Sentinel®

Sentinel Envelope v.1.0 for Linux on ARM
Release Notes

gemalto

Document Revision History

Part number 007-013092-001 Rev A

Revision 1508-1

Disclaimer and Copyrights

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product. SafeNet, Inc. is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions contained herein. The specifications contained in this document are subject to change without notice.

Confidential Information

Sentinel is designed to protect your applications from unauthorized use. The less information that unauthorized people have regarding your security system, the greater your protection. It is in your best interest to protect the information herein from access by unauthorized individuals.

Contents

Sentinel Envelope v.1.0 for Linux on ARM - Release Notes

About This Document

This document contains information about the latest release of the Sentinel Envelope for Linux on ARM product, including features, product documentation, and known limitations.

Sentinel Envelope for Linux on ARM

These release notes contain information about **Sentinel Envelope for Linux on ARM** including features, product documentation, and known limitations

Sentinel Vendor Keys

When you purchase Sentinel Envelope for Linux on ARM, you are provided with one of the Sentinel Vendor keys—the Sentinel Master key or the Sentinel Developer key.

The key that your receive contains the appropriate license to operate Sentinel Envelope for Linux on ARM.

Obtaining Support

You can contact us using any of the following options:

- **Business Contacts** - To find the nearest office or distributor, use the following URL: http://www.safenet-inc.com/contact-us/
- **Technical Support** - To obtain assistance in using SafeNet products, feel free to contact our Technical Support team:
  - Phone: 800-545-6608 (US toll free), +1-410-931-7520 (International)
  - E-mail: support@safenet-inc.com
  - URL: http://sentinelcustomer.safenet-inc.com/sentinelsupport/
- **Downloads** - You can download installers and other updated components using this URL: www.sentinelcustomer.safenet-inc.com/sentineldownloads/

Help Us to Improve Sentinel Envelope for Linux on ARM

You can make a difference! We invite you to send us your ideas and opinions, and tell us what you like (and don't like) about Sentinel Envelope for Linux on ARM. Your input can help shape future versions of the product.

Feedback on Sentinel products can be sent to: ldkfeedback@safenet-inc.com

What's New in This Release?

This section describes the main features that are introduced in Sentinel Envelope v.1.0 for Linux on ARM.

Initial Release of Sentinel Envelope for Linux on ARM

Sentinel Envelope for Linux on ARM is a wrapping application that protects your applications with a secure shield. This application offers advanced protection features to enhance the overall level of security of your software.

Sentinel Envelope protects Linux ARM executables—providing a means to counteract reverse engineering and other anti-debugging measures.

Sentinel Envelope for Linux on ARM has been designed to protect Linux ARM applications. Sentinel Envelope accepts a Linux ARM EABI/EABIhf ELF binary (executable or .so) as input and returns a protected EABI/EABIhf ELF binary. The modified binary contains encrypted code and additional code inserted by Sentinel Envelope.

Supported Platforms

Supported Versions of Linux ARM Binaries

Sentinel Envelope supports the following Linux ARM applications that are compiled for soft/hard float ABI:

- ARMv6
- ARMv7
- ARMv7-a

Supported Platforms of Linux ARM Binaries

In general, Sentinel Envelope supports all Debian-based soft/hard float ABI platforms. The following platforms have been validated:

- Ubuntu 14.04 LTS
- Ubuntu 12.04 LTS
- Raspbian (Only for Raspberry Pi-2)
- Angstrom

Supported Hardware for Linux ARM Binaries

In general, hardware/boards compatible with ARMv7 or ARMv7-a processors are supported. The following hardware/boards have been validated:

- BeagleBoard-xm Rev C
- BeagleBone Black
- PandaBoard ES Rev B3
- Raspberry Pi-2

Supported Platforms for the Sentinel Envelope Tool

x86/x86-64 based Linux platforms

Product Documentation

This section describes how to work with Sentinel Envelope v.1.0 for Linux on ARM.

License Requirements

Sentinel Envelope for Linux on ARM is licensed. You require a Sentinel Master key or Developer key with the appropriate license in order to operate Sentinel Envelope for Linux on ARM.

Applications protected using the evaluation version of Sentinel Envelope for Linux on ARM display the following message at startup:

```
This application is protected using demo version of Sentinel
Envelope for Linux on ARM.
```

Deliverables

Deliverables includes a shell script-based installer and release notes (this file).

Installation

Use the procedure that follows to install Sentinel Envelope for Linux on ARM.

1. Enter the following commands:

```
tar xf SentinelEnvelopeForLinuxArm-1.0.<version>.tar.gz
cd Linux
sudo ./install-SentinelEnvelopeForLinuxArm-1.0.<version>.sh
```

2. Review and accept the EULA. The following files are copied to */usr/local/Gemalto/Sentinel Envelope*:
    - EULA.rtf
    - linuxenv_arm (the Sentinel Envelope for Linux ARM executable)
    - ReleaseNotes.pdf (this document)

Prerequisites

The following are required on the machine where you execute Sentinel Envelope for Linux on ARM:

- Supported Operating systems
    - OpenSUSE 12.3 (x86 and x86_64)
    - Red Hat EL 5.10, 6.5, 7.0 (x86 and x86_64)
    - Ubuntu Server 12.04.3, 14.04 (x86 and x86_64)
    - Ubuntu Desktop 12.04.3 (x86 and x86_64)
    - Debian 6.0.10 (x86 and x86_64)
    - CentOS 6.5 (x86 and x86_64)
- Sentinel LDK Run-time Environment v.6.60 or later. (Click here to download the latest version.)
- Sentinel Master key or Developer key with a valid license to protect Linux ARM binaries

Usage for Sentinel Envelope

Enter the following command to protect a Linux ARM application:

```
./linuxenv_arm <applicationFilePath> <protectedApplicationFilePath>
```

For example:

```
./linuxenv_arm Sample Sample-enveloped
```

By default, debugger detection is enabled for the protected application. To disable debugger detection, execute the following command:

```
./linuxenv_arm --debug –-memdump <applicationFilePath>
<protectedApplicationFilePath>
```

For example:

```
./linuxenv_arm –-debug –-memdump Sample Sample-enveloped
```

Return Codes and Messages

The table below describes return codes and message that may occur while Sentinel Envelope is attempting to protect a Linux ARM application.

Return Code	Message
C0002	File <filename> not found
C0005	I/O access failure
C0009	Unable to open or create file <filename>
C0012	Memory could not be allocated for internal buffers
C0021	<filename/dirname> is an existing directory
C2002	Unable to protect. File does not contain 'dynamic' section.
C2037	No section header found in ELF file
C2044	File already protected
C2049	Unable to protect executable/shared object that uses the following defined symbols: malloc, calloc, free, realloc, dlopen, dlerror, dlsym or dlclose
C2051	Executable cannot be patched because it is prelinked. Use /usr/sbin/prelink -u -o <clean_executable> <executable> to undo prelinking. (Path to prelink may vary)
C2052	File not a valid ELF binary
C2055	Unsupported architecture (only armv6, armv7 and armv7a are supported)
C2056	Only ELF executables and shared objects are supported
C2059	Unsupported ELF version
C2060	No program header found in ELF file
C2061	No segments in ELF file
C2062	No sections in ELF file
C2063	Invalid program header size in ELF file
C2064	Invalid section header size in ELF file
C2066	File cannot be protected because its code is needed for decryption
C2069	Unable to protect, File does not contain 'relocation' section.
C2070	Sentinel Developer key was not found.
C2071	License to protect Linux ARM binaries does not exist in the Sentinel Developer key.
C2072	Error occurred during communication with the Sentinel Developer Key.
C4001	Invalid command-line argument <argument>
C4003	Unable to rename temporary file to <filename>
C4004	Output directory <dirname> does not exist
C65535	Internal error (hint <errrorCode>)

Known Issues

Reference	Issue
LDK-4545	Applications that do not link any object dynamically cannot be protected.
LDK-10666	Protection of applications or dynamic libraries that are compiled with gnu gold linker are not supported.
LDK-11613	Under certain circumstances, an application that contains one or more short functions may not work after protection. (A short function is one that contains fewer than 8 bytes.) **Workaround**: Add dummy code to the function to increase its size to 8 or more bytes. For more information, see Tech Note TE1954.
177241	Applications that implement the symbols malloc, calloc, free, realloc, dlopen, dlerror, dlsym or dlclose cannot be protected. However, applications can use any of these standard library functions.

Recommendations

Gemalto recommends that you allow debugging and memory dumping:

- when you protect the shared library/object.
- when you protect applications that have the 'exec' command.

Gemalto recommends that you not use pthread_exit() in your main thread. If you do, protected applications may not be terminated properly, and you may have to kill the process explicitly.