SPC-4 CDB Encapsulation Alternatives

Because everybody wants to see
the Encapsulated CDB

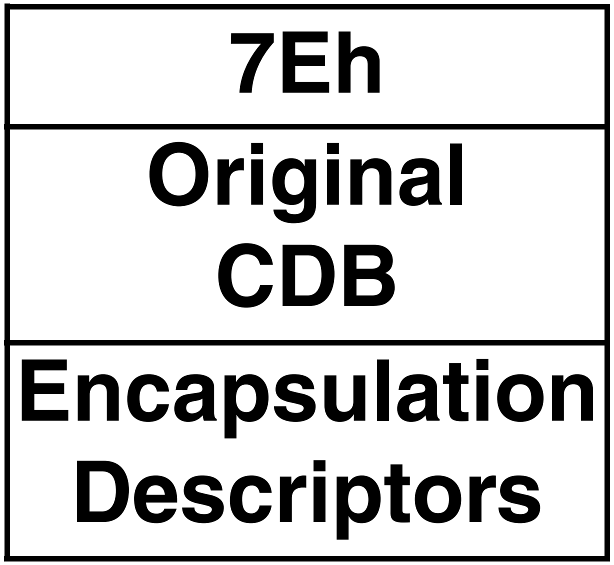
ENDL
TEXAS

Why?

The March CAP WG universally expressed a desire to *see* the original CDB in any ESC CDB (see 07-029r1), so …

- ☆ **Here is a way to do that**
- ✗ **Which could be viewed as totally incompatible with the Encapsulated Security Protocol inspiration for the original plan**

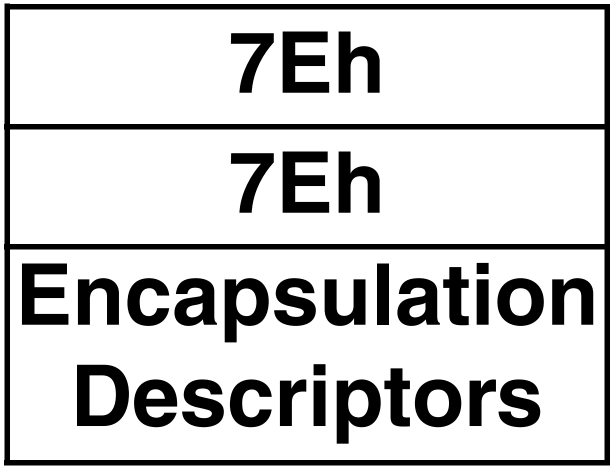
Possible ESC CDB Format(s)



7Eh

Original CDB

Encapsulation Descriptors



7Eh

7Eh

Encapsulation Descriptors

This format used only when CDB is encrypted

Notes

- ☆ Positives
  - ✚ Unencrypted CDB <u>always</u> visible
  - ✚ Encryption still possible using traditional ESP format
    - ✚ Put whole ESP in Encapsulation Desc.
- ✗ Negatives
  - ✗ ESP-format integrity checks are impossible
  - ✗ Might be cart before the horse

Related Ideas

(very random)

- ☆ 7Eh 7Eh works because ESC CDB cannot be inside an ESC CDB
- ☆ Specify exact Encapsulation Desc. order in SPC-4
  - ✓ Newer last
  - ✓ Encrypted CDB very very last
  - ✚ Solves '*new encapsulation*' problem