17.6. Secure Multipurpose Internet Mail Extension

Objective

17.6.1. Secure Multipurpose Internal Mail Extension (S/MIME) is implemented correctly as an approved cryptographic protocol.

Context

Scope

17.6.2. This section covers information on the conditions under which S/MIME can be used as an approved cryptographic protocol.

17.6.3. When using a product that implements S/MIME, requirements for using approved cryptographic protocols will also need to be referenced from Section 17.3 - Approved Cryptographic Protocols.

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

References

17.6.5. Further information on S/MIME can be found at:

Reference	Title	Publisher	Source
	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification	IETF	https://datatracker.ietf.org/doc/html/rfc5751
SP 800-57	**Recommendations for Key Management**	NIST	https://csrc.nist.gov/publications/sp

Rationale & Controls

Decommissioning

17.6.6.R.01. **Rationale**

Decommissioning MUST ensure any remanent cryptographic data is destroyed or unrecoverable.

17.6.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2769]

Decommissioning of faulty or redundant equipment MUST comply with media sanitisation requirements described in Chapter 12 – Product Security.

Using S/MIME

17.6.7.R.01. **Rationale**

S/MIME 2.0 used weaker cryptography (40-bit keys) than is approved for use by the government. Version 3.0 was the first version to become an Internet Engineering Taskforce (IETF) standard.

17.6.7.R.02. **Rationale**

Agencies choosing to implement S/MIME should be aware of the inability of many content filters to inspect encrypted messages and any attachments for inappropriate content, and for server-based antivirus software to scan for viruses and other malicious code.

17.6.7.R.03. **Rationale**

Improper decommissioning and sanitisation presents opportunities for harvesting Private Keys. Products that hosted multiple Private Keys for the management of multiple identities should be considered points of aggregation with an increased “target value”. Where cloud based computing services have been employed, media sanitisation may be problematic and require the revocation and re-issue of new keys.

17.6.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not [CID:2780]**

Agencies MUST NOT allow versions of S/MIME earlier than 3.0 to be used.