NZISM Guidance

Approved Cryptographic Algorithms and Retiring Older Cryptographic Algorithms

It is important to use algorithms that adequately protect sensitive information and the NZISM prescribes approved algorithms and protocols. Each algorithm is carefully assessed for longevity, resistance to attack (cracking), ease of use and consumption of resource. The algorithms are listed in the NZISM Section 17.2 and are divided into two groups; those approved for current use and an older set for use in legacy systems only.

Approved for current use:

- ECDH for agreeing on encryption session keys;
- ECDSA for digital signatures;
- Secure Hashing Algorithm 2 (i.e. SHA-384 and SHA-512); and
- AES using key lengths of at least 256 bits for data encryption.

There is a set of algorithms which are for use in legacy systems only. These have been retained as some older systems do not have the capability to implement algorithms from the current use approved set. It is vital that the very considerable risks of using older algorithms are recognised by agencies and that older algorithms are used only where no other choice exists. The older set comprises:

- DSA for digital signatures;
- DH for agreeing on encryption session keys;
- RSA for digital signatures and passing encryption session keys or similar keys;
- Secure Hashing Algorithm 1 (i.e. SHA-1);
- 3DES.

Transitioning and Retiring Cryptographic Algorithms and Protocols

It is essential that agencies recognise that all cryptographic algorithms and protocols have a finite life. Challenges are posed by new cryptanalysis techniques and methods, the increasing power of computing technology, and the continuing work on the development of quantum computers. In addition, there is an active field of work that continuously seeks to compromise algorithms and protocols currently in use.

Planning for changes in the use of cryptography because of algorithm breaks, the availability of more powerful computing techniques or new technologies is an important consideration for agencies. Awareness of retirement or deprecation of algorithms and associated protocols is essential.

Retiring RSA

RSA was announced in 1976 so is now over 40 years old. Several flaws and attacks have been identified since creation, each of which required specific mitigations, careful implementation and management. Unfortunately there is ample evidence that there are continuing challenges in securely implementing, using and managing RSA.

To counter identified threats from shorter RSA key lengths, longer key lengths have been specified in the NZISM since 2010. Subsequently it was specified in the NZISM that RSA was approved for use in legacy systems only.

This approach was selected to allow agencies to plan the retirement of legacy systems and ensure replacement systems were using only approved algorithms and protocols from the current use set.

There are several strong indicators that RSA will be deprecated in the next few years. For example the TLS 1.3 Working Group has agreed to deprecate RSA in favour of elliptic curve cryptography. The most recent guidance from NIST is also indicative of impending deprecation of RSA.

It is, therefore, essential that agencies are aware of these changes and plan the retirement of RSA from their systems as part of their ongoing operational management.