Pinpad Abecs

Protocolo de Comunicação e Funcionamento

Atualização de Especificação: SU003 (06-nov-2020)

Reativação temporária do suporte ao algoritmo DES.

Este documento destina-se a atualizar a especificação:

- "**Pinpad Abecs - Protocolo de Comunicação e Funcionamento", versão 2.12 (11-abr-19)**

O algoritmo DES é considerado inseguro e, seguindo exigências das principais bandeiras de cartão, seu suporte foi finalmente retirado da especificação v2.12 (11-abr-19). Muitos sistemas de pagamento, entretanto, não se adequarem a esta mudança e continuam usando MK:DES para captura de PIN, principalmente para cartões *private label*, fato que dificulta a instalação de pinpads v2.12 em campo.

Para solucionar este problema, esta atualização de especificação tem como objetivo reinstaurar o algoritmo MK:DES de forma temporária, na condição de que **os fabricantes de pinpad não poderão mais entregar pinpads com suporte ao DES a partir de 31/out/2021**.

Alteração #001

Os seguintes parâmetros definidos na seção **3.1.3.1** da especificação voltam a permitir o suporte a "MK/WK:DES", afetando os comandos **"GOX", "EBX" "GTK"**:

CMD_PARID	Valor	Formato	Descrição
...	...	...	...
SPE_MTHDPIN	0002h	N1	Método a ser usado na criptografia de PIN: "0" = MK/WK:DES:PIN; "1" = MK/WK:TDES:PIN; e ~~"2" = DUKPT:DES:PIN (ANSI X9.24:1998).~~ "3" = DUKPT:TDES:PIN (ver seção 5.1.2).
SPE_MTHDDAT	0003h	N2	Método a ser usado na criptografia de dados: "00" = MK/WK:DES:DAT (criptografia de bloco ECB); "01" = MK/WK:DES:DAT (criptografia de bloco CBC); "10" = MK/WK:TDES:DAT (criptografia de bloco ECB); "11" = MK/WK:TDES:DAT (criptografia de bloco CBC); ~~"30" = DUKPT:TDES:DAT#1 (criptografia de bloco ECB);~~ "50" = DUKPT:TDES:DAT#3 (criptografia de bloco ECB); e "51" = DUKPT:TDES:DAT#3 (criptografia de bloco CBC).
...	...	...	...
SPE_WKENC	000Ah	B8 ou B16	*Working Key* criptografada pela MK~~-TDES~~. ▪ B8 - Se MK:DES; ▪ B16 - Se MK:TDES.

Alteração #002

Os seguintes campos de retorno do comando **"GIX"** definidos na seção **3.1.3.2** da especificação voltam a informar dados sobre as chaves DES:

RSP_DATID	Valor	Formato	Descrição
...	...	...	...
PP_MKDESP (†)	8030h	A100	100 caracteres contendo o mapa de chaves **MK:DES:PIN** contidas no pinpad, sendo que cada caractere corresponde a uma posição (de "00" a "99"), indicando: "0" = Chave ausente (não carregada); "1" = Chave presente (carregada); e "2" = Posição não suportada pelo pinpad. ~~Reservado.~~
PP_MKDESD (†)	8031h	A100	Idem para chaves **MK:DES:DAT**. ~~Reservado.~~
...	...	...	...

Alteração #003

O comando **"ENB"** definido na seção **3.3.7** volta a permitir "MK/WK:DES:DAT":

➲ Comando

Id. do Campo	Formato	Descrição
CMD_ID	A3	Código do comando (= "**ENB**").
CMD_LEN1	N3	Tamanho dos dados a seguir (fixo "051").
ENB_METHOD	N1	Método de criptografia: **"0"** = MK/WK:DES:DAT **"1"** = MK/WK:TDES:DAT
...	...	...

Alteração #004

O comando **"GPN"**, definido na seção **3.3.11**, volta a permitir "MK/WK:DES:PIN":

➲ Comando

Id. do Campo	Formato	Descrição
CMD_ID	A3	Código do comando (= "**GPN**").
CMD_LEN1	N3	Tamanho dos dados a seguir.
GPN_METHOD	N1	Método de criptografia: **"0"** = MK/WK:DES:PIN **"1"** = MK/WK:TDES:PIN ~~**"2" = DUKPT:DES:PIN**~~ **"3"** = DUKPT:TDES:PIN
GPN_KEYIDX	N2	Índice da MK ou do registro de tratamento DUKPT.
GPN_WKENC	H32	*Working Key* (criptografada pela MK indicada em **GPN_KEYIDX**). Se **GPN_METHOD** = "0", somente os 16 primeiros caracteres (8 bytes) são utilizados. Se **GPN_METHOD** = ~~"2" ou~~ "3", este campo é ignorado pelo pinpad.
...	...	...

Alteração #005

O comando **"GOC"**, definido na seção **3.6.3**, volta a permitir "MK/WK:DES:PIN":

➲ Comando

Id. do Campo	Formato	Descrição
CMD_ID	A3	Código do comando (= "**GOC**").
...	...	...
GOC_METHOD	N1	Método de criptografia de PIN *online*, a ser usado caso requerido pelo processamento EMV: **"0"** = MK/WK:DES:PIN **"1"** = MK/WK:TDES:PIN ~~**"2" = DUKPT:DES:PIN**~~ **"3"** = DUKPT:TDES:PIN
GOC_KEYIDX	N2	Índice da MK ou do registro de tratamento DUKPT.

Id. do Campo	Formato	Descrição
GOC_WKENC	H32	*Working Key* (criptografada pela MK indicada em **GOC_KEYIDX**). Se **GOC_METHOD** = "0", somente os 16 primeiros caracteres (8 bytes) são utilizados. Se **GOC_METHOD** = ~~"2" ou~~ "3", este campo é ignorado pelo pinpad.
...	...	...

Alteração #006

O mapa de chaves da seção 5.1 volta a permitir MK:DES:

Os pinpads possuem em sua memória, em uma área protegida, diversas chaves de criptografia "injetadas" pelo fabricante, considerando-se ~~dois~~ três algoritmos diferentes:

- **MK/WK DES**;
- **MK/WK TDES**; e
- ~~**DUKPT DES**; e~~
- **DUKPT TDES**.

Estas chaves são utilizadas pelos comandos desta especificação para criptografia do PIN digitado pelo portador e para outros dados ("DAT"), sendo referenciadas por um índice de dois dígitos numéricos.

Desta forma, esta especificação considera o seguinte mapeamento de chaves, diferenciando ~~quatro~~ seis tipos para cada índice numérico existente:

Índice ⇩	MK:DES		MK:TDES		~~DUKPT:DES~~	DUKPT:TDES	
	PIN	DAT	PIN	DAT	~~PIN~~	PIN	DAT
"00"							
"01"							
"02"							
...							
"31"							
"32"							