11 Protocol implementation conformance statement

11.1 Overview of clause

Implementors of this specification shall supply the information in Clause 11 on request. An “X” in a box means that the implementation supports the listed feature.

11.2 Required algorithms

If the implementor does not declare support for an algorithm marked “(required)”, interoperability cannot be guaranteed.

If an algorithm is not supported due to export restrictions, the implementor shall provide a copy of the export restriction that prohibits its export. This algorithm shall not be supported if and only if export restrictions do not allow any mechanism of exportation. If this algorithm is not supported, the implementation shall be clearly documented as adhering to the export restrictions, as supplied. The documentation shall also specify that the interoperable/base specification requirements are not supported. Samples of the documentation shall be provided.

11.3 MAC algorithms

[X] HMAC-SHA-256 (required)

[ ] Other _____

11.4 Key wrap algorithms

[X] AES-256 Key Wrap (required)

[ ] Other AES-128 _____

11.5 Maximum Error messages sent

[ ] Fixed at 2

[X] Configurable

11.6 Use of Error messages

[X] Transmits Error messages Configurable

11.7 Update Key Change Methods

[ ] None permitted

[x] <4> Symmetric AES-256 / HMAC-SHA-256 (required)

[ ] <5> Symmetric AES-256 / AES-GMAC

[ ] <68> Asymmetric
RSA-2048 / DSA SHA-256 (L=2048 N=256) / HMAC-SHA-256

[ ] <69> Asymmetric
RSA-3072 / DSA SHA-256 (L=3072 N=256) / AES-SHA-256

[ ] <70> Asymmetric
RSA-2048 / DSA SHA-256 (L=2048 N=256) / HMAC-GMAC

[ ] <71> Asymmetric
RSA-3072 / DSA SHA-256 (L=3072 N=256) / AES-GMAC

[ ] Other _____

11.8 User Status Change

[x] Non-certificate method (required)

[ ] Use IEC/TS 62351-8 Certificates

11.9

x Challenge response Supported

x Aggressive Mode Supported

11.10

x Only one user with Configurable ID is supported