17.3. Approved Cryptographic Protocols

Objective

17.3.1. Classified information in transit is protected by an Approved Cryptographic Protocol implementing an Approved Cryptographic Algorithm.

Context

Scope

17.3.2. This section covers information on the cryptographic protocols that the GCSB recognises as being approved for use within government. Implementations of the protocols in this section need to have successfully completed a GCSB recognised cryptographic evaluation before they can be approved for implementation.

17.3.3. High assurance cryptographic protocols are **not** covered in this section.

Approved cryptographic protocols

17.3.4. In general, the GCSB only recognises the use of cryptographic products that have passed a formal evaluation. However, the GCSB may approve the use of some commonly available cryptographic protocols even though their implementations within specific products have not been formally evaluated. This approval is limited to cases where they are used in accordance with the requirements in this manual.

17.3.5. The Approved Cryptographic Protocols are:

- TLS;
- SSH;
- S/MIME;
- OpenPGP Message Format; and
- IPSec.

Rationale & Controls

Using Approved Cryptographic Protocols

17.3.6.R.01. **Rationale**

If a product implementing an Approved Cryptographic Protocol has been inappropriately configured, it is possible that relatively weak cryptographic algorithms or implementations could be inadvertently selected. In combination with an assumed level of security confidence, this can represent a significant level of security risk.

17.3.6.R.02. **Rationale**

When configuring unevaluated products that implement an Approved Cryptographic Protocol, agencies can ensure that only the Approved Cryptographic Algorithm can be used by disabling the unapproved algorithms within the products (which is preferred). Alternatively a policy can be put in place to advise system users not to use the non-approved algorithms.

17.3.6.R.03. **Rationale**

While many Approved Cryptographic Protocols support authentication, agencies should be aware that these authentication mechanisms are not foolproof. To be effective, these mechanisms MUST be securely implemented and protected.
This can be achieved by:

- providing an assurance of private key protection;
- ensuring the correct management of certificate authentication processes including certificate revocation checking; and
- using a legitimate identity registration scheme.

17.3.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2520]

Agencies using a product that implements an Approved Cryptographic Protocol MUST ensure that only Approved Cryptographic Protocols can be used.