17.7. OpenPGP Message Format

Objective

17.7.1. OpenPGP Message Format is implemented correctly as an Approved Cryptographic Protocol.

Context

Scope

17.7.2. This section covers information on the conditions under which the OpenPGP Message Format can be used as an approved cryptographic protocol. It applies to the protocol as specified in IETF's RFC 2440 and RFC 4880, which supersedes RFC 2440.

17.7.3. When using a product that implements the OpenPGP Message Format, requirements for using approved cryptographic protocols will also need to be referenced from the Section 17.3 - Approved Cryptographic Protocols.

17.7.4. Information relating to the development of password selection policies and password requirements can be found in the Section 16.1 - Identification and Authentication.

References

17.7.5. Further information on the OpenPGP Message Format can be found at:

Reference	Title	Publisher	Source
RFC 4880	**OpenPGP Message Format specification**	IETF	https://datatracker.ietf.org/doc/html/rfc4880

Rationale & Controls

Using OpenPGP Message Format

17.7.6.R.01. **Rationale**

If the private certificate and associated key used for encrypting messages is suspected of being compromised i.e. stolen, lost or transmitted over the Internet, then no assurance can be placed in the integrity of subsequent messages that are signed by that private key. Likewise no assurance can be placed in the confidentiality of a message encrypted using the public key as third parties could intercept the message and decrypt it using the private key.

17.7.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2806]

Agencies MUST immediately revoke key pairs when a private certificate is suspected of being compromised or leaves the control of the agency.