Defence Signals Directorate
Information Security Policy Advice 2/2003

Withdrawal of Approval for Single DES

Date of Effect: 10 December 2003

Information Security Group
Locked Bag 5076
KINGSTON ACT 2604
AUSTRALIA

Ph: (02) 6265 0197
Fax: (02) 6265 0328

assist@dsd.gov.au
www.dsd.gov.au/infosec

WITHDRAWAL OF APPROVAL FOR SINGLE DES

Introduction

Background

The Data Encryption Standard (DES/Single DES) was developed in 1977 for the "protection of sensitive information" [FIPS 46-3]. Whilst there are no known flaws in the algorithm, computational power is increasing to the point that exhaustive searches of the key-space are becoming increasingly viable as a means of attack.

With the advent of Triple DES (3DES/TDES/DES-3), the Advanced Encryption Standard (AES) and other DSD-approved cryptographic algorithms, there should be no requirement for Australian Government agencies to continue using DES for the protection of classified Australian Government information.

For more information on …	See …
DSD-approved algorithms	Australian Communications-Electronic Security Instructions (ACSI) 33
DES and Triple DES	http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
AES	http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Policy

DES no longer approved

Effective immediately, the DES algorithm is withdrawn from the list of DSD-approved cryptographic algorithms and is no longer approved by DSD for the protection of classified Australian Government information.

Existing products

Agencies **MUST** migrate away from DES for the protection of classified Australian Government information by 1 January 2005.

Exception: Where there is **no** alternative to DES within legacy systems, agencies:

- **MUST** undertake a risk assessment on the continued use of DES; and
- **SHOULD** contact DSD for advice.

New procurements

Agencies **SHOULD** only procure DSD-approved products, noting that effective immediately, DES is no longer approved.

Affected Products

EPL products

A number of products listed on the EPL utilise DES and are therefore affected by this policy.

Use of affected products

Some products utilise cryptography as their core functionality however others, such as the firewalls, only utilise cryptography in a support function.

In the cases where the cryptography is the core functionality of the product, agencies **MUST** migrate away from the products in accordance with the policy for 'Existing products' on page 2.

In cases where the cryptography provides support functionality, agencies may continue using the product but **MUST** stop using any security services that rely on the single DES cryptography.

Note: the above statements also apply to products not listed on the EPL.
