### Test 070-17-02 RMAC\_I Initial Cryptogram and RMAC Error

#### Description

##### PD

Provide malformed 16-byte MAC array – initial MAC value in 0x78 response to SCRYPT

##### ACU

Process malformed data (see table D.3.2) received in response to SCRYPT and indicated error and cease (restart) secure channel session.

#### Purpose

Determine if the proper cryptogram value is sent in support oof establishing secure channel by issuing SCRYPT and processing the data block for encryption synchronization and in the case of a error restart and reestablish encryption sequence. Stop or restart session when synchronization is lost.

|  |  |
| --- | --- |
| Basic OSDP (PD) | Optional |
| Basic OSDP (ACU) | Optional |
| Secure Channel (PD) | Required |
| Secure Channel (ACU) | Required |
| BIO Match (PD) | Required |
| BIO Match (ACU) | Required |
| BIO Read (PD) | Required |
| BIO Read (ACU) | Required |
| Extended Packet Mode (PD) | Required |
| Extended Packet Mode (ACU) | Required |
| Extended Read/Write (PD) | Required |
| Extended Read/Write (ACU) | Required |

#### Test action

##### PD Test

Provide malformed data in byte format describes in Table D.6.

##### ACU Test

Process malformed data block, record error, restart encryption synchronization to create secure channel.

#### Development status

Available in libosdp-conformance [1.31-Build-4](https://github.com/Security-Industry-Association/libosdp-conformance/releases/tag/1.31-4)

#### Test Results

JSON tags

|  |  |
| --- | --- |
| test | 070-17-02 |
| test-status | 1 for pass, 0 for fail |

#### Revision History

New for 2.4.2