



CANON iR4570/iR3570/iR2870/iR2270 SERIES iR SECURITY KIT-B2 VERSION 2

Product Description

The Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B3 is optional software for the Canon iR4570/iR3570/iR2870/iR2270 series which adds security enhancements to the multifunction device (MFD).

The Canon MFD is a digital copier that offers the combined functionality of a fax, a scanner and a printer for the reception, copying, sending, printing and emailing of documents. It is equipped with a large-capacity hard drive and stores document data there temporarily when performing its functions.

Users may contact their service providers to have the iR Security Kit-B2 V2 installed on the hard disk drive of their MFD. The Security Kit then replaces the pre-existing device control software, providing users with hard disk drive encryption and hard disk drive erasure functions. The security of the existing identification and authentication functions is also enhanced by this installation.

Scope of Evaluation

The scope of the Common Criteria (CC) evaluation included the following functionality:

- HDD (Hard Disk Drive) Data Encryption (stored document encryption);
- HDD Complete Erasure;
- Inbox User Identification and Authentication;
- Inbox Management;
- System Manager Identification and Authentication;
- System Manager Management; and
- Secure Communication (Remote User Interface).

Common Criteria Certification Summary

The product has met the requirements of the Common Criteria evaluation assurance level EAL3.

DSD's Evaluation Findings

As the product employs cryptography, DSD performed a cryptographic evaluation in addition to the Common Criteria certification. DSD found that the cryptography employed by the product meets the requirements stipulated within ACSI 33.

DSD's Recommendations

The scope of the evaluation did not include the following:

- Data export controls capable of blocking information based on protective markings; and
- Audit data generation and protection.

As a result, potential users of the Canon multifunction product should be aware of the following, derived from policy governing the use of MFDs in ACSI 33:

- For IN-CONFIDENCE and RESTRICTED usage:
 - Agencies SHOULD NOT enable a connection from a Canon multifunction product to a telephone network of a lower classification.
- For PROTECTED usage:
 - Agencies SHOULD NOT enable the facsimile functionality for a Canon multifunction product unless the telephone network is accredited to at least the same classification as the computer network.

Due to the electrostatic memory devices present within printers and photocopiers the MFD will retain the classification of the network it is connected to or the highest classification of the documents processed by the MFD when operated in a stand alone manner. The cryptographic functionality of the Security Kit can not be used to reduce the storage and physical transfer requirements of the MFD.

The erasure functions of the MFD are approved to sanitise the HDD from PROTECTED, RESTRICTED or IN-CONFIDENCE to UNCLASSIFIED. To sanitise the entire MFD additional sanitisation procedures need to be used for the electrostatic memory devices.

For additional information regarding MFD usage and sanitisation for national security classifications above RESTRICTED, and for HIGHLY PROTECTED, refer to block 3.10.70 and block 3.4.30 respectively of the SECURITY-IN-CONFIDENCE release of ACSI 33.

Point of Contact

For further information regarding the certification of these products, or compliance with ACSI 33, please contact DSD on (02) 6265 0197 or email assist@dsd.gov.au.

ACSI 33

The advice given in this document is in accordance with ACSI 33 release date September 2007. Australian Government agencies are reminded to periodically check the latest release of ACSI 33 at www.dsd.gov.au/library/infosec/acsi33.html.

Date of this Consumer Guide

This Consumer Guide was issued by DSD on 17 December 2007.