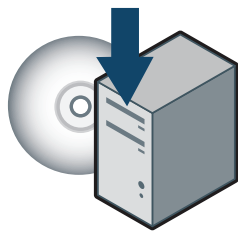
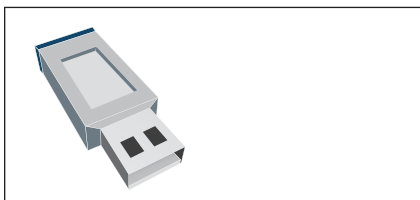


OESISOK™ Peripheral Protection Criteria



Version 1.1

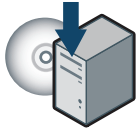
Appendix - PP Verification Test





OESISOK™ Peripheral Protection Criteria – Version 1.1

OESISOK Peripheral Protection designation is currently for peripheral protection applications. Applications submitted for certification must meet the following criteria before designated OESISOK.



Installation Test



Rogue Application Test



OESIS® Local Detection Test

Installation Test

A submitted application is installed on all supported operating systems. In order to complete this test, it must clear the following:

- The application installer completes *without errors* on all supported operating system and language combinations reflected in application documentation.

Rogue Application Test

A submitted application is checked against lists of known rogue applications. In order to complete this test, the application must clear all of the following:

- Application or its vendor is not listed as “rogue” according to the OPSWAT internal database.
- Application installer and binaries are scanned against multiple anti-malware engines, currently:
 - Spybot Search & Destroy 1.5
 - Lavasoft Ad-Aware 2007 Free Edition
 - Symantec Antivirus
 - McAfee VirusScan
 - CA eTrust™
 - Norman Virus Control
 - ESET NOD32 Antivirus Engine
 - VirusBuster EDK
 - Microworld eScan Engine
 - Kaspersky Anti-Virus®
 - ClamAV

*None of these engines should report any application file as “suspicious”, “threat” or other nomenclature indicative of the submitted application being rogue.

OESIS® Local Detection Test

A submitted application is checked to ensure it will be detected by the OESIS Framework.



Appendix – OESISOK™ Peripheral Protection Verification Tests

When an application is submitted for the OESISOK Peripheral Protection designation, the following tests will be performed for statistical data analysis:



Device Identification /
Permission Test

Device Identification / Permission Test

A submitted peripheral protection application is set to the highest protection level; the following tests will be performed for statistical data analysis.

- **Device Identification:** The application should be able to correctly identify the type of external device plugged-in.
- **Permission:** The application will allow or deny usage of the device based on the device policy.

