Protocol Unificat de Pinpads

ADAPTACIÓ PUP PER A.B.A.

LDM

Llista de Modificacions

Autor	Data	Versió	Comentaris
JAiV	05/09/07	1.0	Creació a partir del document d'ABA del 16/07/07
	13/11/07	2.0	Adaptacions sobre versió PUP 1.4.0
	26/05/08	2.1	Adaptacions per PCI/DSS , devolucions ABA i operacions manuals
	30/05/08	2.2	Xifrat dades transaccions manuals, desaparició nom del titular i data/hora per càlcul MAC
JCS	31/03/09	2.3	Devolucions amb lectura de xip a través del MSG0102 Ombrejat parcial del pan per acomplir amb els criteris PCI/DSS
JCS	5/05/09	2.4	Codis d'acció del terminal a 0's al MSG0102. Número aleatori per el xifrat de pistes no viatja doncs l'algorisme emprat es el ECB. Els camps relacionats amb la signatura digitalitzada no viatgen si el terminal no suporta dita signatura digitalitzada. Codi de servei en clar en missatge MSG0300. *Numero de cajones* en missatge MSG2010 a zeros.
JCS	21/12/2009	3.0	Versió revisada
JCS	12/09/2011	3.1	En devolucions manuals no s'introdueix la data de caducitat ni el cvv2.
ROJ	11/09/2014	3.2	No obligatorietat de càlcul del MAC en anul·lacions.
JCS	13/2/2015	3.3	Devolucions automàtiques. Tractament targetes propietàries.

TDC

Taula de Continguts

0. INTRODUCCIÓ

L'objectiu d'aquest document es especificar les modificacions a realitzar en el protocol PUP estàndard en la seva versió 1.4.0 per adaptar-lo a les necessitats específiques d'ABA.

La versió 1.4.0 de Sermepa incorpora nous conceptes com:

Gestió digitalitzada de la firma, que no s'incorpora en l'adaptació ABA. Conseqüentment els camps associats – separador, tipus d'informació, llargària de la signatura i signatura - no viatgen.

Operatòria Offline (Els PIN-PADs EMV ABA són atesos i Online purs)

Gestió de PIN Online (ABA ja havia previst l'operatòria PIN Online)

Els nous indicadors de contactless, tag EMV amb el codi país emissor, indicador de targeta caducada, indicador d'estat;

La versió 2.1 de l'adaptació PUP ABA corregeix la utilització del camp data de caducitat i codi de servei per donar compliment a la normativa PCI/DSS, habilita el procediment per fer devolucions i el procediment per fer transaccions manuals.

La versió 2.2 fa un nou esforç en la protecció de les dades del titular amb la desaparició del nom del titular de la missatgeria i el xifrat de les dades financeres a les transaccions d'entrada manual. També s'inclou el camp data/hora al càlcul del MAC .

La versió 2.3 implementa el tractament de les devolucions amb lectura de xip a través del missatge MSG0102 en lloc del inicialment previst, MSG0100. Amb aquest canvi, s'evita el intercanvi de criptogrames d'altra banda no possible donat que les devolucions en EMV es tracten com si operacions banda fossin. La versió 2.3 també incorpora el emmascarament parcial del PAN per tal d'acomplir amb els criteris PCI/DSS.

La versió 2.4 incorpora el següent:

- S'elimina el camp numero aleatori pel xifrat de pistes en els missatges MSG0300 i MSG0102, donat que l'algorisme emprat es el ECB.

- El codi de servei del missatge MSG0300 anirà sempre en clar, doncs aquest missatge, entre pinpad i tef, no està sotmès a xifrat, la qual cosa no es cap inconvenient pel que fa a PCI/DSS donat que el pan informat en el camp BIN té ombrejat part del seu contingut.

- S'indica que els camps associats a la signatura digitalitzada no viatgen quan el terminal no suporta dita funcionalitat.

- Es modifica el valor que tindrà el camp *Códigos de acción del terminal* en el missatge MSG0102.

- El camp *número de cajones inicializados* del missatge MSG2010 val sempre 00. Conseqüentment, els següents camps: *Número de cajón* i *informació cajón* no viatgen.

Els temes no tractats en aquest document es comportaran exactament igual que en els protocols originals de Sermepa.

1. TRACTAMENT MULTIENTITAT

Una de les característiques principals del pinpad és que ha de ser multientitat; això vol dir que disposa d'una matriu de calaixos i claus idèntica a la utilitzada al TPV EMV ABA. Per fes ús d'aquesta funcionalitat dins del PUP estàndard, cal afegir i modificar uns quants punts:

1.1 Afegir una memòria particular per a cada entitat. Aquesta memòria contindrà els següents conceptes:

- Utilització de MAC (Sí o No)
- Utilització de PIN Online en transaccions amb lectura de banda (Sí o No)
- Utilització de xifrat de dades (Sí o No)
- Utilització de la firma digitalitzada (Sí o No)
- Camps d'us futur

Tot està contingut en un camp d'un byte, amb els bits més pesants identificant MAC, PIN i Xifrat i la resta per usos futurs.

Byte 1:

MAC	**PIN**	**Xifrat**	**Firma digital**	**Ús futur**	**Ús futur**	**Ús futur**	**Ús futur**
8	7	6	5	4	3	2	1

El bit del PIN indica si el pinpad ha de demanar ó no el PIN a l'usuari, passant per davant del camp 'Bypass de PIN' del 'flag' de la 'Taula de Definició d'Aplicacions'. Si l'entitat no vol PIN en banda, posarà el bit 7 a '0' i no sortirà mai el missatge de petició en aquests casos; si el bit 7 està a '1' llavors l'entrada de PIN serà opcional.

En canvi, en EMV, el PIN es demanarà ó no en funció del que digui la targeta y la possibilitat de fer el bypass dependrà del flag de la 'Taula de Definició d'Aplicacions"

Aquestes memòries s'afegiran com a dades propietàries del missatge d'actualització de paràmetres MSG3000 (veure apartat 8).

1.2 Afegir dades propietàries al missatge MSG1000 per indicar per quina entitat es vol operar:

'01' Andbanc
'02' Crèdit Andorrà
'04' BIBM
'06' BPA
'08' BSA

Si no hi ha codi ó aquest no és correcte, el pinpad no farà res i anirà a repòs.

El missatge MSG1000 de la versió 1.4.0 contempla el camp 'cajón' on es situarà el codi de l'entitat.

La versió 2.1 incorpora a les dades propietàries del missatge MSG1000 el tipus d'operació que s'efectuarà a continuació: venda (00), devolució

(01). L'objectiu és que el PIN-PAD sàpiga quina mena de lectura i tractament de dades es produirà en el següent pas del flux transaccional.

1.3 Utilització ABA del missatge MSG0300.

El missatge MSG0300 s'utilitza per subministrar al comerciant informació bàsica de la targeta per tal de poder triar amb quina entitat/calaix es vol operar.

No porta les dades de la pista 2, és a dir, LPISTA2 serà zero.

La identificació de la targeta es fa amb els camps LBIN (forçat a 19 posicions per abastar qualsevol PAN) i BIN què conté el PAN amb els 6 primers dígits començant per l'esquerra en net, els 4 darrers dígits també en net i la resta del PAN ombrejada amb asteriscs.

1.4 Operativa d'operacions manuals.

Una operació amb entrada manual de dades, sigui venda o devolució, tindrà la següent seqüència :

De l'estat repòs s'enviarà un MSG1001; si es fa una entrada manual de dades, es recollirà el PAN entrat manualment en el camp BIN de la targeta del missatge MSG0300. Amb la informació obtinguda del MSG0300 el TEF triarà l'entitat i enviarà un MSG1000 amb l'entitat ('cajón') seleccionada i, si l'operativa és manual i es tracta d'una venda, acabarà de recollir les dades manuals que restin, això es, la caducitat i el CVV2 amb el missatge MSG0200; no seria necessari reintroduir el PAN perquè ja ha estat recuperat en el missatge MSG0300.

La versió 2.2 incrementa la seguretat de les transaccions manuals amb el xifrat de les dades financeres.

2. TRACTAMENT DEL PINBLOCK

2.1 Es modifica l'operativa d'usuari per demanar el pin on-line sempre que l'operació sigui una venda i la memòria de l'entitat ho determini.

]

2.2 La versió 1.4.0 porta un camp específic per omplir el PINBlock, per tant l'adaptació ABA la farà servir.

2.3 S'utilitza el camp "Número aleatori de diversificació de la clau de PIN", [NA], desdoblat a ASCII en 6 bytes.

3. TRACTAMENT DEL MAC

3.1 MAC ENTRE PIN-PAD I TERMINAL

En els missatges MSG0010, MSG0100,MSG0200 i MSG0102, s'afegeix el MAC a les dades propietàries.
Les dades del missatge font del MAC serien les següents:

Nº Sèrie del PIN-PAD	11	Numèric
PAN	19	Alfanumèric
Import	10	Numèric
Codi Operació	2	Numèric
Codi de resposta	3	Numèric
Nº d'autorització	6	Alfanumèric
Data/hora	12	Alfanumèric

- Els camps que no tinguin valor en el moment de la generació s'ompliran amb zeros.
- Els valors del camp 'Codi Operació' seran: '00' venda i '01' devolució. En el PUP no hi ha definida cap operació d'anul·lació. Per generar un MAC d'anul·lació el TEF ha de fer-ho amb el codi '30'. La versió 3.2 treu l'obligació de generar MAC en anul·lacions, podent substituir els 8 caràcters per 'high-values' hexadecimals (hex FF FF FF FF)
- El 'Codi de resposta' y el 'Nº autorització' no hi són quan es genera el missatge MSG0010, MSG0100, MSG0200 ó MSG0102. Només arriben al pinpad en cas de transacció EMV (tag 8A i tag 89) en el missatge MSG0110
- S'envien els 4 primers bytes del MAC calculat desdoblats a ASCII (8 caràcters).
- El camp data/hora està en format AAMMDDHHMMSS i es correspon amb la data/hora del PIN-PAD

3.2 VERIFICACIÓ/GENERACIÓ MAC ENTRE TERMINAL I PIN-PAD

S'afegeixen dos missatges nous: MSG5090 per verificar un MAC i MSG5091 per calcular-lo. Veure el format concret a l'apartat 9.

4. TRACTAMENT DE XIFRAT DE PISTES

Donat que el algorisme de xifrat serà l'ECB, el camp número aleatori de xifrat de pistes no viatjarà.

5. TRACTAMENTS ESPECÍFICS

5.1 PAN

Perquè la Gran Superfície disposi del PAN de la targeta en net, s'habiliten els camps 'LBIN' i 'BIN de la targeta' dels missatges MSG0010, MSG0100, MSG0300, MSG0101 i MSG0102 perquè portin aquesta informació en clar.

En aquest punt no cal fer res ja que el camp 'BIN de la targeta' ja va en clar. Això si, per tenir tot el PAN en clar cal posar el camp 'Longitud del BIN' de la taula 04 igual a 19, i fer el padeig adequat per ajustar la longitud real del PAN.

La versió 2.3 introdueix el ombrejat parcial del camp BIN de la targeta què contindrà el PAN amb les 6 primers dígits començant per l'esquerra en net, els 4 darrers dígits també en net i la resta del PAN ombrejada amb asteriscs.

5.2 NOM DEL TITULAR

La versió 2.2 del PUP ABA ja no contempla el camp 'nom del titular' en els missatges, ni de banda ni de xip. En el missatge MSG0010 el camp 'LPISTA1' anirà a zeros i el camp 'Lectura Pista1' no tindrà cap contingut.

5.3 DATA DE CADUCITAT I CODI DE SERVEI

Amb la finalitat d'ajustar-se a les normatives PCI/DSS, no es posen la data de caducitat ni el codi de servei en clar als missatges MSG0010 i MSG0102; tampoc s'inclouen els tags EMV respectius als missatges MSG0100/0101 quan hi hagi xifrat de dades.

5.4 ADQUISICIÓ DE DADES DEL MISSATGE D'INICIALITZACIÓ DEL PIN-PAD

La resposta del missatge d'inicialització, MSG2010, porta dades específiques de les entitats que ha de ser recollides per la Gran Superfície i traslladades al bit 48-55 de PUC.

6. DEVOLUCIONS AUTOMÀTIQUES

A partir de la versió 3.3, s'incorpora la possibilitat de realitzar devolucions parcials o totals sense introducció de la targeta o de les dades associades.

A tal efecte, en el missatge MSG1001, en el camp de dades propietàries, s'informaran els quatre darrers dígits del PAN de la targeta. El pinpad, en rebre aquesta dada, no sol·licita la introducció de la targeta i continua el flux enviant un MSG0300.En cas contrari, es a dir, si en el camp de dades propietàries no hi ha res informat, el pinpad sol·licita la introducció de la targeta.

7. TRACTAMENT DE TARGETES PROPIETÀRIES

A partir de la versió 3.3, s'incorpora la possibilitat de llegir, a través de pinpad, targetes no financeres.

A través del missatge MSG6000, la caixa sol·licita al pinpad llegeixi la banda magnètica de una targeta.

El pinpad envia el resultat de la lectura a través del missatge MSG6010.

Opcionalment, la caixa te la possibilitat de sol·licitar el pin de la targeta a través del missatge MSG6100.

El pinpad envia el pin en un bloc de format irreversible, fent servir un número aleatori que haurà rebut prèviament de la caixa a través del missatge MSG6100 i amb l'algorisme d'encriptació DES.

Exemple:

- Pin : 1234
- Número aleatori: 987654321098
- Dades d'entrada a DES: 1234987654321098 tant pel que seria dada a xifrar com la clau de xifrat.

En el cas de pin's de més de quatre posicions, les posicions a partir de la 5 solapen el número aleatori.

Exemple:

- Pin : 123456
- Número aleatori: 987654321098
- Dades d'entrada a DES: 1234567654321098 tant pel que seria dada a xifrar com la clau de xifrat.

8. MISSATGES MODIFICATS

MSG3000. ACTUALITZACIÓ DE PARÀMETRES

Camp	Longitud	Valor	Comentaris
Identificador de Mensaje	4	3000	Identificador para MSG3000
Longitud Mensaje	4	Variable	Longitud total del Mensaje
Versión de Parámetros EMV	3	XXX	Versión de parámetros que se envían al PinPad
Versión de claves Públicas	3	XXX	Versión de claves públicas
Separador entre Bloques	1	(40H)	
Bloque Parámetros de Configuración		01 – 09	El formato de estos bloques se especifica en punto 14
Separador	1	(41H)	
DATOS DE SEGURIDAD	Variable		Campo con las claves que necesitan ser telecargadas.
Separador	1	(3F)	
IdClave	1	0	Fixa a zero
Cifrado de Pistas	16	XXXX	Valor en Hexadecimal de cifrar IdClave + FlagCifrado, donde FlagCifrado: 0000001 -> Con Cifrado 0000002 -> Sin Cifrado
Separador dades propietàries	1	@ (40H)	Separador dades propietàries
Longitud de dades propietàries	3	016	Longitud del camp de dades propietàries.
Funcionalitats entitat 1	2	XX	Funcionalitats de l'entitat 1 segons l'apartat 1
Funcionalitats entitat 2	2	XX	Funcionalitats de l'entitat 2 segons l'apartat 1
Funcionalitats entitat 3	2	XX	Funcionalitats de l'entitat 3 segons l'apartat 1
Funcionalitats entitat 4	2	XX	Funcionalitats de l'entitat 4 segons l'apartat 1
Funcionalitats entitat 5	2	XX	Funcionalitats de l'entitat 5 segons l'apartat 1
Funcionalitats entitat 6	2	XX	Funcionalitats de l'entitat 6 segons l'apartat 1
Funcionalitats entitat 7	2	XX	Funcionalitats de l'entitat 7 segons l'apartat 1
Funcionalitats entitat 8	2	XX	Funcionalitats de l'entitat 8 segons l'apartat 1

MSG1000. NOTIFICACIÓ D'ESTAT DE LECTURA

Camp	Longitud	Valor	Comentaris
Identificador de Mensaje	4	1000	Identificador para MSG1000
Longitud Mensaje	4	0024	Longitud total del Mensaje
Importe de la transacción	10		Importe de la transacción, con el formato correspondiente al código de moneda. El formato para el Euro sería dos decimales : 1,45 → 0000000145 32 → 0000003200
Tabla para control de riesgo	02	' '	A blancs. Utilitzarem la taula de control de risc indicada a la taula 01
Cajón	2	XX	Codi Entitat segons l'apartat 1
Separador de dades propietàries	1	@ (40H)	Separador de dades propietàries
Longitud de dades propietàries	3	002	Longitud del camp de dades propietàries.
Tipus de transacció	2	XX	Versió ABA 2.1. Identifica el tipus de transacció per donar viabilitat a les devolucions. Valors possibles: 00 → Venda 01 → Devolució

MSG0010.LECTURA DE BANDA MAGNÈTICA

Camp	Longitud	Valor	Comentaris
Identificador de Mensaje	4	0010	Identificador para MSG0010
Longitud Mensaje	4	Variable	Longitud total del Mensaje
Flag de control	1	0 –1	Según se define en este mismo documento.
Resultado último intento de Chip	1	0 –2	Según se define en este mismo documento.
Tarjeta Caducada	1	0-1	0 No caducada 1 Caducada respecto fecha terminal
Indicador Contactless	1	0-1	0 No contactless1 Lectura contactless
LBIN	2	variable	Longitud del BIN, mínimo 6, máximo 19
BIN de la Tarjeta	LBIN	variable	BIN en claro de la targeta.
Código de Servicio	3	Variable	Código de servicio en claro o si hay cifrado de pistas va a ceros
Cifrado de Pistas	1	0 – 1	0 -> Indica que las pistas no irán cifradas. 1 -> Indica que las pistas irán cifradas.
Identificador de la clave	1	0	Fixe a zero
LPISTA1	4	Variable	Fixe a zeros
Lectura Pista1	LPISTA1		Sense contingut
LPISTA2	4	Variable	
Lectura Pista2	LPISTA2		Datos de la pista 2. esta información puede venir cifrada según anexo I.
Número aleatori pel xifrat del pinblock	6	Variable	Número aleatori de 6 caràcters numèrics (3 bytes desdoblats) emprats per xifrar el pinblock.
Bloque de PIN cifrado	16	Variable	Pinblock generat segons apartat 2
Indice de Zona de la clave de PIN	2	xx	Valor numérico del índice de zona de la clave de pin
Separador de dades propietàries	1	@ (40H)	Separador de dades propietàries
Longitud de dades propietàries	3	020	Longitud del camp de dades propietàries.
MAC	8	Variable	MAC generat segons l'apartat 3
Data/hora PIN-PAD	12	Variable	Data/hora del PIN-PAD usat per generació MAC

MSG0100. PETICIÓ ON-LINE EMV

Camp	Longitud	Valor	Comentaris
Identificador de Mensaje	4	0100	Identificador para MSG0100
Longitud Mensaje	4	Variable	Longitud total del Mensaje
LBIN	2	variable	Longitud del BIN, mínimo 6, máximo 19
BIN de la Tarjeta	LBIN	variable	BIN en claro de la targeta.
Código de Servicio	3	Variable	Código de servicio en claro. Si hay cifrado de pistas va a ceros.
Cifrado de Pistas	1	0 – 1	0 -> Indica que las pistas no irán cifradas. 1 -> Indica que las pistas irán cifradas.
Identificador de la clave	1	0	Fixe a zero
LPETA	4		Longitud del campo Petición de Autorización
Petición de Autorización	LPETA		La información se enviará en formato TLV de acuerdo a lo definido en las especificaciones EMV. Para evitar problemas en los carácteres de control, la información de este campo se codificará en hexadecimal.
Estado	4		0000 Petición Realizada 0001 Tarjeta no valida 0002 Operación Cancelada 0003 Aplicación Incorrecta
Códigos de acción del terminal	30		Se enviarán los códigos de acción del terminal

			aplicados a la transacción en curso. Este campo se codificará en hexadecimal
Número aleatori pel xifrat del pinblock	6	Variable	Número aleatori de 6 caracters numèrics (3 bytes desdoblats) emprats per xifrar el pinblock.
Bloque de PIN cifrado	16	Variable	Pinblock generat segons apartat 2
Indice de Zona de la clave de PIN	2	xx	Valor numérico del índice de zona de la clave de pin
Separador de dades propietàries	1	@ (40H)	Separador de dades propietàries
Longitud de dades propietàries	3	020	Longitud del camp de dades propietàries.
MAC	8	Variable	MAC generat segons l'apartat 3
Data/hora PIN-PAD	12	Variable	Data/hora del PIN-PAD usat per generació MAC

MSG0200.ENTRADA MANUAL

Camp	Longitud	Valor	Comentaris
Identificador de Mensaje	4	0200	Identificador para MSG0200
Longitud Mensaje	4	Variable	Longitud total del Mensaje
Flag de control	1	0 –1	Según se define en este mismo documento.
Resultado último intento de Chip	1	0 –2	Según se define en este mismo documento.
LNUMT	4		Longitud del campo Número de targeta. SI hi ha xifrat de dades va a zeros
Número de targeta	LNUMT		Información del número de targeta. SI hi ha xifrat de dades no té contingut
Caducitat	4		Fecha de caducidad de la targeta en formato "MMAA". SI hi ha xifrat de dades va a zeros
CVC2/CVV2	5		Si el cvc2/cvv2 introducido es inferior a 5 posiciones, se rellenará con el caracter 'X' por la izquierda. Si el titular no introdujo el CVC2/CVV2 se enviará XXXXX. SI hi ha xifrat de dades s'enviarà XXXXX.
Separador de dades propietàries	1	@ (40H)	Separador de dades propietàries
Longitud de dades propietàries	3	0xx	Longitud del camp de dades propietàries.
MAC	8	Variable	MAC generat segons l'apartat 3
Data/hora PIN-PAD	12	Variable	Data/hora del PIN-PAD usat per generació MAC
Xifrat Dades client	n		Xifrat de la cadena LNUMT+Número de targeta+Caducitat+CVC2/CVV2

MSG0300. LECTURA PISTA 2

Camp	Longitud	Valor	Comentaris
Identificador de mensaje	4	0300	Identificador para mensaje 0300
Longitud Mensaje	4	Variable	Longitud total del Mensaje
Flag de control	1	0 –1	Según se define en este mismo documento.
Resultado último intento de Chip	1	0 –2	Según se define en este mismo documento.
Tarjeta Caducada	1	0-1	0 No caducada 1 Caducada respecto fecha terminal
Indicador Contactless	1	0-1	0 No contactless 1 Lectura contactless
LBIN	2	Variable	Longitud del BIN, mínimo 6, máximo 19
BIN de la Tarjeta	LBIN	Variable	BIN en claro de la targeta.
Código de Servicio	3	Variable	Código de servicio.
Cifrado de Pistas	1	0	Fixa a zero.
Identificador de la clave	1	0	Fixa a zero.

LPISTA2	4	0000	
Lectura Pista2	LPISTA2		Sense dades
Separador de dades propietàries	1	@ (40H)	Separador de dades propietàries
Longitud de dades propietàries	3	Variable	Longitud del camp de dades propietàries.
Datos propietarios	xxx	Variable	Contendrá los datos propietarios

MSG2010.RESPOSTA DEL MISSATGE D'INICIALITZACIÓ

La resposta del missatge d'inicialització, inclourà dins de dels dades propietàries les funcionalitats de cada entitat, assignades amb anterioritat en el missatge MSG3000:

Camp	Longitud	Valor	Comentaris
Identificador Missatge	4	2010	Identificador para MSG2010
Longitud Missatge	4	XXXX	Longitud total del Missatge
Número de sèrie	11	Número de sèrie	Número de sèrie del pinpad farcit amb zeros fins completar la longitud.
Mida Buffer Recepció	8		Mida en Bytes del buffer de recepció del pinpad. Es farcirà amb 0 per l'esquerra fins completar la longitud.
Versió de claus públiques RSA	3	XXX	Versió de claus RSA carregada en el PIN-PAD EMV
Versió de claus simètriques	3	000	Fixa a zeros
Versió de paràmetres	3	XXX	Versió de paràmetres que té carregat el pinpad. 000 -> Indica la falta de paràmetres.
Fabricant	2	CC	Valor del Fabricant
Model	2	MM	Valor del Model
Funcionalitats	2	00	Fixa a zeros
Nom del programa software	8	XXXXXXXX	Nom assignat pel fabricant al programa
Versió del Software del pinpad	4	NNNN	4 caràcters numèrics
Versió d'especificacions	2	Variable	'14'
Número de cajones inicializados	2	nn	Aquests camps els posem per alinear-nos amb el protocol 1.4.0. El seu valor serà 00 i conseqüentment, els camps número de cajón i información cajón no viatgen.
Número de cajón	2	CC1	..
Información cajón	Variable	Datos	..
		...	..
Número de cajón	2	CCn	..
Información cajón	Variable	Datos	..
Separador de dades propietàries	1	@ (40H)	Separador de dades propietàries
Longitud de dades propietàries	3	052	Longitud del camp de dades propietàries.
Versió de claus simètriques 1	3	XXX	Versió de claus simètriques de l'entitat 1
Funcionalitats 1	2	XX	Funcionalitats de l'entitat 1
Versió de claus simètriques 2	3	XXX	Versió de claus simètriques de l'entitat 2
Funcionalitats 2	2	XX	Funcionalitats de l'entitat 2
Versió de claus simètriques 3	3	XXX	Versió de claus simètriques de l'entitat 3
Funcionalitats 3	2	XX	Funcionalitats de l'entitat 3
Versió de claus simètriques 4	3	XXX	Versió de claus simètriques de l'entitat 4
Funcionalitats 4	2	XX	Funcionalitats de l'entitat 4

Camp	Longitud	Valor	Comentaris
Versió de claus simètriques 5	3	XXX	Versió de claus simètriques de l'entitat 5
Funcionalitats 5	2	XX	Funcionalitats de l'entitat 5
Versió de claus simètriques 6	3	XXX	Versió de claus simètriques de l'entitat 6
Funcionalitats 6	2	XX	Funcionalitats de l'entitat 6
Versió de claus simètriques 7	3	XXX	Versió de claus simètriques de l'entitat 7
Funcionalitats 7	2	XX	Funcionalitats de l'entitat 7
Versió de claus simètriques 8	3	XXX	Versió de claus simètriques de l'entitat 8
Funcionalitats 8	2	XX	Funcionalitats de l'entitat 8
Data/hora PIN-PAD	12	Variable	Data/hora del PIN-PAD

MSG0102. CONFIRMACIÓ DE LA TRANSACCIÓ OFFLINE.

Missatge per les devolucions amb lectura de xip.

Campo	Longitud	Valor	Comentarios
Identificador de Mensaje	4	0102	Identificador para MSG0102
Longitud Mensaje	4	Variable	Longitud total del Mensaje
LBIN	2	variable	Longitud del BIN, mínimo 6, máximo 19
Bin de la Tarjeta	LBIN	variable	Bin en claro de la targeta.
Código de Servicio	3	Variable	Código de servicio en claro. Si hi ha xifrat de dades va a zeros.
Cifrado de Pistas	1	0 – 1	0 -> Indica que las pistas no irán cifradas. **1 -> INDICA QUE LAS PISTAS ESTÁN CIFRADAS.**
Identificador de la clave	1	0	Fixe a 0.
LRESPA	4		Longitud del campo respuesta
Respuesta a la Autorización	LRESPA		La información se enviará en formato TLV de acuerdo a lo definido en las especificaciones EMV. Para evitar problemas en los carácteres de control, la información de este campo se enviará desdoblando cada caracter hexa en un byte ASCII. Sols hi haurà el TAG57, pista 2 equivalent
Estado	4		0000 Petición aceptada 0001 Tarjeta no valida 0002 Operación Cancelada 0003 Aplicación Incorrecta 0004 Petición denegada
Códigos de acción del terminal	30		Zeros
Separador	1	@ (40H)	Separador
Tipo de información	4		En este campo se indicará el tipo de información enviada: 0000 → No existe firma. 0001 → No existe firma, se ha cancelado la introducción de la firma. 0002 → firma digitalizada.
Longitud de la firma	4	Variable	Longitud del campo que ocupará la firma.
Firma digitalizada	XXXX	Variable	Contendrá la firma digitalizada. La información estará formada por los siguientes campos: - 2 carácteres de formato: ▪ 00: Formato propietario

			▪ 01: BMP ▪ 02: JPG ▪ 03: TIF ▪ 04: GIF ▪ .... - Firma digitalizada: Se enviará cada byte hexadecimal desdoblado para evitar coincidéncia con carácteres de control.
Separador de dades propietàries	1	@ (40H)	Separador de dades propietàries
Longitud de dades propietàries	3	020	Longitud del camp de dades propietàries.
MAC	8	Variable	MAC generat segons l'apartat 3
Data/hora PIN-PAD	12	Variable	Data/hora del PIN-PAD usat per generació MAC

MSG1001. DEVOLUCIÓ AUTOMÀTICA.

En el cas de devolucions automàtiques, en el camp 'Id. Mensaje a mostrar' s'informa 0001, en la 'longitud de datos propietarios' 4 i a continuació els quatre darrers dígits del pan.

Campo	Longitud	Valor	Comentarios
Identificador de Mensaje	4	1001	Identificador para MSG1000
Longitud Mensaje	4	0012	Longitud total del Mensaje
Id. Mensaje a mostrar	4	Variable	0001 – Devolución 0002 – Lectura
Separador para datos popietarios	1	@ (40H)	Separador de datos propietarios
Longitud de datos propietarios	3	004	Longitud del campo de datos propietarios.
4 darrers dígits del PAN	4	xxxx	

9. MISSATGES NOUS

MSG5090.GENERACIÓ DE MAC

Camp	Longitud	Valor	Comentaris
Identificador Missatge	4	5090	Identificador pel missatge 5090
Longitud Missatge	4	Variable	Longitud total del missatge
Codi Entitat	2	XX	Codi de l'entitat
LDADES	4	Variable	Longitud de les dades de les que s'ha de calcular el MAC.
Dades	LDADES	Variable	Dades de les que s'ha de calcular el MAC

MSG5190. RESPOSTA A LA GENERACIÓ DE MAC

Camp	Longitud	Valor	Comentaris
Identificador Missatge	4	5190	Identificador pel missatge 5190
Longitud Missatge	4	0010	Longitud total del missatge
Resultat	2	Variable	Resultat de l'operació
MAC	8	Variable	MAC calculat (si el resultat es "00")

MSG5091 VALIDACIÓ DE MAC

Camp	Longitud	Valor	Comentaris
Identificador Missatge	4	5091	Identificador pel missatge 5091
Longitud Missatge	4	Variable	Longitud total del missatge
Codi Entitat	2	XX	Codi de l'entitat
LDADES	4	Variable	Longitud de les dades de les que s'ha de validar el MAC.
Dades	LDADES	Variable	Dades de les que s'ha de calcular el MAC
MAC	8	Variable	MAC a validar

MSG5191. RESPOSTA A LA VALIDACIÓ DE MAC

Camp	Longitud	Valor	Comentaris
Identificador Missatge	4	5191	Identificador pel missatge 5191
Longitud Missatge	4	0002	Longitud total del missatge
Resultat	2	Variable	Resultat de l'operació ('00'=OK, altres=KO)

MSG6000.PETICIÓ LECTURA TARGETA PROPIETÀRIA.

Camp	Longitud	Valor	Comentaris
Identificador Missatge	4	6000	Identificador pel missatge 6000
Longitud Missatge	4	Variable	Longitud total del missatge
Time-out	3	XXX	Nombre de segons a esperar la lectura de la targeta
Perifèric	1	X	Valor fixe: 1.
Longitud missatge a pantalla	2	XX	Indica la longitud del següent camp
Missatge a pantalla	L'indicat en el camp	X	Màxim de 16 caràcters per línia i 4 línies.

	anterior		

MSG6010. RESPOSTA LECTURA TARGETA PROPIETÀRIA.

Camp	Longitud	Valor	Comentaris
Identificador Missatge	4	6010	Identificador pel missatge 6010
Longitud Missatge	4	XX	Longitud total del missatge
Codi de resposta	2	XX	Possibles valors: 00: OK 01: Error lectura. No s'ha pogut llegir cap pista. 02: cancel·lació per part de l'usuari. 03: cancel·lació per time-out. 10: error en el format del missatge. 11: error, es una targeta financera.
Longitud pista 1	2	XX	Longitud del contingut del següent camp
Pista 1	Variable	XX	Contingut de la pista 1
Longitud pista 2	2	XX	Longitud del contingut del següent camp
Pista 2	Variable	XX	Contingut de la pista 2
Longitud pista 3	2	XX	Longitud del contingut del següent camp
Pista 3	Variable	XX	Contingut de la pista 3

MSG6100.PETICIÓ PIN TARGETA PROPIETÀRIA.

Camp	Longitud	Valor	Comentaris
Identificador Missatge	4	6100	Identificador pel missatge 6100
Longitud Missatge	4	Variable	Longitud total del missatge
Time-out	3	XXX	Nombre de segons a esperar el tecleig del pin
Dades	12	X	Número aleatori per calcular el bloc de pin irreversible.
Nombre mínim de dígits del pin	2	XX	Nombre mínim de dígits que ha de tenir el pin teclejat.
Nombre màxim de dígits del pin	2	XXX	Nombre màxim de dígits que ha de tenir el pin teclejat.
Longitud missatge a pantalla	2	XX	Indica la longitud del següent camp
Missatge a pantalla	L'indicat en el camp anterior	X	Màxim de 16 caràcters per línia i 2 línies.

MSG6110.RESPOSTA PIN TARGETA PROPIETÀRIA.

Camp	Longitud	Valor	Comentaris
Identificador Missatge	4	6110	Identificador pel missatge 6110
Longitud Missatge	4	Variable	Longitud total del missatge
Codi de resposta	2	XX	Possibles valors: 00: OK 02: cancel·lació per part de l'usuari. 03: cancel·lació per time-out. 10: error en el format del missatge. 20: no hi ha número aleatori informat.
Bloc de pin	16	Hexadeci	Aquest camp sols estarà informat quan el codi de

		mal	resposta sigui = 00.