ESPECIFICACIONS TÈCNIQUES PUC EMV. ADAPTACIÓ DE L'ABA

LLISTA DE MODIFICACIONS

Autor	Data	Versió	Comentaris
JRC	2.008	0.0	Creació del document
JCS	Juny 2.009	1.0	Esborrany
JCS	Agost 2.009	1.1	Incorporació de la capçalera amb la longitud
			del missatge.
JCS	Desembre 2.009	2.0	Versió revisada.
			Túnels IPSec per xifrat del canal.
JCS	Setembre 2.010	2.1	Nou codi d'acció per operacions autoritzades
			prèvia identificació
PNB	Octubre 2.011	2.2	Modificació punt 5, afegint l'obligatorietat
			del comerç a complir amb PA-DSS
JCS	Febrer 2.012	2.3	Modificació punt 3.3.2, tractament de les
			anul.lacions automàtiques i devolucions
			centralitzades.
JCS	Juliol 2.012	2.4	Relatiu a les certificacions. Modificació del
			punt 5.
MCC	Novembre 2.013	2.5	Comunicacions xifrades. Modificació del punt 1.1
JRC	Setembre 2014	2.6	No obligatorietat del càlcul de MAC en anul·lacions

0. INTRODUCCIÓ

El present document pretén recollir les consideracions tècniques i operatives de l'adaptació del 'Protocolo Unificado de Comercios PUC-EMV' a les necessitats de l'ABA.

Es tracta d'un document de treball dinàmic, on s'aniran recollint totes les especificacions que la comissió tècnica de l'ABA consideri convenients.

Els temes no tractats en aquest document funcionaran exactament igual que en els protocols PUC originals de Servired/4B/Euro6000.

El públic objectiu d'aquest document és el personal tècnic i de negoci encarregat de desenvolupar el protocol PUC-ABA a les Grans Superfícies.

D'entrada el document tindrà cinc apartats principals:

- Funcionalitats bàsiques
- Adaptacions del PUC
- Adaptacions del Protocol de comunicacions del PIN-PAD
- Protecció de dades
- Certificació

1. FUNCIONALITATS BÀSIQUES

1.1 ENTORN DE COMUNICACIONS

L'entorn de comunicacions entre la Gran Superfície i els bancs estarà basat en el protocol TCP/IP. La connectivitat principal s'efectuarà a través d'una xarxa IPSilon. Opcionalment, les grans superfícies podran configurar un accés de backup a través de línies XDSI.

Tota comunicació fora de l'abast de la xarxa internet Empreses ABA, haurà de ser xifrada.

L'entorn de Grans Superfícies serà Online pur.

El timeout de la comunicació de missatges entre el servidor de la Gran Superfície i el Centre Autoritzador del banc serà com a mínim de 25 segons.

La connexió podrà ser permanent o commutada, cada Gran Superfície només podrà tenir dues connexions establertes a l'hora.

Tots els missatges PUC incorporaran un primer camp de 2 bytes on s'indicarà la longitud en binari del missatge i sense comptar aquest 2 bytes, tal com estableix la especificació PUC per protocols de comunicació sobre IP.

1.2 DESCRIPCIÓ DE LES DADES D'USUARI

La versió 2.0 del PUC EMV de Sermepa està basada en connexions X25 i utilitza dades d'usuari al paquet de trucada per identificar varis aspectes de l'usuari i la connexió. L'adaptació ABA serà sobre protocol TCP/IP i aprofitarà el concepte de dades d'usuari per obtenir informació què pot ser útil per l'aplicació. D'aquesta manera, un cop realitzada la connexió IP, s'ha d' enviar un paquet de dades d'usuari similar al proposat a l'especificació bàsica amb algunes adaptacions ABA.

IE 0 RRRRR AA FFFFFFFFF C TT EE N 0

IE	Identificador de l'element connectat. Per defecte 'C7'
R	Valor reservat. Per defecte '00000'
A	Identificador de l'aplicació a enllaçar. Per defecte '13'
F	FUC del comerç
C	Tipus de servei connectat (0= Gran Superfície, 1= TPV-PC)
T	Tipus d'entorn. (00=proves, 01=certificació, 11= real)
E	Número d'enllaç. Normalment valdrà '01', si hi han varis enllaços prendrà valors seqüencials.
N	Atribut d'enllaç. Per defecte '0'.
0	Valor '0'

1.3 TARGETES ACCEPTADES

S'acceptaran totes les targetes de les marques VISA i MasterCard.
No s'acceptarà cap altres tipus de targeta financera o privada.

1.4 MÈTODES D'AUTENTICACIÓ DEL TITULAR

S'acceptaran els següents mètodes per autenticar el titular:

- PIN Online
- PIN Offline
- Signatura

Sempre seguint les regles marcades pels emissors de les targetes, les marques i les pròpies especificacions EMV.

1.5 OPERACIONS PERMESES

Es podran fer els següent tipus d'operació:

- Vendes
- Devolucions (sempre procedents d'una operació original)
- Anul·lacions automàtiques
- Recàrregues de mòbil
- Preautoritzacions
- Operacions administratives: Consulta de Totals per terminal
  Tancament i conciliació per terminal
  Control de diàleg

No es podran fer les següents operatives:

- Operativa DCC
- Missatgeria d'actualització de fitxers i llistes negres
- Devolucions no procedents d'operacions originals
- Consulta de Totals global per tota una Gran Superfície.

1.6 SEGURETAT DE LA MISSATGERIA

La missatgeria adaptada PUC-ABA portarà les següents mesures de seguretat:

- Pista 2 xifrada
- MAC d'anada i tornada
- PINBlock xifrat

Els tres elements de seguretat i protecció aniran xifrats amb claus propietàries i residents al PIN-PAD.

Addicionalment, es xifrarà el canal de comunicació a través de túnels IPSec construïts a partir d'equipaments tipus router.

1.7 MODES D'ADQUISICIÓ DE DADES

S'accepten els següents mètodes d'adquisició de dades de la targeta:

- Lectura de xip EMV
- Lectura de Banda Magnètica
- Entrada manual de dades

També es permetran operatives especials com :

- Fallback
- Bypass PIN

La facultat d'autoritzar o no les transaccions incorporant dites operatives especials també radiquen en l'emissor de la targeta i en qualsevol cas poden estar subjectes a canvis operatius en el temps.

2. ADAPTACIONS DEL PUC

Les adaptacions ABA apliquen sobre el document:

'Especificaciones técnicas. Protocolo unificado de Comercios (PUC). Adaptación a EMV' versión 2.0.

És altament recomanable que els proveïdors de Grans Superfícies demostrin la seva certificació amb les versions PUC 2.0 el que facilitarà en gran mesurà la adaptació ABA. Els proveïdors de Grans Superfícies hauran de certificar en un entorn de proves les adaptacions ABA amb tots els bancs andorrans abans de poder entrar en producció.

Les operatives permeses i les no acceptades estan recollides en l'apartat 1.4 del present document.

2.1 CONCEPTE TERMINAL/COMERÇ vs ADQUIRENT

El protocol PUC original preveu la utilització del Bit 32 'Código Identificación de Adquirente' com identificació de l'origen del missatge.

L'adaptació ABA inclou els Bits 41 i 42 'Identificación del Terminal' i 'Identificación del Establecimiento' com elements obligatoris en les missatgeries de venda, devolució, anul·lació automàtica i Consulta de totals per terminal; per poder identificar completament el punt de venda. El bit 32 s'haurà de seguir enviant i contindrà el FUC del comerç.

La comissió tècnica de l'ABA gestionarà els valors assignats a aquests camps per cada Gran Superfície.

2.2 CAMP D'INFORMACIÓ COMPLEMENTÀRIA

El protocol PRICE conté el bit 48-55, el qual serveix per subministrar informació complementària de la transacció.

L'adaptació ABA inclou aquest bit dins els camps obligatoris en transaccions comptables (vendes, devolucions, anul·lacions), tant en els missatges de petició del comerç cap el banc com en els missatges de resposta del banc cap el comerç.

Aquest camp servirà per obtenir informació, procedent del PIN-PAD, sobre número de sèrie del PIN-PAD, versions de claus, versions de paràmetres, versions de software i altres característiques del terminal i la transacció.

Camp	Longitud	Valor	Comentaris
Longitud Missatge	3	**XXX**	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	XXXXXXX	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	
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	040	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
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 del PIN-PAD	12	Variable	Data Hora del PIN-PAD per generació MAC

El bit 48-16 no és necessari perquè conté informació redundant amb el 48-55.

2.3 DADES CRIPTOGRÀFIQUES

Totes les claus de PIN, MAC i xifrat de pistes i dades sensibles residiran al PIN-PAD.

El protocol PUC adaptat enviarà el contingut del PINBlock en el bit 52, tal i com ha estat rebut del PIN-PAD

El protocol PUC adaptat enviarà el contingut del MAC en els bits 64/128, tal i com ha estat rebut del PIN-PAD. Així mateix rebrà el MAC de resposta en el mateix camp i l'haurà de verificar amb el PIN-PAD amb una nova transacció de generació/verificació de MAC definida per al PIN-PAD ABA i descrita en l'apartat 3 d'aquest document.

Omplir el MAC d'enviament i tractar el de recepció, és obligatori a les transaccions de venda, devolució i opcional a les anul·lacions.

El protocol PUC adaptat enviarà la pista 2 xifrada, tal i com ha estat generada pel PIN-PAD, dins el bit 48-35. Si la configuració de l'entitat al PIN-PAD no té habilitat el xifrat de dades, llavors la pista 2 en net viatjaria al bit 35.

2.4 OPERATIVA DE RECÀRREGA DE MÒBIL

L'operativa de Recàrrega de Mòbil s'instrumentarà com una venda amb el camp PRICE P48-24 'Identificació del Telèfon' informat, i amb P24=282.

2.5 OPERATIVA DE PREAUTORITZACIONS

Les preautoritzacions engloben tres possibles transaccions cap a les entitats:

- Petició de preautorització: S'instrumenta amb un missatge 1200, similar a la venda amb el camp P24=101
- Confirmació de preautorització: S'utilitzarà el missatge 1220 amb P24=101 i P56 informat
- Cancel·lació de preautorització: S'utilitzarà el missatge 1220 amb P24=103 i P56 informat

2.6 OPERATIVA DE CONCILIACIÓ

L'operativa de tancament/conciliació es farà sempre a nivell de terminal. Totes les transaccions comptables rebran els P28 i P29 informats des de l'entitat, que és qui gestionarà aquests valors per reconèixer les sessions comptables entre comerç i banc.

3. ADAPTACIONS DEL PROTOCOL DE COMUNICACIONS DEL PIN-PAD

El model únic de PIN-PAD triat i proporcionat per l'ABA és l'Ingenico iPP320 o equivalent.

Les adaptacions ABA d'aquest estan basades en el document:

'PIN-PAD EMV Integrado. Protocolo de Comunicación' versió 1.4.0.

Els proveïdors de Grans Superfícies hauran de certificar les aplicacions de Grans Superfícies amb el PIN-PAD i la versió esmentades.

La missatgeria de display entregada pel PIN-PAD serà similar a la presentada pel TPV EMV ABA de sobretaula.

3.1 TRACTAMENT MULTIENTITAT

Un únic terminal PIN-PAD donarà servei a totes les entitats de l'ABA.

Perquè la Gran Superfície pugui indicar al PIN-PAD per quina entitat vol operar s'utilitzarà el missatge MSG1000 'Notificació d'estat de lectura' del TEF al PIN-PAD, el qual disposa del camp '*cajón*' on el TEF podrà posar, amb la codificació numèrica d'entitats ABA, el valor de l'entitat on vol destinar la transacció:

ENTITAT	CALAIX	CSB
Andbanc	01	9924
Crèdit Andorrà	03	9920
BIBM	04	9922
BPA	06	9923
BSA	08	9925

Per altra banda, el missatge MSG0300 serà utilitzat per ABA per facilitar al TEF la informació del PAN i ajudar al comerç en la tria de l'entitat on dirigir l'operació. Aquest missatge portarà el camp LPISTA2 (longitud de la pista 2) igual a 0, el camp 'Lectura Pista2' sense dades i el camp BIN amb el PAN informat. Dit PAN tindrà ombrejades amb '*' totes les posicions a excepció de les 6 primeres i les quatre darreres.

El bit 48-01 'Código de Banco' portarà el codi CSB de l'entitat triada pel comerciant.

3.2 TRACTAMENT PINBLOCK

El PINBlock serà generat i xifrat dins el PIN-PAD.

En els missatges: MSG0010 'Lectura de BM' i MSG0100 'Petició On -Line EMV', del PIN-PAD al TEF, dins el camp 'Pinblock' viatjarà, si s'escau, el PINBlock generat pel PIN-PAD. Les transaccions manuals no portaran PIN.

Dels missatges: MSG0010 'Lectura de BM' i MSG0100 'Petició On-Line EMV', també s'aprofitarà el camp 'Número aleatori per xifrat de pinblock' per introduir-hi el número aleatori de diversificació de la clau de PIN. Aquest valor s'haurà de transportar a les posicions 11-16 del bit 53 de PUC per remetre'l al centre autoritzador del banc.

3.3 TRACTAMENT DEL MAC

El MAC, generat pel PIN-PAD, serà el mètode d'autenticació del missatge PUC enviat pel comerciant. Així mateix, també hi haurà MAC de tornada a la resposta al comerç.

El MAC s'utilitzarà en les transaccions de venda, devolució i opcionalment en anul·lacions.

3.3.1 DESCRIPCIÓ DEL MAC.

És un MAC propietari de l'adaptació ABA.

Les dades amb les quals es generarà/verificarà el MAC són 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 Numèric

Els camps que no tinguin valor en el moment de la generació s'ompliran amb zeros. El MAC es generarà per les transaccions de venda i devolució, essent opcional el càlcul en les anul·lacions. Si no es calcula en anul·lacions, llavors s'haurà d'omplir amb 'high values' hexadecimals (hex FF).

Els valors del camp 'Codi Operació' seran: 00 venda, 01 devolució i 30 anul·lació

El camp data/hora té el format AAMMDDHHMMSS i conté la data/hora del PIN-PAD utilitzada en la generació del MAC.

La següent taula explica com s'obtenen les dades necessàries pel càlcul de MAC en cada cas:

	Peticions (de comerç a banc)	**Respostes** (de banc a comerç)	**Anul·lacions**	
			Peticions (de comerç a banc)	**Respostes** (de banc a comerç)
N.Sèrie PinPad	del P48-55	del P48-55	del P48-55	del P48-55
PAN	(a)	P48-37	zeros	zeros
Import	P4	P4	P4	P4
Codi operació	00 si venda 01 si devolució	00 si venda 01 si devolució	30	30
Codi resposta	zeros	P39	zeros	P39
N. autorització	zeros	P38 si arriba en el missatge, zeros en cas contrari	zeros	zeros
Data/hora	del P12	del P48-55	del P48-55	del P48-55

(a) El PAN s'obté en funció del tipus de captura de la informació de la targeta que s'hagi realitzat: en operacions EMV, de la pista2 equivalent (TAG 57); en operacions amb lectura de banda, de la pista 2, P48-35 si la pista 2 va xifrada o P35 si va en clar; en operacions manuals, P48-35 si hi ha xifrat de dades sensibles i P2 si van en clar.

En qualsevol cas, la obtenció de dades per el càlcul o la verificació del MAC, sols haurà de ser gestionat pel comerç en les respostes i en les peticions i respostes de les anul·lacions.

En peticions, el MAC resultant (4 bytes) serà comunicat al TEF dins les dades propietàries dels missatges MSG0100, MSG0200 i MSG0010. També viatjarà, dins les dades propietàries, el valor del camp 'data/hora' del PIN- PAD ; aquest valor es traslladarà al final del camp P48-55 perquè les entitats puguin tenir tota la informació necessària per validar el MAC.

Si el comerç ha de calcular MAC's per transaccions centralitzades d'anul·lacions i devolucions, pot utilitzar un valor del camp data/hora propi què haurà de comunicar igualment al P48-55.

3.3.2 VERIFICACIÓ/GENERACIÓ MAC

El PIN-PAD disposarà d'uns nous missatges (MSG5090/MSG5190, MSG5091/MSG5191), que permetran generar/verificar el MAC resultant sobre unes dades d'entrada i aplicant la clau de MAC d'un calaix específic. Els missatges MSG0010, MSG0200 i MSG0100 ja disposen del MAC generat dins les dades propietàries.

La nova missatgeria haurà de ser utilitzada obligatòriament pel TEF per verificar el MAC rebut des dels centres autoritzadors.

D'altra banda, el nou missatge serviria al TEF per generar el MAC en els casos de transaccions no necessàriament iniciades al PIN-PAD, com ara les anul·lacions i devolucions amb entrada manual de dades. Per exemple, en el cas de timeout's en resposta, es poden generar anul·lacions automàtiques preventives. Un possible modus operandi consistiria en demanar al Pinpad que està realitzant una operació, el possible MAC de anul.lació i en el cas que cas que es produeixi el timeout utilitzar-lo per efectuar la anul.lació. Recordem que el càlcul del MAC d'anul·lació és opcional i es pot substituir enviant 8 caràcters 'high-values' en el bit 64/128

Per cobrir les casuístiques de devolucions no presencials generades per sistemes centralitzats; es pot comptar amb un PIN-PAD de gestió, connectat al servidor del comerciant i què seria utilitzat per la generació i validació de MACs en aquestes transaccions. A tenir present però que el número de terminal informat haurà de ser el corresponent al quin prèviament haurà efectuat la venda. De no ser així, la devolució no serà acceptada per banc adquirent. Es tractaria de devolucions manuals, on es possible introduir solament els quatre darrers dígits del número de la targeta.

3.4 TRACTAMENT DE XIFRAT DE PISTES I DADES SENSIBLES

Cada entitat tindrà definides unes funcionalitats específiques, establertes a través de la configuració del PinPad, entre les quals hi ha la possibilitat de xifrat de pistes i dades sensibles.

La pista 2 anirà xifrada en mode ECB, mode *omplir* a 1 i *padeig* a 1, d'acord amb l'algorisme de xifrat de dades exposat a la especificació bàsica de Sermepa. Es tracta d'un tractament similar al TPV EMV ABA.

També es podran xifrar, amb el mateix mètode anterior, les dades sensibles de les transaccions manuals: PAN, caducitat i CVV2. En aquest cas, el comerciant haurà de traslladar la informació xifrada al camp P48-35, i si no estès habilitat el xifrat de dades ho haurà de traslladar als camps P2, P14 i P48-11.

3.5 TRACTAMENTS ESPECÍFICS

3.5.1 PAN

Per tal que la Gran Superfície disposi d'informació del PAN de la targeta, s'habilitaran els camps 'LBIN' i 'BIN de la targeta' dels missatges MSG0010, MSG0100 i MSG0300 que contindrà les 6 primeres posicions i les quatre darreres en clar. La resta de posicions estaran ombrejades amb asteriscs.

3.5.2 NOM DEL TITULAR

A fi de protegir les dades sensibles de la targeta, no viatjarà el nom del titular en camp missatge del PUP ABA.

3.5.3 DATA DE CADUCITAT

La data de caducitat no s'inclourà a les transaccions de lectura de banda i xip per tal d'acomplir els criteris de seguretat establerts per PCI/DSS. Específicament no ha de viatjar si la pista 2 va xifrada, essent aquest punt una premissa de l'adaptació ABA Les transaccions manuals sí que poden portar la data de caducitat, però anirà xifrada si la configuració per l'entitat així ho estableix. .

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

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

El contingut específic per l'ABA del missatge MSG2010 es és troba a les especificacions PUP ABA.

3.5.5 TRANSACCIONS AMB ENTITAT PREDEFINIDA PEL COMERCIANT

És possible que alguns comerços tinguin predefinida l'entitat amb la qual volen treballar. Per aquests casos, si la transacció és una venda, haurien d'utilitzar el flux definit a la versió PUP ABA i passar primer pel camí 1001/1011 i 0300/0310. Per als casos de devolucions no presencials generades per sistemes centralitzats de gestió, només caldria recollir del PIN -PAD el MAC adequat per la transacció amb els missatges de MAC habilitats en el PUP ABA.

3.5.6 PROCEDIMENT PER FER DEVOLUCIONS

El missatge MSG0300 del PUP ABA està destinat a subministrar part del PAN al comerciant per tal que aquest pugui triar l'entitat . Aquesta utilització repercuteix en la pèrdua de les funcionalitats per devolucions del PUP estàndard.

A fi de reincorporar aquesta funcionalitat, s'ha inclòs el camp 'Tipus de transacció' a les dades propietàries del MSG1000. Amb aquesta informació el PIN-PAD podrà operar els missatges de lectura manual, banda i EMV d'acord amb el tipus de transacció sol·licitat pel comerciant.

En el cas de devolucions amb lectura de xip, el missatge a utilitzar serà el MSG0102.

Per poder facilitar la identificació de l'operació original s'inclourà obligatòriament, en el missatge 1220 de les transaccions de devolució, el bit P56 'Elemento de Datos Adicionales'.

3.5.7 CODIS D'ACCIÓ.

Addicionalment als codis de raó (P-39) especificats en el PUC, l'adaptació ABA preveu el codi

001, autoritzada prèvia identificació del titular

A pesar que a tots els efectes la operació s'ha de considerar com a autoritzada, en aquest cas el comerciant haurà d'identificar sempre al titular, amb independència del mètode d'autenticació d'aquest (pin, signatura o cvv2) realitzat.

En la butlleta del comerciant haurà de constar la menció:

DNI / PASS .....

on el comerciant informarà del número del document identificació del titular validat.

4. PROTECCIÓ DE DADES

Les entitats bancàries, com responsables davant les marques internacionals dels seus comerços, han de tenir cura de les bones pràctiques a l'hora de protegir la confidencialitat de les dades dels titulars de targetes de crèdit/dèbit.

S'han d'establir garanties sobre la informació confidencial que viatja des del PIN-PAD i dels terminals fins als servidors, i sobre l'emmagatzemament i utilització que se'n fa de la mateixa.

En aquest marc, l'establiment haurà de seguir les recomanacions internacionals de seguretat PCI-DSS (Payment Card Industry. Data Security Standards). Es pot trobar informació sobre aquestes normes a: http://www.visaeurope.com/documents/ais/merchants_guide.pdf

El PIN- PAD proporcionat per les entitats tindrà els nivells d'encriptació necessaris per protegir les dades essencials.

5. CERTIFICACIÓ

L'ABA demanarà la certificació del protocol PUP EMV ABA, per cada instal·lació de Gran Superfície i per a totes les entitats.

Les aplicacions de pagament dels comerços hauran d'acomplir amb els estàndards de seguretat aplicables vigents. En aquest sentit, l'ABA es reserva el dret de exigir al comerç evidències que certifiquin dit acompliment.

L'ABA subministrarà els següents elements per les proves i la certificació:

- Descripció de l'entorn de proves de les entitats
- Quadern de proves de certificació
- Joc de targetes de prova
- PIN-PAD de prova
- Documentació de les adaptacions ABA dels protocols PUP i PUC.

Quan les entitats, el comerç i el proveïdor donin el vist-i-plau a les proves de certificació, és considerarà el comerç certificat i en disponibilitat de treballar a l'entorn PUC EMV ABA.

Les targetes i PIN-PADs per les proves es gestionaran a les oficines de l'ABA; on s'entregaran als comerços sol·licitants i es recolliran un cop acabades les proves.