Pinpad Abecs

Protocolo de Comunicação e Funcionamento

Atualização de Especificação: SU004 (17-fev-2021)

Implementação de segurança contra ataques de *replay*.

Este documento destina-se a atualizar a especificação:

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

As alterações aqui contempladas serão incorporadas na próxima versão desta especificação.

Alteração #001

A tabela seção **3.1.1** da especificação passa a incluir o novo código de retorno ↳ST_SECURITY.

...	...	...
↳ST_ERRCRYPT	046	Erro genérico de validação criptográfica.
↳ST_SECURITY	**047**	**Operação finalizada por motivo de segurança.**
↳ST_DUMBCARD	060	ICC inserido, mas não responde (“mudo”).
...	...	...

Alteração #002

Incluída a nova seção **6.3.5** para tratar exclusivamente deste tema.

6.3.5. Proteção contra ataques de replay em ICC

A norma EMV para ICC (🕮**EMV#3**) prevê que o comando GENERATE APPLICATION CRYPTOGRAM (ou “GENERATE AC”) seja enviado ao cartão até duas vezes durante o processamento de uma transação. Caso o SPE envie comandos ao pinpad que resultem na submissão de mais de dois GENERATE AC ao cartão em uma única transação, isso deve ser caracterizado como tentativa de ataque de *replay*.

Para identificar essa situação, o pinpad deve contar quantos GENERATE AC estão sendo enviados ao cartão durante uma transação e retornar o erro ↳ST_SECURITY como resposta ao comando que faria terceira tentativa.

> ⚠ Para este fim, define-se como uma transação todo o período em que um ICC está inserido no pinpad, independentemente de quantas vezes o chip foi ativado (*reset*) ou quais comandos foram a ele submetidos. Uma nova transação somente será iniciada quando o cartão for removido e inserido novamente.

De acordo com esta especificação, o comando GENERATE AC somente é enviado ao ICC nos comandos “**GOC**”, “**GOX**”, “**FNC**”, “**FCX**” ou de forma explícita no comando “**CHP**” (se o byte INS dentro de **CHP_CMD** tiver o valor “AE”).

O fluxograma a seguir ilustra uma maneira simples de se implementar essa proteção dentro do software do pinpad, valendo-se de uma variável “CtrGAC” para contar quantos GENERATE AC foram submetidos dentro da mesma transação: