
Release Documentation

MB WAY

SDK / API

Emissores

Versão: 01.70

Data: 2019-01-10

Estado: Final

Classificação: Restrito

Referência: DCSIBS180059



Certificação no âmbito dos serviços AT2, SEPA e SWIFT

© SIBS FPS

A informação contida neste documento é propriedade da SIBS FPS e não pode ser duplicada, publicada ou divulgada a terceiros, na totalidade ou em parte, sem o seu prévio consentimento por escrito, o qual nunca deverá ser presumido.

SIBS Forward Payment Solutions, S.A.
Rua Soeiro Pereira Gomes, Lote 1, 1649-031 LISBOA, PORTUGAL
Telephone: +351-217 813 000 / Fax: +351- 217 935 755

Ficha Técnica

Referência:	DCSIBS180059
Título do Documento:	API_SDK MB WAY
Versão:	01.70
Estado:	Final
Classificação:	Restrito
Tipo de Documento:	Release Documentation
Área Funcional Responsável:	AF Desenvolvimento de Serviços - Consumidor

Documentos Relacionados

Referência	Título	Origem
n.a.		

Revisões

Versão	Data	Descrição	Autor
01.00	2018-03-02	Criação do documento.	AF Desenvolvimento de Serviços
01.10	2018-04-17	Relativamente à versão anterior, efetuaram-se as seguintes alterações: <ul style="list-style-type: none"> Inserção do capítulo 2 Descrição da solução; Alteração ao <i>layout</i> da mensagem 3173 - Notificação de Operação (V01); Alteração da secção 3.1.1.1.3 Dados Variáveis das mensagens de pedido; Alteração do <i>layout</i> da mensagem H036 - S036: Confirmação de Operação Financeira (V01); Inserção da mensagem H520 - S520: Pedido de Código de Ativação para MB WAY Parceiro (V01); Eliminação da mensagem H526 - S526: Associação de Cartão ao MB WAY (V04); Alteração da secção 3.2 Especificações SDK (inserção de novas tabelas, alteração de tabelas existentes e criação de novas subsecções); Inserção do Anexo B Fluxos de Suporte à Implementação. Outras alterações editoriais sem impacto na informação técnica.	AF Desenvolvimento de Serviços
01.20	2018-05-07	Relativamente à versão anterior, efetuaram-se as seguintes alterações: <ul style="list-style-type: none"> Atualização da secção 3.1.1.1.3 Dados Variáveis das mensagens de pedido (Inserção do atributo (8282) COM_ADIOPE nos dados variáveis presentes na mensagem 3173 relativos à Notificação de Compra Pendente 'WOP'); Atualização do texto introdutório do <i>layout</i> da mensagem H520 - S520: Pedido de Código de Ativação para MB WAY Parceiro (V01), com a eliminação da indicação de que é necessário enviar como <i>Input</i> da mensagem o "Cartão MB (PAN + Data de expiração)"; Atualização do texto introdutório do <i>layout</i> da mensagem H552 - S552: Pedido de Referência para Levantamento MB WAY (V02); Atualização do texto introdutório do <i>layout</i> da mensagem H553 - S553: Consulta de Referências para Levantamento MB WAY (V03). Outras alterações editoriais sem impacto na informação técnica.	AF Desenvolvimento de Serviços
01.30	2018-06-08	Relativamente à versão anterior, efetuaram-se as seguintes alterações: <ul style="list-style-type: none"> Inserção da mensagem 1161 - Pedido de Operação com cartão (Emissor) (V00); 	AF Desenvolvimento de Serviços

Versão	Data	Descrição	Autor
		<ul style="list-style-type: none"> Atualização da secção 3.1.1.1.3 Dados Variáveis das mensagens de pedido (Inserção dos dados variáveis presentes na mensagem 1161 correspondentes às operações '001' Levantamento, '010' Compra MB e '013' Autorização Outdoor MB). 	
01.40	2018-08-09	<p>Relativamente à versão anterior, efetuaram-se as seguintes alterações:</p> <ul style="list-style-type: none"> Atualização do capítulo 1 Introdução; Atualização da secção 1.1 Âmbito; Inserção da secção 2.2.3 Funcionamento das notificações na operação de Pedido de Envio de Dinheiro (e da correspondente Tabela 2); Atualização da secção 4.4.4 Iconografia; Inserção da Secção 4.8 Pedir dinheiro; Atualização da mensagem H553 - S553: Consulta de Referências para Levantamento MB WAY (V03) (mensagem passa da V02 para a V03); Inserção da mensagem H623 - S623: Pedido de Envio de Dinheiro (V01); Inserção da mensagem H624 - S624: Gestão de Pedido de Envio de Dinheiro (V01); Inserção da mensagem H625 - S625: Consulta de Pedidos de Envio de Dinheiro (V01); Atualização da mensagem 3173 - Notificação de Operação (V01) (mensagem passa da V00 para a V01); <ul style="list-style-type: none"> Atualização do texto introdutório; Atualização da tabela incluída na nota A); Atualização da secção 3.1.1.1.3 Dados Variáveis das mensagens de pedido: <ul style="list-style-type: none"> Inserção dos dados variáveis presentes na mensagem 3173 correspondentes às operações 'WOE' Pedido de Envio de Dinheiro e 'WOR' Relembrar Pedido de Envio de Dinheiro; Inserção de novas versões dos dados variáveis presentes na mensagem 1161 correspondentes às operações '001' Levantamento, '010' Compra MB e '013' Autorização Outdoor MB; Inserção dos dados variáveis presentes na mensagem 1161 correspondentes à operação '179' (Transferência P2P Instantânea (Ordenante)). 	AF Desenvolvimento de Serviços
01.50	2018-10-10	<p>Relativamente à versão anterior, efetuaram-se as seguintes alterações:</p> <ul style="list-style-type: none"> Atualização da mensagem 3273 – Resposta a Notificação de Operação Pendente (mensagem passa da V00 para a V01 sem alterações no <i>layout</i>); Atualização da mensagem H625 - S625: Consulta de Pedidos de Envio de Dinheiro (V01) – Alteração do texto introdutório, inserção do atributo (10308) 'SEE_IDEOPR_NTV' e atualização de notas. 	AF Desenvolvimento de Serviços
01.60	2018-12-05	<p>Relativamente à versão anterior, efetuaram-se as seguintes alterações:</p> <ul style="list-style-type: none"> Inserção de nota na mensagem H524 - S524: Adesão ao Serviço MB WAY (V04); Atualização da secção 4.4 <i>Guidelines</i> gerais. <p>Outras alterações editoriais sem impacto na informação técnica.</p>	AF Desenvolvimento de Serviços

Versão	Data	Descrição	Autor
01.70	2019-01-10	<p>Relativamente à versão anterior, efetuaram-se as seguintes alterações:</p> <p>Atualização de secções/capítulos</p> <ul style="list-style-type: none"> • Capítulo 1 Introdução; • Secção 3.2.2.1 Interfaces do SDK Android; • Secção 3.2.3.1 Interfaces do SDK iOS; • Secção 3.2.4 Tabela de erros. <p>Inserção de novas secções/capítulos</p> <ul style="list-style-type: none"> • Secção 3.2.2.1.11 Utilizar MULTIBANCO (Android); • Secção 3.2.3.1.7 Utilizar MULTIBANCO (iOS); • Secção 4.9 Utilizar MULTIBANCO. <p>Outras alterações editoriais sem impacto na informação técnica.</p>	AF Desenvolvimento de Serviços

Índice

1	Introdução.....	11
1.1	Âmbito	12
2	Descrição da solução	13
2.1	Ciclo de vida do serviço MB WAY	13
2.2	Funcionamento das notificações	14
2.2.1	Funcionamento das notificações na operação de compra MB WAY não presencial	14
2.2.2	Funcionamento das notificações na operação de transferências MB WAY	14
2.2.3	Funcionamento das notificações na operação de Pedido de Envio de Dinheiro	17
2.3	Levantamento MB WAY	19
2.4	Transferências MB WAY	19
2.5	Compra MB WAY (não presencial, <i>Contactless</i> e QR Code)	20
2.5.1	Compra não presencial.....	20
2.5.2	Compra MB WAY <i>Contactless</i> (NFC)	21
2.5.3	Compra MB WAY QR Code.....	23
3	Implementação do Serviço.....	25
3.1	Especificações Técnicas das mensagens <i>Host-to-Host</i> e <i>Real-Time</i>	25
3.1.1	Mensagens	25
3.1.1.1	Mensagens <i>Real-Time</i> com Iniciativa na SIBS	25
3.1.1.1.1	1161 - Pedido de Operação com cartão (Emissor) (V00)	25
3.1.1.1.2	3173 - Notificação de Operação (V01).....	28
3.1.1.1.3	Dados Variáveis das mensagens de pedido.....	29
3.1.1.2	Mensagens <i>Real-Time</i> com Iniciativa no Participante	31
3.1.1.2.1	3273 - Resposta a Notificação de Operação Pendente (V01)	31
3.1.1.3	Mensagens <i>Host-to-Host</i>	31
3.1.1.3.1	H028 - S028: Pedido Pagamento P2P (V03).....	32
3.1.1.3.2	H029 - S029: Cancelamento Transferência Instantânea P2P (V02)	34
3.1.1.3.3	H035 - S035: Consulta de Estado de Transferência P2P (V02)	36
3.1.1.3.4	H036 - S036: Confirmação de Operação Financeira (V01)	37
3.1.1.3.5	H520 - S520: Pedido de Código de Ativação para MB WAY Parceiro (V01)	39
3.1.1.3.6	H524 - S524: Adesão ao Serviço MB WAY (V04).....	40
3.1.1.3.7	H525 - S525: Cancelamento do MB WAY (V04).....	42
3.1.1.3.8	H527 - S527: Desassociação de Cartão ao MB WAY (V04).....	43
3.1.1.3.9	H532 - S532: Alteração do PIN MB WAY (V04).....	44
3.1.1.3.10	H534 - S534: Alteração de Alias de Registo do Serviço MB WAY (V03)	45
3.1.1.3.11	H552 - S552: Pedido de Referência para Levantamento MB WAY (V02)	46
3.1.1.3.12	H553 - S553: Consulta de Referências para Levantamento MB WAY (V03).....	48
3.1.1.3.13	H554 - S554: Cancelamento de Referência para Levantamento MB WAY (V02)	50
3.1.1.3.14	H623 - S623: Pedido de Envio de Dinheiro (V01).....	51
3.1.1.3.15	H624 - S624: Gestão de Pedido de Envio de Dinheiro (V01)	53
3.1.1.3.16	H625 - S625: Consulta de Pedidos de Envio de Dinheiro (V01)	55
3.2	Especificações SDK	58
3.2.1	Pressupostos	58
3.2.2	Integração para Android	59
3.2.2.1	Interfaces do SDK Android	59
3.2.2.1.1	Inicialização do SDK	61
3.2.2.1.2	Pesquisa de Operações Pendentes.....	62
3.2.2.1.3	Confirmação de uma compra pendente (Compra/Autorização)	63

3.2.2.1.4	Recusa de uma operação pendente (Compra/Autorização)	64
3.2.2.1.5	Consultar estado do SDK	65
3.2.2.1.6	Selecionar cartão default para pagamentos MB WAY Contactless	66
3.2.2.1.7	Configuração de pagamentos MB WAY Contactless	67
3.2.2.1.8	Consulta de cartões aprovisionados para MB WAY Contactless	68
3.2.2.1.9	Passagem de PIN MB WAY ao SDK	68
3.2.2.1.10	Registo de um pagamento QRCode	69
3.2.2.1.11	Utilizar MULTIBANCO	70
3.2.2.2	Objetos Referenciados pelo SDK Android	71
3.2.2.2.1	StatusResult	71
3.2.2.2.2	PendingOperation	72
3.2.2.3	Callbacks para pagamentos <i>Contactless</i>	72
3.2.2.3.1	Registo do Callback de Eventos por Listener	72
3.2.2.3.2	Callback por Intent	72
3.2.2.3.3	Callback por notificação	72
3.2.2.3.4	Bundle SDK Info	73
3.2.3	Integração para iOS	77
3.2.3.1	Interfaces do SDK iOS	77
3.2.3.1.1	Inicialização do SDK	78
3.2.3.1.2	Pesquisa de Operações Pendentes	79
3.2.3.1.3	Confirmação de uma operação pendente (Compra/Autorização)	80
3.2.3.1.4	Recusa de uma operação pendente (Compra/Autorização)	81
3.2.3.1.5	Consultar estado do SDK	82
3.2.3.1.6	Registo de um pagamento QRCode	83
3.2.3.1.7	Utilizar MULTIBANCO	84
3.2.3.2	Objetos referenciados pelo SDK iOS	85
3.2.3.2.1	PendingOperation	85
3.2.4	Tabela de erros	85
3.3	Dicionário de dados	86
4	User Experience – Regras e Guidelines	102
4.1	Apresentação	102
4.2	Princípios de <i>design</i>	102
4.2.1	Orientação ao contexto móvel	102
4.2.2	Segmentação por passos	103
4.2.3	Notificar eventos importantes	103
4.3	Regras a considerar	103
4.4	Guidelines gerais	104
4.4.1	Arquitetura de informação	104
4.4.1.1	Transações MB WAY	104
4.4.1.2	Operações secundárias	104
4.4.2	Nomenclatura	105
4.4.2.1	Transações MB WAY	105
4.4.2.2	Nos movimentos/extratos	106
4.4.2.3	Outros	106
4.4.3	Notificações	107
4.4.4	Iconografia	107
4.5	Enviar dinheiro	108
4.5.1	Primeira experiência	108
4.5.2	Enviar	108
4.6	Pedir dinheiro	109

4.6.1	Primeira experiência	109
4.6.2	Pedir	109
4.7	Pagar com MB WAY	110
4.7.1	Primeira experiência	110
4.7.2	Pagar	111
4.8	Levantar dinheiro	112
4.8.1	Casas decimais	112
4.8.2	Primeira experiência	112
4.8.3	Gerar um código	112
4.8.4	Código de levantamento	113
4.8.5	Ajuda	113
4.9	Utilizar MULTIBANCO	113
4.9.1	Primeira experiência	114
Anexo A.	Algoritmo <i>Diffie-Hellman</i>	115
A.1.	Requisitos	115
A.1.1	Exemplo	118
Anexo B.	Fluxos de Suporte à Implementação	128
B.1.	Registo do SDK	128
B.2.	Interfaces <i>AppParceiro</i> - SDK	129
B.2.1	Inicialização do SDK	129
B.2.2	Pesquisa de Operações Pendentes	130
B.2.3	Confirmação de uma Compra Pendente (Compra/Autorização)	131
B.2.4	Recusa de uma Operação Pendente (Compra/Autorização)	132
B.2.5	Consultar Estado do SDK	133
B.2.6	Selecionar cartão <i>Default</i> para Pagamentos MB WAY <i>Contactless</i>	134
B.2.7	Configuração de Pagamentos MB WAY <i>Contactless</i>	134
B.2.8	Consulta de Cartões Aprovisionados para MB WAY <i>Contactless</i>	135
B.2.9	Passagem de PIN MB WAY ao SDK	135
B.2.10	Registo de um Pagamento QRCode	136
B.3.	Interfaces <i>Parceiro</i> - Mainframe	137
B.3.1	Associação de Cartão ao MB WAY	137
B.3.2	Cancelamento do MB WAY	137
B.3.3	Cancelamento de Transferência Instantânea P2P	138
B.3.4	Cancelamento de Referência para Levantamento MB WAY	138
B.3.5	Confirmação de Operação Financeira	139
B.3.6	Adesão ao Serviço MB WAY	139
B.3.7	Desassociação de Cartão ao MB WAY	140
B.3.8	Alteração do PIN MB WAY	140
B.3.9	Alteração de <i>Alias</i> de Registo do Serviço MB WAY	141
B.3.10	Notificação de Operação Pendente	141
B.3.11	Pedido de Código de Ativação para MB WAY <i>Parceiro</i>	142
B.3.12	Pedido de Pagamento P2P	142
B.3.13	Pedido de Referência para Levantamento MB WAY	143
B.3.14	Consulta de Estado de Transferência P2P	143
B.3.15	Consulta de Referências para Levantamento MB WAY	144

Índice de Figuras

Figura 1 - Funcionamento das notificações na operação de compra MB WAY não presencial	14
Figura 2 - Fluxo de compra não presencial (não exaustivo).....	20
Figura 3 - Fluxo de compra NFC (não exaustivo)	22
Figura 4 - Fluxo de compra NFC (experiência cliente ilustrativa).....	22
Figura 5 - Fluxo de compra QR Code (não exaustivo)	23
Figura 6 - Fluxo de compra QR Code (experiência cliente ilustrativa)	24
Figura 7 - Nomenclatura MB WAY	105
Figura 8 - Ícones representativos das operações MB WAY	107
Figura 9 - Funcionalidade “Enviar Dinheiro”	108
Figura 10 - Como funciona o “Envio de Dinheiro”	108
Figura 11 - Funcionalidade “Pedir Dinheiro”	109
Figura 12 - Como funciona o “Pedido de Dinheiro”	109
Figura 13 - Funcionalidade “Pagar com MB WAY”	110
Figura 14 - Como funciona o “Pagamento com MB WAY”	111
Figura 15 - Funcionalidade “Levantar dinheiro”	112
Figura 16 - Como funciona o “Levantamento de Dinheiro”	112
Figura 17 - Código de Levantamento	113
Figura 18 - Funcionalidade “Utilizar MULTIBANCO”	114
Figura 19 - Como funciona a opção “Utilizar MULTIBANCO”	114
Figura 20 - C(2e, 0s) <i>schemes: each party contributes only and ephemeral key pair</i>	117
Figura 21 - Registo do SDK	128
Figura 22 - Inicialização do SDK (iOS).....	129
Figura 23 - Inicialização do SDK (Android)	129
Figura 24 - Pesquisa de Operações Pendentes (iOS)	130
Figura 25 - Pesquisa de Operações Pendentes (Android)	130
Figura 26 - Confirmação de uma Compra Pendente (iOS)	131
Figura 27 - Confirmação de uma Compra Pendente (Android)	131
Figura 28 - Recusa de uma Operação Pendente (iOS)	132
Figura 29 - Recusa de uma Operação Pendente (Android)	132
Figura 30 - Consultar Estado do SDK (iOS).....	133
Figura 31 - Consultar Estado do SDK (Android)	133
Figura 32 - Selecionar Cartão <i>Default</i> para Pagamentos MB WAY <i>Contactless</i>	134
Figura 33 - Configuração de Pagamentos MB WAY <i>Contactless</i>	134
Figura 34 - Consulta de Cartões Aprovisionados para MB WAY <i>Contactless</i>	135
Figura 35 - Passagem de PIN MB WAY ao SDK	135
Figura 36 - Registo de um Pagamento QRCode (iOS)	136
Figura 37 - Registo de um Pagamento QRCode (Android)	136
Figura 38 - Associação de Cartão ao MB WAY	137
Figura 39 - Cancelamento do MB WAY	137
Figura 40 - Cancelamento de Transferência Instantânea P2P.....	138
Figura 41 - Cancelamento de Referência para Levantamento MB WAY	138
Figura 42 - Confirmação de Operação Financeira	139
Figura 43 - Adesão ao Serviço MB WAY	139
Figura 44 - Desassociação de Cartão ao MB WAY	140
Figura 45 - Alteração do PIN MB WAY.....	140
Figura 46 - Alteração de <i>Alias</i> de Registo do Serviço MB WAY.....	141
Figura 47 - Notificação de Operação Pendente	141
Figura 48 - Pedido de Código de Ativação para MB WAY Parceiro.....	142
Figura 49 - Pedido de Pagamento P2P.....	142

Figura 50 - Pedido de Referência para Levantamento MB WAY	143
Figura 51 - Consulta de Estado de Transferência P2P	143
Figura 52 - Consulta de Referências para Levantamento MB WAY	144

Índice de Tabelas

Tabela 1 - Funcionamento das notificações na operação de transferências MB WAY	15
Tabela 2 - Funcionamento das notificações na operação de Pedido de Envio de Dinheiro	17
Tabela 3 - Mensagens notificações locais	59
Tabela 4 - Lista de Operações Suportadas pelo SDK Android	60
Tabela 5 - Lista de Listeners utilizados pelo SDK Android	60
Tabela 6 - <i>Input</i> do pedido de inicialização do SDK (Android)	61
Tabela 7 - <i>Input</i> do método MBWAYSdkInitListener.onInitResult() (Android)	62
Tabela 8 - Possíveis estados de retorno (status) da inicialização do SDK (Android)	62
Tabela 9 - <i>Input</i> do pedido de pesquisa de operações pendentes (Android)	62
Tabela 10 - <i>Input</i> do método MBWAYSdkPendingOperationsListener.onPendingOperationResult() (Android)	63
Tabela 11 - Possíveis estados de retorno (status) do pedido de operações pendentes (Android)	63
Tabela 12 - <i>Input</i> do pedido de confirmação de compra pendente (Android)	63
Tabela 13 - <i>Input</i> do método MBWAYSdkOperationListener.onOperationResult() (Android)	64
Tabela 14 - Possíveis estados de retorno (status) do pedido de confirmação de compra pendente (Android)	64
Tabela 15 - <i>Input</i> do pedido de recusa de compra pendente (Android)	64
Tabela 16 - <i>Input</i> do método MBWAYSdkOperationListener.onOperationResult() (Android)	65
Tabela 17 - Possíveis estados de retorno (status) do pedido de recusa de compra pendente (Android)	65
Tabela 18 - <i>Input</i> do pedido de consulta do estado do SDK (Android)	65
Tabela 19 - <i>Input</i> do método MBWAYSdkGetStatusListener.onGetSdkStatusResult() (Android)	66
Tabela 20 - <i>Input</i> do pedido de selecionar cartão default para compras MB WAY Contactless (Android)	66
Tabela 21 - <i>Input</i> do método MBWAYSdkSetCardForContactlessPaymentListener.onSetCardForContactless PaymentResult() (Android)	67
Tabela 22 - Possíveis estados de retorno (status) do pedido para selecionar cartão default para compras MB WAY Contactless (Android)	67
Tabela 23 - <i>Input</i> do pedido de configuração de pagamentos MB WAY Contactless (Android)	67
Tabela 24 - <i>Input</i> do pedido de consultar a lista de cartões provisionados (Android)	68
Tabela 25 - <i>Input</i> do método MBWAYSdkGetProvisionedCardsListener.onGetProvisionedCardsResult() (Android)	68
Tabela 26 - <i>Input</i> do pedido de passagem de PIN MB WAY ao SDK	69
Tabela 27 - <i>Input</i> do pedido de pagamento QRCode (Android)	69
Tabela 28 - <i>Input</i> do método MBWAYSdkQRCodePaymentListener.onQRCodePaymentResult() (Android)	69
Tabela 29 - Possíveis estados de retorno (status) do pedido de pagamento QRCode (Android)	70
Tabela 30 - <i>Input</i> do pedido de pagamento QRCode (Android)	70
Tabela 31 - <i>Input</i> do método MBWAYSdkQRCodeUnlockATMLListener.onQRCodeUnlockATMResult() (Android)	71
Tabela 32 - Possíveis estados de retorno (status) do pedido de acesso ao MULTIBANCO via MB WAY (Android)	71
Tabela 33 - Definição do objeto <i>Output</i> Get Status (Android)	71
Tabela 34 - Possíveis estados do SDK (state)	71
Tabela 35 - Definição do objeto PendingOperation (SDK Android)	72
Tabela 36 - Chaves do Bundle SDK	73
Tabela 37 - Tipos de HCE_CALLBACKTYPE	73
Tabela 38 - Lista de Operações Suportadas pelo SDK iOS	77
Tabela 39 - Lista de <i>Callbacks</i> utilizados pelo SDK iOS	77
Tabela 40 - <i>Input</i> do pedido de inicialização do SDK (iOS)	78
Tabela 41 - <i>Input</i> do <i>Callback</i> onInitResult:andMessage: (iOS)	78
Tabela 42 - Possíveis estados de retorno (status) da inicialização do SDK (iOS)	78

Tabela 43 - <i>Input</i> do pedido de pesquisa de operações pendentes (iOS)	79
Tabela 44 - <i>Input</i> do método onPendingOperationResult:andStatus:andMessage: (iOS)	79
Tabela 45 - Possíveis estados de retorno (status) do pedido de consulta de operações pendentes (iOS)	79
Tabela 46 - <i>Input</i> do pedido de confirmação de compra pendente (iOS)	80
Tabela 47 - <i>Input</i> do método onOperationResult:andStatus:andMessage: (iOS)	80
Tabela 48 - Possíveis estados de retorno (status) do pedido de confirmação de compra pendente (iOS)	80
Tabela 49 - <i>Input</i> do pedido de recusa de compra pendente (iOS)	81
Tabela 50 - <i>Input</i> do método onOperationResult:andStatus:andMessage: (iOS)	81
Tabela 51 - Possíveis estados de retorno (status) do pedido de recusa de compra pendente (iOS)	82
Tabela 52 - <i>Input</i> do pedido de consulta do estado do SDK (iOS)	82
Tabela 53 - <i>Input</i> do método onGetSDKStatusResult: (iOS)	82
Tabela 54 - Possíveis estados do SDK (iOS)	82
Tabela 55 - <i>Input</i> do pedido de pagamento QRCode (iOS)	83
Tabela 56 - <i>Input</i> do método onQRCodePaymentResult:status andMessage: (iOS)	83
Tabela 57 - Possíveis estados de retorno (status) do pedido de pagamento QRCode (iOS)	84
Tabela 58 - <i>Input</i> do pedido de acesso ao MULTIBANCO via MB WAY (iOS)	84
Tabela 59 - <i>Input</i> do método onQRCodeUnlockATMResult:status andMessage: (iOS)	84
Tabela 60 - Possíveis estados de retorno (status) do pedido de acesso ao MULTIBANCO via MB WAY (iOS)	85
Tabela 61 - Definição do objeto PendingOperation (SDK iOS)	85
Tabela 62 - Código e descrição de erros retornados pelo SDK	85

1 Introdução

O MB WAY tem vindo a disponibilizar interfaces das várias funcionalidades que disponibiliza na *app* MB WAY para que os Bancos possam incorporar essas mesmas funcionalidades nos seus canais de *homebanking* e *mobile banking*.

Atualmente os Emissores têm disponíveis as **interfaces necessárias para permitir a um cliente que use a *app* MB WAY**:

1. **Aderir ao MB WAY - Operativa de adesão e gestão do MB WAY** – Estas interfaces devem ser implementadas sempre que o Banco Emissor pretenda disponibilizar a possibilidade dos seus clientes aderirem ao MB WAY nos seus canais, sendo que para usar as várias funcionalidades MB WAY, o Cliente tem de usar a *app* MB WAY. Estas interfaces permitem:
 - Adesão e definição de PIN MB WAY;
 - Associação/desassociação de cartão;
 - Alteração de PIN MB WAY;
 - Alteração de número de telemóvel;
 - Alteração de limite diário.
2. **Transferir com MB WAY - Operativa de transferências MB WAY** – Esta interface deve ser implementada sempre que o Banco Emissor pretenda disponibilizar a possibilidade dos seus clientes iniciarem uma transferência MB WAY nos seus canais, sendo que, para receber transferências, é necessário o Cliente instalar a *app* MB WAY.
Sempre que o número destino ainda não é MB WAY, é enviado um SMS de convite à adesão. A receção é na *app* MB WAY.
3. **Levantar com MB WAY - Operativa de levantamento MB WAY** – Esta interface deve ser usada sempre que o Banco pretenda disponibilizar a possibilidade dos seus clientes MB WAY (já aderiram e ativaram a *app* MB WAY) efetuarem um pedido de geração de código de levantamento MB WAY.
4. **Utilizar MULTIBANCO - Operativa de acesso ao MULTIBANCO via *app* do Banco** – Esta interface deve ser utilizada sempre que o Banco pretenda disponibilizar aos seus clientes a possibilidade de utilizarem a *app* do Banco como alternativa ao cartão bancário, para acederem às funcionalidades do MULTIBANCO.

Por forma a poder suportar a nova configuração em que o Cliente MB WAY pode usar a *app* do Banco como alternativa à *app* MB WAY, para ter acesso a todas as funcionalidades MB WAY, as interfaces atuais evoluíram e surgiram novas interfaces relativas à operação de compra MB WAY.

Esta evolução inclui a **adaptação das interfaces atuais**:

- **interfaces de adesão**, inerentes ao facto de o cliente poder usar a *app* do Banco como alternativa à *app* MB WAY, onde a fidelização do número de telemóvel e a autenticação das operações passa a ser da responsabilidade do Banco;

- **interfaces de transferências e de levantar dinheiro**, inerentes ao desvívulo de a necessidade do cliente ter *app* MB WAY para receber transferências.

Esta evolução inclui igualmente as **novas interfaces** que se apresentam em seguida:

- **interfaces de compra MB WAY com NFC (SDK);**
- **interfaces de compra não presencial com número de telemóvel (SDK);**
- **interfaces de notificação (compras, transferências pedidas e enviadas)** – permitem notificar os bancos quando existe uma compra e quando existe uma transferência para clientes que utilizam a *app* dos Bancos. São os Bancos que depois notificam as *apps* dos seus clientes;
- **Interface de aprovação de transferência** – aplica-se sempre que existe aceitação da transferência na *app* do Banco;
- **Interfaces de Pedido de Envio de Dinheiro (Pedido, Gestão de Pedido e Consulta de Pedido)** – permitem que um utilizador do serviço MB WAY possa pedir a um dos seus contactos que lhe envie um determinado montante e que possa gerir esses pedidos (incluindo “relembrar” e “cancelar” pedidos efetuados), bem como consultar os mesmos;
- **Interfaces de Utilizar MULTIBANCO (SDK).**

Decorrente do facto das *apps* dos Emissores poderem constituir-se como um canal alternativo para os clientes usufruírem das funcionalidades MB WAY, este documento congrega igualmente um **conjunto de *user experience guidelines***.

Estas *guidelines* incluem regras a cumprir em âmbito de implementação, bem como recomendações gerais que ficam inteiramente ao critério das equipas de cada Emissor.

1.1 Âmbito

Este documento identifica as novas interfaces necessárias para que os Emissores disponibilizem as funcionalidades MB WAY nas suas mobile *apps*, funcionando estas, para os seus clientes, como uma alternativa à utilização da *app* MB WAY.

Nesta *release* estão detalhadas as seguintes interfaces:

1. Adesão e Gestão do serviço MB WAY
2. Envio de transferências
3. Receção de transferências
4. Levantamento MB WAY
5. Compra NFC (SDK)
6. Compra não presencial (SDK)
7. Compra QR Code (SDK)
8. Pedido de Envio de Dinheiro
9. **Utilizar MULTIBANCO (SDK)**

2 Descrição da solução

Com a implementação das várias interfaces, o Banco fica apto a disponibilizar as várias funcionalidades MB WAY nos seus canais proprietários.

Para que o Banco possa ficar desvinculado da *app* MB WAY, é condição obrigatória que implemente as novas versões das várias interfaces MB WAY que estão descritas neste documento. Neste cenário é de salientar que a responsabilidade de fidelização do número de telemóvel é do Banco, ou seja, quando a SIBS recebe o pedido de criação de um serviço MB WAY, é assumido que o Banco efetuou os procedimentos de segurança necessários que atestam que o número de telemóvel está na posse do Cliente.

2.1 Ciclo de vida do serviço MB WAY

Neste tipo de serviços, o Banco desempenha a função de *Owner*, pelo que o ciclo de vida dos serviços MB WAY é gerido pelo Banco e é da sua total responsabilidade.

Os estados que estão previstos para este tipo de serviço, são:

1. **Estado ativo** – estado em que o serviço fica quando é criado pelo banco através da interface H524.
2. **Estado desativo sem cartões** – estado em que o serviço fica caso deixe de ter cartões associados, como, por exemplo, no caso dos seus cartões expirem e não serem renovados. O serviço pode passar novamente a “ativo” com a associação de um cartão por parte do Banco. No caso de um cartão expirar, é o Banco que tem que enviar o novo cartão para salvaguardar que o serviço se mantém a funcionar.
3. **Estado removido** – estado em que o serviço fica quando é cancelado pelo Banco através da interface H525 - S525: Cancelamento do MB WAY.
4. **Estado bloqueado por fraude** – O serviço fica “bloqueado por fraude” sempre que a SIBS identificar atividade fraudulenta por parte do utilizador. A SIBS é responsável por monitorizar e bloquear o serviço ao utilizador nesta situação. O Banco não pode colocar um serviço neste estado, devendo sempre informar a SIBS caso pretenda fazê-lo ou, em alternativa, enviar um pedido de cancelamento do serviço.
5. **Estado suspenso** – O serviço fica em estado “suspenso” uma vez atingido um número máximo de tentativas de ativação do SDK. Este estado é irreversível, só podendo passar para o estado “removido” através da interface da mensagem H525 - S525: Cancelamento do MB WAY. A passagem para o estado “removido” tem de ser efetuada pelo Banco. Caso o Banco pretenda ativar novamente o serviço para aquele Cliente, o serviço anterior tem, obrigatoriamente, de estar removido.

2.2 Funcionamento das notificações

O comportamento no envio de notificações tem de ser ajustado ao novo paradigma MB WAY em que é possível existir no mesmo telemóvel a *app* de um ou mais bancos e a *app* MB WAY.

Para garantir uma experiência em linha com o que é prática no mercado, cada uma das aplicações é responsável por notificar o seu cliente e, desta forma, garantir uma experiência própria.

2.2.1 Funcionamento das notificações na operação de compra MB WAY não presencial

No caso de uma compra não presencial MB WAY, a SIBS recebe o pedido de pagamento por parte do comerciante e o comportamento é o seguinte: caso o cliente MB WAY tenha *apps* de Banco e *app* MB WAY, recebe uma notificação em todas. A notificação para a *app* de bancos é o Banco que envia, ao passo que a SIBS envia para a *app* MB WAY.

A *app* na qual o cliente aceita o pagamento é a *app* que recebe, posteriormente, a confirmação do pagamento.




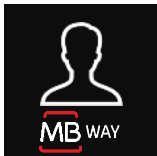




Figura 1 - Funcionamento das notificações na operação de compra MB WAY não presencial



2.2.2 Funcionamento das notificações na operação de transferências MB WAY

No caso das transferências P2P, apresentamos em baixo uma tabela que visa expor o comportamento esperado em diversos cenários, com as respetivas interfaces associadas para concretizar as transferências.

Tabela 1 - Funcionamento das notificações na operação de transferências MB WAY

	Ordenante	Destinatário	Notificações	Observações
1	Aderente Banco exclusivo 	Não aderente 	Banco é informado na resposta ao pedido de p2p de que este ficou pendente de adesão do destinatário. 1) Com esta informação, banco pode informar o ordenante que a p2p ficou pendente de adesão 2) SIBS envia SMS ao destinatário para que adira ao MB WAY	- Uma vez pendente de adesão apenas pode ser executada quando o cliente aderir ao MB WAY. - Banco pode consultar estado da transferência, por forma a saber quando foi executada (se o destinatário aderir), através da pesquisa de Transferências H2H (Bank Key ou Service Operation Code) - mensagem H035
2	Aderente Banco exclusivo 	Aderente MB WAY exclusivo 	Destinatário recebe notificação na <i>app</i> MB WAY e: 1) Se p2p fica pendente de aceitação – Banco é informado na resposta ao pedido de p2p de que este ficou pendente de aceitação do destinatário. 2) Se p2p não fica pendente (caso em que tem 1 cartão na <i>app</i> MB WAY ou um cartão <i>default</i> para receber) - A transferência é processada de imediato com operações 179 (débito) e 199 (crédito).	Para o ponto 1) o Banco pode consultar estado da transferência, por forma a saber quando foi executada (se o destinatário aderir), através da pesquisa de Transferências H2H (Bank Key ou Service Operation Code) - mensagem H035
3	Aderente Banco exclusivo 	Aderente MB WAY e Banco 	1) Se destinatário tem apenas 1 cartão no MB WAY ou tem 1 cartão <i>default</i> definido na <i>app</i> MB WAY, o destinatário é notificado na <i>app</i> MB WAY e a p2p é processada no imediato com operações 179 (débito) e 199 (crédito). O Banco tem informação para notificar o ordenante. 2) Se destinatário tem mais do que um cartão na <i>app</i> MB WAY e não tem definido um cartão <i>default</i> , as 2 <i>apps</i> são notificadas - SIBS notifica MB WAY e Banco notifica a sua <i>app</i> . a) Se o destinatário aceita na <i>app</i> MB WAY com cartão que não seja do próprio Banco - operação segue para processamento e Banco recebe operação (179 débito) e fica com informação para notificar o ordenante. O destinatário é informado pela SIBS b) Se o destinatário aceita na <i>app</i> MB WAY com cartão do próprio banco - operação segue para processamento e banco recebe operação 179 débito e a operação 199 de crédito. O destinatário é informado pela SIBS na <i>app</i> MB WAY. c) Se o destinatário aceita na <i>app</i> do Banco - operação segue para	- O Banco é notificado com a PRT 3173 , de que existe uma transferência pendente - O Banco não é notificado em casos de aceitação/rejeição no MB WAY. Para poder informar o ordenante em conformidade, pode consultar o estado da operação com o ServiceOperationCode na pesquisa com a mensagem H035 . - Para aceitar/rejeitar a p2p na <i>app</i> do Banco, o Banco utiliza a mensagem H036 e recebe sempre a resposta de sucesso/erro sincronamente. No que diz respeito ao ponto 2) , será necessário o envio de um Código de Aceitação P2P por SMS para o número de telefone do utilizador




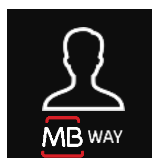
	Ordenante	Destinatário	Notificações	Observações
			processamento e Banco recebe operação 179 débito e a operação 199 de crédito. Neste caso o Banco notifica ordenante e destinatário.	
4	Aderente MB WAY exclusivo 	Aderente exclusivo Banco 	<p>1) Se destinatário só tem um cartão na <i>app</i> do Banco - A p2p é processada no imediato com operações 179 (débito ao Banco do ordenante) e 199 (crédito). O Banco tem informação para notificar o destinatário. SIBS notifica o ordenante na <i>app</i> MB WAY.</p> <p>2) Se destinatário tem mais do que um cartão na <i>app</i> do Banco, Banco notifica o cliente para que escolha o cartão. Quando cartão é escolhido, o Banco notifica o cliente quando a p2p é processada e a SIBS notifica o ordenante.</p>	- Na situação 2), o Banco é notificado com a PRT 3173 , de que existe uma transferência pendente- Para aceitar/rejeitar a p2p na <i>app</i> do Banco. O Banco utiliza a mensagem H036 e recebe sempre a resposta de sucesso/erro sincronamente.
5	Aderente MB WAY exclusivo 	Aderente MB WAY e Banco 	<p>1) Se destinatário tem apenas 1 cartão no MB WAY ou tem 1 cartão <i>default</i> definido na <i>app</i> MB WAY, o destinatário é notificado na <i>app</i> MB WAY e a p2p é processada no imediato com operações 179 (débito) e 199 (crédito). O Banco tem informação para notificar o ordenante.</p> <p>2) Se destinatário tem mais do que um cartão na <i>app</i> MB WAY e não tem definido um cartão <i>default</i>, as 2 <i>apps</i> são notificadas - SIBS notifica MB WAY e Banco notifica a sua <i>app</i>.</p> <p>a) Se o destinatário aceita na <i>app</i> MB WAY com cartão que não seja o do próprio Banco - operação segue para processamento e Banco recebe operação (179 débito) e fica com informação para notificar o ordenante. O destinatário é informado pela SIBS</p> <p>b) Se o destinatário aceita na <i>app</i> MB WAY com cartão do próprio Banco - operação segue para processamento e Banco recebe operação 179 débito e a operação 199 de crédito. O destinatário é informado pela SIBS na <i>app</i> MB WAY.</p> <p>c) Se o destinatário aceita na <i>app</i> do Banco - operação segue para processamento e Banco recebe operação 179 débito e a operação 199 de crédito. Neste caso, o Banco notifica ordenante e destinatário.</p>	<p>- O Banco é notificado com a PRT 3173, de que existe uma transferência pendente</p> <p>- O Banco não é notificado em casos de aceitação/rejeição no MB WAY. Para poder informar o ordenante em conformidade, pode consultar o estado da operação com o ServiceOperationCode na pesquisa com a mensagem H035.</p> <p>- Para aceitar/rejeitar a p2p na M-Wallet o banco utiliza a mensagem H036 e recebe sempre a resposta de sucesso/erro sincronamente.</p> <p>No que diz respeito ao ponto 2), será necessário o envio de um Código de Aceitação P2P por SMS para o número de telefone do utilizador</p>







	Ordenante	Destinatário	Notificações	Observações
6	Aderente MB WAY e Banco 	Aderente exclusivo Banco 	<p>1) Se destinatário só tem um cartão na <i>app</i> do Banco - A p2p é processada no imediato com operações 179 (débito ao Banco do ordenante) e 199 (crédito). O Banco tem informação para notificar o destinatário. SIBS notifica o ordenante na <i>app</i> MB WAY.</p> <p>2) Se destinatário tem mais do que um cartão na <i>app</i> do Banco, Banco notifica o cliente para que escolha o cartão. Quando cartão é escolhido na <i>app</i> do Banco, o Banco notifica o cliente quando a p2p é processada e a SIBS notifica o ordenante.</p>	<p>- Na situação 2) O Banco é notificado com a PRT 3173, de que existe uma transferência pendente</p> <p>- Para aceitar/rejeitar a p2p na M-Wallet o banco utiliza a mensagem H036 e recebe sempre a resposta de sucesso/erro sincronamente.</p>

2.2.3 Funcionamento das notificações na operação de Pedido de Envio de Dinheiro

Apresentamos em baixo uma tabela que visa expor o funcionamento das notificações na operação de Pedido de Envio de Dinheiro.

Tabela 2 - Funcionamento das notificações na operação de Pedido de Envio de Dinheiro

	Ordenante do Request Money	Destinatário do Request Money	Notificações	Observações
1	Aderente Banco exclusivo 	Não aderente 	- É sugerido que quem está a pedir dinheiro envie um SMS ao destinatário para que este adira ao MB WAY. A decisão de envio é de quem está a pedir o dinheiro.	- O Banco tem de saber a priori se o número destinatário é, ou não, MB WAY através da interface que já existe. Esta interface permite verificar se determinado número de telemóvel é aderente ao MB WAY. Se não é aderente, não chega a gerar pedido de dinheiro. Este cenário não deve chegar a gerar o pedido de dinheiro na SIBS. No entanto, se o Banco enviar a H623 – Pedido de Envio de Dinheiro, mas destinatário não é aderente ao MB WAY, é devolvido um erro.
2	Aderente Banco exclusivo 	Aderente MB WAY exclusivo 	<p>Destinatário recebe notificação de Pedido de Envio de Dinheiro na <i>app</i> MB WAY e:</p> <p>1) Se aceitar – é processada uma transferência em que o destinatário é quem pediu o dinheiro. Banco tem de ser notificado de que este pedido foi fechado para poder informar o seu cliente de que recebeu o dinheiro que tinha pedido.</p> <p>2) Se não aceitar – a transferência não é processada, mas o Banco</p>	<p>- Banco Ordenante do Pedido de Envio de Dinheiro envia H623 – Pedido de Envio de Dinheiro e recebe o ID da operação (SEE_IDEOPR).</p> <p>- Quando o Destinatário do Pedido de Envio de Dinheiro aceita, o Ordenante do Pedido de Envio de Dinheiro vai ser notificado na mensagem <i>real-time</i> do crédito (1163, operação 199, onde é enviado o ID da operação (SEE_IDEOPR)).</p> <p>- Quando o Pedido de Envio de Dinheiro expira, é cancelado, recusado ou anulado, é enviada uma</p>

	Ordenante do Request Money	Destinatário do Request Money	Notificações	Observações
			tem de saber para poder informar quem pediu o dinheiro.	mensagem <i>real-time</i> 3173 com o Código de Operação e o Estado.
3	Aderente Banco exclusivo 	Aderente MB WAY e Banco 	Destinatário recebe notificação de Pedido de Envio de Dinheiro na <i>app</i> MB WAY e na <i>app</i> do Banco: 1) Se aceitar – é processada uma transferência em que o destinatário é quem pediu o dinheiro. Banco tem de ser notificado de que este pedido foi fechado para poder informar o seu cliente de que recebeu o dinheiro que tinha pedido. 2) Se não aceitar – a transferência não é processada, mas o Banco tem de saber para poder informar quem pediu o dinheiro.	- Banco Ordenante do Pedido de Envio de Dinheiro envia H623 – Pedido de Envio de Dinheiro e recebe o ID da operação (SEE_IDEOPR) - O Banco Destinatário do Pedido de Envio de Dinheiro é notificado via mensagem <i>real-time</i> 3173 que tem um Pedido de Envio de Dinheiro (Código de operação e o Estado = Pendente). - Quando o Destinatário do Pedido de Envio de Dinheiro aceita, o Ordenante do Pedido de Envio de Dinheiro vai ser notificado na mensagem <i>real-time</i> do crédito (mensagem <i>real-time</i> 1163, operação 199, onde é enviado o ID da operação (SEE_IDEOPR)). - Quando o Pedido de Envio de Dinheiro expira, é cancelado, recusado ou anulado é enviada uma mensagem <i>real-time</i> 3173 com o Código de Operação e o Estado. - O Banco Destinatário do Pedido de Envio de Dinheiro é notificado pela mensagem <i>real-time</i> 1161, operação 179, onde é enviado o ID da operação (SEE_IDEOPR).
4	Aderente MB WAY exclusivo 	Aderente exclusivo Banco 	Destinatário do pedido recebe notificação de Pedido de Envio de Dinheiro na <i>app</i> do Banco: 1) Se aceitar - é processada uma transferência em que o destinatário é quem pediu o dinheiro. SIBS tem de notificar o utilizador na <i>app</i> MB WAY de que recebeu o dinheiro que tinha pedido.	- Para o Banco conseguir notificar o seu cliente, recebe uma notificação através da mensagem <i>real-time</i> 3173. - Quando o destinatário aceita na <i>app</i> do Banco, o Pedido de Envio de Dinheiro é processado com as mensagens já existentes. - SIBS informa na <i>app</i> MB WAY.
5	Aderente MB WAY exclusivo 	Aderente MB WAY e Banco 	Destinatário recebe notificação de Pedido de Envio de Dinheiro na <i>app</i> do Banco e na <i>app</i> MB WAY: 1) Se aceitar na <i>app</i> do Banco - é processada uma transferência em que o destinatário é quem pediu o dinheiro. SIBS tem de notificar o utilizador na <i>app</i> MB WAY de que recebeu o dinheiro que tinha pedido. 2) Se aceitar na <i>app</i> MB WAY - é processada uma transferência em que o destinatário é quem pediu o dinheiro. As notificações são enviadas pela SIBS.	- SIBS notifica na <i>app</i> MB WAY.

2.3 Levantamento MB WAY

Para disponibilizar a operação de levantamento nos seus canais, sem qualquer dependência da *app* MB WAY, o Banco tem de implementar as novas versões das mensagens nas seguintes interfaces:

- H524 - S524: Adesão ao MB WAY;
- H525 - S525: Cancelamento do MB WAY;
- H526 - S526: Associação de cartão ao MB WAY;
- H527 - S527: Desassociação de Cartão ao MB WAY;
- H532 - S532: Alteração do PIN MB WAY;
- H534 - S534: Alteração de Alias de Registo do MB WAY;
- H552 - S552: Geração de Referência para Levantamento MB WAY;
- H553 - S553: Consulta de Referências para Levantamento MB WAY;
- H554 - S554: Cancelamento de referência para Levantamento MB WAY.

Para mais informações sobre a operativa de levantamento MB WAY, deve ser consultado o documento DCSIBS100026_MI_PT_Manual de Implementação – Serviços para Emissores – Emissores_V03.50-docx.

2.4 Transferências MB WAY

Para disponibilizar a operação de levantamento nos seus canais, sem qualquer dependência da *app* MB WAY, o Banco tem de implementar as novas versões das mensagens das seguintes interfaces:

- H524 - S524: Adesão ao MB WAY;
- H525 - S525: Cancelamento do MB WAY;
- H526 - S526: Associação de Cartão ao MB WAY;
- H527 - S527: Desassociação de Cartão ao MB WAY;
- H532 - S532: Alteração do PIN MB WAY;
- H534 - S534: Alteração de Alias de Registo do MB WAY;
- H028 - S028: Pedido Pagamento P2P;
- H029 - S029: Cancelamento Transferência instantânea P2P;
- H035 - S035: Consulta de Estado de Transferência P2P;
- H036 - S036: Confirmação de Operação Financeira.

Para além destas interfaces, é ainda necessário implementar a mensagem PRT 3173 - Notificação de Operação Pendente.

Para mais informações sobre esta operativa de transferências MB WAY, deve ser consultado o documento DCSIBS100026_MI_PT_Manual de Implementação - Serviços para Emissores - Emissores_V03.50-docx.

2.5 Compra MB WAY (não presencial, *Contactless* e QR Code)

Para disponibilizar a operação de compra nos seus canais, o Banco tem de implementar as novas versões das mensagens das seguintes interfaces:

- H524 - S524: Adesão ao MB WAY;
- H525 - S525: Cancelamento do MB WAY;
- H526 - S526: Associação de Cartão ao MB WAY;
- H527 - S527: Desassociação de Cartão ao MB WAY;
- H532 - S532: Alteração do PIN MB WAY;
- H534 - S534: Alteração de Alias de Registo do MB WAY.

Para além destas interfaces, é ainda necessário implementar a mensagem PRT 3173 - Notificação de Operação Pendente e o SDK.

Em seguida apresentamos os vários fluxos da compra.

2.5.1 Compra não presencial

Este modelo de compra é fortemente utilizado no comércio online. O cliente indica ao comerciante o seu número de telemóvel e recebe uma notificação na(s) sua(s) *app(s)* para confirmar o pagamento.

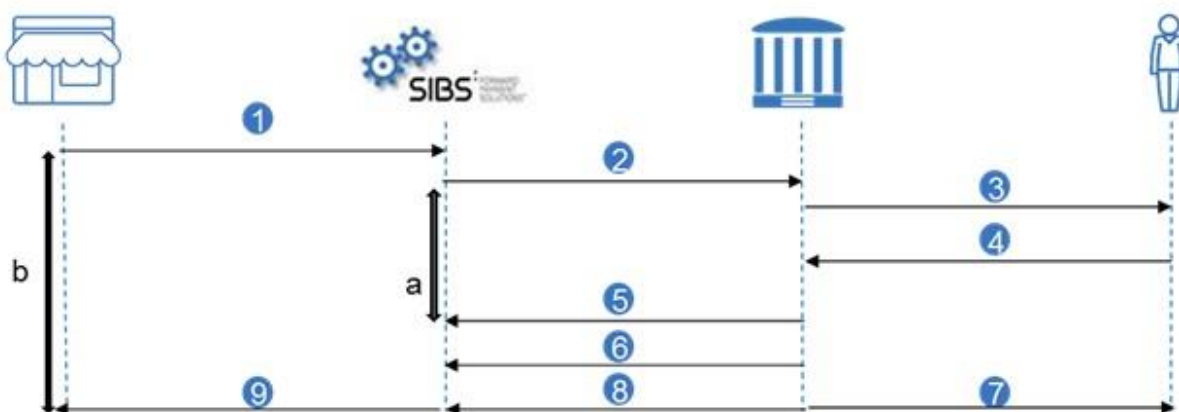


Figura 2 - Fluxo de compra não presencial (não exaustivo)

1. Comerciante envia um pedido de compra para a SIBS;
2. SIBS verifica se número está associado a um serviço MB WAY. Caso exista, SIBS trata a informação recebida e informa Banco que há um pedido de compra para que este notifique o cliente na sua *app mobilebanking*. Se o cliente também tiver *app* MB WAY, notifica;

3. Banco faz verificações internas e notifica cliente¹;
4. Cliente escolhe cartão e confirma compra com autenticação na *app* do Banco;
5. Banco confirma autenticação;
6. SIBS envia para autorização;
7. Banco processa pedido de autorização e notifica cliente do resultado da compra;
8. Banco envia resultado do pedido de autorização;
9. SIBS notifica comerciante sobre o resultado da compra.

2.5.2 Compra MB WAY *Contactless* (NFC)

Este tipo de compra está disponível para aplicações com sistema operativo Android. É utilizada em ambientes presenciais quando os terminais da Rede MULTIBANCO têm capacidade *contactless* MB.

Para poder realizar um pagamento MB WAY *contactless*, o cliente tem de ligar a antena NFC do seu telemóvel, bem como ter a aplicação do Banco definida como preferida para pagamentos.

Depois de ter as configurações ativadas, o Cliente encosta o telemóvel ao TPA MULTIBANCO. Existem várias opções para efetuar este pagamento:

- a. Com telemóvel desbloqueado e *app* fechada;
- b. Com telemóvel desbloqueado e *app* aberta;
- c. Com telemóvel bloqueado (disponível sempre que o próprio telemóvel assim o permita).

Ao encostar o telemóvel ao terminal, é o SDK que trata das comunicações entre a *app* do Banco e o TPA MULTIBANCO enquanto canal de comunicação com a SIBS, para processar a transação.

Para transações acima de 20€ a autenticação é obrigatória. Esta parametrização deve estar disponível na *app* do Banco para que o Cliente possa ter também a opção de colocar autenticação para operações de valor abaixo dos 20€.

O processamento da transação, na SIBS, segue o mesmo processo de uma compra com cartão, sendo que neste caso a SIBS converte o *token* do cartão que é enviado para o TPA, no cartão real para envio da autorização da transação ao Banco. O TPA apresenta o resultado da transação ao cliente, sendo que o Banco também deve notificar o seu cliente sobre o resultado da transação na *app* do Banco.

¹ Serão previstos códigos de erro/sucesso a enviar por parte do banco à SIBS e por parte da SIBS ao Banco (o que atualmente é a SIBS a notificar o Cliente, passará a ser o Banco)

- a) Deverá ser definido um tempo máximo para o banco responder ao pedido de compra enviado pela SIBS
- b) Ter em conta o tempo de resposta total (fator crítico de sucesso)

O procedimento de compra é o seguinte:

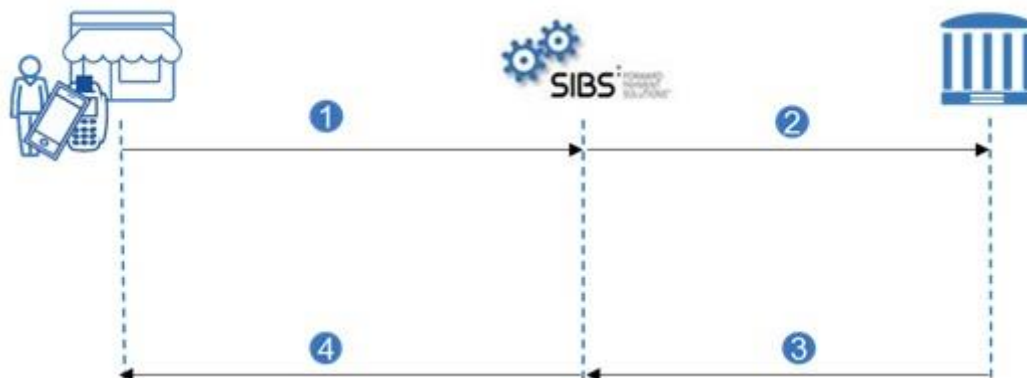


Figura 3 - Fluxo de compra NFC (não exaustivo)

1. Cliente encosta telemóvel no TPA MULTIBANCO do comerciante e inicia-se comunicação entre SDK MB WAY que está na *app* do Banco e o TPA. De acordo com as validações e funções, o SDK vai interagindo em conformidade com a *app* do Banco e com o TPA e, quando a interação fica completa, a transação segue para processamento. Esta interação é *tokenizada* para o terminal, bem como a autenticação do cliente, na *app* do Banco, sempre que necessário.
2. SIBS *destokeniza* a operação que recebe do terminal, no cartão real, e prossegue com o envio da transação para autorização junto do Banco.
3. Banco processa pedido de autorização e envia resultado do pedido de autorização para a SIBS.
4. TPA e SDK recebem o resultado da transação por forma a ser possível a *app* do Banco notificar o Cliente sobre o sucesso da transação.



Figura 4 - Fluxo de compra NFC (experiência cliente ilustrativa)

2.5.3 Compra MB WAY QR Code

A compra com QR Code está disponível para aplicações com sistema operativo Android e iOS. É utilizada em ambientes presenciais quando os terminais da Rede MULTIBANCO têm capacidade para apresentar um QR Code no seu visor.

À semelhança da compra MB WAY *Contactless*, para transações acima de 20€ a autenticação é obrigatória. Esta parametrização deve estar disponível na *app* do Banco para que o Cliente possa ter também a opção de colocar autenticação para operações de valor abaixo dos 20€.

A aplicação do Banco permitirá, através da ativação da câmara do telemóvel, a leitura deste QR Code.

É o SDK que está na *app* do Banco que trata da comunicação entre o TPA MULTIBANCO e a SIBS.

O Cliente abre a *app* do Banco e seleciona a opção de pagar com leitura de QR Code. Com esta leitura, é enviado o pedido de pagamento para a SIBS, que prossegue com o pedido de autorização junto do Banco. A resposta sobre o sucesso do pagamento é enviada para o TPA MULTIBANCO e o Banco deve também notificar o cliente na *app* do Banco em conformidade.

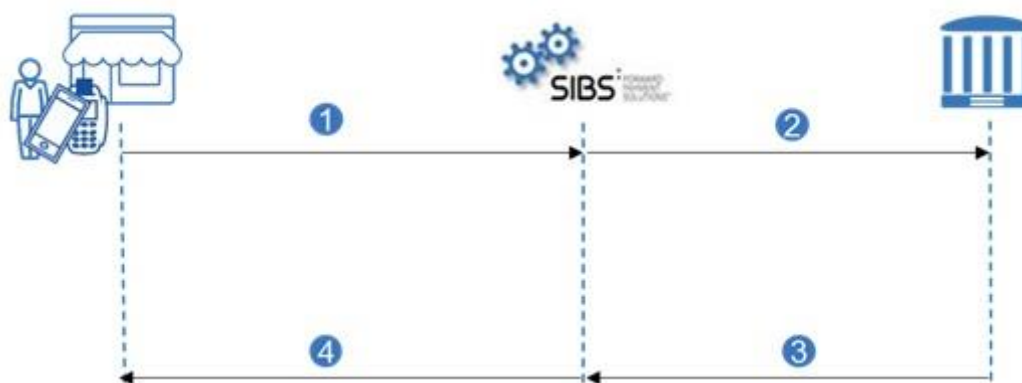


Figura 5 - Fluxo de compra QR Code (não exaustivo)

1. Cliente abre *app* do Banco e lê o QR Code no TPA MULTIBANCO do Comerciante. De acordo com as validações e funções, o SDK vai interagir com a *app* do Banco e, caso seja necessário, é solicitada ao cliente a sua autenticação na *app* do Banco.
2. SIBS recebe comunicação do TPA, bem como confirmação já autenticada da transação do SDK da *app* do Banco e segue com a transação para autorização junto do Banco.
3. Banco processa pedido de autorização e envia resultado do pedido de autorização para a SIBS.

4. TPA e SDK recebem o resultado da transação por forma a ser possível a *app* do Banco notificar o cliente sobre o sucesso da transação.



Figura 6 - Fluxo de compra QR Code (experiência cliente ilustrativa)

3 Implementação do Serviço

3.1 Especificações Técnicas das mensagens *Host-to-Host* e *Real-Time*

3.1.1 Mensagens

No âmbito do Serviço MB a SIBS envia ao Participante mensagens específicas da operação solicitada por um cliente e recebe deste as correspondentes respostas. De igual modo, o Participante pode desencadear mensagens específicas e enviá-las à SIBS, obtendo desta as correspondentes respostas.

Esta iniciativa prevê a inclusão de novas mensagens *Real-Time*, a inserção de uma nova mensagem *Host-to-Host*, bem como evoluções às mensagens *Host-to-Host* já existentes.

3.1.1.1 Mensagens *Real-Time* com Iniciativa na SIBS

- 1161 - Pedido de Operação com Cartão (Emissor)
- 3173 - Notificação de Operação

3.1.1.1.1 1161 - Pedido de Operação com cartão (Emissor) (V00)

Nº	Sigla	Nome	Comp.	Pos.	Rep.	Obs.
Header						
0001	MSG_TIP	Código da mensagem	4	1	A	
0002	MSG_VER	Versão de mensagem	2	5	N	'00'
1709	LOG_SIS	Sistema do <i>log</i> associado à transação (novo código expandido)	2	7	A	
0320	LOG_PERN01	Identificação do período do <i>log</i> central	4	9	N	
0117	LOG_NUMN01	Número de registo <i>log</i> central	8	13	N	
0004	MSG_DTH	Data/hora da transmissão	14	21	N	
0699	SIS_OPRTIP	Código de transação expandido	3	35	A	A)
0233	EXT_MOECOD	Código de moeda	3	38	N	
Dados Terminal Global						
0003	TRM_TIP	Tipo de terminal	1	41	A	
0241	BAN_COD_APO	Código do banco de apoio	4	42	N	
0006	TRM_IDE	Identificação do terminal	10	46	A	
2354	TRM_CAPN01	Capacidades do terminal	1	56	N	
0105	SIS_DTH	Data/hora	14	57	N	
0007	LOC_TRM	Localização/morada do terminal	40	71	A	
0157	SPI_MCCCOD	<i>Merchant category code</i>	4	111	N	
0226	EXT_CTYCOD	Código de país	3	115	N	

Nº	Sigla	Nome	Comp.	Pos.	Rep.	Obs.
Dados Terminal Rede MULTIBANCO						
0068	TRM_IDEPRO	Identificação do proprietário	7	118	N	
0118	TRM_PERNUM	Número do período contabilístico local	3	125	N	
0323	TRM_REGNUM	Número de registo local	5	128	N	
0158	TRM_DICCOD	Distrito e concelho do terminal	4	133	N	
Dados do Cartão						
2324	CAR_PANLGT	Comprimento do PAN	2	137	N	
2325	CAR_PAN	Primary account number	19	139	A	
0126	CAR_EXPDATN02	Data de expiração do cartão	4	158	N	
Dados Adicionais do Cartão						
0119	CAR_MOVNUM	Número de movimento do cartão	2	162	N	
0129	CAR_SEQCOD	Sequência do cartão	1	164	N	
1716	BAN_PDREMV	EMV - aplicação do cartão (padrão EMV)	3	165	N	
8146	TRM_ATTCODA01	Tipo de autenticação	2	168	A	
Dados da Conta						
0132	SAN_NUM	Número da conta (SAN1, SAN2 ou outra)	15	170	N	
Montantes da Operação						
2326	LOG_MOVMNTN01_2	Montante do movimento - 2	11	185	N	
0318	LOG_SINMOV	Sinal	1	196	A	
2327	LOG_ADIMNT	Montante adicional	9	197	N	
0318	LOG_SINMOV	Sinal	1	206	A	
Dados Variáveis						
2336	MSG_DADLGT	Comprimento dos dados variáveis	4	207	N	B)
Total				210		

A) Identifica o tipo de transação realizada. Os valores possíveis deste campo encontram-se identificados na seguinte tabela:

Código de Transação	Descrição	Versões suportadas dos dados variáveis
001	Levantamento	v00 e v01
002	Pedido de Livro de cheques	
005	Alteração de PIN	v00
008	Transferência entre contas do cartão	v00
009	Pagamento serviços/compras	v00
031	Levantamento a crédito	
502	Emissão de cheques	v00
010	Compra MB	v00
013	Autorização Outdoor	

Código de Transação	Descrição	Versões suportadas dos dados variáveis
015	Compras outras vertentes	v00 e v01
018	Autorização Outdoor - outras vertentes	v00
022	Serviço Especial bancário	
023	Serviço Especial não bancário	v00
034	Adiantamento de Dinheiro - MB	
037	Transferência bancária - ordenante	v00
038	Pagamento letra/recibo	v00
039	Adiantamento Dinheiro - outras vertentes	v00
081	Levantamento a crédito - sem vertente MB	
094	Autorização MB NET	v00
0P0	Pagamento serviços/compras - outras marcas	v00
0PA	Pagamento Via Card	
0PC	Carregamento Vodafone	
0PF	Carregamento de Títulos de Transporte	
0PG	Pagamento Sapo ADSL	
0PI	UZO Carregamentos	
0PJ	Carregamentos Rede4	
0PL	Licenciamento Pesca Lúdica	
0PN	Licenciamento de Caça	
0PO	Licenciamento de Pesca em Águas Doces	
0PP	Ser Solidário	
014	Compra Baixo Valor	
0PT	Paysafe Card	
4PF	Confirmação de Carregamento de Título	
179	Transferência P2P Instantânea (Ordenante)	v00
183	Personal Payment and Immediate PaymentTransaction	v00
083	Personal Payment and Immediate Payment Authorisation	v00
012	Autorização Estrangeiro	v00 e v01
017	Autorização outras vertentes	v00 e v01
049	Cancelamento	v00
025	Compra Outdoor - MB	v00

B) Sempre presente. Se não existirem dados variáveis, preencher com '0000'.

3.1.1.1.2 3173 - Notificação de Operação (V01)

Nesta operação procede-se à notificação de uma operação que se encontra pendente de ação por parte do cliente. Nesta interface, o Emissor será notificado das seguintes operações pendentes de aceitação/rejeição:

- '010' – Compras MB (notificada pela 3173 sob o código de operação WOP);
- '013' – Autorizações Outdoor MB (notificada pela 3173 sob o código de operação WOP);
- '199' – Crédito de Transferências P2P (notificada pela 3173 sob o código de operação WOT);
- 'WR1' – Pedido de Envio de Dinheiro (notificada pela 3173 sob o código de operação WOE);
- 'WR2' – Relembrar de Pedido de Envio de Dinheiro (notificada pela 3173 sob o código de operação WOR);
- '001' – Levantamento MB WAY (Notificada pela 3173 sob o código de operação WOL).

Será igualmente enviada a indicação se, no momento de aceitação da operação pendente, deve ser enviado o Token SMS.

Deverá ser escrita no Log com o código de operação WOT (Notificação de Transferência P2P Pendente), com a informação da operação que foi notificada pela MSP ('199'). O objetivo é permitir consultar este registo na execução da transação H036, para informar a MSP na M036 qual o código de operação que está a ser transmitido ('199').

Deverá ser escrita no Log com o código de operação WOP (Notificação de Compra Pendente), com a informação da operação que foi notificada pela MSP ('010' ou '013'). O objetivo é permitir consultar este registo na execução da transação H036, para informar a MSP na M036 qual o código de operação que está a ser transmitido ('010' ou '013'). Nos dados variáveis para a operação WOP, será indicado se a operação se trata de uma '010' – Compra MB, ou uma '013' – Autorização Outdoor MB.

N.º	Sigla do Campo	Nome do Campo	Comp.	Pos.	Rep.	Obs.
Header						
0001	MSG_TIP	Código da Mensagem	4	1	A	
0002	MSG_VER	Versão de Mensagem	2	5	N	'01'
1709	LOG_SIS	Sistema do Log Associado à Transação	2	7	A	
0320	LOG_PERN01	Identificação do Período do Log Central	4	9	N	
0117	LOG_NUMN01	Número de Registo Log Central	8	13	N	
0004	MSG_DTH	Data/hora da Transmissão	14	21	N	
0699	SIS_OPRTIP	Código de Transação Expandido	3	35	A	A)
0233	EXT_MOECOD	Código de Moeda	3	38	N	
Dados da Autorização						
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	41	A	
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	71	N	
8227	COM_SERIDEA01	Identificador do Serviço	40	73	A	
9870	SEE_APLCOD	Código de Aplicação	2	113	N	
0008	TRM_TRNMNTN02	Montante da Transação	13	115	N	

N.º	Sigla do Campo	Nome do Campo	Comp.	Pos.	Rep.	Obs.
9982	TOK_SMSIND	Indicador Token SMS	1	128	N	
10270	SEE_SITOPRA01	Estado da Operação	3	129	A	
Dados Variáveis						
2336	MSG_DADLGT	Comprimento dos Dados Variáveis	4	132	N	B)
Total			Min	135		
			Max			

A) Identifica o tipo de transação realizada. Os valores possíveis deste campo encontram-se identificados na seguinte tabela:

Código de Transação	Descrição	Versões suportadas dos dados variáveis
WOT	Notificação de Transferência P2P Pendente	v00
WOP	Notificação de Compra Pendente	v00
WOE	Notificação de Pedido de Envio de Dinheiro	v00
WOR	Notificação de Relembra de Pedido de Envio de Dinheiro	v00
WOL	Notificação de Levantamento MB WAY	

B) Sempre presente. Se não existirem dados variáveis, preencher com '0000'.

3.1.1.1.3 Dados Variáveis das mensagens de pedido

N.º	Sigla	Nome	Comp.	Rep.	Obs.
(0699) SIS_OPRTIP = '001' (Levantamento) (Dados variáveis presentes na mensagem 1161)					
2337	MSG_VERDAD	Versão dos Dados Variáveis	2	N	'03'
Client Data					
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	
8227	COM_SERIDEA01	Identificador do Serviço	40	A	
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A	
(0699) SIS_OPRTIP = '010' (Compra MB) (Dados variáveis presentes na mensagem 1161)					
2337	MSG_VERDAD	Versão dos Dados Variáveis	2	N	'02'
Client Data					
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	
8227	COM_SERIDEA01	Identificador do Serviço	40	A	
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A	
(0699) SIS_OPRTIP = '013' (Autorização Outdoor MB) (Dados variáveis presentes na mensagem 1161)					
2337	MSG_VERDAD	Versão dos Dados Variáveis	2	N	'01'
Client Data					
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	
8227	COM_SERIDEA01	Identificador do Serviço	40	A	

N.º	Sigla	Nome	Comp.	Rep.	Obs.
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A	
(0699) SIS_OPRTIP = '179' (Transferência P2P Instantânea (Ordenante)) (Dados variáveis presentes na mensagem 1161)					
2337	MSG_VERDAD	Versão dos Dados Variáveis	2	N	'01'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A	
0320	LOG_PERN01	Identificação do Período do Log Central	4	N	
0117	LOG_NUMN01	Número de Registo Log Central	8	N	
8200	EXT_TLMPRX	Prefixo de Telemóvel	7	N	
8106	EXT_TLMNUMN03	Número de Telemóvel	11	N	
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A	
(0699) SIS_OPRTIP = 'WOP' (Notificação de Compra Pendente) (Dados variáveis presentes na mensagem 3173)					
2337	MSG_VERDAD	Versão dos Dados Variáveis	2	N	'00'
0699	SIS_OPRTIP	Código de Transação Expandido	3	A	
8282	COM_ADIOPE	Dados Adicionais da Operação	250	A	
0179	EST_NOM	Nome do Estabelecimento	40	A	
0181	EST_LOC	Local do Estabelecimento	20	A	
(0699) SIS_OPRTIP = 'WOT' (Notificação de Transferência P2P Pendente) (Dados variáveis presentes na mensagem 3173)					
2337	MSG_VERDAD	Versão dos Dados Variáveis	2	N	'00'
8130	SEE_SELTIP	Tipo de Alias	3	N	O), F)
8121	SEE_SELDSG	Designação do Alias	150	A	A), O), F)
8435	SEE_OBSP2P	Observações do P2P	250	A	F)
3390	EXT_IBA	IBAN (International Bank Account Number)	34	A	O)
0137	CLI_NOMA02	Nome do Cliente	27	A	O), F)
(0699) SIS_OPRTIP = 'WOE' (Pedido de Envio de Dinheiro) (Dados variáveis presentes na mensagem 3173)					
2337	MSG_VERDAD	Versão dos Dados Variáveis	2	N	'00'
8130	SEE_SELTIP	Tipo de Alias	3	N	O), F)
8121	SEE_SELDSG	Designação do Alias	150	A	B), O), F)
8435	SEE_OBSP2P	Observações do P2P	250	A	F)
3390	EXT_IBA	IBAN (International Bank Account Number)	34	A	O)
0137	CLI_NOMA02	Nome do Cliente	27	A	O), F)
4464	SIS_DTH_FIM	Data/hora Fim	14	N	
(0699) SIS_OPRTIP = 'WOR' (Relembrar Pedido de Envio de Dinheiro) (Dados variáveis presentes na mensagem 3173)					
2337	MSG_VERDAD	Versão dos Dados Variáveis	2	N	'00'
8130	SEE_SELTIP	Tipo de Alias	3	N	O), F)
8121	SEE_SELDSG	Designação do Alias	150	A	B), O), F)
8435	SEE_OBSP2P	Observações do P2P	250	A	F)

N.º	Sigla	Nome	Comp.	Rep.	Obs.
3390	EXT_IBA	IBAN (International Bank Account Number)	34	A	O)
0137	CLI_NOMA02	Nome do Cliente	27	A	O), F)
4464	SIS_DTH_FIM	Data/hora Fim	14	N	

- A) Quando SEE_SELTIPTIP = '001', este campo contém o número de telemóvel do ordenante da transferência. O número de telemóvel terá a seguinte representação: 00000000#999999999999, em que, '00000000' representa o indicativo, e '999999999999' representa o número de telemóvel. Por exemplo: 0000351#00919191919.
- B) Quando SEE_SELTIPTIP = '001' ou '011', este campo contém o número de telemóvel do ordenante da transferência. O número de telemóvel tem a seguinte representação: 00000000#999999999999 em que, '00000000' representa o indicativo, e '999999999999' representa o número de telemóvel. Por exemplo: 0000351#00919191919.
- F) Campo facultativo.
- O) Dados do Ordenante.

3.1.1.2 Mensagens *Real-Time* com Iniciativa no Participante

- 3273 - Resposta a Notificação de Operação Pendente

3.1.1.2.1 3273 - Resposta a Notificação de Operação Pendente (V01)

N.º	Sigla do Campo	Nome do Campo	Comp.	Pos.	Rep.	Obs.
Header						
0001	MSG_TIP	Código da Mensagem	4	1	A	
0002	MSG_VER	Versão de Mensagem	2	5	N	'01'
1709	LOG_SIS	Sistema do Log Associado à Transação	2	7	A	
0320	LOG_PERN01	Identificação do Período do Log Central	4	9	N	
0117	LOG_NUMN01	Número de Registo Log Central	8	13	N	
Dados da Resposta						
0012	MSG_RESTIPA00	Código de Resposta	1	21	A	
0013	MSG_IDE	Número Identificação da Resposta	14	22	A	
Dados Variáveis						
2336	MSG_DADLGT	Comprimento dos Dados Variáveis	4	36	N	
Total			Min	39		
			Max			

3.1.1.3 Mensagens *Host-to-Host*

- H028 - S028: Pedido Pagamento P2P;
- H029 - S029: Cancelamento Transferência instantânea P2P;
- H035 - S035: Consulta de Estado de Transferência P2P;
- H036 - S036: Confirmação de Operação Financeira;

- H520 – S520: Pedido de Código de Ativação para MB WAY Parceiro;
- H524 - S524: Adesão ao MB WAY;
- H525 - S525: Cancelamento do MB WAY;
- H526 - S526: Associação de Cartão ao MB WAY;
- H527 - S527: Desassociação de Cartão ao MB WAY;
- H532 - S532: Alteração do PIN MB WAY;
- H534 - S534: Alteração de *Alias* de Registo do MB WAY;
- H552 - S552: Geração de Referência para Levantamento MB WAY;
- H553 - S553: Consulta de Referências para Levantamento MB WAY;
- H554 - S554: Cancelamento de referência para Levantamento MB WAY;
- H623 - S623: Pedido de Envio de Dinheiro;
- H624 - S624: Gestão de Pedido de Envio de Dinheiro;
- H625 – S625: Consulta de Pedidos de Envio de Dinheiro.

3.1.1.3.1 H028 - S028: Pedido Pagamento P2P (V03)

Nesta operação são ordenadas Transferências Instantâneas P2P. Esta operação encontra-se sempre disponível para execução pelo cliente. Para a sua correta execução deverão ser recebidos os seguintes dados:

- Comprimento do PAN
- PAN
- Data de Expiração do Cartão
- Montante Transferência Instantânea P2P
- Moeda
- Prefixo de Telemóvel (Indicativo de País) (D) – Destinatário
- Número de Telemóvel (D) – Destinatário
- Código do Tipo de Serviço do Ordenante:
 - 00 – Sem Tipo de Serviço Associado
 - 01 – Tipo de Serviço MB WAY
 - 07 – Tipo de Serviço MB WAY Parceiro
- Identificador do Serviço é obrigatório caso o Código de Tipo de Serviço seja preenchido com '01' ou '07'
- Identificador de Participante Externo é obrigatório caso o Código de Tipo de Serviço seja preenchido com '01' ou '07'
- Código de Aplicação é obrigatório caso o Código de Tipo de Serviço seja preenchido com '07'

Com carácter facultativo podem ainda ser preenchidos os seguintes dados:

- Prefixo de Telemóvel (Indicativo de País) (O) – Ordenante
- Número de Telemóvel (O) – Ordenante
- Dados adicionais

Na resposta a este pedido será retornado o resultado do processamento, que poderá assumir os seguintes estados:

- Aceite
- Pendente de Aceitação
- Pendente de Adesão
- Rejeitado

Será igualmente retornada a chave que identifica a transferência instantânea P2P solicitada.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem Bs	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'03'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
2324	CAR_PANLGT	Comprimento do PAN	2	N	21			M)
5402	CAR_PANA03	Primary Account Number	19	A	23			M)
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	42			M)
8200	EXT_TLMPRX	Prefixo de Telemóvel	7	N	48			F) O)
8106	EXT_TLMNUMN03	Número de Telemóvel	11	N	55			F) O)
0008	TRM_TRNMNTN02	Montante da Transação	13	N	66			M)
0233	EXT_MOECOD	Código de Moeda	3	N	79			M)
8200	EXT_TLMPRX	Prefixo de Telemóvel	7	N	82			D) M)
8106	EXT_TLMNUMN03	Número de Telemóvel	11	N	89			D) M)
8435	SEE_OBSP2P	Observações do P2P	250	A	100			F)
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	350			A)
8227	COM_SERIDEA01	Identificador do Serviço	40	A	352			B)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	392			B)
9870	SEE_APLCOD	Código de Aplicação	2	N	401			C)
8436	SEE_RESCOD	Código do Resultado do Processamento do P2P	2	N		52		
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A		54		
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
Total				Min.	402	83	135	
				Máx.				

- A) Campo a ser preenchido com um dos seguintes valores: 00, 01, 07.
 B) Campo a ser preenchido se SEE_TIPCOD for preenchido com: 01 ou 07.
 C) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.
 D) Dados do Destinatário da Transferência.
 F) Campo facultativo.
 M) Campo obrigatório.
 O) Dados do Ordenante da Transferência.

3.1.1.3.2 H029 - S029: Cancelamento Transferência Instantânea P2P (V02)

Nesta operação são efetuados cancelamentos de Transferência Instantâneas P2P que se encontram Pendentes (Pendentes de Adesão ou Pendentes de Aceitação). O Cancelamento de Transferência Instantâneas P2P deve ser sempre precedido de uma Consulta de Transferências Instantâneas P2P. Sobre as Transferências Instantâneas P2P que se encontrem Pendentes de Adesão ou Pendentes de Aceitação devolvidos na consulta, será possível proceder ao seu cancelamento. Para a sua correta execução deverão ser recebidos os seguintes dados:

- ID de Operação
- Timestamp de Transferência Instantânea P2P
- Comprimento do PAN
- PAN
- Data de Expiração do Cartão
- Montante Transferência Instantânea P2P
- Moeda
- Código do Tipo de Serviço do Ordenante:
 - 00 – Sem Tipo de Serviço Associado
 - 01 – Tipo de Serviço MB WAY
 - 07 – Tipo de Serviço MB WAY Parceiro
- Identificador do Serviço é obrigatório caso o Código de Tipo de Serviço seja preenchido com '01', '03', ou '07'
- Identificador de Participante Externo é obrigatório caso o Código de Tipo de Serviço seja preenchido com '01', '03', ou '07'
- Código de Aplicação é obrigatório caso o Código de Tipo de Serviço seja preenchido com '07'

- Identificação da Mensagem do Banco é obrigatório caso o Código de Tipo de Serviço seja preenchido com '07'

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'02'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A	21			M)
8129	SEE_OPRDAT	Data da Operação no Serviço	14	N	51			M)
2324	CAR_PANLGT	Comprimento do PAN	2	N	65			M)
5402	CAR_PANA03	Primary Account Number	19	A	67			M)
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	86			M)
0008	TRM_TRNMNTN02	Montante da Transação	13	N	92			M)
0233	EXT_MOECOD	Código de Moeda	3	N	105			M)
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	108			A)
8227	COM_SERIDEA01	Identificador do Serviço	40	A	110			B)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	150			B)
9870	SEE_APLCOD	Código de Aplicação	2	N	159			C)
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	161			C)
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
				Total	Min.	174	51	
					Máx.		135	

- A) Campo a ser preenchido com um dos seguintes valores: 00, 01, 03, 07.
- B) Campo a ser preenchido se SEE_TIPCOD for preenchido com: 01, 03, ou 07.
- C) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.
- F) Campo facultativo.
- M) Campo obrigatório.

3.1.1.3.3 H035 - S035: Consulta de Estado de Transferência P2P (V02)

Nesta operação procede-se à consulta do estado em que se encontra uma Transferência P2P. Para a sua correta execução deverão ser preenchidos os seguintes dados:

- Identificação Mensagem do Banco
- Cartão (PAN Length + PAN + Data de expiração)

Ou:

- Código do Tipo de Serviço:
 - 00 – Sem Tipo de Serviço Associado
 - 01 – Tipo de Serviço MB WAY
 - 07 – Tipo de Serviço MB WAY Parceiro
- Identificador do Serviço é obrigatório caso o Código de Tipo de Serviço seja preenchido com '01', '03', ou '07'
- Identificador de Participante Externo é obrigatório caso o Código de Tipo de Serviço seja preenchido com '01', '03', ou '07'
- Código de Aplicação é obrigatório caso o Código de Tipo de Serviço seja preenchido com '07'
- Identificação da Operação no Serviço

Na resposta serão informados a Identificação da Operação no Serviço, assim como o Estado da Transferência P2P.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem Bs	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'02'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	21			F)
2324	CAR_PANLGT	Comprimento do PAN	2	N	35			D)
5402	CAR_PANA03	Primary Account Number	19	A	37			D)
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	56			D)
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	62			A)
8227	COM_SERIDEA01	Identificador do Serviço	40	A	64			B)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	104			B)

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
9870	SEE_APLCOD	Código de Aplicação	2	N	113			C)
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A	115	52		F) E)
8440	SEE_P2PSIT	Situação do Pagamento P2P	2	N		82		
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela Sibs	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
				Total	Min.	144	83	135
					Máx.			

- A) Campo a ser preenchido com um dos seguintes valores: 00, 01, 03, 07.
- B) Campo a ser preenchido se SEE_TIPCOD for preenchido com: 01, 03, ou 07.
- C) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.
- D) Campo obrigatório se campo MSG_IDE_H2H do Body da mensagem for preenchido.
- E) Quando preenchido no *Input* da mensagem, devem ser preenchidos os campos:
- SEE_TIPCOD
- COM_SERIDEA01
- SEE_EPTCOD
- SEE_APLCOD
- F) Campo facultativo.

3.1.1.3.4 H036 - S036: Confirmação de Operação Financeira (V01)

Nesta mensagem procede-se à indicação de que existe uma operação que se encontra pendente e que deve ser aceite ou rejeitada. Para a sua correta execução deverão ser preenchidos os seguintes dados:

- Código do Tipo de Serviço
 - 07 – Tipo de Serviço MB WAY Parceiro
- Identificador do Serviço
- Identificador de Participante Externo
- Código de Aplicação
- Identificação da Operação no Serviço
- Cartão (PAN Length + PAN + Data de expiração)
- SMS Token
- Indicador de Ação (Aceitação/Rejeição)
- Logkey da notificação da operação (enviada na 3173)

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'01'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A	21			M)
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	51			A) M)
8227	COM_SERIDEA01	Identificador do Serviço	40	A	53			M)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	93			M)
9870	SEE_APLCOD	Código de Aplicação	2	N	102			M)
2324	CAR_PANLGT	Comprimento do PAN	2	N	104			M)
5402	CAR_PANA03	Primary Account Number	19	A	106			M)
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	125			M)
9872	SEE_ACCTIPN01	Tipo de Ação a Executar	1	N	131			B) M)
9895	TOK_SMS	Token SMS	7	A	132			F)
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A	139			M)
0320	LOG_PERN01	Identificação do Período do Log Central	4	N	141			M)
0117	LOG_NUMN01	Número de Registo Log Central	8	N	145			M)
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
				Total	Min.	152	51	135
					Máx.			

A) Campo a ser preenchido com o seguinte valor: 07.

B) Campo a ser preenchido para indicar se a operação pendente deve ser Aceite ou Rejeitada:

Aceite: 1

Rejeitada: 0

F) Campo facultativo.

M) Campo obrigatório.

3.1.1.3.5 H520 - S520: Pedido de Código de Ativação para MB WAY Parceiro (V01)

Esta mensagem deve ser utilizada para solicitar à SIBS o código de ativação que é necessário colocar no SDK para este poder ser ativado. Desde que esta mensagem é invocada, existem 120 segundos disponíveis para colocar o código e ativar o SDK. Esta função está disponível apenas para Serviços do Tipo MB WAY Parceiro. Para a sua correta execução deverão ser preenchidos os seguintes dados:

- *Token Alias*;
- Código de Tipo de Serviço;
 - 07 – Tipo de Serviço MB WAY Parceiro;
- Identificador de Participante Externo, que deve ser o número de Comerciante atribuído ao Banco que enviou a mensagem;
- Código de Aplicação.

Na resposta ao Emissor, é devolvido o código de ativação.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'01'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	21			M)
8227	COM_SERIDEA01	Identificador do Serviço	40	A	23			M)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	63			M)
9870	SEE_APLCOD	Código de Aplicação	2	N	72			M)
9974	SEE_ATVCOD_SDK	Código de Ativação do SDK	7	A		52		
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
				Total	Min.	73	58	
					Máx.		135	

M) Campo mandatário.

3.1.1.3.6 H524 - S524: Adesão ao Serviço MB WAY (V04)

Nesta operação são tratados os pedidos de adesão e associação de cartão ao serviço MB WAY. Esta operação encontra-se sempre disponível para execução pelo cliente. Para a sua correta execução deverão ser preenchidos os seguintes dados:

- Código de Tipo de Serviço:
 - 01' – Serviço MB WAY
 - '07' – Serviço MB WAY Parceiro
- N.º Telemóvel (Prefixo + Número de Telemóvel)
- Email – (Facultativo)²
- Limite Diário e respetivo código de moeda (facultativo caso Código de Tipo de Serviço seja preenchido com '07')
- Código Autenticação
- Cartão MB (PAN + Data de expiração)
- Identificador de Participante Externo (obrigatório caso Código de Tipo de Serviço seja preenchido com '07')
- Código de Aplicação (obrigatório caso Código de Tipo de Serviço seja preenchido com '07')

O Código de Autenticação (PIN MB WAY) deve ter 6 dígitos.

O Limite Diário (facultativo caso Código de Tipo de Serviço seja preenchido com '07') não deverá ser sujeito a *Input* do utilizador, devendo ser sempre enviado com valor 50 euros.

A Adesão ao Serviço MB WAY é permitida para cartões que respeitem pelo menos uma das seguintes condições:

- Acesso ao Serviço Especial MB WAY;
- BIN Temporário associado;
- Levantamento MB WAY autorizado;
- Operações com tecnologia NFC autorizada.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'04'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		

² Caso o tipo de serviço seja '07' – Serviço MB WAY Parceiro, o email não é preenchido.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	21			C) M)
8200	EXT_TLMPRX	Prefixo de Telemóvel	7	N	23			M)
8106	EXT_TLMNUMN03	Número de Telemóvel	11	N	30			M)
8121	SEE_SELDSG	Designação do Alias	150	A	41			F)
8135	CHV_HASA01	Secure Hash	64	A	191			A) M)
8119	SEE_MAXLIM	Limite Máximo Diário	7	N	255			B) F)
0233	EXT_MOECOD	Código de Moeda	3	N	262			M)
2324	CAR_PANLGT	Comprimento do PAN	2	N	265			M)
5402	CAR_PANA03	Primary Account Number	19	A	267			M)
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	286			M)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	292			D) M)
9870	SEE_APLCOD	Código de Aplicação	2	N	301			E)
8227	COM_SERIDEA01	Identificador do Serviço	40	A		52		
8226	SEE_NUMCARA01	Numero do Cartão no Serviço	40	A		92		
8195	SEE_SELCD	Código do Alias	10	N		132		
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
				Total	Min. Máx.	302	141	135

- A) Código de Autenticação. Deve ter 6 dígitos. O mesmo deve ser recolhido duas vezes e comparado para garantir que são iguais. Exemplo deste cálculo (valores fictícios):
PIN MB WAY - 926317
Salt do Serviço - F56F4E33789920DA4E77E39A020FC6F2338DFA7EFADC637DF35FE53012937DDA
|| 393236333137F56F4E33789920DA4E77E39A020FC6F2338DFA7EFADC637DF35FE53012937DDA
Secure Hash = SHA256(||) 1D4E16294A432E9A83203081DD00F9E0BB64F47358E11A43AD5662D52E128296
- B) O limite máximo diário é sempre considerado às unidades, ou seja, as duas últimas casas (decimais) são ignoradas.
- C) Campo a ser preenchido com um dos seguintes valores: 01 ou 07.
- D) Campo a ser preenchido se SEE_TIPCOD for preenchido com: 01 ou 07.
- E) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.
- F) Campo facultativo.
- M) Campo obrigatório.

3.1.1.3.7 H525 - S525: Cancelamento do MB WAY (V04)

Nesta operação são tratados os pedidos de cancelamento de Serviços MB WAY. Para a sua correta execução deverão ser preenchidos os seguintes dados:

- Token Alias
- ID do Cartão
- Cartão MB (PAN + Data de expiração)
- Código do Tipo de Serviço:
 - 01 – Tipo de Serviço MB WAY
 - 07 – Tipo de Serviço MB WAY Parceiro
- Identificador do Serviço
- Identificador de Participante Externo
- Código de Aplicação é obrigatório caso o Código de Tipo de Serviço seja preenchido com '07'

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'04'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
8227	COM_SERIDEA01	Identificador do Serviço	40	A	21	52		M)
8226	SEE_NUMCARA01	Numero do Cartão no Serviço	40	A	61			F)
2324	CAR_PANLGT	Comprimento do PAN	2	N	101			M)
5402	CAR_PANA03	Primary Account Number	19	A	103			M)
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	122			M)
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	128			A) M)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	130			B)
9870	SEE_APLCOD	Código de Aplicação	2	N	139			C)
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
Total					Min. Máx.	140 91	135 135	

- A) Campo a ser preenchido com um dos seguintes valores: 01 ou 07.
B) Campo a ser preenchido se SEE_TIPCOD for preenchido com: 01 ou 07.
C) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.
F) Campo facultativo.
M) Campo obrigatório.

3.1.1.3.8 H527 - S527: Desassociação de Cartão ao MB WAY (V04)

Nesta operação são tratados os pedidos de desassociação de um cartão de um determinado Serviço MB WAY. Esta operação permitirá que se desassocie apenas cartões emitidos pelo Banco. Para a sua correta execução deverão ser preenchidos os seguintes dados:

- Código de Tipo de Serviço
 - 01 – Tipo de Serviço MB WAY
 - 07 – Tipo de Serviço MB WAY Parceiro
- Cartão MB (PAN + Data de expiração)
- Identificador do Serviço
- Identificador de Participante Externo
- Código de Aplicação é obrigatório caso o Código de Tipo de Serviço seja preenchido com '07'

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'04'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
8227	COM_SERIDEA01	Identificador do Serviço	40	A	21	52		M)
8226	SEE_NUMCARA01	Numero do Cartão no Serviço	40	A	61	92		F)
2324	CAR_PANLGT	Comprimento do PAN	2	N	101			M)
5402	CAR_PANA03	Primary Account Number	19	A	103			M)
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	122			M)
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	128			A)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	130			B)
9870	SEE_APLCOD	Código de Aplicação	2	N	139			C)

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
				Total	Min. Máx.	140	131	135

- A) Campo a ser preenchido com um dos seguintes valores: 01 ou 07.
 B) Campo a ser preenchido se SEE_TIPCOD for preenchido com: 01 ou 07.
 C) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.
 F) Campo facultativo.
 M) Campo obrigatório.

3.1.1.3.9 H532 - S532: Alteração do PIN MB WAY (V04)

Nesta operação são tratados os pedidos de alteração do PIN MB WAY. Para a sua correta execução deverão ser preenchidos os seguintes dados:

- Código Autenticação
- Código de Tipo de Serviço
 - 01 – Tipo de Serviço MB WAY
 - 07 – Tipo de Serviço MB WAY Parceiro
- Cartão MB (PAN + Data de expiração)
- Identificador do Serviço
- Identificador de Participante Externo
- Código de Aplicação é obrigatório caso o Código de Tipo de Serviço seja preenchido com '07'

O Código de Autenticação (PIN MB WAY) deve ter 6 dígitos.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'04'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Detalhe								
8227	COM_SERIDEA01	Identificador do Serviço	40	A	21	52		M)
8226	SEE_NUMCARA01	Numero do Cartão no Serviço	40	A	61			F)
8135	CHV_HASA01	Secure Hash	64	A	101			A) M)
2324	CAR_PANLGT	Comprimento do PAN	2	N	165			M)
5402	CAR_PANA03	Primary Account Number	19	A	167			M)
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	186			M)
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	192			B)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	194			C)
9870	SEE_APLCOD	Código de Aplicação	2	N	203			D)
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
				Total	Min.	204	91	135
					Máx.			

- A) PIN MB WAY. Deve ter 6 dígitos. O mesmo deve ser recolhido duas vezes e comparado para garantir que são iguais.
Exemplo deste cálculo (valores fictícios):
PIN MB WAY - 926317
Salt do Serviço - F56F4E33789920DA4E77E39A020FC6F2338DFA7EFADC637DF35FE53012937DDA
|| 393236333137F56F4E33789920DA4E77E39A020FC6F2338DFA7EFADC637DF35FE53012937DDA
Secure Hash = SHA256(||) 1D4E16294A432E9A83203081DD00F9E0BB64F47358E11A43AD5662D52E128296
- B) Campo a ser preenchido com um dos seguintes valores: 01 ou 07.
- C) Campo a ser preenchido se SEE_TIPCOD for preenchido com: 01 ou 07.
- D) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.
- F) Campo facultativo.
- M) Campo obrigatório.

3.1.1.3.10 H534 - S534: Alteração de Alias de Registo do Serviço MB WAY (V03)

Nesta operação procede-se à alteração do *alias* de registo do MB WAY. O *alias* de registo é sempre um número de telemóvel. O número de telemóvel pretendido deve ter até 7 dígitos de indicativo telefónico internacional (prefixo) e 11 dígitos de número de telemóvel, e não pode ter o serviço MB WAY já associado. Os primeiros 2 dígitos do número de telemóvel devem ser: 91, ou 92, ou 93, ou 96.

Para a sua correta execução devem ser preenchidos os seguintes dados:

- *Token alias*;
- ID do cartão;
- Número de telemóvel pretendido (prefixo + número telemóvel).

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'03'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
8227	COM_SERIDEA01	Identificador do Serviço	40	A	21	52		M)
8226	SEE_NUMCARA01	Numero do Cartão no Serviço	40	A	61			F)
8200	EXT_TLMPRX	Prefixo de Telemóvel	7	N	101			M)
8106	EXT_TLMNUMN03	Número de Telemóvel	11	N	108			M)
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	119			A)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	121			B)
9870	SEE_APLCOD	Código de Aplicação	2	N	130			C)
8195	SEE_SELCOD	Código do Alias	10	N		92		
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
				Total	Min.	131	101	135
					Máx.			

- A) Campo a ser preenchido com um dos seguintes valores: 01 ou 07.
 B) Campo a ser preenchido se SEE_TIPCOD for preenchido com: 01 ou 07.
 C) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.
 F) Campo facultativo.
 M) Campo obrigatório.

3.1.1.3.11 H552 - S552: Pedido de Referência para Levantamento MB WAY (V02)

Esta operação permite a geração de uma referência que possibilita o Levantamento MB WAY. Os seguintes campos são obrigatórios apenas se o Código de Tipo de Serviço for igual a 07 – MB WAY Parceiro:

- Identificador de Participante Externo (obrigatório caso o Código de Tipo de Serviço seja preenchido com '07');
- Código de Aplicação (obrigatório caso o Código de Tipo de Serviço seja preenchido com '07').

Todos os restantes campos de *Input* são de preenchimento obrigatório. Na resposta (S552), a SIBS FPS envia a referência que permite o Levantamento MB WAY.

No caso de o Código de Tipo de Serviço ser igual a 01 – MB WAY, antes de enviar a mensagem H552, o Emissor deve enviar a mensagem H537. Na resposta (S537), a SIBS FPS indica o identificador de serviço associado a um cartão bancário. Com esta informação, o Emissor pode preencher os campos de *Input* da mensagem H552.

De forma a garantir a confidencialidade desta referência, é gerada uma chave secreta (dinâmica) entre a SIBS FPS e o Emissor através de uma variante do algoritmo *Diffie-Hellman* baseada na norma ANSI X9.42, que também pressupõe uma troca de informação (Anexo A). Com essa finalidade, no pedido deve ser preenchido o atributo (9156) CHV_SPKA01 “SIBS *Public Key*” e, na resposta, serão devolvidos os atributos (9156) CHV_SPKA01 “SIBS *Public Key*”, (9157) CHV_INIVTR “Vetor de Inicialização”, e (9158) CHV_REFLSC “Referência de Levantamento sem cartão”.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'02'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	21			A)
8227	COM_SERIDEA01	Identificador do Serviço	40	A	23			M)
8130	SEE_SELTIPT	Tipo de Alias	3	N	63			M)
8121	SEE_SELDSEG	Designação do Alias	150	A	66			M)
2324	CAR_PANLGT	Comprimento do PAN	2	N	216			M)
5402	CAR_PANA03	Primary Account Number	19	A	218			M)
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	237			M)
9116	SEE_MNTLSC	Montante de Levantamento Sem Cartão	5	N	243			M)
0233	EXT_MOECOD	Código de Moeda	3	N	248			M)
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A		52		
9157	CHV_INIVTR	Vetor de Inicialização	32	A		82		
9156	CHV_SPKA01	SIBS Public Key	512	A	251	114		M)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	763			B)
9870	SEE_APLCOD	Código de Aplicação	2	N	772			C)

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
9158	CHV_REFLSC	Referência de Levantamento Sem Cartão	32	A		626		
9164	SEE_DURSGN	Duração em Segundos	9	N		658		
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
				Total	Min.	773	666	135
					Máx.			

- A) Campo a ser preenchido com um dos seguintes valores: 01 ou 07.
 B) Campo a ser preenchido se SEE_TIPCOD for preenchido com: 01 ou 07.
 C) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.
 M) Campo obrigatório.

3.1.1.3.12 H553 - S553: Consulta de Referências para Levantamento MB WAY (V03)

Esta operação permite a consulta de referências para Levantamento MB WAY. Os seguintes campos são obrigatórios apenas se o Código de Tipo de Serviço for igual a 07 – MB WAY Parceiro:

- Identificador de Participante Externo (obrigatório caso o Código de Tipo de Serviço seja preenchido com '07');
- Código de Aplicação (obrigatório caso o Código de Tipo de Serviço seja preenchido com '07').

Todos os restantes campos de *Input* são de preenchimento obrigatório. Na resposta (S553), a SIBS FPS envia todas as referências que possibilitam efetuar uma operação de Levantamento MB WAY associadas a cartões emitidos por esse Banco.

No caso de o Código de Tipo de Serviço ser igual a 01 – MB WAY, antes de enviar a mensagem H553, o Emissor deve enviar a mensagem H537: Consulta de *Alias* de Registo. Na resposta (S537), a SIBS FPS indica o identificador de serviço associado a um cartão bancário. Com esta informação, o Emissor pode preencher os campos de *Input* da mensagem H553: Consulta de Referências para Levantamento MB WAY.

As referências que se encontrem expiradas são transmitidas com uma máscara em que são visíveis apenas os 4 algarismos de menos expressão (ex.: *****1234).

De forma a garantir a confidencialidade das referências, é gerada uma chave secreta (dinâmica) entre a SIBS FPS e o Emissor através de uma variante do algoritmo *Diffie-Helman* baseada na norma ANSI X9.42, que também pressupõe uma troca de informação (Ver Anexo A). Com essa finalidade, no pedido deve ser preenchido o atributo (9156) CHV_SPKA01 "SIBS *Public Key*" e, na resposta, serão devolvidos os atributos (9156) CHV_SPKA01 "SIBS *Public Key*", (9157) CHV_INIVTR "Vetor de Inicialização", e (9158) CHV_REFLSC "Referência de Levantamento sem cartão". O atributo (8128) SEE_IDEOPR "Identificação da Operação no Serviço" deve ser contemplado para paginação.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'03'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	21			B)
8227	COM_SERIDEA01	Identificador do Serviço	40	A	23			M)
9157	CHV_INIVTR	Vetor de Inicialização	32	A		52		
9156	CHV_SPKA01	SIBS Public Key	512	A	63	84		M)
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A	575			P)
1002	MSG_OPETIP	Código Operador	1	A	605			P)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	606			C)
9870	SEE_APLCOD	Código de Aplicação	2	N	615			D)
0428	MSG_OCONUM	Número de Ocorrências	2	N		596		A)
8128	SEE_IDEOPR *	Identificação da Operação no Serviço	30	A		598		E)
8130	SEE_SELTIP *	Tipo de Alias	3	N		628		E)
8121	SEE_SELDSG *	Designação do Alias	150	A		631		E)
8130	SEE_SELTIP *	Tipo de Alias	3	N		781		E)
8121	SEE_SELDSG *	Designação do Alias	150	A		784		E)
2324	CAR_PANLGT *	Comprimento do PAN	2	N		934		E)
5402	CAR_PANA03 *	Primary Account Number	19	A		936		E)
0637	CAR_EXPDAT *	Data de Expiração do Cartão Expandida	6	N		955		E)
9116	SEE_MNTLSC *	Montante de Levantamento Sem Cartão	5	N		961		E)
0233	EXT_MOECOD *	Código de Moeda	3	N		966		E)
9158	CHV_REFLSC *	Referência de Levantamento Sem Cartão	32	A		969		E)
9164	SEE_DURSGN *	Duração em Segundos	9	N		1001		E)
9163	SEE_SITLSC_REF *	Situação da Referência de Levantamento Sem Cartão MB WAY	3	N		1010		E)
2247	SIS_ACTDTH *	Data-hora de Atualização	14	N		1013		E)
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
Total				Min.	616	597	135	
				Máx.		1884		

- A) Valores entre 00 e 03.
 B) Campo a ser preenchido com um dos seguintes valores: 01 ou 07.
 C) Campo a ser preenchido se SEE_TIPCOD for preenchido com: 01 ou 07.
 D) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.
 E) Pode ocorrer de 0 a 3 vezes.
 M) Campo obrigatório.
 P) Campo usado para efetuar paginação de resultados.

3.1.1.3.13 H554 - S554: Cancelamento de Referência para Levantamento MB WAY (V02)

Esta operação permite o cancelamento de uma referência para Levantamento MB WAY. Através da mensagem H554 – S554, o Emissor envia à SIBS FPS um Identificador de Operação, o qual obteve a partir da mensagem H553 – S553: Consulta de Referências para Levantamento MB WAY. Na resposta, a SIBS FPS efetua o cancelamento da referência que está associada ao Identificador de Operação.

As referências só podem ser alvo de cancelamento se o seu estado for '000' – Ativa.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'02'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A	21			M)
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	51			A)
8227	COM_SERIDEA01	Identificador do Serviço	40	A	53			M)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	93			B)
9870	SEE_APLCOD	Código de Aplicação	2	N	102			C)

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
				Total	Min. Máx.	103	51	135

- A) Campo a ser preenchido com um dos seguintes valores: 01 ou 07.
 B) Campo a ser preenchido se SEE_TIPCOD for preenchido com: 01 ou 07.
 C) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.
 M) Campo obrigatório.

3.1.1.3.14 H623 - S623: Pedido de Envio de Dinheiro (V01)

Nesta operação são ordenados Pedidos de Envio de Dinheiro. Para a sua correta execução devem ser recebidos os seguintes dados:

- Código do Tipo de Serviço do Ordenante:
 - 01 – Tipo de Serviço MB WAY;
 - 07 – Tipo de Serviço MB WAY Parceiro.
- Identificador do Serviço;
- Identificador de Participante Externo;
- Código de Aplicação é obrigatório caso o Código de Tipo de Serviço seja preenchido com '07';
- Tipo de Alias do Ordenante:
 - '001' no caso do Código do Tipo de Serviço for igual a '01';
 - '011' no caso do Código do Tipo de Serviço for igual a '07'.
- Designação do Alias do Ordenante;
- Comprimento do PAN;
- PAN;
- Data de Expiração do Cartão;
- Prefixo de Telemóvel (Indicativo de País) (D) – Destinatário do Pedido;
- Número de Telemóvel (D) – Destinatário do Pedido;
- Montante Transferência Instantânea P2P;
- Moeda.

Com carácter facultativo podem ainda ser preenchidos os seguintes dados:

- Dados adicionais.

Na resposta a este pedido serão retornados os seguintes dados:

- Identificador da Operação no Serviço – Este campo funciona como chave do Pedido de Envio de Dinheiro;
- Data/Hora Fim do Pedido – Será dada a indicação em formato AAAAMMDDHHMMSS da validade do Pedido de Envio de Dinheiro.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'01'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	21			A), M)
8227	COM_SERIDEA01	Identificador do Serviço	40	A	23			M)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	63			M)
9870	SEE_APLCOD	Código de Aplicação	2	N	72			B)
8130	SEE_SELTIPT	Tipo de Alias	3	N	74			M)
8121	SEE_SELDSEG	Designação do Alias	150	A	77			M)
2324	CAR_PANLGT	Comprimento do PAN	2	N	227			M)
5402	CAR_PANA03	Primary Account Number	19	A	229			M)
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	248			M)
8200	EXT_TLMPRX	Prefixo de Telemóvel	7	N	254			C), M)
8106	EXT_TLMNUMN03	Número de Telemóvel	11	N	261			C), M)
0008	TRM_TRNMNTN02	Montante da Transação	13	N	272			M)
0233	EXT_MOECOD	Código de Moeda	3	N	285			M)
8435	SEE_OBSP2P	Observações do P2p	250	A	288			F)
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A		52		
4464	SIS_DTH_FIM	Data/hora Fim	14	N		82		
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Total				Min.	537	95	135	
				Máx.				

- A) Campo a ser preenchido com um dos seguintes valores: 01 ou 07.
 B) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.
 C) Dados do Destinatário do Pedido.
 F) Campo facultativo.
 M) Campo obrigatório.

3.1.1.3.15 H624 - S624: Gestão de Pedido de Envio de Dinheiro (V01)

Nesta interface podem ser ordenados:

- Cancelamento de Pedidos de Envio de Dinheiro;
- Relembrar Pedidos de Envio de Dinheiro.

O Cancelamento de Pedidos de Envio de Dinheiro pode ser solicitado apenas pelo Ordenante do Pedido de Envio de Dinheiro e, somente, se o Pedido se encontrar no estado 'Pendente'.

O Relembrar do Pedido de Envio de Dinheiro pode ser solicitado apenas pelo Ordenante do Pedido de Envio de Dinheiro e, somente, se o Pedido se encontrar no estado 'Pendente'. Só pode ser efetuado um Relembrar Pedido de Envio de Dinheiro por dia.

Para a sua correta execução devem ser recebidos os seguintes dados:

- Código de Ação:
 - 'C' - Cancelamento de Pedidos de Envio de Dinheiro;
 - 'R' - Relembrar Pedidos de Envio de Dinheiro.
- Identificador da Operação no Serviço;
- Código do Tipo de Serviço do Ordenante:
 - 01 – Tipo de Serviço MB WAY;
 - 07 – Tipo de Serviço MB WAY Parceiro.
- Identificador do Serviço;
- Identificador de Participante Externo;
- Código de Aplicação é obrigatório caso o Código de Tipo de Serviço seja preenchido com '07';
- Comprimento do PAN;
- PAN;
- Data de Expiração do Cartão.

Na resposta a este pedido é retornado um status indicando se a operação foi finalizada com sucesso ou não.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'01'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
2483	MSG_ACCCOD	Código de Gestão da Mensagem	1	A	21			C), M)
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A	22			M)
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	52			A), M)
8227	COM_SERIDEA01	Identificador do Serviço	40	A	54			M)
9868	SEE_EPTCOD	Código de Participante Externo	9	N	94			M)
9870	SEE_APLCOD	Código de Aplicação	2	N	103			B)
2324	CAR_PANLGT	Comprimento do PAN	2	N	105			M)
5402	CAR_PANA03	Primary Account Number	19	A	107			M)
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N	126			M)
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
				Total	Min. Máx.	131	51	135

A) Campo a ser preenchido com um dos seguintes valores: 01 ou 07.

B) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.

C) Preencher com:

- C - Cancelamento de Pedido de Envio de Dinheiro;
- R – Relembrar Pedido de Envio de Dinheiro.

M) Campo obrigatório.

3.1.1.3.16 H625 - S625: Consulta de Pedidos de Envio de Dinheiro (V01)

Nesta operação são ordenadas Consultas de Pedidos de Envio de Dinheiro. Para a sua correta execução devem ser recebidos os seguintes dados:

- Código do Tipo de Serviço do Ordenante:
 - 01 – Tipo de Serviço MB WAY;
 - 07 – Tipo de Serviço MB WAY Parceiro.
- Identificador do Serviço;
- Identificador de Participante Externo;
 - Código de Comerciante do Banco caso o Código de Tipo de Serviço seja igual a '07';
 - Não deve ser validado caso o Código de Tipo de Serviço seja igual a '01'.
- Código de Aplicação:
 - Obrigatório ser superior a zeros caso o Código de Tipo de Serviço seja preenchido com '07';
 - Preenchido com zeros caso o Código de Tipo de Serviço seja preenchido com '01'.
- Código de Operador (a ordem será sempre aplicada sobre o Identificador da Operação no Serviço, e Identificador do Interveniente na Operação):
 - '>' – para obter a página seguinte;
 - '<' – para obter a página anterior;
 - '=' – para obter o registo correspondente à chave colocada no campo de paginação.
- Número de ocorrências pretendidas (entre 1 e 10);

Com carácter facultativo podem ainda ser preenchidos os seguintes dados:

- Identificador da Operação no Serviço + Identificador do Interveniente na Operação:
 - Quando se pretende a primeira página de consulta, estes campos devem ser preenchidos a espaços, e o Código de Operador deve ser preenchido com '>';
 - Quando se pretende uma página seguinte, estes campos devem ser preenchidos com o Identificador da Operação no Serviço e Identificador do Interveniente na Operação do último registo da página de resultados em que se encontra, e o Código de Operador deve ser preenchido com '>';
 - Quando se pretende uma página anterior, estes campos devem ser preenchidos com o Identificador da Operação no Serviço e Identificador do Interveniente na Operação do primeiro registo da página de resultados em que se encontra, e o Código de Operador deve ser preenchido com '<';
 - Quando se pretende obter os dados de um Pedido de Envio de Dinheiro em específico, este campo deve ser preenchido com o Identificador da Operação no Serviço correspondente, o Identificador do Interveniente na Operação deve ser preenchido com zeros, e o Código de Operador deve ser preenchido com '='. Nestes casos, é possível que sejam devolvidos dois registos. Isto pode acontecer para um Pedido de Envio de Dinheiro em que o Autor do Pedido e o Recetor do Pedido são o mesmo Identificador do Serviço. Estes dois registos vão coincidir

no Identificador da Operação no serviço, mas será possível distinguir ambos pelo Identificador do Interveniente na Operação.

Na resposta a este pedido são retornados os seguintes dados:

- Identificador da Operação no Serviço – Este campo funciona como chave do Pedido de Envio de Dinheiro juntamente com o Identificador do Interveniente na Operação;
- Identificador do Interveniente na Operação – Este campo funciona como chave do Pedido de Envio de Dinheiro juntamente com o Identificador da Operação no Serviço;
- Tipo de Intervenção no Pedido de Envio de Dinheiro:
 - Ordenante;
 - Destinatário.
- Cartão Bancário:
 - Comprimento do PAN;
 - PAN;
 - Data de Expiração.
- Telemóvel do Ordenante;
- Montante do Pedido;
- Telemóvel do Destinatário;
- Data/Hora Início do Pedido – É dada a indicação em formato AAAAMMDDHHMMSS em que o Pedido foi efetuado;
- Data/Hora Fim do Pedido – É dada a indicação em formato AAAAMMDDHHMMSS da validade do Pedido de Envio de Dinheiro;
- Data/Hora Atualização do Pedido – É dada a indicação em formato AAAAMMDDHHMMSS em que o Pedido foi Aceite/Rejeitado pelo Destinatário do Pedido. Se o Pedido estiver no estado 'Pendente', esta data/hora é igual à data/hora Início do Pedido.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'01'
0471	MSG_IDE_H2H	Identificação Mensagem do Banco	14	A	7	7	7	
0004	MSG_DTH	Data/hora da Transmissão	14	N		21	21	
0492	MSG_RESCOD	Código de Resposta da Mensagem da SIBS	3	N		35	35	
1709	LOG_SIS	Sistema do Log Associado à Transação	2	A		38		
0320	LOG_PERN01	Identificação do Período do Log Central	4	N		40		
0117	LOG_NUMN01	Número de Registo Log Central	8	N		44		
Detalhe								
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	21			A), M)
8227	COM_SERIDEA01	Identificador do Serviço	40	A	23			M)

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
9868	SEE_EPTCOD	Código de Participante Externo	9	N	63			M)
9870	SEE_APLCOD	Código de Aplicação	2	N	72			B)
8128	SEE_IDEOPR	identificação da Operação no Serviço	30	A	74			P)
10308	SEE_IDEOPR_NTV	Identificação de Interveniente na Operação	30	A	104			P)
1002	MSG_OPETIP	Código Operador	1	A	134			
8192	MSG_OCOIND	Indicador de Ocorrências	1	N		52		
0428	MSG_OCONUM	Número de Ocorrências	2	N	135	53		
8128	SEE_IDEOPR *	Identificação da Operação no Serviço	30	A		55		C)
10308	SEE_IDEOPR_NTV *	Identificação de Interveniente na Operação	30	A		85		C)
10213	SEE_RQMTIP *	Tipo de Interveniente no Request Money	1	A		115		C)
2324	CAR_PANLGT *	Comprimento do PAN	2	N		116		C)
5402	CAR_PANA03 *	Primary Account Number	19	A		118		C)
0637	CAR_EXPDAT *	Data de Expiração do Cartão Expandida	6	N		137		C)
8200	EXT_TLMPRX *	Prefixo de Telemóvel	7	N		143		C), O)
8106	EXT_TLMNUMN03 *	Número de Telemóvel	11	N		150		C), O)
0008	TRM_TRNMNTN02 *	Montante da Transação	13	N		161		C)
0233	EXT_MOECOD *	Código de Moeda	3	N		174		C)
8200	EXT_TLMPRX *	Prefixo de Telemóvel	7	N		177		C), D)
8106	EXT_TLMNUMN03 *	Número de Telemóvel	11	N		184		C), D)
4463	SIS_DTH_INI *	Data/hora Início	14	N		195		C)
4464	SIS_DTH_FIM *	Data/hora Fim	14	N		209		C)
2247	SIS_ACTDTH *	Data-hora De Atualização	14	N		223		C)
8440	SEE_P2PSIT *	Situação do Pagamento P2P	2	N		237		C)
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem Pela SIBS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
				Total	Min.	54	135	
					Máx.	1894		

- A) Campo a ser preenchido com um dos seguintes valores: 01 ou 07.
- B) Campo a ser preenchido se SEE_TIPCOD for preenchido com 07.
- C) Pode ocorrer de 0 a 10 vezes.
- D) Dados do Destinatário do Pedido de Envio de Dinheiro.
- M) Campo obrigatório.
- O) Dados do Ordenante do Pedido de Envio de Dinheiro.
- P) Campo de paginação de resultados da consulta em lista.

3.2 Especificações SDK

A especificação funcional do SDK MB WAY, daqui em diante referido apenas por SDK, define as interfaces e os comportamentos do SDK, para realizar operações MB WAY³. O SDK pretende ser integrado numa aplicação de pagamento móvel de um Banco, também designado como Parceiro.

3.2.1 Pressupostos

Serão disponibilizados ao parceiro integrador do SDK uma biblioteca *aar* para integração com aplicações Android e uma *framework* para integração com aplicações iOS.

A biblioteca *aar* está desenvolvida na linguagem nativa de Android (Java) e a *framework* segue a linguagem Objective-C.

O SDK utiliza as seguintes permissões:

- Permissões de acesso a geolocalização (dados recolhidos pelo SDK)
 - *Coarse Location*
 - *Fine Location*
- Permissões de escrita e leitura em ficheiro
- Permissão de acesso à Internet
- Permissão de acesso ao estado da rede
- Permissão de acesso ao estado do WI-FI
- Permissão de acesso a vibração
- Permissão de acesso NFC
- Permissão de acesso à Câmara

Para disponibilização do SDK, o parceiro deverá contactar previamente a SIBS, para requerer a atribuição de:

- Código de Participante
- Código de Aplicação

Para disponibilização do SDK o banco deverá enviar à SIBS a seguinte informação:

- Imagem para seleção de *app default* para compras *Contactless (apdubanner)* nos tamanhos:
 - mdpi-260x96
 - hdpi-340x144
 - xhdpi-520x192
 - xxhdpi-780x288
- Imagem para notificações locais emitidas pelo SDK
 - mdpi-48x48

³ As operações MB WAY suportadas pelo SDK nesta fase são: Compras MB WAY (Compra e Autorização).

- hdpi-72x72
- xhdpi-96x96
- xxhdpi-144x144
- xxxhdpi-192x192
- Mensagens de notificações locais

Tabela 3 - Mensagens notificações locais

Propriedade	Texto exemplo
info_start_payment_message	Insira o PIN MB WAY para confirmar a compra de @(amount)@.
info_finish_payment_message	Compra no valor de @(amount)@. Verifique sucesso da transação no terminal.
info_max_limit_exceed_insert_pin_message	Insira PIN MB WAY para confirmar a compra de @(amount)@.
info_apdu_deactivated_link_loss	A sua operação não foi realizada. Encoste novamente.
info_apdu_deactivated_deselected	Utilizador escolheu outra aplicação para pagamento.
request_connectivity_and_pin_to_continue_transaction_message	Antes do próximo pagamento contactless MB WAY
doesnt_have_default_card_for_payments_contactless	Não tem cartão predefinido para compras. Abra a <i>app</i> e utilize a opção Pagar com MB WAY.
doesnt_have_cards_with_payment_contactless	Não é possível realizar a operação. Nenhum dos seus cartões permite pagar contactless.
info_device_rooted	O sistema não se encontra seguro para proceder ao pagamento contactless através da aplicação.
info_screen_locked_payment_denied	Desbloqueie o ecrã para proceder ao pagamento.
info_common_error	Neste momento não é possível realizar a sua operação. Tente novamente.
info_payments_disabled	Ligue a opção de pagar contactless na <i>app</i> MB WAY.
info_pos_doesnt_support_contactlessmbway	Possivelmente o terminal ainda não suporta contactless MB WAY.

3.2.2 Integração para Android

3.2.2.1 Interfaces do SDK Android

Esta secção define todas as interfaces que estão disponíveis para integração do SDK Android.

Tabela 4 - Lista de Operações Suportadas pelo SDK Android

Interface	Descrição	Origem	Destino
init	Inicialização de parâmetros de aplicação sempre que a <i>app</i> do parceiro é aberta	<i>App</i> Parceiro	SDK
searchPendingOperations	Este serviço retorna todas as operações de compras que ele tem pendentes de ação	<i>App</i> Parceiro	SDK
confirmFinancialOperation	Confirmação de uma compra pelo utilizador na <i>app</i>	<i>App</i> Parceiro	SDK
rejectFinancialOperation	Rejeição de compras pelo utilizador na <i>app</i>	<i>App</i> Parceiro	SDK
getStatus	Função para pedir informação sobre o SDK: <ul style="list-style-type: none"> Estado SDK Estado Funcionalidade Pagamentos MB WAY Contactless Estado Funcionalidade Pagamentos MB WAY Contactless com ecrã bloqueado Estado da obrigatoriedade de autenticação em todas as operações com PIN MB WAY 	<i>App</i> Parceiro	SDK
selectCardforContactlessPayment	Função para selecionar um cartão como default para Pagamentos MB WAY Contactless	<i>App</i> Parceiro	SDK
configContactlessPayments	Função para: <ul style="list-style-type: none"> Ativar/desativar Pagamentos MB WAY Contactless Ativar/desativar os Pagamentos com o ecrã bloqueado Obrigatoriedade de autenticação em todas as operações com PIN MB WAY 	<i>App</i> Parceiro	SDK
getContactlessProvisionedCards	Função para informar à <i>app</i> Parceiro a lista de cartões aprovisionados para Pagamentos MB WAY Contactless.	<i>App</i> Parceiro	SDK
setPINMBWAY	Função para fornecer o PIN MB WAY ao SDK. Deve ser usada após o <i>Callback_request_pin</i>	<i>App</i> Parceiro	SDK
registerQRCodePayment	Registo de um pedido de pagamento QRCode	<i>App</i> Parceiro	SDK

Tabela 5 - Lista de Listeners utilizados pelo SDK Android

Listener	Descrição	Origem	Destino
MBWAYSdkInitListener <ul style="list-style-type: none"> onInitResult 	<i>Callback</i> de retorno que informa a <i>app</i> parceiro com o resultado do estado da inicialização do SDK	SDK	<i>App</i> Parceiro
MBWAYSdkPendingOperationsListener <ul style="list-style-type: none"> onPendingOperationResult 	<i>Callback</i> de retorno que passa à <i>app</i> parceiro a listagem de operações pendentes	SDK	<i>App</i> Parceiro
MBWAYSdkOperationListener <ul style="list-style-type: none"> onOperationResult 	<i>Callback</i> de retorno que informa a <i>app</i> parceiro com o resultado da operação que acabou de realizar	SDK	<i>App</i> Parceiro
MBWAYSdkSetCardForContactlessPaymentListener <ul style="list-style-type: none"> onSetCardForContactlessPaymentResult 	<i>Callback</i> utilizado pelo SDK para informar a <i>app</i> Parceiro com o resultado da seleção de um cartão para pagamentos MB WAY Contactless	SDK	<i>App</i> Parceiro

<i>Listener</i>	<i>Descrição</i>	<i>Origem</i>	<i>Destino</i>
MBWAYSdkGetStatusListener <ul style="list-style-type: none"> onGetStatusResult 	Callback utilizado pelo SDK para informar a <i>app</i> Parceiro com o resultado da consulta de estado	SDK	App Parceiro
MBWAYSdkGetProvisionedCards <ul style="list-style-type: none"> onGetProvisionedCardsResult 	Callback utilizado pelo SDK para informar a <i>app</i> Parceiro com o resultado da consulta de cartões aprovacionados	SDK	App Parceiro
MBWAYSdkContactlessPaymentListener <ul style="list-style-type: none"> onReceivedInformation getCardforPayment 	Callback utilizado pelo SDK para informar a <i>app</i> Parceiro com informações de um Pagamento MB WAY Contactless	SDK	App Parceiro
MBWAYSdkQRCodePaymentListener <ul style="list-style-type: none"> onQRCodePaymentResult 	Callback utilizado pelo SDK para informar a <i>app</i> Parceiro com o resultado da operação QRCode que acabou de realizar	SDK	App Parceiro
MBWAYSdkQRCodeUnlockATMLListener <ul style="list-style-type: none"> onQRCodeUnlockATMResult 	Callback utilizado pelo SDK para informar a <i>app</i> Parceiro com o resultado de acesso ao MULTIBANCO via MB WAY	SDK	App Parceiro

3.2.2.1.1 Inicialização do SDK

O SDK deverá ser inicializado, sempre que a *app* do Parceiro seja lançada, utilizando o método MBWAYSdk.init().

3.2.2.1.1.1 Input

Tabela 6 - Input do pedido de inicialização do SDK (Android)

Nome	Descrição	Formato	Tamanho	Mandatário
application	Objeto Application	Application	-	S
phonePrefix	Indicativo do telemóvel. Ex: 00351	String	5	S
phone	Número de telemóvel nacional, no formato 9*****	String	9	S
pinMBWAY	PIN MB WAY de 6 dígitos passado em claro	String	6	S
codAct	Código de ativação	String	7	S
ids	Identificador de Serviço fornecido na criação de serviço	String	40	S
env	Ambiente do SDK. Ex. Qualidade ou Produção	EnumSdkEnv	-	S
initListener	Callback de retorno que é chamado no fim da inicialização do SDK	MBWAYSdkInitListener	-	S

3.2.2.1.1.2 Output

Esta interface é *void*.

3.2.2.1.1.3 Listener MBWAYSdkInitListener

O resultado da inicialização do SDK será passado à *app* do parceiro através do *Callback* MBWAYSdkInitListener.onInitResult.

Tabela 7 - Input do método MBWAYSdkInitListener.onInitResult() (Android)

Código de retorno (status)	Nome	Descrição
status	Campo com um status do resultado	String
description	Campo com descrição técnica relativa ao caso de erro	String

Tabela 8 - Possíveis estados de retorno (status) da inicialização do SDK (Android)

Código de retorno (status)	Nome	Descrição
000	SUCCESS	Inicialização com sucesso
001	GENERIC_ERROR	Inicialização com erros
004	INPUT_VALIDATION_FAILED	Erro na validação dos campos do pedido
008	CONTACTLESS_CONFIG_ERROR	Inicialização da funcionalidade de Pagamentos MB WAY Contactless com erros.

O campo *description* contém informação técnica adicional relativa ao caso de erro.

3.2.2.1.2 Pesquisa de Operações Pendentes

Esta interface deverá ser chamada sempre que a *app* do Parceiro queira consultar a lista de operações pendentes para o serviço MB WAY Parceiro, utilizando o método MBWAYSdk.searchPendingOperations().

3.2.2.1.2.1 Input

Tabela 9 - Input do pedido de pesquisa de operações pendentes (Android)

Nome	Descrição	Formato	Tamanho	Mandatário
pinMBWAY	PIN MB WAY de 6 dígitos passado em claro	String	6	S
operationsListener	Callback de retorno que é chamado no fim da inicialização do SDK	MBWAYSdkPendingOperationsListener	-	S

3.2.2.1.2.2 Output

Esta interface é *void*.

3.2.2.1.2.3 Listener MBWAYSdkPendingOperationsListener

O resultado da pesquisa de operações pendentes será passado à *app* do parceiro através do *Callback* MBWAYSdkPendingOperationsListener.onPendingOperationResult().

Tabela 10 - Input do método MBWAYSdkPendingOperationsListener.onPendingOperationResult() (Android)

Nome	Descrição	Formato
pendingOpsList	Campo com uma lista de objetos PendingOperation	List<PendingOperation>
status	Campo com um status do resultado	String
description	Campo com descrição técnica relativa ao caso de erro	String

O objeto PendingOperation está definido na secção 3.2.3.2.1.

Tabela 11 - Possíveis estados de retorno (status) do pedido de operações pendentes (Android)

Código de retorno (status)	Nome	Descrição
000	SUCCESS	Pedido de inicialização com sucesso
001	GENERIC_ERROR	Confirmação com erros
004	INPUT_VALIDATION_FAILED	Erro na validação dos campos do pedido
002	APP_NOT_REGISTERED	Aplicação não registada

O campo *description* contém informação técnica adicional relativa ao caso de erro.

O atributo *pendingOpsList* é uma lista de objetos PendingOperation.

3.2.2.1.3 Confirmação de uma compra pendente (Compra/Autorização)

Esta interface deve ser chamada sempre que a *app* do Parceiro queira confirmar uma compra/autorização, utilizando o método MBWAYSdk.confirmFinancialOperation().

3.2.2.1.3.1 Input

Tabela 12 - Input do pedido de confirmação de compra pendente (Android)

Nome	Descrição	Formato	Tamanho	Mandatário
pinMBWAY	PIN MB WAY	String	Var.	S
idc	Identificador do cartão	String	40	S
serviceOperationCode	Código que identifica a operação pendente	String	Var.	S
serviceOperationTypeCode	Código que identifica o tipo de operação	String	Var.	S
operationListener	Callback de retorno que é chamado no fim da compra	MBWAYSdkOperationListener	Var.	S

3.2.2.1.3.2 Output

Esta interface é *void*.

3.2.2.1.3.3 Listener MBWAYSdkOperationListener

O resultado da confirmação da compra/autorização será passado à *app* do parceiro através do *Callback* `MBWAYSdkOperationListener.onOperationResult()`.

Tabela 13 - Input do método MBWAYSdkOperationListener.onOperationResult() (Android)

Nome	Descrição	Formato
<code>serviceOperationCode</code>	Campo com o identificador enviado na confirmação da operação	String
<code>status</code>	Campo com um status do resultado	String
<code>description</code>	Campo com descrição técnica relativa ao caso de erro	String

Tabela 14 - Possíveis estados de retorno (status) do pedido de confirmação de compra pendente (Android)

Código de retorno (status)	Nome	Descrição
000	SUCCESS	Confirmação com sucesso
001	GENERIC_ERROR	Confirmação com erros
004	INPUT_VALIDATION_FAILED	Erro na validação dos campos do pedido
002	APP_NOT_REGISTERED	Aplicação não registada
003	IDC_NOT_RECONIZED	O idc não está registado para a aplicação do parceiro

O campo *description* contém informação técnica adicional relativa ao caso de erro.

O campo *serviceOperationCode* contém o id da operação enviada na confirmação de uma compra.

3.2.2.1.4 Recusa de uma operação pendente (Compra/Autorização)

Esta interface deve ser chamada sempre que a *app* do Parceiro queira rejeitar uma compra/autorização, utilizando o método `MBWAYSdk.rejectFinancialOperation()`.

3.2.2.1.4.1 Input

Tabela 15 - Input do pedido de recusa de compra pendente (Android)

Nome	Descrição	Formato	Tamanho	Mandatário
<code>pinMBWAY</code>	PIN MB WAY	String	Var.	S
<code>serviceOperationCode</code>	Código que identifica a operação pendente	String	Var.	S
<code>serviceOperationTypeCode</code>	Código que identifica o tipo de operação	String	Var.	S

Nome	Descrição	Formato	Tamanho	Mandatário
operationListener	Callback de retorno que é chamado no fim da recusa	MBWAYSdkOperationListener	Var.	S

3.2.2.1.4.2 Output

Esta interface é *void*.

3.2.2.1.4.3 Listener MBWAYSdkOperationListener

O resultado da rejeição da compra/autorização será passado à *app* do parceiro através do *Callback* MBWAYSdkOperationListener.onOperationResult().

Tabela 16 - Input do método MBWAYSdkOperationListener.onOperationResult() (Android)

Nome	Descrição	Formato
serviceOperationCode	Campo com o identificador enviado na recusa da operação	String
status	Campo com um status do resultado	String
description	Campo com descrição técnica relativa ao caso de erro	String

Tabela 17 - Possíveis estados de retorno (status) do pedido de recusa de compra pendente (Android)

Código de retorno (status)	Nome	Descrição
000	SUCCESS	Confirmação com sucesso
001	GENERIC_ERROR	Confirmação com erros
004	INPUT_VALIDATION_FAILED	Erro na validação dos campos do pedido
002	APP_NOT_REGISTERED	Aplicação não registrada

O campo *description* contém informação técnica adicional relativa ao caso de erro.

O campo *serviceOperationCode* contém o id da operação enviada na recusa de uma compra.

3.2.2.1.5 Consultar estado do SDK

Esta interface deve ser chamada sempre que a *app* do Parceiro queira consultar o estado do SDK, utilizando o método MBWAYSdk.getStatus().

3.2.2.1.5.1 Input

Tabela 18 - Input do pedido de consulta do estado do SDK (Android)

Nome	Descrição	Formato	Tamanho	Mandatário
getStatusListener	Callback de retorno que é chamado com o resultado da consulta do estado do SDK	MBWAYSdkGetStatusListener	Var.	S

3.2.2.1.5.2 Output

Esta interface é *void*.

3.2.2.1.5.3 Listener MBWAYSdkGetStatusListener

O resultado do pedido de consulta de estado será passado à *app* do parceiro através do *Callback* `MBWAYSdkGetStatusListener.onGetStatusResult()`.

Tabela 19 - *Input* do método `MBWAYSdkGetStatusListener.onGetSdkStatusResult()` (Android)

Nome	Descrição	Formato
sdkStatus	Campo com o objeto que contém a informação do estado do SDK	SDKStatus

O objeto `StatusResult` está definido na secção 3.2.2.2.1.

3.2.2.1.6 Selecionar cartão default para pagamentos MB WAY Contactless

Esta interface deve ser chamada sempre que a *app* do Parceiro queira selecionar um cartão *default* para pagamentos, utilizando o método `MBWAYSdk.selectCardforContactlessPayment()`.

3.2.2.1.6.1 Input

Tabela 20 - *Input* do pedido de selecionar cartão default para compras MB WAY Contactless (Android)

Nome	Descrição	Formato	Tamanho	Mandatário
idc	Identificador do cartão	String	40	S
selectCardListener	<i>Callback</i> de retorno que é chamado no fim da seleção do cartão	<code>MBWAYSdkSetCardForContactlessPaymentListener</code>	Var.	S

3.2.2.1.6.2 Output

Esta interface é *void*.

3.2.2.1.6.3 Listener MBWAYSdkSetCardForContactlessPaymentListener

O resultado da rejeição da compra/autorização será passado à *app* do parceiro através do *Callback* `MBWAYSdkSetCardForContactlessPaymentListener.onSetCardForContactlessPaymentResult()`.

Tabela 21 - *Input* do método MBWAYSdkSetCardForContactlessPaymentListener.onSetCardForContactlessPaymentResult() (Android)

Nome	Descrição	Formato
status	Campo com um status do resultado	String
description	Campo com descrição técnica relativa ao caso de erro	String

Tabela 22 - Possíveis estados de retorno (status) do pedido para selecionar cartão default para compras MB WAY Contactless (Android)

Código de retorno (status)	Nome	Descrição
000	SUCCESS	Confirmação com sucesso
001	GENERIC_ERROR	Confirmação com erros
002	APP_NOT_REGISTERED	Aplicação não registada
003	IDC_NOT_RECONIZED	O idc não está registado para a aplicação do parceiro

O campo *description* contém informação técnica adicional relativa ao caso de erro.

3.2.2.1.7 Configuração de pagamentos MB WAY Contactless

Esta interface deve ser chamada sempre que a *app* do Parceiro queira modificar as opções de pagamentos MB WAY Contactless, utilizando o método MBWAYSdk.configContactlessPayments().

3.2.2.1.7.1 Input

Tabela 23 - *Input* do pedido de configuração de pagamentos MB WAY Contactless (Android)

Nome	Descrição	Formato	Tamanho	Mandatário
mbContactlessPaymentsEnabled	Indicador para definição do estado dos pagamentos MB WAY contactless	Boolean	-	S
mbContactlessLockedScreenPayments	Indicador para definição de pagamento MB WAY contactless com o telemóvel bloqueado	Boolean	-	S
mbContactlessAlwaysRequirePin	Indicador para definição de obrigatoriedade de autenticação em todas as operações com PIN MB WAY	Boolean	-	S

3.2.2.1.7.2 Output

Esta interface é *void*.

3.2.2.1.8 Consulta de cartões provisionados para MB WAY Contactless

Esta interface deve ser chamada sempre que a *app* do Parceiro queira consultar a lista de cartões provisionados para MB WAY contactless, utilizando o método `MBWAYSdk.getContactlessProvisionedCards()`.

3.2.2.1.8.1 Input

Tabela 24 - Input do pedido de consultar a lista de cartões provisionados (Android)

Nome	Descrição	Formato	Tamanho	Mandatário
provisionedCardsListener	Callback de retorno que é chamado com o resultado da consulta de cartões provisionados	MBWAYSdkGetProvisionedCards	Var.	S

3.2.2.1.8.2 Output

Esta interface é *void*.

3.2.2.1.8.3 Listener MBWAYSdkGetProvisionedCards

O resultado da rejeição da compra/autorização é passado à *app* do parceiro através do *Callback* `MBWAYSdkGetProvisionedCards.onGetProvisionedCardsResult()`

Tabela 25 - Input do método `MBWAYSdkGetProvisionedCardsListener.onGetProvisionedCardsResult()` (Android)

Nome	Descrição	Formato
idcList	Campo que contém a lista de identificadores de cartões que estão provisionados	List<String>
status	Campo com um status do resultado	String
description	Campo com descrição técnica relativa ao caso de erro	String

O *Input* do método `onGetProvisionedCardsResult` contém a lista de identificadores de cartões que estão provisionados.

3.2.2.1.9 Passagem de PIN MB WAY ao SDK

Esta interface deve ser chamada sempre que a *app* do Parceiro precise de informar ao SDK o PIN MB WAY, utilizando o método `MBWAYSdk.setPINMBWAY()`.

Esta interface deve ser chamada sempre que a *app* do Parceiro receber o *Callback* de request PIN.

3.2.2.1.9.1 Input

Tabela 26 - Input do pedido de passagem de PIN MB WAY ao SDK

Nome	Descrição	Formato	Tamanho	Mandatário
pinMBWAY	PIN MB WAY de 6 dígitos passado em claro	String	6	S

3.2.2.1.9.2 Output

Esta interface é *void*.

3.2.2.1.10 Registo de um pagamento QRCode

Esta interface deve ser chamada sempre que a *app* do Parceiro queira fazer um pagamento por QRCode, utilizando o método MBWAYSdk.registerQRCodePayment().

3.2.2.1.10.1 Input

Tabela 27 - Input do pedido de pagamento QRCode (Android)

Nome	Descrição	Formato	Tamanho	Mandatário
qrcodeInfo	Conteúdo lido do QRCode	String	61	S
pinMBWAY	PIN MB WAY	String	Var.	S
idc	Identificador do cartão	String	40	S
qrcodePaymentListener	Callback de retorno que é chamado no fim do pedido de pagamento QRcode	MBWAYSdkQRCodePaymentListener	Var.	S

3.2.2.1.10.2 Output

Esta interface é *void*.

3.2.2.1.10.3 Listener MBWAYSdkQRCodePaymentListener

O resultado do pagamento QRCode será passado à *app* do parceiro através do Callback MBWAYSdkQRCodePaymentListener.onQRCodePaymentResult().

Tabela 28 - Input do método MBWAYSdkQRCodePaymentListener.onQRCodePaymentResult() (Android)

Nome	Descrição	Formato
status	Campo com um status do resultado	String
description	Campo com descrição técnica relativa ao caso de erro	String

Tabela 29 - Possíveis estados de retorno (status) do pedido de pagamento QRCode (Android)

Código de retorno (status)	Nome	Descrição
000	SUCCESS	Confirmação com sucesso
001	GENERIC_ERROR	Confirmação com erros
004	INPUT_VALIDATION_FAILED	Erro na validação dos campos do pedido
002	APP_NOT_REGISTERED	Aplicação não registrada
003	IDC_NOT_RECONIZED	O idc não está registrado para a aplicação do parceiro
009	QRCODE_PARSE_FAILED	QRCode mal formatado

3.2.2.1.11 Utilizar MULTIBANCO

Esta interface deve ser chamada sempre que a *app* do Parceiro queira fazer um acesso ao MULTIBANCO via MB WAY, utilizando o método MBWAYSdk.registerQRCodeUnlockATM().

3.2.2.1.11.1 Input

Tabela 30 - Input do pedido de pagamento QRCode (Android)

Nome	Descrição	Formato	Tamanho	Mandatório
qrCodeInfo	Conteúdo lido do QRCode	String	104	S
pinMBWAY	PIN MB WAY	String	Var.	S
idc	Identificador do cartão	String	40	S
qrCodeUnlockATMListener	Callback de retorno que é chamado no fim do pedido de pagamento QRcode	MBWAYSdkQRCodeUnlockATMListener	Var.	S

3.2.2.1.11.2 Output

Esta interface é *void*.

3.2.2.1.11.3 Listener MBWAYSdkQRCodeUnlockATMListener

O resultado de uma tentativa de acesso ao MULTIBANCO via MB WAY será passado à *app* do parceiro através do callback MBWAYSdkQRCodeUnlockATMListener.onQRCodeUnlockATMResult().

Tabela 31 - Input do método MBWAYSdkQRCodeUnlockATMListener.onQRCodeUnlockATMResult() (Android)

Nome	Descrição	Formato
status	Campo com um status do resultado	String
description	Campo com descrição técnica relativa ao caso de erro	String

Tabela 32 - Possíveis estados de retorno (status) do pedido de acesso ao MULTIBANCO via MB WAY (Android)

Código de retorno (status)	Nome	Descrição
000	SUCCESS	Confirmação com sucesso
001	GENERIC_ERROR	Confirmação com erros
004	INPUT_VALIDATION_FAILED	Erro na validação dos campos do pedido
002	APP_NOT_REGISTERED	Aplicação não registada
003	IDC_NOT_RECONIZED	O idc não está registado para a aplicação do parceiro
009	QRCODE_PARSE_FAILED	QRcode mal formatado
012	QRCODE_INVALID	QRcode inválido ou hmac inválido no desbloqueio do ATM

3.2.2.2 Objetos Referenciados pelo SDK Android

3.2.2.2.1 StatusResult

Tabela 33 - Definição do objeto Output Get Status (Android)

Nome	Descrição	Formato
state	Informação do estado do SDK	Enum
idc	Cartão default para pagamentos	String
mbContactlessPaymentsEnabled	Indicador para definição do estado dos pagamentos MB WAY contactless	Boolean
mbContactlessLockedScreenPayments	Indicador para definição de pagamento MB WAY contactless com o telemóvel bloqueado	Boolean
mbContactlessAlwaysRequirePin	Indicador para definição de obrigatoriedade de autenticação em todas as operações com PIN MB WAY	Boolean

Tabela 34 - Possíveis estados do SDK (state)

Enum	Descrição
APP_NOT_REGISTERED	Aplicação não registada
APP_REGISTERED_WITHOUT_CARDS	Aplicação registada sem cartões. Neste estado não é possível fazer pagamentos
APP_REGISTERED_WITH_CARDS	Aplicação registado

3.2.2.2.2 PendingOperation

Tabela 35 - Definição do objeto PendingOperation (SDK Android)

Nome	Descrição	Formato
serviceOperationCode	Código que identifica a operação pendente	String
serviceOperationTypeCode	Código que indentifica o tipo de operação	String
amount	Valor da transação no formato inteiro. Ex: 9€ = 900	Integer
currencyCode	Código da moeda. Ex: Euro = 9782	Integer
description	Informação adicional da operação pendente	String
merchantName	Nome do comerciante que gerou a compra	String

3.2.2.3 Callbacks para pagamentos Contactless

Esta secção define todos os *Callback* que o SDK Android necessita de invocar à *app* Parceiro. Os *Callbacks* podem ser chamados de três maneiras diferentes:

- Por *listener* (telemóvel desbloqueado e *listener* registado);
- Por *Intent* (telemóvel desbloqueado e *listener* não registado);
- Por notificação (telemóvel bloqueado).

3.2.2.3.1 Registo do Callback de Eventos por Listener

O *Callback* de eventos deverá ser inicializado, sempre que a *app* do Parceiro seja lançada, utilizando o método MBWAYSdk.registerOnSDKListener().

O objeto MBWAYSdkContactlessPaymentListener dispõe dos seguintes métodos:

Método	Input	Output	Descrição
onReceivedInformation	Bundle	Void	Método invocado sempre que o SDK precisa de passar alguma informação à <i>app</i> do Parceiro. Ver secção 3.2.2.3.4
getCardForPayment	Void	String (idc)	Método invocado sempre que o SDK inicia um pagamento MB WAY Contactless e pergunta à <i>app</i> Parceiro qual o cartão a ser utilizado. No caso deste <i>listener</i> não estar registado ou ser enviado <i>null</i> na resposta, o SDK irá utilizar o cartão <i>default</i>

3.2.2.3.2 Callback por Intent

O *Callback* por *Intent* é chamado sempre que o dispositivo estiver desbloqueado e o *listener* não estiver registado. O SDK chama a *LaunchActivity* da aplicação parceiro e passa um *Bundle* (ver secção 3.2.2.3.4).

3.2.2.3.3 Callback por notificação

O *Callback* por notificação é chamado sempre que o dispositivo estiver bloqueado. O SDK gera uma notificação local com as mensagens definidas pelo parceiro para cada situação. O click na notificação tem o mesmo comportamento que o *Callback* por *Intent*, é chamada a *LaunchActivity* com um *Bundle* (ver secção 3.2.2.3.4)

3.2.2.3.4 Bundle SDK Info

O *Bundle* recebido em qualquer um dos métodos de *Callback* pode conter uma das chaves da tabela Tabela 36 - Chaves do Bundle SDK.

Tabela 36 - Chaves do Bundle SDK

Chave (String)	Tipo	Descrição
HCE_CALLBACKTYPE	Integer	Identificador do <i>Callback</i> chamado. Todos os tipos de <i>Callbacks</i> descritos na secção 3.2.2
HCE_TERMINATEDPAYMENT	Integer	Resultado do pagamento. Este campo é enviado juntamente com o HCE_CALLBACKTYPE = CB_PAYMENT_TERMINATED. É neste campo que é passada a informação de pagamento em secondTap
HCE_AMOUNT	Integer	Valor da operação no formato inteiro. Ex: 9€ = 900
HCE_CURRENCYCODE	Integer	Código da moeda. Ex: Euro = 9782
HCE_SECONDTAPTIME	Integer	Data de expiração do secondTap (Pagamentos com PIN MB WAY)
HCE_CARDNUMBER	String	Identificador de cartão utilizado na operação
HCE_MESSAGEINFO	String	Mensagem com informação adicional. Esta mensagem é a mesma mostrada na notificação local

Tabela 37 - Tipos de HCE_CALLBACKTYPE

Código (Integer)	Nome	Descrição
1	CB_PAYMENT_TERMINATED	<i>Callback</i> para informar a <i>app</i> do Parceiro que se finalizou uma <i>compra</i> MB WAY Contactless
2	CB_REQUEST_PIN	<i>Callback</i> para informar a <i>app</i> do Parceiro o SDK necessita de PIN MB WAY
3	CB_REQUEST_CONNECTIVITY	<i>Callback</i> para informar que será necessário conectividade e introdução de PIN MB WAY
4	CB_PAYMENT_WITHOUT_SDK_ACTIVATE	<i>Callback</i> para informar que foi tentado um pagamento MB WAY Contactless sem a <i>app</i> estar ativa
5	CB_PAYMENT_WITH_SCREEN_LOCK	<i>Callback</i> para informar que foi tentado um pagamento MB WAY Contactless sem a <i>app</i> estar ativa
7	CB_INFO_NFC_DISCONNECTED	<i>Callback</i> executado quando se perde a ligação entre o POS e o telemóvel
8	CB_DOESNT_HAVE_CARDS_TO_PERFORM_CONTACTLESS_PAYMENTS	<i>Callback</i> utilizado para informar que o utilizador tentou fazer uma compra sem ter cartões disponíveis para pagamento
9	CB_DOESNT_HAVE_DEFAULT_CARD_FOR_CONTACTLESS_PAYMENTS	<i>Callback</i> utilizado para informar que o utilizador não tem nenhum cartão selecionado para pagamento
10	CB_DEVICE_ROOTED	<i>Callback</i> para informar aplicação que o telemóvel está ROOTED
11	CB_CARD_DOESNT_EXIST	<i>Callback</i> para informar que o utilizador tentou pagar com um cartão que não existe provisionado no HCE
13	CB_DEACTIVATED_PAYMENTS	<i>Callback</i> para informar que o utilizador tentou pagar quando os pagamentos estavam desativos

Código (Integer)	Nome	Descrição
14	CB_POS_DOESNT_SUPPORT_MB_CONTACTLESS	<i>Callback</i> para informar que o utilizador tentou pagar num POS que não suporta o <i>schema</i> MB Contactless

3.2.2.3.4.1 Pagamento Terminado (CB_PAYMENT_TERMINATED)

Callback com o código 1.

É chamado sempre que o SDK termina um pagamento MB WAY Contactless. Este *Callback* pode ser chamado em secondTap.

Juntamente com este *Callback* serão passadas as seguintes chaves no Bundle:

- HCE_CARDNUMBER
- HCE_TERMINATEDPAYMENT
- HCE_AMOUNT
- HCE_CURRENCYCODE
- HCE_MESSAGEINFO

O campo HCE_TERMINATEDPAYMENT é um inteiro que pode assumir os seguintes valores:

- 0: pagamento processado com sucesso
- 1: pagamento em secondTap (precisa de PIN)
- 2: pagamento não processado

3.2.2.3.4.2 Pedir Pin (CB_REQUEST_PIN)

Callback com o código 2.

É chamado sempre que o SDK necessita de um PIN MB WAY para uma compra MB WAY Contactless. Este *Callback* é chamado logo após ser recebido um *Callback* de pagamento terminado com o HCE_TERMINATEDPAYMENT = 1.

Juntamente com este *Callback* serão passadas as seguintes chaves no Bundle:

- HCE_CARDNUMBER
- HCE_AMOUNT
- HCE_CURRENCYCODE
- HCE_SECONDTAPTIME
- HCE_MESSAGEINFO

O campo HCE_SECONDTAPTIME é um campo long (dateTime) que contem a data do tempo limite para inserir o PIN MB WAY . Um pagamento em secondTap é utilizado para pagamentos superiores ao limite do cartão sem PIN.

3.2.2.3.4.3 Pedido de conectividade (CB_REQUEST_CONNECTIVITY)

Callback com o código 3.

É chamado sempre que o SDK necessita de internet de da introdução de um PIN MB WAY para uma compra MB WAY Contactless. Esta *Callback* irá ser chamado quando o utilizador fizer múltiplas compras MB WAY *Contactless* em modo *offline*.

Juntamente com este *Callback* serão passadas as seguintes chaves no *Bundle*:

- HCE_MESSAGEINFO

3.2.2.3.4.4 SDK não está ativo (CB_PAYMENT_WITHOUT_SDK_ACTIVATE)

Callback com o código 4.

É chamado sempre que o utilizador inicia um pagamento e o SDK deteta não está ativo para pagamentos (não foi chamado a inicialização do SDK ou aconteceu um erro na inicialização).

Juntamente com este *Callback* serão passadas as seguintes chaves no *Bundle*:

- HCE_MESSAGEINFO

3.2.2.3.4.5 Pagamento com o ecrã bloqueado (CB_PAYMENT_WITH_SCREEN_LOCK)

Callback com o código 5.

É chamado sempre que o utilizador inicia um pagamento com o ecrã bloqueado e o SDK deteta que a configuração para pagamentos MB WAY Contactless com ecrã bloqueado está desligada.

Juntamente com este *Callback* serão passadas as seguintes chaves no *Bundle*:

- HCE_MESSAGEINFO

3.2.2.3.4.6 Ligação com POS quebrada (CB_INFO_NFC_DISCONNECTED)

Callback com o código 7.

É chamado sempre que é quebrada a ligação do SDK com o POS a meio de uma transação.

Juntamente com este *Callback* serão passadas as seguintes chaves no *Bundle*:

- HCE_MESSAGEINFO

3.2.2.3.4.7 SDK sem cartões aprovisionados (CB_DOESNT_HAVE_CARDS_TO_PERFORM_CONTACTLESS)

Callback com o código 8.

É chamado sempre que o utilizador inicia um pagamento e o SDK deteta que não tem cartões aprovisionados para pagamentos (não foi chamado a inicialização do SDK ou aconteceu um erro na inicialização).

Juntamente com este *Callback* serão passadas as seguintes chaves no *Bundle*:

- HCE_MESSAGEINFO

3.2.2.3.4.8 SDK sem cartão default selecionado (CB_DOESNT_HAVE_DEFAULT_CARD_FOR_CONTACTLESS)

Callback com o código 9.

É chamado sempre que o utilizador inicia um pagamento e o SDK deteta que não tem cartão default para pagamentos (não foi chamado o `selectCardForPayment`, ou o mesmo resultou em erro).

Juntamente com este *Callback* serão passadas as seguintes chaves no Bundle:

- HCE_MESSAGEINFO

3.2.2.3.4.9 Dispositivo está rooted (CB_DEVICE_ROOTED)

Callback com o código 10.

É chamado sempre que o utilizador inicia um pagamento e o SDK deteta que o dispositivo está rooted.

Juntamente com este *Callback* serão passadas as seguintes chaves no Bundle:

- HCE_MESSAGEINFO

3.2.2.3.4.10 Cartão não existe (CB_CARD_DOESNT_EXIST)

Callback com o código 11.

É chamado sempre o SDK deteta que cartão passado no `getCardForPayment` não existe ou não está provisionado.

Juntamente com este *Callback* serão passadas as seguintes chaves no Bundle:

- HCE_MESSAGEINFO

3.2.2.3.4.11 Pagamentos MB WAY Contactless estão desligados (CB_DEACTIVATED_PAYMENTS)

Callback com o código 13.

É chamado sempre que o utilizador inicia um pagamento e o SDK deteta que os pagamentos estão desligados.

Juntamente com este *Callback* serão passadas as seguintes chaves no Bundle:

- HCE_MESSAGEINFO

3.2.2.3.4.12 POS não suporta pagamentos MB Contactless (CB_POS_DOESNT_SUPPORT_MB_CONTACTLESS)

Callback com o código 14.

É chamado sempre que o utilizador inicia um pagamento e o POS não suporta pagamentos MB WAY Contactless.

Juntamente com este *Callback* serão passadas as seguintes chaves no Bundle:

- HCE_MESSAGEINFO

3.2.3 Integração para iOS

3.2.3.1 Interfaces do SDK iOS

Esta secção define todas as interfaces que estão disponíveis para integração do SDK iOS.

Tabela 38 – Lista de Operações Suportadas pelo SDK iOS

Interface	Descrição	Origem	Destino
init	Inicialização de parâmetros de aplicação sempre que a <i>app</i> do parceiro é aberta	<i>App</i> Parceiro	SDK
searchPendingOperations	Este serviço retorna todas as operações de compras que ele tem pendentes de ação	<i>App</i> Parceiro	SDK
confirmFinancialOperation	Confirmação de uma compra pelo utilizador na <i>app</i>	<i>App</i> Parceiro	SDK
rejectFinancialOperation	Rejeição de compras pelo utilizador na <i>app</i>	<i>App</i> Parceiro	SDK
getStatus	Função para pedir informação sobre o SDK: <ul style="list-style-type: none"> Estado SDK 	<i>App</i> Parceiro	SDK
registerQRCodePayment	Registo de um pedido de pagamento QRCode	<i>App</i> Parceiro	SDK

O SDK dispõe de um protocolo *MBWAYSDKDelegate* que disponibiliza os *Callbacks* da Tabela 39 - Lista de *Callbacks* utilizados pelo SDK iOS.

Tabela 39 - Lista de *Callbacks* utilizados pelo SDK iOS

<i>Callback</i>	Descrição	Origem	Destino
MBWAYSDKInitDelegate <ul style="list-style-type: none"> <i>onInitResult:andMessage:</i> 	<i>Callback</i> de retorno que informa a <i>app</i> parceiro com o resultado do estado da inicialização do SDK	SDK	<i>App</i> Parceiro
MBWAYSDKPendingOperationsDelegate <ul style="list-style-type: none"> <i>onPendingOperationResult:andStatus:andMessage:</i> 	<i>Callback</i> de retorno que passa à <i>app</i> parceiro a listagem de operações pendentes	SDK	<i>App</i> Parceiro
MBWAYSDKOperationDelegate <ul style="list-style-type: none"> <i>onOperationResult:andStatus:andMessage:</i> 	<i>Callback</i> de retorno que informa a <i>app</i> parceiro com o resultado da operação que acabou de realizar	SDK	<i>App</i> Parceiro
MBWAYSDKGetSDKStatusDelegate <ul style="list-style-type: none"> <i>onGetSDKStatusResult:</i> 	<i>Callback</i> de retorno que informa a <i>app</i> parceiro com o estado do SDK	SDK	<i>App</i> Parceiro
MBWAYSDKRegisterQRCodePaymentDelegate <ul style="list-style-type: none"> <i>onQRCodePaymentResult:status andMessage:</i> 	<i>Callback</i> utilizado pelo SDK para informar a <i>app</i> Parceiro com o resultado da operação QRCode que acabou de realizar	SDK	<i>App</i> Parceiro
MBWAYSDKRegisterQRCodeUnlockATMDelegate <ul style="list-style-type: none"> <i>onQRCodeUnlockATMResult: andMessage:</i> 	<i>Callback</i> utilizado pelo SDK para informar a <i>app</i> Parceiro com o resultado de acesso ao MULTIBANCO via MB WAY	SDK	<i>App</i> Parceiro

3.2.3.1.1 Inicialização do SDK

O SDK deverá ser inicializado, sempre que a *app* do Parceiro seja lançada, utilizando o método [MBWAYSDK init].

3.2.3.1.1.1 Input

Tabela 40 - Input do pedido de inicialização do SDK (iOS)

Nome	Descrição	Formato	Tamanho	Mandatário
delegate	Id do delegate que deverá ser chamado com a resposta do init	id<MBWAYSDK InitDelegate>	-	S
phonePrefix	Indicativo do telemóvel. Ex: 00351	NSString	5	S
phone	Número de telemóvel nacional, no formato 9*****	NSString	9	S
pinMBWAY	PIN MB WAY de 6 dígitos passado em claro	NSString	6	S
codAct	Código de ativação	NSString	7	S
ids	Identificador de Serviço fornecido na criação de serviço	NSString	40	S
env	Ambiente do SDK. Ex. Qualidade ou Produção	EnumSdkEnv	-	S

3.2.3.1.1.2 Output

Esta interface é *void*.

3.2.3.1.1.3 Callback

O resultado da inicialização do SDK será passado à *app* do parceiro através do *Callback* do protocolo MBWAYSDKInitDelegate com o método `onInitResult:andMessage:`.

Tabela 41 - Input do *Callback onInitResult:andMessage:* (iOS)

Nome	Descrição	Formato
status	Campo com um status do resultado	NSString
description	Campo com descrição técnica relativa ao caso de erro	NSString

Tabela 42 - Possíveis estados de retorno (status) da inicialização do SDK (iOS)

Código de retorno (status)	Nome	Descrição
000	SUCCESS	Inicialização com sucesso
001	GENERIC_ERROR	Inicialização com erros
004	INPUT_VALIDATION_FAILED	Erro na validação dos campos do pedido
008	CONTACTLESS_CONFIG_ERROR	Inicialização da funcionalidade de Pagamentos MB WAY Contactless com erros.

O campo *description* contém informação técnica adicional relativa ao caso de erro.

3.2.3.1.2 Pesquisa de Operações Pendentes

Esta interface deve ser chamada sempre que a *app* do Parceiro queira consultar a lista de operações pendentes para o serviço MB WAY Parceiro, utilizando o método [MBWAYSdk searchPendingOperations].

3.2.3.1.2.1 Input

Tabela 43 - Input do pedido de pesquisa de operações pendentes (iOS)

Nome	Descrição	Formato	Tamanho	Mandatário
delegate	Id do delegate que deverá ser chamado com a resposta do serachPendingOperations	id<MBWAYSdkPendingOperationsDelegate>	-	S
pinMBWAY	PIN MB WAY	NSString	Var.	S

3.2.3.1.2.2 Output

Esta interface é *void*.

3.2.3.1.2.3 Callback

O resultado da pesquisa de operações pendentes é passado à *app* do parceiro através do *Callback* do protocolo [MBWAYSdkPendingOperationsDelegate](#) com o método [onPendingOperationResult:andStatus:andMessage:](#).

Tabela 44 - Input do método [onPendingOperationResult:andStatus:andMessage:](#) (iOS)

Nome	Descrição	Formato
pendingOpsList	Campo com uma lista de objetos PendingOperation	NSArray<PendingOperation >
status	Campo com um status do resultado	NSString
description	Campo com descrição técnica relativa ao caso de erro	NSString

Tabela 45 - Possíveis estados de retorno (status) do pedido de consulta de operações pendentes (iOS)

Código de retorno (status)	Nome	Descrição
000	SUCCESS	Pedido de inicialização com sucesso
001	GENERIC_ERROR	Confirmação com erros
004	INPUT_VALIDATION_FAILED	Erro na validação dos campos do pedido
002	APP_NOT_REGISTERED	Aplicação não registrada

O campo *description* contém informação técnica adicional relativa ao caso de erro.

O atributo *pendingOpsList* é uma lista de objetos

PendingOperation.

3.2.3.1.3 Confirmação de uma operação pendente (Compra/Autorização)

Esta interface deve ser chamada sempre que a *app* do Parceiro queira confirmar uma compra/autorização, utilizando o método [MBWAYSdk confirmFinancialOperation].

3.2.3.1.3.1 Input

Tabela 46 - Input do pedido de confirmação de compra pendente (iOS)

Nome	Descrição	Formato	Tamanho	Mandatário
delegate	Id do delegate que deverá ser chamado com a resposta da confirmação da operação	id<MBWAYSdkOperationDelegate>	-	S
pinMBWAY	PIN MB WAY	NSString	Var.	S
idc	Identificador do cartão	NSString	40	S
serviceOperationCode	Código que identifica a operação pendente	NSString	Var.	S
serviceOperationTypeCode	Código que identifica o tipo de operação	NSString	Var.	S

3.2.3.1.3.2 Output

Esta interface é *void*.

3.2.3.1.3.3 Callback

O resultado da confirmação da compra/autorização será passado à *app* do parceiro através do *Callback* do protocolo MBWAYSdkOperationDelegate com o método `onOperationResult:andStatus:andMessage:`.

Tabela 47 - Input do método `onOperationResult:andStatus:andMessage:` (iOS)

Nome	Descrição	Formato
serviceOperationCode	Campo com o identificador enviado na confirmação da operação	NSString
status	Campo com um status do resultado	NSString
description	Campo com descrição técnica relativa ao caso de erro	NSString

Tabela 48 - Possíveis estados de retorno (status) do pedido de confirmação de compra pendente (iOS)

Status Code	Código de Retorno	Descrição
000	SUCCESS	Confirmação com sucesso
001	GENERIC_ERROR	Confirmação com erros
004	INPUT_VALIDATION_FAILED	Erro na validação dos campos do pedido
002	APP_NOT_REGISTERED	Aplicação não registrada

Status Code	Código de Retorno	Descrição
003	IDC_NOT_RECONIZED	O idc não está registrado para a aplicação do parceiro

O campo *description* contém informação técnica adicional relativa ao caso de erro.

O campo *serviceOperationCode* contém o id da operação enviada na confirmação de uma compra.

3.2.3.1.4 Recusa de uma operação pendente (Compra/Autorização)

Esta interface deve ser chamada sempre que a *app* do Parceiro queira rejeitar uma compra/autorização, utilizando o método [MBWAYSdk rejectFinancialOperation];

3.2.3.1.4.1 Input

Tabela 49 - Input do pedido de recusa de compra pendente (iOS)

Nome	Descrição	Formato	Tamanho	Mandatário
delegate	Id do delegate que deverá ser chamado com a resposta da recusa da operação	id<MBWAYSdkOperationDelegate>	-	S
pinMBWAY	PIN MB WAY	NSString	Var.	S
serviceOperationCode	Código que identifica a operação pendente	NSString	Var.	S
serviceOperationTypeCode	Código que identifica o tipo de operação	NSString	Var.	S

3.2.3.1.4.2 Output

Esta interface é *void*.

3.2.3.1.4.3 Callback

O resultado da confirmação da compra/autorização será passado à *app* do parceiro através do *Callback* do protocolo MBWAYSdkOperationDelegate com o método *onOperationResult:andStatus:andMessage:*.

Tabela 50 - Input do método *onOperationResult:andStatus:andMessage:* (iOS)

Nome	Descrição	Formato
serviceOperationCode	Campo com o identificador enviado na recusa da operação	NSString
status	Campo com um status do resultado	NSString
description	Campo com descrição técnica relativa ao caso de erro	NSString

Tabela 51 - Possíveis estados de retorno (status) do pedido de recusa de compra pendente (iOS)

Status Code	Código de Retorno	Descrição
000	SUCCESS	Confirmação com sucesso
001	GENERIC_ERROR	Confirmação com erros
004	INPUT_VALIDATION_FAILED	Erro na validação dos campos do pedido
002	APP_NOT_REGISTERED	Aplicação não registrada
003	IDC_NOT_RECONIZED	O idc não está registrado para a aplicação do parceiro

O campo *description* contém informação técnica adicional relativa ao caso de erro.

O campo *serviceOperationCode* contém o id da operação enviada na confirmação de uma compra.

3.2.3.1.5 Consultar estado do SDK

Esta interface deve ser chamada sempre que a *app* do Parceiro queira consultar o estado do SDK, utilizando o método [MBWAYSdk getStatus].

3.2.3.1.5.1 Input

Tabela 52 - Input do pedido de consulta do estado do SDK (iOS)

Nome	Descrição	Formato	Tamanho	Mandatário
delegate	Id do delegate que deverá ser chamado com a resposta da consulta do estado	id<MBWAYSdkGetSDKStatusDelegate>	-	S

3.2.3.1.5.2 Output

Esta interface é *void*.

3.2.3.1.5.3 Callback

O resultado do pedido de consulta de estado será passado à *app* do parceiro através do *Callback* do protocolo [MBWAYSdkGetSDKStatusDelegate](#) com o método [onGetSDKStatusResult](#).

Tabela 53 - Input do método onGetSDKStatusResult: (iOS)

Nome	Descrição	Formato
state	Campo com o estado do SDK	NSEnum

Tabela 54 - Possíveis estados do SDK (iOS)

Enum	Descrição
APP_NOT_REGISTERED	Aplicação não registrada

Enum	Descrição
APP_REGISTERED_WITHOUT_CARDS	Aplicação registrada sem cartões. Neste estado não é possível fazer pagamentos
APP_REGISTERED_WITH_CARDS	Aplicação registrado

3.2.3.1.6 Registo de um pagamento QRCode

Esta interface deve ser chamada sempre que a *app* do Parceiro queira fazer um pagamento por QRCode, utilizando o método [MBWAYSdk registerQRCodePayment].

3.2.3.1.6.1 Input

Tabela 55 - Input do pedido de pagamento QRCode (iOS)

Nome	Descrição	Formato	Tamanho	Mandatário
delegate	Id do delegate que deverá ser chamado com a resposta da confirmação da operação	id<MBWAYSdkRegisterQRCodePaymentDelegate>	-	S
qrcodeInfo	Conteúdo lido do QRCode	NSString	61	S
pinMBWAY	PIN MB WAY	NSString	Var.	S
idc	Identificador do cartão	NSString	40	S

3.2.3.1.6.2 Output

Esta interface é *void*.

3.2.3.1.6.3 Callback

O resultado do pagamento QRCode é passado à *app* do parceiro através do *Callback* do protocolo `MBWAYSdkRegisterQRCodePaymentDelegate` com o método `onQRCodePaymentResult:status andMessage:..`

Tabela 56 - Input do método `onQRCodePaymentResult:status andMessage:` (iOS)

Nome	Descrição	Formato
status	Campo com um status do resultado	NSString
description	Campo com descrição técnica relativa ao caso de erro	NSString

Tabela 57 - Possíveis estados de retorno (status) do pedido de pagamento QRCode (iOS)

Status Code	Código de Retorno	Descrição
000	SUCCESS	Confirmação com sucesso
001	GENERIC_ERROR	Confirmação com erros
004	INPUT_VALIDATION_FAILED	Erro na validação dos campos do pedido
002	APP_NOT_REGISTERED	Aplicação não registrada
003	IDC_NOT_RECONIZED	O idc não está registrado para a aplicação do parceiro
009	QRCODE_PARSE_FAILED	QRCode mal formatado

3.2.3.1.7 Utilizar MULTIBANCO

Esta interface deve ser chamada sempre que a *app* do Parceiro queira fazer um acesso ao MULTIBANCO via MB WAY, utilizando o método [MBWAYSdk registerQRCodeUnlockATM].

3.2.3.1.7.1 Input

Tabela 58 – Input do pedido de acesso ao MULTIBANCO via MB WAY (iOS)

Nome	Descrição	Formato	Tamanho	Mandatário
delegate	Id do delegate que deve ser chamado com a resposta da confirmação da operação	id<MBWAYSdkRegisterQRCodeUnlockATMDelegate>	-	S
qrcodeInfo	Conteúdo lido do QRCode	NSString	104	S
pinMBWAY	PIN MB WAY	NSString	Var.	S
idc	Identificador do cartão	NSString	40	S

3.2.3.1.7.2 Output

Esta interface é *void*.

3.2.3.1.7.3 Callback

O resultado do pagamento QRCode é passado à *app* do parceiro através do *callback* do protocolo MBWAYSdkRegisterQRCodeUnlockATMDelegate com o método onQRCodeUnlockATMResult:andMessage:.

Tabela 59 - Input do método onQRCodeUnlockATMResult:status andMessage: (iOS)

Nome	Descrição	Formato
status	Campo com um status do resultado	NSString
description	Campo com descrição técnica relativa ao caso de erro	NSString

Tabela 60 - Possíveis estados de retorno (status) do pedido de acesso ao MULTIBANCO via MB WAY (iOS)

Status Code	Código de Retorno	Descrição
000	SUCCESS	Confirmação com sucesso
001	GENERIC_ERROR	Confirmação com erros
004	INPUT_VALIDATION_FAILED	Erro na validação dos campos do pedido
002	APP_NOT_REGISTERED	Aplicação não registada
003	IDC_NOT_RECONIZED	O idc não está registado para a aplicação do parceiro
009	QRCODE_PARSE_FAILED	QRCode mal formatado
012	QRCODE_INVALID	QRcode inválido ou hmac inválido no desbloqueio do ATM

3.2.3.2 Objetos referenciados pelo SDK iOS

3.2.3.2.1 PendingOperation

Tabela 61 - Definição do objeto PendingOperation (SDK iOS)

Nome	Descrição	Formato
serviceOperationCode	Código que identifica a operação pendente	NSString
serviceOperationTypeCode	Código que indentifica o tipo de operação	NSString
amount	Valor da transação no formato inteiro. Ex: 9€ = 900	NSInteger
currencyCode	Código da moeda. Ex: Euro = 9782	NSInteger
description	Informação adicional da operação pendente	NSString
merchantName	Nome do comerciante que gerou a compra	NSString

3.2.4 Tabela de erros

A *app* do Parceiro pode receber um dos seguintes erros na resposta do SDK.

Tabela 62 - Código e descrição de erros retornados pelo SDK

Código de erro	Descrição	Causa
000	Sucesso	Operação com sucesso
001	Erro Genérico	Erro Genérico
002	<i>App</i> MB WAY não instalada	Aplicação não instalada
003	IDC não reconhecido	O SDK não reconhece o IDC
004	Dados inválidos	Um dos dados passados ao SDK é inválido (tamanho, etc...)
008	Erro Configuração <i>contactless</i>	Erro de configuração de pagamentos <i>Contactless</i> (Inicialização ou aprovisionamento de cartões)
009	Erro no QRCode	QRCode mal formatado
012	QRCODE_INVALID	QRcode inválido ou hmac inválido no desbloqueio do ATM

3.3 Dicionário de dados

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

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
0001	MSG_TIP	CÓDIGO DA MENSAGEM	4	A		Trata-se do campo que identifica o objetivo da mensagem e a natureza dos dados que são transmitidos: pedido de levantamento, resposta a pedido de levantamento, etc., bem como o tipo de mensagem: operação com cartão, operação com NIB, operação comerciante, notificação de pagamento a empresa, etc.	
0002	MSG_VER	VERSÃO DE MENSAGEM	2	N		Identifica a versão da mensagem indicada no campo (0001) MSG_TIP ou no campo (0470) MSG_TIP_H2H. Identifica a versão da mensagem que está em uso com o Banco; permite que a SIBS possa suportar mensagens com formatos diferentes relativas ao mesmo serviço.	
0003	TRM_TIP	TIPO DE TERMINAL	1	A		Identifica o Tipo de Terminal usado.	
0004	MSG_DTH	DATA/HORA DA TRANSMISSÃO	14	N	AAAAMDD HHMMSS	Campo que contém a data e a hora em que se efetuou a transmissão da mensagem do CPU da SIBS para o CPU do Banco. Não aplicável a registos correspondentes a mensagens trocadas no canal Host-to-Host.	
0006	TRM_IDE	IDENTIFICAÇÃO DO TERMINAL	10	A		Este campo identifica o terminal no qual a transação teve lugar. A estrutura deste campo depende do campo (0003) TRM_TIP, constante na mensagem ou no registo. para mais detalhes. O atributo (6216) TRM_IDEN01 é a variante numérica deste atributo.	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
0007	LOC_TRM	LOCALIZAÇÃO/MORADA DO TERMINAL	40	A		Identifica a localização/morada onde se encontra instalado o terminal no qual foi efetuada a operação do cliente. A informação incluída neste campo depende do campo (0003) TRM_TIP. Consultar https://intra.sibs.corp/sites/EA_Documents/D ata%20Dictionary%20Attachs/0003_TRM_TI P_0006_TRM_IDE_0007_LOC_TRM.docx para mais detalhes.	
0008	TRM_TRNMNTN02	MONTANTE DA TRANSACÇÃO	13	N	11 int. 2 dec.	Indica o valor da transação. Se o código de transação referir uma operação sem valor contabilístico (pedido livro de cheques, alteração de PIN, etc.), então este campo está a zeros. No caso de operações comerciante, indica o total faturado no fecho contabilístico local do TPA (total bruto). No caso de uma operação no estrangeiro, ou de um eurocheque papel, corresponde ao produto do valor total da operação (campo 238) pelo câmbio (campo 236), acrescido do valor do imposto de venda de moeda (campo 240) se este estiver preenchido.	
0068	TRM_IDEPRO	IDENTIFICAÇÃO DO PROPRIETÁRIO	7	N		Identifica a entidade que, do ponto de vista do tarifário SIBS FPS e interbancário, corresponde ao 'Banco de Apoio do Terminal' para o Terminal indicado no campo (006) TRM_IDE. Corresponde também ao número de comerciante matriculado no Sistema MULTIBANCO (Banco de Apoio do Terminal - BAT, Acquirer ou Comerciante) que adquiriu o TPA. Em Caixas Automáticas assume o valor do proprietário da sub-rede de CAs (se MB=1).	Em CA: 0 ou 1 - rede MULTIBANCO; 332 - rede interna MBGP.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
0105	SIS_DTH	DATA/HORA	14	N	AAAAMMDD HHMMSS	Identifica a data e hora a que foi produzida a informação. Esta poderá ser o momento em que foi feito um processamento (por exemplo, fecho no CPU da SIBS FPS) ou em que foi feita uma determinada operação (por exemplo, uma operação cliente, um fecho local no ATM, o processamento do ficheiro de Clearing do país origem). No caso de operações em TPAs EMV indica a data/hora do terminal.	
0117	LOG_NUMN01	NÚMERO DE REGISTO LOG CENTRAL	8	N		Identifica o número do registo no Ficheiro de Log do CPU-SIBS FPS referente à transação. Conjugado com os campos (1709) LOG_SIS, (0320) LOG_PERN01 e (2148) SIS_DTHN01, identifica univocamente um registo no sistema MULTIBANCO. No caso das autorizações, a identificação posicionada para o Acquirer será feita utilizando as 6 posições da direita do registo do log central.	
0118	TRM_PERNUM	NÚMERO DO PERÍODO CONTABILÍSTICO LOCAL	3	N		Indica o número do período local do terminal em que se executaram as transações.	
0119	CAR_MOVNUM	NÚMERO DE MOVIMENTO DO CARTÃO	2	N		Número atribuído ao movimento executado no ATM pelo cartão e que o identificará no extrato do Banco. Nas operações POS este campo será preenchido também, mas a partir de uma nova sequência aplicável só às operações POS (ou online). É impresso no recibo do POS e destina-se ao controlo da operação nos extratos bancários. A primeira operação do cartão é 00 e incrementada de 1 em 1 até 99, voltando a 00.	
0126	CAR_EXPDATN02	DATA DE EXPIRAÇÃO DO CARTÃO	4	N	AAMM	Último mês e ano em que o cartão ainda é válido (zona 18 - Norma ISO 4909).	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
0129	CAR_SEQCOD	SEQUÊNCIA DO CARTÃO	1	N		Este campo destina-se a completar a identificação do cartão.	0 - Não existe informação 1 - Cartão normal de Cliente bancário. 2 - Cartão de serviço Universal - acesso em ATM+POS p/ Cartões Empresa. 3 - Cartão de Serviço Pagamento Automático - acesso a POS p/ Cartões Empresa. 4 - Cartão Serviço ATM - acesso a ATM p/ Cartões Empresa. 5 - Cartão Serviço Sector - acesso a POS pertencente a estabelecimentos do mesmo sector de atividade. (62071 - Gasolineiros) (71161 - Portagens). 6 - Cartão Serviço Comerciante - acesso a POS pertencentes a estabelecimentos de um Comerciante específico. 7 - Cartão Serviço Terminal - acesso a terminal de Acesso ao MB para serviços proprietários do Banco. 8 - Cartão Rede Privada.
0132	SAN_NUM	NÚMERO DA CONTA (SAN1, SAN2 OU OUTRA)	15	N		Identificação do número da primeira (SAN1) ou da segunda (SAN2) conta bancária a que o cartão está associado. Pode também ser utilizada para referir o número de conta do cliente mesmo que não tenha cartão associado (Ex. Conta do Comerciante POS, da Central de Clearing, etc). No caso de novos Bancos, é aconselhável preencher as quatro posições da esquerda com o Código de Agência (0134) BAN_AGECD e os restantes com o número	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
						<p>de conta tal como vem na linha ótica do cheque.</p> <p>Poderá ser equacionada a possibilidade de passar a uma estrutura NIB, caso os Bancos pretendam migrar as contas MULTIBANCO para esse formato, sendo incluídos neste campo os campos Balcão + Conta do NIB (o código de Banco é implícito e o cheque dígito calculável).</p> <p>No caso das mensagens e registos que correspondem a operações com cartão, este campo é normalmente preenchido pela SIBS FPS com o SAN1 informado pelo Banco na emissão ou personalização do cartão; nos produtos cartão que tenham como cenário possível (principal ou de degradação) o 'Saldo Disponível da Conta Crédito', sempre que a operação em causa tem este cenário como possível, a SIBS FPS envia, neste campo, o número da Conta Crédito em lugar da SAN1 (campo (0085) CAR_SCDNUM, enviado pelo Banco nos ficheiros EECB e ESCD.</p>	
0137	CLI_NOMA02	NOME DO CLIENTE	27	A		<p>Campo a preencher com o nome do cliente que constará no visual dos cartões personalizados e no endereço das cartas de PIN. Nos cartões Visa e Europay, o título, nome e sobrenome, devem ser separados por "/". No caso da Visa devem ser preenchidas apenas 26 posições, no caso da Europay apenas 21.</p> <p>Se o cliente não tem título, o campo deve começar "/", seguido do nome. No caso de pretender colocar apenas o sobrenome, deve começar por "//".</p> <p>Existe um conjunto de caracteres limitado para o preenchimento do campo.</p>	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
0157	SPI_MCCCOD	MERCHANT CATEGORY CODE	4	N		Campo que identifica, no âmbito dos sistemas de pagamento internacionais (Visa, MasterCard), o tipo de comerciante.	
0179	EST_NOM	NOME DO ESTABELECIMENTO	40	A		Nome do estabelecimento ou do Departamento onde se encontre instalado o POS ou outro Terminal.	
0181	EST_LOC	LOCAL DO ESTABELECIMENTO	20	A		Local do estabelecimento ou Departamento onde se encontra instalado o POS ou Terminal.	
0226	EXT_CTYCOD	CÓDIGO DE PAÍS	3	N		É o código internacional atribuído ao País a que pertence o Centro de Clearing a quem se destinam os movimentos feitos por cartões na rede Multibanco, ou onde o cartão nacional foi utilizado; ou onde o eurocheque foi negociado. Indica, nos dados de endereçamento, se a morada é em Portugal (=620) ou no estrangeiro.	
0233	EXT_MOECOD	CÓDIGO DE MOEDA	3	N		É o código da moeda em que a operação foi realizada, ou o código da denominação em que é efetuada a liquidação financeira da operação. O campo é preenchido conforme o código da ISO 4217. O código mais utilizado é o 978 (euro).	
0241	BAN_COD_APO	CÓDIGO DO BANCO DE APOIO	4	N		É o código do Banco que apoia a Central de Clearing ou um terminal ou uma entidade cobradora. Pode estar preenchido a zeros indicando que não existe Banco de Apoio. Para aplicação de reclamações é o banco com que o utilizador se autentica.	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
0318	LOG_SINMOV	SINAL	1	A		Preenchido com C, movimento a Crédito do Banco; preenchido com D, movimento de Débito ao Banco. Nota: Caso o montante associado seja zero, deve considerar-se o valor "C".	C - Crédito D - Débito
0320	LOG_PERN01	IDENTIFICAÇÃO DO PERÍODO DO LOG CENTRAL	4	N		Identificação do número do ficheiro de log da SIBS FPS onde foi registada a operação. Este campo combinado com os campos (0117) LOG_NUMN01 e (0320) LOG_PERN01 ou (1709) LOG_SIS, constitui uma chave única da operação. A SIBS FPS usa mais do que um ficheiro de log por dia, pelo que, num mesmo ficheiro da Compensação MULTIBANCO, são encaminhadas operações de vários ficheiros de log; os do dia e eventualmente também os de dias precedentes, caso tenha havido algo que impediu a compensação desse log.	
0323	TRM_REGNUM	NÚMERO DE REGISTO LOCAL	5	N		Identificação do registo da operação no período contabilístico local (TRM_PERNUM) do terminal.	
0428	MSG_OCONUM	NÚMERO DE OCORRÊNCIAS	2	N		Número de vezes em que ocorrem os conjuntos de campos definidos a seguir e que se encontram assinalados com (*).	
0470	MSG_TIP_H2H	CÓDIGO DA MENSAGEM BS	4	A		Código da mensagem na sessão Banco - SIBS.	
0471	MSG_IDE_H2H	IDENTIFICAÇÃO MENSAGEM DO BANCO	14	A		No caso de a mensagem ser originada do CPD de um Banco, o seu preenchimento tem o formato que este quiser. No caso de a mensagem ser de um terminal bancário: COD.TERMINAL 6 NUM.PERIODO 2 NUM.TRANSACÇÃO 5 COD.OPERADOR 1	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
0472	MSG_RESTXT	TEXTO RESPOSTA	45	A		Texto preenchido pela SIBS numa mensagem recusada, com os textos que justificam a recusa para o cliente.	
0492	MSG_RESCOD	CÓDIGO DE RESPOSTA DA MENSAGEM DA SIBS	3	N		Código de resposta da mensagem de sessão Banco ->SIBS. (= 000 - operação aprovada) (>000 - operação recusada). Normalmente os dois dígitos da direita identificam o código do erro.	
0493	MSG_NOKTIP	CÓDIGO DE RECUSA DA MENSAGEM PELA SIBS	8	A		Código da recusa da SIBS a uma mensagem na sessão Banco ->SIBS. (este campo é normalmente preenchido com o modulo do erro, quando existe um erro na msg (campo 492 >0)).	
0637	CAR_EXPDAT	DATA DE EXPIRAÇÃO DO CARTÃO EXPANDIDA	6	N	AAAAMM	Último mês e ano em que o cartão ainda é válido.	
0699	SIS_OPRTIP	CÓDIGO DE TRANSAÇÃO EXPANDIDO	3	A		Identifica o tipo de transação realizada. Relacionado com o atributo 120 (SIS_OPRTIPA01).	
1002	MSG_OPETIP	CÓDIGO OPERADOR	1	A		Indica se se pretende obter os elementos iguais, inferiores ou superiores aos indicados no(s) campo(s) de seleção.	'=' dados solicitados na mensagem de pedido e superiores, no caso da msg de resposta ter ocorrências '>' dados imediatamente superiores aos enviados na mensagem de pedido '<' dados imediatamente inferiores aos enviados na mensagem de pedido

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
1709	LOG_SIS	SISTEMA DO LOG ASSOCIADO À TRANSAÇÃO	2	A		Código utilizado nas mensagens e nos registos de detalhe correspondentes a cada operação e que indica ao Banco qual o subsistema transaccional em que esta se realizou. Corresponde à versão expandida do campo (0312) SIS_APLPDD. Este campo pode não estar preenchido (espaços) em registos gerados na Compensação MULTIBANCO, resultantes do apuramento de valores agregados, para os quais não é criado um registo no ficheiro de log da SIBS FPS.	
1716	BAN_PDREMV	EMV - APLICAÇÃO DO CARTÃO (PADRÃO EMV)	3	N		Identificação do Padrão EMV (parâmetros previamente definidos) correspondente a uma determinada Aplicação EMV a posicionar no cartão. Esta identificação é sequencial por código de Emissor.	001 - valor reservado para identificação do Padrão EMV em que é parametrizada a Aplicação Multibanco; 002 a 989 - valores disponíveis para utilização pelos Emissores; 990 a 999 - (valores de utilização reservada).
2247	SIS_ACTDTH	DATA-HORA DE ACTUALIZAÇÃO	14	N		Este campo regista a data e hora em que o sistema foi actualizado.	
2324	CAR_PANLGT	COMPRIMENTO DO PAN	2	N		Indica qual o comprimento do PAN apresentado nos campos (1967) CAR_PANN01, (2325) CAR_PAN e (5402) CAR_PANA03.	
2325	CAR_PAN	PRIMARY ACCOUNT NUMBER	19	A		Número completo do cartão encostado à esquerda. Formato no âmbito da norma ISO 7812-1. Os caracteres não utilizados (à direita) são preenchidos com os espaços necessários para preencher os 19 bytes de comprimento do campo.	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
2326	LOG_MOVMNTN01_2	MONTANTE DO MOVIMENTO - 2	11	N	9 int. 2 dec.	<p>Indica o valor a movimentar. O montante pode corresponder à movimentação de valores individuais ou de valores agregados, como por exemplo:</p> <ul style="list-style-type: none"> - Total faturado por um comerciante - Total a movimentar a um representante - Somatório de um conjunto de operações - Total de custos/receitas - Etc. <p>No caso de uma operação no estrangeiro realizada noutra moeda, corresponde ao produto do valor total da operação (campo 0238) pelo câmbio (campo (0236) EXT_CAM).</p> <p>Atualmente o valor máximo admissível no SPGT por operação está limitado a 100.000 Eur.</p> <p>Corresponde à versão Euro do atributo (0008).</p>	
2327	LOG_ADIMNT	MONTANTE ADICIONAL	9	N	7 int. 2 dec.	<p>Indica o valor a lançar adicionalmente, a débito ou a crédito, para além do MONTANTE. Este é devido a:</p> <ul style="list-style-type: none"> - Taxas cliente; - Taxas de processamento; - Valor do desconto ou comissionamento aplicado; - Montante de incentivos ou promoções; - Etc. 	
2336	MSG_DADLGT	COMPRIMENTO DOS DADOS VARIÁVEIS	4	N		Indica o tamanho do bloco de dados variáveis presentes nas mensagens real-time associados a um código de transação. O comprimento destes dados não inclui os 4 bytes deste atributo, i.e., refere-se apenas	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
						aos dados que se seguem à definição do comprimento.	
2337	MSG_VERDAD	VERSÃO DOS DADOS VARIÁVEIS	2	N		Indica a versão do bloco de dados variáveis presentes nas mensagens real associados a um código de transação.	
2354	TRM_CAPN01	CAPACIDADES DO TERMINAL	1	N		<p>Informa a capacidade de processamento de operações por parte do Terminal, face à evolução tecnológica registada na rede nacional.</p> <p>Os códigos de versão de especificações dos TPAs até à 10 correspondem a capacidades do tipo 1, superiores a 20 correspondem a capacidades do tipo 2. Os códigos de versão de especificações dos CAs 7.xx correspondem a capacidade do tipo 1, superiores a 8.00 correspondem a capacidades do tipo 2.</p> <p>As capacidades 3 e 4 são para terminais <i>contactless</i>.</p>	<p>0 - Terminal sem capacidades Euro/não aplicável</p> <p>1 - Terminal com capacidades Euro</p> <p>2 - Terminal com capacidades Euro e EMV</p> <p>3 - Terminal com capacidades Euro e EMV com e sem contacto</p> <p>4 - Terminal com contactless magnetic stripe</p>
2483	MSG_ACCCOD	CÓDIGO DE GESTÃO DA MENSAGEM	1	A		Código que determina a ação que a mensagem desenvolve.	<p>1 - Inserção</p> <p>2 - Consulta</p> <p>3 - Alteração</p> <p>4 - Abate</p> <p>5 - Confirmação</p> <p>6 - Alteração Método Autenticação</p> <p>7-Inserir adiantamento</p> <p>8-Altera-adiantamento/promotor</p> <p>9-Abate-adiantamento</p> <p>I - Inativar</p> <p>A - Ativar</p> <p>P - Principal</p>

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
3361	MSG_RESTXT_LI2	TEXTO RESPOSTA	45	A		Texto preenchido pela SIBS. Numa mensagem aceite com informações que completam os dados da operação. Numa mensagem recusada com os textos que justificam a recusa para o cliente. (versão do atributo (0472) MSG_RESTXT)	
3390	EXT_IBA	IBAN (INTERNATIONAL BANK ACCOUNT NUMBER)	34	A		Versão expandida do número de conta nacional (por ex., NIB para Portugal), utilizado internacionalmente para identificar inequivocamente a conta de um cliente numa Instituição Financeira. O IBAN funciona segundo o princípio do "envelope", sendo formado pelo código de país (dois caracteres - letras), pelo <i>check digit</i> (dois caracteres - números) mais o número de conta nacional (até 30 caracteres alfanuméricos - 0-9, A-Z (apenas maiúsculas), sem separadores). No caso português é facilmente identificado por PT50 + NIB.	
4463	SIS_DTH_INI	DATA/HORA INÍCIO	14	N	AAAAMMDD HHMMSS	Identifica a data e hora de início a que foi produzida a informação.	
4464	SIS_DTH_FIM	DATA/HORA FIM	14	N	AAAAMMDD HHMMSS	Identifica a data e hora fim a que foi produzida a informação.	
5402	CAR_PANA03	PRIMARY ACCOUNT NUMBER	19	A		Número completo do cartão encostado à esquerda. Formato no âmbito da norma ISO 7812-1.	
8106	EXT_TLMNUMN03	NÚMERO DE TELEMÓVEL	11	N		Campo que identifica o número de telemóvel,	
8119	SEE_MAXLIM	LIMITE MAXIMO DIARIO	7	N		Indica o montante máximo que o Cliente pode usar diariamente.	
8121	SEE_SELD SG	DESIGNACAO DO ALIAS	150	A		Designação do Alias (ex. mail, telemóvel, matrícula, etc...)	
8128	SEE_IDEOPR	IDENTIFICACAO DA OPERACAO NO SERVICO	30	A		Identifica as operações efetuadas através do Serviço.	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
8129	SEE_OPRDAT	DATA DA OPERACAO NO SERVICO	14	N		Data em que foi efetuada a operação através do Serviço.	
8130	SEE_SELTIPI	TIPO DE ALIAS	3	N		Identifica o Tipo de Alias associado ao Serviço.	001 - MSISDN; 002 - Mail; 003 – Matrícula; 004 – ID Box; 006 - Telemóvel; 007 - CAP; 008 - ID APP; 010 - Merchant User Token. Nota: O valor 005 encontra-se descontinuado.
8135	CHV_HASA01	SECURE HASH	64	A		Secure Hash com SHA256	
8146	TRM_ATT CODA01	TIPO DE AUTENTICAÇÃO	2	A		Identifica o tipo de autenticação da operação. Trata-se de um campo composto	1º dígito (instrumento) 0 - sem indicação 1 - c/leitura pista cartão (P2 ou P2 e 3 ou P1 no estrangeiro) 2 - key entered (introdução manual dados cartão) 3 - sem leitura do cartão 4 - c/leitura chip cartão (track2 equivalent data) 5 - c/leitura chip cartão (PAN+Data exp.+Seq.) 6 - c/leitura apenas da pista 2 de cartão com vertente MB em CA MB 7 - Fallback para pista (transação decidida sobre pista por não ter sido possível leitura dos dados do chip) 8 - Contactless Chip 9 - Contactless Pista 2º dígito (autorização)

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
							0 - sem indicação 1 - c/PIN 2 - c/assinatura 3 - Mail/telephone 4 - Telecódigo/telemóvel 5 - Pagamento Internet/MBNET 6 - s/PIN 7 - PIN Offline ou Pin Offline com assinatura 8 - MBNet / 3D Secure 9 - PIN Supervisor
8192	MSG_OCOIND	INDICADOR DE OCORRÊNCIAS	1	N		Indica se há mais ocorrências além das listadas.	
8195	SEE_SELCD	CÓDIGO DO ALIAS	10	N		Código de Identificação do Alias	
8196	SEE_TIPCD	CÓDIGO DO TIPO DE SERVIÇO	2	N		Código do tipo de Serviço da Plataforma Multi-Serviços.	01 - MB WAY; 02 - 3D Secure; 03 – P2P Lite 04 - Blocking Service; 05 – Authentication Value; 06 - Envio PIN; 07 - MB WAY Parceiro.
8200	EXT_TLMPRX	PREFIXO DE TELEMÓVEL	7	N		Prefixo de telemóvel para números nacionais e internacionais	
8226	SEE_NUMCARA01	NUMERO DO CARTAO NO SERVICO	40	A		Identifica o Cartão na Plataforma Multi-Serviços (Hexadecimal).	
8227	COM_SERIDEA01	IDENTIFICADOR DO SERVIÇO	40	A		Identificador único do Serviço na Plataforma de Pagamentos Móveis (Hexadecimal).	
8282	COM_ADIOPE	DADOS ADICIONAIS DA OPERAÇÃO	250	A		Identifica os dados adicionais da operação financeira.	
8435	SEE_OBSP2P	OBSERVACOES DO P2P	250	A		Observações sobre o Pagamento P2P.	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
8436	SEE_RESCOD	CODIGO DO RESULTADO DO PROCESSAMENTO DO P2P	2	N		Código do resultado do processamento do pagamento P2P.	10 - Aceite 20 - Pendente Adesão 30 - Pendente Aceitação 90 - Rejeitada
8440	SEE_P2PSIT	SITUACAO DO PAGAMENTO P2P	2	N		Situação em que se encontra o pagamento P2P.	10 - Pendente Adesão 20 - Pendente Aceitação 30 - Aceite 40 - Rejeitada 50 - Realizada 60 - Recusada 70 - Expirada 80 - Cancelada 90 - Removida
9116	SEE_MNTLSC	MONTANTE DE LEVANTAMENTO SEM CARTÃO	5	N		Montante referente a Levantamento sem Cartão MB WAY.	
9156	CHV_SPKA01	SIBS PUBLIC KEY	512	A		Atributo que contém a chave pública para a cifra.	
9157	CHV_INIVTR	VECTOR DE INICIALIZAÇÃO	32	A		Atributo que contém o parâmetro de cifra Vetor de Inicialização.	
9158	CHV_REFLSC	REFERÊNCIA DE LEVANTAMENTO SEM CARTÃO	32	A		Atributo que contém a Referência de Levantamento sem Cartão, cifrada.	
9163	SEE_SITLSC_REF	SITUAÇÃO DA REFERÊNCIA DE LEVANTAMENTO SEM CARTÃO MB WAY	3	N		Atributo que informa qual a situação da referência de levantamento sem cartão MB WAY.	'000' – Ativa; '001' – Geração de Referência Rejeitada; '002' – Registada; '003' – Cancelada; '004' – Rejeitada; '005' – Expirada; '006' – Realizada.

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
9164	SEE_DURSGN	DURAÇÃO EM SEGUNDOS	9	N		Atributo que contém a duração em segundos da referência para Levantamento MB WAY.	
9868	SEE_EPTCOD	CÓDIGO DE PARTICIPANTE EXTERNO	9	N		Atributo que identifica o Código de Participante Externo.	
9870	SEE_APLCOD	CÓDIGO DE APLICAÇÃO	2	N		Atributo que identifica o Código da Aplicação do Participante Externo.	
9872	SEE_ACCTIPN01	TIPO DE ACÇÃO A EXECUTAR	1	N		Atributo que identifica se a operação pendente deve ser aceite ou rejeitada.	0 - Rejeição; 1 - Aceitação.
9895	TOK_SMS	TOKEN SMS	7	A		Atributo que acolhe um token enviado por SMS.	
9974	SEE_ATVCOD_SDK	CÓDIGO DE ATIVAÇÃO DO SDK	7	A		Código de Ativação que será usado para ativar o SDK numa nova App de MB WAY Parceiro	
9982	TOK_SMSIND	INDICADOR DE TOKEN SMS	1	N		Atributo que indica se é necessário o Token enviado por SMS.	0 - Não é necessário; 1 - É necessário.
10213	SEE_RQMTIP	TIPO DE INTERVENIENTE NO REQUEST MONEY	1	A		Atributo que indica o tipo de intervenção que o utilizador teve no Request Money.	D - Destinatário do Request Money; O - Ordenante do Request Money.
10270	SEE_SITOPRA01	ESTADO DA OPERAÇÃO	3	A		Estado da Operação MB WAY.	CAN - Cancelada; EXP - Expirada; PND - Pendente; REJ - Rejeitada.
10308	SEE_IDEOPR_NTV	IDENTIFICAÇÃO DE INTERVENIENTE NA OPERAÇÃO	30	A		Atributo que identifica univocamente o interveniente numa operação específica.	

4 *User Experience – Regras e Guidelines*

4.1 Apresentação

Este documento congrega um **conjunto de *user experience guidelines*** - recomendações de usabilidade, design e interação, **para as operações MB WAY**.

Estas orientações visam:

1. **auxiliar as equipas de design e desenvolvimento** dos bancos na implementação das funcionalidades MB WAY nas suas *apps*, *homebanking* ou outras plataformas digitais;
2. **garantir que um utilizador tem uma experiência agradável e consistente**, quer efetue uma operação MB WAY (um levantamento de dinheiro, por exemplo) na *app* MB WAY, na *mobile banking app* no *homebanking* ou noutra plataforma do seu banco.

As *guidelines* listadas no documento vão desde regras a cumprir, em âmbito de implementação pelo Emissor, a recomendações gerais, que ficam inteiramente ao critério das equipas. Refira-se ainda que, apesar de se pretender **fornecer uma experiência familiar aos utilizadores**, não se deseja de modo algum:

- desvirtuar ou restringir a filosofia de design e interação de cada *app/homebanking*;
- limitar a criatividade para utilização em contextos ou de formas distintas e inovadoras.

Para acompanhar a evolução da disponibilização das funcionalidades através de interfaces para os Bancos, este manual deve ser visto como um **documento vivo**; e deve ser atualizado sempre que necessário.

4.2 Princípios de *design*

O MB WAY é uma ferramenta que visa **ajudar as pessoas a pagarem bens e serviços** através um leque de operações que vão desde: a compra de algo numa loja via *Contactless*, ao levantamento de dinheiro num MULTIBANCO sem cartão, até à criação de cartões virtuais MB NET para pagar um serviço *on-line*.

4.2.1 Orientação ao contexto móvel

O MB WAY é uma solução fundamentalmente ***mobile oriented*** e que tenta tirar partido das características únicas dos dispositivos móveis: acesso à lista de contactos, câmara, antena NFC, etc.

Como base para muitas operações está o **número de telemóvel**, e a **lista de contactos do telemóvel** do utilizador. Por exemplo, para enviar dinheiro.

Contudo, a maioria das funcionalidades, são passíveis de implementação em outros contextos - web, *desktop*, *chatbots*,

4.2.2 Segmentação por passos

À semelhança do MULTIBANCO, pretende-se que o MB WAY seja **utilizado por um leque cada vez mais diversificado de utilizadores**, com conhecimentos, apetências e utilizações distintas e com diferentes graus de literacia informática ou financeira.

Como tal:

- As **transações** (na sua maioria, pagamentos) estão tipicamente **divididas por vários passos**. Cada passo tenta pedir ao utilizador apenas um item, como por exemplo, o montante a enviar a um amigo.
- Antes de validar uma operação, existe tipicamente um **ecrã de resumo** com todos os dados preenchidos pelo utilizador nos vários passos, com outros dados pré-preenchidos pelo MB WAY com valores expectáveis ou comuns, dados adicionais que o utilizador pode indicar caso o deseje, e informação adicional sobre a operação (ex.: custo).

4.2.3 Notificar eventos importantes

Envio de alertas (recorrendo a *push notifications*, listados numa eventual secção de notificações da interface e através do envio de SMS) para informar o utilizador de eventos importantes, como: confirmar um pagamento por MB WAY que está a fazer num site de e-commerce, aceitar um pedido de dinheiro do filho, ser informado que o código de levantamento que gerou expirou, entre outros.

4.3 Regras a considerar

A tabela abaixo apresenta as regras a considerar aquando da implementação das funcionalidades MB WAY em outros canais:

Regras	Tipo de regra	Descrição da regra
Regra 1	Movimento/Extratos	Sempre que nas listas de movimentos/extratos do banco seja permitido o acesso a detalhes, é obrigatório indicar nos detalhes das operações que a operação foi efetuada via MB WAY.
Regra 2	Explicação das funcionalidades	Explicar aos utilizadores como funciona cada uma das funcionalidades. Recomenda-se na primeira interação com a funcionalidade, podendo, no entanto, ser em qualquer outro momento que seja mais conveniente. Apresentação do logotipo do MB WAY junto a esta informação.
Regra 3	Logotipo MB WAY	O logotipo MB WAY deve ser aplicado nos ecrãs de confirmação de uma operação e nos ecrãs de explicação das funcionalidades
Regra 4	Designação de funcionalidade de pagamento	A designação a adotar para os pagamentos por <i>contactless</i> , QR Code e número de telemóvel é “Pagar com MB WAY”
Regra 5	Confirmação de pagamento – “Pagar com MB WAY”	<ul style="list-style-type: none">• Caso o pagamento tenha sido bem-sucedido, apresentar uma mensagem sobre o passo que deve ser tomado de seguida (exemplo, “Pago. — Recolha o ticket da loja”). É obrigatório incluir o logo do MB WAY.• Caso o pagamento não tenha sido bem-sucedido, apresentar uma mensagem sobre a razão do insucesso assim como instruções

Regras	Tipo de regra	Descrição da regra
		sobre o que deve ser feito de seguida (exemplo, “Ocorreu um erro de comunicação — por favor, tente novamente”). É obrigatório incluir o logo do MB WAY. <ul style="list-style-type: none"> Colocar o logo MB WAY no pedido de confirmação do pagamento, nos casos em que é utilizado o número de telemóvel como forma de pagamento. (exemplo, o utilizador coloca o número de telemóvel no site do comerciante e recebe uma push notification com um pedido de confirmação do pagamento. Esta confirmação tem que ter o logotipo MB WAY).
Regra 6	Execução da operação	Sempre que existe mensagem ao cliente sobre a execução da operação, é obrigatório incluir o logo do MB WAY. Este comportamento permite identificar que a funcionalidade é MB WAY.
Regra 7	Mensagens de erro	As mensagens de erro devem ser claramente identificadas e mostradas ao utilizador.

4.4 Guidelines gerais

Recomendações de arquitetura de informação, nomenclatura, notificações e iconografia.

4.4.1 Arquitetura de informação

A integração das funcionalidades MB WAY na arquitetura de informação das plataformas de cada banco deve ser efetuada em função da filosofia de design da *app* ou plataforma em questão, para garantir uma experiência consistente ao utilizador ao longo de todo o sistema.

4.4.1.1 Transações MB WAY

Deixamos ao critério de cada equipa a escolha de qual a melhor forma de incluir as funcionalidades MB WAY no seu sistema/aplicação. Assim, e apenas a título de exemplo, a funcionalidade “Enviar dinheiro”, tanto pode ser:

- um botão — diretamente no ecrã inicial da *app* do banco;
- um submenu — dentro de um menu “MB WAY” ou dentro de um menu “Transferências”;
- uma escolha — dentro de um formulário de fazer uma transferência.

4.4.1.2 Operações secundárias

Para além das operações financeiras em si (pagar por MB WAY, levantar dinheiro, etc.), também a arquitetura de informação de operações secundárias (cancelar códigos de levantamentos, consultar estados de pedidos de dinheiro, etc.), fica à liberdade de cada banco, caso deseje implementar este tipo de operações.

4.4.2 Nomenclatura

Recomendações para nomes das operações, dados, e outros conceitos MB WAY.

4.4.2.1 Transações MB WAY

As operações começam todas por verbos. Ex.: “Pagar”, “Levantar”, “Criar”:

- “Enviar dinheiro”;
- “Pedir dinheiro”;
- “Dividir conta”;
- “Pagar com MB WAY”;
- “Levantar dinheiro”.

O logo MB WAY deve estar presente em todas as funcionalidades ao longo da *app*.

	Nomenclatura da funcionalidade	Nomenclatura a apresentar nos movimentos do cartão
Transferências	Enviar dinheiro 	TRF MB WAY
	Pedir dinheiro 	
	Dividir conta 	
Compras	Pagar 	No caso das compras NFC: COMP contactless MB WAY
		No caso das compras QR Code: COMP QR Code MB WAY
		No caso das compras remotas: COMP MB WAY
Levantamentos sem cartão	Levantar dinheiro 	LEV MB WAY

Figura 7 - Nomenclatura MB WAY

Alterações a esta nomenclatura são aceitáveis em casos onde seja importante manter uma consistência com a nomenclatura da *app/homebanking*. Por exemplo: “Enviar dinheiro” poderá ser “Transferir por MB WAY”, caso esta opção seja implementada dentro da área de transferências.

4.4.2.2 Nos movimentos/extratos

Recomendamos:

- Enviar e receber dinheiro - utilizar a nomenclatura idêntica à utilizada no banco para uma transferência;
- Pagamentos com MB WAY - utilizar a mesma nomenclatura utilizada no banco para compras com outros tipos de pagamentos e compras;
- Levantamentos MB WAY - utilizar a nomenclatura idêntica à de um levantamento com cartão.

Regra: Caso nas listas de movimentos/extratos permitam o acesso a detalhes, **é obrigatório** indicar nos detalhes das operações que a operação foi efetuada via MB WAY.

Estas são as designações a adotar para os movimentos:

- Transferências - **TRF MB WAY**;
- Compras NFC - **COMP *contactless* MB WAY**;
- Compras QR Code - **COMP QR Code MB WAY**;
- Compra Remota - **COMP MB WAY**;
- Levantamentos - **LEV MB WAY**.

4.4.2.3 Outros

Transversal a todo o MB WAY são utilizados os termos:

- “Valor” - para referir montantes. Ex.: transferir 20€ entre contas.
- “Dinheiro” - para referir um “fundo” ou uma quantidade monetária.
- “De” e “Para” – em vez de termos com “destinatário”, por exemplo.
- “Custo” - preço/comissão das operações.
- “Receber em” e “Pagar de” – em vez dos termos tipo “crédito” ou “débito”.
- “Descrição” - utilizado para o utilizador descrever ou adicionar notas as operações (que podem ficar visíveis em tanto para o utilizador como para o destinatário da transferência, por exemplo).
- “Cancelar” – Para interromper operações. Ex.: cancelar um código de levantamento gerado.

Podem ser utilizados outros termos em casos onde seja importante manter uma consistência com a nomenclatura da *app/homebanking*.

4.4.3 Notificações

Recomendamos notificar o utilizador (por *push notification*, ou outra forma de alerta apropriado) sempre que existam:

- **Operações sobre as quais seja necessária uma ação** - por exemplo: aceitar ou recusar um pedido de dinheiro, confirmar uma compra, etc.
- **Outros eventos relevantes para o utilizador** - por exemplo: um familiar enviou-lhe dinheiro, todos os amigos pagaram a divisão de conta do jantar, um código de levantamento expirou, etc.

Recomendamos evitar sobrecarregar o utilizador com notificações fora do contexto *core* da aplicação.

4.4.4 Iconografia

As principais operações MB WAY têm, cada uma, um ícone representativo. Os ícones visam ajudar a distinguir mais rapidamente as operações:

- quer no momento em que são efetuadas;
- quer nas listas de histórico e notificações.









Enviar dinheiro 	Um avião de papel.	
Pedir dinheiro 	Balão de fala com símbolo do euro.	
Pagar 	Símbolo do euro	
Levantar dinheiro 	Uma nota a sair do MULTIBANCO	

Figura 8 - Ícones representativos das operações MB WAY

Alguns ícones podem ter algumas variantes, nomeadamente para representar:

- **estados de operações** (ex.: pedido pendente, envio recusado, etc.)
- **a orientação da operação** (ex: enviar dinheiro e receber dinheiro tem o mesmo ícone, mas com o avião de papel a apontar em direções opostas).

A utilização ou a não utilização de ícones junto das operações deve ser decidido por cada equipa, em função da filosofia de design de cada *app/homebanking*.

- Os ícones podem ser ajustados em termos de design e cores de forma a ficarem consistentes com o sistema iconográfico da *app/homebanking*.
- Os ícones podem também ser substituídos por outro ícone - em casos de ícones similares já estarem a ser utilizados para outras operações - desde que seja mantida a ideia que se pretende transmitir com o ícone.

4.5 Enviar dinheiro

Descrição da funcionalidade: O objetivo desta funcionalidade é permitir a uma pessoa enviar dinheiro para um contato de forma imediata.

Nomenclatura: “Enviar dinheiro MB WAY” ou similar.



Figura 9 - Funcionalidade “Enviar Dinheiro”

4.5.1 Primeira experiência

Regra: Explicar aos utilizadores como funciona o envio de dinheiro. Recomenda-se na primeira interação, podendo, no entanto, ser em qualquer outro momento que seja mais conveniente. Exemplo:

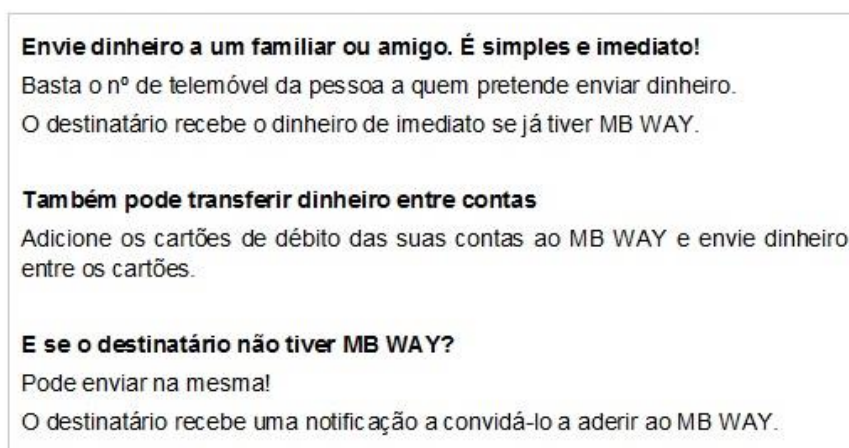


Figura 10 - Como funciona o “Envio de Dinheiro”

Regra: Apresentação do logotipo do MB WAY junto a esta informação.

4.5.2 Enviar

Na lista de contactos, distinguir os contactos MB WAY dos restantes.

Caso o destinatário não seja ainda MB WAY, recomendamos informá-lo sobre como pode aderir ao MB WAY — via MULTIBANCO ou através da *app* MB WAY.

4.6 Pedir dinheiro

Descrição da funcionalidade: Solicitar um envio de dinheiro de forma imediata a um contacto MB WAY. Útil para um utilizador pedir dinheiro a um amigo que lhe ficou a dever um almoço.

Nomenclatura obrigatória: “Pedir dinheiro”.



Figura 11 - Funcionalidade “Pedir Dinheiro”

4.6.1 Primeira experiência

Regra: Explicar aos utilizadores como funciona o pedido de dinheiro. Recomenda-se na primeira interação, podendo, no entanto, ser em qualquer outro momento que seja mais conveniente. Exemplo:

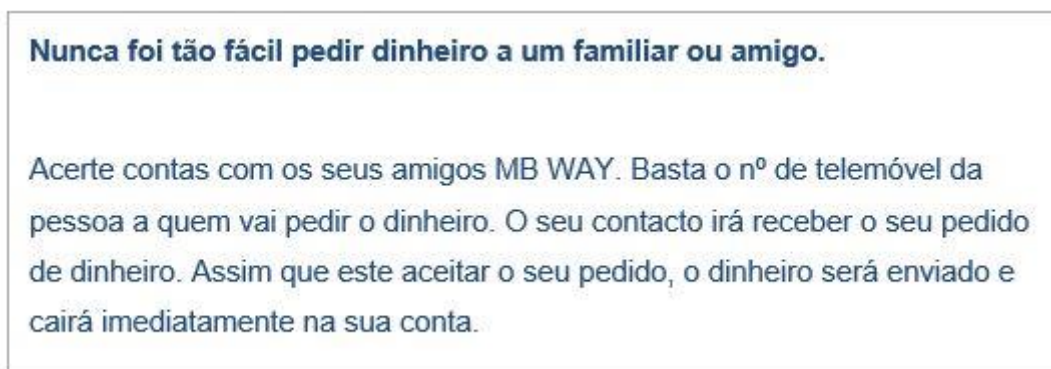


Figura 12 - Como funciona o “Pedido de Dinheiro”

Regra: Apresentação do logotipo do MB WAY junto a esta informação.

4.6.2 Pedir

Na lista de contactos, distinguir os contactos MB WAY dos restantes.

Caso o contacto a quem se pretende pedir dinheiro não seja ainda MB WAY, sugerimos que o utilizador seja convidado a enviar um SMS ao seu contacto, a incentivá-lo a aderir ao MB WAY — via MULTIBANCO ou através da app MB WAY.

4.7 Pagar com MB WAY

Descrição da funcionalidade: Pagar utilizando apenas o telemóvel — via *Contactless* em smartphones android com antena NFC ou pagamento por QR-Code, para as lojas físicas. No caso das lojas on-line é possível fazer o pagamento MB WAY usando o número de telemóvel.

Nomenclatura obrigatória: “Pagar com MB WAY”




	Funcionalidade agrupada de Pagar com MB WAY que poderá, posteriormente, ter um pagamento <i>contactless</i> e/ou pagamento com QR Code após o acesso.	€
	Pagamento <i>contactless</i> : Deve indicar o icon <i>contactless</i>	
	Pagamento com QR Code: Deve indicar o icon QR Code.	

Figura 13 - Funcionalidade “Pagar com MB WAY”

4.7.1 Primeira experiência

Regra: Explicar aos utilizadores como funciona o pagamento por MB WAY nomeadamente a sua aplicação *on-line* e em lojas físicas e as suas variantes (via *contactless*, QR Code ou número de telemóvel). Recomenda-se na primeira interação, podendo, no entanto, ser em qualquer outro momento que seja mais conveniente.

Exemplo:

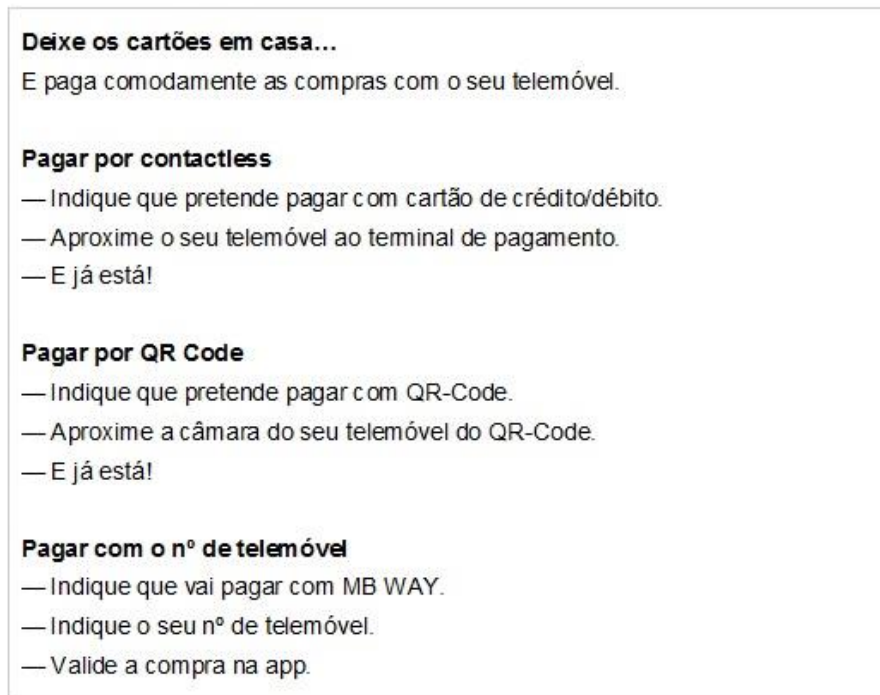


Figura 14 - Como funciona o “Pagamento com MB WAY”

Regra: Apresentar junto desta informação, o logotipo do MB WAY.

4.7.2 Pagar

Após a escolha por parte do utilizador do tipo de pagamento, indicar instruções sucintas sobre como deve proceder para os pagamentos *contactless* MB WAY, QR Code e por número de telemóvel, após terem sido selecionados. Apresentar juntamente com esta informação, o logo do MB WAY.

Regra: Caso o pagamento tenha sido bem sucedido, apresentar uma mensagem sobre o passo que deve ser tomado de seguida (exemplo, “Pago. — Recolha o ticket da loja”). É obrigatório incluir o logo do MB WAY.

Regra: Caso o pagamento não tenha sido bem-sucedido, apresentar uma mensagem sobre a razão do insucesso assim como instruções sobre o que deve ser feito de seguida (exemplo, “Ocorreu um erro de comunicação — por favor, tente novamente”). É obrigatório incluir o logo do MB WAY.

Regra: Colocar o logo MB WAY no pedido de confirmação do pagamento, nos casos em que é utilizado o número de telemóvel como forma de pagamento. (exemplo, o utilizador coloca o número de telemóvel no site do comerciante e recebe uma *push notification* com um pedido de confirmação do pagamento. Esta confirmação tem que ter o logotipo MB WAY).

4.8 Levantar dinheiro

Descrição da funcionalidade: Permite fazer um levantamento de dinheiro num MULTIBANCO sem ter de introduzir um cartão, tirando partido de um código de 10 dígitos previamente gerado.

Nomenclatura: “Levantar dinheiro”



Figura 15 - Funcionalidade “Levantar dinheiro”

4.8.1 Casas decimais

Os montantes levantados devem ser sempre apresentados sem casas decimais. Ex: 10€, 150€, etc.

4.8.2 Primeira experiência

Regra: Explicar aos utilizadores como funciona o levantamento de dinheiro. Recomenda-se na primeira interação, podendo, no entanto, ser em qualquer outro momento que seja mais conveniente. Exemplo:

Levante dinheiro no Multibanco sem cartão.
Precisa de levantar dinheiro mas não tem a carteira consigo?

Gere um código de levantamento no MB WAY.
É válido por 30 minutos.

Num Multibanco à sua, escolha, prima o botão Verde.

Introduza o código de levantamento, e já está!
Basta seguir as instruções do Multibanco.

Figura 16 - Como funciona o “Levantamento de Dinheiro

Regra: Apresentar junto desta informação, o logotipo do MB WAY.

4.8.3 Gerar um código

Para gerar um código o utilizador deve indicar a quantia a levantar e a conta/cartão de onde pretende efetuar o débito.

Exibir ao utilizador informação sobre o limite: 200€/levantamento. Indicar que o valor tem de ser um múltiplo de 10€.

4.8.4 Código de levantamento

O código de levantamento tem 10 dígitos. Recomenda-se:

- Formatar o código em grupos de 3 dígitos, com um espaço entre os grupos. Exemplo: 810 085 233 4;
- Apresentar junto ao código, o montante a levantar;
- É obrigatória a apresentação do logotipo do MB WAY junto ao código de levantamento e respetivo montante. Exemplo:



Figura 17 - Código de Levantamento

4.8.5 Ajuda

Ponderar indicar ao utilizador que o código pode ser utilizado noutro MULTIBANCO caso o MULTIBANCO onde se tenha dirigido não possua dinheiro.

Ponderar notificar o utilizador (por *push notification* ou na secção de notificações, caso exista) quando um código de levantamento expira e quando é utilizado.

Ponderar permitir ao utilizador cancelar códigos de utilização criados.

4.9 Utilizar MULTIBANCO

Descrição da funcionalidade: Permite que o Banco disponibilize aos seus clientes a possibilidade de utilizarem a *app* do Banco como alternativa ao cartão bancário, para acederem às funcionalidades do MULTIBANCO.

Nomenclatura: "Utilizar MULTIBANCO".

Utilizar MULTIBANCO 	Símbolo representativo de uma chave.	
---	--------------------------------------	---

Figura 18 – Funcionalidade “Utilizar MULTIBANCO”

4.9.1 Primeira experiência

Regra: Explicar aos utilizadores como funciona a Utilização do MULTIBANCO através da *app* do Banco. Recomenda-se na primeira interação, podendo, no entanto, ser em qualquer outro momento que seja mais conveniente. Exemplo:

Aceda ao MULTIBANCO através da *app* do Banco

Prima a tecla verde num Caixa Automático (CA) da Rede MULTIBANCO e seleccione a opção “Utilizar MULTIBANCO”. No ecrã do CA é apresentado um QR Code. Abra a *App* do Banco no seu *smartphone* e leia o QR Code. Siga os passos indicados pela aplicação. Em seguida o CA é desbloqueado e poderá efetuar as operações que pretender.

Figura 19 - Como funciona a opção “Utilizar MULTIBANCO”

Anexo A. Algoritmo *Diffie-Hellman*

A solução Levantamento MB WAY realizada através da *app* MB WAY assegura a confidencialidade do código de levantamento através de uma cifra aplicacional utilizando o algoritmo AES, entre a componente central *Security Manager* (SM) e a *app*. Esta cifra aplicacional utiliza uma chave AES dinâmica para cada interação com a *app*.

O canal *Host-to-Host* (H2H) utilizado para transportar o código de levantamento entre a SIBS FPS e o Emissor não contempla atualmente mecanismos que assegurem a confidencialidade da informação através de cifra aplicacional. Os mecanismos de confidencialidade existentes no canal H2H são assegurados unicamente pelo canal de comunicações, através de um túnel IPSEC entre os equipamentos periféricos de comunicações da SIBS FPS e do Banco.

Dada a criticidade elevada do código de levantamento e o risco de comprometimento durante o transporte, é gerada uma chave secreta (dinâmica) entre a SIBS FPS e o Emissor para a cifra aplicacional dos elementos das mensagens H2H que contêm um código de Levantamento válido através de uma variante do algoritmo *Diffie-Hellman* baseada na norma ANSI X9.42 (RFC 2631 *Diffie-Hellman Key Agreement Method*).

O *Diffie-Hellman* é um algoritmo de *key agreement* através do qual ambas as partes obtêm um mesmo segredo partilhado, de forma que o segredo não ficará disponível a quem estiver a escutar o canal de comunicações. O segredo partilhado é transformado numa chave simétrica através de um processo definido na norma ANSI X9.42.

O documento NIST *Special Publication 800-56A Revision 2*⁴ resume um conjunto de *schemes* para o processo de *key agreement*. Neste anexo são definidos os detalhes e opções de implementação que são adotados pela funcionalidade Levantamento MB WAY.

A.1. Requisitos

- ***Cryptographic Hash Functions***

Onde seja requerido a utilização de uma função de *hash*, deve ser sempre utilizado o algoritmo SHA-256.

- ***Random Number Generation***

A geração de números aleatórios deve ser realizada através de algoritmos aprovados de acordo com o normativo NIST *Special Publication 800-90A Revision 1*.

- ***Domain Parameters***

A geração dos pares de chaves Pública/Privada de cada entidade é realizada de acordo com um conjunto particular de *Domain Parameters*: *p* (*prime number*) e *g* (*generator of the cyclic subgroup*).

⁴ <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf>

Considere-se os seguintes *Domain Parameters* para utilização nos ambientes não produtivos:

- Valores dos parâmetros codificados em ASN.1 (DER *encoded*):

```
-----BEGIN DH PARAMETERS-----
MIIBCAKCAQEAgdTdGS6CTznBymOstYi9RLAFxTlmy2R54me7GNJ8xhp2mehsOc+X
7WumynmESW+JH+ISVK/L6Ku/PHiharwawvsSdJ3rf6gjVWGdlD66Cww9lMbX2BQs
Qku2pmNLTMzLib6TIgI+973RSmPr5dBXQ/ZEd5ObgnCpfldv13/p0YESILP2SGHB
5Y54Qeasq/oBAd5K9tYFLIwTkK3kUHTmMPMNkZgYMRkpJ7V6ShrKOBAYH6CeeUE
UmYZpEfQkyr5mQMr55G8/U4uwgUXYWzPb7n7DaiAKSTm++gUa3NhQHELY54dmAzW
GrmmMOqh0Q2GdDcUwWCJD9veVj14aVACCwIBAg==
-----END DH PARAMETERS-----
```

- Os parâmetros *p* (*prime*) e *g* (*generator*) acima indicados são, respetivamente:

DH Parameters: (2048 bit)

prime:

```
00:81:d4:c3:19:2e:82:4f:39:c1:ca:63:ac:b5:88:
bd:44:b0:05:c5:3d:66:cb:64:79:e2:67:bb:18:d2:
7c:c6:1a:76:99:e8:6c:39:cf:97:ed:6b:a6:ca:79:
84:49:6f:89:1f:e2:12:54:af:cb:e8:ab:bf:3c:78:
a1:6a:bc:1a:c2:fb:12:74:9d:eb:7f:a8:23:55:61:
9d:94:3e:ba:0b:0c:3d:94:c6:d7:d8:14:2c:42:4b:
b6:a6:63:4b:4c:cc:cb:89:be:93:22:02:3e:f7:bd:
d1:4a:63:eb:e5:d0:57:43:f6:44:77:93:9b:82:70:
a9:7e:57:6f:97:7f:e9:d1:81:12:20:b3:f6:48:61:
c1:e5:8e:78:41:e6:ac:ab:fa:01:01:de:4a:f6:d6:
05:2c:8c:13:90:ad:e4:50:74:e6:30:f3:0d:91:98:
18:31:19:29:27:b5:7a:4a:1a:ca:38:10:04:60:7e:
82:79:e5:04:52:66:19:a4:47:d0:93:2a:f9:99:03:
2b:e7:91:bc:fd:4e:2e:c2:05:17:61:6c:cf:6f:b9:
fb:0d:a8:80:29:24:e6:fb:e8:14:6b:73:61:40:71:
25:63:9e:1d:98:0c:f0:1a:b9:a6:30:ea:a1:d1:0d:
86:74:37:14:c1:60:89:0f:db:de:56:39:78:69:50:
02:0b
```

generator: 2 (0x2)

Estes parâmetros são definidos pela SIBS FPS e distribuídos pelas Instituições Financeiras numa fase inicial de *setup*, através de um canal *out-of-band*.

- Key-Derivation Methods for Key-Agreement Schemes*

O processo para a derivação da chave simétrica a partir do segredo compartilhado (Z) deve seguir o método *Single-step Key-Derivation* (seção 5.8.1, NIST 800-56A Revision 2), utilizando a Opção 1 para a definição da função H (*Option 1*: $H(x) = \text{hash}(x)$).

O campo *OtherInfo* deve ser definido de acordo com a seguinte concatenação de valores:

AlgorithmID || PartyUInfo || PartyVInfo

- *AlgorithmID* – Campo que indica a forma como o material criptográfico derivado será obtido (*parsed*) e qual o algoritmo utilizado pela chave secreta derivada (AES).
- *PartyUInfo* – Identificador associado a cada Instituição Financeira.
- *PartyVInfo* – Identificador associado à SIBS FPS.

O valor obtido no processo de derivação (*DerivedKeyingMaterial*) será uma chave AES-128 para a cifra aplicacional do(s) Código(s) de Levantamento transmitidos pela SIBS FPS na mensagem H2H (*keydatalen* = 128 bits).

Como parâmetros da cifra devem ser definidos: *Initialization Vector (IV)* = 16 bytes determinados aleatoriamente e com o IV enviado na mensagem, deve ser utilizado o modo CBC (*Cipher Block Chaining*) e o método de *padding* deverá ser PKCS#7.

- *Key-Agreement*

Deve ser usado o seguinte *scheme* para *key-agreement*, sendo gerado pela SIBS FPS e Banco um par de chaves a cada nova interação (*ephemeral key pair*), não sendo usadas chaves estáticas.

Category	Subcategory	Primitive	Scheme	Notation
C(2e)	C(2e, 0s)	FFC DH	dhEphem	C(2e, 0s, FFC DH)

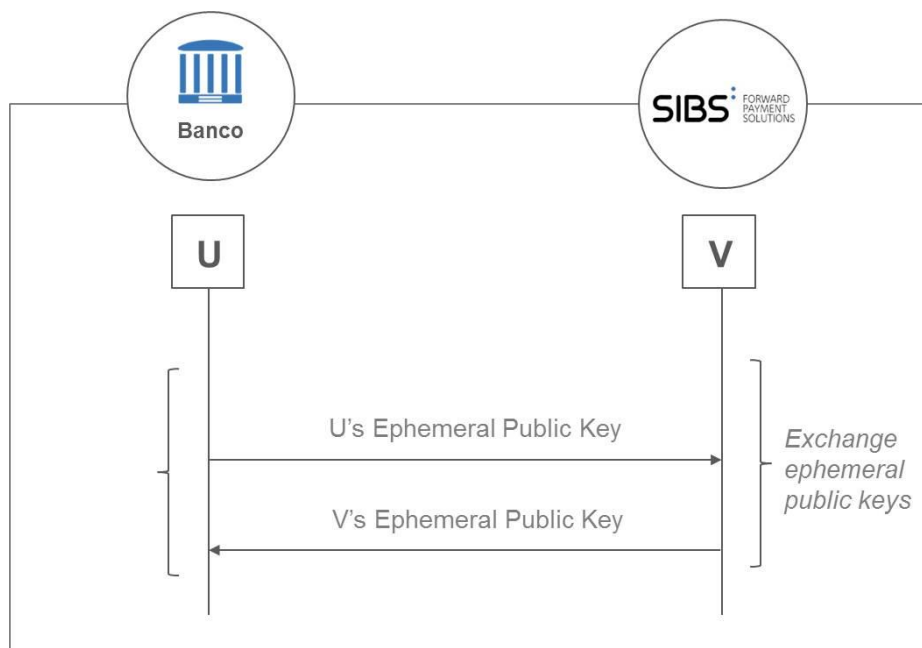


Figura 20 - C(2e, 0s) schemes: each party contributes only and ephemeral key pair

A.1.1 Exemplo

Exemplo de computação do segredo compartilhado (Z) entre duas entidades, utilizando os *Domain Parameters* definidos anteriormente. Cada entidade gera o seu par de chaves (Pública/Privada), exporta a sua chave Pública que é transmitida ao outro interlocutor e calcula o segredo compartilhado a partir da sua chave Privada e da chave Pública que recebeu do outro interlocutor.

Para a produção do exemplo, foi utilizado o utilitário OpenSSL (1.0.2k 26 Jan 2017).

```
===== View DH Group =====
C:\TEMP\dh\dh-group-2048>openssl pkeyparam -in dh-group-2048.pem -text
-----BEGIN DH PARAMETERS-----
MIIBCAKCAQEAgdTDGS6CTznBymOstYi9RLAFxT1my2R54me7GNJ8xhp2mehsOc+X
7WumynmESW+JH+ISVK/L6Ku/PHiharwawvsSdJ3rf6gjVWGdlD66Cww9lMbX2BQs
Qku2pmNLTmzLib6TIgI+973RSmPr5dBXQ/ZEd5ObgnCpfldv13/p0YESILP2SGHB
5Y54Qeasq/oBAd5K9tYFLIwTkK3kUHTmMPMNkZgYMRkpJ7V6ShrKOBAYH6CeeUE
UmYZpEfQkyr5mQMr55G8/U4uwgUXYWzPb7n7DaiAKSTm++gUa3NhQHElY54dmAzW
GrmmMOqh0Q2GdDcUwWCJD9veVj14aVACCwIBAg==
-----END DH PARAMETERS-----
```

DH Parameters: (2048 bit)

prime:

```
00:81:d4:c3:19:2e:82:4f:39:c1:ca:63:ac:b5:88:
bd:44:b0:05:c5:3d:66:cb:64:79:e2:67:bb:18:d2:
7c:c6:1a:76:99:e8:6c:39:cf:97:ed:6b:a6:ca:79:
84:49:6f:89:1f:e2:12:54:af:cb:e8:ab:bf:3c:78:
a1:6a:bc:1a:c2:fb:12:74:9d:eb:7f:a8:23:55:61:
9d:94:3e:ba:0b:0c:3d:94:c6:d7:d8:14:2c:42:4b:
b6:a6:63:4b:4c:cc:cb:89:be:93:22:02:3e:f7:bd:
d1:4a:63:eb:e5:d0:57:43:f6:44:77:93:9b:82:70:
a9:7e:57:6f:97:7f:e9:d1:81:12:20:b3:f6:48:61:
c1:e5:8e:78:41:e6:ac:ab:fa:01:01:de:4a:f6:d6:
05:2c:8c:13:90:ad:e4:50:74:e6:30:f3:0d:91:98:
18:31:19:29:27:b5:7a:4a:1a:ca:38:10:04:60:7e:
82:79:e5:04:52:66:19:a4:47:d0:93:2a:f9:99:03:
2b:e7:91:bc:fd:4e:2e:c2:05:17:61:6c:cf:6f:b9:
fb:0d:a8:80:29:24:e6:fb:e8:14:6b:73:61:40:71:
25:63:9e:1d:98:0c:f0:1a:b9:a6:30:ea:a1:d1:0d:
86:74:37:14:c1:60:89:0f:db:de:56:39:78:69:50:
02:0b
```

generator: 2 (0x2)

===== Generate Private/Public Key (#1) =====

C:\TEMP\dh\dh-group-2048>openssl pkey -in dhkey_1.pem -text -noout

DH Private-Key: (2048 bit)

private-key:

```
7a:03:63:98:eb:93:ea:92:c0:22:b6:7d:4d:84:b5:
e8:69:f8:08:db:5a:5a:22:81:31:25:fa:8d:9c:ff:
1f:41:44:c0:8c:a7:9a:59:1e:c9:5a:91:79:b3:c9:
69:95:0d:d9:51:9a:98:4c:d2:c8:14:d4:f6:17:88:
47:b6:95:c2:c3:4a:52:61:ff:68:52:ed:1e:ac:6e:
d3:44:a2:88:c2:b8:54:39:23:00:08:39:06:e2:76:
1d:eb:4d:21:91:83:bf:d8:58:1f:f0:4f:0e:b4:3f:
a3:8f:d9:49:f7:45:42:76:ae:0c:a8:22:2d:02:79:
6a:5f:76:af:ca:d4:d7:86:9f:82:a6:11:bb:14:08:
fa:e4:f8:44:cb:0d:ba:6c:c1:04:74:67:a4:78:0c:
80:5e:25:35:d1:e9:e7:9d:53:ea:82:e5:c6:df:7d:
50:19:65:e5:14:04:cc:17:1b:39:55:86:48:11:28:
dd:4b:63:fb:66:fe:35:90:47:b1:51:84:34:9e:d6:
03:80:15:a5:e4:c3:c6:31:a4:2f:26:27:a6:6c:99:
98:cd:23:23:7c:7b:b8:da:b2:83:ed:e1:fa:1f:5e:
3a:8b:64:93:fb:23:c8:10:f7:2d:05:e2:df:ad:16:
1a:64:fb:13:b3:68:07:a7:07:27:78:a4:d5:87:73:
ba
```

public-key:

```
1e:a5:15:09:92:e1:b8:f7:19:43:fc:7d:e2:76:c7:
0d:ca:71:6e:3a:07:09:d0:3a:ce:fd:55:76:ff:f3:
34:bb:10:14:b5:3c:38:62:f0:7a:ce:68:d4:69:5b:
de:43:64:3c:1b:51:29:40:5b:cd:13:77:d3:79:85:
96:15:74:d2:fd:e7:3a:b5:37:7e:a4:f5:23:95:b4:
53:e9:ff:15:11:90:40:0b:28:a9:dd:00:b4:99:67:
66:3a:d0:81:7c:ec:bb:fe:86:b3:1d:03:3a:d3:d5:
66:ca:02:44:8a:40:5a:14:7d:21:7a:53:14:4e:07:
ce:4b:8c:32:1d:ce:43:c5:b1:8d:60:12:49:5b:c7:
3f:81:d7:74:fd:d1:da:3c:da:79:04:94:77:b6:61:
c8:16:ad:9c:6f:25:1a:4e:96:ad:45:b4:63:3a:36:
39:d6:3c:12:5e:86:19:7c:6d:94:82:1e:89:71:58:
4f:06:50:ea:34:f0:ac:40:b0:16:fa:ac:c7:85:44:
```

```
c8:28:39:58:30:a8:29:af:0a:3b:d2:7d:f9:a7:ab:
64:7f:14:ce:40:ac:b1:b1:f8:00:34:37:da:2a:6d:
3f:7e:4a:33:58:c9:09:fd:6c:ad:e2:bd:f5:ce:1a:
cb:b2:3e:90:6d:29:64:f5:35:cc:63:63:83:c8:22:
33
prime:
00:81:d4:c3:19:2e:82:4f:39:c1:ca:63:ac:b5:88:
bd:44:b0:05:c5:3d:66:cb:64:79:e2:67:bb:18:d2:
7c:c6:1a:76:99:e8:6c:39:cf:97:ed:6b:a6:ca:79:
84:49:6f:89:1f:e2:12:54:af:cb:e8:ab:bf:3c:78:
a1:6a:bc:1a:c2:fb:12:74:9d:eb:7f:a8:23:55:61:
9d:94:3e:ba:0b:0c:3d:94:c6:d7:d8:14:2c:42:4b:
b6:a6:63:4b:4c:cc:cb:89:be:93:22:02:3e:f7:bd:
d1:4a:63:eb:e5:d0:57:43:f6:44:77:93:9b:82:70:
a9:7e:57:6f:97:7f:e9:d1:81:12:20:b3:f6:48:61:
c1:e5:8e:78:41:e6:ac:ab:fa:01:01:de:4a:f6:d6:
05:2c:8c:13:90:ad:e4:50:74:e6:30:f3:0d:91:98:
18:31:19:29:27:b5:7a:4a:1a:ca:38:10:04:60:7e:
82:79:e5:04:52:66:19:a4:47:d0:93:2a:f9:99:03:
2b:e7:91:bc:fd:4e:2e:c2:05:17:61:6c:cf:6f:b9:
fb:0d:a8:80:29:24:e6:fb:e8:14:6b:73:61:40:71:
25:63:9e:1d:98:0c:f0:1a:b9:a6:30:ea:a1:d1:0d:
86:74:37:14:c1:60:89:0f:db:de:56:39:78:69:50:
02:0b
generator: 2 (0x2)
```

===== Generate Private/Public Key (#2) =====

C:\TEMP\dh\dh-group-2048>openssl pkey -in dhkey_2.pem -text -noout

DH Private-Key: (2048 bit)

private-key:

```
61:7e:94:56:9f:ba:1e:a3:3f:8f:d9:1c:f2:28:bf:
01:3f:44:1e:2b:8f:fa:02:f5:6b:c0:61:50:bd:6b:
59:56:b0:64:6d:ed:b8:58:e5:39:82:67:cd:8d:39:
93:d2:e7:fa:26:eb:8c:62:e4:8e:3e:c0:1d:15:53:
45:70:61:35:f8:37:43:a2:31:c2:e9:a9:cc:d3:5e:
62:ec:7d:ff:42:3d:c1:ea:6d:2d:ce:f5:be:dc:d2:
60:07:89:be:25:dd:35:eb:ec:01:10:2b:e0:14:85:
06:0b:55:8a:0b:9b:9a:3a:1b:53:d3:81:00:b5:ec:
5e:7f:40:3b:f6:1d:24:e1:2e:88:72:89:e1:99:b5:
00:93:65:25:0a:69:6d:e5:7a:27:31:a4:15:b3:21:
67:e7:d2:c8:75:a7:0f:3f:d1:a7:6e:0c:18:31:99:
6e:07:8e:bf:22:af:eb:0a:ec:59:56:73:cc:d4:6e:
77:70:60:70:91:01:1b:c7:e4:b8:df:a4:d2:8e:d7:
98:fd:e2:22:8b:02:04:26:d8:fe:11:fe:5b:e5:84:
ec:92:be:2b:fd:95:89:be:ec:c3:28:fe:8f:98:f0:
0c:c3:38:47:3f:1d:6b:f5:e6:20:44:e5:26:79:81:
80:9f:a8:be:5e:ae:15:82:a8:7f:3d:38:81:3d:bf:
49
```

public-key:

```
1b:58:18:d7:79:e3:ef:31:ac:4d:ae:3e:b3:e9:2b:
f0:1d:60:ed:21:d4:4c:d4:c9:27:d9:35:6a:92:c3:
93:57:a6:47:10:78:66:c9:0f:a0:c3:21:19:7a:e7:
bb:89:46:92:f8:71:23:7b:e5:56:3d:87:1d:4e:ae:
a3:46:db:d0:4d:20:5d:9c:86:b7:61:0e:a6:46:2c:
11:35:9d:a5:bd:38:ca:42:74:01:c6:e9:d9:de:f7:
ad:ae:b1:62:9c:53:be:ef:d4:57:c3:d0:d8:aa:54:
71:b8:98:69:23:93:93:0f:64:c2:fa:09:83:67:34:
84:5f:ed:a7:e4:24:aa:f3:2f:01:6c:95:16:56:63:
```



```

9f:a6:70:c0:27:c0:e6:2c:8e:a4:9e:a6:c4:af:d3:
bd:11:c5:90:8f:16:d7:63:b8:65:82:41:a2:72:f4:
18:57:26:8d:46:fd:e3:be:4f:58:3f:a2:2c:24:92:
41:03:de:e4:6a:76:ec:41:23:80:fc:2e:2c:e7:58:
4f:90:b6:7b:82:b2:80:13:d6:8e:ed:c8:ad:2a:80:
5d:a6:d0:a8:75:42:8f:b0:73:77:49:fa:7e:17:c6:
c2:56:2a:d9:8b:ae:fd:54:1d:a8:a7:af:a3:af:05:
83:a9:13:0b:19:32:5e:42:f6:ba:da:cb:48:7b:55:
2e
prime:
00:81:d4:c3:19:2e:82:4f:39:c1:ca:63:ac:b5:88:
bd:44:b0:05:c5:3d:66:cb:64:79:e2:67:bb:18:d2:
7c:c6:1a:76:99:e8:6c:39:cf:97:ed:6b:a6:ca:79:
84:49:6f:89:1f:e2:12:54:af:cb:e8:ab:bf:3c:78:
a1:6a:bc:1a:c2:fb:12:74:9d:eb:7f:a8:23:55:61:
9d:94:3e:ba:0b:0c:3d:94:c6:d7:d8:14:2c:42:4b:
b6:a6:63:4b:4c:cc:cb:89:be:93:22:02:3e:f7:bd:
d1:4a:63:eb:e5:d0:57:43:f6:44:77:93:9b:82:70:
a9:7e:57:6f:97:7f:e9:d1:81:12:20:b3:f6:48:61:
c1:e5:8e:78:41:e6:ac:ab:fa:01:01:de:4a:f6:d6:
05:2c:8c:13:90:ad:e4:50:74:e6:30:f3:0d:91:98:
18:31:19:29:27:b5:7a:4a:1a:ca:38:10:04:60:7e:
82:79:e5:04:52:66:19:a4:47:d0:93:2a:f9:99:03:
2b:e7:91:bc:fd:4e:2e:c2:05:17:61:6c:cf:6f:b9:
fb:0d:a8:80:29:24:e6:fb:e8:14:6b:73:61:40:71:
25:63:9e:1d:98:0c:f0:1a:b9:a6:30:ea:a1:d1:0d:
86:74:37:14:c1:60:89:0f:db:de:56:39:78:69:50:
02:0b
generator: 2 (0x2)

```

```
===== Export Public Key (#1) =====
C:\TEMP\dh\dh-group-2048>openssl pkey -pubin -in dhp_1.pem -text
-----BEGIN PUBLIC KEY-----
MIICJDCCARcGCSqGSIb3DQEDATCCAQgCggEBAIHUwxkugk85wcpjrLWivUSwBcU9
ZstkeeJnuxjSfMYadpnobDnPl+1rpsp5hElviR/iElSvy+irvzx4oWq8GsL7EnSd
63+oI1VhnZQ+ugsMPZTG19gULEJLtgZjS0zMy4m+kyICPve90Upj6+XQV0P2RHeT
m4JwqX5Xb5d/6dGBEiCz9khweWOeEHmrKv6AQHeSvbWBSyME5Ct5FB05jDzDZGY
GDEZKSelekoayjgQBGB+gnnlBFJmGaRH0JMq+ZkDK+eRvP1OLsIFF2Fsz2+5+w2o
gCkk5vvoFGtzYUBxJWoeHZgM8Bq5pjDqodENhnQ3FMFgiQ/b3lY5eG1QAgsCAQID
ggEFAAKCAQAepRUJkuG49x1D/H3idscNynFuOgcJ0DrO/VV2//M0uxAUtTw4YvB6
zmjUaVveQ2Q8G1EpQFvNE3fTeYWWFXTS/ec6tTd+pPUjlbRT6f8VEZBACyip3QC0
mWdmOtCBfOy7/oazHQM609VmygJEikBaFH0helMUTgfOS4wyHc5DxbGNYBJJW8c/
gdd0/dHaPNp5BJR3tmHIFq2cbyUaTpatRbRjOjY51jwSXoYZfG2Ugh6JcVhPB1Dq
NPCsQLAW+qzHhUTIKD1YMKgprwo70n35p6tkfxTOQKyxsfGANDfaKm0/fkozWMkK
/Wyt4r31zhrLsj6QbSlk9TXMY2ODyCIz
-----END PUBLIC KEY-----
DH Public-Key: (2048 bit)
  public-key:
    1e:a5:15:09:92:e1:b8:f7:19:43:fc:7d:e2:76:c7:
    0d:ca:71:6e:3a:07:09:d0:3a:ce:fd:55:76:ff:f3:
    34:bb:10:14:b5:3c:38:62:f0:7a:ce:68:d4:69:5b:
    de:43:64:3c:1b:51:29:40:5b:cd:13:77:d3:79:85:
    96:15:74:d2:fd:e7:3a:b5:37:7e:a4:f5:23:95:b4:
    53:e9:ff:15:11:90:40:0b:28:a9:dd:00:b4:99:67:
    66:3a:d0:81:7c:ec:bb:fe:86:b3:1d:03:3a:d3:d5:
    66:ca:02:44:8a:40:5a:14:7d:21:7a:53:14:4e:07:
    ce:4b:8c:32:1d:ce:43:c5:b1:8d:60:12:49:5b:c7:
    3f:81:d7:74:fd:d1:da:3c:da:79:04:94:77:b6:61:
```



```

c8:16:ad:9c:6f:25:1a:4e:96:ad:45:b4:63:3a:36:
39:d6:3c:12:5e:86:19:7c:6d:94:82:1e:89:71:58:
4f:06:50:ea:34:f0:ac:40:b0:16:fa:ac:c7:85:44:
c8:28:39:58:30:a8:29:af:0a:3b:d2:7d:f9:a7:ab:
64:7f:14:ce:40:ac:b1:b1:f8:00:34:37:da:2a:6d:
3f:7e:4a:33:58:c9:09:fd:6c:ad:e2:bd:f5:ce:1a:
cb:b2:3e:90:6d:29:64:f5:35:cc:63:63:83:c8:22:
33
prime:
00:81:d4:c3:19:2e:82:4f:39:c1:ca:63:ac:b5:88:
bd:44:b0:05:c5:3d:66:cb:64:79:e2:67:bb:18:d2:
7c:c6:1a:76:99:e8:6c:39:cf:97:ed:6b:a6:ca:79:
84:49:6f:89:1f:e2:12:54:af:cb:e8:ab:bf:3c:78:
a1:6a:bc:1a:c2:fb:12:74:9d:eb:7f:a8:23:55:61:
9d:94:3e:ba:0b:0c:3d:94:c6:d7:d8:14:2c:42:4b:
b6:a6:63:4b:4c:cc:cb:89:be:93:22:02:3e:f7:bd:
d1:4a:63:eb:e5:d0:57:43:f6:44:77:93:9b:82:70:
a9:7e:57:6f:97:7f:e9:d1:81:12:20:b3:f6:48:61:
c1:e5:8e:78:41:e6:ac:ab:fa:01:01:de:4a:f6:d6:
05:2c:8c:13:90:ad:e4:50:74:e6:30:f3:0d:91:98:
18:31:19:29:27:b5:7a:4a:1a:ca:38:10:04:60:7e:
82:79:e5:04:52:66:19:a4:47:d0:93:2a:f9:99:03:
2b:e7:91:bc:fd:4e:2e:c2:05:17:61:6c:cf:6f:b9:
fb:0d:a8:80:29:24:e6:fb:e8:14:6b:73:61:40:71:
25:63:9e:1d:98:0c:f0:1a:b9:a6:30:ea:a1:d1:0d:
86:74:37:14:c1:60:89:0f:db:de:56:39:78:69:50:
02:0b
generator: 2 (0x2)

```

```
===== Export Public Key (#2) =====
C:\TEMP\dh\dh-group-2048>openssl pkey -pubin -in dhpub_2.pem -text
-----BEGIN PUBLIC KEY-----
MIICJDCCARcGCSqGSIb3DQEBQgCggEBAIHUwxkugk85wcpjrLWIVUSwBcU9
ZstkeeJnuxjSfMYadpnobDnPl+lrpsp5hElviR/iElSvy+irvzx4oWq8GsL7EnSd
63+oI1VhnZQ+ugsMPZTG19gULEJLtgZjS0zMy4m+kyICPve90Upj6+XQV0P2RHeT
m4JwqX5Xb5d/6dGBEiCz9khhwEWOeEHmrKv6AQHeSvbWBSyME5Ct5FB05jDzDZGY
GDEZKSelekoayjgQBGB+gnnlBFJmGarH0JMq+ZkDK+eRvP1OLsIFF2Fsz2+5+w2o
gCkk5vvoFGtzYUBxJWOeHZgM8Bq5pjDgodENhnQ3FMFgiQ/b31Y5eG1QAgsCAQID
ggEFAAKCAQAbWBJXeePvMaxNrj6z6SvWHDtIdRM1Mkn2TVqksOTV6ZHEHhmyQ+g
wyEZeue7iUaS+HEje+VWPYcdTq6jRtvQTSBdnIa3YQ6mRiwRNZ21vTjKQnQBxunZ
3vetrrFinFO+79RXw9DYqlRxuJhpI5OTD2TC+gmDZzSEX+2n5CSq8y8BbJUWVmOf
pnDAJ8DmLI6knqbEr9O9EcWQjxbXY7hlgkGicvQYVyaNRv3jvk9YP6IsJJJBA97k
anbsQSOA/C4s51hPkLZ7grKAE9aO7citKoBdptCodUKPsHN3Sfp+F8bCVirZi679
VB2op6+jrwWDqRMLGTJeQva62stIeiUu
-----END PUBLIC KEY-----
DH Public-Key: (2048 bit)
    public-key:
        1b:58:18:d7:79:e3:ef:31:ac:4d:ae:3e:b3:e9:2b:
        f0:1d:60:ed:21:d4:4c:d4:c9:27:d9:35:6a:92:c3:
        93:57:a6:47:10:78:66:c9:0f:a0:c3:21:19:7a:e7:
        bb:89:46:92:f8:71:23:7b:e5:56:3d:87:1d:4e:ae:
        a3:46:db:d0:4d:20:5d:9c:86:b7:61:0e:a6:46:2c:
        11:35:9d:a5:bd:38:ca:42:74:01:c6:e9:d9:de:f7:
        ad:ae:b1:62:9c:53:be:ef:d4:57:c3:d0:d8:aa:54:
        71:b8:98:69:23:93:93:0f:64:c2:fa:09:83:67:34:
        84:5f:ed:a7:e4:24:aa:f3:2f:01:6c:95:16:56:63:
        9f:a6:70:c0:27:c0:e6:2c:8e:a4:9e:a6:c4:af:d3:
        bd:11:c5:90:8f:16:d7:63:b8:65:82:41:a2:72:f4:
```

```

18:57:26:8d:46:fd:e3:be:4f:58:3f:a2:2c:24:92:
41:03:de:e4:6a:76:ec:41:23:80:fc:2e:2c:e7:58:
4f:90:b6:7b:82:b2:80:13:d6:8e:ed:c8:ad:2a:80:
5d:a6:d0:a8:75:42:8f:b0:73:77:49:fa:7e:17:c6:
c2:56:2a:d9:8b:ae:fd:54:1d:a8:a7:af:a3:af:05:
83:a9:13:0b:19:32:5e:42:f6:ba:da:cb:48:7b:55:
2e
prime:
00:81:d4:c3:19:2e:82:4f:39:c1:ca:63:ac:b5:88:
bd:44:b0:05:c5:3d:66:cb:64:79:e2:67:bb:18:d2:
7c:c6:1a:76:99:e8:6c:39:cf:97:ed:6b:a6:ca:79:
84:49:6f:89:1f:e2:12:54:af:cb:e8:ab:bf:3c:78:
a1:6a:bc:1a:c2:fb:12:74:9d:eb:7f:a8:23:55:61:
9d:94:3e:ba:0b:0c:3d:94:c6:d7:d8:14:2c:42:4b:
b6:a6:63:4b:4c:cc:cb:89:be:93:22:02:3e:f7:bd:
d1:4a:63:eb:e5:d0:57:43:f6:44:77:93:9b:82:70:
a9:7e:57:6f:97:7f:e9:d1:81:12:20:b3:f6:48:61:
c1:e5:8e:78:41:e6:ac:ab:fa:01:01:de:4a:f6:d6:
05:2c:8c:13:90:ad:e4:50:74:e6:30:f3:0d:91:98:
18:31:19:29:27:b5:7a:4a:1a:ca:38:10:04:60:7e:
82:79:e5:04:52:66:19:a4:47:d0:93:2a:f9:99:03:
2b:e7:91:bc:fd:4e:2e:c2:05:17:61:6c:cf:6f:b9:
fb:0d:a8:80:29:24:e6:fb:e8:14:6b:73:61:40:71:
25:63:9e:1d:98:0c:f0:1a:b9:a6:30:ea:a1:d1:0d:
86:74:37:14:c1:60:89:0f:db:de:56:39:78:69:50:
02:0b
generator: 2 (0x2)

```

===== Calculate Secret (#1) =====

```
C:\TEMP\dh\dh-group-2048>openssl pkeyutl -derive -inkey dhkey_1.pem -peerkey dhpup_2.pem -out
secret_1.bin
```

===== Calculate Secret (#2) =====

```
C:\TEMP\dh\dh-group-2048>openssl pkeyutl -derive -inkey dhkey_2.pem -peerkey dhpup_1.pem -out
secret_2.bin
```

===== Shared Secret (Z) =====

```
(secret_1.bin = secret_2.bin)
```

```

1C 92 2F B8 12 7C 37 D5 86 BA 00 3C 3B E4 17 5C 78 2C 3C 2A 2D 76 63 12 B4 ED BE C9 26 84 B6 4C
87 0D 6E F2 20 A4 80 D2 29 8B 86 04 39 8D 3A 37 B9 87 A5 C7 93 51 5A 55 D7 E0 8D 6D D6 96 8C CC
24 C2 EF 9B 5C 40 58 72 40 16 FC E8 4F 4F 6E B2 84 31 0C 9B 98 C0 26 B5 7D 9D 88 00 67 3B 92 E9
1D 4C FA 7A 21 44 32 93 5F EB DB 2A D0 39 FA 95 7D 99 AE 6F 33 0B 0D 3C D7 87 6D 60 50 3D 83 A8
CE C3 B5 F2 87 47 EB B0 B4 04 4B 16 45 3B A6 DE F4 B6 96 57 B0 9D AF 30 A7 1A 5F 99 02 39 A0 53
69 9B 6F 20 BE 4D 16 4C 84 FA C1 42 F0 60 82 A5 A9 B9 0D 48 0E 50 10 32 E5 D7 E0 E8 C7 85 DF 6B
93 1E 84 3D DD A5 74 BB CC 09 EE 76 37 7E A0 2B 2F 4C 99 55 8A C9 E6 B8 DE E8 90 9C D2 EC EF B4
0E 0B CF 0C C7 33 18 44 EE 89 DA E0 25 43 AA EE 74 77 6E 38 79 6D 24 46 A5 46 9D 51 79 5B D8 9E

```

secret_1.bin																	
	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
000:	1C	92	2F	B8	12	7C	37	D5	86	BA	00	3C	3E	E4	17	5C	./... 7...<...;
010:	78	2C	3C	2A	2D	76	63	12	B4	ED	BE	C9	26	84	B6	4C	x,<*-vc...&...L
020:	87	0D	6E	F2	20	A4	80	D2	29	8B	86	04	39	8D	3A	37	.n...)...9:;7
030:	B9	87	A5	C7	93	51	5A	55	D7	E0	8D	6D	D6	96	8C	CCQZU...m...
040:	24	02	EF	9B	5C	40	58	72	4D	16	EC	E8	4F	4F	6E	B2	\$...\\@Xr@...00n.
050:	84	31	0C	9B	98	C0	26	B5	7D	9D	88	00	67	3B	92	E9	.1...&...}.g:...
060:	1D	4C	FA	7A	21	44	32	93	5F	EB	DB	2A	D0	39	FA	95	.Lz;lD2...)*.9...
070:	7D	99	AE	6F	33	0B	0D	3C	D7	87	6D	60	50	3D	83	A8	}.o3...<...m'P=...
080:	CE	C3	B5	F2	87	47	EB	B0	B4	04	4B	16	45	3B	A6	DEG...K.E:...
090:	F4	B6	96	57	B0	9D	AF	30	A7	1A	5F	99	02	39	A0	53	...W...0..._...9.S
0A0:	69	9B	6F	20	BE	4D	16	4C	B4	FA	C1	42	F0	6D	82	A5	i.o.M.L...B...`...
0B0:	A9	B9	0D	48	0E	50	10	32	E5	D7	E0	E8	C7	85	DF	6B	...H.P.2...)...k...
0C0:	93	1E	84	3D	DD	A5	74	BB	CC	09	EE	76	37	7E	A0	2B	...=.t...v7~.+...
0D0:	2F	4C	99	55	8A	C9	E6	B8	DE	E8	90	9C	D2	EC	EF	B4	/L.U...)...<...C...
0E0:	0E	0B	CF	0C	C7	33	18	44	EE	89	DA	E0	25	43	AA	EE3.D...)%C...
0F0:	74	77	6E	38	79	6D	24	46	A5	46	9D	51	79	5B	D8	9E	twngym\$F.F.Qy[...]

Anexo B. Fluxos de Suporte à Implementação

B.1. Registo do SDK

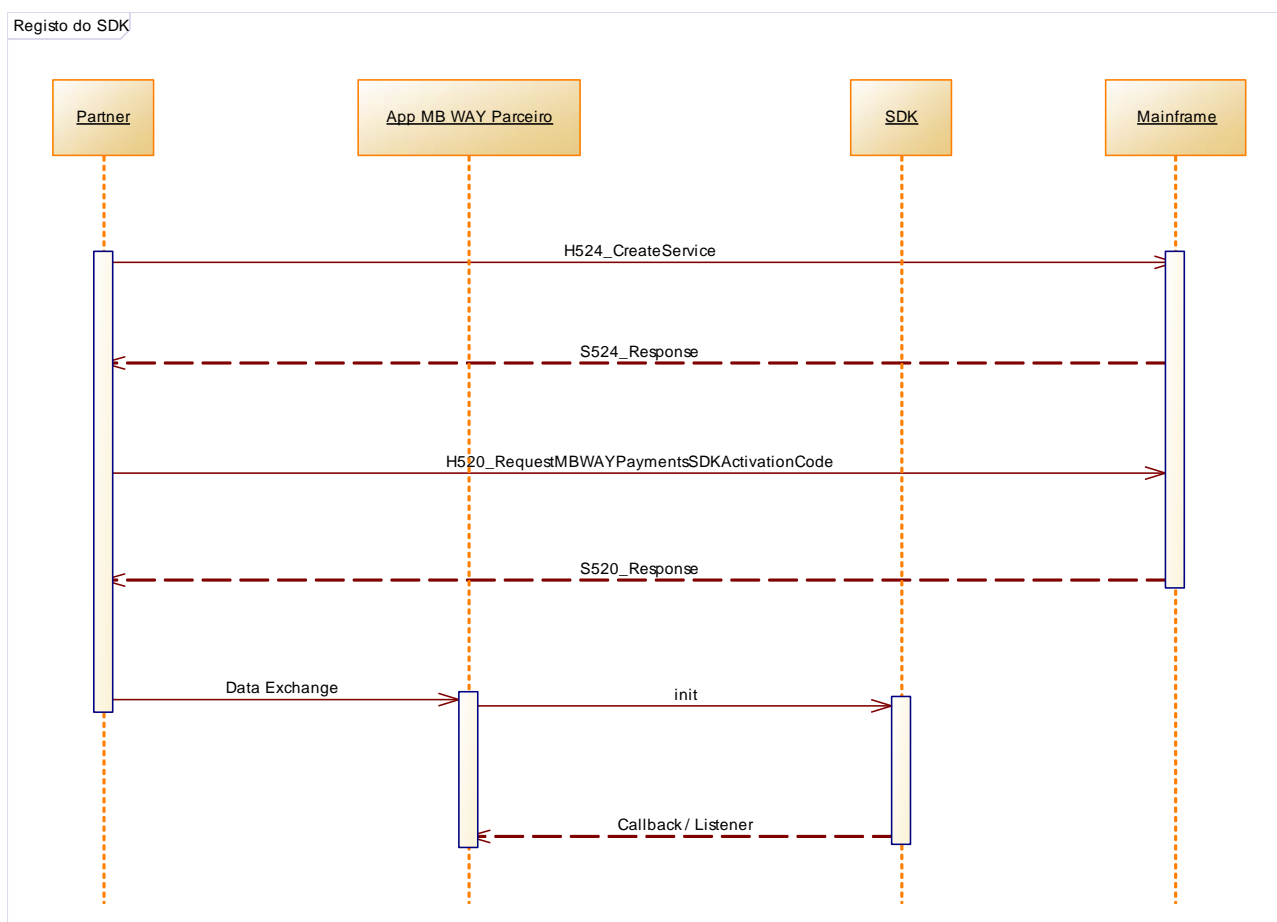


Figura 21 - Registo do SDK

B.2. Interfaces *AppParceiro* - SDK

B.2.1 Inicialização do SDK

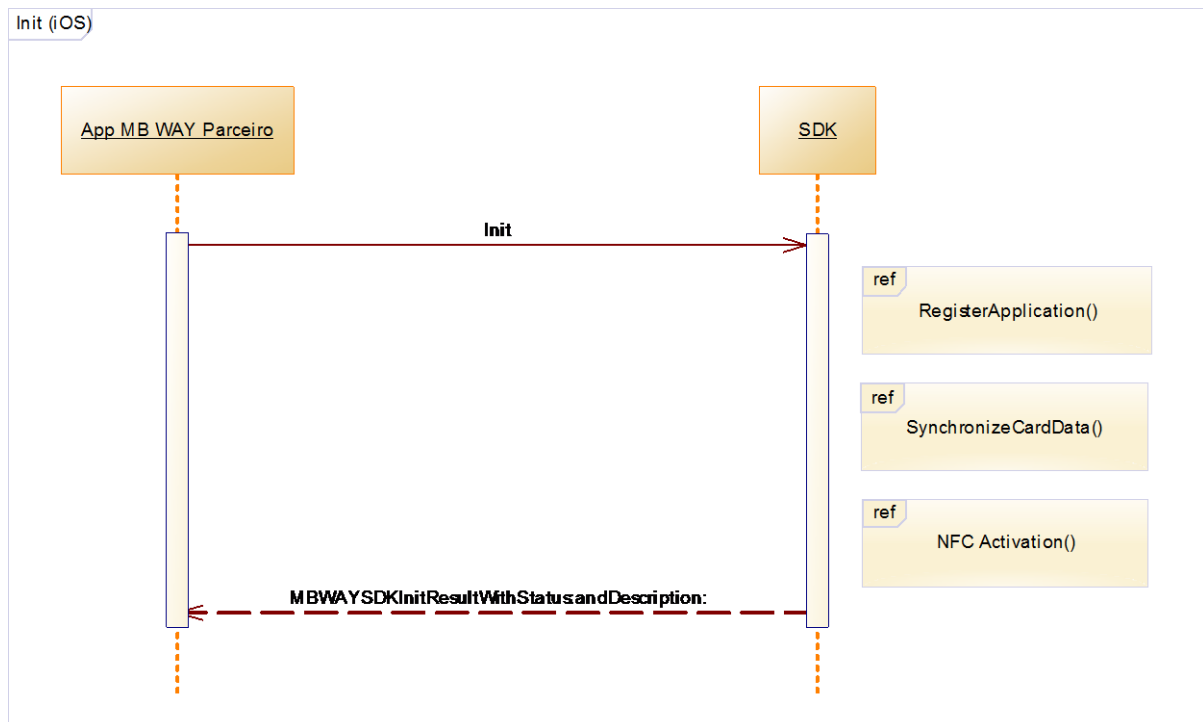


Figura 22 - Inicialização do SDK (iOS)

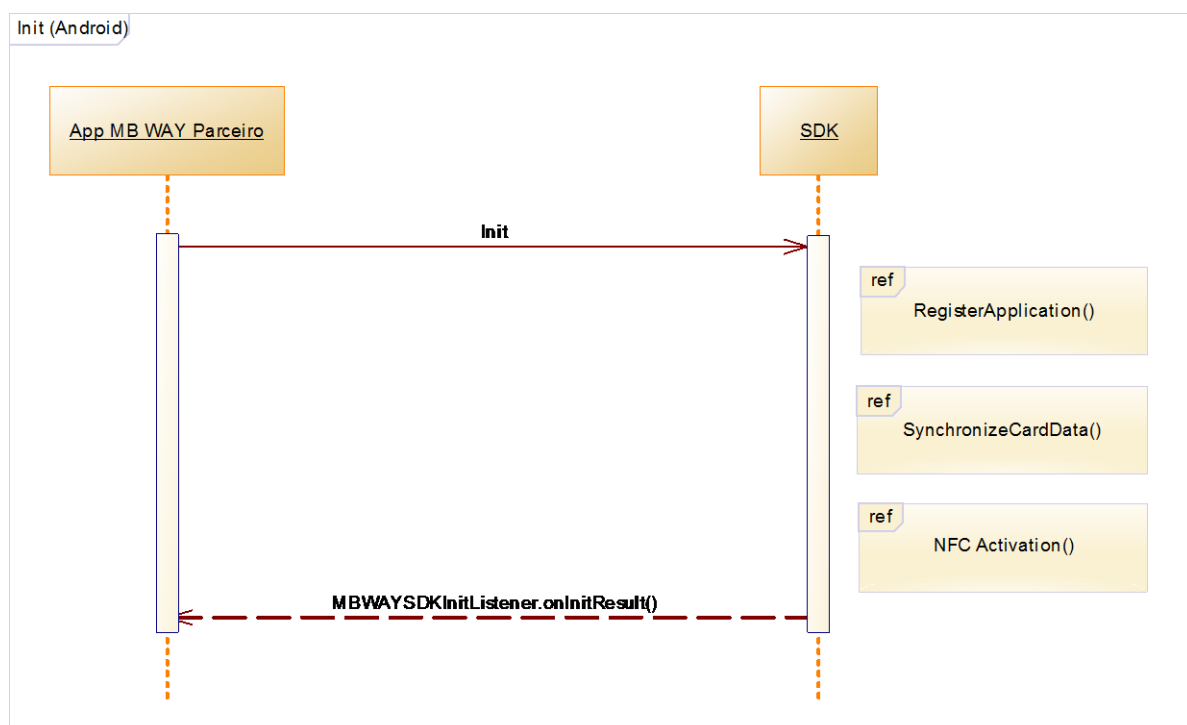


Figura 23 - Inicialização do SDK (Android)

B.2.2 Pesquisa de Operações Pendentes

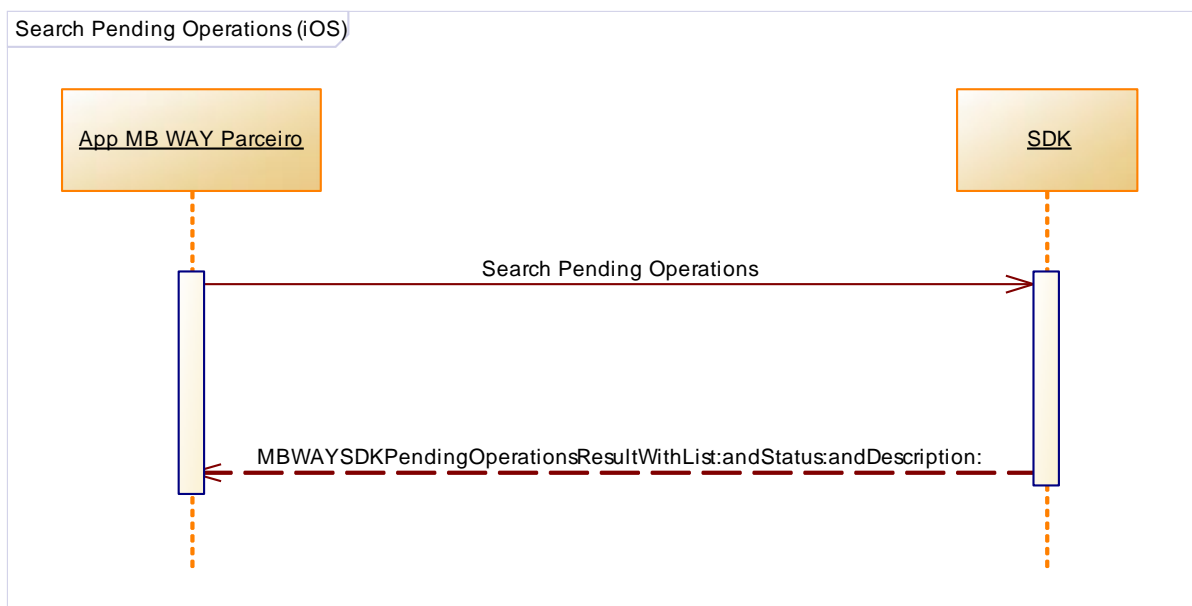


Figura 24 - Pesquisa de Operações Pendentes (iOS)

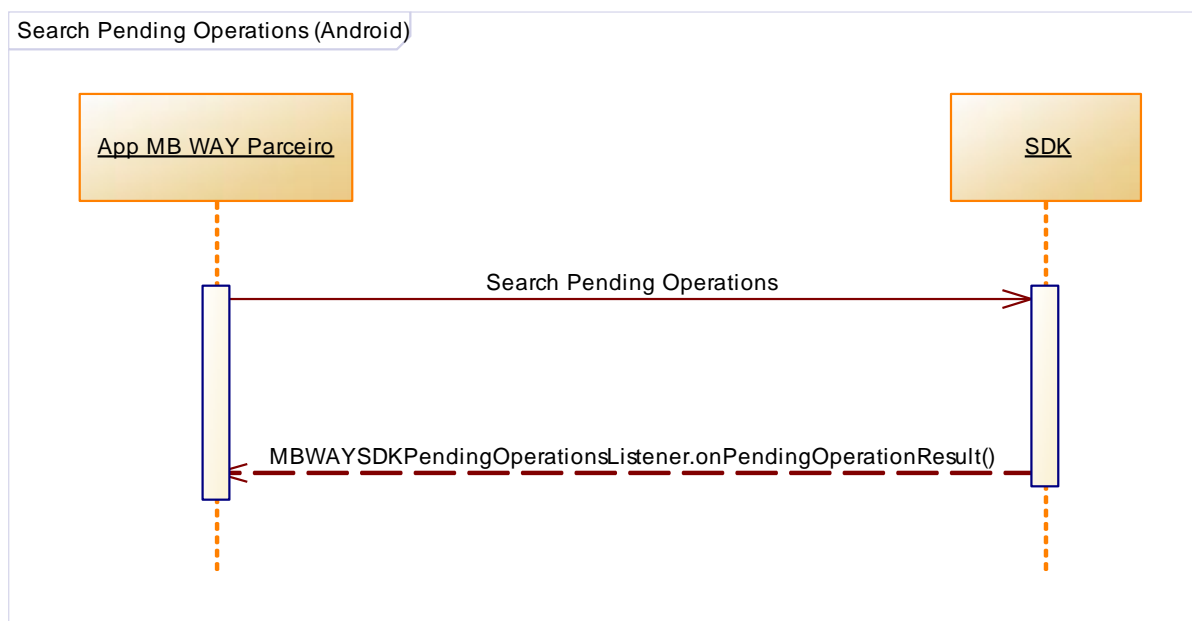


Figura 25 - Pesquisa de Operações Pendentes (Android)

B.2.3 Confirmação de uma Compra Pendente (Compra/Autorização)

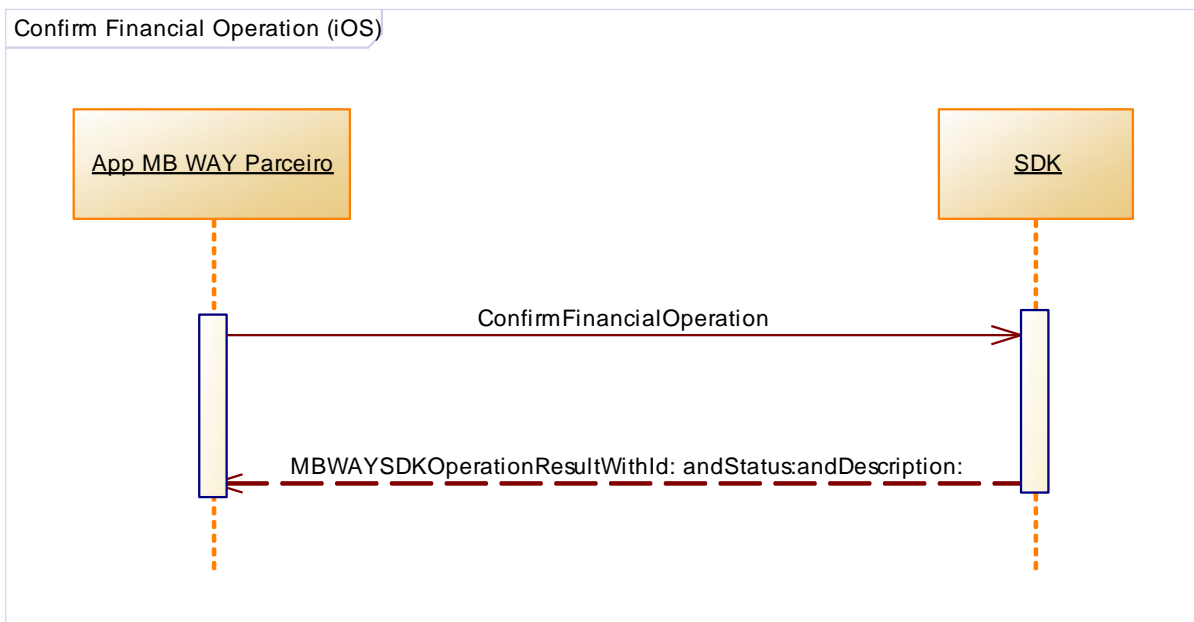


Figura 26 - Confirmação de uma Compra Pendente (iOS)

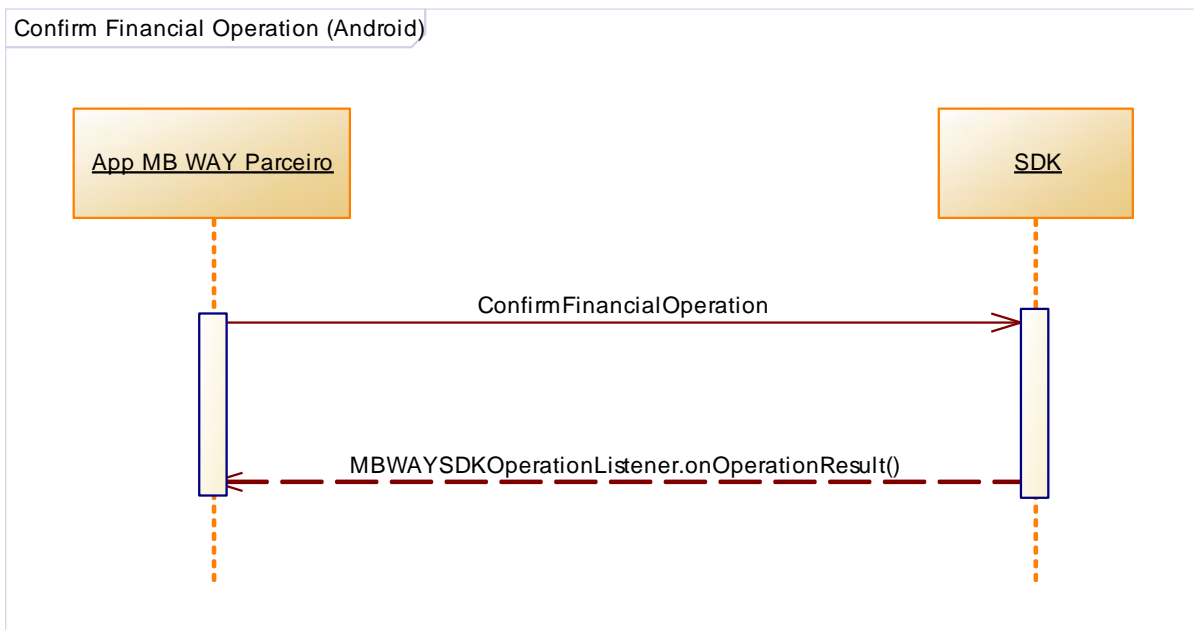


Figura 27 - Confirmação de uma Compra Pendente (Android)

B.2.4 Recusa de uma Operação Pendente (Compra/Autorização)

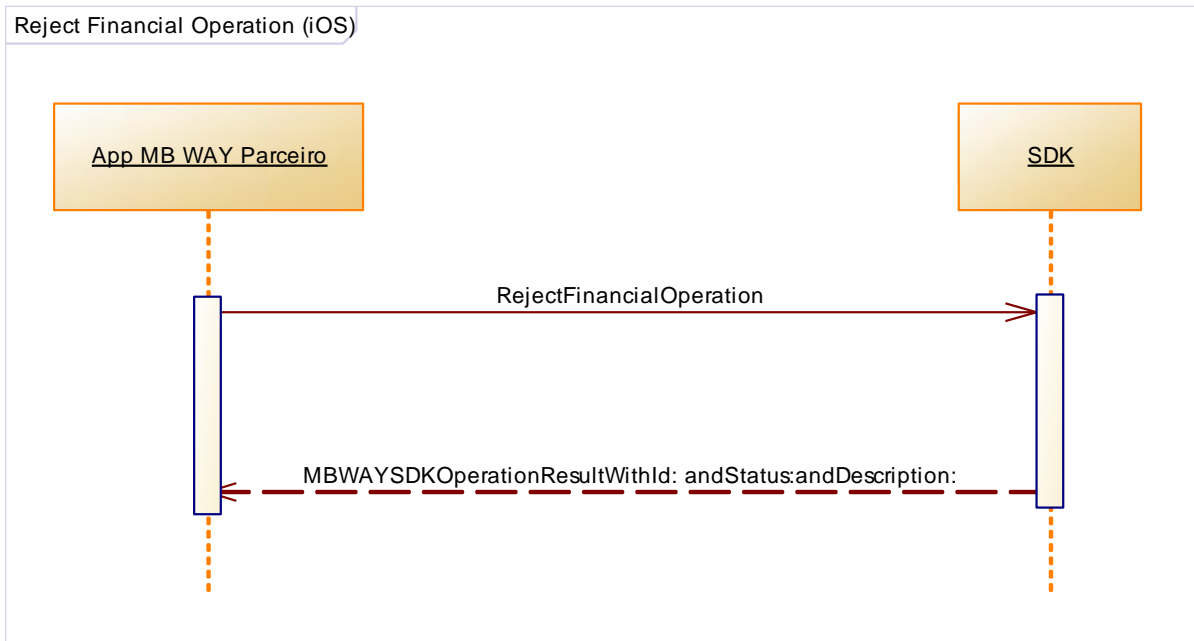


Figura 28 - Recusa de uma Operação Pendente (iOS)

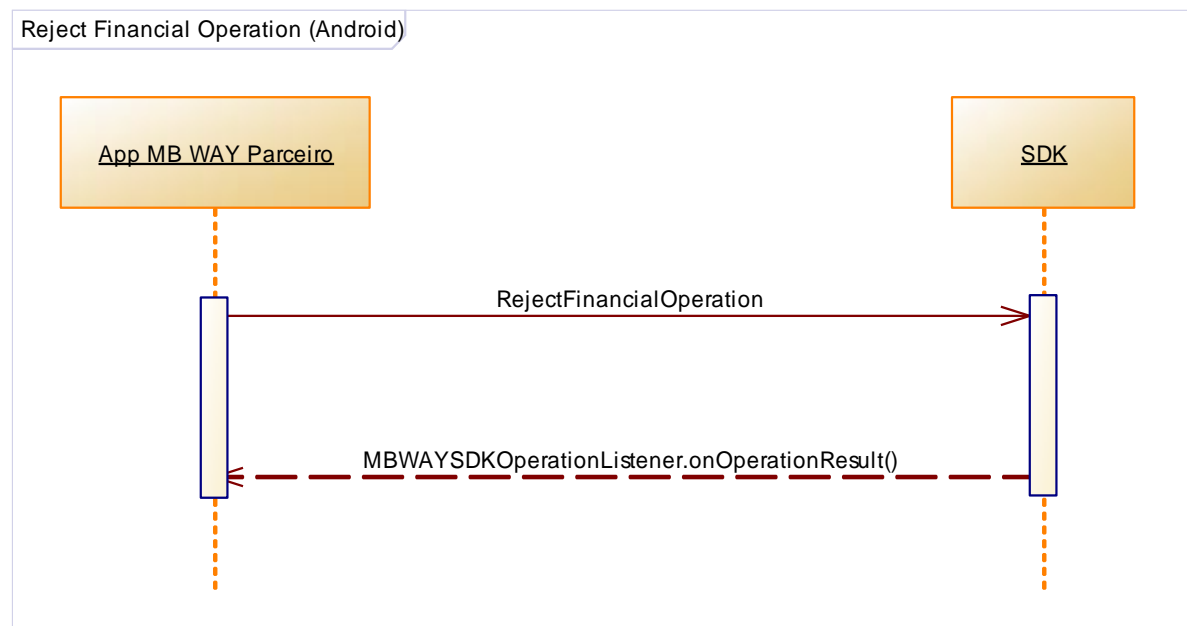


Figura 29 - Recusa de uma Operação Pendente (Android)

B.2.5 Consultar Estado do SDK



Figura 30 - Consultar Estado do SDK (iOS)

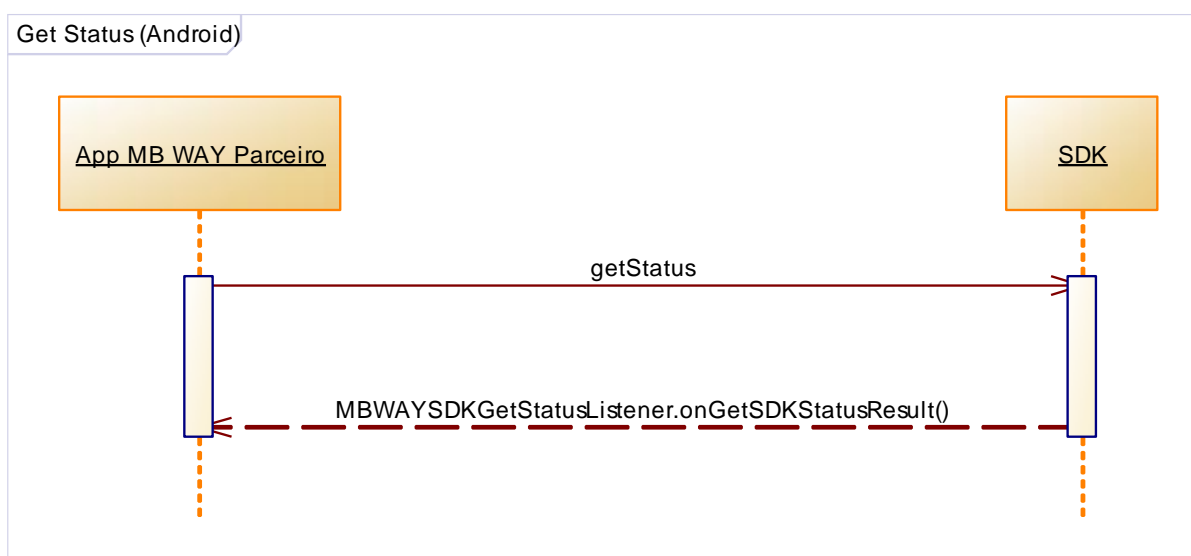


Figura 31 - Consultar Estado do SDK (Android)

B.2.6 Selecionar cartão *Default* para Pagamentos MB WAY *Contactless*

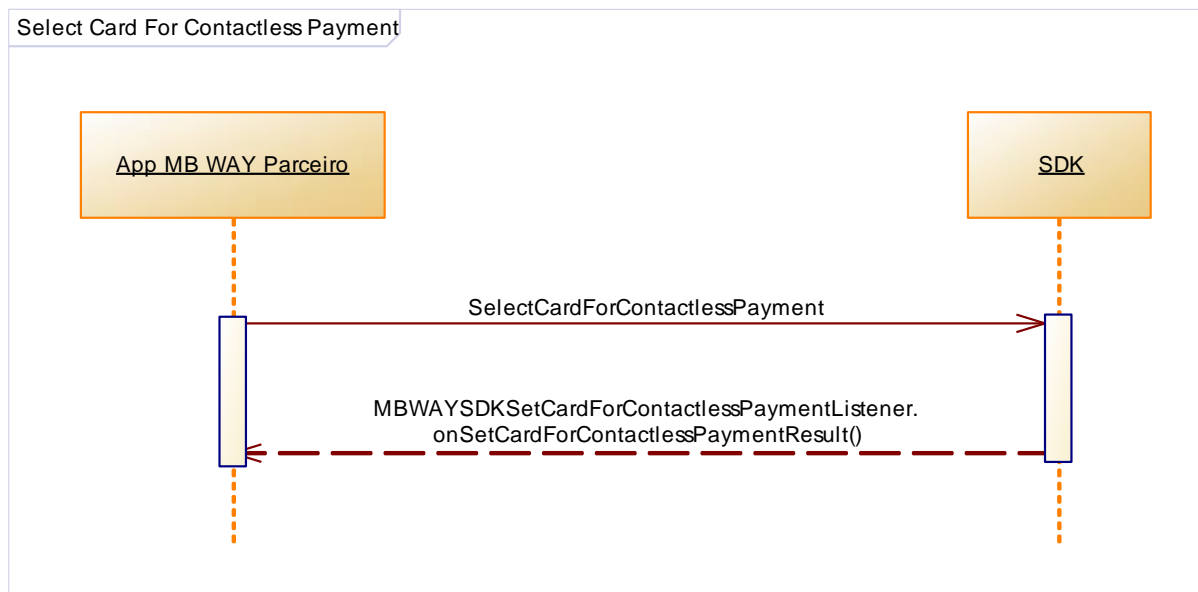


Figura 32 - Selecionar Cartão *Default* para Pagamentos MB WAY *Contactless*

B.2.7 Configuração de Pagamentos MB WAY *Contactless*

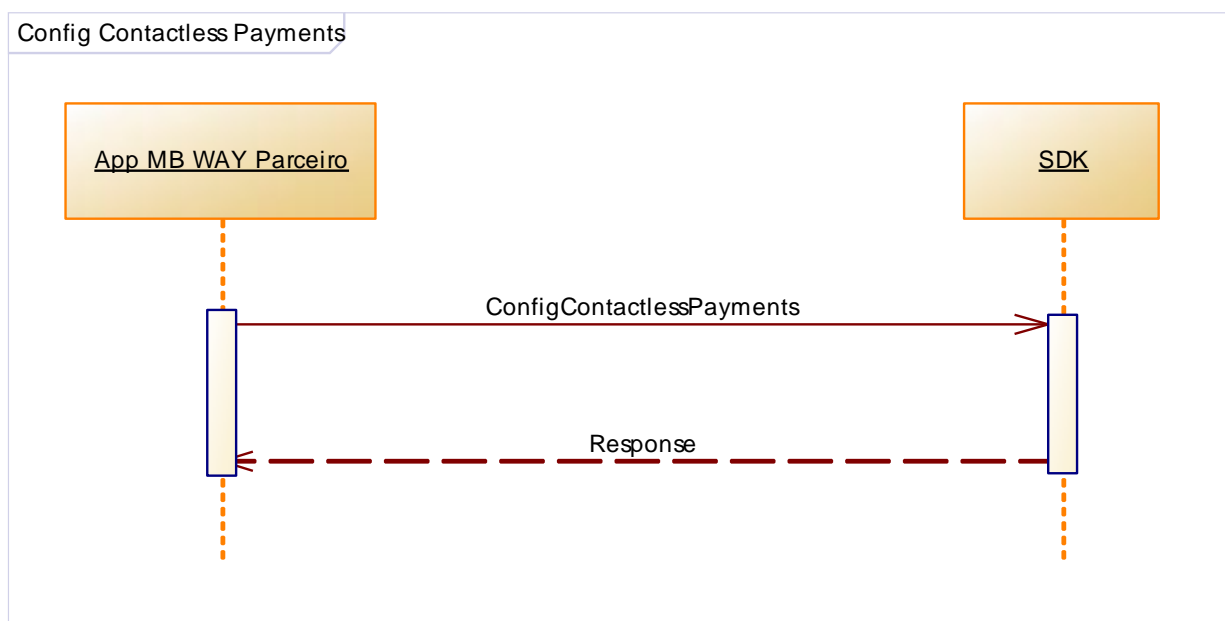


Figura 33 - Configuração de Pagamentos MB WAY *Contactless*

B.2.8 Consulta de Cartões Aprovisionados para MB WAY *Contactless*

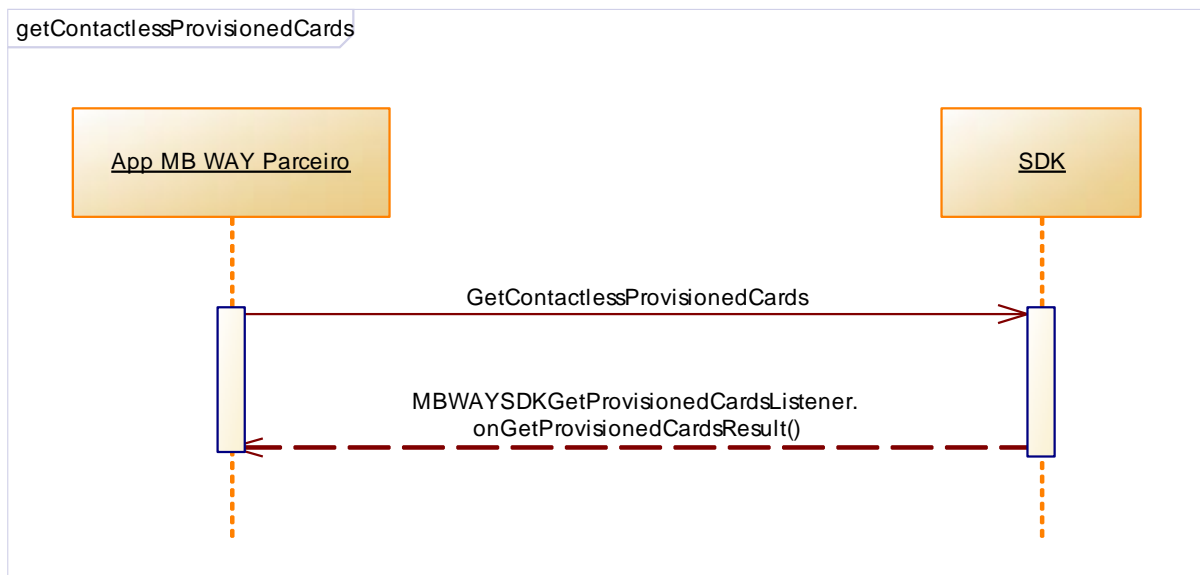


Figura 34 - Consulta de Cartões Aprovisionados para MB WAY *Contactless*

B.2.9 Passagem de PIN MB WAY ao SDK

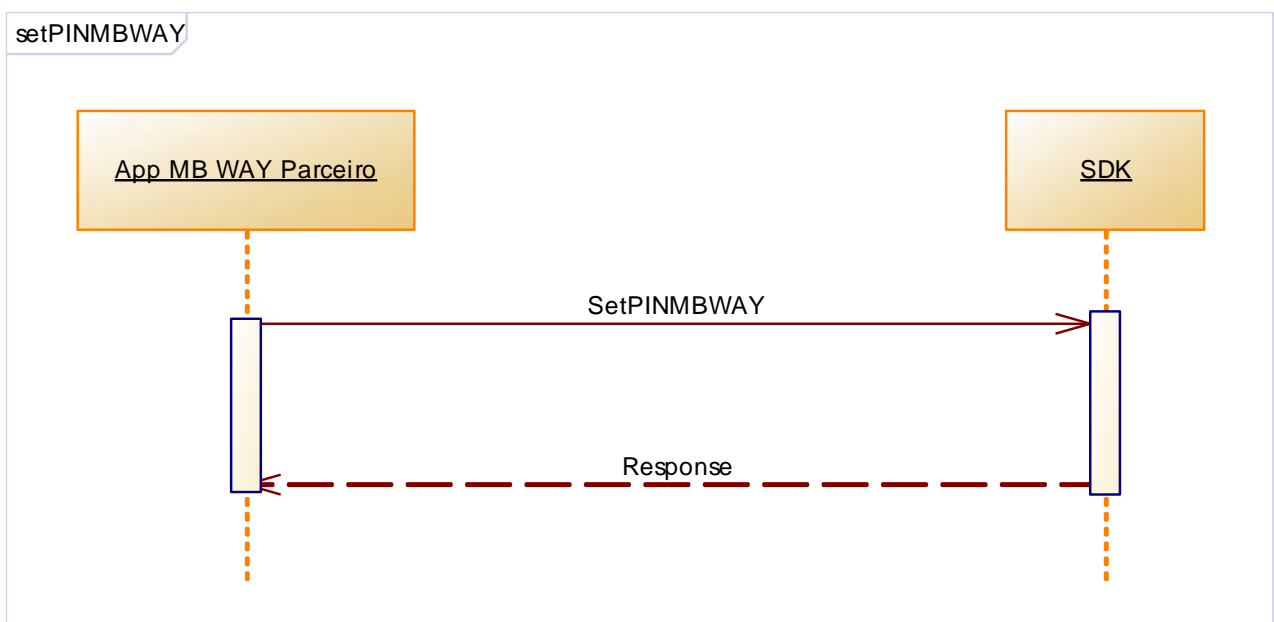


Figura 35 - Passagem de PIN MB WAY ao SDK

B.2.10 Registo de um Pagamento QRCode



Figura 36 - Registo de um Pagamento QRCode (iOS)

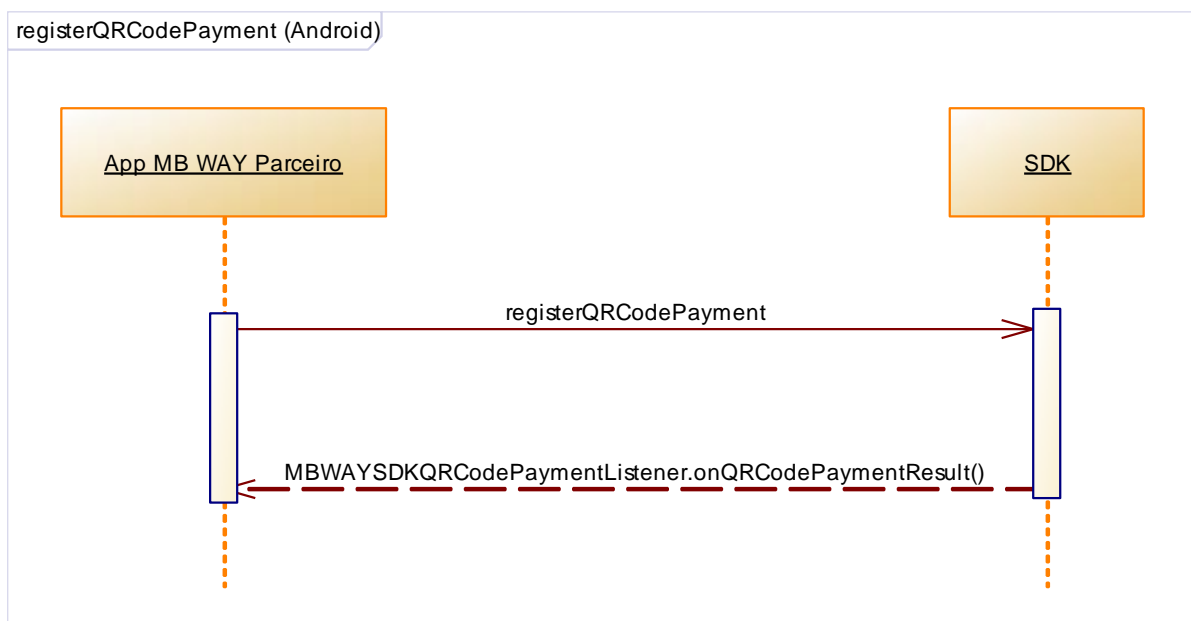


Figura 37 - Registo de um Pagamento QRCode (Android)

B.3. Interfaces Parceiro - Mainframe

B.3.1 Associação de Cartão ao MB WAY



Figura 38 - Associação de Cartão ao MB WAY

B.3.2 Cancelamento do MB WAY

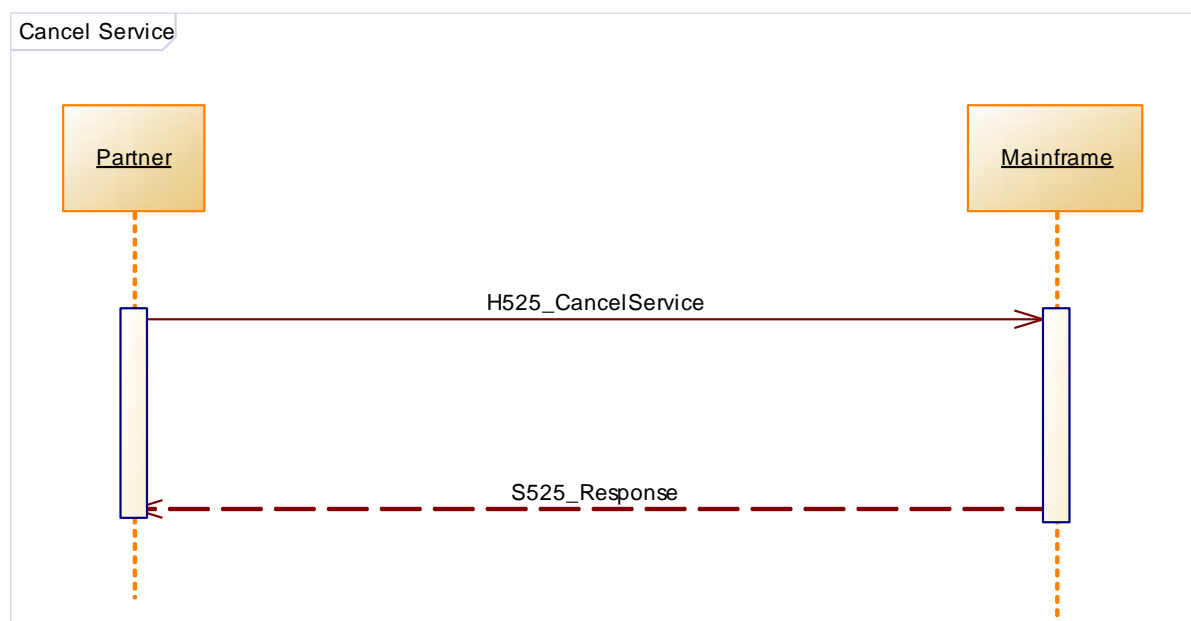


Figura 39 - Cancelamento do MB WAY

B.3.3 Cancelamento de Transferência Instantânea P2P

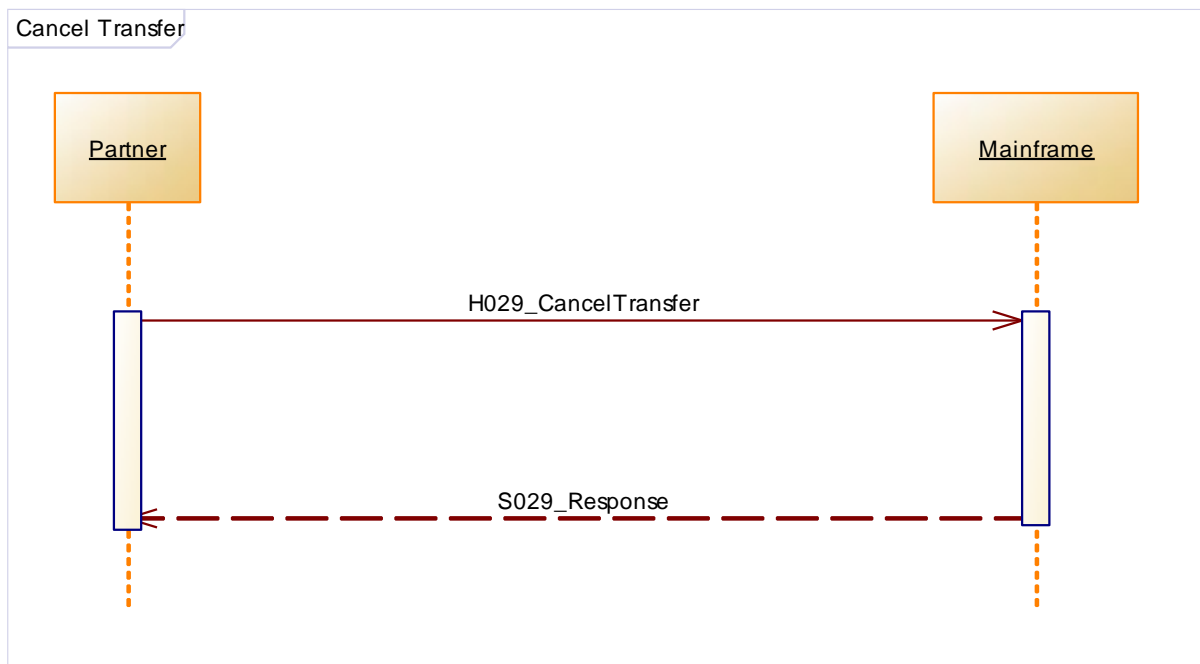


Figura 40 - Cancelamento de Transferência Instantânea P2P

B.3.4 Cancelamento de Referência para Levantamento MB WAY

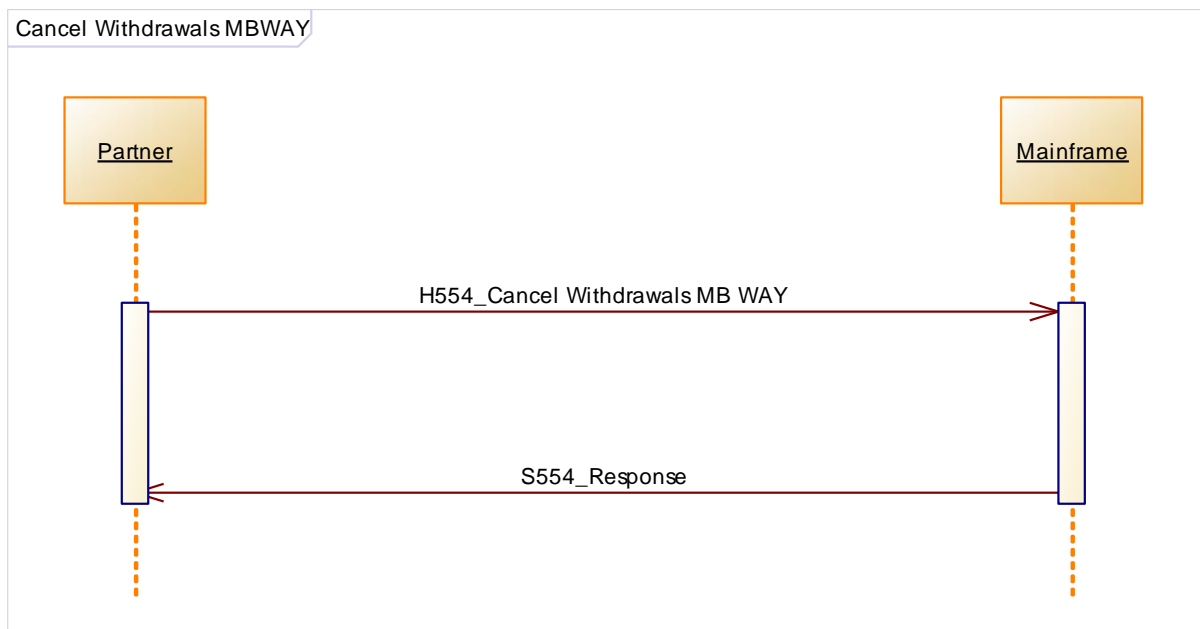


Figura 41 - Cancelamento de Referência para Levantamento MB WAY

B.3.5 Confirmação de Operação Financeira

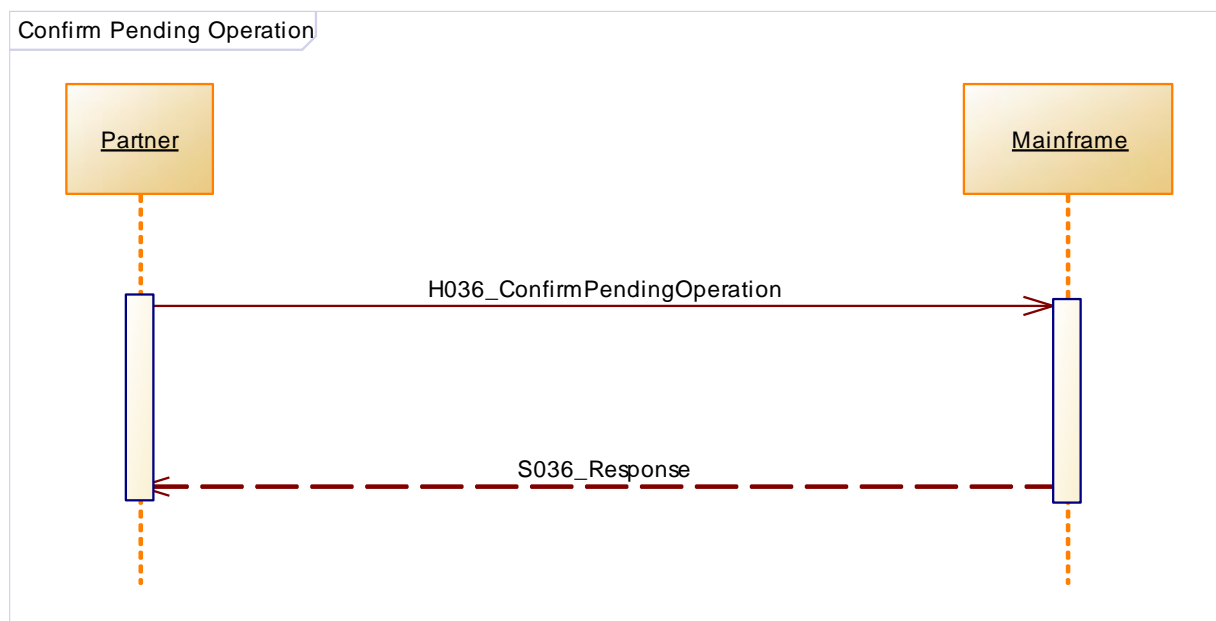


Figura 42 - Confirmação de Operação Financeira

B.3.6 Adesão ao Serviço MB WAY

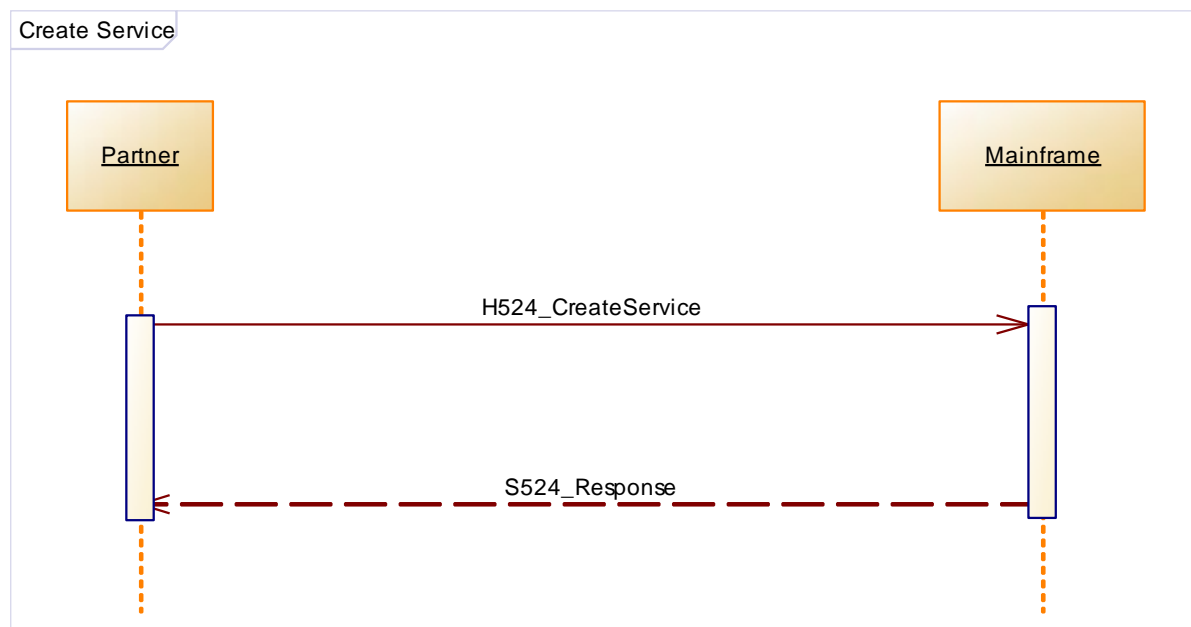


Figura 43 - Adesão ao Serviço MB WAY

B.3.7 Desassociação de Cartão ao MB WAY



Figura 44 - Desassociação de Cartão ao MB WAY

B.3.8 Alteração do PIN MB WAY



Figura 45 – Alteração do PIN MB WAY

B.3.9 Alteração de *Alias* de Registo do Serviço MB WAY

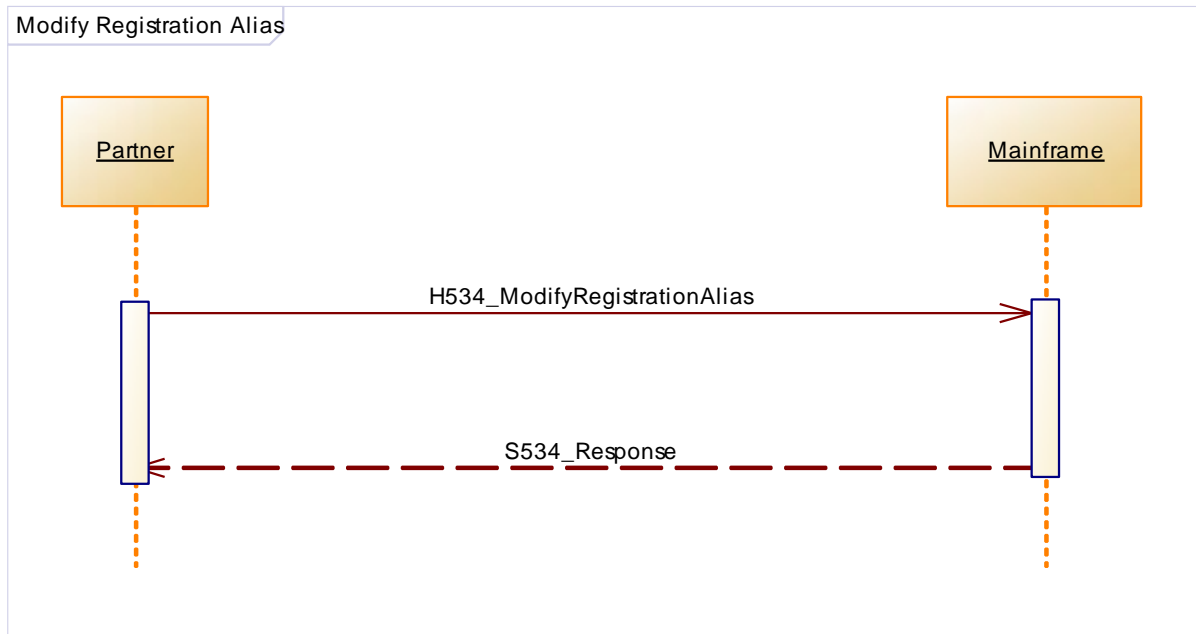


Figura 46 - Alteração de *Alias* de Registo do Serviço MB WAY

B.3.10 Notificação de Operação Pendente

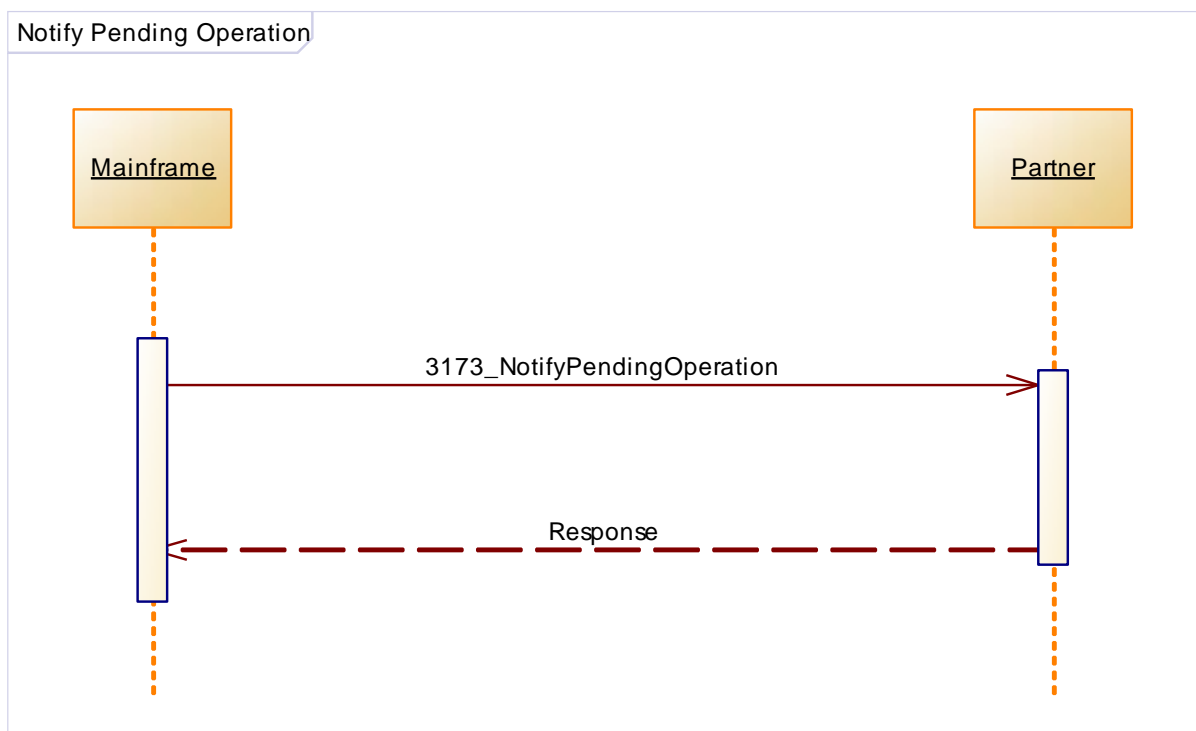


Figura 47 - Notificação de Operação Pendente

B.3.11 Pedido de Código de Ativação para MB WAY Parceiro

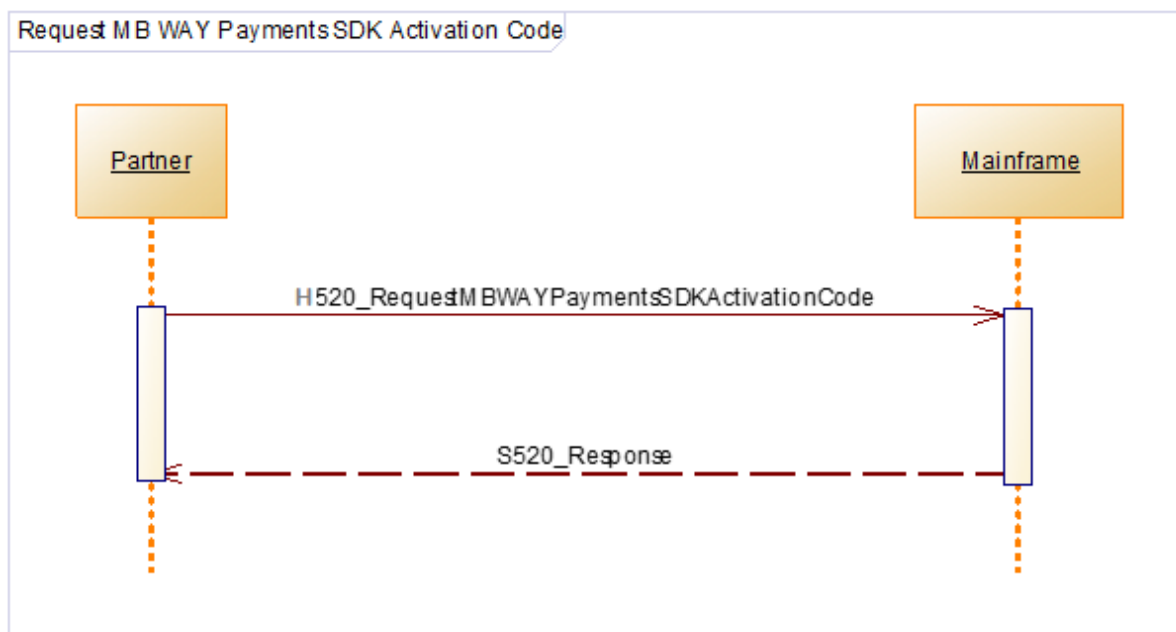


Figura 48 - Pedido de Código de Ativação para MB WAY Parceiro

B.3.12 Pedido de Pagamento P2P

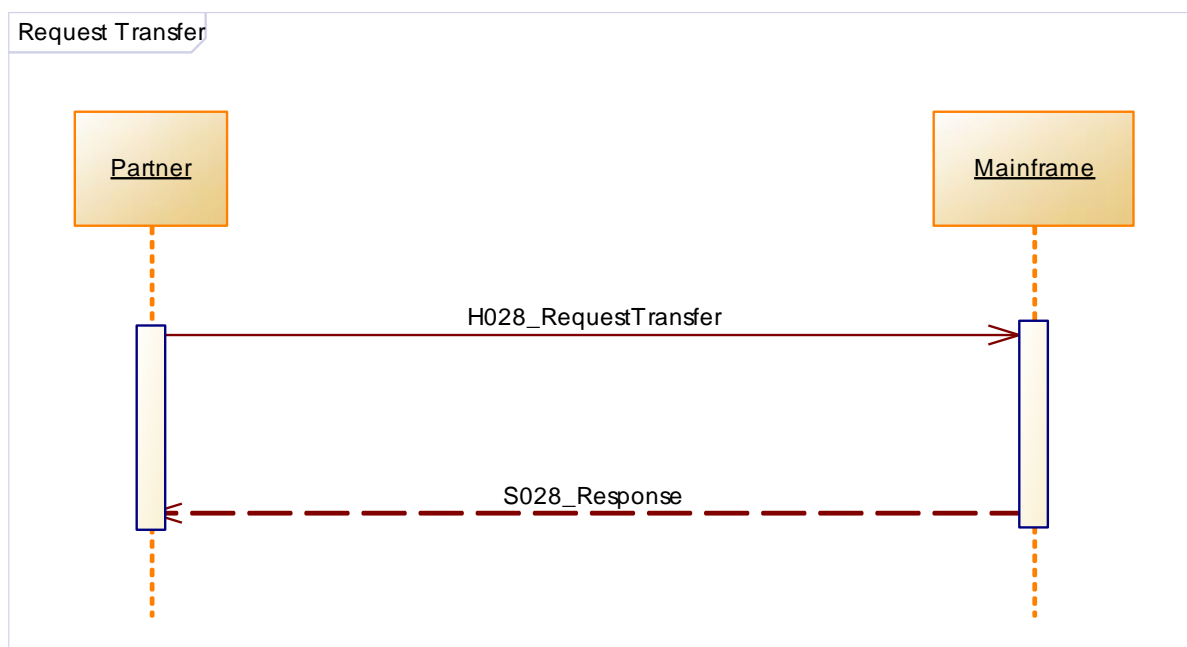


Figura 49 - Pedido de Pagamento P2P

B.3.13 Pedido de Referência para Levantamento MB WAY

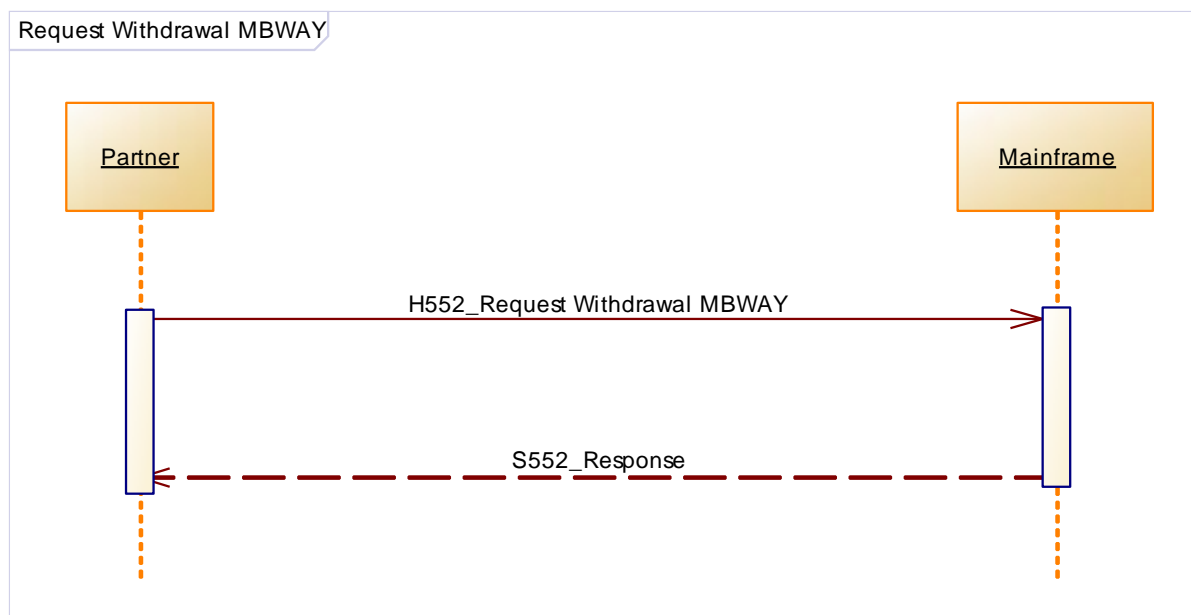


Figura 50 - Pedido de Referência para Levantamento MB WAY

B.3.14 Consulta de Estado de Transferência P2P

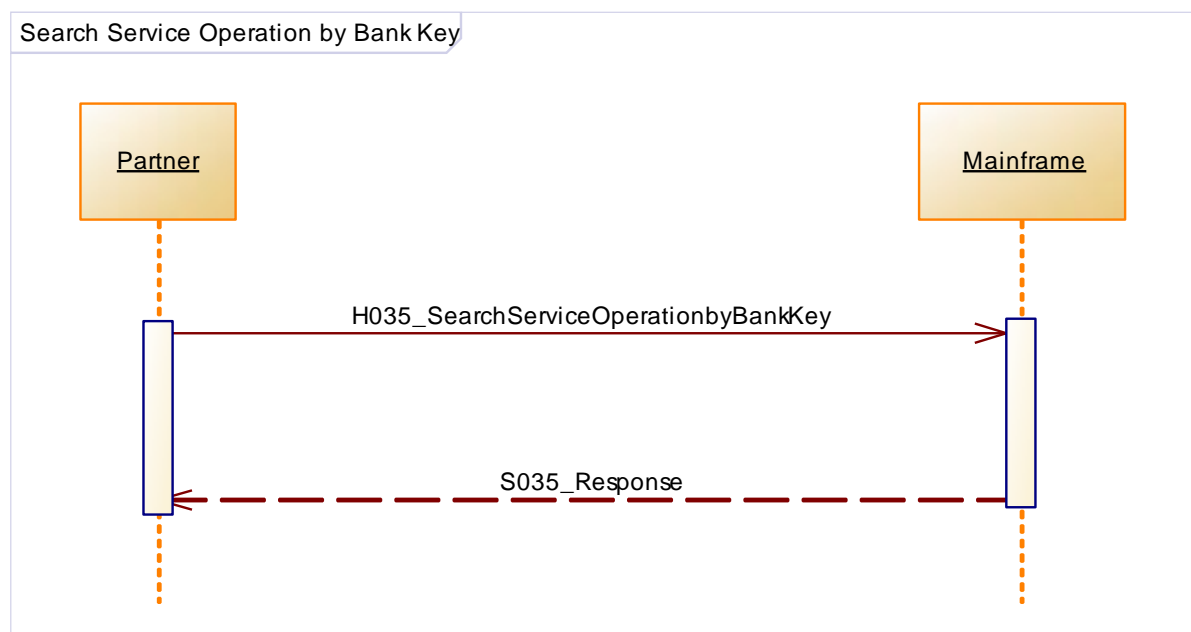


Figura 51 - Consulta de Estado de Transferência P2P

B.3.15 Consulta de Referências para Levantamento MB WAY



Figura 52 - Consulta de Referências para Levantamento MB WAY