Release Documentation

MB WAY

Levantamento MB WAY

Emissores

Versão: 01.00

Data: 2017-04-03

Estado: Final

Classificação: Restrito

Referência: DCSIBS170116

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

Ficha Técnica

Referência:	DCSIBS170116
Título do Documento:	Levantamento MB WAY
Versão:	01.00
Estado:	Final
Classificação:	Restrito
Tipo de Documento:	Release Documentation
Área Funcional Responsável:	AF Desenvolvimento de Serviços

Documentos Relacionados

Referência	Título	Origem
DCSIBS140055	Manual do Serviço - MB WAY	Área de Desenvolvimento de Serviços SIBS FPS

Revisões

Versão	Data	Descrição	Autor
01.00	2017-04-03	Criação do documento	Área de Desenvolvimento de Serviços SIBS FPS

Índice

Índice de Figuras

Índice de Tabelas

1 Introdução

O Levantamento MB WAY é a mais recente funcionalidade do MB WAY, que permite efetuar levantamentos em CA MULTIBANCO sem necessidade de introdução do cartão físico. O levantamento é feito através de um código de levantamento gerado na *app* MB WAY, ou através dos canais do Emissor – *homebanking* ou *mobile banking* –, pelo Utilizador que pode escolher o montante e o cartão a ser debitado. Para efetivar o levantamento, o Utilizador deve dirigir-se a um CA MULTIBANCO, premir a tecla verde / confirmação e, de seguida, introduzir o código de levantamento gerado na *app* MB WAY ou nos canais do Emissor. No momento em que o dinheiro é dispensado, o Utilizador recebe na *app* uma notificação a informar sobre a conclusão da operação.

1.1 Âmbito

Este documento identifica os interfaces necessários para que os Emissores disponibilizem a funcionalidade de Levantamento MB WAY para Utilizadores aderentes MB WAY nos seus próprios canais.

2 Apresentação da Funcionalidade para canais dos Emissores

O Levantamento MB WAY para canais dos Emissores conta com as seguintes operações associadas:

- Geração de Referência para Levantamento MB WAY;
- Consulta de Referências para Levantamento MB WAY;
- Cancelamento de Referência para Levantamento MB WAY.
  Esta operação será possível para Utilizadores aderentes MB WAY pelo que os Emissores devem garantir que implementam a mensagem que permite identificar se um determinado número de telemóvel é aderente. Só se este for aderente ao MB WAY é que esta operação deverá ser disponibilizada (mensagem H531 – S531: Consulta do MB WAY por *alias* de registo (V01). A especificação desta mensagem está incluída na secção Mensagens *Host-to-Host* do Manual de Implementação de Processamento para Emissores (DCSIBS100026).

2.1 Geração de Referência para Levantamento MB WAY

Esta operação permite a geração de uma referência que possibilita o Levantamento MB WAY.

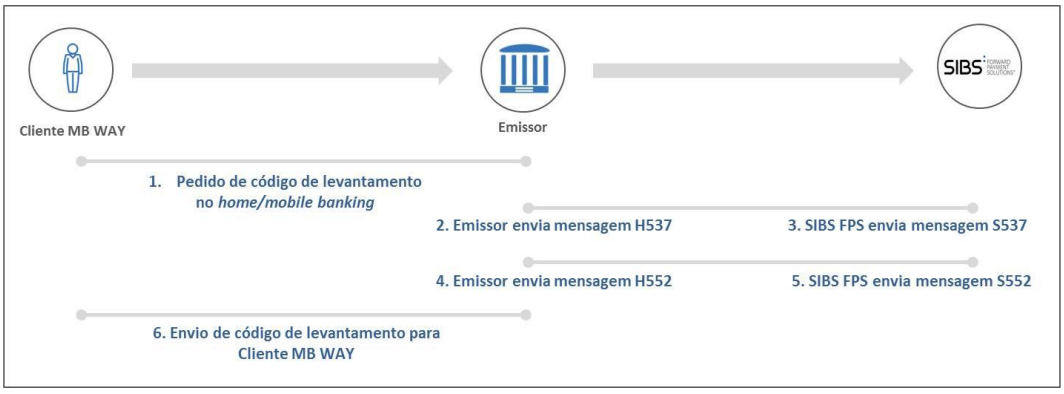


Figura 1 – Geração de Referência para Levantamento MB WAY

1. O Cliente MB WAY solicita ao seu Emissor um código de Levantamento MB WAY;
2. O Emissor envia à SIBS FPS a mensagem H537 (Consulta de *Alias* de Registo associado a um cartão Bancário);
3. A SIBS FPS responde à mensagem H537 com a mensagem S537;
4. O Emissor envia à SIBS FPS a mensagem H552 (Geração de referência para Levantamento MB WAY);
5. A SIBS FPS responde à mensagem H552 com a mensagem S552;
6. O Emissor envia ao Cliente o código de Levantamento MB WAY.

Consultar secção 3.1.1.1 – H552 – S552: Geração de Referência para Levantamento MB WAY (V01).

2.2 Consulta de Referências para Levantamento MB WAY

Esta operação permite a consulta de referências para Levantamento MB WAY.

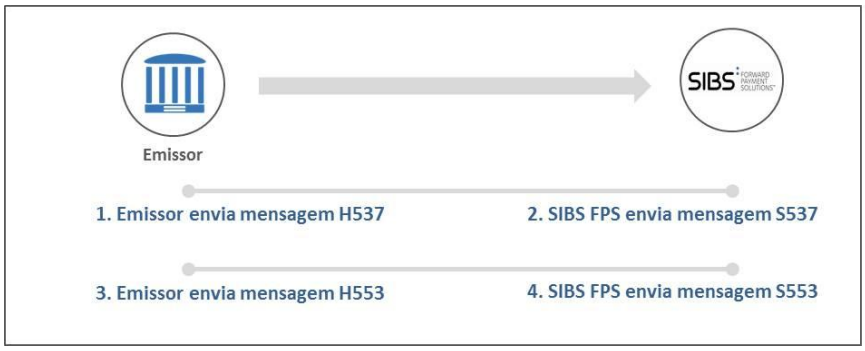


Figura 2 – Consulta de Referências para Levantamento MB WAY

1. O Emissor envia à SIBS FPS a mensagem H537 (Consulta de *Alias* de Registo associado a um cartão Bancário);
2. A SIBS FPS responde à mensagem H537 com a mensagem S537;
3. O Emissor envia à SIBS FPS a mensagem H553 (Consulta de referências para Levantamento MB WAY);
4. A SIBS FPS responde à mensagem H553 com a mensagem S553.

Consultar secção 3.1.1.2 – H553 – S553: Consulta de Referências para Levantamento MB WAY (V01).

2.3 Cancelamento de Referência para Levantamento MB WAY

Esta operação permite o cancelamento de uma referência para Levantamento MB WAY.

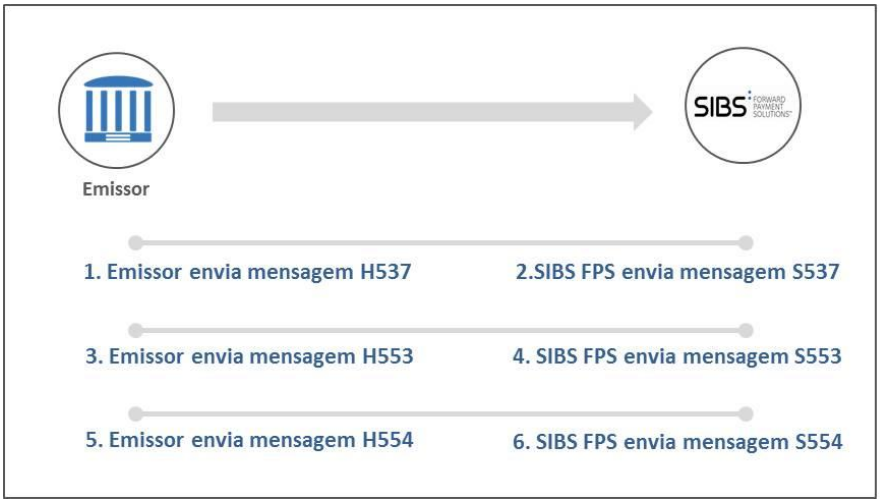


Figura 3 – Cancelamento de Referência para Levantamento MB WAY

1. O Emissor envia à SIBS FPS a mensagem H537 (Consulta de *Alias* de Registo associado a um cartão Bancário);
2. A SIBS FPS responde à mensagem H537 com a mensagem S537;
3. O Emissor envia à SIBS FPS a mensagem H553 (Consulta de referências para Levantamento MB WAY);
4. A SIBS FPS responde à mensagem H553 com a mensagem S553;
5. O Emissor envia à SIBS FPS a mensagem H554 (Cancelamento de referência para Levantamento MB WAY);
6. A SIBS FPS responde à mensagem H554 com a mensagem S554.

Consultar secção 3.1.1.3 – H554 – S554: Cancelamento de Referência para Levantamento MB WAY (V01).

3 Implementação do Serviço

3.1 Especificações Técnicas

3.1.1 Mensagens

No *Host-to-Host* foram criadas as seguintes mensagens para possibilitar aos Emissores a implementação da funcionalidade Levantamento MB WAY:

- H552 – S552: Geração de Referência para Levantamento MB WAY (V01);
- H553 – S553: Consulta de Referência para Levantamento MB WAY (V01);
- H554 – S554: Cancelamento de Referência para Levantamento MB WAY (V01).

3.1.1.1 H552 – S552: Geração de Referência para Levantamento MB WAY (V01)

Esta operação permite a geração de uma referência que possibilita o Levantamento MB WAY.

Antes de enviar a mensagem H552, 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 H552: Geração de Referência para Levantamento MB WAY. Na resposta (S552), a SIBS FPS envia a referência que permite o Levantamento MB WAY.

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 (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".

Tabela 1 – H552 – S552: Geração de Referência para Levantamento MB WAY (V01)

N.º	Sigla	Nome	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'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 FPS	3	N		35	35	

N.º	Sigla	Nome	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
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			
8227	COM_SERIDEA01	Identificador do Serviço	40	A	23			
8130	SEE_SELTIP	Tipo de *Alias*	3	N	63			
8121	SEE_SELDSG	Designação do *Alias*	150	A	66			
2324	CAR_PANLGT	Comprimento do PAN	2	N	216			
5402	CAR_PANA03	*Primary Account Number*	19	A	218			
0637	CAR_EXPDAT	Data de Expiração do cartão Expandida	6	N	237			
9116	SEE_MNTLSC	Montante de Levantamento sem cartão	5	N	243			
0233	EXT_MOECOD	Código de Moeda	3	N	248			
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		
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 FPS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
			Total		**762**	**666**	**135**	

3.1.1.2 H553 – S553: Consulta de Referências para Levantamento MB WAY (V01)

Esta operação permite a consulta de referências para Levantamento 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. 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 e associados ao Identificador de Serviço informado no pedido.

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-Hellman* 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.

Tabela 2 – H553 – S553: Consulta de Referências para Levantamento MB WAY (V01)

N.º	Sigla	Nome	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'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 FPS	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			
8227	COM_SERIDEA01	Identificador do Serviço	40	A	23			
9157	CHV_INIVTR	Vetor de Inicialização	32	A		52		
9156	CHV_SPKA01	SIBS *Public Key*	512	A	63	84		
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A	575			
1002	MSG_OPETIP	Código Operador	1	A	605			
0428	MSG_OCONUM	Número de Ocorrências	2	N		596		A)
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A		598		B)
8130	SEE_SELTIP	Tipo de *Alias*	3	N		628		B)
8121	SEE_SELDSG	Designação do *Alias*	150	A		631		B)
8130	SEE_SELTIP	Tipo de Alias	3	N		781		B)
8121	SEE_SELDSG	Designação do *Alias*	150	A		784		B)
2324	CAR_PANLGT	Comprimento do PAN	2	N		934		B)
5402	CAR_PANA03	*Primary Account Number*	19	A		936		B)
0637	CAR_EXPDAT	Data de Expiração do Cartão Expandida	6	N		955		B)
9116	SEE_MNTLSC	Montante de Levantamento sem cartão	5	N		961		B)
0233	EXT_MOECOD	Código de Moeda	3	N		966		B)
9158	CHV_REFLSC	Referência de Levantamento sem cartão	32	A		969		B)

N.º	Sigla	Nome	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
9164	SEE_DURSGN	Duração em Segundos	9	N		1001		B)
9163	SEE_SITLSC_REF	Situação da Referência de Levantamento sem cartão	3	N		1010		B)
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem pela SIBS FPS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
		Total		**Min**	**605**	**597**	**135**	
				Max		**1842**		

Observações:

A) Valores possíveis de '00' a '03'.

B) Pode ocorrer de 0 a 3 vezes.

3.1.1.3 H554 – S554: Cancelamento de Referência para Levantamento MB WAY (V01)

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.

Tabela 3 – H554 – S554: Cancelamento de Referência para Levantamento MB WAY (V01)

N.º	Sigla	Nome	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Header								
0470	MSG_TIP_H2H	Código da Mensagem BS	4	A	1	1	1	
0002	MSG_VER	Versão de Mensagem	2	N	5	5	5	'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 FPS	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	Nome	Comp.	Rep.	Pedido (Pos.)	Resp. Aceite (Pos.)	Resp. Recusada (Pos.)	Obs.
Detalhe								
8128	SEE_IDEOPR	Identificação da Operação no Serviço	30	A	21			
8196	SEE_TIPCOD	Código do Tipo de Serviço	2	N	51			
8227	COM_SERIDEA01	Identificador do Serviço	40	A	53			
Trailer								
0493	MSG_NOKTIP	Código de Recusa da Mensagem pela SIBS FPS	8	A			38	
0472	MSG_RESTXT	Texto Resposta	45	A			46	
3361	MSG_RESTXT_LI2	Texto Resposta	45	A			91	
			Total		**92**	**51**	**135**	

3.2 Dicionário de dados

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

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
0002	MSG_VER	Versão 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 FPS possa suportar mensagens com formatos diferentes relativas ao mesmo serviço.	
0004	MSG_DTH	Data/hora da transmissão	14	N		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*.	
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.	
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).	
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	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
						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*.	
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 FPS.	
0471	MSG_IDE_H2H	Identificação mensagem do Banco	14	A		No caso da mensagem ser originada do CPD de um Banco, o seu preenchimento tem o formato que este quiser. No caso da mensagem ser de um terminal bancário: COD.TERMINAL 6 NUM.PERIODO 2 NUM.TRANSACÇÃO 5 COD.OPERADOR 1	
0472	MSG_RESTXT	Texto resposta	45	A		Texto preenchido pela SIBS FPS numa mensagem recusada, com os textos que justificam a recusa para o cliente.	
0492	MSG_RESCOD	Código de resposta da mensagem da SIBS FPS	3	N		Código de resposta da mensagem de sessão Banco ->SIBS FPS. (= 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 SIB FPS	8	A		Código da recusa da SIBS FPS a uma mensagem na sessão Banco ->SIBS FPS. (este campo é normalmente preenchido com o modulo do erro, quando existe um erro na mensagem (campo 492 >0)).	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
0637	CAR_EXPDAT	Data de expiração do cartão expandida	6	N	AAAAMM	Último mês e ano em que o cartão ainda é válido.	
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 mensagem de resposta ter ocorrências '>' dados imediatamente superiores aos enviados na mensagem de pedido '<' dados imediatamente inferiores aos enviados na mensagem de pedido
1709	LOG_SIS	Sistema do *log* associado à transação	2	A		Código utilizado nas mensagens e nos registos de detalhe correspondentes a cada operação e que indica ao Banco qual o subsistema transacional em que esta se realizou. Corresponde à versão expandida do campo (0312) SIS_APLPDD. Este campo pode não estar preenchido (espaços) em registos gerados na Compensação MULTIBANCO, resultantes do apuramento de valores agregados, para os quais não é criado um registo no ficheiro de *log* da SIBS FPS. Conjugado com os campos (0117) LOG_NUMN01, (0320) LOG_PERN01 e (2148) SIS_DTHN01 identifica univocamente um registo no sistema MULTIBANCO.	
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.	
3361	MSG_RESTXT_LI2	Texto resposta	45	A		Texto preenchido pela SIBS FPS. 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)	

N.º	Sigla do Campo	Nome do Campo	Comp.	Rep.	Formato	Descrição	Valores
5402	CAR_PANA03	*Primary Account Number*	19	A		Número completo do cartão encostado à esquerda. Formato no âmbito da norma ISO 7812-1.	
8121	SEE_SELDSG	Designação do *Alias*	150	A		Designação do *Alias* (ex. mail, telemóvel, matrícula, etc...).	
8128	SEE_IDEOPR	Identificação da operação no serviço	30	A		Identifica as operações efetuadas através do Serviço.	
8130	SEE_SELTIP	Tipo de *Alias*	3	N		Identifica o Tipo de *Alias* associado ao Serviço.	001 – MSISDN; 002 – Mail.
8196	SEE_TIPCOD	Código do tipo de serviço	2	N		Código do tipo da *Tokenization Platform*	
8227	COM_SERIDEA01	Identificador do serviço	40	A		Identificador único do *Tokenization Platform* (Hexadecimal).	
9116	SEE_MNTLSC	Montante de Levantamento sem cartão	5	N		Montante referente a Levantamento MB WAY sem cartão.	
9156	CHV_SPKA01	SIBS *Public Key*	512	A		Atributo que contém a chave pública para a cifra.	
9157	CHV_INIVTR	Vetor de inicialização	32	A		Atributo que contém o parâmetro de cifra Vetor de Inicialização.	
9158	CHV_REFLSC	Referência de Levantamento MB WAY sem cartão	32	A		Atributo que contém a Referência de Levantamento MB WAY sem cartão, cifrada.	
9163	SEE_SITLSC_REF	Situação referência Levantamento MB WAY sem cartão	3	N		Atributo que informa qual a situação da referência de Levantamento MB WAY sem cartão.	000 – Ativa; 001 – Geração de Referência Rejeitada; 002 – Registada; 003 – Cancelada; 004 – Rejeitada; 005 – Expirada; 006 – Realizada.
9164	SEE_DURSGN	Duração em segundos	9	N		Atributo que contém a duração em segundos da referência para Levantamento MB WAY.	

4 Glossário

Termo	Definição
Alias (Dados de identificação)	Dado chave para identificar o Utilizador no MB WAY. São estes *Alias* que são evocados pelo Autoridade Tributária no pedido de pagamento e que na SIBS FPS se relacionam a cartões de pagamento. Para o Utilizador são os seus dados de identificação.
N.A.	Não Aplicável
SIBS FPS	SIBS *Forward Payment Solutions*

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*[1] 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*).

[1] 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-----
MIIBCAKCAQEAgdTDGS6CTznBymOstYi9RLAFxT1my2R54me7GNJ8xhp2mehsOc+X
7WumynmESW+JH+ISVK/L6Ku/PHiharwawvsSdJ3rf6gjVWGdlD66Cww9lMbX2BQs
Qku2pmNLTMzLib6TIgI+973RSmPr5dBXQ/ZEd5ObgnCpfldvl3/p0YESILP2SGHB
5Y54Qeasq/oBAd5K9tYFLIwTkK3kUHTmMPMNkZgYMRkpJ7V6ShrKOBAEYH6CeeUE
UmYZpEfQkyr5mQMr55G8/U4uwgUXYWzPb7n7DaiAKSTm++gUa3NhQHElY54dmAzw
GrmmMOqh0Q2GdDcUwWCJD9veVjl4aVACCwIBAg==
-----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 partilhado (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) = *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)

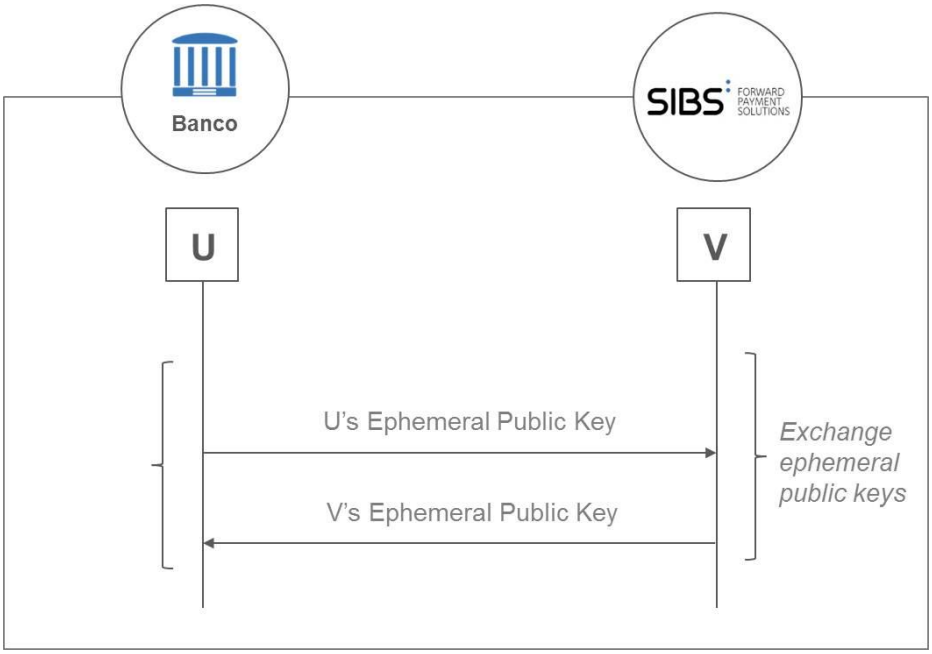


Figura 4 – C(2e, 0s) *schemes: each party contributes only and ephemeral key pair*

A.1.1 Anexo I

Exemplo de computação do segredo partilhado (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 partilhado 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/PHiharwawvsSdJ3rf6gjVWGdlD66Cww91MbX2BQs
Qku2pmNLTMzLib6TIgI+973RSmPr5dBXQ/ZEd5ObgnCpfldvl3/p0YESILP2SGHB
5Y54Qeasq/oBAd5K9tYFLIwTkK3kUHTmMPMNkZgYMRkpJ7V6ShrKOBAEYH6CeeUE
UmYZpEfQkyr5mQMr55G8/U4uwgUXYWzPb7n7DaiAKSTm++gUa3NhQHElY54dmAzw
GrmmMOqh0Q2GdDcUwWCJD9veVjl4aVACCwIBAg==
-----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 dhpub_1.pem -text
-----BEGIN PUBLIC KEY-----
MIICJDCCARcGCSqGSIb3DQEDATCCAQgCggEBAIHUwxkugk85wcpjrLWIvUSwBcU9
ZstkeeJnuxjSfMYadpnobDnPl+1rpsp5hElviR/iElSvy+irvzx4oWq8GsL7EnSd
63+oI1VhnZQ+ugsMPZTG19gULEJLtqZjS0zMy4m+kyICPve90Upj6+XQV0P2RHeT
m4JwqX5Xb5d/6dGBEiCz9khhweWOeEHmrKv6AQHeSvbWBSyME5Ct5FB05jDzDZGY
GDEZKSe1ekoayjgQBGB+gnnlBFJmGaRH0JMq+ZkDK+eRvP1OLsIFF2Fsz2+5+w2o
gCkk5vvoFGtzYUBxJWOeHZgM8Bq5pjDqodENhnQ3FMFgiQ/b31Y5eG1QAgsCAQID
ggEFAAKCAQAepRUJkuG49xlD/H3idscNynFuOgcJ0DrO/VV2//M0uxAUtTw4YvB6
zmjUaVveQ2Q8G1EpQFvNE3fTeYWWFXTS/ec6tTd+pPUjlbRT6f8VEZBACyip3QC0
mWdmOtCBfOy7/oazHQM609VmygJEikBaFH0helMUTgfOS4wyHc5DxbGNYBJJW8c/
gdd0/dHaPNp5BJR3tmHIFq2cbyUaTpatRbRjOjY51jwSXoYZfG2Ugh6JcVhPBlDq
NPCsQLAW+qzHhUTIKDlYMKgprwo70n35p6tkfxTOQKyxsfgANDfaKm0/fkozWMkJ
/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-----
MIICJDCCARcGCSqGSIb3DQEDATCCAQgCggEBAIHUwxkugk85wcpjrLWIvUSwBcU9
ZstkeeJnuxjSfMYadpnobDnPl+1rpsp5hElviR/iElSvy+irvzx4oWq8GsL7EnSd
63+oI1VhnZQ+ugsMPZTG19gULEJLtqZjS0zMy4m+kyICPve90Upj6+XQV0P2RHeT
m4JwqX5Xb5d/6dGBEiCz9khhweWOeEHmrKv6AQHeSvbWBSyME5Ct5FB05jDzDZGY
GDEZKSe1ekoayjgQBGB+gnnlBFJmGaRH0JMq+ZkDK+eRvP1OLsIFF2Fsz2+5+w2o
gCkk5vvoFGtzYUBxJWOeHZgM8Bq5pjDqodENhnQ3FMFgiQ/b3lY5eGlQAgsCAQID
ggEFAAKCAQAbWBjXeePvMaxNrj6z6SvwHWDtIdRM1Mkn2TVqksOTV6ZHEHhmyQ+g
wyEZeue7iUaS+HEje+VWPYcdTq6jRtvQTSBdnIa3YQ6mRiwRNZ2lvTjKQnQBxunZ
3vetrrFinFO+79RXw9DYqlRxuJhpI5OTD2TC+gmDZzSEX+2n5CSq8y8BbJUWVmOf
pnDAJ8DmLI6knqbEr9O9EcWQjxbXY7hlgkGicvQYVyaNRv3jvk9YP6IsJJJBA97k
anbsQSOA/C4s51hPkLZ7grKAE9aO7citKoBdptCodUKPsHN3Sfp+F8bCVirZi679
VB2op6+jrwWDqRMLGTJeQva62stIe1Uu
-----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:
```

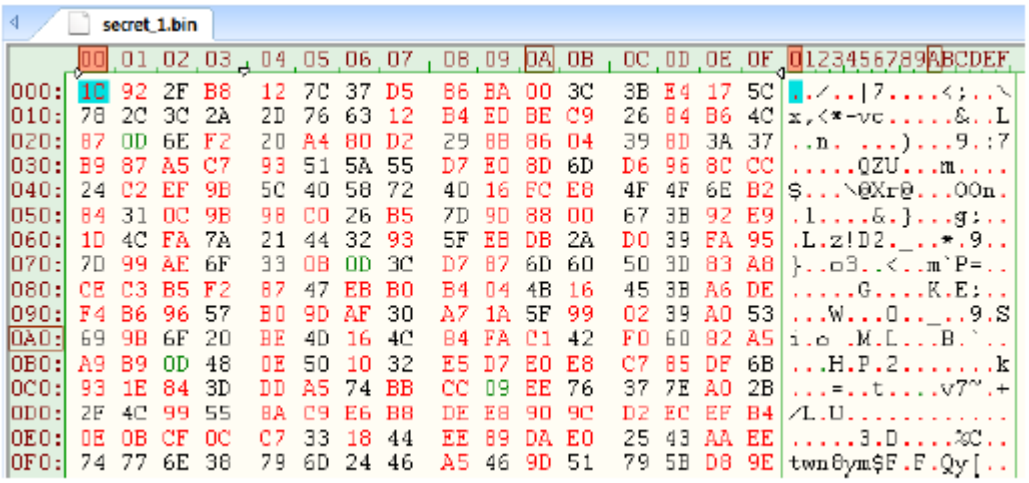
```
        18:57:26:8d:46:fd:e3:be:4f:58:3f:a2:2c:24:92:
        41:03:de:e4:6a:76:ec:41:23:80:fc:2e:2c:e7:58:
        4f:90:b6:7b:82:b2:80:13:d6:8e:ed:c8:ad:2a:80:
        5d:a6:d0:a8:75:42:8f:b0:73:77:49:fa:7e:17:c6:
        c2:56:2a:d9:8b:ae:fd:54:1d:a8:a7:af:a3:af:05:
        83:a9:13:0b:19:32:5e:42:f6:ba:da:cb:48:7b:55:
        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 dhpub_2.pem -out
secret_1.bin

====== Calculate Secret (#2) ========
C:\TEMP\dh\dh-group-2048>openssl pkeyutl -derive -inkey dhkey_2.pem -peerkey dhpub_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 3B E4 17 5C
010: 78 2C 3C 2A 2D 76 63 12 B4 ED BE C9 26 84 B6 4C
020: 87 0D 6E F2 20 A4 80 D2 29 8B 86 04 39 8D 3A 37
030: B9 87 A5 C7 93 51 5A 55 D7 E0 8D 6D D6 96 8C CC
040: 24 C2 EF 9B 5C 40 58 72 40 16 FC E8 4F 4F 6E B2
050: 84 31 0C 9B 98 C0 26 B5 7D 9D 88 00 67 3B 92 E9
060: 1D 4C FA 7A 21 44 32 93 5F EB DB 2A D0 39 FA 95
070: 7D 99 AE 6F 33 0B 0D 3C D7 87 6D 60 50 3D 83 A8
080: CE C3 B5 F2 87 47 EB B0 B4 04 4B 16 45 3B A6 DE
090: F4 B6 96 57 B0 9D AF 30 A7 1A 5F 99 02 39 A0 53
0A0: 69 9B 6F 20 BE 4D 16 4C 84 FA C1 42 F0 60 82 A5
0B0: A9 B9 0D 48 0E 50 10 32 E5 D7 E0 E8 C7 85 DF 6B
0C0: 93 1E 84 3D DD A5 74 BB CC 09 EE 76 37 7E A0 2B
0D0: 2F 4C 99 55 8A C9 E6 B8 DE E8 90 9C D2 EC EF B4
0E0: 0E 0B CF 0C C7 33 18 44 EE 89 DA E0 25 43 AA EE
0F0: 74 77 6E 38 79 6D 24 46 A5 46 9D 51 79 5B D8 9E