### 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 an error, cease establishment of a secure channel session. A restart of the sequence, from the beginning, may follow the test action.

|  |  |
| --- | --- |
| 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

Not applicable, applies to ACU processing of a PD response.

##### ACU Test

Calculate the RMAC-I response value, then change the first octet to 0xff. Send that. Inspect an external OSDP trace to confirm the ACU does not proceed to set up that secure channel session. The EAC may emit telemetry when this event occurs.

#### 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

Text updated 2.5.6