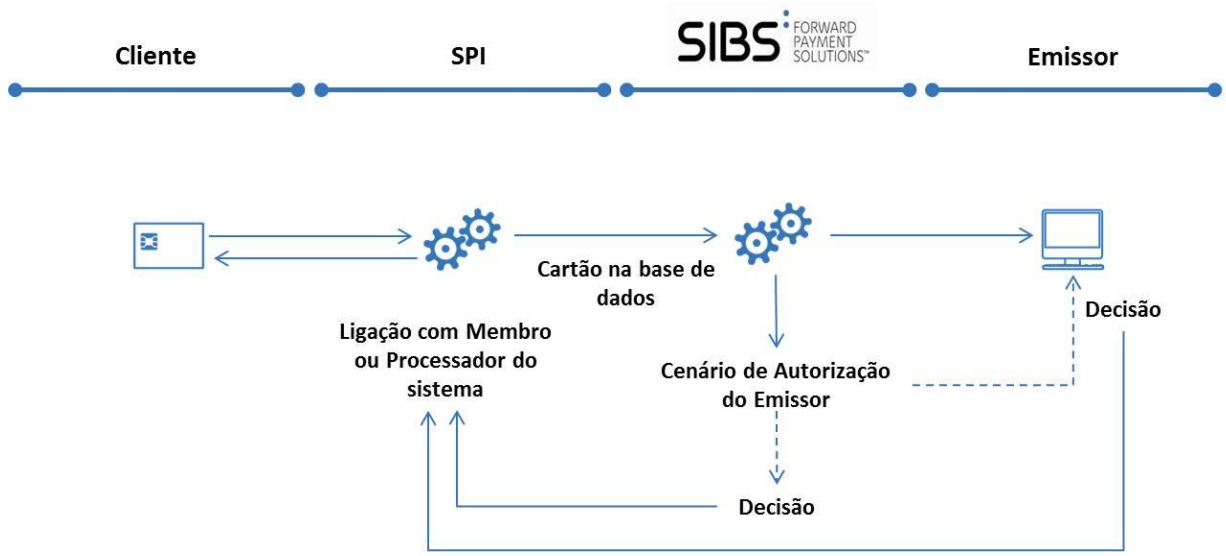

Figura 3 - Funcionamento de um cartão *on-us* noutras redes

3.4.1 Tipos de cartões

A emissão de um cartão bancário (cartão emitido com uma conta bancária associada) pode ser efectuada através da produção dos seguintes tipos de cartões:

- **Débito** - Cartão de débito de marca MB ou marca de SPI com conta-corrente associada ao cartão;
  - **Débito diferido** - Cartão de débito com cobrança de movimentos diferida.
- **Crédito** - Cartão de crédito de marca internacional com conta-crédito associada ao cartão;
  - ***Charge cards*** - Cartão com prazo de pagamento fixo, aplicável a cada transacção.
- **Misto** - Cartão de crédito *co-branded* de marcas MB e internacional com, por exemplo, uma conta-corrente e uma conta-crédito associadas simultaneamente ao cartão.

Cada tipo de cartão pode ter uma utilização genérica, onde o cartão é livremente utilizado de acordo com as operações disponibilizadas e os respectivos cenários de autorização definidos pelo Emissor, ou uma utilização restrita baseada em critérios definidos pelo Emissor.

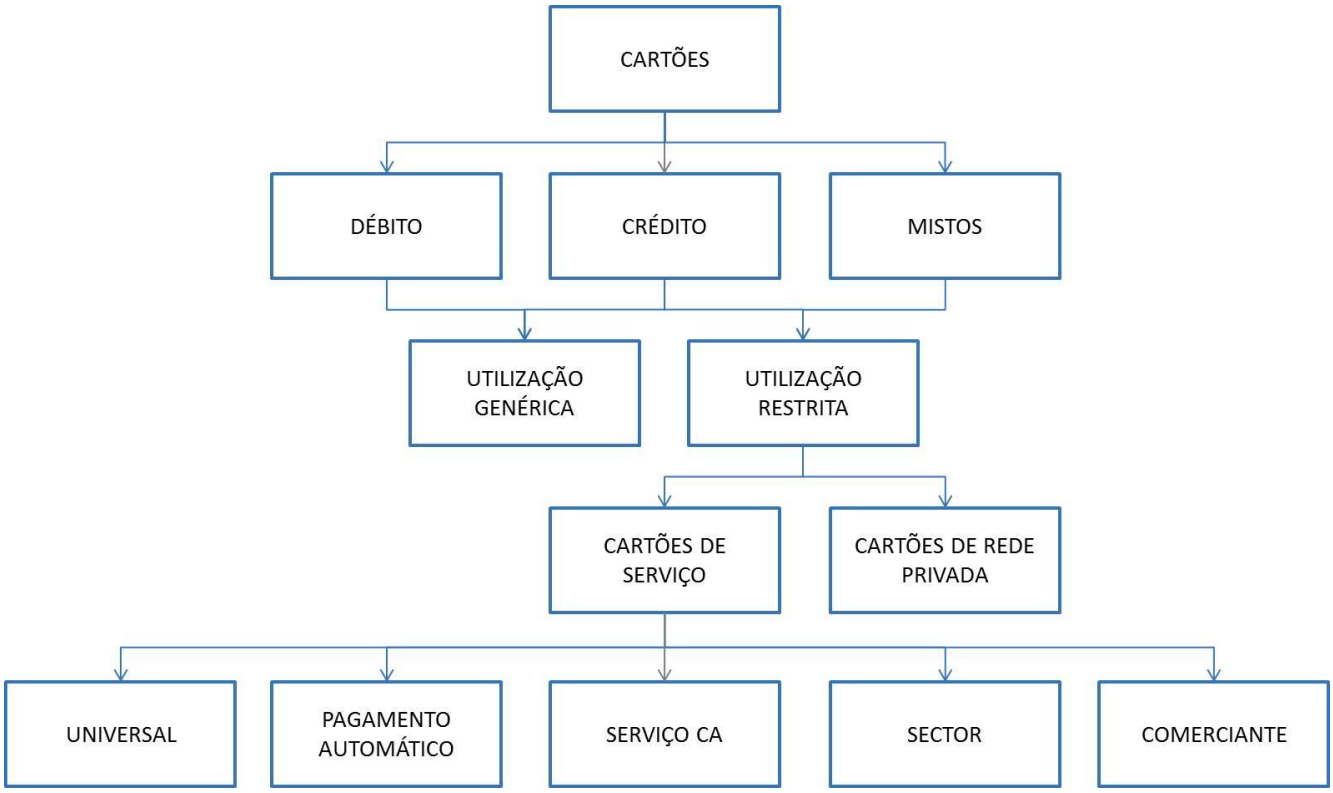

Figura 4 - Tipificação de cartões

Os cartões de utilização restrita subdividem-se em dois grupos distintos:

- **Cartões de serviço** - Cartões geralmente pertencentes a uma empresa, de utilização restrita a certos estabelecimentos comerciais ou sectores de actividade, e com um âmbito limitado de funcionalidades disponibilizadas na Rede CA MULTIBANCO. Um cartão de serviço pode ser:
  - **Universal -** Este tipo de cartão pode aceder à Rede CA e TPA MULTIBANCO;
  - **Pagamento automático –** Cartão com o princípio de funcionamento atrás descrito e cujo âmbito de acesso é apenas à Rede TPA MULTIBANCO. Este cartão é expulso quando introduzido na Rede CA MULTIBANCO, excepto se o Emissor pretender que se mantenham disponíveis algumas das seguintes operações:
    - Alteração de PIN;
    - Consulta a movimentos de baixo valor;
    - Consulta a NIB (Número de Identificação Bancária).
  - **Serviço CA –** Cartão que apenas acede à Rede CA MULTIBANCO, sendo rejeitado sempre que utilizado na Rede TPA MULTIBANCO;
  - **Sector –** Cartão que só acede à Rede TPA MULTIBANCO instalados em estabelecimentos pertencentes a um determinado tipo de actividade económica (por exemplo, terminais instalados em estações de serviço gasolineiras ou restaurantes). O acesso à Rede CA MULTIBANCO está limitado às seguintes operações:
    - Alteração de PIN;
    - Consulta a movimentos de baixo valor;

- Consulta a NIB;
- Via Verde, dependente do código do sector de actividade do Comerciante.

▪ **Comerciante –** Cartão que apenas pode ser utilizado nos TPA instalados em estabelecimentos de uma dada rede comercial. Quando o cartão é emitido é indicada a identificação do Comerciante em causa.

- **Rede privada** - Cartão de utilização restrita aos TPA instalados num estabelecimento ou numa cadeia de estabelecimentos comerciais de uma entidade com a qual o Emissor estabelece um contrato para a emissão e utilização desses cartões. Este cartão também é aceite na Rede CA MULTIBANCO, podendo efectuar as seguintes operações, desde que estas se encontrem disponíveis para o respectivo BIN:
  - Alteração de PIN;
  - Consulta de saldos;
  - Consulta de movimentos;
  - Consulta às operações MB.

3.4.2 Tipos de produção

No âmbito dos Serviços para Emissores, a SIBS FPS suporta os seguintes tipos de produção:

- **Cartão personalizado** - Cartão que foi produzido para um cliente específico, a pedido deste ou por iniciativa do Emissor, e que possui uma conta associada;
- **Cartão não personalizado** - Cartão que, estando emitido, não tem ainda uma conta associada. Neste tipo de produção, o cliente interessado no produto pode levantá-lo no primeiro contacto com o balcão do Emissor. O Titular de Cartão não possui o seu nome sobre o cartão devendo usar o painel de assinatura. Os dados da conta são informados posteriormente pelo Emissor para actualização do cartão;
- ***Instant issuing*** - Cartão não personalizado ou pré-produzido que, estando emitido, não possui ainda uma conta associada. Os dados da conta são informados num momento posterior pelo Banco para actualização no cartão. O Banco procede à associação da conta e ao *embossing* do plástico no momento da entrega ao Titular do Cartão.

3.4.3 Marcas

A SIBS FPS disponibiliza a emissão lógica de cartões bancários de várias marcas, de acordo com as opções escolhidas pelo Emissor:

- MB;
- MB SPOT;
- VISA;
- MasterCard;

- American Express (AMEX);

Um cartão pode ser emitido com apenas uma das marcas acima referidas com a combinação de duas marcas (marca MB e/ou MB SPOT e uma das marcas de SPI) dando origem a um cartão *co-branded*. Nos cartões *co-branded* existe uma marca principal (a marca internacional, colocada na face do cartão (e também no verso, no caso dos cartões multi-aplicação)) e uma marca secundária (a marca MB e/ou MB SPOT, colocada no verso). Este aspecto determina o modo como um cartão *co-branded* é reconhecido nos terminais que realizam operações, as operações disponibilizadas no menu do terminal e os custos / proveitos associados à transacção, entre outras funcionalidades.

3.4.3.1 Funcionamento de um cartão de marca MB / MB SPOT *(on-us)*

Um cartão MB e/ou MB SPOT é visto como cartão MB e/ou MB SPOT na Rede CA e TPA MULTIBANCO. Noutras redes, caso o cartão não tenha associado mais nenhuma marca de pagamento, o cartão não funciona pois não é reconhecido como um cartão válido para essa rede.

A SIBS FPS é o suporte quer à emissão lógica de cartões pelos Emissores participantes, quer à interligação da Rede CA e TPA MULTIBANCO.

3.4.3.2 Funcionamento de um cartão de marca internacional *(on-us)*

Um cartão de marca internacional é visto como um cartão dessa marca na Rede CA e TPA MULTIBANCO. Noutras redes, o cartão também é reconhecido no âmbito dessa marca, caso a mesma seja aceite nessa rede.

O Emissor tem de indicar ao respectivo SPI qual é o seu processador para autorização de operações realizadas nos terminais de aceitação da marca respectiva. O Emissor possui ainda a opção de indicar a SIBS FPS como seu processador e, nesse caso, a SIBS FPS assegura a autenticação do cartão e o envio do pedido de autorização para o Emissor em *real-time* (ou aplicação de outro cenário de autorização – ver secção 4.8.1.2), de forma semelhante à utilização do cartão na Rede MULTIBANCO.

Nas redes dos SPI, para além do suporte mencionado anteriormente, a SIBS FPS assegura a ligação à Rede CA e TPA MULTIBANCO dos respectivos *Acquirers* domésticos através do SPI do qual estes são aderentes.

3.4.3.3 Funcionamento de um cartão *co-branded (on-us)*

Um cartão *co-branded* é um cartão que junta dois ou mais Sistemas de Pagamento: MB e/ou MB SPOT e marca internacional. Consoante a rede em que esteja a operar, o cartão terá um determinado funcionamento. Na Rede MULTIBANCO o cartão *co-branded* é visto de diferentes formas mediante o canal:

- CA - As marcas MB ou MB SPOT são prioritárias na utilização de um cartão *co-branded* neste ambiente;
- TPA - O que define a forma de utilização do cartão *co-branded* é o acordo que o Comerciante estabeleceu com o *Acquirer* para o terminal.

A emissão lógica de cartões *co-branded* permite a realização de transacções na Rede CA e TPA MULTIBANCO (ver secção 4.6) e ainda em canais como a Internet (MB NET e *homebanking*) ou a rede móvel (MB PHONE), de acordo com as condições previamente parametrizadas pelo Emissor.

O Emissor tem ainda a opção de indicar a SIBS FPS como seu processador e, nesse caso, a SIBS FPS assegura a autenticação do cartão e o envio do pedido de autorização para o Emissor (ou aplicação de outro cenário de autorização – ver secção 4.8.1.2), de forma semelhante à utilização do cartão na Rede CA e TPA MULTIBANCO.

3.4.4 Tipo de tecnologia

Cada cartão corresponde a um plástico que serve de suporte físico aos suportes digitais e/ou magnéticos de dados (*chip* e/ou pista / banda magnética), aos suportes corporativos (marcas, logótipos, nomes, *layouts*), aos suportes pessoais (nome do titular) e suportes de segurança (número do cartão, data de validade, hologramas, chaves de segurança e outros elementos).

3.4.4.1 Pista / banda magnética

A componente de pista / banda magnética inclui informações sobre o cartão que, uma vez enviadas ao Emissor, permitem validar o cartão e o respectivo titular, e autorizar ou não uma transacção. A pista / banda magnética é lida por contacto físico ao ser passada por um terminal equipado com uma cabeça de leitura.

As pistas / bandas magnéticas podem ser de dois tipos: alta coercividade (Hi-Co) ou baixa coercividade (Lo-Co). As pistas / bandas magnéticas Hi-Co são mais resistentes do ponto de vista de desmagnetização e, por isso, mais apropriadas para cartões que são utilizados frequentemente ou que seja esperada uma duração de vida maior.

3.4.4.2 *Chip EMV*

O *standard* EMV representa uma plataforma tecnológica baseada num conjunto de especificações desenvolvidas e acordadas pelos SPI. As tecnologias de segurança subjacentes à produção de cartões com *chip* EMV são as seguintes:

- ***SDA (Static Data Authentication)*** - O *chip* SDA utiliza chaves públicas de infra-estrutura para verificar se o conteúdo do *chip* de um cartão condiz com a sua assinatura digital;
- ***DDA (Dynamic Data Authentication)*** - À semelhança do SDA, o *chip* DDA procede a uma verificação do conteúdo do *chip* de um cartão. Esta tecnologia também detecta se um cartão EMV foi copiado e contrabandeado através de um mecanismo adicional de validação que obriga o cartão a responder correctamente a um teste específico relativo à informação do cartão.
  O *chip* DDA gera uma assinatura digital usando dados específicos da transacção que são validados pelo terminal, protegendo o Titular de Cartão e Emissor de situações de fraude;
- ***CDA (Combined Dynamic Data Authentication)*** – O *chip* CDA é o método de autenticação mais avançado e seguro utilizável na emissão lógica de um cartão. O CDA é similar ao DDA com a

vantagem adicional de validar a autenticidade do criptograma aplicacional do cartão, o que assegura que o criptograma não foi corrompido.

3.4.4.3 *Contactless*

Os cartões *contactless* são emitidos com duas interfaces: *contactless* e contacto. Estes cartões possuem um *chip* EMV, uma banda magnética e uma antena RFID que integra a tecnologia *contactless*.

As funcionalidades de pagamento da vertente *contactless* são idênticas às que existem na vertente de contacto do cartão, isto é, podem funcionar como qualquer outro cartão. A utilização da vertente *contactless* do cartão faz-se através da simples aproximação do cartão a um leitor / terminal também *contactless*, isto é, sem que seja necessário o contacto físico entre o cartão e o terminal. O Titular de Cartão não tem que introduzir o PIN e nunca deixa de ter o cartão na sua posse.

Os cartões *contactless* são emitidos com parâmetros *offline* definidos pelo Emissor (através do formulário "Caracterização de BIN"), de acordo com as regras EMV e as normas definidas pelos SPI.

3.4.5 PIN

O PIN (*Personal Identification Number)* é um código secreto, pessoal e intransmissível, que permite autenticar a identidade do detentor de um cartão na Rede CA e TPA MULTIBANCO e em outras redes. Este código é gerado durante o processo de emissão lógica de cartões, sendo posteriormente enviado ao Titular de Cartão através de uma carta remetida pelo Emissor do cartão ou directamente pelo Personalizador, nos casos aplicáveis.

3.4.6 *CVM List*

A *Cardholder Verification Method List* (*CVM List*) é um dos parâmetros do *chip* do cartão que é gravado aquando da sua personalização lógica e física, não podendo ser alterado ao longo da vida do cartão. Este parâmetro informa o terminal dos métodos de autenticação do Titular de Cartão que podem ser executados pelo cartão.

Existem *CVM List* diferentes para cada tipo de cartão, consoante as aplicações de pagamento emitidas no cartão (MB, MB SPOT, VISA, VISA Electron, MasterCard, Maestro, AMEX). Um cartão terá tantas *CVM List* quantas as aplicações de pagamento existentes no *chip* (por exemplo, aplicação de SPI, aplicação de MB e aplicação *contactless*), podendo a *CVM List* assumir os valores apresentados no formulário "Caracterização de BIN" e seleccionados pelo Emissor (com excepção do *contactless* que apenas tem 1 CVM).

Sempre que um Emissor decida seleccionar outra *CVM List*, deve submeter o BIN para certificação do respectivo SPI.

Cada TPA possui uma chave de identificação única que é atribuída no momento do registo do terminal no sistema da SIBS FPS. O tipo de TPA utilizado determina as funcionalidades que se encontram disponíveis

para cada Comerciante, só sendo permitido o registo de terminais de marcas / modelos certificados pela SIBS.

O cartão possui informação, por aplicação de pagamento, dos métodos de autenticação que permite, sendo sempre o cartão que indica ao TPA a ordem da autenticação a realizar durante a operação.

Cada marca do cartão tem uma CVM própria e consoante as marcas suportadas pelo TPA é lida a CVM da marca associada a esse cartão. Uma parte do parque de terminais da Rede TPA MULTIBANCO lê a aplicação MB (TPA com acordos exclusivos MB) e a restante a aplicação de marca internacional (TPA com acordos de marcas internacionais). No segundo caso, se o TPA suportar tecnologia *contactless* e for esse o modo de pagamento, a CVM a aplicar é a do *contactless*.

No início de uma transacção estabelece-se um diálogo dinâmico entre o cartão e o TPA. A primeira etapa passa pela selecção da aplicação de pagamento que vai ser utilizada na operação, com o cartão a indicar ao terminal qual é o primeiro método de autenticação que pretende utilizar. Se o TPA tiver parametrizado esse método é feita a autenticação do Titular de Cartão; em caso contrário, o terminal informa o cartão de que não possui esse método parametrizado devendo o cartão indicar uma segunda opção em termos de autenticação. Este diálogo entre cartão e TPA prossegue até surgir um emparelhamento da CVM, ou seja, até se encontrar um método de autenticação de Titular de Cartão comum ao cartão e TPA.

3.4.7 Cartões não bancários

Na SIBS FPS é também possível a emissão de cartões sem uma conta bancária associada, o qual pode ser utilizado por Emissores de cartões ou outras entidades. Para este tipo de produção são necessários os mesmos requisitos indispensáveis à emissão de cartões bancários, exceptuando os tipos de ficheiro a entregar para a produção (ver Manual de Implementação dos Serviços para Emissores).

Na contratação do serviço de emissão de cartões não bancários, o Emissor pode optar por duas modalidades distintas:

- **Com processamento SIBS** - Cartões com ou sem função de pagamento (universitários, redes privadas, cartões com Sistema de Autenticação Forte/MB CODE, entre outros) e parqueados na base de dados SIBS;
- **Sem processamento SIBS** - Cartões com ou sem função de pagamento enviados pela SIBS FPS directamente para o Personalizador.

Quadro 2 - Apresentação de conceitos dos Serviços para Emissores

- Existe um conjunto de conceitos associados aos serviços de emissão que a SIBS FPS disponibiliza aos seus Emissores que são originários de definições processuais e parametrizações necessárias ao bom funcionamento do serviço.
- O cálculo lógico diz respeito à geração de dados para funcionamento do cartão, de segurança e o parqueamento de cartões representa o carregamento de dados de cartão de um Emissor na base de dados da SIBS FPS.
- Para que o cálculo lógico e o parqueamento de cartões sejam realizados, o Emissor tem de registar um conjunto de elementos necessários à parametrização dos cartões a emitir, através do preenchimento dos formulários “Caracterização do Emissor”, “Caracterização do Centro de Processamento de Dados (CPD) do Emissor”, “Caracterização do Padrão EMV” e “Caracterização do BIN”.
- A SIBS FPS faz uma distinção entre os cartões parqueados na sua base de dados (cartões *on-us*), para os quais disponibiliza um serviço de processamento e um conjunto de funcionalidades, e cartões sobre os quais apenas possui informações base guardadas (cartões *not-on-us*).
- A SIBS FPS realiza a emissão de cartões de crédito, débito ou mistos que podem ter uma utilização genérica (onde o cartão é usado de forma livre e de acordo com o que está parametrizado pelo Emissor) ou uma utilização restrita (cartões de serviço – universal, pagamento automático, serviço CA, sector, Comerciante – ou cartões de rede privada).
- Os tipos de cartões descritos anteriormente podem ser emitidos já personalizados (já com dados de Titular de Cartão), por personalizar (sem dados de Titular de Cartão) ou através de *instant issuing* (em que os dados de Titular de Cartão são registados no cartão no acto da respectiva entrega ao Titular).
- A SIBS FPS processa cartões das seguintes marcas:
  - MB;
  - MB SPOT;
  - VISA;
  - MasterCard;
  - American Express (AMEX).

  Os cartões podem ter apenas uma marca ou serem *co-branded* (cartões que reúnem a marca MB ou MB SPOT e uma das marcas de SPI).
- Em termos de tecnologia, um cartão é composto por *chip* EMV, podendo este ser SDA (*Static Data Authentication*), DDA (*Dynamic Data Authentication*) ou CDA (*Combined Dynamic Data Authentication*), e/ou por banda / pista magnética, podendo esta ser Lo-Co ou Hi-Co.

- Adicionalmente, um cartão EMV pode ser emitido com tecnologia *contactless* que permite a realização de pagamentos através da aproximação do cartão a um POS sem que o Titular de Cartão introduza PIN.
- O PIN é um código secreto, pessoal e intransmissível gerado durante o processo de emissão lógica do cartão.
- Durante o processo de emissão lógica, o cartão é gerado também com base nas características de produto que o Emissor definiu no formulário "Caracterização de BIN", onde indicou qual a *CVM List* a aplicar. A CVM é um parâmetro que regista os métodos de autenticação do Titular de Cartão que o Emissor decide usar e que é comunicado ao terminal para que este possa aceitar ou não um dos métodos do cartão.
- A SIBS FPS disponibiliza também a emissão de cartões não bancários, cartões sem uma conta bancária associada.

4 Serviços para Emissores

Para qualquer Emissor, a SIBS FPS dispõe de um conjunto de serviços e funcionalidades que podem ser relacionadas entre si e que percorre a cadeia de valor associada à gestão do ciclo de vida de um cartão e processamento e autorização das suas operações.

A disponibilização destes serviços estão assentes na troca de ficheiros e mensagens entre a SIBS FPS, o Emissor e outros intervenientes. A descrição do *layout* destes interfaces está descrita no documento Manual de Implementação - Serviços para Emissores.

4.1 Emissão de Cartões Bancários

A emissão de um cartão pode ser dividida em duas fases: emissão lógica e emissão física. A SIBS FPS fornece aos seus Emissores a vertente de emissão lógica dos seus cartões e integração com os personalizadores que efectuam a vertente de emissão física dos cartões.

4.1.1 Emissão lógica de cartão bancário

A emissão de um cartão com as características pretendidas pelo Emissor implica que este seja devidamente caracterizado antes de se iniciarem as tarefas para a sua execução.

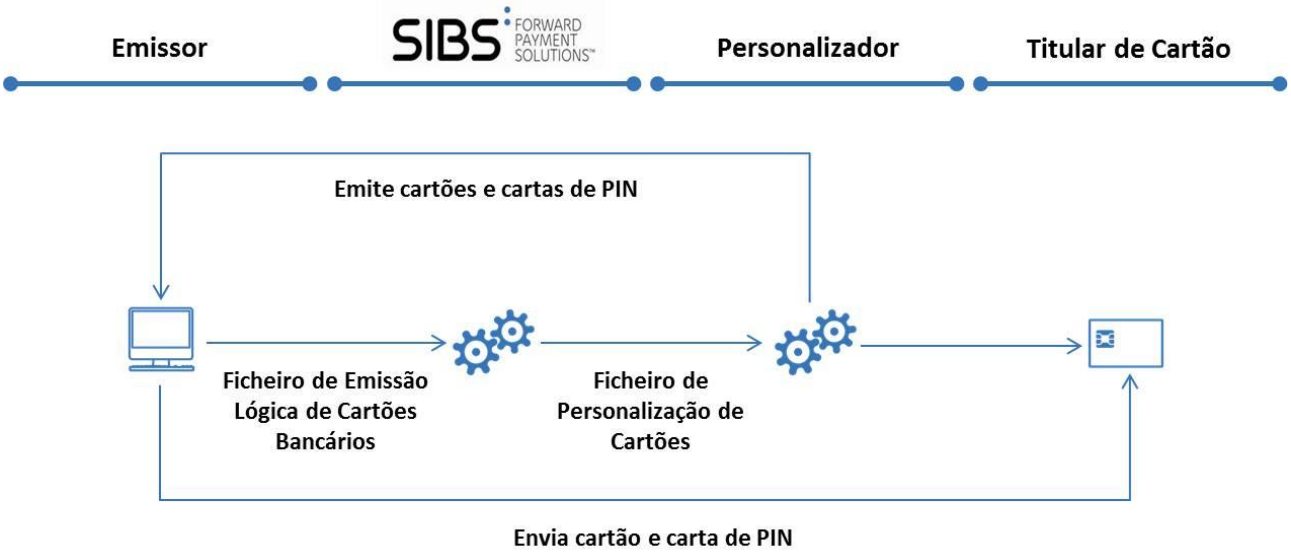

Figura 5 - Emissão de cartões bancários

O primeiro passo para o início do processo de emissão é a recepção de um ficheiro de produção de cartões - Ficheiro ELCB – Emissão Lógica de Cartões Bancários. O processamento do ficheiro recepcionado (caso

não se trate de uma produção urgente) será realizado de acordo com os horários de processamento descritos na secção 4.3.

A aplicação de produção de cartões é suportada por duas fases de processamento distintas: a primeira é relativa à recepção e validação dos ficheiros e a segunda relativa ao processamento lógico e geração dos dados lógicos a incluir no cartão e aos respectivos *outputs*.

- **RECEPÇÃO DE FICHEIROS**

  O ficheiro ELCB - Emissão Lógica de Cartões Bancários remetido pelos Emissores chega à SIBS via *File Transfer* e é submetido automaticamente à aplicação de cartões.

  De seguida, o ficheiro é submetido a um conjunto de validações genéricas, tais como: verificação da sequência de ficheiro, verificação se produção é urgente e validação da formatação dos registos.

  Se o ficheiro não cumpre alguma das validações indicadas, transita para a fase seguinte, na qual é criado o correspondente ficheiro CFER - Confirmações e Erros do ficheiro ELCB que é enviado para o Emissor como retorno e o processamento é terminado. Caso o ficheiro cumpra todas as validações, transita para a fase seguinte.

  As informações adicionais para efeitos de personalização do cartão são enviadas pelo Emissor directamente ao Personalizador através dos ficheiros DACB – Dados Adicionais de Cartões (cartões bancários) e/ou ficheiro IMGB – Imagens de Cartões (cartões bancários).

- **PROCESSAMENTO LÓGICO**

  A passagem a esta fase de processamento é efectuada automaticamente mediante a validação do seguinte conjunto de regras:

  - Cálculos de segurança (PVV, CCD, CVV com base nas chaves EMV);
  - Carregamento na base de dados de cartões (caso o Emissor tenha contratado o parqueamento dos seus cartões junto da SIBS FPS).

  Estando presentes todos os ficheiros necessários à produção em causa, verifica-se se a infra-estrutura de segurança está disponível. Se não existirem módulos de segurança disponíveis para o processamento lógico, o ficheiro fica em espera até ser possível o respectivo acesso.

  Se as validações descritas forem concluídas com sucesso, e se estiverem satisfeitas as condições necessárias, dá-se início ao processamento lógico.

  A emissão lógica dos cartões é efectuada com os parâmetros *offline* a zeros, sempre que o cartão é emitido no estado “Por activar” ou “Por activar, activável em CA”. Esses parâmetros são incorporados no chip do cartão através de um *script* que apenas é enviado pela SIBS FPS aquando da primeira transacção do cartão, feita *online* e com PIN.

- ***OUTPUTS* DO PROCESSAMENTO LÓGICO**

  Após o fim do processo de carregamento da base de dados, o Emissor recebe o ficheiro CFER - Confirmações e Erros do ficheiro ELCB e o Emissor ou Personalizador (por delegação do Emissor) recebe o ficheiro PERS - Personalização de Cartões.

O Emissor deve negociar com um Personalizador um contrato de produção de cartões que inclui todas as características inerentes à produção do cartão e da carta de PIN[1]. A SIBS FPS sabe qual é o Personalizador a enviar o ficheiro PERS - Personalização de Cartões mediante a prévia apresentação do contrato de produção de cartões. A identificação deste contrato tem de ser informada à SIBS FPS em cada envio de um ficheiro de produção de cartões.

4.1.1.1 Operativa em descontinuação

Na operativa de produção de cartões que se encontra em fase de descontinuação, a emissão lógica de cartões bancários diferencia-se da operativa anteriormente descrita quer ao nível dos ficheiros processados, quer dos processos adoptados pelos diversos intervenientes.

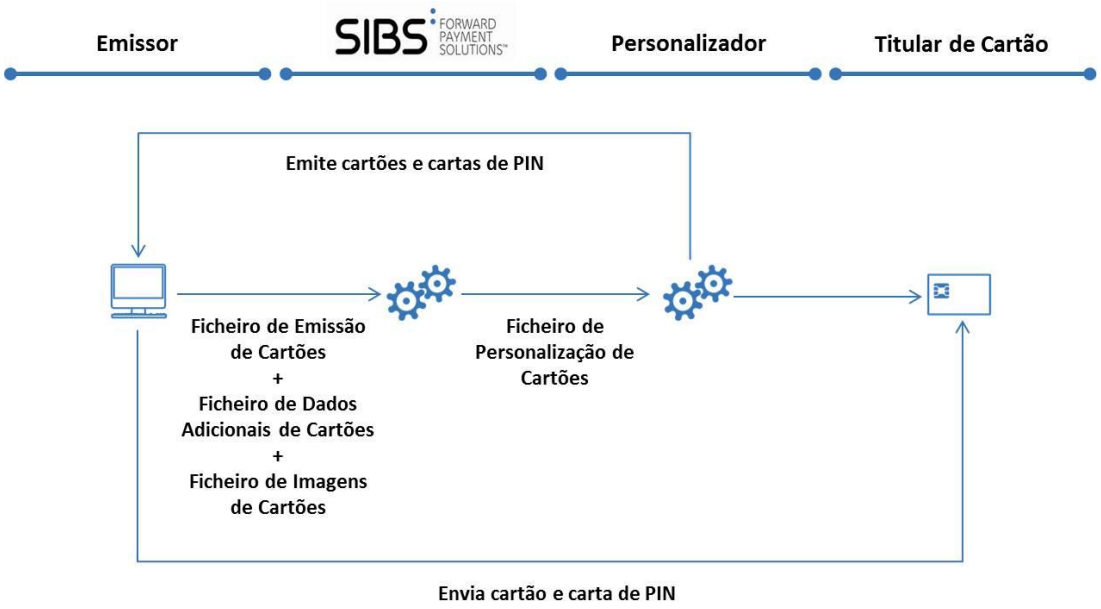

Figura 6 - Emissão de cartões bancários (operativa em descontinuação)

O primeiro passo para o início do processo de emissão é a recepção de um ficheiro de produção de cartões - Ficheiro EECB – Emissão de Cartões. O processamento do ficheiro recepcionado (caso não se trate de uma produção urgente) será realizado de acordo com os horários de processamento descritos na secção 4.3..

A aplicação de produção de cartões, é suportada por duas fases de processamento distintas: a primeira é relativa à recepção e validação dos ficheiros e a segunda relativa ao processamento lógico e aos respectivos *outputs*.

- **RECEPÇÃO DE FICHEIROS**

  Os ficheiros de produção de cartões remetidos pelos Emissores chegam à SIBS via *File Transfer* e são submetidos automaticamente à aplicação de cartões.

[1] Actualmente, só o Personalizador SIBS CARTÕES está certificado para emissão de cartas PIN.
O personalizador pode definir com o Emissor um ficheiro de retorno próprio.

De seguida, os ficheiros são submetidos a um conjunto de validações genéricas tais como: verificação da sequência de ficheiro, verificação da existência de contrato de produção de cartões (e se o mesmo é válido para a produção em causa), verificação se o contrato implica tratamento urgente e validação da formatação dos registos. Para o ficheiro EECB - Emissão de Cartões, verifica-se através do contrato a eventual necessidade de outros recursos - ficheiro DACB – Dados Adicionais de Cartões (cartões bancários) e/ou ficheiro IMGB – Imagens de Cartões (cartões bancários).

Se os ficheiros não cumprem alguma das validações indicadas, transitam para a fase seguinte na qual são criados os correspondentes ficheiros EERR – Erros de Cartões, DACB – Dados Adicionais de Cartões (cartões bancários) e/ou ficheiro IMGB – Imagens de Cartões (cartões bancários) que são enviados ao Emissor como retorno e o processamento é terminado. Caso os ficheiros cumpram todas as validações, transitam para a fase seguinte.

- **PROCESSAMENTO LÓGICO**

  A passagem a esta fase de processamento é efectuada automaticamente mediante a validação do seguinte conjunto de regras:

  - Caso se aplique, verifica-se se já foram recepcionados todos os ficheiros necessários à produção em causa;
  - Efectua cálculos de segurança (PVV, CCD, CVV com base nas chaves EMV);
  - Efectua carregamento na base de dados de cartões (caso o Emissor tenha contratado o parqueamento dos seus cartões junto da SIBS FPS).

  Estando presentes todos os ficheiros necessários à produção em causa, verifica-se se a infra-estrutura de segurança está disponível. Se não existirem módulos de segurança disponíveis para o processamento lógico, o ficheiro fica em espera até ser possível o respectivo acesso.

  Se as validações descritas forem concluídas com sucesso, e se estiverem satisfeitas as condições necessárias, dá-se início ao processamento lógico.

- **OUTPUTS DO PROCESSAMENTO LÓGICO**

  Após o fim do processo de carregamento da base de dados, os seguintes ficheiros são formatados e remetidos aos Emissores:

  - Ficheiro ECCF - Confirmação de Cartões;
  - Ficheiro IPER e IPIN, para personalizador SIBS Cartões;
  - Ficheiro PEMV - Personalização de Cartões EMV e EELC – Personalização de Cartões com pista, para outros personalizadores;
  - Ficheiro EERR - Erros de Cartões.

  Os ficheiros ECCF - Confirmação de Cartões e EERR - Erros de Cartões são enviados ao Emissor em todos os casos.

4.1.2 Emissão de PIN

A geração de um *pinblock* ocorre no mesmo momento de geração de dados do cálculo lógico do cartão. Na base de dados da SIBS FPS, os dois números gerados – número de cartão e número de *pinblock* – ficam automaticamente associados, pelo que não existe o conceito de produção diferida. Os Emissores que pretenderem a existência de diferimento terão de negociar um acordo com o Personalizador neste sentido.

4.1.2.1 Guarda de *pinblock*s

Este serviço, parametrizado no formulário "Caracterização de BIN", consiste em guardar na SIBS FPS um ficheiro com a informação referente aos *pinblock*s (PIN cifrados) associados aos cartões.

Através desta funcionalidade, os Emissores disponibilizam aos seus clientes cartões cujo PIN se mantém constante em emissões subsequentes (renovações e/ou substituições). Na eventual alteração do PIN por parte do Titular de Cartão, a informação relativa ao respectivo *pinblock* é actualizada na base de dados da SIBS FPS. A guarda de *pinblocks* só está disponível para cartões bancários.

4.1.2.2 Emissão de PIN aleatórios

A emissão de PIN aleatórios consiste na produção massiva de *pinblocks* sem que estes estejam associados a um número de cartão. Após emissão física, este processo permite ao Emissor ter na sua posse cartas de PIN que poderá entregar ao Titular de Cartão no momento da requisição de um cartão bancário. Na carta de PIN está inscrita uma referência que tem de ser enviada à SIBS FPS no pedido da emissão lógica do cartão correspondente ao Titular de Cartão.

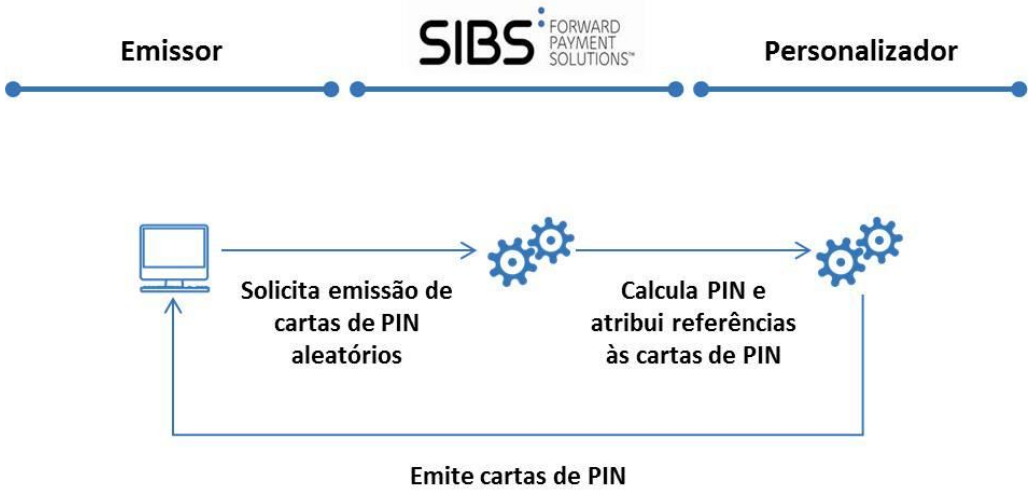

Figura 7 - Emissão de PIN aleatórios

As diferentes conjugações possíveis entre a emissão de um cartão, a carta de PIN e a guarda de *pinblock* são apresentadas na tabela a seguir:

Tabela 2 - Combinações de emissão de cartão, carta de PIN e guarda de *pinblock*

Emissão do cartão	Tipo de emissão	Emissão de carta de PIN	Guarda de *pinblock*
Sem guarda de *pinblock*	Novo	Sim	Não
	Renovação ou substituição	Sim	Não
Com guarda de *pinblock*	Novo	Sim	Sim
	Renovação ou substituição	Não	O PIN mantém-se
	Renovação ou substituição	Sim	Sim
Com utilização de carta de PIN aleatório	Novo	Carta de PIN emitida previamente	No momento da emissão da carta de PIN
	Renovação ou substituição	Não	O PIN mantém-se
	Renovação ou substituição	Carta de PIN emitida previamente	No momento da emissão da carta de PIN

4.1.2.3 Reatribuição de PIN

A funcionalidade de Reatribuição de PIN permite aos Emissores associar um novo PIN para um cartão emitido e já em circulação, cujo titular perdeu a noção do PIN que lhe estava associado. A utilização deste serviço pressupõe que o Emissor detém uma carta de PIN aleatória para associar ao cartão já existente, o que significa que já tem subscrito o serviço de guarda de *pinblock* junto da SIBS FPS, parametrizado ao nível do formulário "Caracterização de BIN".

A guarda do *pinblock* é realizada no momento da geração aleatória de PIN. Aquando da associação da carta de PIN a cartão, a SIBS FPS fará corresponder ao cartão o *pinblock* anteriormente guardado.

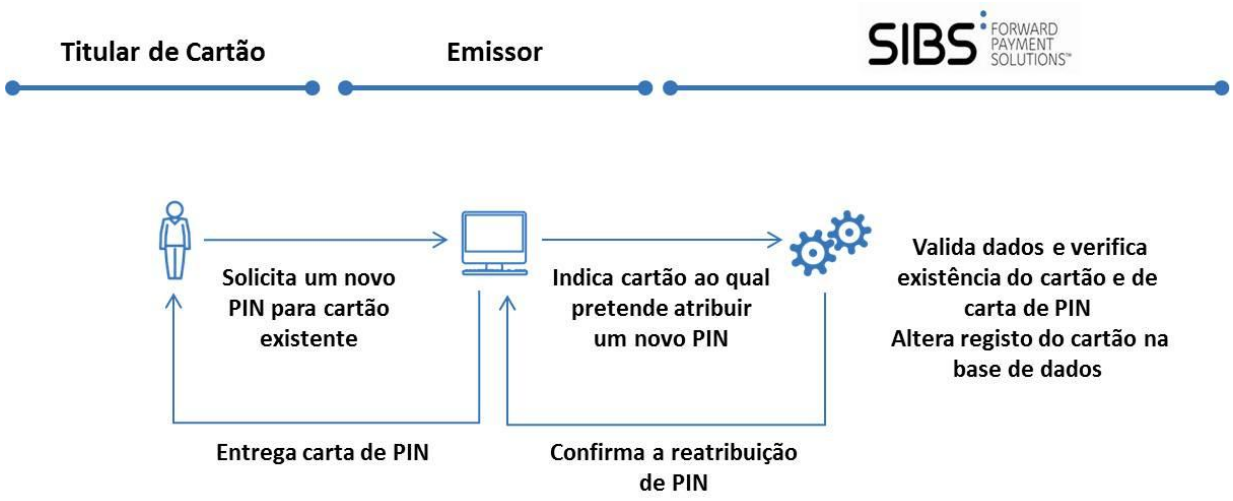

Figura 8 - Reatribuição de PIN

Para obter a funcionalidade desejada o Emissor deverá enviar à SIBS FPS uma mensagem (via *Host-to-Host*), indicando qual o cartão para o qual é pretendido a associação de um novo PIN e qual a identificação da carta de PIN a associar (previamente em posse do Emissor).

Na sequência da recepção deste pedido, o sistema central da SIBS FPS realiza as validações necessárias a este processo, nomeadamente:

- Verifica se a carta de PIN indicada existe para o Emissor que realiza o pedido (*pinblock* em base de dados);
- Verifica se esta carta de PIN já não está atribuída a um outro cartão;
- Verifica se o cartão indicado existe;
- Verifica se o cartão está em situação normal.

Caso alguma destas validações origine um erro no processamento, o pedido é recusado e apresentado o respectivo motivo via mensagem de resposta, de acordo com as validações acima expostas.

Tendo sucesso nas validações descritas, serão realizadas as seguintes acções:

- Alteração ao registo de cartão na base de dados;
- Criação de dados para reescrita da pista em CA MULTIBANCO (cartões Lo-Co);
- Criação de dados para envio de *script* para o chip (cartões EMV - Hi-Co);
- Enviar ao Emissor na mensagem de resposta *Host-to-Host* os novos valores dos *Personal Validation Values* (PVV's).

Dado que o pedido de associação de novo PIN ao cartão é um processo *online*, o Emissor receberá logo a confirmação se o pedido teve sucesso ou não, e qual o respectivo motivo no caso de recusa.

A SIBS FPS informa e confirma a operação *Host-to-Host* na compensação, através do ficheiro DST5. Neste caso, a operação terá o valor "RNP" como código CODTRN e valor "zeros" no atributo MODENV. Os novos PVVs são enviados ao Sistema de Pagamento com base num processo *batch* que corre diariamente após os actuais fechos/subfechos de compensação na SIBS, ou seja, cerca das 09h00, 15h00 e 20h00.

Uma operação que seja efectuada fora da Rede MULTIBANCO e que seja efectuada em stand-in na MasterCard/VISA, só terá sucesso após a MasterCard/VISA ter actualizado o seu ficheiro com o novo valor de PVV.

Após uma Reatribuição de PIN, o Emissor deve indicar ao cliente que este deve proceder de imediato a uma transacção na Rede CA MULTIBANCO, para que, no caso de cartões com PIN no chip (offline PIN), o PIN também seja actualizado no cartão.

4.1.3 Cartões EMV não personalizados

A emissão lógica de cartões EMV não personalizados possibilita aos Emissores entregar directamente aos seus clientes um cartão bancário não personalizado ou personalizado no momento em que o mesmo é solicitado nos balcões do Banco. Não existe diferença da emissão lógica de cartões EMV não personalizados face a outras emissões, ou seja, é sempre criado um *pinblock*, ficando a emissão de PIN dependente do que ficar estabelecido no contrato com o Personalizador.

A emissão lógica de cartões EMV não personalizados tem como princípio base a produção de cartões cuja informação relativa ao Titular de Cartão (nome e número de conta) não se encontra gravada no cartão aquando da sua emissão física. Este serviço não tem restrições de marca ou tecnologia de cartão e os

cartões emitidos por este serviço podem, posteriormente, ser personalizados fisicamente recorrendo a gravadores existentes a nível do Balcão (funcionalidade *Instant Issuing*).

O Emissor procede à actualização dos dados no cartão no momento da entrega do cartão físico ao seu cliente. Para o cliente activar o cartão ser-lhe-á entregue uma carta de PIN, previamente emitida, que o Emissor associou ao cartão entregue. O Emissor terá de informar a SIBS FPS do nome e número de conta do Titular de Cartão de acordo com os canais existentes.

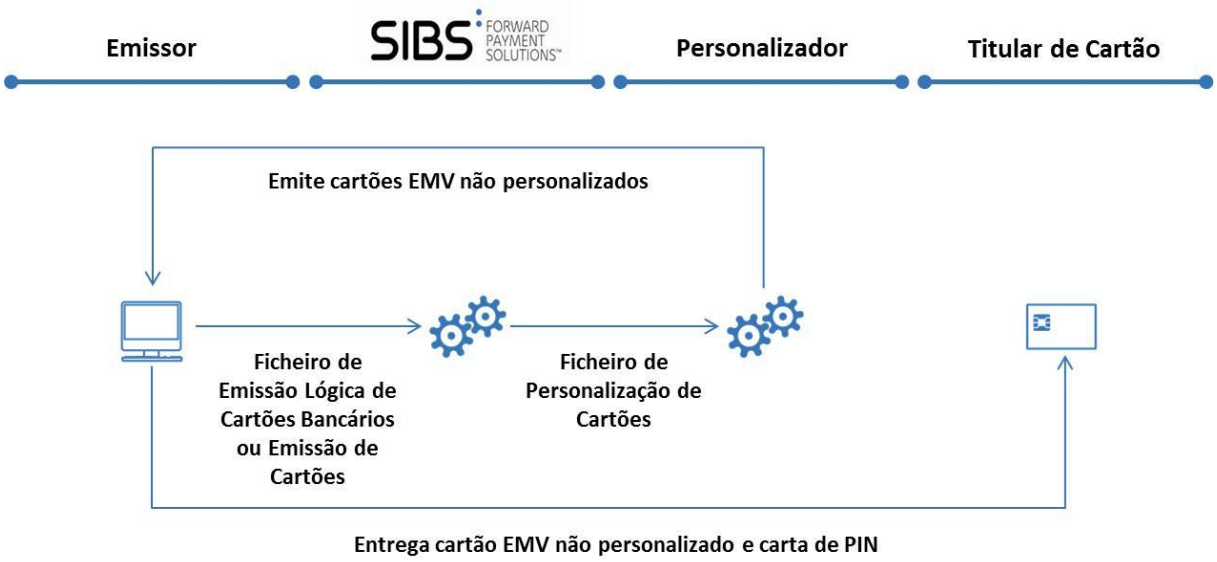

Figura 9 - Emissão de cartões EMV não personalizados

O serviço de emissão lógica de cartões EMV não personalizados assenta nas seguintes etapas:

- O Emissor envia um ficheiro ELCB – Emissão Lógica de Cartões Bancários ou EECB – Emissão de Cartões para a SIBS FPS com o nome do titular e número de conta preenchidos com valores predefinidos (espaços ou zeros dependendo do tipo de campo) e com um número de contrato previamente acordado com o Personalizador;
- A SIBS FPS executa a produção lógica dos cartões, gerando os dados necessários para a sua personalização física mas sem associar os cartões a um titular e uma conta bancária e deixando-os num estado inactivo;
- A SIBS FPS envia o ficheiro de personalização de cartões para o Personalizador com todos os dados preenchidos, excepto o nome do titular e o número de conta que são preenchidos com valores predefinidos (espaços ou zeros dependendo do tipo de campo);
- O Personalizador personaliza os cartões (*chip*, pistas / bandas magnéticas e CVV2). No interior do *chip*, o nome do titular e número de conta são escritos num ficheiro actualizável por *scripts*, a enviar posterior e remotamente ao cartão;
- O Personalizador envia os cartões pré-personalizados para os balcões dos Emissores ou outra opção acordada entre as partes.

A emissão lógica de cartões EMV não personalizados não tem restrições de marca ou de tecnologia de cartão, permitindo a produção de cartões de crédito e débito.

Após a recolha dos dados relativos ao Cliente ao qual será entregue o cartão, deverá ser associado um *pinblock* ao cartão (caso o cartão tenha sido emitido sem *pinblock)*, utilizando a funcionalidade de Reatribuição de PIN, passando o cartão a estar no estado "activo" na base de dados da SIBS FPS.

Os passos para esta associação de *pinblock* são:

- O Emissor actualiza os dados do cartão no sistema da SIBS FPS (via *Host-to-Host*), sendo gerada uma mensagem em *real-time* que envia o nome do titular, número de conta.
- Caso seja necessário associar um *pinblock*, deve ser enviada outra mensagem para a associação ao PAN no sistema central da SIBS FPS;
- Após a primeira autenticação do cartão na Rede CA MULTIBANCO com o PIN fornecido na carta PIN associada ao cartão, o cartão passa para o estado "Activo" na base de dados da SIBS FPS. No final da activação do cartão são enviados *scripts* de actualização dos dados do titular, restrições de conta e PIN no caso de cartões com *offline* PIN, para actualização do chip.

4.1.4 Cartões *contactless*

Os cartões bancários *contactless* permitem aos Emissores a emissão lógica de cartões com capacidade de efectuar pagamentos sem contacto e em *offline*, criando um serviço adicional ao Titular de Cartão. Por outro lado, permitem reduzir custos com processamento e telecomunicações nas operações de pagamento e o respectivo tempo de transacção. Estes cartões são utilizados para efectuar pagamentos de pequenas quantias, até ao valor máximo de 20 euros.

A utilização da vertente *contactless* faz-se com a simples aproximação do cartão a um leitor / terminal também *contactless*, isto é, sem que seja necessário o contacto físico entre o cartão e o terminal. O Titular de Cartão não tem que introduzir o PIN e nunca deixa de ter o cartão na sua posse. A emissão do recibo para o Titular de Cartão é opcional.

A actualização dos parâmetros *offline* do cartão é efectuada sempre que se verifique uma operação *online* (na Rede CA ou TPA MULTIBANCO) com contacto autorizada pelo Emissor. Quando o pagamento for inferior a um montante predefinido e o cartão já tiver esgotado o valor autorizado em *offline*, o terminal pede a inserção do cartão e introdução do PIN para a enviar em *online* para autorização, caso tenha essa componente activa.

O Emissor tem de tomar duas decisões relativas aos cartões a emitir, designadamente:

- Valor Máximo Acumulado (VMA) para o cartão efectuar transacções *offline*, sejam as transacções *contactless* ou com contacto (um só limite partilhado por ambas as operativas);
- Emitir cartão com antena para *contactless*.

Na altura da emissão, as capacidades *contactless* do cartão encontram-se inactivas. Uma vez que o cartão se encontre na posse do utilizador, aquelas capacidades serão automaticamente activadas aquando da primeira transacção efectuada *online* com contacto na Rede CA ou TPA MULTIBANCO.

Sempre que o cartão efectua uma operação com contacto e *online*, autorizada pelo Emissor, há lugar a um *reset* do valor acumulado de operações *offline* consecutivas. Os parâmetros de controlo de risco poderão nesse momento ser alterados no cartão, por ordem do Emissor.

O *upload* de transacções *contactless* para o sistema da SIBS FPS é executado através dos seguintes métodos:

- Manual (sempre que o Comerciante o desejar, acciona transacção específica para o efeito);
- *Online* (sempre que o terminal tenha de efectuar uma transacção *online* com o sistema da SIBS FPS, envia também a informação referente a transacções *offline* registadas desde o último *upload*);
- Ao fim de um determinado número de transacções acumuladas no terminal (adoptando 10 como o valor *default* mas passível de alteração pelo *Acquirer*);
- Automático no fecho (todas as operações de fecho do terminal passarão a despoletar automaticamente o envio das transacções *offline* - *contactless* incluídas – para a SIBS FPS).

Para as situações de falha do terminal, deve ser adoptado um processo alternativo de recuperação e registo ou *upload* das transacções para o sistema da SIBS FPS.

4.1.5 *Replacement cards*

Sempre que um cliente de um Banco se encontra no estrangeiro e fica impossibilitado de utilizar o seu cartão bancário devido a uma situação de extravio, de roubo ou mesmo de deterioração, poderá substitui-lo por um outro cartão. Este novo cartão que será entregue ao Titular de Cartão é designado como *replacement card*.

O processo para entrega de um *replacement card* inicia-se com o envio pelo Emissor de um ficheiro de produção de cartões onde é incluída uma tranche específica de cartões para serem utilizados como cartões de substituição. Após o correcto processamento do ficheiro, o Emissor altera o estado destes cartões para a situação de activo, parametriza-os de modo a que o cenário de decisão das suas operações seja sempre em modo de degradação (ver secção 4.8.1.2), e informa a SIBS FPS de quais os números a utilizar pelo serviço, sempre que um cliente solicitar a atribuição de um *replacement card*.

Deste modo, quando um Titular de Cartão entra em contacto com o respectivo SPI e solicita junto desta instituição a emissão de um novo cartão de substituição, o serviço de atendimento do SPI entrará em contacto com a SIBS FPS e informa o pedido do Titular de Cartão, facultando os elementos necessários para a sua correcta identificação no sistema do Emissor.

A SIBS FPS na posse destes elementos valida a exequibilidade do pedido e, através da funcionalidade existente no Portal de Serviços SIBS (PSS), associa o número de conta do cartão anterior ao *replacement card* e informa o SPI.

No final de cada turno, a SIBS FPS elabora um relatório de ocorrências, onde indicará os dados relevantes relativos ao pedido concretizado, nomeadamente com informação referente a: data/hora do pedido do Titular de Cartão; local onde se encontrava; nome do Titular de Cartão; número de cartão substituído; número de cartão de substituição; e outros elementos que o Emissor venha a solicitar.

O número de cartões que a SIBS FPS deve ter na sua posse será no mínimo três e no máximo oito. A responsabilidade da gestão de *stocks* é do Emissor que sempre que detectar que o número de *replacement card* chegou a três, deverá produzir uma nova tranche e informar a SIBS FPS dos novos cartões.

Um *replacement card* pode ser emitido com um BIN+EXT diferentes do BIN+EXT do cartão original.

Este serviço tem uma excepção relacionada com a emissão de um *replacement card* com extensão de BIN diferente do BIN original do cartão: caso o Emissor tenha como cenário de degradação para o BIN do cartão original o cenário de saldo disponível conta-crédito, os *replacement card* desse BIN+EXT tem de ser o mesmo que o cartão original.

4.1.6 Cartões multi-aplicação

O cartão multi-aplicação consiste num cartão físico que agrega duas aplicações de pagamento do mesmo SPI, permitindo que o Emissor possa oferecer aos seus clientes um cartão com várias funcionalidades de pagamento e que os titulares destes cartões possam escolher, em cada compra em TPA, qual das aplicações pretendem utilizar. No caso da MasterCard este produto denomina-se Combo Card e no caso da VISA, denomina-se VISA SimplyOne.

Este cartão tem a particularidade de ter dois números de cartão (PAN) associados, um por cada uma das aplicações de pagamento do SPI, que são classificados como cartão principal e secundário. No caso de um cartão VISA SimplyOne é possível qualquer combinação de marcas VISA, entre o cartão principal e secundário; no caso de um Combo Card, a aplicação principal tem de ser obrigatoriamente MasterCard (débito ou crédito) e a aplicação secundária pode ser MasterCard, Maestro ou Cirrus. O PAN associado à aplicação principal é apresentado na frente do cartão e tem os seus dados gravados quer ao nível do *chip*, quer ao nível da banda magnética do cartão. A aplicação secundária é apresentada na parte de trás do cartão e os seus dados estão presentes apenas ao nível do *chip*.

Adicionalmente à marca do SPI, o cartão principal, e apenas este, pode ter também mais uma, ou várias, das seguintes aplicações: MB, MB SPOT, CAP ou DAP, e *contactless.* Assim, e desde que o chip, obrigatoriamente[2] com tecnologia DDA, o suporte, o cartão pode ter até 6 aplicações.

Existem características comuns entre os dois cartões lógicos, suportados no mesmo cartão físico:

- ambos são emitidos com a mesma data de expiração;
- ambos são gerados com o mesmo *pinblock* e, consequentemente, têm o mesmo PIN. Quando o titular altera o PIN de um dos cartões, esse PIN novo passa a vigorar em ambos os cartões;
- ambos têm sempre o mesmo estado, sendo que a primeira activação é sempre efectuada sobre o cartão principal (ver secção 4.5.1).

Os seguintes dados não são partilhados entre os cartões, principal e secundário:

- parâmetros de risco *offline;*

[2] Conforme determinado pelos SPI.

- parâmetros de degradação;
- operações autorizadas;
- tentativas de PIN.

As operações *card present* realizadas com o cartão multi-aplicação são sempre efectuadas ao abrigo do cartão principal, com a excepção de quando está a transaccionar num TPA EMV com a funcionalidade de selecção, pelo cliente, da aplicação a utilizar. Neste caso o cliente pode escolher qual o cartão que pretende utilizar.

Relativamente às operações *card-not-present* existem as seguintes diferenças entre os cartões multi-aplicação das marcas VISA e MasterCard:

- Para os cartões VISA, quer o cartão principal quer o secundário, tem um código CVV2, distinto entre si, pelo que ambos podem ser usados em operações *card-not-present*. O CVV2 do cartão principal é apresentado no painel de assinatura; o CVV2 do cartão secundário é apresentado no verso do cartão, em local indicado pela VISA.
- para os cartões MasterCard, a utilização em operações *card-not-present* só pode ser feita a partir da aplicação principal, já que para a secundária não é gerado CVC2 no momento da emissão do cartão.

Um cartão multi-aplicação não pode ser *instant issuing,* nem *replacement card*.

É possível solicitar reatribuição de PIN para qualquer um dos cartões, desde que o Emissor tenha subscrito o serviço de guarda de *pinblock* junto da SIBS FPS.

A renovação dos cartões multi-aplicação é efectuada por PAN, como para qualquer outro cartão. Assim, quando o Emissor pretende renovar um cartão multi-aplicação, tem de enviar dois registos no ficheiro de Emissão Lógica de Cartões, um por cada PAN a renovar, devidamente preenchidos para o efeito.

4.1.7 Renovação e substituição de cartões

O período de utilização de um cartão pode ser prolongado através da sua renovação automática. Nos casos em que a renovação automática não é possível, a renovação é exclusivamente da responsabilidade do Emissor. A renovação e substituição de cartões pressupõem sempre o envio do ficheiro com o pedido de renovação do Emissor.

A renovação e substituição de cartões ocorre por decisão de um Emissor. Quando um cartão está perto de chegar à sua data de expiração, o Emissor pode optar por substituí-lo por qualquer outro tipo de cartão e enviá-lo para o Cliente mesmo antes da data de expiração do primeiro cartão. Um cartão pode ser substituído por qualquer outro cartão (seja débito ou crédito; seja VISA, MasterCard ou AMEX) e ambos os cartões podem estar simultaneamente activos.

Caso a substituição seja feita por um cartão com o mesmo produto / padrão, com as mesmas aplicações EMV, o novo cartão herda todos os parâmetros *offline* do anterior.

A renovação e substituição de cartões apenas está disponível para cartões bancários.

4.2 Emissão de Cartões Não Bancários

O processo de emissão lógica de cartões bancários também está disponível para cartões não bancários, com a adaptação necessária às particularidades destes cartões.

4.2.1 Emissão lógica de cartão não bancário

A emissão de cartões não bancários reveste-se de duas modalidades distintas: com processamento SIBS e sem processamento SIBS.

Se o Emissor optar pela primeira opção, o processo de produção inicia-se com o envio à SIBS FPS de um ficheiro ECPS – Emissão de Cartões com Processamento SIBS o qual é colocado em espera por um determinado período de tempo, consoante se trate ou não de uma produção urgente (ver secção 4.3 - Horários de processamento dos ficheiros de emissão de cartões).

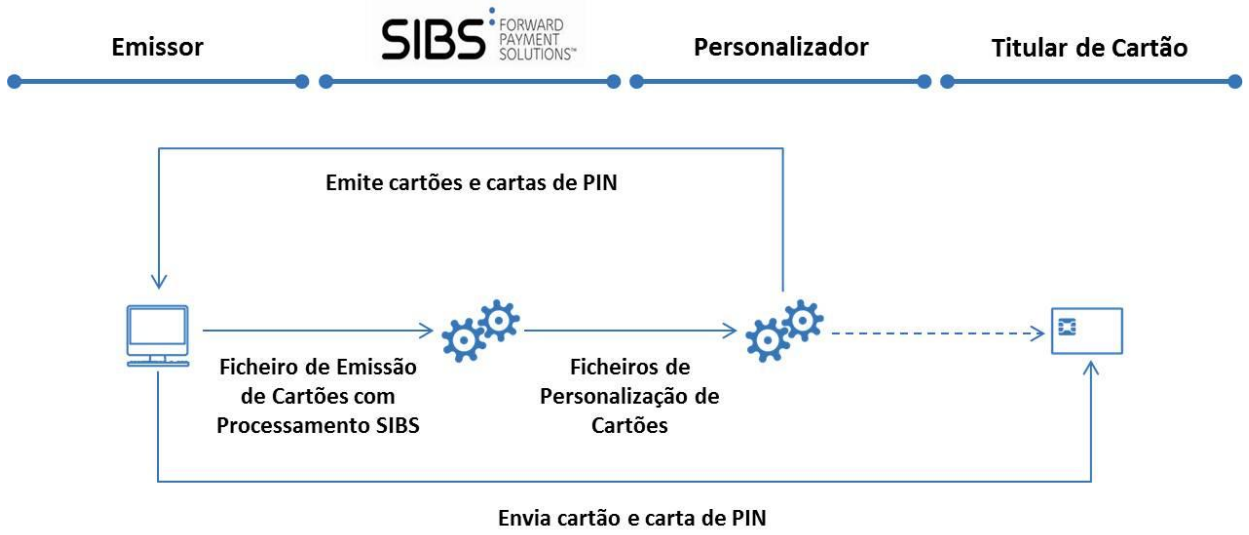

Figura 10 - Emissão de cartões não bancários com processamento SIBS

Na vertente de produção de cartões não bancários sem processamento SIBS, a emissão é descontinuada através da passagem do ficheiro EDAC – Dados Adicionais de Cartões (cartões não bancários) directamente para o personalizador.

A aplicação de produção de cartões não bancários é suportada por duas fases de processamento distintas: a primeira é relativa à recepção e validação dos ficheiros e a segunda relativa ao processamento lógico e aos respectivos *outputs*.

- **RECEPÇÃO DE FICHEIROS**

  O ficheiro de produção de cartões remetido pelos Emissores chega à SIBS via *File Transfer* e é submetido automaticamente à aplicação de cartões.

  De seguida, o ficheiro é submetido a um conjunto de validações genéricas, tais como: verificação da sequência de ficheiro, verificação se produção é urgente e validação da formatação dos registos.

Se o ficheiro não cumpre alguma das validações indicadas, transita para a fase seguinte, na qual é criado o correspondente ficheiro ERCF - Confirmações e Erros do ficheiro ECPS que é enviado para o Emissor como retorno e o processamento é terminado.

- **PROCESSAMENTO LÓGICO**

  A passagem a esta fase de processamento é efectuada automaticamente mediante a validação do seguinte conjunto de regras:

  - Verifica sequência do ficheiro;
  - Valida formato do ficheiro;
  - Efectua cálculos de segurança (validação de inclusão de PIN);
  - Efectua carregamento na base de dados de cartões.

  Estando presentes todos os ficheiros necessários à produção em causa, verifica-se se a infra-estrutura de segurança está disponível. Se não existirem módulos de segurança disponíveis para o processamento lógico, o ficheiro fica em espera até ser possível o respectivo acesso.

  Se as validações descritas forem concluídas com sucesso, e se estiverem satisfeitas as condições necessárias, dá-se início ao processamento lógico.

- ***OUTPUTS* DO PROCESSAMENTO LÓGICO**

  Após o fim do processo de carregamento da base de dados, os seguintes ficheiros são formatados e remetidos:

  - Ao Emissor, o ficheiro ERCF - Confirmações e Erros do ficheiro ECPS;
  - Ao Personalizador[3] os ficheiros PERS e IPIN.

4.2.1.1 Operativa em descontinuação

Na operativa de produção de cartões que se encontra em fase de descontinuação, a emissão lógica de cartões não bancários diferencia-se quer ao nível dos ficheiros processados, quer dos processos adoptados pelos diversos intervenientes.

[3] A personalização de cartões não bancários é realizada através da SIBS Cartões. Este processo estará disponível para qualquer Personalizador assim que estiverem reunidas as condições técnicas e de segurança indispensáveis a esta etapa.

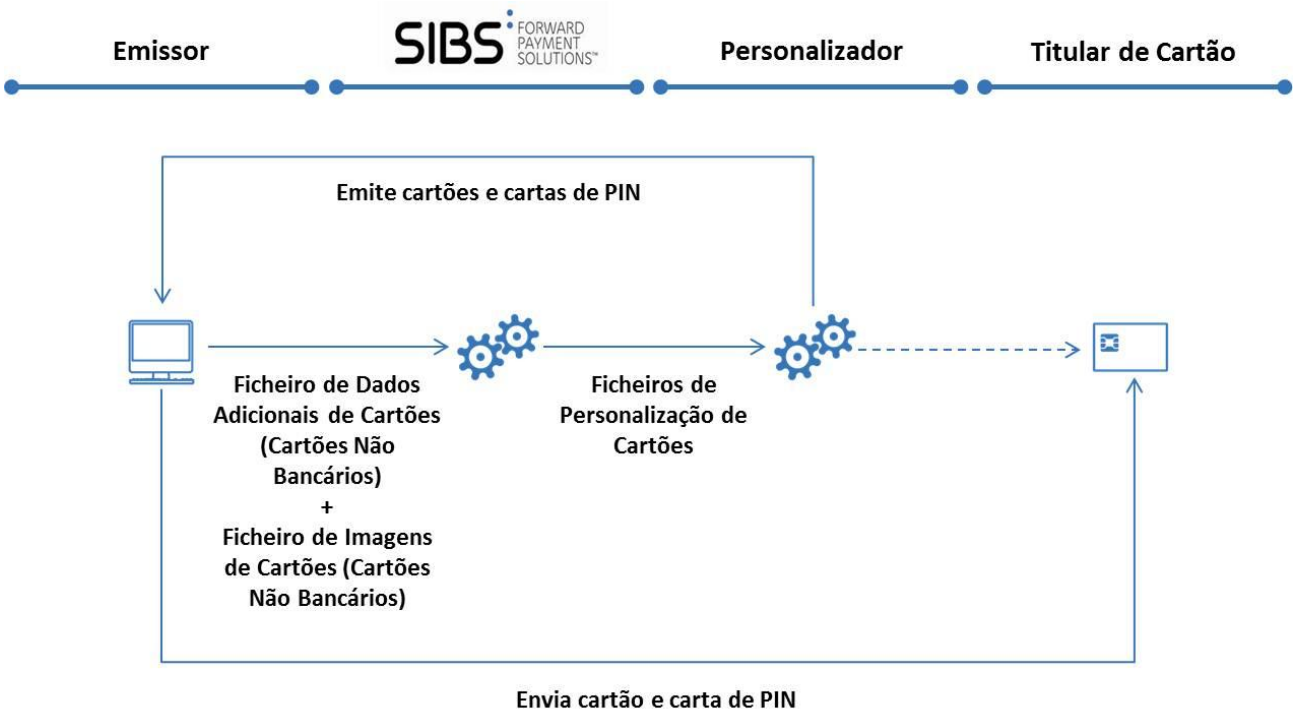

Figura 11 - Emissão de cartões não bancários (operativa em descontinuação)

Considera-se a recepção de um ficheiro de produção de cartões como o despoletar do processo de emissão. Caso não estejam presentes todos os ficheiros necessários à produção, os ficheiros EDAC – Dados Adicionais de Cartões (cartões não bancários) e ficheiro MIMG – Imagens de Cartões (cartões não bancários) são colocados em espera por um determinado período de tempo, consoante se trate ou não de uma produção urgente.

A aplicação de produção de cartões é suportada por duas fases de processamento distintas: a primeira é relativa à recepção e validação dos ficheiros e a segunda relativa ao processamento lógico e aos respectivos *outputs*.

- **RECEPÇÃO DE FICHEIROS**

  Os ficheiros de produção de cartões remetidos pelos Emissores chegam à SIBS via *File Transfer* e são submetidos automaticamente à aplicação de cartões.

  De seguida, os ficheiros são submetidos a um conjunto de validações genéricas, tais como: verificação da sequência de ficheiro, validação da formatação dos registos e verificação da existência de contrato de produção de cartões, e se o mesmo é válido para a produção em causa.

  Se os ficheiros não cumprem alguma das validações indicadas, transitam para a fase seguinte, na qual são criados os correspondentes ficheiros ERAC – Erros de Dados Adicionais de Cartões (cartões não bancários) e/ou RIMG – Erros de Imagens de Cartões que são enviados para o Emissor como retorno e o processamento é terminado.

- **PROCESSAMENTO LÓGICO**

A passagem a esta fase de processamento é efectuada automaticamente mediante a validação do seguinte conjunto de regras:

- Verifica sequência do ficheiro;
- Valida formato do ficheiro;
- Valida existência de contrato de produção de cartões (caso do ficheiro EDAC – Dados Adicionais de Cartões (cartões não bancários));
- Efectua cálculos de segurança (validação de inclusão de PIN);
- Efectua carregamento na base de dados de cartões (caso o Emissor tenha contratado o parqueamento dos seus cartões junto da SIBS FPS).

Estando presentes todos os ficheiros necessários à produção em causa, verifica-se se a infra-estrutura de segurança está disponível. Se não existirem módulos de segurança disponíveis para o processamento lógico, o ficheiro fica em espera até ser possível o respectivo acesso.

Se as validações descritas forem concluídas com sucesso, e se estiverem satisfeitas as condições necessárias, dá-se início ao processamento lógico.

- ***OUTPUTS* DO PROCESSAMENTO LÓGICO**

  Após o fim do processo de carregamento da base de dados, os seguintes ficheiros são formatados e remetidos:

  - Ao Emissor, os ficheiros ERAC – Erros de Dados Adicionais de Cartões (cartões não bancários) e/ou RIMG – Erros de Imagens de Cartões;
  - Ao Personalizador[4] os ficheiros IPER e IPIN.

4.3 Horários de Processamento dos Ficheiros de Emissão

Os horários de processamento dos ficheiros utilizados nos Serviços para Emissores são os seguintes:

Tabela 3 - Horários de processamento dos ficheiros de emissão de cartões

Ficheiro	Horário de Processamento
ELCB – Emissão Lógica de Cartões Bancários	Entre as 20h e as 8h do dia seguinte (aplicável a processamentos não urgentes) a)
EECB - Emissão de Cartões	Entre as 20h e as 8h do dia seguinte (aplicável a processamentos não urgentes) a)
ECPS - Emissão de Cartões com Processamento SIBS	Assim que recepcionado
EDAC - Dados Adicionais de Cartões (cartões não bancários)	Assim que recepcionado
MIMG – Imagens de Cartões (cartões não bancários)	Assim que recepcionado
DACB – Dados Adicionais de Cartões (cartões bancários)	Assim que recepcionado
IMGB – Imagens de Cartões (cartões bancários)	Assim que recepcionado

[4] A personalização de cartões não bancários é realizada através da SIBS Cartões. Este processo estará disponível para qualquer Personalizador assim que estiverem reunidas as condições técnicas e de segurança indispensáveis a esta etapa.

Ficheiro	Horário de Processamento
EALM - Actualização de Limite Mensal	Entre as 20h e as 8h do dia seguinte
ECSV - Comunicação de Saldos de Véspera	Entre as 20h e as 8h do dia seguinte
EDNP - Dados dos Titulares de Cartões	Entre as 20h e as 8h do dia seguinte
EGCC - Gestão de Cartões e Contas	Entre as 20h e as 8h do dia seguinte
EMVC - Movimentos de Conta	Entre as 20h e as 8h do dia seguinte
ESCD - Comunicação de Saldos de Crédito	Entre as 20h e as 8h do dia seguinte
EASC - Alteração de Situação de Cartão	Assim que recepcionado (ficheiros com mais de 5.000 registos e sem urgência deverão ser enviados preferencialmente entre as 20h e as 8h)
ECLN - Lista Negra	Assim que recepcionado

Notas:

a) Os pedidos de Emissão de Cartões Urgentes são processados assim que recepcionados. Após recepção dos ficheiros são efectuadas as validações de estrutura, sequência e validade do contrato, sendo retornado um ficheiro com erros. Durante o horário de processamento serão efectuadas as restantes validações.

4.4 Segurança na Emissão de Cartões EMV

A gestão de chaves para emissão de cartões EMV tem subjacente uma evolução significativa na componente de segurança associada à emissão e operação dos cartões com *chip*. Para além das componentes já existentes nos cartões que apenas possuem banda / pista magnética, as especificações EMV introduzem uma série de novos elementos criptográficos que é necessário considerar.

Com a evolução dos cartões para *chip* passaram a existir novas aplicações nos cartões como, por exemplo, as aplicações CAP / DPA e novos modelos de pagamento como o *contactless* que requerem também novos elementos criptográficos.

As chaves necessárias à emissão de cartões EMV são as seguintes:

- **Chaves Simétricas (3DES)**
  - De Emissão;
  - Transaccionais de Emissor para Banda / Pista Magnética;
  - Transaccionais de Emissor para *Chip*.
- **Chaves Públicas (RSA)**
  - *Certification Authority*;
  - Emissor;
  - Cartão (apenas para cartões DDA - *Dynamic Data Authentication* / CDA - *Combined Data Authentication*);
  - PIN (opcional e apenas para cartões DDA / CDA).

Todas as chaves são geradas aleatoriamente na SIBS FPS através de módulos de segurança centrais (HSM) com geradores de números aleatórios criptograficamente seguros.

Todas as chaves podem ser exportadas para o Emissor ou para o respectivo Sistema de Pagamento, mediante solicitação e autorização do primeiro.

4.4.1 Chaves simétricas

- **De Emissão**
  - Chaves de Guarda de PIN cifrados na SIBS FPS

    Estas chaves têm como função cifrar os PIN guardados pela SIBS FPS para reemissões de cartões sem modificação / geração de PIN;
- **Transaccionais de Emissor para Banda / Pista Magnética**
  - Chaves de PVV (MB, VISA, MCI e AMEX)

    Estas chaves são utilizadas na fase de emissão de cartões para geração do criptograma PVV e na validação do PIN numa transacção;
  - Chaves de CCD (MB), CVV (VISA), CVC (MCI) e CSC (AMEX)

    Estas chaves são utilizadas na fase de emissão de cartões para geração de CCD / CVV / CVC / CSC e na validação da integridade das pistas / bandas magnéticas 2 e 3 em momento de utilização do cartão em transacções presenciais.

    São também utilizadas na fase de emissão de cartões para geração dos criptogramas CVV2 / CVC2 / 3CSC e na autenticação do cartão em transacções não presenciais (*card not present*);
- **Transaccionais de Emissor para *Chip***
  - Chaves de iCVV (VISA), *chip* CVC (MCI) e iCSC (AMEX)

    Estas chaves são as mesmas chaves transaccionais de Emissor utilizadas no cálculo do criptograma da integridade da banda / pista magnética. As chaves são utilizadas na fase de emissão de cartões, para geração dos iCVV / Chip CVC / iCSC e, posteriormente, nas validações de integridade de dados da imagem da pista / banda magnética 2 (*track 2 equivalent data*) contida no *chip*;
  - Chave de *Application Cryptogram EMV*[5]

    Estas chaves são utilizadas na derivação das chaves de cartão para geração e validação de criptogramas do *chip*;
  - Chave de Cifra para *Secure Messaging EMV*

    Estas chaves são utilizadas na derivação das chaves de cartão para confidencialidade no *Secure Messaging*;
  - Chave de MAC para *Secure Messaging EMV*

[5] Chaves partilhadas com as aplicações *contactless chip* e, no caso da VISA, também partilhadas com o *contactless* magnético.

Estas chaves são utilizadas na derivação das chaves de cartão para integridade *Secure Messaging*;

- Chaves de Geração de *ICC Dynamic Number*

  Estas chaves são utilizadas na derivação das chaves de cartão para geração de *ICC Dynamic Number* (apenas usada na MCI para cartões DDA / CDA);

- Chaves de Geração de *Data Authentication Code*

  Estas chaves são utilizadas na derivação das chaves de cartão para geração de *Data Authentication Code* (apenas usada na MCI para cartões DDA / CDA);

- Chaves de validação do criptograma *Dynamic* CVC3 para a aplicação *contactless* MCI (*PayPass*)

  Estas chaves são utilizadas na derivação das chaves de cartão, para validação do criptograma *Dynamic* CVC3, numa transacção *contactless PayPass* em modo *Mag Stripe*;

- Chave de *Application Cryptogram CAP / DPA*

  Estas chaves são utilizadas na derivação das chaves de cartão na aplicação CAP / DPA, para geração e validação de criptogramas do *chip*;

- Chave de Cifra para *Secure Messaging CAP / DPA*

  Estas chaves são utilizadas na derivação das chaves de cartão na aplicação CAP / DPA para confidencialidade *Secure Messaging*;

- Chave de MAC para *Secure Messaging CAP / DPA*

  Estas chaves são utilizadas na derivação das chaves de cartão a aplicação CAP / DPA para integridade *Secure Messaging*.

4.4.2 Chaves públicas

- ***Certification Authority***
  - Chave Privada de CA

    As chaves privadas de CA são utilizadas pelos Sistemas de Pagamento para assinar chaves públicas de Emissor através da geração de um certificado;

  - Chave Pública de CA

    As chaves públicas de CA servem para validação de certificados de chave pública de Emissor. Estas chaves são distribuídas pelos terminais EMV de respectiva rede de aceitação;

- **Emissor**
  - Chave Privada de Emissor

    As chaves privadas de Emissor são utilizadas na emissão de cartões para assinar dados estáticos de cartões *chip*, SDA e DDA e, no caso de cartões DDA, para assinar as respectivas chaves públicas de cartão e, se aplicável, de PIN;

- Chave Pública de Emissor

  As chaves públicas de Emissor são utilizadas pelo terminal na fase de autenticação dos dados e chaves dos cartões;

- **Cartão**
  - Chave Privada de Cartão

    As chaves privadas de cartão são utilizadas para assinar dados dinâmicos do cartão e do terminal durante as transacções.

    Caso o cartão não tenha chaves específicas de PIN servirá também para decifrar o PIN no método Offline PIN;
  - Chave Pública de Cartão

    As chaves públicas de cartão são utilizadas pelos terminais para validar os dados dinâmicos gerados pelos cartões.

    Caso o cartão não tenha chaves específicas de PIN servirá também para cifrar o PIN no método Offline PIN;
- **PIN**
  - Chave Privada de PIN

    As chaves privadas de PIN são utilizadas pelo cartão para decifrar o PIN no método Offline PIN;
  - Chave Pública de PIN

    As chaves públicas de PIN são utilizadas pelos terminais para cifrar o PIN no método Offline PIN.

4.4.3 Responsabilidades da SIBS FPS na gestão de chaves

São da responsabilidade da SIBS FPS os seguintes processos de gestão de chaves:

- **Gestão de chaves de *Certification Authority* MB**
  - Geração dos pares de chaves públicas do Sistema de Pagamento MB;
  - Distribuição da componente pública pelos Emissores e *Acquirers*;
  - Gestão segura dos pares de chaves públicas do Sistema de Pagamento MB;
  - Certificação das chaves públicas de Emissor.
- **Gestão de chaves dos Emissores**
  - Geração de chaves de Emissor necessárias à emissão de cartões;
  - Pedidos de certificados das chaves públicas de Emissor aos respectivos Sistemas de Pagamento necessários à personalização e emissão dos cartões *chip*;
  - Importação dos certificados das chaves públicas de Emissor recebidos dos Sistemas de Pagamento;

- Exportação das chaves simétricas para os Emissores que operem redes privadas ou para os Sistemas de Pagamento no serviço *stand-in*;
- No final do tempo de vida das chaves de Emissor, tratar de todo o processo de renovação das chaves de Emissor com os Sistemas de Pagamento se até à data não houver um pedido expresso pelos Emissores de cancelamento das chaves. Estes procedimentos incluem o arquivo e desactivação das chaves expiradas, para além da geração e emissão de certificados de novas chaves;
- Substituição das chaves caso se verifique o seu comprometimento;
- Gestão das chaves públicas de *Certification Authority* dos vários Sistemas de Pagamento, tratando, nomeadamente, da sua importação, armazenamento e controlo permanente (por exemplo, possível comprometimento, alteração de datas de expiração, entre outros dados);
- Protecção da integridade de todas as chaves geradas pela SIBS FPS e recebidas dos diversos Sistemas de Pagamento.

4.4.4 Política de gestão de chaves

4.4.4.1 Regras gerais de segurança

Toda a política de gestão de chaves públicas adoptada pela SIBS FPS é baseada nas regras e requisitos definidos na documentação da EMV, nomeadamente:

- *EMV2000 Integrated Circuit Card Specification for Payment Systems - Book 2 - Security and Key Management, Version 4.2, December, 2008;*
- *EMV Issuer Security Guidelines - Version 2.1, November, 2007;*
- *EMVCo Annual RSA Key Lengths Assessment.*

A política implementada tem por objectivo garantir que sejam cumpridas as seguintes regras gerais de segurança:

- **Segurança das Chaves Privadas e Secretas**
  As chaves são geradas de forma aleatória em Módulos de Segurança e apenas existem em claro dentro do Módulo de Segurança; fora deste estão sempre devidamente protegidas por chaves criptográficas ou separadas em componentes garantindo o princípio de *split knowledge*. As chaves são geridas em todas as fases do seu ciclo de vida de modo a garantir que não sejam comprometidas e que seja mantida a sua integridade. Caso seja necessário exportar as chaves, existem mecanismos de protecção da sua confidencialidade e integridade durante o seu transporte;
- **Auditoria e Controlo**
  Todos os procedimentos de gestão de chaves realizados na SIBS FPS encontram-se documentados e estão implementados mecanismos de controlo dos processos envolvidos. Estes processos visam melhorar a gestão das chaves em termos de segurança e qualidade;
- **Detecção de Fraude**

Existem mecanismos de detecção de comprometimento de chaves e estão definidos procedimentos a seguir em casos de suspeitas de comprometimento de chaves.

4.4.4.2 Critérios para a escolha dos parâmetros das chaves públicas

Na geração das chaves públicas (de *Certification Authority* MB, de Emissor, de cartão e de PIN) é necessário definir alguns parâmetros que garantam um equilíbrio entre o nível de segurança requerido e o tempo de transacção. Na sua definição são tidos em conta os seguintes critérios:

- Estudos publicados sobre a robustez do RSA e dimensão mínima das chaves a utilizar de modo a que ataques por criptoanálise não sejam praticáveis com a tecnologia actual;
- Tabela publicada anualmente pela EMVco com as dimensões das chaves de *Certification Authority* e respectivos limites máximos das datas de expiração;
- Tabela publicada anualmente pelos Sistemas de Pagamento com as dimensões de chaves de *Certification Authority* e respectivas datas de expiração;
- Capacidade de memória e de processamento dos cartões *chip*;
- Tempo gasto no processo de autenticação em função das capacidades dos terminais. A autenticação baseia-se em operações RSA cujo processamento é pesado, podendo degradar o tempo de processamento das transacções;
- Minimizar o número de chaves geradas reduzindo assim a complexidade da logística de gestão de chaves;
- Possibilidade dos Emissores definirem alguns parâmetros em função dos seus cartões e requisitos de segurança.

As características actualmente definidas para as chaves públicas de *Certification Authority* MB são apresentadas na tabela “Chaves públicas de *Certification Authority* MB” apresentada de seguida.

Todos os valores definidos são revistos anualmente em função dos factores atrás referidos. A revisão é realizada após a actualização da tabela de chaves de *Certification Authority* publicada anualmente pela EMVCo.

Tabela 4 - Chaves públicas de *Certification Authority* MB

Índice	Dimensão	Expoente público	Data de expiração
07	1152 *bits*	03	31/12/2015
08	1152 *bits*	03	31/12/2017
09	1408 *bits*	03	31/12/2021

As características actualmente definidas por defeito para as chaves públicas de Emissor, de cartão e de PIN são apresentadas na tabela 5 - Elementos criptográficos utilizados na produção de cartões na secção 4.4.4.3.

Importa referir que todas estas definições de parâmetros são revistas anualmente em função dos factores acima referidos. A revisão é realizada após a actualização da tabela de chaves de *Certification Authority*

publicada anualmente pela EMVCo ou sempre que os SPI publiquem boletins com regulamentação relativa a dimensões de chaves.

Os seguintes critérios aplicam-se à definição dos parâmetros das chaves públicas:

- Dimensão da chave de Emissor seja menor ou igual à dimensão da chave de *Certification Authority*;
- O expoente público é igual a 03;
- A dimensão do certificado é igual à dimensão da chave que emite o certificado.

4.4.4.3 Utilização de chaves públicas na produção de cartões

Quando um Emissor solicita a produção de cartões de determinado BIN, existem três possíveis cenários de utilização de chaves para cada Sistema de Pagamento que estão resumidos na tabela "Elementos criptográficos utilizados na produção de cartões". A opção utilizada será dependente da validade pretendida para os cartões a produzir.

Tabela 5 - Elementos criptográficos utilizados na produção de cartões

	Validade da chave	Chave de *Certification Authority*		Chave de Emissor		Chave de cartão (DDA)		Marca
		Qtd.	Dim.	Qtd.	Dim.	Qtd.	Dim.	
Cenário 1	Até 31/12/2017	1	1152 *bits*	1/BIN/APL	1024 *bits*	1/BIN/APL/cartão	768 *bits*	MB/MB SPOT e MCI
Cenário 2	Até 31/12/2017	1	1152 *bits*	1/BIN/APL	1152 *bits*	1/BIN/APL/cartão	768 *bits*	VISA
Cenário 3	Até 31/12/2021	1	1408 *bits*	1/BIN/APL	1152 *bits*	1/BIN/APL/cartão	768 *bits*	MB/MB SPOT, VISA e MCI

Actualmente, a opção utilizada para a geração de chaves públicas de Emissor para as aplicações MB/MB SPOT e MCI é a descrita no cenário 1, sendo aquele que utiliza as chaves com as características por defeito definidas na política de gestão de chaves em vigor na SIBS FPS. A opção utilizada para a VISA é a descrita no cenário 2 por imposição regulamentar definida pelo Sistema de Pagamento. Para cartões que se pretendam emitir com validade superior a 31/12/2017 terá que ser utilizado o cenário 3.

Numa emissão lógica de cartões, o certificado escolhido é aquele que tem uma data de expiração igual ou superior à data de expiração dos cartões indicada nos ficheiros EECB - Emissão de Cartões e ELCB - Emissão Lógica de Cartões Bancários e que, simultaneamente, tenha a menor dimensão. O certificado nunca poderá expirar antes do cartão.

Os elementos de pesquisa do certificado são os seguintes:

- Sistema de Pagamento;
- Emissor do cartão;
- BIN do cartão indicado nos ficheiros EECB - Emissão de Cartões e ELCB - Emissão Lógica de Cartões Bancários;

- Data de expiração do certificado (igual à data de expiração da correspondente chave pública de Emissor);
- Dimensão do certificado.

4.4.5 Impacto para os Emissores

O Emissor terá de solicitar o pedido de geração de chaves sempre que deseje migrar um BIN para EMV ou no momento da parametrização de novos BIN no sistema central da SIBS FPS. Anualmente, a SIBS FPS envia ao Banco uma tabela com as dimensões das chaves públicas de Emissor e respectivas datas de expiração. A renovação destas chaves é um processo igualmente desencadeado pelo Emissor.

A gestão desta componente é assegurada pela SIBS FPS de acordo com a política de segurança descrita na secção anterior, caso não haja indicação em contrário da parte do Emissor. O Emissor poderá optar por escolher os parâmetros como, por exemplo, a dimensão e as datas de expiração, sendo as alterações pedidas sujeitas a uma avaliação de modo a garantir que estejam dentro dos valores possíveis e que não comprometam os requisitos mínimos de segurança.

O Emissor só poderá emitir cartões EMV após a geração, no sistema central da SIBS FPS, das novas chaves para EMV do(s) BIN(s) em causa e depois de devidamente assinadas pelas entidades de certificação (*Certification Authorities*) das marcas MB, VISA, MasterCard ou AMEX.

4.5 Gestão do Ciclo de Vida do Cartão

A situação de um cartão, ou seja, a condição que possibilita a realização de operações na Rede CA e TPA MULTIBANCO ou em outras redes, pode mudar durante a sua vida:

- Por problemas na utilização do cartão pelo Titular de Cartão (por exemplo, perda ou roubo do cartão);
- Por desígnio do Emissor (através do envio de ficheiros ou mensagens em *real-time*);
- Como resultado de processos automáticos intrínsecos ao sistema da SIBS FPS;
- Por acção do serviço da PAYWATCH que realiza a monitorização da rede;
- Na sequência da correcta validação do PIN aquando da sua primeira utilização.

A alteração do estado de um cartão pode ser despoletada pelo Emissor ou pela SIBS FPS e excepcionalmente pela PAYWATCH. Os meios possíveis para a execução dessa tarefa são os seguintes:

- Utilização do PSS pelo Emissor;
- Envio de um ficheiro EASC - Alteração de Situação de Cartão pelo Emissor à SIBS FPS;
- Envio de uma mensagem *Host-to-Host* pelo Emissor à SIBS FPS;
- Automaticamente, via Rede MULTIBANCO;
- Pelos serviços de atendimento da SIBS FPS, na sequência de um telefonema do Titular de Cartão;
- Envio de um ficheiro EASC - Alteração de Situação de Cartão, específico da PAYWATCH (EASCSDF) à SIBS FPS ou utilização do PSS, pela PAYWATCH.

Neste sentido, o ciclo de vida de um cartão pode ter os seguintes estados:

- **Normal** – Todas as operações e serviços posicionados pelo Emissor estão disponíveis;
- **Por Personalizar** – Trata-se de cartões que ainda não foram associados a uma conta, podendo ser efectuadas todas as operações disponíveis excepto aquelas que implicam obrigatoriamente a indicação da conta como, por exemplo, consulta de saldos e consulta de movimentos. As restantes operações são enviadas ao Emissor com o número de conta a zeros.

  Se o Emissor quiser produzir cartões não personalizados, estes assumem o estado de "Por Personalizar" no período entre a sua emissão e o processamento pela SIBS FPS do ficheiro EDNP - Dados dos Titulares de Cartões enviado pelo Emissor com os dados da conta dos respectivos titulares;
- **Capturado a Devolver** – É um cartão que foi capturado mas que pode ser devolvido ao respectivo titular porque o seu motivo de captura foi um dos indicados abaixo:
  - Foram excedidas as três tentativas de introdução do PIN;
  - Esquecimento (*time-out* de recolha no ATM);
  - Avaria do ATM.

  A devolução do cartão ao seu titular pela agência bancária pressupõe:
  - A verificação da identidade do Titular de Cartão;
  - A realização de um fecho contabilístico ao CA onde o cartão foi capturado.

  O estado "Capturado a Devolver" é assumido automaticamente quando:
  - O estado prévio do cartão era "Capturado a Devolver Após Fecho CA";
  - E não existindo entretanto qualquer tentativa de utilização, é efectuado o fecho de período contabilístico do CA no qual foi capturado o cartão.

  Após a devolução do cartão ao respectivo titular, a passagem à situação "Normal" é efectuada no momento da realização de uma nova operação na Rede CA MULTIBANCO, se o Titular de Cartão inserir correctamente o PIN na primeira utilização num CA após a sua captura;
- **Lista Negra** – A colocação de um cartão em "Lista Negra" actua imediatamente sobre a informação existente no sistema da SIBS FPS, impedindo a sua utilização em qualquer CA ou TPA após o correcto processamento desta informação. A informação da comunicação de "Lista Negra" deve ser transmitida sempre pelo ficheiro EASC - Alteração de Situação de Cartão ou mensagem *Host-to-Host*, excepto quando existe urgência no envio da informação porque:
  - O utilizador indicou que o PIN se encontra junto do cartão;
  - É possível validar as operações do cartão através de assinatura.

  Podem existir alterações de situação que resultam de acções do serviço que realiza a monitorização da rede. Estes podem colocar cartões em lista negra por delegação do Emissor, através do PSS ou de um ficheiro EASC - Alteração de Situação de Cartão próprio para esse fim. Os cartões colocados em "Lista Negra" pela PAYWATCH, e apenas estes, podem ser colocados novamente em situação "Normal" por este serviço;

- **Lista Cinzenta** – A colocação de um cartão em "Lista Cinzenta" inibe-o de realizar transacções com carácter financeiro, podendo o Titular de Cartão continuar a utilizar o cartão na execução das seguintes operações:
  - Consulta de saldos;
  - Consulta de movimentos;
  - Pedido de livro de cheques;
  - Alteração de PIN.

  Podem existir alterações de situação que resultam de acções do serviço que realiza a monitorização da rede. Estes podem colocar cartões em lista cinzenta por delegação do Emissor, através do PSS, de um ficheiro EASC - Alteração de Situação de Cartão próprio para esse fim ou mensagem *real-time* (H2H). Os cartões colocados em "Lista Cinzenta" pela PAYWATCH, e apenas estes, podem ser colocados novamente em situação "Normal" por este serviço;
- **Capturado a Não Devolver** - Um cartão no estado "Capturado a Não Devolver" fica inibido de realizar operações até que o Emissor analise o motivo que levou à captura e altere a situação, enviando um ficheiro EASC - Alteração de Situação de Cartão ou mensagem *real-time* (H2H).
  Um cartão pode ser capturado na Rede CA MULTIBANCO e ficar neste estado por várias razões:
  - Por ordem do Emissor através de um código de resposta presente nas mensagens *real-time*;
  - Porque o PIN é inserido incorrectamente após a devolução de um cartão na situação "Capturado a Devolver" por tentativas de PIN excedidas;
  - Porque o cartão se encontra na situação "Capturado a Não Devolver" (esta situação ocorre quando, por exemplo, o Emissor ainda não ordenou à SIBS FPS para repor a situação do cartão para "Normal");
  - Porque o cartão utilizado provocou a anomalia «*Timeout* na recolha de notas» duas vezes consecutivas.
- **Anulado** – O Emissor é a única entidade que pode atribuir este estado a um cartão e tal ocorre sempre que este é devolvido pelo respectivo titular, ou seja, pressupõe-se que o plástico não volta a aparecer na Rede MULTIBANCO. Deste modo, os cartões que forem informados como anulados são retirados da base de dados de cartões activos da SIBS FPS.
  Se o Emissor não tem na sua posse o cartão para o qual pretende impedir a realização de transacções, deve colocá-lo na situação de "Lista Negra", ou seja, a colocação na situação de "Anulado" não assegura este objectivo. Na eventualidade do Emissor fazer um uso incorrecto deste estado, a SIBS FPS não assume quaisquer responsabilidades pela utilização indevida do cartão;
- **Capturado e em Lista Negra** - O sistema da SIBS FPS captura um cartão e altera-lhe automaticamente a situação para "Capturado" e em "Lista Negra" quando este é utilizado na Rede MULTIBANCO e se verifica uma das seguintes situações:
  - Porque está em "Lista Negra";
  - Porque o CCD está errado, isto é, o dígito de validação dos dados da pista / banda magnética do cartão está incorrecto;

- Por incoerência entre os dados da pista 3 da banda magnética e os dados da base de dados de cartões da SIBS FPS;
- A sua situação é "Capturado a Não Devolver".

O Emissor é a única entidade que pode retirar um cartão da situação de "Capturado" e em "Lista Negra", colocando o cartão novamente na situação de "Normal" ou "Anulado";

- **Anulado e em Lista Negra** - O sistema da SIBS FPS altera automaticamente a situação de um cartão para "Anulado e em Lista Negra" quando:
  - Este é utilizado em operações de TPA ou em serviço reduzido e a sua situação é "Anulado";

  O Emissor é a única entidade que pode retirar um cartão da situação de "Anulado e em Lista Negra", colocando o cartão novamente na situação de "Anulado";
- **Por Activar -** Um cartão assume este estado após a sua produção lógica se foi caracterizado para apenas ser utilizado após o Titular de Cartão comunicar a sua boa recepção ao Emissor;
- **Activável em CA** - Um cartão neste estado está exactamente igual ao estado "Por Activar" mas tem a possibilidade de fazer a sua activação através da correcta utilização e introdução do PIN numa primeira transacção num CA MULTIBANCO.

  A activação de cartões na Rede CA MULTIBANCO através da introdução correcta do PIN pode ser definida de acordo com o modo de adesão do Emissor ao serviço: através do formulário "Caracterização de BIN" ou via ficheiro de produção de cartões. Esta funcionalidade tem aplicação para todos os cartões emitidos, relativos ao BIN.

  A definição posicionada ao nível do BIN prevalece face à que seja recebida no ficheiro de produção de cartões pelo que se o BIN for caracterizado como "Activável em CA", todos os cartões emitidos terão esta funcionalidade activa. Se optar pela activação ao nível do processo de emissão de cartões, o Emissor terá de identificar cartão a cartão se pretende que o cartão seja também activável na Rede CA MULTIBANCO.

  Os cartões serão emitidos e ficarão registados na base de dados com este novo estado que define a possibilidade de activação na Rede CA MULTIBANCO. O posicionamento do estado inicial do cartão face ao indicador de activação no BIN far-se-á aquando do registo do cartão na base de dados de cartões.
- **Capturado a Devolver Após Fecho CA** - Esta situação ocorre na Rede CA MULTIBANCO quando:
  - Existe um esquecimento do cartão (*time-out* de recolha no CA);
  - Foram excedidas as três tentativas de introdução do PIN e o Emissor indica que nestas circunstâncias pretende que o cartão seja capturado. Após a captura, o cartão volta a ter as três tentativas de PIN disponíveis.

  Neste estado, é importante ter em atenção as seguintes notas adicionais:

  - O Emissor pode, em alternativa, indicar que o cartão deve ser expulso (sem alteração da sua situação). Neste caso, o cartão deixa de estar válido para quaisquer operações electrónicas. As tentativas de PIN só poderão ser repostas a zeros pelo próprio emissor.

- Sempre que um Titular de Cartão introduzir uma vez o código secreto correcto, após falha(s) anterior(es), volta a ter as três tentativas de PIN em futuras operações.

- Ao realizar-se um fecho contabilístico do CA no qual o cartão foi capturado, o estado do cartão evolui automaticamente para "Capturado a Devolver". Se o cartão for devolvido e utilizado pelo Titular de Cartão previamente à realização do fecho de período contabilístico do CA, o estado do cartão evolui para "Capturado a Não Devolver".

A tabela seguinte ilustra a evolução de estados que um cartão pode sofrer ao longo do seu ciclo de vida:

Tabela 6 - Evolução de estados de cartão

DE \ PARA	(02)	(03)	(05)	(06)	(07)	(08)	(09)	(0A)	(0B)	(0D) (15)	(0E)
(02) Normal				✓	✓	✓	✓	◆			◆
(03) Por Personalizar	✓			✓	✓	✓	✓	◆			◆
(05) Capturado a Devolver	◆	◆		✓	✓	✓	✓	◆			
(06) Lista Negra	✓	✓		✓**a**)		✓	✓	◆			
(07) Lista Cinzenta	✓	✓		✓	✓**a**)		✓				
(08) Capturado a Não Devolver	✓	✓		✓	✓		✓	◆			
(09) Anulado									◆		
(0A) Capturado e em Lista Negra	✓	✓					✓	✓**a**)			
(0B) Anulado e em Lista Negra							✓				
(0D [13]) Por Activar **(OF [15])** Por Activar, Activável em CA	✓	✓		✓		✓	✓				
(0E) Capturado a Devolver Após Fecho de CA			◆				✓	◆			

Legenda:

✓ - Evolução de estados que pode ser solicitada pelo Emissor ou efectuada em nome deste (ex: PAYWATCH).

◆ - Evolução de estados automática (efectuada pelo sistema da SIBS FPS).

a) - Para alteração de dados no Sistema de Pagamento/Representante.

Diariamente, no último fecho de compensação, a SIBS FPS envia ao Emissor informação sobre os cartões capturados na Rede CA MULTIBANCO e os cartões que foram informados como "Lista Negra ou "Lista Cinzenta" durante o dia (excepto os informados via ficheiro), através do ficheiro CLN5 - Cartões Capturados e em Lista Negra.

Ainda no âmbito da Gestão de Cartões, um Emissor pode, a qualquer momento, alterar dados de emissão de um cartão através do envio de um ficheiro EGCC - Gestão de Cartões e Contas. Um dos exemplos de alteração é o número de conta à ordem e/ou conta crédito, ou a alteração dos montantes de Saldo de Cartão.

4.5.1 Ciclo de vida dos cartões multi-aplicação

O ciclo de vida de um cartão multi-aplicação apresenta algumas particularidades, devido ao facto do mesmo cartão físico conter dados de dois cartões, o principal e o secundário.

Na emissão lógica dos cartões, a SIBS FPS efectua validação à caracterização dos BINs dos cartões multi-aplicação e ao estado de cada cartão no ficheiro de emissão lógica de cartões (ELCB) e, com vista a manter a coerência da situação entre o cartão principal e o secundário, efectua as alterações apresentadas na tabela seguinte.

Tabela 7 – Estado dos cartões multi-aplicação na emissão

Caracterização de BIN:	Estado no ELCB:		Estado na emissão:	
Activável em CA?	Cartão Principal	Cartão secundário	Cartão Principal	Cartão secundário
Sim	(02) Normal (03) Por Personalizar (13) Por activar (15) Por activar, activável em CA	(02) Normal (03) Por Personalizar (13) Por activar (15) Por activar, activável em CA	(15) Por activar, activável em CA	(13) Por activar
Não	(13) Por activar (15) Por activar, activável em CA	(02) Normal (03) Por Personalizar (13) Por activar (15) Por activar, activável em CA	(13) Por activar (15) Por activar, activável em CA	(13) Por activar

Sempre que o cartão secundário seja emitido no estado “Por activar”, quer como resultado do processamento descrito na tabela anterior, quer como resultado do indicado pelo Emissor no ficheiro de emissão de cartões, este só pode ser activado através de canais do Emissor e após a activação do cartão principal (e caso este esteja em situação normal).

Se um cartão multi-aplicação for emitido “Por personalizar”, quando for efectuada a atribuição de conta ao cartão secundário, este passa do estado “Por personalizar” para o estado “Por activar”.

A partir do momento em que o cartão principal está activo, qualquer mudança, para qualquer estado, de qualquer um dos cartões é reflectida no outro de forma automática, pelo sistema da SIBS FPS.

Sempre que for alterada a situação de um cartão multi-aplicação, a SIBS FPS envia ao Emissor dois registos, um por cada cartão (principal e secundário) no ficheiro CLN5 - Cartões Capturados e em Lista Negra, inclusive quando a alteração de situação tem origem no Emissor, através do envio de ficheiro EASC - Alteração de Situação de Cartão à SIBS FPS. Na captura de cartões em CA, a SIBS FPS informa no ficheiro CLN5, apenas o registo do cartão lógico capturado, mas garante a correspondente actualização da situação do outro cartão.

Quando o Emissor altera os dados de emissão de um cartão através do envio do ficheiro EGCC - Gestão de Cartões e Contas, tem de enviar um registo por cada um dos PAN (principal e secundário) que pretende alterar.

4.6 Operações

4.6.1 Tipo de operações

Para que um cartão possa realizar uma determinada operação, a mesma tem de estar autorizada no formulário "Caracterização de BIN" e no formulário "Caracterização do CPD do Emissor" a que o cartão pertence. Sempre que um cartão seja introduzido num canal da Rede MULTIBANCO, as operações disponibilizadas são as que o Emissor definir no formulário "Caracterização do Emissor". O tipo de operação disponibilizada aos utilizadores da Rede CA e TPA MULTIBANCO varia consoante a marca do cartão.

De seguida detalham-se as operações disponíveis em cartão, de acordo com a respectiva marca.

4.6.1.1 Operações de marca MB / MB SPOT

As operações disponibilizadas nas marcas MB / MB SPOT são as seguintes:

- **Levantamento -** Permite a entrega de numerário, em forma de notas, ao detentor do cartão, em contrapartida do respectivo débito da conta associada ao cartão. Existe um limite máximo diário permitido para levantamentos na Rede CA MULTIBANCO. Estes limites são aplicados para todos os cartões, nacionais ou internacionais;
- **Levantamento a crédito -** Esta operação é tecnicamente idêntica à operação "Levantamento" mas está apenas disponível para cartões de crédito de BIN que possuam o Sistema de Pagamento MB parametrizado na respectiva caracterização;
- **Compra -** Possibilita a aquisição de um bem ou serviço no âmbito da marca MB. Esta transacção ocorre nas seguintes situações:
  - O cartão possui apenas a marca MB ou esta coexiste com uma marca de um SPI, o BIN do cartão tem esta operação disponível e o cartão é utilizado num local onde existe um TPA que possui apenas o acordo geral para aceitação de serviços MB;
  - Independentemente dos acordos de aceitação existentes no TPA, o cartão possui apenas a marca MB e esta operação foi disponibilizada no formulário "Caracterização de BIN".
- **Devolução de compra -** Permite que o Comerciante execute a devolução de uma compra, total ou parcial, sob o acordo MB e apenas é possível nos terminais parametrizados com esta função. Apesar de a operação "Devolução de Compra" estar associada a uma operação de "Compra", não existe emparelhamento entre ambas visto que esta última pode ter ocorrido num período contabilístico anterior. Deste modo, a "Devolução de Compra" é considerada como uma operação a crédito da conta do Titular de Cartão;

- **Autorização outdoor e compra outdoor -** Possibilita a aquisição de bens em máquinas que funcionem em regime de auto-serviço e quando se verifique que:
  - A marca MB coexiste no cartão com uma marca de um SPI, o BIN do cartão tem esta operação disponível e o cartão é utilizado num local onde existe um TPA que possui apenas o acordo geral para aceitação de serviços MB;
  - O cartão possui apenas a marca MB e esta operação foi disponibilizada no formulário "Caracterização de BIN" (a existência no TPA de outros acordos de aceitação é, neste caso, irrelevante uma vez que a transacção apenas se pode realizar no âmbito do acordo geral para aceitação de serviços MB).

  Nos TPA em causa, a compra efectua-se em dois tempos:

  1. O terminal envia um pedido de autorização à SIBS FPS. Esta efectua os procedimentos de segurança e retorna o montante máximo autorizado para a compra, em função do menor dos valores seguintes:
     a. Limite definido para a marca/modelo do TPA;
     b. Valor máximo determinado pelo *Acquirer* e por este parametrizado nos dados operacionais de estabelecimento;
     c. Valor definido pelo centro de autorizações do Emissor.
  2. Se a autorização foi positiva e se o bem foi adquirido, o terminal envia o valor da compra no final da transacção.
- **Adiantamento de dinheiro -** Garante a entrega de numerário a um Titular de Cartão num local onde existe um TPA que possui apenas o acordo geral para aceitação de serviços MB;
- **Consulta de saldos -** Fornece os saldos contabilístico e disponível da conta associada ao cartão;
- **Consulta de movimentos -** Apresenta, no máximo, os dez últimos movimentos e os saldos contabilístico e disponível de uma das possíveis contas associadas ao cartão. No caso de o cartão estar associado a mais do que uma conta, o Titular de Cartão tem de seleccionar a conta para a qual pretende consultar os movimentos;
- **Alteração de PIN -** Permite a alteração do PIN por iniciativa do Titular de Cartão. Para cartões que apenas possuem pista / banda magnética Lo-Co, é efectuada a reescrita da pista / banda magnética para actualização dos *Personal Validation Values* (PVV) das pistas 2 e 3 da bandas magnéticas (PVV2 e PVV3) do cartão antes da devolução deste ao respectivo titular.
  Para cartões com pista / banda magnética Hi-Co, a operação "Alteração de PIN" actualiza apenas a informação guardada centralmente. Adicionalmente, no caso dos cartões com *chip* EMV é necessário actualizar elementos contidos no *chip* sempre que o cartão suporte o método de autenticação de PIN *offline*, ou seja, sempre que existam elementos relativos ao PIN posicionados no próprio cartão (aplicável exclusivamente a cartões EMV nacionais que suportem o *chip* DDA).
  Assim, no caso de alterações de PIN efectuadas com cartões EMV DDA são actualizados os seguintes campos contidos no *chip*:

- *Track 2 Equivalent Data* - Elemento no *chip* que equivale aos dados da pista / banda magnética 2 do cartão;
- *Pinblock* posicionado no *chip*.

De referir também que a validação de PVV nos cartões com pistas / bandas magnéticas Hi-Co é efectuada apenas considerando o valor guardado centralmente e não o valor presente na pista / banda magnética do cartão, uma vez que esta não é actualizável na Rede CA MULTIBANCO;

- **Pagamento de serviços -** Permite ao Titular de Cartão efectuar o pagamento de uma factura (ou outro débito) enviada pela empresa prestadora do serviço, onde constam os seguintes campos:
  - Código de entidade da empresa;
  - Referência do pagamento;
  - Montante a pagar.

  No serviço de compensação, a SIBS FPS envia um crédito para a conta da empresa através do seu Banco de Apoio pelo total dos pagamentos recebidos e envia-lhe directamente um ficheiro com o detalhe de cada pagamento;
- **Transferência bancária (ordenante) -** Possibilita a transferência de um montante da conta associada ao cartão para uma outra pertencente a um Banco participante no sistema da SIBS FPS ou no sistema de compensação de Transferências Electrónicas Interbancárias (TEI), bastando indicar o valor da transferência e o NIB da conta de destino;
- **Devolução de transferência bancária (ordenante) -** Esta operação só é aplicável quando o Emissor de um cartão realizou uma transferência bancária e esta foi devolvida pelo Banco destinatário. A operação "Devolução de transferência bancária (ordenante)" pode ter origem:
  - No sistema de TEI - O Banco destinatário recebeu um registo para creditar um NIB através do sistema de TEI. Se por qualquer motivo necessita efectuar uma devolução do movimento (por inexistência do NIB indicado como destinatário, por exemplo), tem que desencadear essa operação no âmbito do sistema de compensação de TEI e dentro dos calendários previstos para a devolução;
  - No sistema da SIBS FPS - O Banco destinatário recebeu o registo para creditar um NIB via sistema da SIBS FPS. Se pretender efectuar uma devolução, tal é efectuado igualmente via sistema da SIBS FPS. O Banco destinatário desencadeia a devolução da transferência bancária através do PSS ou via mensagem *Host-to-Host*.
- **Transferência bancária (destinatário) -** Ao disponibilizar esta operação no formulário "Caracterização do CPD do Emissor", o Banco determina que todos os créditos que lhe são informados enquanto destinatário de operações de transferências bancárias sejam enviados e compensados no âmbito do sistema da SIBS FPS;
- **Devolução de transferência bancária (destinatário) -** Garante a devolução de uma transferência bancária gerada pelo Banco destinatário dessa mesma transferência. Quando o Banco destinatário tem a transacção de transferência bancária disponível no seu CPD, e verificando a necessidade de

efectuar a devolução de uma operação em concreto, pode utilizar o PSS ou uma mensagem *Host-to-Host* para efectuar a devolução;

- **Pedido de livro de cheques -** Permite requisitar um livro de cheques para a conta associada ao cartão. No caso de o cartão estar associado a mais do que uma conta, o Titular de Cartão tem de seleccionar a conta para a qual pretende requisitar o livro de cheques.

4.6.1.2 Serviços especiais de marca MB SPOT

Os serviços especiais disponibilizados nas marcas MB SPOT enquadram-se em duas categorias distintas: bancários e não bancários.

No caso dos serviços especiais bancários, estão disponíveis as seguintes operações:

- **Consulta de operações de baixo valor -** Permite uma consulta ao detalhe e validação dos movimentos de baixo valor (nomeadamente pagamentos de portagens, Via Verde e telecomunicações) realizados nos diferentes subsistemas da Rede MULTIBANCO, movimentados na conta associada ao cartão que efectua a operação;
- **Consulta de movimentos MB –** Garante uma consulta aos movimentos realizados nos diferentes pontos da Rede MULTIBANCO, sendo composto por três funcionalidades distintas. Nestas funções de consulta podem ser listados os dez últimos movimentos realizados pelo cartão utilizado na operação; podem ser listados os dez últimos movimentos, anteriores a uma data indicada pelo utilizador do serviço; ou podem ser seleccionados os movimentos para os quais o Titular de Cartão pretenda a emissão duma segunda via de um talão comprovativo;
- **Consulta a NIB / IBAN -** Faculta aos Titulares de Cartão a emissão de um talão onde é impresso o NIB referente às contas associadas ao cartão que efectua a operação.
  A impressão do NIB é efectuada num formato BBBB AAAA CCCC CCCC CCCD D, em que:
  - BB – Banco Emissor do cartão;
  - AA - Número de agência;
  - CC – Número de conta;
  - DD – Dígitos de controlo.
- **MB NET via CA -** Disponibiliza aos utilizadores da Rede de CA MULTIBANCO e Titulares de Cartões cujos Emissores são aderentes ao serviço MB NET funcionalidades de adesão, alteração do código pessoal secreto e actualização do montante máximo de compras por dia;

No caso dos serviços especiais não bancários, as operações disponibilizadas são as seguintes:

- **Venda de bilhetes CP -** Possibilita a aquisição de bilhetes para utilização do sistema de transportes gerido pela empresa CP mediante um débito na conta associado ao cartão que efectua a operação;
- **Pagamentos ao Estado -** Os contribuintes podem efectuar na Rede CA MULTIBANCO o pagamento de Documentos Únicos de Cobrança (DUC) emitidos pela Administração Fiscal. O documento na posse do contribuinte apresenta a informação a introduzir para executar a transacção na forma de uma referência para pagamento.

Os tipos de imposto passíveis de pagamento na Rede MULTIBANCO dividem-se em dois grupos: DUC suportados por documentos de cobrança (informados à SIBS FPS pela Direcção Geral do Tesouro através do ficheiro de Documentos em Cobrança) e DUC com submissão via Internet. Neste serviço não são permitidos pagamentos duplicados;

- **Carregamento de telefones fixos, telemóveis e cartões virtuais -** Possibilita a um utilizador de telefone fixo, telemóveis ou de um acesso à Internet, cujos operadores aderiram ao pagamento na Rede MULTIBANCO, efectuar carregamentos antecipados de chamadas ou outros serviços (por exemplo, carregamentos PT Comunicações, TMN, Vodafone ou Optimus) ou efectuar carregamentos antecipados das suas sessões (por exemplo, Netpac);
- **Jogos Santa Casa -** A Rede MULTIBANCO suporta o pagamento de prémios dos Jogos Santa Casa, ficando a gestão dos diversos prémios a pagamento a cargo do Departamento de Jogos da Santa Casa.

  Nesta operação são recolhidos os elementos do Titular de Cartão utilizador do serviço (número de cartão de jogador e respectivo código secreto associado) e é enviado à Santa Casa um pedido encriptado para confirmação de dados. O Departamento de Jogos da Santa Casa valida a informação recebida e, caso existam prémios passíveis de pagamento pelo canal MB, cativa o prémio disponibilizado respondendo com uma mensagem em *real-time*.

  Perante uma resposta positiva, o sistema da SIBS FPS processa a respectiva informação de modo a que seja efectuado um débito na conta da Santa Casa por contrapartida de um crédito no NIB indicado na transacção.
- **Via Verde -** Esta operação permite a associação (ou substituição) de um ou mais identificadores do serviço Via Verde a um cartão / conta para pagamento das passagens efectuadas. A entidade responsável pela gestão da informação referente aos dispositivos é a Via Verde Portugal.

4.6.1.3 Operações de marcas internacionais

As operações disponibilizadas nas marcas de SPI são as seguintes:

- **Compra (outras vertentes) -** Esta operação é tecnicamente idêntica à operação “Compra” mas sob o acordo para aceitação de uma marca de um SPI. Os cenários de funcionamento da operação dependem da posição do Emissor face ao representante do cartão:
  - Se o Emissor for autónomo, a operação é enviada pela SIBS FPS ao Emissor em *real-time* (quando aplicável) e nos ficheiros de compensação;
  - No caso de o Emissor não ser autónomo, esta operação é encaminhada para o centro de autorizações escolhido. Neste caso, o Emissor recebe os dados da operação através dos ficheiros desta entidade e não da SIBS FPS directamente.
- **Devolução de compra (outras vertentes) -** Esta operação é tecnicamente idêntica à operação “Devolução de Compra” mas sob o acordo para aceitação de uma determinada marca de um SPI;

- **Autorização (outras vertentes) -** Trata-se de uma operação destinada apenas a cartões que não têm operações puramente electrónicas como, por exemplo, cartões VISA ou MasterCard. Estas operações podem ser realizadas em:
    - Comerciantes da rede comercial de um *Acquirer* que, não tendo TPA, efectuem uma chamada telefónica para autorização. O operador do terminal introduz o pedido de autorização e a SIBS FPS envia-o ao Emissor do cartão ou decide noutro cenário. A resposta é entregue no terminal do representante e comunicada ao Comerciante. Posteriormente, o Comerciante apresenta uma factura ao representante;
    - Comerciantes com TPA cuja actividade comercial implique um pedido de autorização antes da concretização da compra (por exemplo, hotéis nas operações de *check-in* e *check-out*);
    - Terminais que só efectuam pedidos de autorização.

  Esta operação não tem valor contabilístico. Porém o montante de autorizações efectuado para um dado cartão deve ser controlado, visto que existe desfasamento entre o momento do pedido de autorização e o débito correspondente;
- **Cancelamento de autorização (outras vertentes)** – Esta operação deve ser utilizada quando um Comerciante enviar um pedido de autorização ao Emissor de um cartão e a compra não se concretiza. Com o cancelamento, o Emissor deve repor a capacidade de crédito do Titular de Cartão anterior ao pedido de autorização.

  Na operação "Cancelamento de Autorização" o Comerciante indica qual o número da autorização original que pretende cancelar de modo a que o sistema do Emissor (ou a sua central de autorizações) garanta este emparelhamento. A operação não possui valor contabilístico para o Comerciante e para o Emissor do cartão;
- **Autorização outdoor e compra outdoor (outras vertentes) -** Esta operação é tecnicamente idêntica à operação "Autorização Outdoor e Compra Outdoor" mas sob o acordo para aceitação de uma marca de um SPI;
- **Adiantamento de dinheiro (outras vertentes) -** Esta operação é tecnicamente idêntica à operação "Adiantamento de Dinheiro" mas sob o acordo para aceitação de uma marca de um SPI;
- ***Fees* de cartão recebidas do estrangeiro -** Permite aos Emissores e *Acquirers* cobrarem entre si valores devidos pelos serviços prestados no âmbito internacional como, por exemplo, cobrança de despesas por envio de cartões capturados, envio de faxes para colocação de cartões em Lista Negra, bem como a resolução financeira de processos de reclamação disputados no ciclo de *chargebacks*. Estas *fees* têm indicação do número de cartão;
- **Devolução de *fees* de cartão para o estrangeiro -** São operações tecnicamente idênticas às "*Fees* de Cartão Recebidas do Estrangeiro" com a diferença que não se destinam a cartão mas sim ao Emissor. São normalmente utilizadas para cobrar ao Emissor valores relativos a facturação de serviços como, por exemplo, valores relativos a formação de colaboradores.

- **Levantamento a Crédito** - Esta operação é tecnicamente idêntica à operação "Levantamento" mas está apenas disponível para cartões de crédito de BIN que possuam o Sistema de Pagamento de uma Marca Internacional parametrizado na respectiva caracterização.

4.6.2 Serviços disponibilizados em canais próprios do Emissor

O Emissor pode ainda implementar a aceitação de operações disponíveis no sistema da SIBS FPS em canais próprios como, por exemplo, o serviço de *homebanking* de uma instituição bancária.

Neste canal não é necessária a presença física do cartão, sendo enviados à SIBS FPS os elementos do NIB da conta e/ou os elementos identificadores do cartão que efectua a operação. É o único canal do sistema da SIBS FPS em que o interface com o utilizador e a respectiva segurança é da exclusiva responsabilidade do Emissor, e ainda o único no qual a SIBS FPS não aplica os cenários de decisão (por exemplo, saldo de conta ou saldo de cartão) posicionados para o BIN do cartão ou para o CPD do Emissor, dado que a operação é validada pelo Emissor previamente ao seu envio à SIBS FPS.

Estão disponíveis a partir dos canais dos Emissores as seguintes operações disponibilizadas nas marcas MB SPOT:

- Consulta de operações de baixo valor;
- Pagamento de serviços;
- Carregamento de telefones fixos, telemóveis e cartões virtuais;
- Transferências bancárias;
- Via Verde;
- Pagamentos ao Estado;
- Pagamentos de custas judiciais;
- Pagamento à Segurança Social;
- Jogos Santa Casa.

4.7 Autenticação

A autenticação é um processo que ocorre numa fase imediatamente anterior à autorização de uma operação e consiste em várias validações que uma transacção deve ultrapassar para poder ser efectuada. Os dados que são validados variam conforme o tipo de tecnologia do cartão que se está a utilizar para efectuar a transacção e se se trata de uma operação presencial ou não presencial.

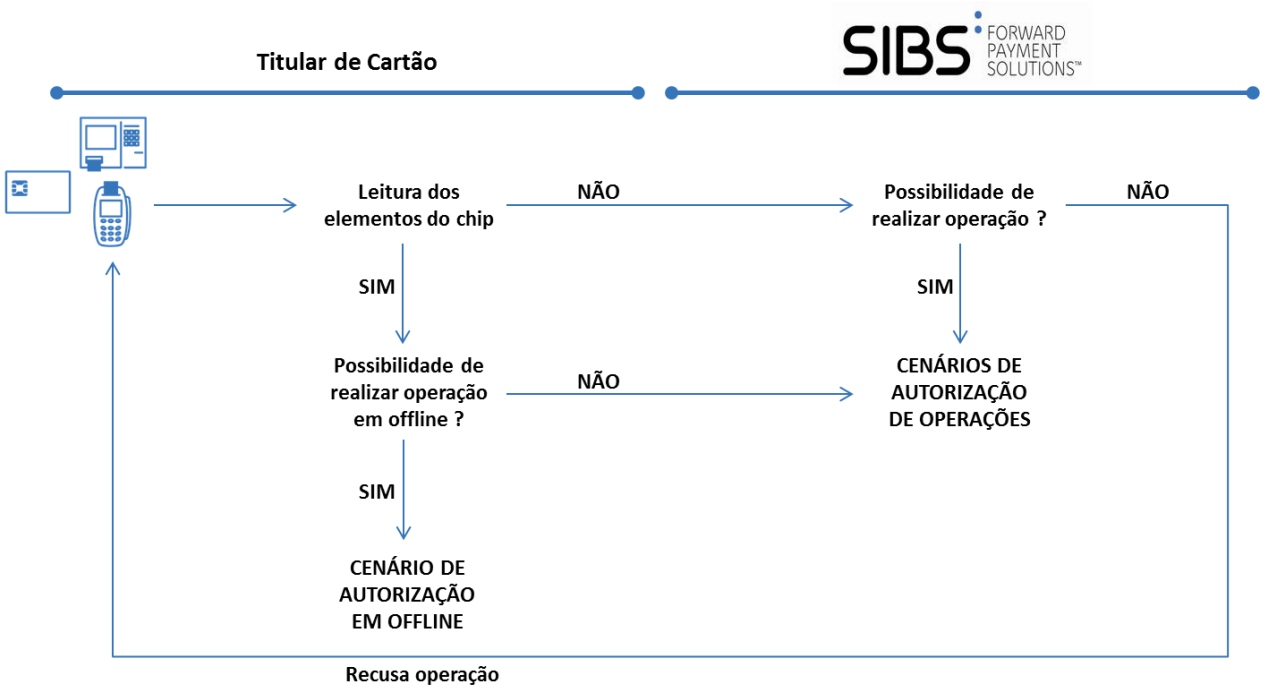

Figura 12 - Modelo operativo de autenticação de cartões EMV

Quando um cartão com *chip* EMV é utilizado na Rede CA ou TPA MULTIBANCO, o terminal procura obter um conjunto de dados posicionados no *chip*:

- Se for possível ler os elementos existentes no *chip*, a transacção prossegue sobre *chip*. O diálogo entre terminal e cartão determina a lista de aplicações EMV candidatas para realização da transacção seleccionada. Após escolha da aplicação a ser utilizada, existe um diálogo adicional entre terminal e cartão para aferir da possibilidade de realização da transacção em cenário de *offline*;
- A impossibilidade de leitura dos dados contidos no *chip* é devidamente identificada. Quando se verifique que, para um cartão com *chip* EMV utilizado num terminal com capacidades EMV, foi desencadeada uma transacção com base nos dados contidos na pista / banda magnética, existe um conjunto de elementos de risco a validar (parâmetros de *fallback* definidos no formulário "Caracterização de BIN"), independentes do cenário de decisão aplicável.

Na sequência dos pontos anteriores, se não for possível realizar a transacção em *offline*, é desencadeado o envio de uma mensagem para o sistema central da SIBS FPS com os elementos da transacção e elementos de segurança recolhidos. Previamente ao processo de autorização, e independentemente do cenário de funcionamento, o sistema valida se:

- O cartão existe na base de dados de cartões da SIBS FPS;
- Os dados da pista / banda magnética do cartão ou do *chip*, no caso de cartões EMV, são consistentes com a informação da referida base de dados;
- Os dados de segurança (na pista / banda magnética ou *chip* EMV) estão correctos;
- O PIN inserido pelo Titular de Cartão está correcto;

- A situação do cartão é admissível para o cartão efectuar a operação escolhida;
- A operação está autorizada para o cartão.

Caso alguma das validações anteriores não seja ultrapassada com sucesso, a transacção é finalizada com a mensagem de erro prevista para o efeito. Se todas as validações forem bem-sucedidas segue-se o processo de autorização.

4.8 Autorização

A realização de operações com cartões de pagamento está dependente da sua autorização. Para tal, a SIBS FPS disponibiliza vários cenários de funcionamento de modo a adequar o modo de decisão de autorização à estratégia individual de cada Emissor. Deste modo, a autorização da operação poderá 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 de autorização da operação é delegada pelo Emissor na SIBS FPS.

É sempre possível que um Emissor inicie a sua actividade num determinado cenário e posteriormente evolua para outros. Normalmente, os CPD dos Emissores cujo cenário de funcionamento principal é o *real-time* têm um cenário de degradação como meio alternativo de decisão, no caso de ocorrerem interrupções da sessão *real-time*.

Adicionalmente, o Emissor pode definir um cenário controlado para as situações em que planeia desligar a sessão de *real-time* (por exemplo, num fim de semana ou feriado para proceder à manutenção ou melhoramento do seu sistema).

4.8.1 Cenários para autorização de operações na Rede MULTIBANCO

De seguida, são apresentados os cenários disponíveis para autorização de operações na Rede MULTIBANCO de CA e TPA. As operações realizadas noutros canais (MB NET, MB PHONE) são objecto do conjunto destas validações aplicáveis à sua forma de caracterização particular.

4.8.1.1 *Real-time*

No cenário de *real-time*, o Emissor decide directamente as autorizações / recusas de operações. A SIBS FPS envia uma mensagem ao CPD do Emissor que tem um período de tempo parametrizável para responder. Se tal não acontecer, a operação passa para o cenário de degradação (ver secção 4.8.1.2) desse CPD, conforme posicionado no formulário "Caracterização do CPD do Emissor". Se o Emissor responder dentro do tempo disponível, a SIBS FPS regista a resposta e devolve uma mensagem ao terminal.

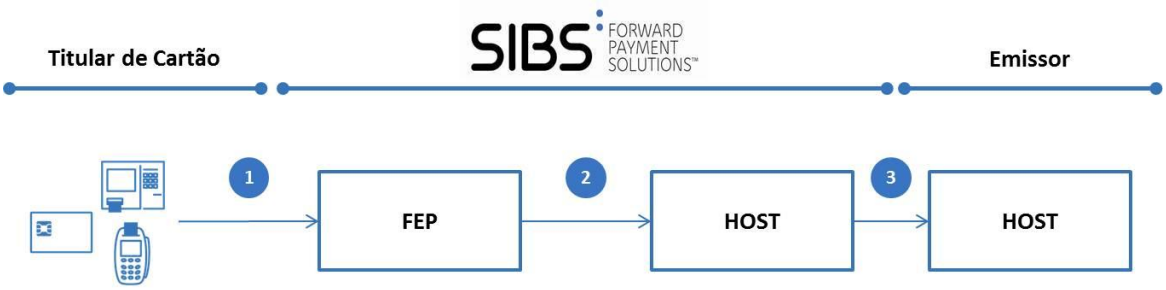

Figura 13 - Autorização de operações em real-time

No processo de decisão de autorização das operações, o Emissor pode:

- Aceitar a operação;
- Pedir à SIBS FPS para decidir a autorização no cenário de degradação existente;
- Recusar a operação (por saldo insuficiente, erro aplicacional, suspeita de fraude ou outro motivo);
- Pedir para capturar o cartão (segundo os seus critérios internos), através do código de resposta presente nas mensagens *real-time*.

A decisão do Emissor relativamente às operações financeiras é efectuada em função do saldo disponível na conta do Titular de Cartão e de eventuais limites internos de autorização, permitindo a actualização imediata da conta e a total integração com outros lançamentos de retaguarda ou realizados nos terminais do Emissor. Exceptuam-se as operações de levantamento e levantamento a crédito que estão sujeitas a um limite específico da Rede MULTIBANCO.

A concretização das operações não financeiras (por exemplo, uma consulta de movimentos), quando disponibilizadas pelo Emissor, não está dependente do saldo mas sim da existência de informação relevante para apresentar ao Titular de Cartão.

Quando ocorre uma interrupção da sessão de *real-time* entre a SIBS FPS e o Emissor, a SIBS FPS decide consoante o cenário e parâmetros posicionados pelo Emissor, que serão apresentados nas secções seguintes.

4.8.1.2 Degradação na SIBS FPS

Em determinadas circunstâncias, o Emissor pode adoptar métodos de aceitação de operações alternativos ao cenário *real-time*: os cenários de degradação na SIBS FPS.

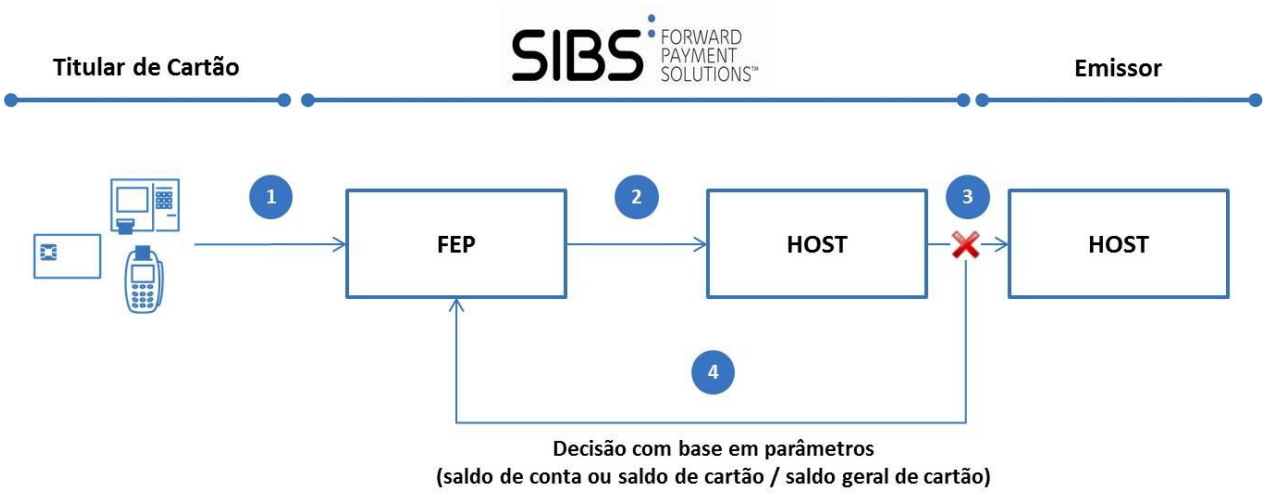

Figura 14 - Autorização de operações com degradação na SIBS FPS

4.8.1.2.1 Saldo de conta

No cenário de saldo de conta é a SIBS FPS que gere as autorizações. As operações são decididas com base nos limites de decisão parametrizados pelo Emissor e na informação residente na SIBS FPS relativamente ao saldo disponível da conta associada ao cartão utilizado, a qual é actualizada com base nos ficheiros ECSV – Comunicação de Saldos de Véspera enviados periodicamente pelo Emissor. Estes ficheiros contêm a informação relativa aos saldos, disponível e contabilístico, das contas que sofreram variações desde o último ficheiro enviado pelo Emissor.

Sempre que o Emissor transmitir um novo ficheiro ECSV – Comunicação de Saldos de Véspera, pressupõe-se que este indica o novo saldo de uma conta. Se tal não acontecer para uma conta cujos cartões efectuaram operações financeiras na Rede MULTIBANCO, a SIBS FPS actualiza os respectivos saldos disponível e contabilístico com os últimos valores informados pelo Emissor, isto é, desprezando as importâncias das operações entretanto feitas pelos Titulares de Cartões.

A decisão de uma operação pela SIBS FPS é efectuada com base nos seguintes valores:

- Saldo disponível da conta associada ao cartão, enviado no ficheiro ECSV – Comunicação de Saldos de Véspera, que também pode ser actualizado pelo valor do campo saldo disponível enviado nas mensagens de resposta *real-time*, no caso de o Emissor posicionar o indicador "Actualização do Saldo de Conta em *Real-Time*" no formulário “Caracterização do CPD do Emissor”;

- Montante máximo diário para operações na Rede TPA MULTIBANCO até ao qual a SIBS FPS autoriza operações de compras, pagamento de serviços e transferências interbancárias, podendo o Emissor parametrizar este montante para cada um dos BIN, no formulário "Caracterização do BIN" ~~(as operações de compra e pagamento de serviços não estão abrangidos por este limite)~~;
- O limite diário para a Rede CA MULTIBANCO relativamente às operações levantamento e levantamento a crédito.

Diariamente, na primeira operação do cartão, o menor destes dois valores é utilizado como o montante disponível para decidir operações:

- Se o valor de uma operação a débito for inferior ou igual ao montante disponível, aquela é autorizada e o seu valor é deduzido a este até ser igual a zero;
- Em caso contrário, aquela é recusada.

Se a SIBS FPS aceitar uma operação a crédito adiciona o valor desta ao saldo disponível da conta associada ao cartão.

O cenário de saldo de conta permite a introdução de um limite mensal para uma conta que define o risco do Titular de Cartão, ou seja, é o valor máximo para a realização de todos os movimentos aceites dos cartões dessa conta, sendo reposto no mesmo dia de cada mês.

4.8.1.2.2 Saldo de cartão

No cenário de saldo de cartão é a SIBS FPS que gere as autorizações. As operações são decididas pela SIBS FPS com base no saldo de cartão (para levantamentos) e saldo geral de cartão (para todas as operações) atribuído a cada cartão no momento da sua emissão (ou posteriormente através do ficheiro EGCC - Gestão de Cartões e Contas):

- **Saldo de cartão** - É o montante utilizável para autorizar apenas operações de levantamento na Rede CA MULTIBANCO. Se aquele for posicionado a zero, o levantamento é impossível quando o sistema da SIBS FPS está em serviço reduzido (ver secção 4.8.1.3);
- **Saldo geral de cartão** - É o montante utilizável para autorizar operações de débito (levantamentos, compras, pagamento de serviços, transferências interbancárias e serviços especiais) na Rede CA e TPA MULTIBANCO.

O saldo de cartão e o saldo geral de cartão são definidos individualmente para cada cartão:

- No momento da sua produção, através do ficheiro ELCB - Emissão Lógica de Cartões Bancários;
- Em eventuais alterações que ocorram ao longo da vida do cartão através do ficheiro EGCC - Gestão de Cartões e Contas.

No caso de operações de levantamento na Rede MULTIBANCO, a decisão tomada pela SIBS FPS baseia-se nos seguintes valores:

- Saldo de cartão;
- Saldo geral de cartão;
- Limite máximo diário de levantamento (valor da Rede MULTIBANCO).

No início do período de utilização definido para o cartão, o menor destes três valores é utilizado como o montante disponível para decidir operações:

- Se o valor de uma operação a débito for inferior ao montante disponível, aquela é autorizada e o seu valor é deduzido a este até ser igual a zero;
- Em caso contrário, aquela é recusada.

No caso das restantes operações a débito, a decisão tomada pela SIBS FPS assenta no saldo geral de cartão:

- Se o valor da operação a débito for inferior ao saldo geral de cartão, aquela é autorizada e o seu valor é deduzido a este até ser igual a zero;
- Em caso contrário, aquela é recusada.

O saldo de cartão está associado a um período diário, semanal ou mensal que estabelece o intervalo de tempo em que o saldo pode ser utilizado, enquanto o saldo geral de cartão possui uma periodicidade diária. O saldo de cartão é guardado centralmente e gravado na pista 3 da banda magnética de cada cartão no momento da sua emissão. Para cartões que apenas possuem pista / banda magnética regravável, a pista 3 da banda magnética é reescrita sempre que se verifique uma alteração ao montante do saldo de cartão.

Historicamente, a validação do saldo de cartão é efectuada sobre o valor gravado na pista 3 da banda magnética. No entanto, tendo em conta que não é possível reescrever as pistas / bandas magnéticas na Rede CA MULTIBANCO para cartões que possuam pista / banda magnética Hi-Co, os dados inscritos na pista 3 da banda magnética no momento da emissão não podem ser actualizados.

Assim, a validação do montante de saldo de cartão depende do indicador de tecnologia da pista / banda magnética, gravado na própria:

- Se o cartão não possui *chip* EMV e a pista / banda magnética é Lo-Co, valida-se o saldo de cartão gravado na pista 3 da banda magnética;
- Se o cartão é EMV ou, não sendo EMV, possui pista / banda magnética Hi-Co, a gestão e validação do valor do saldo de cartão é efectuada no sistema central da SIBS FPS.

4.8.1.3 Serviço reduzido

No caso de interrupções ocasionais ou programadas do sistema central da SIBS FPS, as operações não podem realizar-se segundo os cenários de funcionamento indicados pelo Emissor entrando em funcionamento o serviço reduzido. Neste cenário é a SIBS FPS que gere as autorizações através dos equipamentos *Front-End Processor* (FEP) que efectuam as validações de segurança e decidem as operações.

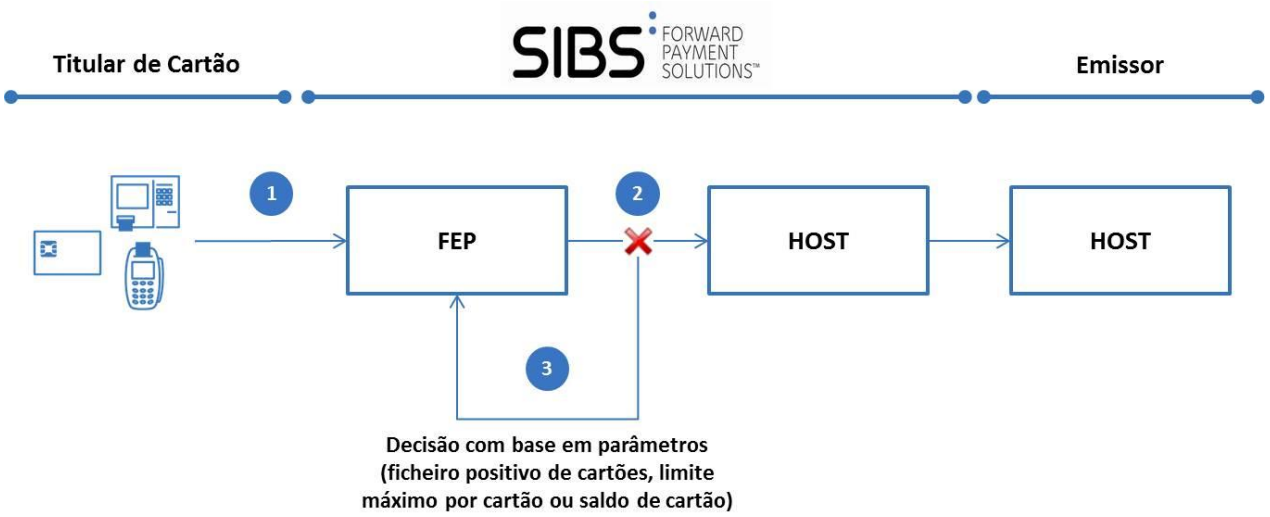

Figura 15 - Autorização de operações com serviço reduzido

As operações provenientes da Rede TPA MULTIBANCO são decididas com base em:

- Ficheiro positivo de cartões – validação da existência do cartão e estado do cartão;
- Limite máximo por cartão (definido no formulário "Caracterização do BIN").

As operações provenientes da Rede CA MULTIBANCO são decididas em função de:

- Ficheiro positivo de cartões – validação da existência do cartão e estado do cartão;
- Saldo de Cartão (ver secção 4.8.1.2.2)

Se a operação for realizada por um cartão EMV num terminal EMV, mas não é possível efectuar a leitura de elementos contidos no *chip* necessários à autorização, a transacção é recusada.

O ficheiro positivo que contém informação sobre os cartões é actualizado no FEP uma vez por semana, independentemente de os cartões já terem passado na Rede CA MULTIBANCO (ou seja, abrange tanto os novos cartões como os cartões já existentes). A Lista Negra é actualizada no FEP de 30 em 30 minutos.

4.8.1.4 *Real-time* dos Emissores com o FEP

O cenário de *real-time* dos Emissores com o FEP da SIBS FPS permite o funcionamento de ligações *real-time* aos Emissores, quando a ligação do sistema central da SIBS FPS com os Emissores não se encontra disponível, passando nestes casos o FEP a assegurar o processamento em *real-time* dos pedidos de autorização de transacções. Caso não seja possível a ligação *real-time* dos Emissores com o FEP, continuará a haver lugar à degradação para autorização das operações com base no serviço reduzido.

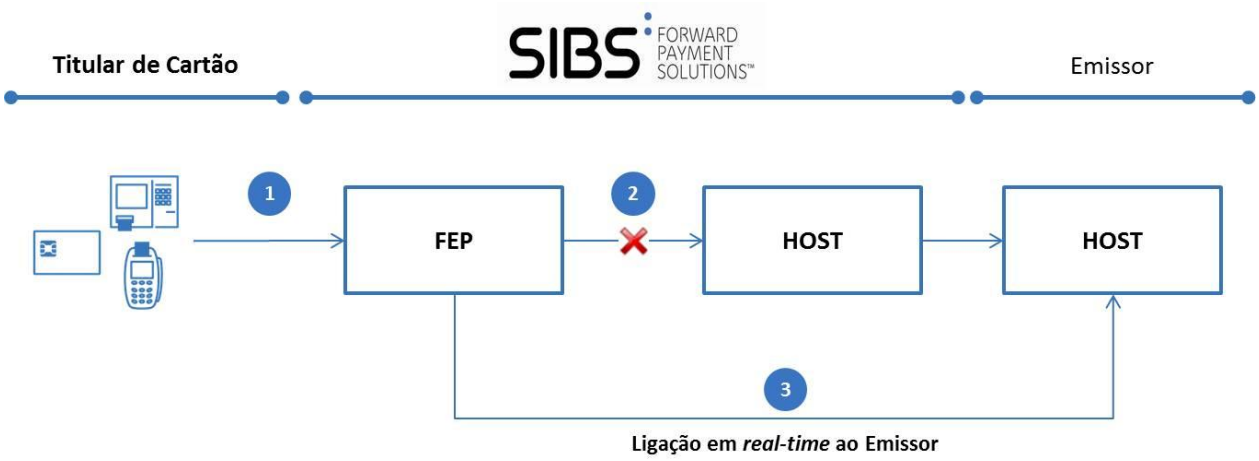

Figura 16 - Autorização de operações em real-time com o FEP da SIBS FPS

O *real-time* dos Emissores com o FEP contempla a autorização das seguintes operações da Rede MULTIBANCO:

- Levantamentos a débito na Rede CA MULTIBANCO;
- Compras na Rede TPA MULTIBANCO;
- Pagamento de serviços e pagamento de compras na Rede CA e TPA MULTIBANCO;
- Consulta de saldos na Rede CA MULTIBANCO;
- Consulta de movimentos na Rede CA MULTIBANCO;
- Operações de autorização *outdoor* na Rede TPA MULTIBANCO;
- Depósitos com validação na Rede CA MULTIBANCO.

Este cenário garante uma cobertura de cerca de 85% das operações realizadas na Rede CA MULTIBANCO e 99% das transacções realizadas na Rede TPA MULTIBANCO.

Quando o sistema central da SIBS FPS está indisponível e é o FEP que assegura o *real-time*, os CA apresentam no ecrã apenas as operações contempladas por este cenário de autorização. As restantes transacções na Rede CA MULTIBANCO não sofrem qualquer tipo de alteração, bem como as operações realizadas por cartões *on-us* no estrangeiro.

4.8.1.5 Pagamentos de baixo valor

As autorizações de pagamentos de baixo valor aplicam-se às transacções efectuadas em portagens com cartão, pagamentos Via Verde e Publifones.

A autorização deste tipo de transacções ocorre com base em parâmetros posicionados pelo Emissor parametrizados no formulário "Caracterização do BIN" e que servem para que a SIBS FPS decida, em nome do Emissor, a aceitação ou rejeição destas transacções.

Após a autorização de uma transacção de baixo valor, o Emissor é informado no ficheiro DST5 – Destinos da autorização e respectivo montante associado (ver secção 4.9).

4.8.1.5.1 Devoluções de pagamentos Via Verde

No âmbito das transacções de pagamentos de portagens e parques com dispositivo Via Verde, existe um processo de devolução do pagamento com dispositivo Via Verde em momento prévio à sua cobrança aos Emissores, via ficheiro DST5 – Destinos, da compensação.

O processo de devoluções de pagamentos Via Verde é apresentado na figura seguinte:

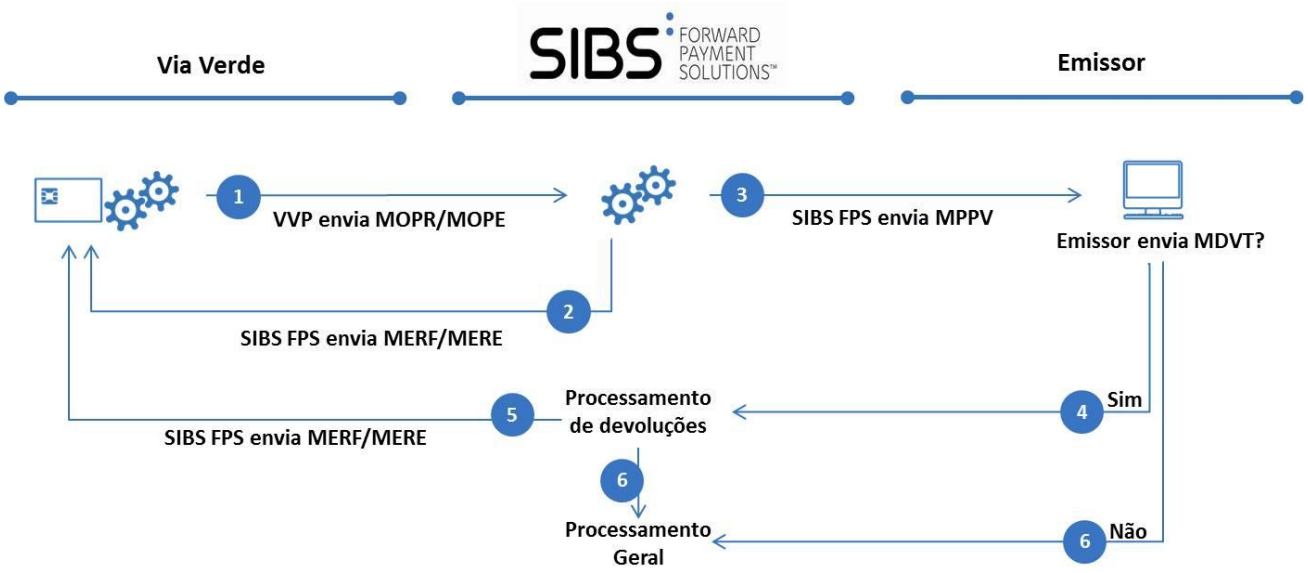

Figura 17 - Fluxograma do processo de devoluções de pagamento Via Verde

Neste processo o Emissor é o responsável pela gestão das devoluções e está assente nos seguintes pressupostos:

- Após a recepção do ficheiro de movimentos para cobrança, o Emissor do cartão dispõe de um prazo de 2 dias úteis para devolver os que não possam ser cobrados;
- No final desse prazo os movimentos aceites serão enviados aos Emissores e bancos de apoio dos operadores, nos ficheiros de compensação;
- É estabelecido um fecho diário às 18:00 para este tipo de operações.

Os fluxos de informação relacionados com estas devoluções são:

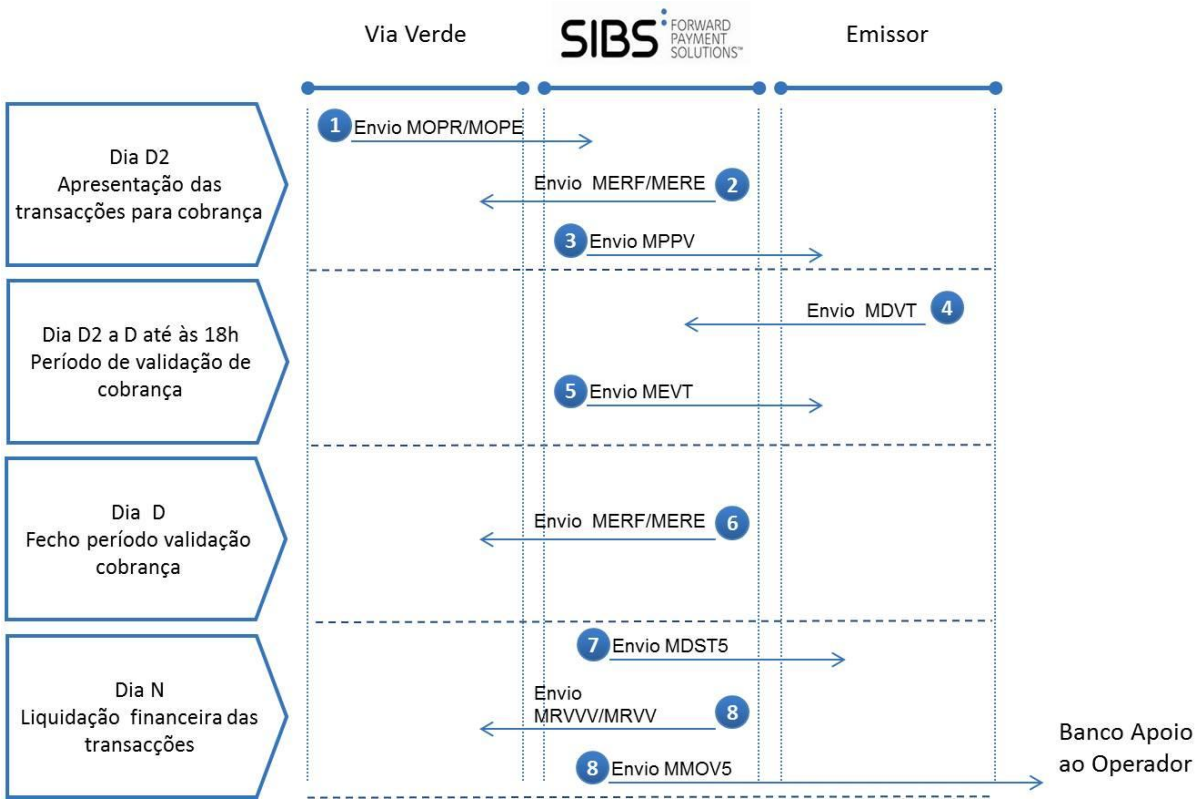

Figura 18 - Fluxos de informação da devolução de um pagamento Via Verde

A Via Verde Portugal pode reenviar à SIBS FPS as transacções anteriormente devolvidas pelo Emissor. A SIBS FPS processará essa transacção de acordo com o descrito no fluxograma do processo (Figura 17). Não estão definidos limites para o número de reenvios de transacções pela Via Verde Portugal, nem para o número de vezes que o Emissor pode devolver as transacções.

Para terem disponível a possibilidade de devolver transacções, os Emissores apenas efectuam alterações aos seus sistemas e actua sobre as operações que impliquem efectiva devolução.

4.8.1.6 Transacções *offline*

Este cenário de autorização é aplicável quando o terminal suporta as especificações EMV, o cartão possui *chip* EMV e contém neste uma ou mais aplicações de pagamento. Mediante estas condições, as transacções são aprovadas entre o cartão e o terminal (*offline*) sem que seja necessário efectuar o seu envio para decisão central.

No diálogo entre cartão e terminal são validadas as componentes de segurança aplicáveis e verificados parâmetros posicionados no *chip* do próprio cartão correspondentes a limites de risco que o Emissor está disposto a assumir para este tipo de transacções.

Quando o valor de uma qualquer transacção supera um dos limites aplicáveis, esta não pode ser autorizada *offline*. A transacção é enviada para decisão *online* e a autorização da operação é efectuada no cenário de funcionamento que for aplicável.

Ao comunicar com o TPA, é verificado se o cartão permite a sua utilização como *offline*:

- Se não permite utilização como *offline*, a transacção é realizada *online* pela SIBS FPS;
- Se permite utilização como *offline*, são verificados os limites de risco do cartão no momento da sua emissão:
    - Se os limites de risco do cartão são atingidos, a transacção é feita *online* com a SIBS FPS;
    - Se os limites de risco do cartão não são atingidos, a operação é realizada *offline*.

Os limites para decisão de transacções em *offline* são posicionados no momento da emissão dos cartões, a partir dos elementos parametrizados no formulário "Caracterização do BIN". Podem ser alterados em qualquer momento posterior à emissão através do ficheiro EGCC - Gestão de Cartões e Contas.

Uma qualquer transacção realizada com utilização de dados de *chip* EMV só é aceite *offline* se verificar todos os valores posicionados no cartão, na respectiva aplicação EMV, para os seguintes parâmetros:

- Limites em valor
    - Valor acumulado para transacções *offline* realizadas nas moedas principal e secundária:
        - Máximo quando o terminal pode efectuar a transacção *online* – se o valor de uma transacção adicionada aos valores já despendidos em *offline* ultrapassar este limite, o terminal tenta enviar a transacção para decisão *online*. Se não for possível, a transacção pode ser aceite *offline* (depende dos restantes parâmetros);
        - Máximo a partir do qual a transacção tem obrigatoriamente que ser decidida *online* – se o valor de uma transacção adicionada aos valores já despendidos em *offline* ultrapassar este limite, essa transacção é rejeitada.
- Limites em número máximo de transacções consecutivas
    - Transacções internacionais:
        - Número de transacções quando o código de moeda é diferente do código de moeda principal da aplicação EMV;
        - Número de transacções quando o código de país é diferente do código de país da aplicação EMV.
- Limites globais
    - Número de transacções quando o terminal pode efectuar a transacção *online*;
    - Número de transacções a partir do qual a transacção tem que ser decidida *online*.

Os parâmetros de risco para autorização de transacções *offline* são inicialmente definidos através do formulário "Caracterização do BIN" ou da informação recebida para emissão dos cartões. Porém, no momento da emissão lógica, os parâmetros de risco podem ser alterados no ficheiro de produção de cartões.

Sempre que o Emissor envia um novo ficheiro EGCC - Gestão de Cartões e Contas com novos parâmetros para actualização, são formatados *scripts* para envio dos novos valores ao cartão. Os parâmetros de risco

posicionados no *chip* do cartão são actualizados num primeiro momento em que tal seja possível, quando se realizar uma transacção *online*.

4.8.1.7 Saldo de crédito disponível

O cenário de saldo de crédito disponível é utilizado quando o Emissor delega a decisão das operações dos seus cartões de crédito na SIBS FPS, quer por interrupção temporária da sessão de *real-time*, quer como cenário principal para esses cartões.

Neste cenário, e se não existirem motivos para recusa resultantes das validações descritas no início da secção 4.7 - Autorização, as operações são decididas pela SIBS FPS com base nos ficheiros ESCD – Comunicação de Saldos de Crédito enviados periodicamente pelo Emissor, com a informação relativa aos saldos disponíveis, geral e para levantamentos, das respectivas contas crédito que sofreram variações desde o último ficheiro ESCD – Comunicação de Saldos de Crédito enviado pelo Emissor.

Sempre que o Emissor transmitir um novo ficheiro ESCD – Comunicação de Saldos de Crédito, pressupõe-se que indica os novos saldos de uma conta-crédito. Se tal não acontecer para uma conta cujos cartões efectuaram operações financeiras na Rede MULTIBANCO, a SIBS FPS actualiza os respectivos saldos com os últimos valores informados pelo Emissor, isto é, desprezando as importâncias das operações entretanto feitas pelos Titulares de Cartões na Rede MULTIBANCO.

4.8.1.7.1 Levantamentos

A decisão de uma operação de levantamento pela SIBS FPS é efectuada com base nos seguintes valores:

- Saldo disponível geral da conta-crédito associada ao cartão, enviado no ficheiro ESCD – Comunicação de Saldos de Crédito;
- Saldo disponível para levantamentos da mesma conta-crédito, enviado no ficheiro ESCD – Comunicação de Saldos de Crédito.

Diariamente, na primeira operação do cartão, o menor destes dois valores é utilizado como o montante disponível para decidir operações:

- Se o valor de uma operação for inferior ao montante disponível, aquela é autorizada e o seu valor é deduzido a este até ser igual a zero;
- Em caso contrário, aquela é recusada.

4.8.1.7.2 Outras operações

A autorização das restantes operações pela SIBS FPS é efectuada com base no saldo disponível geral da conta-crédito:

- Se o valor da operação a débito for inferior ao saldo disponível geral da conta-crédito, aquela é autorizada e o seu valor é deduzido a este até ser igual a zero;
- Em caso contrário, aquela é recusada.

4.8.1.8 Utilização múltipla de cenários

Um Emissor pode seleccionar um cenário de autorização inicial para decisão das suas transacções e depois evoluir para outro cenário de autorização, fazendo uma utilização múltipla de cenários.

Normalmente, os CPDs dos Emissores cujo cenário de funcionamento principal é o *real-time* têm um cenário de degradação (Saldo de Conta ou Saldo de Cartão) como meio alternativo de decisão, no caso de ocorrerem interrupções da sessão *real-time*.

Adicionalmente, o Emissor pode definir um cenário controlado para as situações em que planeia desligar a sessão de *real-time* (por exemplo, num fim de semana ou feriado para proceder à manutenção ou melhoramento do seu sistema).

Especificamente para os cartões de serviço (ver secção 3.4.1), a SIBS FPS desenvolveu um cenário que permite viabilizar as especificidades destes cartões. O cenário Saldo de Cartão / Saldo de Conta (ou *real-time*) associando aos cartões de serviço permite a validação da disponibilidade do saldo de cartão antes de verificar o saldo de conta ou efectuar uma mensagem *real-time* com o Emissor.

Assim, as operações dos utilizadores estão controladas por um saldo individual de cartão, mas a totalidade dos movimentos de todos os cartões de uma conta não pode ultrapassar o limite posicionado na conta (saldo de conta) ou existente no Emissor (*real-time*).

4.8.2 Cenários para autorização de operações noutras redes

A autorização das operações realizadas noutras redes processa-se, preferencialmente, através da troca de mensagens *real-time* com o Emissor. Caso esse cenário não esteja disponível, as operações são autorizadas através do cenário de degradação escolhido pelo Emissor em conjugação com limites de autorização. Estes limites são diários e pretendem baixar os montantes autorizados em degradação com o intuito de minimizar o risco do Emissor na aceitação de operações desta natureza.

De seguida, são apresentados os cenários disponíveis para autorização de operações noutras redes.

4.8.2.1 Limite de autorização

O cenário de limite de autorização destina-se a operações realizadas no estrangeiro, por cartões nacionais pertencentes a um SPI, sempre que as mensagens desencadeadas em *real-time*, do terminal ou ponto de serviço para a SIBS FPS, são apenas “pedidos de autorização” e não mensagens financeiras.

No cenário de limite de autorização, a gestão das autorizações é processada consoante o cenário principal do CPD do Emissor para as operações acima referidas.

A utilização do cenário de Limite de autorização pode ter variantes descritas de seguida.

LIMITE DE AUTORIZAÇÃO EM *REAL-TIME* COM O EMISSOR

Este limite de autorização ocorre na ligação *real-time*, onde mensagens recebidas de um Sistema de Pagamento são enviadas da SIBS FPS ao Emissor como pedidos de autorização, sendo o Emissor que decide, em tempo real, destino a realização das operações:

- Aceitando a autorização;
- Pedindo à SIBS FPS para decidir a autorização em função do cenário de degradação existente;
- Recusando o pedido (por saldo insuficiente, suspeita de fraude ou outro motivo);
- Pedindo para capturar o cartão.

O Emissor tem de cumprir os tempos mínimos de resposta impostos pelos SPI que não podem exceder os dois segundos.

As autorizações concretizadas são enviadas pelo serviço de compensação. O processo de compensação (*clearing*) efectuado pelo Sistema de Pagamento pode ser realizado pela SIBS FPS ou directamente pelo Emissor. No primeiro caso, sempre que a SIBS FPS receba, no *clearing* do sistema internacional, uma operação firme que consiga emparelhar com uma mensagem de autorização prévia, preenche o correspondente registo do ficheiro DST5 – Destinos de modo a informar o Emissor deste facto.

Adicionalmente, para operações de levantamento, o Emissor pode ter indicado à SIBS FPS um montante máximo diário para levantamentos que é validado previamente ao envio do pedido de autorização ao Emissor, sendo este recusado, caso o montante de autorizações relativas a operações de levantamento tenha excedido, no dia, o limite posicionado.

Caso o Emissor não indique nenhum montante, a SIBS FPS considera o montante máximo diário de 500€.

Neste cenário, o Emissor pode obter serviço de degradação da SIBS FPS e controlo total dos pedidos recebidos incluindo as operações que foram aceites em *real-time* pelo CPD do Emissor.

Caso o Emissor não pretenda utilizar o serviço de degradação da SIBS FPS, tem de indicar qual a resposta a enviar pela SIBS FPS ao Sistema de Pagamento, sempre que não seja obtida uma resposta em *real-time* do Emissor:

- Recusa;
- Pedido de degradação no Sistema de Pagamento (nos parâmetros de *stand-in* previamente posicionados pelo Emissor);
- Pedido de *referral* (este pedido ocorre quando o Emissor não consegue aprovar a operação, segundo os processos habituais, mas não quer que o Titular de Cartão saia sem realizar a operação; por isso pede ao Comerciante para telefonar ao aceitante / representante local do cartão, no sentido de obter mais informações sobre a operação em causa para ajudar à sua concretização).

O Emissor pode ainda parametrizar qual destes três tipos de resposta devem ser enviados pela SIBS FPS, caso tenha sido activado um dos cenários de degradação descritos em seguida e a autorização exceda os limites posicionados na SIBS FPS.

LIMITE DE AUTORIZAÇÃO EM DEGRADAÇÃO COM O EMISSOR

O cenário posicionado para o Emissor é um dos seguintes:

- *Real-time* com o Emissor mas, embora o Emissor processe os pedidos de autorização, este respondeu com um pedido de degradação na SIBS FPS, ou não respondeu a tempo e posicionou um cenário de degradação na SIBS FPS;
- Saldo de conta;

- Saldo de cartão;
- Saldo disponível de conta-crédito.

Nestes casos é a SIBS FPS que, por delegação do Emissor, decide o pedido de autorização. A decisão é tomada de acordo com os valores posicionados nos montantes máximos diários por BIN, nos saldos disponíveis informados por conta-corrente ou conta-crédito (competindo ao Emissor garantir a sua actualização quando posiciona novos valores na SIBS FPS), ou no valor presente no saldo de cartão.

Com o objectivo de reduzir o factor de risco e antes de se verificar qual o cenário de processamento da autorização, efectua-se uma validação prévia às autorizações de levantamento ou autorizações de *cash-advance* parametrizadas para serem decididas como levantamento sobre o montante máximo diário para levantamentos (caso o Emissor o tenha informado no formulário "Caracterização do BIN") ou o valor predefinido no sistema central da SIBS FPS.

No caso de uma **operação de levantamento**, dependente do cenário de degradação escolhido pelo Emissor, a decisão do pedido de autorização pela SIBS FPS é efectuada com base nos seguintes valores:

Saldo de Conta

- Saldo disponível da conta associada ao cartão, enviado no ficheiro ECSV – Comunicação de Saldos de Véspera;
- Montante máximo diário para levantamentos até ao qual a SIBS FPS autoriza operações de levantamento no estrangeiro, parametrizado no formulário "Caracterização do BIN".

Diariamente, na primeira operação do cartão, o menor destes dois valores é utilizado como o montante disponível para decidir autorizações:

- Se o valor do pedido de autorização for inferior ao montante disponível, aquele é autorizado e o seu valor é deduzido a este até ser igual a zero;
- Em caso contrário, aquele é recusado.

Saldo de Cartão

- Saldo utilizável para autorizar apenas operações de levantamento na Rede CA MULTIBANCO, (montante guardado na Pista 3 da pista magnética do cartão ou guardado no sistema central da SIBS FPS)
- Montante máximo diário para levantamentos até ao qual a SIBS FPS autoriza operações de levantamento no estrangeiro, parametrizado na "Caracterização do BIN".

Diariamente, na primeira operação do cartão, o menor destes dois valores é utilizado como o montante disponível para decidir autorizações:

- Se o valor do pedido de autorização for inferior ao montante disponível, aquele é autorizado e o seu valor é deduzido a este até ser igual a zero;
- Em caso contrário, aquele é recusado.

Saldo Disponível de Conta-Crédito

- Saldo disponível para *cash-advance* da conta-crédito associada ao cartão, enviado no ficheiro ESCD – Comunicação de Saldos de Crédito que também é actualizado pelas mensagens de resposta *real-time* a pedidos de levantamento a crédito que contenham o campo saldo disponível provenientes da Rede CA MULTIBANCO.

Diariamente, na primeira operação do cartão, este saldo é utilizado como o montante disponível para decidir autorizações:

- Se o valor do pedido de autorização for inferior ao montante disponível, aquele é autorizado e o seu valor é deduzido a este até ser igual a zero;
- Em caso contrário, aquele é recusado.

No caso de **outras operações**, as descrições seguintes reportam-se sempre a um total de autorizações pendentes, que correspondem ao somatório dos montantes de operações autorizadas na Rede TPA MULTIBANCO que ainda não se tornaram "firmes" (isto é, das quais ainda não foi recebido o respectivo movimento financeiro no ficheiro de compensação do Sistema de Pagamento) e que não atingiram o limite do número de dias posicionado pelo Emissor para o BIN, para manutenção de uma autorização como pendente.

Desta forma e consoante o cenário escolhido pelo Emissor, a SIBS efectua a decisão do pedido de autorização com base nos seguintes valores:

Real-Time

- Saldo disponível da conta associada ao cartão, recebido na resposta da consulta;
- Total de autorizações pendentes.

O processo de decisão do pedido de autorização é o seguinte:

- Se o somatório do valor do pedido de autorização com o total das autorizações pendentes for inferior ao saldo disponível, aquele é autorizado e o seu valor é adicionado ao total das autorizações;
- Em caso contrário, aquele é recusado.

Saldo de Conta

- Saldo disponível da conta associada ao cartão, enviado no ficheiro ECSV – Comunicação de Saldos de Véspera, que também é actualizado pelas mensagens de resposta *real-time* que contenham o campo saldo disponível provenientes da Rede CA MULTIBANCO;
- Total de autorizações pendentes.

O processo de decisão do pedido de autorização é o seguinte:

- Se o somatório do valor do pedido de autorização com o total das autorizações pendentes for inferior ao saldo disponível, aquele é autorizado e o seu valor é adicionado ao total das autorizações;
- Em caso contrário, aquele é recusado.

Saldo de Cartão

- Montante máximo diário para outras operações até ao qual a SIBS FPS autoriza outras operações (que não levantamentos) no estrangeiro, parametrizado no formulário "Caracterização do BIN";
- Total de autorizações pendentes.

O processo de decisão do pedido de autorização é o seguinte:

- Se o somatório do valor do pedido de autorização com o total das autorizações pendentes for inferior ao montante máximo diário, aquele é autorizado e o seu valor é adicionado ao total das autorizações;
- Em caso contrário, aquele é recusado.

Saldo Disponível de Conta-Crédito

- Saldo disponível da conta-crédito associada ao cartão, enviado no ficheiro ESCD – Comunicação de Saldos de Crédito, que também é actualizado pelas mensagens de resposta *real-time* a pedidos de levantamento a crédito que contenham o campo saldo disponível provenientes da Rede CA MULTIBANCO;
- Total de autorizações pendentes.

O processo de decisão do pedido de autorização é o seguinte:

- Se o somatório do valor do pedido de autorização com o total das autorizações pendentes for inferior ao saldo disponível, aquele é autorizado e o seu valor é adicionado ao total das autorizações;
- Em caso contrário, aquele é recusado.

Diariamente, todas as autorizações que tenham sido dadas há mais de X dias (X = número indicado pelo Emissor para cada BIN, ou 4 dias por defeito) são subtraídas ao total de autorizações pendentes pois considera-se que a operação já não será enviada ou foi enviada e não foi possível emparelhá-la com uma autorização prévia.

A SIBS FPS valida todas as autorizações para detectar operações duplicadas e todas as anulações de autorizações prévias, são deduzidas ao total de autorizações pendentes.

LIMITE DE AUTORIZAÇÃO EM *REAL-TIME* COM O REPRESENTANTE

Este cenário é semelhante ao cenário de limite de autorização em *real-time* com o Emissor mas, neste cenário, as mensagens *real-time* são trocadas entre a SIBS FPS e um representante de cartões. As mensagens recebidas de um Sistema de Pagamento são enviadas pela SIBS FPS em *real-time* ao representante como pedidos de autorização, sendo o representante que decide, em tempo real, a realização das operações:

- Aceitando a autorização;
- Recusando o pedido (por saldo insuficiente, suspeita de fraude ou outro motivo);
- Pedindo para capturar o cartão.

O representante tem de cumprir os tempos mínimos de resposta impostos pelos SPI que não podem exceder os dois segundos.

As autorizações concretizadas são apresentadas ao Emissor pelo representante, através de interfaces próprios definidos entre ambos. O processo de compensação efectuado pelo Sistema de Pagamento é realizado pelo representante.

Para operações de levantamento, o Emissor pode ter indicado à SIBS FPS um montante máximo diário para levantamentos que é validado previamente ao envio do pedido de autorização ao representante. A SIBS FPS recusa o levantamento se o montante de autorizações relativas a operações de levantamento tenha excedido, no dia, o limite posicionado. Caso o Emissor não indique nenhum montante, a SIBS FPS considera o montante máximo diário de 500€.

Nestas circunstâncias, não é enviada ao representante nenhuma mensagem de pedido de autorização. Este cenário não inclui serviço de degradação na SIBS FPS.

Para as situações em que não exista uma recusa da SIBS FPS resultante da validação prévia do montante para operações de levantamento, o Emissor tem de indicar qual a resposta a enviar pela SIBS FPS ao Sistema de Pagamento sempre que não seja obtida uma resposta em tempo real do representante:

- Recusa;
- Pedido de degradação no Sistema de Pagamento (nos parâmetros de *stand-in* previamente posicionados pelo Emissor);
- Pedido de *referral* (este pedido ocorre quando o representante não consegue aprovar a operação, segundo os processos habituais mas o Emissor não quer que o Titular de Cartão saia sem realizar a operação; por isso pede ao Comerciante para telefonar ao aceitante / representante local do cartão, no sentido de obter mais informações sobre a operação em causa para ajudar à sua concretização).

4.8.2.2 Saldo de crédito disponível

O cenário de crédito disponível é utilizado quando o Emissor delega a decisão das operações dos seus cartões de crédito na SIBS, seja por interrupção temporária da sessão *real-time* ou como cenário principal para esses cartões.

Neste cenário também são aplicadas as validações iniciais descritas na secção 4.7, e caso não existam motivos para recusa, as operações são decidas pela SIBS FPS com base no ficheiro ESCD – Comunicação de Saldos de Crédito enviado periodicamente pelo Emissor com a informação relativa as saldos disponíveis, geral e para levantamentos, das respectivas contas crédito que sofreram variações desde o último ficheiro enviado.

Sempre que um Emissor enviar um novo ficheiro ESCD – Comunicação de Saldos de Crédito, a SIBS FPS pressupõe que este indica novos saldos de uma conta-crédito. Se tal não acontecer para uma conta cujos cartões realizaram operações financeiras na Rede CA e TPA MULTIBANCO, a SIBS FPS actualiza o respectivo saldo com os últimos valores informados pelo Emissor, isto é, desprezando as importâncias das operações entretanto realizadas pelos clientes na Rede MULTIBANCO.

No caso de **operações de levantamento**, a SIBS FPS efectua a decisão com base nos seguintes valores comunicados via ficheiro ESCD – Comunicação de Saldos de Crédito:

- Saldo disponível geral da conta-crédito associada ao cartão;
- Saldo disponível para levantamentos da mesma conta-credito.

Diariamente, na primeira operação do cartão, o menor destes dois valores é utilizado como montante disponível para decidir operações.

- Se o valor de uma operação for inferior ao montante disponível, aquela é autorizada e o seu valor é deduzido a este até ser igual a zero;
- Em caso contrário, é recusada.

No caso das **restantes operações a crédito**, a autorização é feita com base no saldo disponível geral da conta-crédito, onde:

- Se o valor da operação a débito for inferior ao montante disponível, aquela é autorizada e o seu valor é deduzido a este até ser igual a zero;
- Em caso contrário, é recusada.

4.8.3 3D Secure

O serviço de 3D Secure para Cartões Reais permite a realização de operações de autenticação, autorização, compensação e liquidação de compras efectuadas na Internet, com garantias acrescidas de segurança para os clientes e comerciantes *online* (vertente 3D Secure Emissor). No momento da compra, e antes de ser autorizada a transacção, será efectuada a autenticação do cliente.

Para que o cliente possa efectuar transacções com segurança, terá de realizar numa primeira fase a adesão ao serviço 3D Secure com cartão reais. No momento de adesão, o cliente irá escolher com qual dos métodos de autenticação disponíveis pretende utilizar o serviço. Os métodos disponibilizados nesta fase são parametrizados pelo Emissor ao nível do formulário “Caracterização de BIN”.

O processo transaccional para a realização de um de pagamento online com cartões reais 3D Secure em comerciante 3D Secure, considerando que o portador de cartão aderiu ao serviço, encontra-se esquematizado na seguinte figura.

4.8.3.1 Processo de compra

O processo transaccional para a realização de um de pagamento online com cartões reais 3D Secure em comerciante 3D Secure, considerando que o portador de cartão aderiu ao serviço, encontra-se esquematizado na seguinte figura:

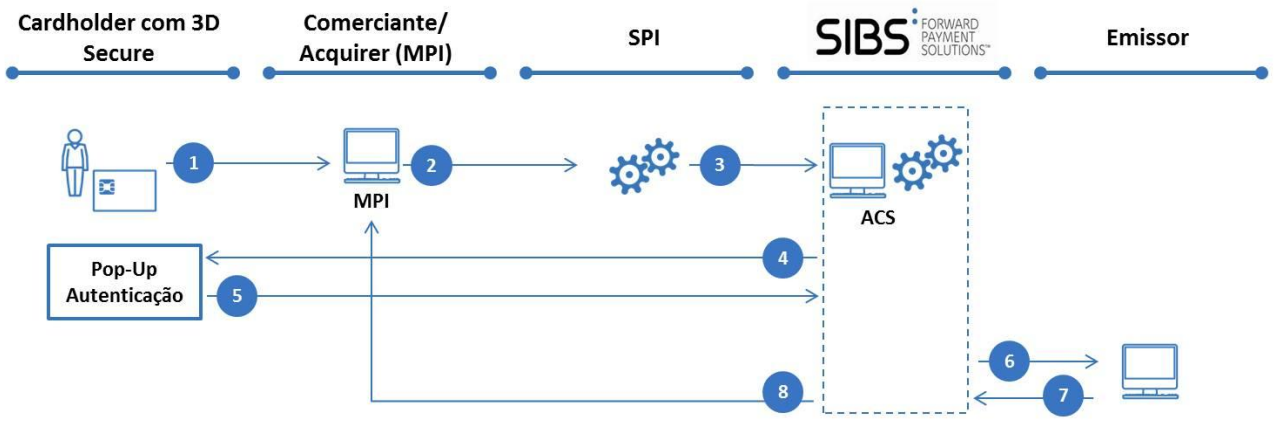

Figura 19 - Processo de Compra 3D Secure

Tabela 8 - Processo de Compra 3D Secure

N.º	Actividade
1	O Cardholder com um cartão 3D Secure introduz o número de cartão, data de expiração e CVV2 (ou equivalente) no *website* do comerciante 3D Secure, através do servidor MPI – *Merchant Plug-in* – do *Acquirer*.
2	Comerciante envia os dados de cartão para o SPI, para que este valide o cartão.
3	SPI dá *feedback* sobre registo do BIN do cartão à SIBS FPS, após validação de que o BIN foi inscrito como 3D Secure.
4	O *Access Control Server* (ACS) da SIBS FPS despoleta um *pop-up* para recolha das credenciais adicionais (*password*) para a autenticação do *Cardholder*.
5	*Cardholder* coloca *password* das credenciais 3D Secure no *pop-up.*
6	O ACS da SIBS FPS valida a *password* das credenciais e se esta estiver correcta, é feita a autorização da transacção via *real-time* com o Emissor ou através do cenário de autorização seleccionado pelo Emissor. (ver Cenários de Autorização na secção 4.7).
7	SIBS FPS recebe do Emissor 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.
8	SIBS FPS envia decisão da autorização da transacção para o Comerciante/*Acquirer*. Em processo de final de dia, o Emissor deverá receber, via Ficheiro de Destinos as operações de autenticação efectuadas para os seus cartões, com indicação do canal.

4.8.3.2 Princípios orientadores

As componentes chave de uma autenticação através de 3D Secure são:

- Para uma compra ser considerada 3D Secure, o Comerciante também tem que ser 3D Secure;
- O ACS da SIBS só irá processar autorizações 3D Secure para cartões reais para os sistemas de pagamento internacionais VISA e MasterCard;
- O processo de decisão da operação será similar ao processo actual do MBNET em operações Verified By VISA (VISA) / SecureCode (MasterCard), sendo a operação classificada sempre uma transacção nacional no estrangeiro;
- Não basta somente o Emissor caracterizar o BIN dos seus cartões reais no processo de adesão ao novo serviço 3D Secure da SIBS. O Emissor deverá previamente assegurar que o SPI respectivo

tem essa informação caracterizada, caso contrário a operação será recusada e/ou degradada no ponto inicial da Autenticação;

- Não é obrigatório (mas sim recomendável) que os cartões Maestro *on-us* estejam inscritos no MasterCard SecureCode, por razões de *liability shift* em processos de disputa;
- Na renovação de cartões, e se o cartão anterior for aderente ao método de autenticação por MB CODE, é necessário que o novo cartão tenha a aplicação SAF associada;
- Na alteração de situação do cartão, quando um cartão real for colocado em lista negra, e se este for aderente ao serviço 3D Secure cartões reais, o processo terá de cancelar o serviço.

4.8.4 *Recurring transactions*

Uma *Recurring Transaction* é uma transacção recorrente, isto é, uma transacção em que um Titular de um cartão autoriza um Comerciante a que, de forma periódica, proceda a débitos na sua conta, pelo fornecimento recorrente de bens ou serviços, ao longo do tempo.

Exemplos de *Recurring Transaction*s:

- Assinatura de uma publicação, com existência de pagamentos periódicos em intervalos regulares (mensais, ou anuais, etc.), cada um dos quais corresponde a um período da assinatura;
- Compra de publicidade na Internet, com existência de pagamentos periódicos em intervalos regulares, cada um dos quais corresponde a um período da vigência da acção publicitária.

O intervalo temporal entre duas operações consecutivas associadas a uma *recurring transaction* não pode exceder um ano. Neste sentido, se o titular de um cartão estabelecer, por exemplo, um acordo com um Comerciante pelo prazo de cinco anos, então, até ao final do quinto ano, duas transacções consecutivas podem ter qualquer período de intervalo entre si (incluindo um ano) mas não podem exceder mais do que um ano de intervalo.

As transacções Recurring podem ser iniciadas em vários ambientes: *Card Present* ou *Card-Not-Present (CNP)*; e, dentro destes ambientes, podem ser presenciais, em POS, ou via correio, telefone, fax, e-mail, internet (E-commerce). Muitas destas transacções são também transacções MO/TO (Mail Order/Telephone Order).

O acesso a esta funcionalidade por um Emissor implica que este tenha parametrizado no formulário "Caracterização de BIN" a permissão para a realização destas transacções. Uma autorização que chegue à SIBS FPS para um BIN que não esteja caracterizado para aceitar transacções *recurring* será recusada.

4.8.4.1 Princípios orientadores

As componentes chave de uma *recurring transaction* são:

- Entre o Titular de Cartão e o Comerciante tem que ser estabelecida uma autorização (dada pelo Titular de Cartão) para a realização da transacção. Esta autorização pode ser conservada pelo Comerciante, quer em formato papel, quer em formato electrónico, durante o prazo de vigência da *recurring transaction*;

- As múltiplas transacções associadas a uma *recurring transaction* reportam-se ao acordo estabelecido entre o Comerciante e o Titular de Cartão, segundo o qual a relação de pagamentos inclui mais de um pagamento durante um período que, entre dois pagamentos, não pode ser superior a um ano;
- O início de uma *recurring transaction* pode ser assegurado quer pelo Titular de Cartão, quer pelo Comerciante. Nas operações subsequentes, é o Comerciante quem, na maior parte dos casos, toma a iniciativa de processar o pagamento. Contudo, por vezes pode ser o Titular de Cartão a fazê-lo, de acordo com os termos do acordo estabelecido com o Comerciante;
- O montante da transacção pode manter-se o mesmo ou variar de um período para outro (por exemplo, uma instituição que preste um serviço baseado numa assinatura pode cobrar o mesmo montante todos os meses, enquanto que uma instituição fornecedora de serviços públicos pode cobrar montantes diferentes, de acordo com os níveis de consumo mensais);
- Os titulares de cartões devem ser informados de que, caso aconteça alguma mudança no número do seu cartão / PAN, devem dar conhecimento desse facto ao Comerciante de modo a refazer o acordo.

4.8.4.2 Autorização de *recurring transactions*

A principal diferença entre as *recurring transactions* e as transacções de outros tipos reside no tratamento diferenciado entre a primeira transacção apresentada para autorização e as transacções subsequentes.

Na primeira transacção são enviados ao Emissor, quer via pedido de autorização, quer via ficheiro de compensação, todos os dados da transacção, incluindo os dados do cartão. Nesta transacção, a SIBS FPS passa a reconhecer o indicador que identifica uma *recurring transaction*, registando qual o cartão utilizado e o Comerciante que acolheu a operação.

Nas transacções subsequentes, desencadeadas pelo Comerciante, estar-se-á sempre em ambiente *card-not-present* pelo que o CVV2 pode não ser incluído pelo Comerciante no detalhe da transacção (essa inclusão é opcional).

Em qualquer dos casos, a SIBS FPS envia um pedido de autorização ao Emissor em *real-time*. Se o Emissor não comunicar uma resposta nesse âmbito, a SIBS FPS passa a autorização para o cenário de degradação delegado pelo Emissor na SIBS FPS e fornece a resposta em conformidade.

Na primeira *recurring transaction*, a SIBS FPS assegura um conjunto de validações com vista a garantir a integridade da operação:

- Identificação da autorização como estando associada a uma *recurring transaction*;
- Validação da correcta formatação da autorização (preenchimento dos elementos obrigatórios para a *recurring transaction*);
- Confirmação da parametrização do BIN para realizar *recurring transactions*, via consulta à caracterização do indicador de *recurring*.

- Inserção da primeira operação de *recurring transaction* pela chave, PAN / Comerciante, no novo repositório (base de dados) criado para a gestão das operações de *recurring*.

Alguns dados da primeira transacção são guardados num repositório de dados especialmente criado para se identificar as operações subsequentes a partir da primeira transacção. A alimentação dessa base de dados será feita a partir de uma mensagem em *real-time*. Os Emissores acedem a esse repositório de dados via PSS, no qual podem consultar *recurring transactions* e os respectivos cartões e ainda listar e alterar acordos.

Nas operações de *card-not-present* é assegurada a validação da informação presente na mensagem de autenticação. Caso o campo da mensagem de *recurring* esteja preenchido com uma data válida (data superior à data do dia da autenticação) é assegurado que esta data nunca é superior à data de expiração do cartão.

Nas transacções subsequentes à primeira operação, a recepção e gestão das transacções é controlada a partir do repositório de *recurring transactions*, com base no acordo e na combinação do número de cartão / Comerciante e no estado da autorização para o serviço de *recurring transactions*. A cada pedido de autorização, a SIBS FPS verifica se existe a primeira operação para aquele número de cartão e se o estado do acordo entre esse número e o Comerciante se encontra activo.

Todos os contractos presentes no repositório com a combinação número do cartão / Comerciante, em que a data da última autorização seja superior a um ano, serão automaticamente desactivados e passados para histórico, permitindo que o Titular de Cartão possa realizar um novo acordo *recurring* com o mesmo Comerciante e gerar assim um novo pedido de autorização, caso o deseje. A data da última autorização é actualizada a cada novo pedido de autorização subsequente aceite.

As validações dos pedidos de autorização do serviço de *recurring transactions* têm algumas particularidades que as distinguem das restantes autorizações:

- O Comerciante deverá ter fornecido os seus contactos junto com o envio do pedido de autorização;
- Há verificação do CVV2: A verificação deste código é obrigatória na primeira transacção *recurring*; as operações subsequentes podem ser aceites sem a sua verificação;
- O Montante da transacção poderá não ser constante entre as várias transacções que, para o mesmo acordo *recurring*, forem chegando ao longo do tempo. Tal sucede porque um Comerciante poderá cobrar importâncias diferentes, de acordo, p. ex. com a variação do consumo do Titular do Cartão.
- Data de expiração do cartão: se a data de expiração do cartão vier preenchida na mensagem, esta será validada. Se a validação foi bem sucedida, a transacção procede, caso contrário, rejeita-se. Caso a data de expiração não venha preenchida na mensagem, a transacção não é recusada por este motivo.
    - Pedido de autorização intra-regional: Não é possível rejeitar pedidos de autorização apenas por motivo de data de expiração incorrecta, data de expiração inválida, ou data de expiração ausente (não formatada);

- Pedido de autorização inter-regional: Em caso de ocorrência de situações associadas à data de expiração descritas no ponto anterior, fica ao critério do Emissor a decisão de aceitação ou rejeição do pedido de autorização;

- Tendo um Acordo PAN / Comerciante sido cancelado pelo Emissor no PSS, perante a chegada de um pedido de autorização respeitante a esse Acordo, a SIBS FPS emitirá uma rejeição de autorização. Isto implica que o Titular do cartão tenha comunicado previamente o cancelamento do acordo ao respectivo Comerciante; presume-se assim que esse procedimento tenha sido assegurado;
- Quando um PAN é inibido por um Emissor, via PSS, para todas as operações de *recurring*, a SIBS FPS emitirá um outro tipo de rejeição de autorização. Presume-se que o Emissor inibiu esse PAN, a pedido do Titular do cartão, pelo que se assume que o recebimento de pedidos de autorização tem origem fraudulenta.
- Sempre que o PAN do cartão que fez um acordo *recurring* for alterado (p. ex. pelo motivo de o cartão original ter sido substituído ou renovado), o Cliente deve informar o Comerciante da mudança do PAN, para que este actualize o Acordo. Perante a chegada de uma transacção subsequente à 1ª, em que o PAN em vigor não coincida com o da 1ª transacção, a SIBS FPS recusará a transacção.

4.8.4.3 Marcas internacionais

A aplicação deste serviço está disponível para a marca VISA/VISA Electron e MasterCard/Maestro.

Como já foi referido acima, para que isso seja possível o acesso do Emissor a esta funcionalidade, este deve seleccionar a opção disponível no formulário “Caracterização de BIN”.

Contudo, existe uma particularidade associada aos Cartões Maestro: segundo as regras da MasterCard, um Emissor só pode aceitar uma *recurring transaction* com validação 3D Secure caso o Comerciante esteja inscrito no programa MARP (MasterCard Advanced Registration Program) da MasterCard. Nesse caso, quando é enviada uma *recurring transaction* o código dinâmico gerado pelo ACS resultante da autenticação é um código fixo para que a transacção possa ser aceite.

4.8.5 *Account verification*

A operação de *Account Verification* permite aos Comerciantes confirmar a autenticidade do cartão apresentado pelo Cliente e da conta associada, sem gerar um cativo na conta.

A VISA introduziu a funcionalidade de *Account Verification* para permitir aos Comerciantes a confirmação dos dados do cartão apresentado pelo Cliente e a MasterCard publicou a existência do *Account Status Inquiry Service*, uma operação com os mesmos princípios de funcionamento.

A operação de *Account Verification* faculta aos Comerciantes a possibilidade de confirmação dos dados do cartão apresentado pelo Cliente. Esta funcionalidade permite que estes Comerciantes (por exemplo, com TPA físico ou TPA Virtual) efectuem uma verificação da existência da conta do cartão utilizando uma

autorização com montante "zero" como valor da transacção. Permite ainda validar o código de segurança (CVV2 ou CVC2, no caso da VISA e MasterCard respectivamente).

O *Account Verification* tem como objectivo eliminar as transacções de uma unidade monetária para validar o estado do cartão (por exemplo, 1,00 €), bem como eliminar os cativos indevidos nas contas dos clientes.

Para aceder a esta funcionalidade, os Emissores devem parametrizar os BINs através do formulário "Caracterização de BIN", para passarem a permitir esta validação de dados.

4.9 Compensação

Este serviço de contratação obrigatória pelos Emissores consiste no apuramento do saldo diário, financeiro, de cada instituição interveniente do serviço, bem como dos Sistemas de Pagamento Internacional, e respectivo envio de informação de suporte e para liquidação.

Assim, compensação é o apuramento do saldo financeiro de cada instituição participante no serviço e liquidação é a afectação financeira das suas contas.

Para o apuramento dos saldos de compensação, a SIBS FPS utiliza o registo de todas as operações aceites na Rede MULTIBANCO ao longo do dia. Os saldos da compensação são enviados para o TARGET2[6], servindo de base à sua liquidação neste sistema.

Cada operação na Rede MULTIBANCO dá origem a uma troca de mensagens e/ou ficheiros entre o TPA onde decorre a operação, o BAC, a SIBS FPS, o Emissor do cartão utilizado na operação e o *Acquirer*, ou o SPI (como intermediário do Emissor) no caso dos cartões *not-on-us*. Para o apuramento dos saldos de compensação, a SIBS FPS utiliza o registo de todas as operações aceites ao longo do dia.

No caso das operações realizadas na Rede MULTIBANCO, Os saldos são enviados para o TARGET2, servindo de base à sua liquidação no Sistema de Pagamentos Global.

No caso das operações realizadas noutras redes, Cada operação realizada noutra rede, que não a Rede MULTIBANCO, dá origem a uma troca de mensagens e ficheiros entre o *Acquirer* da operação e o Emissor tendo como intermediários o SPI e a SIBS FPS (como processador do Emissor). O serviço de compensação apura os valores que devem ser lançados aos clientes do Emissor por contrapartida da Entidade de Apoio ao *Settlement* (esta função é normalmente também assegurada pelo Emissor). Neste caso, a SIBS FPS não envia saldos para liquidação financeira junto do TARGET2. A responsabilidade da liquidação é do SPI e do *Acquirer*.

4.9.1 Horários da compensação

O fecho da compensação realiza-se no final de cada dia de calendário, no horário estabelecido pelo regulamento do Sistema de Compensação Interbancária (SICOI), ocorrendo a liquidação no dia útil seguinte

[6] O TARGET2 é o sistema de liquidação do Eurosistema, destinado às transacções de grande montante, em tempo real. Está baseado numa infra-estrutura central e integrada, designada "*Single Shared Platform*". Para além do processamento de pagamentos, inclui ainda outras funcionalidades, tais como a gestão de liquidez e o interface avançado para a liquidação dos *Ancillary systems*.

de funcionamento do sistema TARGET2. Os processos de compensação executados aos fins-de-semana e feriados são liquidados pelo TARGET2 no dia útil seguinte deste sistema.

De modo a diminuir o volume de dados a processar em cada compensação e a reduzir o risco inerente a eventuais problemas de processamento, a SIBS FPS realiza diariamente três sub-fechos a que corresponde uma única compensação e um único envio para liquidação.

A compensação no ambiente de Produção é efectuada de acordo com o seguinte horário, todos os dias (incluindo sábados, domingos e feriados):

- 09h00 - Sub-fecho;
- 15h00 - Sub-fecho;
- 20h00 - Fecho.

Cada sub-fecho da compensação origina uma actualização de período contabilístico dos diversos sub-sistemas da SIBS FPS. O fecho da compensação, para além de originar também uma actualização de período contabilístico dos diversos sub-sistemas, gera também os ficheiros da compensação e o envio para liquidação.

No ambiente de Pré-Produção, a compensação realiza-se de acordo com o seguinte horário, todos os dias (incluindo sábados, domingos e feriados):

- 11h00 - Sub-fecho;
- 15h00 - Sub-fecho;
- 22h00 - Fecho.

4.9.2 Tipo de participante na compensação

A participação dos Emissores no sistema da SIBS FPS pode realizar-se a dois níveis:

- Participante directo (ou liquidatário) - A SIBS FPS procede ao apuramento diário dos saldos de compensação do participante e envia para liquidação no TARGET2.
- Participante indirecto (ou não liquidatário): A SIBS FPS procede ao apuramento diário dos saldos de compensação do participante e envia para liquidação no TARGET2 através do participante directo que o representa. O participante indirecto recebe da SIBS FPS informação sobre os valores considerados. O acerto dos fundos entre o participante indirecto e o seu representante é efectuado entre as duas Instituições através da informação da compensação enviada pela SIBS FPS ao participante directo.

4.9.3 Compensação de operações na Rede MULTIBANCO

O serviço da SIBS FPS que consiste na compensação de operações na Rede MULTIBANCO tem como objectivo o apuramento diário dos saldos interbancários resultantes das operações realizadas nesta rede. Os saldos são enviados para o TARGET2, servindo de base à sua liquidação no Sistema de Pagamentos Global.

A compensação debita os Emissores da sua movimentação para creditar os Bancos de Apoio aos Terminais onde as transacções foram realizadas.

4.9.4 Compensação de operações noutras redes

O serviço da SIBS FPS que trata da compensação de operações noutras redes apura os valores que devem ser lançados aos clientes do Emissor por contrapartida da Entidade de Apoio ao *Settlement* (esta função é normalmente também assegurada pelo Emissor).

Nesta vertente, a SIBS FPS debita o Emissor mas a creditação dos valores movimentados é feita na conta de apoio ao *Settlement* que o SPI tem em Portugal.

Nesta vertente, a SIBS FPS não envia saldos para liquidação financeira junto do TARGET2. A responsabilidade da liquidação é directamente entre o Emissor e o SPI.

4.9.5 Compensação de operações baixo valor

As operações baixo valor – pagamentos com dispositivos Via Verde, pagamentos com cartão em portagens e pagamentos em publifones são processadas pela SIBS FPS assim que recebidas dos respectivos terminais de pagamento do sistema Via Verde. Toas as transacções processadas pela SIBS FPS até às 9h00 de cada dia são integradas no fecho da compensação seguinte, que ocorre diariamente.

Após a sua compensação, as operações são enviadas para liquidação e integradas nos interfaces da compensação - Ficheiro DST5 – Destinos – dos respectivos Emissores, em lotes. Cada lote é constituído agregando as transacções do tipo de operação baixo valor e sempre que se atinja um dos seguintes parâmetros do serviço:

- Saldo da pista 3 do cartão;
- 15 transacções para o mesmo cartão;
- 150€ em transacções para o mesmo cartão;
- Dia da consolidação da compensação de baixo valor – 3º dia útil de cada mês e dia 7, 14, 21 e ultimo dia do mês.

O sistema de compensação também tem em conta a Directiva de Serviços de Pagamentos nº2007/64/CE que indica que cada transacção maior ou igual a 30€ constitui, por si só, um lote.

4.9.6 Ficheiros da compensação

Sempre que a SIBS FPS executa um processamento de compensação, é produzido um conjunto de ficheiros destinados a diferentes tipos de participante no sistema da SIBS FPS: Os ficheiros e detalhes que mais impacto têm nos Emissores são:

- Ficheiro de Destinos;
- Ficheiro de Movimentos, vertente Banco;

- Ficheiro de Pagamentos de Baixo Valor;
- Ficheiro Resumo da Compensação.

4.9.6.1 Ficheiro de Destinos

É o ficheiro (código DST5) enviado aos Emissores *on-us*, com o detalhe de cada transacção efectuada com os seus cartões e que informa:

- As operações efectuadas com cartões *on-us* na Rede MULTIBANCO e em outras redes;
- As operações com NIB (pagamentos realizados nos canais *homebanking*) ou para NIB (créditos de transferências);
- Todas as operações do Banco realizadas com sucesso (mesmo aquelas que tenham sido aceites nas sessões *real-time* e mesmo nos próprios canais do Banco) e todas as anuladas desde que a autorização tenha ido ao Banco em *real-time;*
- Movimentos para a conta de regularização dos Emissores de cartões de marca internacional resultantes de reclamações apresentadas pelos Clientes;
- Reclamações nacionais;
- Fees que o Emissor recebe dos SPIs.

O seu processamento pode ser agregado por ficheiros, quer por CPD quer por range de BIN. O processamento por CPD é considerado o standard, excepto para os BIN que estejam identificados com essa opção no formulário “Caracterização de BIN”.

4.9.6.2 Ficheiros de Movimentos - vertente Banco

É o ficheiro (código MOV5) que informa:

- Os totais das contas de apoio ao *settlement* dos SPI;
- Os movimentos de regularização do sistema da SIBS FPS.

4.9.6.3 Ficheiro de Pagamentos de Baixo Valor

É o ficheiro (código PBV) com informação não financeira, cuja recepção é parametrizável a nível de BIN, sendo opcional a sua recepção. Neste ficheiro está a informação detalhada das operações de baixo valor do Banco, porque esta informação aparece agregada no Ficheiro de Destinos.

4.9.6.4 Ficheiro Resumo da Compensação

É o ficheiro (código RMB5) destinado aos Bancos de liquidação, isto é, os participantes directos do sistema da SIBS FPS. Contém um registo com os impactos contabilísticos de cada ficheiro enviado ao Banco.

4.10 Gestão de Disputas

A Gestão de Disputas é um serviço que permite ao Emissor efectuar o tratamento de reclamações derivadas de operações realizadas com cartões *on-us* (marca MULTIBANCO e marcas internacionais) na Rede CA e TPA MULTIBANCO e redes de marcas internacionais, de acordo com as regras de cada Sistema de Pagamento (MULTIBANCO, VISA, MasterCard e AMEX).

Estas operações realizam-se de acordo com um ciclo de vida determinado, regido por regras definidas pelo respectivo Sistema de Pagamento aplicáveis tanto aos Emissores dos cartões como aos *Acquirers* das operações.

A gestão dos processos de reclamação pode ser executada pelos Emissores através dos diferentes canais colocados à sua disposição: PSS, mensagens *Host-to-Host* e ficheiro de Gestão de Dados do Serviço MULTIBANCO. O Emissor tem disponíveis várias funcionalidades no PSS, através das seguintes vertentes:

- **Acordo MB** - Permite o tratamento de reclamações de operações realizadas com cartões *on-us* com vertente MULTIBANCO, quando usados nessa vertente na Rede de CA e TPA MULTIBANCO;
- **Outras marcas -** Permite o tratamento de reclamações de operações realizadas com cartões *on-us* na Rede de CA e TPA MULTIBANCO ao abrigo de acordos de marcas internacionais. Este serviço será o canal único para troca de informação, e subsequentes impactos contabilísticos, entre Emissores de cartões e Acquirers *on-us*;
- **Operações estrangeiro** - Permite o tratamento de reclamações de operações realizadas com cartões *on-us* com marca internacional (VISA, MasterCard ou AMEX) quando usados noutras redes que não a Rede MULTIBANCO.

4.10.1 Ciclo de vida das transacções

O ciclo de vida de uma transacção é constituído por várias acções, algumas das quais só ocorrem a partir do momento em que o Emissor considere a transacção inválida. A partir do momento em que a transacção é considerada inválida, o seu ciclo de vida, e, consequentemente, as etapas que o constituem, varia consoante a marca do cartão que originou a transacção.

Para as transacções cuja concretização obriga a uma autorização prévia, o *Acquirer* apresenta o pedido de autorização ao Emissor do cartão que, por sua vez, devolve uma resposta ao pedido de autorização. Perante uma resposta afirmativa do Emissor, o *Acquirer* faz a apresentação dos dados da transacção efectuada ao Emissor do cartão. Nos casos em que não são necessárias autorizações, o *Acquirer* procede imediatamente à apresentação dos dados da transacção ao Emissor.

Na sequência da apresentação inicial que o *Acquirer* faz ao Emissor de uma transacção efectuada por um cartão podem surgir dúvidas quanto à validade da mesma. Perante estas dúvidas, o Emissor do cartão pode ter necessidade de verificar os elementos constantes no documento comprovativo da transacção e/ou devolver ao *Acquirer* a responsabilidade financeira da operação original. Nestas situações, o Emissor inicia o processo de reclamação da transacção.

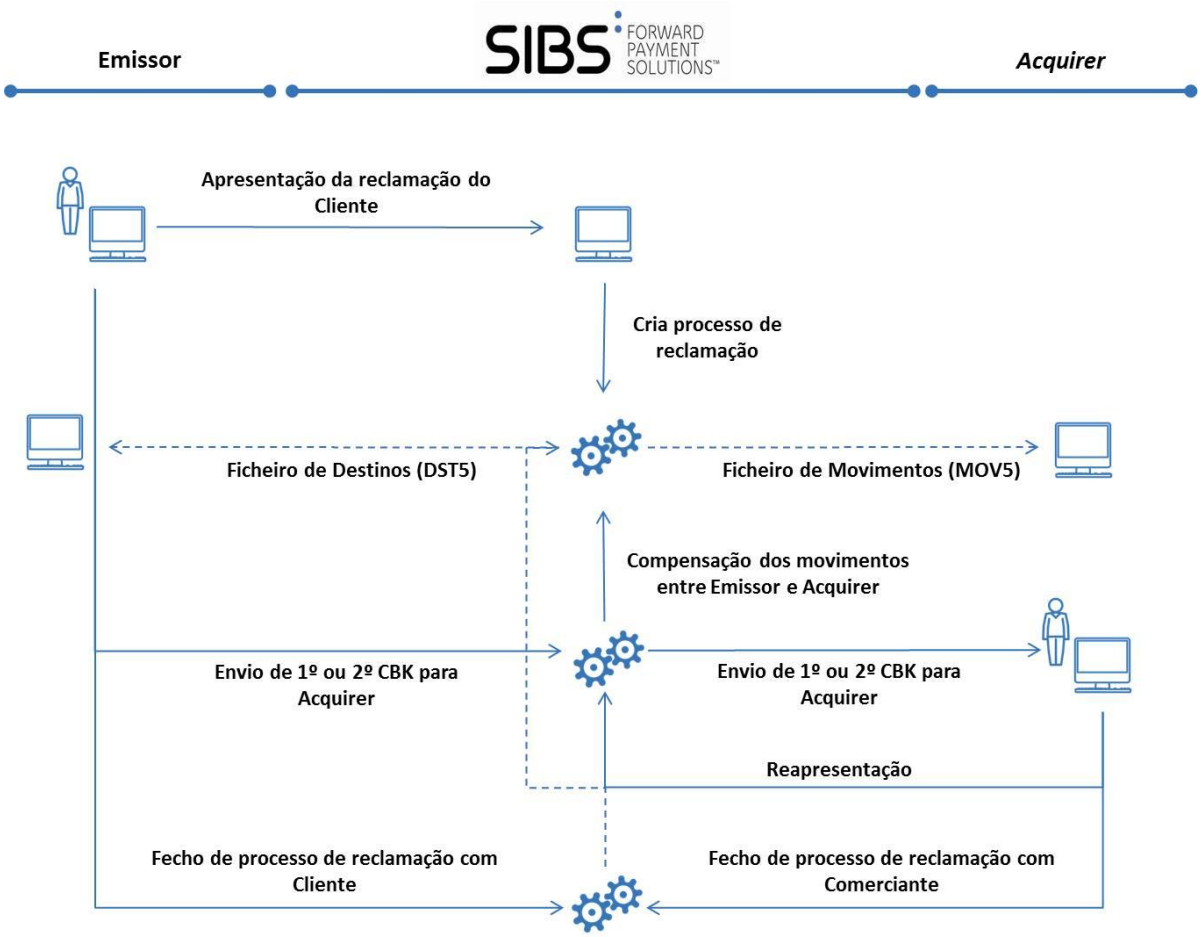

Figura 20 - Exemplo de evolução de um processo de reclamação na Rede TPA MULTIBANCO

A partir do momento em que o Emissor inicia um processo de reclamação, as subsequentes acções de regularização do ciclo de vida da transacção devem ser controladas tanto pelo *Acquirer* como pelo Emissor do cartão. A concretização destas etapas está delimitada no tempo, obedecendo a prazos estabelecidos pelo Sistema de Pagamento associado ao cartão que efectuou a transacção.

Uma reclamação constitui-se a partir dum processo de inserção de reclamação, normalmente desencadeado pelo Emissor do cartão. A evolução da reclamação efectua-se através de sucessivas inserções de acções, efectuadas tanto pelo Emissor como pelo *Acquirer*, que implicam mudanças de situação da reclamação e que se reflectem no estado da mesma ao longo do tempo.

Se a reclamação for enviada por um *Acquirer not-on-us*, através dos ficheiros de *outgoing* para o SPI, o respectivo SPI encaminha-a para o devido *Acquirer*. As confirmações dos processos de reclamação são recebidas pela SIBS FPS através dos ficheiros de *incoming* enviados pelo SPI.

O Emissor desencadeia o processo de reclamação e envia o primeiro *chargeback* para o *Acquirer*. Esta entidade aceita a reclamação e fecha o processo com o Comerciante ou procede à reapresentação do processo de reclamação, ou seja, devolve o *chargeback* ao Emissor apresentando novos dados no âmbito do processo de reclamação. Caso o Emissor e o *Acquirer* não cheguem a um acordo sobre a resolução do processo de reclamação, inicia-se o mecanismo de *pre-arbitration* em que o caso é submetido a avaliação

pela SIBS FPS, no caso das transacções com cartões *on us*, que fica encarregue de tomar uma decisão final sobre o assunto, esgotadas as anteriores etapas do processo de reclamação.

A evolução do processo de reclamação pode ainda contemplar algumas acções de cariz administrativo – *pre-compliance*, *compliance* e *goodfaith* - que não produzem qualquer impacto contabilístico para as diferentes entidades envolvidas na transacção. Estas acções traduzem-se numa troca de correspondência entre o Emissor e o *Acquirer* em que estas entidades procuram chegar a uma plataforma de entendimento de modo a evitar a escalada do processo de reclamação para uma *pre-arbitration*. As acções da *pre-arbitration* e *arbitration* também não têm impacto contabilístico no caso dos *Acquirers not-on-us*.

Outras acções a salientar são o *credit voucher* e o crédito a Cliente. O *credit voucher* é um mecanismo em que o próprio *Acquirer* assume a regularização do processo de reclamação quando, por exemplo, o Comerciante se apercebe que debitou, indevidamente, um Titular de Cartão por uma quantia superior ao real valor da transacção. Depois de o Comerciante reportar a situação ao *Acquirer*, este pode desencadear um processo de inserção de uma acção de *credit voucher* que, automaticamente, credita o Emissor do cartão e debita o Comerciante pelo valor a regularizar.

A acção de crédito a Cliente (Titular de Cartão) é desencadeada sempre que o Emissor decidir creditar o seu Cliente, pelo montante que foi reclamado, total ou parcial.

Atendendo a que o ciclo de vida de uma transacção reclamada depende da marca do cartão que a originou, a tabela seguinte apresenta uma síntese desse ciclo, em função da mesma:

Tabela 9 - Processo de reclamação por marca de cartão

Etapas da Transacção Reclamada	Sistema de Pagamento		
	VISA	MasterCard	AMEX
Abertura de Processo	Emissor	Emissor	Emissor
Pedido de Documento	Emissor	Emissor	Emissor
Resposta a Pedido de Documento	*Acquirer*	*Acquirer*	*Acquirer*
Primeiro *Chargeback*	Emissor	Emissor	Emissor
Reapresentação	*Acquirer*	*Acquirer*	*Acquirer*
Segundo *Chargeback*	N/A	Emissor	Emissor
Pre-Arbitration	Emissor	*Acquirer*	*Acquirer*
Arbitration	Emissor	*Acquirer*	*Acquirer*
Finalização de Processo	Emissor	Emissor	Emissor

Concluída a avaliação da reclamação, executa-se o fecho do processo de reclamação. Estes fechos de processo produzem impactos contabilísticos ao nível das diferentes entidades envolvidas na transacção (Emissor, Titular de Cartão, *Acquirer* ou Comerciante) de acordo com as conclusões geradas pela avaliação da reclamação.

Para encerrar um processo de reclamação, sob a perspectiva do Emissor, existem disponíveis no PSS as seguintes acções:

- **Fim da reclamação com débito a Cliente** - Esta acção encerra o processo de reclamação com:
  - Débito ao cartão do montante líquido – montante deduzido da eventual comissão – indicado pelo utilizador aquando da realização da acção;
  - Lançamento, na conta de regularização do Emissor, do valor que encerra / salda o processo;
  - Lançamento na rubrica de ganhos e perdas[7], por ser considerado como ganho ou perda do Emissor, do valor debitado ao Cliente subtraído do montante que salda o processo.

  Tanto o débito ao Cliente como os lançamentos efectuados na rubrica de ganhos e perdas são enviados, ao Emissor, via ficheiro da compensação.
- **Fim da reclamação com perda para Emissor** - O Emissor assume a responsabilidade financeira do processo e salda-o, não afectando a conta do Cliente. Esta acção encerra o processo de reclamação, na perspectiva do Emissor:
  - Sem lançamento no cartão;
  - Se o saldo que encerra / salda o processo é diferente de zeros, é retirado da conta de regularização do Emissor (lançamento a débito ou crédito pelo montante da reclamação) por contrapartida da sua rubrica de ganhos e perdas.
    Esta movimentação é enviada ao Emissor, via ficheiro da compensação.

As seguintes tabelas apresentam as acções típicas de um processo de reclamação com impacto contabilístico nos intervenientes das acções associadas à transferência de responsabilidade financeira.

Tabela 10 - Operações de marcas internacionais na Rede MULTIBANCO

Acção	Conta do Cliente	Conta de Regularização do Emissor	Conta de Regularização (Disputas) do *Acquirer*
Reclamação Cliente	Crédito	Débito	
Primeiro *Chargeback*		Crédito	Débito
Reapresentação		Débito	Crédito
Segundo *Chargeback*		Crédito	Débito
Credit Voucher		Crédito	Débito
Emissor Aceita *Pre-Arbitration*		Débito	Crédito
Acquirer Aceita *Pre-Arbitration*		Crédito	Débito
Fim da Reclamação com Débito a Cliente	Débito a)	Salda Processo b)	
Fim da Reclamação com Perda para Emissor		Salda Processo c)	

Notas:

[7] Esta rubrica é alimentada pela diferença entre o débito lançado à conta do Comerciante e o montante do processo de reclamação, pelos fechos de processo com impacto no Emissor e as regularizações Comerciante associadas ao processo de reclamação.

a) O Emissor debita o Cliente pelo valor da reclamação.
b) A conta de regularização do Emissor é creditada pelo valor que salda o processo. A conta do Cliente é debitada pelo valor referido na alínea (a). A eventual diferença entre os dois valores será considerada na rubrica contabilística de ganhos e perdas.
c) A conta de regularização do Emissor é creditada pelo valor que salda o processo por contrapartida do débito da sua rubrica contabilística de ganhos e perdas.

Tabela 11 - Operações noutras redes

Acção	Conta do Cliente	Conta de Regularização do Emissor	Conta de Apoio ao *Settlement*
Reclamação Cliente	Crédito	Débito	
Operação Suspeita ou Cartão Alheio		Débito	Crédito
Primeiro *Chargeback*		Crédito	Débito
Reapresentação		Débito	Crédito
Segundo *Chargeback*		Crédito	Débito
Credit Voucher		Crédito	Débito
Fim da Reclamação com Débito a Cliente	Débito a)	Salda Processo b)	
Fim da Reclamação com Perda para Emissor		Salda Processo c)	

Notas:

a) O Emissor debita o Cliente pelo valor da reclamação.
b) A conta de regularização do Emissor é creditada pelo valor que salda o processo. A conta do Cliente é debitada pelo valor referido na alínea (a). A eventual diferença entre os dois valores será considerada na rubrica contabilística de ganhos e perdas.
c) A conta de regularização do Emissor é creditada pelo valor que salda o processo por contrapartida do débito da sua rubrica contabilística de ganhos e perdas.

4.10.2 *Fees*

Uma *fee* é uma comissão que permite aos Emissores e *Acquirers* cobrarem entre si os valores devidos pela prestação de serviços como, por exemplo, a resolução financeira de reclamações disputadas no ciclo de *chargebacks*, envio de fax para colocação de cartões em Lista Negra, entre outras tarefas.

Existem dois tipos de *fee*:

- ***Fees* com PAN** - *Fees* associadas a um número de cartão (por exemplo, relativas a processos de reclamação);
- ***Fees* sem PAN** - *Fees* sem indicação de qualquer número de cartão (por exemplo, uma *fee* cobrada na sequência do envio de documentação para o *Acquirer*). Estas *fees* estão fora deste âmbito.

Uma *fee* pode ser criada tanto pelo Emissor como pelo *Acquirer*. Neste contexto, existem os seguintes cenários para a gestão de *fees*:

- **Emissor e *Acquirer on-us*** - As *fees* enviadas pelo Emissor são por este inseridas, através das funcionalidades disponíveis no PSS, sobre um processo de reclamação, e são consultadas pelo *Acquirer* também no PSS e vice-versa;
- **Emissor e *Acquirer not-on-us*** - As *fees* remetidas pelo Acquirer chegam à SIBS FPS através dos ficheiros de *incoming*[8] remetidos pelo SPI e são consultáveis no PSS. As *fees* emitidas pelo Emissor são enviadas a partir das funcionalidades disponibilizadas no PSS e seguem nos ficheiros de *outgoing*[9] para o SPI.

O tratamento de *fees* aplica-se, exclusivamente, a processos de reclamação remetidos através dos Sistemas de Pagamento VISA ou MasterCard.

O Emissor tem à sua disposição um módulo que lhe permite executar a gestão das *fees* associadas às operações relacionadas com processos de reclamação e outros serviços de cariz administrativo. A gestão de *fees* permite ao Emissor:

- Consultar as *fees* com PAN remetidas pelos *Acquirers*:
  - O *Acquirer* pode ter necessidade de emitir uma *fee*, a débito ou a crédito do Emissor, para, por exemplo, regularizar um processo de reclamação que atingiu o fim do ciclo de *chargebacks* ou outras *fees* não relacionadas com disputas mas para lançamento a cartão;
- Devolver aos *Acquirers fees* com PAN recebidas indevidamente (por exemplo, *fees* com valores incorrectos ou *fees* que nem sequer deveriam ter sido enviadas; outras *fees*);
- Emitir *fees* para os *Acquirers* no sentido de resolver financeiramente processos de reclamação que encerraram o ciclo de *chargebacks* e só podem ser remediados por meio do envio de uma *fee*;

4.10.3 Ficheiro de listagem de movimentos (MLIS)

A SIBS FPS realiza, periodicamente, o arquivo das transacções realizadas, deixando as mesmas de estarem disponíveis para consulta imediata, através do PSS. Quando existe, por parte do Emissor, a necessidade de consulta de uma transacção já não disponível, essa consulta é possível mediante um pedido de listagem de movimentos. O acesso a este pedido de listagem está disponível no PSS.

Após o processamento do pedido pela SIBS FPS, as transacções constantes da listagem ficam disponíveis para consulta no PSS. Após a sua consulta, o Emissor pode dar início ao tratamento do pedido de reclamação.

[8] Ficheiro de *clearing*, enviado pelo SPI à SIBS FPS, que é processado e remetido para o Emissor.

[9] Ficheiros de apresentação das transacções, enviadas pela SIBS FPS para o SPI, que são encaminhados para os respectivos *Acquirers*.

4.10.4 Ficheiro de estatísticas de reclamações

Este ficheiro, disponível no PSS, em formato texto (extensão ".txt"), permite ao Emissor de cartões *on-us* de marcas internacionais efectuar a extracção da quantidade e do volume de operações de reclamações, originadas por transacções realizadas na Rede de CA e TPA MULTIBANCO, efectuadas durante o mês anterior ao corrente e por Sistema de Pagamento.

A partir do dia 1 de cada mês o Emissor pode realizar o *download* dos ficheiros de estatísticas mensais relativos ao mês anterior. O sistema disponibiliza somente a informação referente ao ano corrente e ao ano anterior.

Este ficheiro pode ser guardado pelo utilizador para posterior tratamento.

O ficheiro de estatísticas mensais é constituído, por exemplo, pelos seguintes dados:

- Número de pedidos de documento;
- Número de respostas a pedidos de documentos;
- Número de primeiros *chargebacks* e montante total;
- Número de segundos *chargebacks* e montante total;
- Número de reapresentações e montante total;
- Número de rejeições de reapresentações e montante total (Emissores *not-on-us*);
- Número de *credit vouchers* e montante total;
- Número de *pre-arbitrations* e montante total;
- Número de *pre-arbitrations* aceites e montante total;
- Número de *pre-arbitrations* recusadas e montante total;
- Número de *arbitrations* e montante total;
- Número de *pre-compliances* e montante total (Emissores *not-on-us*);
- Número de *compliances* e montante total (Emissores *not-on-us*);
- Número de *good faiths* e montante total (Emissores *not-on-us*);
- Número de fechos de processo de reclamação e montante total, com afectação ao *Acquirer*;
- Número de fechos de processo de reclamação e montante total, com afectação a Comerciantes;
- Número de fechos de processo de reclamação e montante total, com afectação aos Emissores;
- Número de fechos de processo de reclamação e montante total, com afectação à SIBS FPS;
- Número de fechos de processo de reclamação e montante total, sem impacto na compensação;
- Número de *fees* enviadas sobre processos de reclamação e montante total;
- Número de *fees* recebidas sobre processos de reclamação e montante total;
- Número de *fees* rejeitadas sobre processos de reclamação e montante total (Emissores *not-on-us*).

Quadro 3 - Serviços para Emissores

- Em termos de serviços de Processamento para Emissores MB e SPI, a SIBS FPS disponibiliza aos Emissores o serviço de Emissão de Cartões Bancários que passa pelo cálculo dos dados lógicos do cartão, emissão de carta PIN com ou sem guarda de *pinblock*, emissão de cartas PIN aleatórias, reatribuição de PIN, emissão de cartões com tecnologia EMV não personalizados, cartões *contactless*, *replacement cards* e renovação e substituição de cartões.
- No âmbito da Emissão de Cartões Não Bancários, está também disponível o cálculo dos dados lógicos do cartão.
- Para que o Emissor possa usufruir destes serviços, devem ser trocados ficheiros standardizados com a informação necessária para a emissão de cartões. O horário de processamento dos ficheiros é algo importante para o Emissor para que este esteja informado de quando dá início a emissão lógica dos seus cartões.
- A emissão de um cartão EMV tem uma componente de segurança muito importante que deve ser coordenada entre a SIBS FPS e o Emissor assegura que a troca de informação entre estes dois intervenientes e a colocação dos dados em cada cartão é feita com base em chaves encriptadas que previnem o comprometido da informação.
- Complementando a emissão lógica de cartões, a SIBS FPS desenvolveu serviços e produtos que aportam valor acrescentado ao Emissor e consequentemente ao Cliente final, permitindo o uso de um conjunto de funcionalidades que optimizam a utilização do cartão e a gestão do cartão e das suas transacções. Exemplo disso é a gestão do ciclo de vida do cartão que condiciona a realização de operações na Rede CA e TPA MULTIBANCO ou em outras redes. Por problemas de utilização, opção do Emissor ou derivado de validações de segurança da SIBS FPS, o estado do cartão no seu ciclo de vida por ser alterado e ter qualquer um dos seguintes estados: Normal, Por Personalizar, Capturado a Devolver, Lista Negra, Lista Cinzenta, Capturado a Não Devolver, Anulado, Capturado e em Lista Negra; Anulado e em Lista Negra, Por Activar, Activável em CA e Capturado a Devolver após Fecho de CA.
- Consoante as marcas de Sistemas de Pagamento incluídas no cartão, estão disponíveis para o utilizador do cartão, um conjunto de operações base e operações de valor acrescentado. Nas marcas MB/MB SPOT estão disponíveis operações como Levantamento, Compra, Consulta de Saldos e Consulta de Movimentos, Alteração de PIN, Pagamento de Serviços, Transferência Bancária, entre outros. Como serviços especiais destas marcas temos a Consulta NIB/IBAN, MB NET, Via Verde, Pagamentos ao Estado, Carregamentos de Telemóveis, entre outros. No caso de cartões com uma Marca de Sistema de Pagamento Internacional, estão disponíveis, entre outras, as operações de Compra, Autorização, Adiantamento de Dinheiro e Levantamento a Crédito.

- Complementar ao processamento de cartões, a SIBS FPS disponibiliza vários cenários de funcionamento de Autorização de transacções, que permitem uma adequação do modo de decisão de autorização à estratégia do Emissor.
- A selecção dos cenários de Autorização é feita pelo Emissor, e a aplicar na Rede MULTIBANCO, as opções disponíveis para o Emissor são *Real-time*, Cenários de Degradação, Cenário de Serviço Reduzido, *Real-time* dos Emissores com o FEP, Pagamentos de Baixo Valor, Transacções *Offline* e Utilização Múltipla dos Cenários apresentados.
- A aplicar noutras Redes, a SIBS FPS disponibiliza aos seus Emissores os cenários de Limite de Autorização e o Saldo de Crédito Disponível.
- Existem ainda outros métodos de autorização de transacções, como a autorização 3D Secure para Cartões Reais que permite a realização de operações de autenticação, autorização, compensação e liquidação de compras efectuadas na Internet, com garantias acrescidas de segurança para os clientes e comerciantes *online* (vertente 3D Secure Emissor).
- Outro serviço disponível da SIBS FPS para autorizações de transacções é a autorização de *Recurring Transations* que tem por base a autorização de uma transacção recorrente, isto é, uma transacção em que um Titular de um cartão autoriza um Comerciante a que, de forma periódica, proceda a débitos na sua conta, pelo fornecimento recorrente de bens ou serviços, ao longo do tempo. Nesta situação, na primeira transacção são enviados ao Emissor todos os dados da transacção, incluindo os dados do cartão e a transacção fica indicada como *recurring transaction* na SIBS, em conjunto com a informação de qual o cartão utilizado e o Comerciante que acolheu a operação. As transacções subsequentes, desencadeadas pelo Comerciante, são realizadas sempre em ambiente ca*rd-not-present* pelo que o CVV2 pode não ser incluído pelo Comerciante no detalhe da transacção.
- O *Account Verification* também faz parte das opções de autorização de transacções implementadas e à disposição dos Emissores. Nesta opção, o comerciante pode confirmar a autenticidade do cartão apresentado pelo Cliente e da conta associada, sem gerar um cativo na conta.
- O serviço compensação e Informação para Liquidação de Transacções consiste no apuramento do saldo financeiro de cada instituição participante no sistema e respectiva liquidação quando aplicável.
- A Gestão de Disputas garante a gestão das reclamações e as inerentes acções de regularização derivadas da utilização de cartões das marcas MB e de SPI, de acordo com as regras dos Sistemas de Pagamento nacional e internacionais.

5 Canais de Comunicação SIBS - Emissor

5.1 Portal de Serviços SIBS

O Portal de Serviços SIBS é disponibilizado ao Emissor num acesso via Extranet possibilitando, de uma forma segura e fácil, o acesso à informação residente no sistema central da SIBS FPS. Este canal integra a utilização das seguintes funcionalidades:

- **Cartões Bancários -** Este serviço disponibiliza as opções de consulta que possibilitam a verificação dos valores posicionados permitindo também actuar directamente no sistema da SIBS FPS alterando a situação dos cartões. Permite ainda a consulta aos parâmetros das caracterizações de Emissor, CPD e BIN carregados na SIBS FPS;
- **Produção Lógica de Cartões -** Possibilita o acompanhamento dos diversos acontecimentos através da disponibilização de consultas (como, por exemplo, as produções do dia, produções entre datas e elementos de uma produção em particular) que permitem controlar o processo de produção na óptica dos Emissores;
- **Caracterização Emissor -** O objectivo deste serviço é possibilitar a consulta aos parâmetros das caracterizações do Emissor, CPD e BIN carregados na SIBS FPS;
- **Reclamações - Acordo MB -** Este serviço destina-se aos serviços centrais dos Emissores, proporcionando-lhes os meios para o eficaz desempenho da sua função centralizadora de todas as reclamações e/ou pedidos de esclarecimento apresentados pelos Titulares de Cartões;
- **Reclamações – Emissor Outras Vertentes -** Este serviço destina-se aos serviços centrais dos Emissores, proporcionando-lhes os meios necessários ao tratamento de reclamações de operações realizadas com cartões *on-us* na Rede TPA MULTIBANCO ao abrigo de acordos de marcas internacionais. Permite o relacionamento, no âmbito do tratamento de reclamações, entre os Emissores de cartões *on-us* e os *Acquirers* utilizadores do serviço;
- **Reclamações – Operações Estrangeiro -** Este serviço destina-se aos serviços centrais dos Emissores, proporcionando-lhes os meios para o eficaz desempenho da sua função centralizadora de todas as reclamações de operações noutras redes, e/ou pedidos de esclarecimento, apresentados pelos Titulares de Cartões.

5.2 Mensagens *Host-to-Host*

As entidades participantes no sistema da SIBS FPS têm a possibilidade de alargar a utilização do seu leque de canais próprios (tipicamente *homebanking* ou bancas telefónicas) disponibilizando serviços existentes no sistema da SIBS FPS através desses canais.

É também possível às entidades participantes no sistema da SIBS FPS utilizarem as funcionalidades de gestão dos serviços que estão disponíveis no PSS, através de interfaces próprias.

A disponibilização do serviço nos canais acima referidos é efectuada mediante a troca de mensagens entre o sistema central da Instituição e o sistema central da SIBS FPS.

5.3 Protocolo Multibanco *File Transfer*

O diálogo entre dois sistemas residentes em computadores diferentes permite que estes possam transferir entre si um conjunto de informação normalmente designado por ficheiros (sequências de registos), usando unicamente como meio de comunicação um circuito lógico, suportado por linhas/redes de comunicação de dados.

O sistema normalmente utilizado na transferência de ficheiros é o *File Transfer System* (FTS) que consiste num processo de teletransmissão à qual os computadores intervenientes têm acesso.

O sistema de transferência de ficheiros utilizado pela SIBS FPS é designado por Protocolo MULTIBANCO *File Transfer* (MFT), desenhado e implementado pela mesma para gerir a comunicação e efectuar o transporte dos dados de uma forma transparente. Tal significa que o conteúdo dos ficheiros a transportar não tem relevância para o *File Transfer*. Este sistema tem por objectivo satisfazer as necessidades de transferência constante de grandes quantidades de informação de âmbito bancário, centralizadas pela SIBS com o seu sistema da SIBS FPS.

A integridade dos dados recebidos pelo *File Transfer* na origem será respeitada, de forma a garantir a entrega dos mesmos dados no destino. Apenas o código de representação dos dados poderá sofrer conversão (ASCII / EBCDIC ou vice-versa), sempre que as máquinas trabalhem em códigos diferentes e o utilizador assim o pretenda.

6 Fluxos de Dados e Informação

No âmbito dos Serviços para Emissores, o Emissor pode constituir ficheiros de gestão do serviço e enviá-los à SIBS FPS, obtendo desta as correspondentes respostas. Por outro lado, a SIBS FPS é responsável pelo envio ao Emissor de um conjunto de ficheiros com informações diversas sobre o serviço.

6.1 Ficheiros com iniciativa no participante

Os ficheiros enviados pelos participantes para processamento na SIBS FPS são os seguintes:

- **Ficheiro ELCB – Emissão Lógica de Cartões Bancários**

  Ficheiro enviado com os dados dos cartões a emitir, que incluem informação sobre o titular do cartão, as contas associadas e os critérios dos cenários de decisão das suas operações. Este ficheiro é usado apenas na nova operativa de emissão lógica de cartões;

- **Ficheiro PERS – Personalização de Cartões**

  Ficheiro destinado a dar suporte à personalização de todos os tipos de cartão emitidos pela SIBS FPS, sendo um interface único para a emissão de produtos bancários e produtos não bancários para todos os Personalizadores de Cartões que os Emissores contratem. Este ficheiro é produzido após a recepção e processamento do Ficheiro ELCB – Emissão Lógica de Cartões Bancários e do Ficheiro ECPS - Emissão de Cartões com Processamento SIBS;

- **Ficheiro EECB – Emissão de Cartões**

  Ficheiro enviado com os dados dos cartões a emitir, que incluem informação sobre o titular do cartão, as contas associadas e os critérios dos cenários de decisão das suas operações. Este ficheiro é usado apenas na operativa em descontinuação de emissão lógica de cartões;

- **Ficheiro ECPS – Emissão de Cartões**

  Ficheiro enviado por um Emissor que pretenda emitir cartões empresa que utilizem o serviço de Autenticação Forte, ou outros cartões com aplicações específicas de acordo com o contrato estabelecido entre as partes;

- **Ficheiro DACB – Dados Adicionais de Cartões (cartões bancários)**

  Ficheiro com dados adicionais para produção de cartões, isto é, permite incluir outros dados que se desejam colocar na frente ou verso do cartão bancário e comunicar dados de uma segunda aplicação que esteja presente no cartão;

- **Ficheiro IMGB – Imagens de Cartões (cartões bancários)**

  Ficheiro com as imagens necessárias para a produção dos cartões;

- **Ficheiro EDAC – Dados Adicionais de Cartões (cartões não bancários)**

  Ficheiro com dados adicionais para produção de cartões não bancários, isto é, permite incluir outros dados que se desejam colocar na frente ou verso do cartão bancário e comunicar dados de uma segunda aplicação que esteja presente no cartão não bancário;

- **Ficheiro MIMG – Imagens de Cartões (cartões não bancários)**

  Ficheiro com as imagens necessárias para a produção dos cartões não bancários;

- **Ficheiro EMVC – Movimentos de Conta**

  Ficheiro enviado sempre que um Emissor com cenário de saldo de conta pretenda proporcionar a operação MB SPOT – Consulta de Movimentos;

- **Ficheiro EGCC – Gestão de Cartões e Contas**

  Ficheiro enviado sempre que seja necessário actualizar os dados dos cartões e das contas DO associadas;

- **Ficheiro EDNP – Dados dos Titulares dos Cartões**

  Ficheiro enviado sempre que tenham sido atribuídos cartões não personalizados a Clientes;

- **Ficheiro EASC – Alteração de Situação de Cartão**

  Ficheiro enviado para actualização da base de dados da SIBS FPS. Tem como objectivo completar o que já existe para gerir os cartões de débito, podendo também gerir a informação que existe noutros sistemas;

- **Ficheiro ECLN – Lista Negra**

  Ficheiro enviado pelo Emissor ou Representante de cartões e tem como objectivo permitir a gestão da Lista Negra para o serviço de baixo valor e outros serviços;

- **Ficheiro APAL – Abate de PIN**

  Ficheiro que permite que o Emissor proceda ao abate de *pinblocks* ainda sem associação a algum cartão. Esse abate pode ser realizado com base em diferentes critérios (ex: *range* de PIN; *range* temporal (data de início: data de fim));

- **Ficheiro TCAR – Cartões Carregados na SIBS**

  Ficheiro que a SIBS FPS produz esporadicamente e a pedido do Emissor e que contém a informação de cartões por este emitidos e que se encontram no ficheiro de cartões da SIBS FPS.

  O Emissor deve indicar expressamente à SIBS FPS que o pretende receber num dado momento. No pedido a efectuar, o Emissor deve também indicar o endereço de *File Transfer* para o qual o ficheiro deve ser enviado.

  A selecção dos dados a incluir no ficheiro é feita mediante determinados parâmetros. Assim, o Emissor deve indicar que pretende um TCAR com:

  - Todos os cartões existentes no data base da SIBS FPS e emitidos pelo Emissor ou;
  - cartões só de determinados BIN e/ou só de determinados CPD e/ou;
  - cartões pertencentes a um determinado intervalo.

Em conjunto com o acima exposto, o Emissor pode ainda indicar que pretende excepcionar os cartões expirados (situação de *default*), incluir os cartões expirados ou só receber informação dos cartões expirados.

- **Ficheiro TCPD – Migração de Cartões de CPD**

  Ficheiro enviado para o Emissor quando este último pretende efectuar a migração de cartões específicos que se encontram num CPD para um outro CPD distinto;

- **Ficheiro ECSV – Comunicação de Saldos de Véspera**

  Ficheiro enviado pelo Emissor para actualizar os saldos de véspera e o saldo contabilístico dos dados da conta DO a que estão associados os cartões de débito;

- **Ficheiro ESCD – Comunicação de Saldos de Crédito**

  Ficheiro enviado pelo Emissor para actualizar os saldos disponíveis das contas crédito geridas pelo Emissor, a que estão associados cartões;

- **Ficheiro EALM – Actualização do Limite Mensal**

  Ficheiro enviado pelo Emissor para actualizar para actualizar o limite mensal das contas que se encontram associadas a cartões onde o Emissor pretende que, no cenário de Saldo de Conta, a SIBS FPS aplique também um limite mensal e não apenas o saldo de véspera;

- **Ficheiro MDVT – Devolução Transacções Pagamento com Dispositivo Via Verde**

  Após a recepção do (novo) ficheiro de movimentos para cobrança (MPPV) o Emissor do cartão dispõe de um prazo de 2 dias úteis para devolver os que não possam ser cobrados. No final desse prazo os movimentos aceites serão enviados tal como actualmente aos Emissores nos ficheiros de compensação/liquidação aos bancos e operadores.

Estes ficheiros podem ser enviados pelo participante com a periodicidade e no horário que lhe for mais conveniente. O processamento, por parte da SIBS FPS, é desencadeado no mesmo momento, por ordem de chegada.

6.2 Ficheiros de resposta da SIBS FPS

Os ficheiros de resposta enviados pela SIBS FPS como resultado do processamento dos ficheiros descritos na secção 6.1 são os seguintes:

- **Ficheiro CFER – Erros e Confirmações**

  Ficheiro que contém o retorno positivo para o Emissor do ELCB recebido, que agrega tanto os erros ocorridos como as confirmações de produção;

- **Ficheiro EERR – Erros de Cartões**

  Ficheiro enviado sempre que for processado qualquer ficheiro relativo a cartões, quer tenham ocorrido erros ou não;

- **Ficheiro ERCF – Confirmação** e **Erros do ECPS**

  Ficheiro enviado para permitir que o Emissor detecte a ocorrência de erros no processamento do ficheiro de Novos Cartões e qual a razão que justificou a rejeição de cada referência, e registe cada cartão que ficou registado na base de dados da SIBS FPS;

- **Ficheiro ECCF – Confirmação de Cartões**

  Ficheiro que contém o retorno positivo para o Emissor do ficheiro EECB recebido;

- **Ficheiro RACB – Erros de Dados Adicionais de Cartões (cartões bancários)**

  Ficheiro que contém os dados do registo original que apresentou erros no ficheiro DACB – Dados Adicionais de Cartões (cartões bancários);

- **Ficheiro RIMG – Erros de Imagens de Cartões**

  Ficheiro enviado sempre que for recebido um ficheiro de Imagens. O ficheiro produzido é:

  - Um ficheiro RIMB, se o ficheiro de imagens respectivo for o ficheiro IMGB – Imagens de Cartões (cartões bancários);
  - Um ficheiro RIMG, se o ficheiro de imagens respectivo for o ficheiro MIMG – Imagens de Cartões (cartões não bancários).

- **Ficheiro ERAC – Erros de Dados Adicionais de Cartões (cartões não bancários)**

  Ficheiro que contém os dados do registo original que apresentou erros no ficheiro EDAC – Dados Adicionais de Cartões (cartões não bancários);

- **Ficheiro ERLN – Erros de Lista Negra**

  Ficheiro enviado para permitir que o Emissor/Representante conheça o resultado do processamento do ficheiro ECLN – Lista Negra e que detecte com rapidez um eventual processamento anormal do ficheiro;

- **Ficheiro EERC – Erro de Conta**

  Ficheiro enviado como resultado do processamento de um ficheiro relativo a contas. A SIBS FPS informa que o processamento teve lugar e, se houver erros, quais os registos, respectivo código e valor do registo original;

- **Ficheiro TCDP – Erros de Migração de Cartões de CPD**

  Ficheiro enviado sempre que é processado um ficheiro TCDP - Migração de Cartões de CPD, que contém os erros verificados durante o processamento;

- **Ficheiro ECRE – Cartões Expirados**

  Ficheiro enviado no início de cada mês com a identificação dos cartões expirados.

6.3 Ficheiros com iniciativa na SIBS FPS

Os ficheiros disponibilizados pela SIBS FPS aos Emissores com informação sobre o serviço são os seguintes:

- **Ficheiro ORI5 – Origens**

  Ficheiro enviado ao Banco de Apoio de cada CA da Rede MULTIBANCO com as importâncias distribuídas no período, por utilizadores nacionais e estrangeiros, os depósitos em numerário confirmados, as tarifas interbancárias recebidas dos Emissores nacionais e as comissões internacionais, as rubricas aplicáveis do Tarifário da SIBS FPS e as regularizações de operações de supervisão dos CA com falhas ou sobras e confirmadas pela SIBS FPS;

- **Ficheiro DST5 – Destinos**

  Ficheiro enviado a cada Emissor com os movimentos correspondentes a diversas operações efectuadas com os seus cartões, quer na Rede MULTIBANCO quer noutras redes. Este ficheiro inclui todas as operações realizadas pelos cartões do Emissor, incluindo as que tenham sido aceites em *real-time*;

- **Ficheiro MOV5 – Movimentos**

  Ficheiro enviado com o registo dos movimentos correspondentes a diferentes tipos de operações relacionadas com o negócio de *acquiring* TPA;

- **Ficheiro CLN5 – Capturas e Lista Negra**

  Ficheiro enviado a cada Emissor com informação sobre cartões capturados, cartões que foram informados como "Lista Negra Urgente" e cartões anónimos ou duais, capturados na Rede CA MULTIBANCO, durante o dia;

- **Ficheiro RMB5 – Resumo de Compensação**

  Ficheiro enviado aos Bancos de liquidação participantes no Sistema da SIBS FPS onde estão indicadas a origem dos valores, correspondentes ao trailer de cada um dos restantes ficheiros da Compensação dirigidos ao Banco, considerados para apurar o saldo a movimentar na conta de liquidação;

- **Ficheiro RMB5 – Resumo de Compensação**

  Ficheiro de liquidação enviado aos participantes no sistema da SIBS FPS. Indica a origem dos valores, correspondentes ao *trailer* de cada um dos restantes ficheiros da compensação dirigidos ao Banco, considerados para apurar o saldo a movimentar na conta de liquidação;

- **Ficheiro PBV5 – Pagamentos de Baixo Valor**

  Ficheiro enviado com os detalhes das operações de Baixo Valor;

- **Ficheiro AUT5 – Autorizações Estrangeiro**

  Ficheiro enviado com detalhe dos pedidos de autorização no estrangeiro - aceites e recusados - efectuados com cartões do Emissor, no âmbito de Sistemas de Pagamento Internacionais (VISA, MasterCard, etc.);

- **Ficheiro EEMM – Estatísticas Matriciais**

  Ficheiro enviado com registo de dados estatísticos mensais nas vertentes de Emissão;

- **Ficheiro EFAC - Facturação**

  Ficheiro de facturação electrónica complementar à factura papel resumo enviada pela SIBS FPS;

- **Ficheiro CFAC - Comprovativo de Facturação**

  Ficheiro que apresenta os dados dos pagamentos de tarifário interbancário, complementar aos resumos papel;

- **Ficheiro ETAR - Tarifário**

  Ficheiro enviado pela SIBS FPS para os participantes do negócio de Emissão sempre que há uma nova versão de tarifário, necessário ao processamento da facturação da SIBS FPS / SIBS PAGAMENTOS;

- **Ficheiro PPV - Transacções Pagamento com Dispositivo Via Verde**

  Ficheiro enviado para os Emissores de cartões associados a identificadores Via Verde. Informa o valor e o detalhe das transacções efectuadas por cada identificador associado ao cartão de acordo com a informação remetida pela Via Verde;

- **Ficheiro ETV – Erro do ficheiro Transacções Pagamento com Dispositivo Via Verde**

  Ficheiro enviado para Emissores de cartões associados a identificadores Via Verde que enviem ficheiros de devoluções (MDVT).

7 Glossário

Termo	Definição
Autorização	O processo pelo qual uma transacção é aprovada ou recusada. Para cartões com *chip*, a decisão pode ser realizada *offline*. No caso de cartões com pista / banda magnética, a transacção é realizada *online* com o Emissor do cartão quando excede um dos limites aplicáveis.
Bank Identification Number	Sequência única de algarismos, atribuído pelo esquema de pagamento, para identificar o Emissor do cartão e o tipo de produto. Alguns produtos requerem um BIN dedicado. O BIN é incluído nos primeiros dígitos do *Primary Account Number*.
Cartão *co-branded*	Cartão que reúne dois Sistemas de Pagamento distintos: MB e marca internacional.
Cartão de pagamento	Qualquer tipo de cartão utilizado na aquisição de bens e serviços.
Cartão de rede privada	Cartão emitido por um Comerciante que apenas pode ser utilizado na rede de estabelecimentos desse Comerciante.
Chargeback	A mensagem enviada por um Emissor para reclamar do *Acquirer* a totalidade ou parte de uma quantia relativa a uma disputa.
Chip	Circuito integrado de tecnologia no cartão. Termo utilizado especificamente para descrever o *chip* no cartão ou a própria tecnologia, em termos genéricos.
Chip e PIN	Combinação de uma tecnologia segura (*chip*) com um método de verificação do Titular de Cartão seguro (PIN).
Co-branding	O processo de associação entre um Emissor e um parceiro comercial. Os cartões *co-branded* são direccionados à clientela do parceiro comercial e ostentam, normalmente, os logótipos do Emissor e do parceiro comercial.
Código de validação do cartão	Um código criptográfico especial gravado na pista de dados e utilizado pelo Emissor para autenticar a validade de um cartão.
Combined Data Authentication	Um tipo de criptograma gerado por um cartão durante uma transacção com *chip*. Trata-se do método de verificação do cartão mais seguro da actualidade.
Compensação	O processo que medeia a troca de detalhes financeiros relativos a uma transacção entre o Emissor e o *Acquirer*.
Contactless	Tecnologia que não requer um contacto físico entre o cartão e um terminal, sendo antes utilizada uma interface de rádio frequência para a respectiva troca de dados.
Criptograma do pedido de autorização	O criptograma gerado pelo *chip* do cartão quando uma transacção é realizada *online* com o Emissor do cartão. O criptograma permite ao Emissor verificar que o cartão é autêntico.
Data de expiração	A data (mês e ano) em que o cartão deixa de ser válido. O cartão pode ser utilizado até ao último dia do mês indicado.
Dynamic Data Authentication	Um tipo de criptograma gerado por um cartão durante uma transacção com *chip*. Trata-se de um método de verificação do cartão seguro.
e-Commerce	Negócios realizados através da Internet.
Emergency Card Replacement	Um serviço opcional disponibilizado pelos Emissores aos Titulares de Cartões com vista à substituição de um cartão perdido ou roubado.
EMV	Acrónimo de Europay, MasterCard e VISA que simboliza a estandardização de circuitos integrados nos cartões, terminais e aplicações.
Fallback	Situação em que um cartão com *chip* é apresentado num terminal mas a tecnologia do *chip* não pode ser utilizada. Neste caso, a realização da transacção reverte para a pista / banda magnética do cartão.
Método de verificação do cartão	Método utilizado para assegurar que um cartão é autêntico.

Termo	Definição
Método de verificação do Titular de Cartão	Os meios utilizados para verificar a autenticidade de um Titular de Cartão como, por exemplo, PIN e assinatura.
PayPass	O produto de pagamento *contactless* comercializado pela MasterCard.
PayWave	O produto de pagamento *contactless* comercializado pela VISA.
Personal Identification Number	Um código secreto, conhecido apenas pelo Titular de Cartão, que permite ao Emissor (ou seu representante) validar a autenticidade do Titular de Cartão.
Pista / banda magnética	Uma fita magnetizada na face traseira do cartão que contém informações sobre o cartão, o Titular de Cartão e a conta bancária. Estas informações são enviadas nos pedidos de autorização, a par de outros dados imprescindíveis à autorização ou recusa de uma transacção pelo Emissor.
Primary Account Number	Uma sequência única de algarismos, atribuída pelo Emissor, que identifica uma conta bancária de um Titular de Cartão. O PAN é composto pelo *major industry identifier*, BIN, número de conta bancária do Titular de Cartão e um *check digit*.
Recurring transaction	Transacção em que um Titular de Cartão autoriza um Comerciante a efectuar débitos na sua conta bancária pelo fornecimento recorrente de bens ou serviços ao longo do tempo.
Sistema central do Emissor	Sistema computadorizado e de comunicações do Emissor que executa o processamento das transacções.
Static Data Authentication	Um tipo de criptograma gerado por um cartão durante uma transacção com *chip*. Trata-se do nível de entrada dos diferentes métodos de verificação do cartão.
Transacção de *cashback*	O processo em que um Titular de Cartão realiza uma compra e pede uma quantia em numerário de contrapartida.
Validação da personalização do cartão	Um dos testes que o Emissor de um cartão com *chip* EMV tem de realizar antes do arranque da aceitação de transacções firmes.

8 Anexos

Os seguintes anexos podem ser encontrados no Portal de Serviços SIBS:

- Formulário de Caracterização do Emissor;
- Formulário de Caracterização do CPD do Emissor;
- Formulário de Caracterização do Padrão EMV;
- Formulário de Caracterização do BIN;
- Formulário de Acção sobre o Resultado da Validação ao CAVV.