Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

Phone: 02 6265 0197 Email: assist@dsd.gov.au

HANDBOOK 9

CRYPTOGRAPHIC SYSTEMS

Version 1.0

Objectives

901. Cryptographic services are critical in providing sound security countermeasures for systems and applications. They are used for protecting confidentiality and integrity, and for ensuring strong authentication and non-repudiation. The purpose of this handbook is to:

a. Define cryptographic standards for protection of non-national security information.

b. Define minimum standards for key recovery applicable to Commonwealth agencies.

c. Provide guidance on the cryptographic evaluation of cryptographic products, performed in support of the Australasian Information Security Evaluation Programme (AISEP) (see **Handbook 2 - Evaluated Products**).

d. Provide guidance on development of cryptographic Key Management Plans.

Cryptographic Standards

902. The following sections describe the cryptographic standards sufficient for the protection of Government information that could be passed over public transmission facilities, or in some way accessed by uncleared users. This also applies to

classified information that is encrypted for storage on media, notwithstanding the security issues associated with the use of such media as detailed in **Handbook 6 - Media Security**.

903. The following sections define the minimum cryptographic standards that are appropriate when providing adequate secure authentication, non-repudiation, integrity and confidentiality for the protection of Commonwealth information. It is important to note that these recommended standards are generic; there is no guarantee that particular commercial implementations actually achieve these minimum standards. Consequently, it is imperative that commercial products and systems be evaluated and certified by DSD before acceptance.

904. Commercial encryption products used by Australian Government agencies must be evaluated under the Australasian Information Security Evaluation Programme (AISEP). The implementations of these algorithms will be validated by DSD as part of the evaluation process.

Digital Signature Standards

905. It is recommended and preferred that Commonwealth agencies use Digital Signature Algorithm (DSA) [1] with a modulus of at least 1024 bits for use in digital signatures. Not preferred but still acceptable would be RSA (Rivest-Shamir-Adleman)[2], again with a modulus of at least 1024 bits. The Secure Hash Algorithm SHA-1 [3] is to be used for hash or digest totalling, when using the DSA. If RSA is used then it is appropriate and acceptable to use the ISO standard hashing algorithm, namely "MD5"[4].

Encryption Algorithm Standards

906. The Data Encryption Algorithm (DEA) [5], more commonly referred to as the Data Encryption Standard (DES), with a key length of at least 56 bits is suitable for the encryption for transmission or storage of information classified **IN-CONFIDENCE** or **PROTECTED**. It may also be suitable for the protection of information classified **RESTRICTED** or **HIGHLY PROTECTED**, in consultation with DSD. DES is also suitable for **CABINET-IN-CONFIDENCE** which has no national security information. DES is only suitable if either the Cipher Block Chaining or Cipher Feedback mode is used. DSD does not approve the use of the Electronic Code Book mode.

907. Proprietary algorithms of equivalent strength to DES are also acceptable once DSD has established their strength. It should also be noted that there are a number of other public algorithms that have a reputation for high security, such as IDEA, RC4, RC5 and BLOWFISH. **None** of these algorithms have been formally evaluated by DSD, and to do so can take several years of effort. The same applies to proprietary algorithms. At this time, these proprietary algorithms should not be used by Australian Government agencies.

908. National security classified information at **CONFIDENTIAL**, **SECRET** or **TOP SECRET** markings must be encrypted using Government Furnished Encryption (GFE) systems. The algorithms described above are ***not*** suitable. Details on the use

of GFE for protection of national security classified information are available from DSD.

Session Key Standard

909. Where encryption session or similar keys are to be passed using public key systems, DSD recommends RSA or the Diffie-Hellman protocol [6] with a modulus of not less than 1024 bits. Public keys used for this purpose should be distinct from the public keys used for digital signature even if the same algorithm is employed.

Key Recovery

910. In response to a submission made by the Attorney-General's Department, which was approved by Cabinet on 21 July 1998, encryption products listed on DSD's **Evaluated Products List**, where practical, must provide a means of key or data recovery. The decision's objective was to safeguard Commonwealth information by requiring encryption products that allow recovery of encrypted data in circumstances where the encryption key is unavailable due to loss, damage or failure.

911. The following criteria have been formulated to assist Australian industry implement Key Recovery (KR) facilities in encryption products to be used by Commonwealth agencies. The KR facility of an encryption product provides access to the key(s) or other material/information required to derive the plain text from the encrypted data. For a product to be approved by DSD for use by Commonwealth agencies, it must satisfy the following criteria:

a. The KR capability can be implemented technically and/or procedurally.

b. The KR facility must be exercised only in Australia.

c. The key(s) or other material or information required to decrypt enciphered data (including that which has been archived) must be accessible for the life of that data.

d. Encrypted information must be recoverable in a reasonable time.

e. The KR facility cannot be altered, bypassed, disabled or otherwise rendered inoperative by a user of the product.

f. The output of the product must include information sufficient for a KR agent to identify the keys or other material or information required to decrypt the ciphertext.

g. An audit capability must be present.

h. Where appropriate, the KR facility must allow access to the key(s) or other material or information needed to decrypt the ciphertext regardless of whether the product generated or received the ciphertext.

912. It will be necessary for the responsible company to submit a full technical description of the KR facility in an encryption product to DSD for evaluation. All other product information required by DSD, such as details of its cryptographic functionality, must also be made available. Products on DSD's **Evaluated Products List** that incorporate acceptable KR facilities will be so identified. The responsibility to protect Government information by using the KR facility in an approved product properly lies with the Commonwealth agencies, not with DSD. Therefore, these criteria do not include requirements for KR agents.

Guidelines for Developers considering AISEP Evaluation of their Encryption Product

913. The validation and assessment of the cryptographic functionality within a product is performed by the Cryptographic Evaluation Section, Information Security Group at DSD, when a product is submitted for evaluation under the AISEP. This is different from the testing and evaluation of the "trustedness" of a product, which is performed by an Australasian Information Security Evaluation Facility (AISEF).

914. Prior to entering into a contract with an AISEF, it is required that the vendor obtain a "Cryptographic Advisory Note" from the Cryptographic Evaluation Section at DSD. The purpose of this note is to verify that the product will meet the minimum requirements for Australian Government use as outlined in the Standards paragraphs above. Provided that the product meets the criteria for entry into the AISEP, it will then be subject to cryptographic evaluation as outlined below.

915. The cryptographic assessment remains the same regardless of the Evaluation Level sought. This means that the outcome is essentially a "yes" or "we need to make some amendments" result. In order to perform the cryptographic evaluation it may be necessary to supply more information than the AISEF normally requires. For example, the AISEF will not require source code for E1 and E2 (EAL-2, EAL-3) levels, however, it may be required for the cryptographic evaluation.

916. The following is an example only, to demonstrate the level of detail that may be required for a cryptographic evaluation. In this example, the product has DES implemented in Cipher Block Chaining mode for confidentiality. In terms of key generation, the following is required:

a. Information on the random number generator being used.

b. The method by which this random number generator is seeded.

c. A description of the process used to generate DES keys from the output of the random number generator.

d. Information on any tests used to check the output of the random number generator.

e. The ability to collect and analyse the output of the random number generator.

f. The ability to collect and analyse DES keys.

In terms of DES validation, the ability to input known plain text and encrypt with a known key and initialisation vector and collect the encrypted output will be required.

Key Management

917. The successful management of cryptographic keys is paramount to the security of most types of modern cryptosystems. DSD has long been involved in key management, and has published numerous documents to assist client agencies to develop their capabilities. There are two publications that are directly related to key management methods and procedures, these being the ACSI 53 and ACSI 57.

918. The ACSI 57 ("Guidelines for the use of Cryptographic Systems Listed in Section VIII of the Defence Signals Directorate Evaluated Products List (EPL)") provides guidelines for the establishment of procedures which will satisfy minimum requirements for the safeguarding and control of commercial grade cryptographic systems and associated keying material. Commercial grade cryptographic systems, listed as such in Section VIII of the DSD **Evaluated Products List**, are those cryptographic security systems approved by DSD for the protection of non-national security classified information and information that is national security classified **RESTRICTED**.

919. Detailed procedures on key management aspects are contained in ACSI 53, which, although focussed on the national security environment, are equally appropriate for ensuring privacy of communications. ACSI 53 first deals with the management infrastructure that must be established within an agency to safeguard communications security (key) material employed within the agency. It addresses personnel security, physical security, accounting procedures, violation reporting procedures that must be implemented by management with respect to communications security, and release of Comsec information to commercial firms. ACSI 53 is only available from DSD on request, to all Government agencies and organisations, or authorised agencies working on behalf of Government agencies.

920. A Key Management Plan is required for the successful deployment of cryptographic services within an agency. An example of those issues that need to be addressed in a plan is detailed in **Annex A** to this Handbook. There is no "template" or "standard" way a key management plan should be structured. Agencies are encouraged to draft the plan in their own terms and definitions, and in a manner that relevant agency management and staff would best accept. A key management plan should be developed regardless of whether the cryptographic system is implemented in hardware or software.

921. For grades of assurance required for cryptographic systems deployed in government, refer to **Handbook 1** in conjunction with **Handbook 2**.

REFERENCES

[1] Federal Information Processing Standard FIPS-186, US National Institute for Standards and Technology (NIST)

[2] Public Key Cryptography Standards PKCS#1, RSA Laboratories

[3] Australian Standard AS 2805 / FIPS-180, US National Institute for Standards and Technology (NIST)

[4] R.L Rivest, "The MD5 Message Digest", RFC:1321, April 1992

[5] FIPS 46, ANSI X9.42

[6] W Diffie and M E Hellman, *New Directions in Cryptography,* IEEE Transactions on Information Theory, v IT-22, n.6, Nov 1976, 644-654

ANNEX A

KEY MANAGEMENT PLAN

A Key Management Plan is not required to be rigid in either content or formatting. Rather it should be easy to read and simple in its layout. Ideally, all of the following components should be covered but can be omitted if they add nothing to the value of the plan. Similarly, any information that is considered appropriate but not included in this example should be added to your plan.

Objectives of the Plan

- State the aim and scope of the plan.
- Briefly state the hardware and/or software covered by the plan.
- State any policies relating to the use of the equipment.
- State the equipment (is it listed on the EPL?).

References

- Include relevant DSD ACSI or other documents.
- Internal policy or user manuals.
- Installation or configuration diagrams.

Classification of the hardware and/or software

- State the maximum classification of information to be protected by the system.

Details of hardware and/or software

- Include a brief description of the hardware and software configuration, interfaces and functionality. This section is only to include that information which is relevant to the overall key management plan.
- It may be appropriate to discuss the overall network topology, depending

on the complexity of the network.

Key Management

- Provide a description of how the key(s) will be sourced. This may be via another agency or may be key generation processes or equipment. It may be required to provide details of the initial key generation or seeding.
- Provide details on how the key is to be physically loaded into the hardware and/or software cryptographic system.
- Provide details on how traffic or session keys are produced and distributed to the relevant parties.

Key Accounting

- Detail the number of copies of key to be produced and distributed to the various parties.
- Provide details on the identification of the various key(s) to be produced and/or receipted.
- Detail the procedures for labelling and recording of the name, version and number of copies that were distributed, and the recipients of the key(s).
- Detail the cryptoperiod(s) for the various key(s).
- Provide details of how the key(s) will be electronically and physically stored. Include security countermeasures that will be used to protect the key(s) from compromise.
- Provide details of any formal or informal crypto accounts, as per either the ACSI 53 or ACSI 57.

Distribution of Keys

- Provide details on how keys will be distributed electronically or physically. This should include security details of courier(s), if used, as well as how the couriers will handle contingencies such as loss or compromise of keys. Electronic distribution of keys may already have been discussed in the section titled "Key Management" above.

Contingency

- Describe the conditions under which a compromise of cryptographic key material should be declared. This should include loss or theft of keying material, unauthorised access to keys or equipment, and unauthorised extensions of cryptoperiods. Ideas on categories of compromise are included in both the ACSI 53 and ACSI 57.
- Describe the reporting action that is to be effected as part of a compromise declaration. This should include the addressees of the report,

the details of the minimum amount of information that should be included in the report, and any action that is or will be taken to further scope the compromise and/or limit the exposure.

Hardware and/or Software Maintenance

- Detail the maintenance procedures for hardware and/or software items that are critical to successful operation of the cryptographic services. This should include the security measures taken to protect the integrity of the hardware and/or software by uncleared maintenance staff, as well as ensuring hardware and/or software has been adequately sanitised prior to release.
- Detail the procedures for testing or verification of software upgrades to critical cryptographic services in either the hardware (through firmware) or software.