

Entrust[®] Securing Digital Identities & Information



**Securing Your
Digital Life**

Entrust Technical Integration Guide for Entrust Security Manager 7.1 SP3 and
SafeNet Luna CA4

July 2008

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

Copyright © 2008. Entrust. All rights reserved.

Table Of Contents

Introduction	1
Entrust Product Information	1
Entrust Authority.....	1
Entrust Entelligence.....	1
Partner Product Information	1
Luna CA4.....	1
Integration Overview	1
Integration Details	2
Installation Overview.....	2
<i>New Install Luna CA4 with Entrust Security Manager 7.1 SP3</i>	2
System Behavior/Limitations	4
System Components	4
Partner Contact Information	4
Additional Information.....	4

Introduction

This technical integration guide provides an overview of how to integrate Entrust Security Manager with Luna CA4.

The Entrust/Authority serves as the Certification Authority in an Entrust infrastructure. Although it can operate in “software” mode, it can optionally use hardware devices where cryptographic operations and key storage are performed.

Entrust Product Information

Entrust Authority

By managing the full lifecycles of certificate-based digital identities, Entrust Authority enables encryption, digital signature and authentication capabilities to be consistently, transparently applied across a broad range of applications and platforms.

Entrust Entelligence

It delivers a single security layer that can encompass an enterprise's entire set of enhanced security needs, including authentication, authorization, digital signatures and encryption, for greater accountability and privacy. Entrust Entelligence empowers employees to work efficiently, communicate effectively, and use products and services online.

Partner Product Information

Partner Name: SafeNet Inc.

Website: www.safenet-inc.com

Product Name: Luna CA4

Product Version: 2.3

Platform and Service pack: Windows 2000 SP4 32-bit, Solaris 10 SPARC 64-bit

Luna CA4

Product description: The Luna CA4 addresses the security and operational needs required to maintain the integrity of PKIs with true hardware key management, trusted path multi-person authentication, and direct hardware-to-hardware backup. Featuring comprehensive key management technology, under review for FIPS 140-2, Level 3 validation and PKCS#11 compatibility, Luna CA4 is the trusted choice and de facto standard for Root Key protection.

Integration Overview

Entrust Authority Security Manager serves as the Certification Authority in an Entrust infrastructure. When using it in “hardware” mode, you can use the Luna CA4 hardware devices for cryptographic operations and key storage. Among the operations performed on hardware devices are:

- Secure generation of the CA signing private key
- Secure storage of the CA root key
- Signing of certificates and CRL's using the generated or imported key.

Entrust Authority utilizes the following APIs: PKCS #11.

Integration Details

Installation Overview

New Install Luna CA4 with Entrust Security Manager 7.1 SP3

Windows 2000 SP4 32-bit, Solaris 10 SPARC 64-bit

This section describes how to integrate new installations of Entrust Authority Security Manager 7.1 SP3 with Luna CA4. Note that in the following discussion, there is a single server system, the Entrust Authority Security Manager Server, and the Luna CA4 HSM is attached to this server system using a Luna Dock card reader.

1. Preparing the Luna CA4 HSM Server

- i. Install the Luna CA4 Client software on the Entrust/PKI server prior to the installation of Entrust software. Refer to the SafeNet Luna CA4 On-line Help documentation.
- ii. Ensure that a HSM Partition is created on the Luna CA4. The HSM Partition Pin will be used during the Entrust installation. Confirm that CKDEMO can login to the partition.

Note Luna CA4 supports only PKCS#11 V2.

1.1 Installing Entrust Security Manager 7.1 SP3 with Luna CA4 on Windows 2000 SP4 32-bit

- i. Install Informix 9.4 for Entrust Security Manager 7.1, following Entrust documentation.
- ii. Install Entrust Security Manager 7.1, following Entrust documentation.
- iii. Run the Entrust Security Manager 7.1 Configuration Utility. At the point where you choose whether to store keys in hardware or in software, select hardware. Point to the Luna CA4 library path for libcryptoki *C:\Program Files\LunaPCM\cryptoki.dll*.
- iv. Entrust Configuration Utility presents the option to use Luna CA4 hardware, with a given serial number. Select the Luna CA4 hardware.
- v. Continue with the Configuration Utility until complete.
- vi. Initialize Entrust Security Manager for the first time with Entrust Master Control. Add the passwords for Master1, Master2, Master3 and First Officer, following Entrust documentation.
- vii. Entrust Security Manager detects hardware requesting the HSM partition pin. Ensure that the black PED Key is inserted in the PED and enter the HSM Partition Pin that was generated at the creation of the HSM Partition.
- viii. Entrust Security Manager generates the root CA keys on the Luna CA4 partition.
- ix. Entrust Security Manager performs a database backup.

- x. Entrust/PKI is now running.

Installing Entrust 7.1 SP3

- xi. Login as Master1 and stop the Entrust Services.
- xii. Install Informix 9.4 for Entrust Security Manager 7.1 SP3 following Entrust Documentation.
- xiii. Install Entrust Security Manager 7.1 SP3, following Entrust documentation.

1.2 Installing Entrust Security Manager 7.1 SP3 with Luna CA4 on Solaris 10 SPARC 64-bit

- i. Install Informix 9.4 for Entrust Security Manager 7.1 SP3, following Entrust documentation.
- ii. Install Entrust Security Manager 7.1 SP3, following Entrust documentation.
- iii. Run the Entrust Security Manager 7.1 SP3 Configuration Utility. At the point where you choose whether to store keys in hardware or in software, select hardware. Point to the Luna CA4 library path for libcryptoki */usr/lib/libCryptoki2.so*.
- iv. Entrust Configuration Utility presents the option to use Luna CA4 hardware, with a given serial number. Select the Luna CA4 hardware.
- v. Continue with the Configuration Utility until complete.
- vi. Initialize Entrust Security Manager for the first time with Entrust Master Control. Add the passwords for Master1, Master2, Master3 and First Officer, following Entrust documentation.
- vii. Entrust Security Manager detects hardware requesting the HSM partition pin. Ensure that the black PED Key is inserted in the PED and enter the HSM Partition Pin that was generated at the creation of the HSM Partition.
- viii. Entrust Security Manager generates the root CA keys on the Luna CA4 in the provided partition.
- ix. Entrust Security Manager performs a database backup.
- x. Entrust/PKI is now running.

System Behavior/Limitations

When running Entrust Security Manager 7.1 SP3 on Solaris 10 64-bit, use Luna CA4 client software 32-bit as Entrust Security Manager 7.1 SP3 only understands 32-bit.

System Components

CP (Critical Path) Directory Server 4.2 Informix 9.4 Informix 9.4 for Entrust Security Manager 7.1 SP3 Entrust Security Manager 7.1 Entrust Security Manager 7.1 SP3 Entrust Security Manager Administration 7.1 Entrust Security Manager Administration 7.1 SP3 Entrust Entelligence/Desktop Solutions 7.0	Luna CA4 Client software Luna CA4 Token with Firmware 4.6.1 (RoHS)
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

Partner Contact Information

Sales Contact: (800) 533-3958

Support Contact: (800) 545-6608

Please check PSIC for the latest supported version information at:

<https://www.entrust.com/support/psic/index.cfm>

Additional Information

The SafeNet Luna® family of products comprises range of hardware security solutions for digital identity applications. Luna products feature true hardware key management to maintain the integrity of encryption keys. Sensitive keys are created, stored, and used exclusively within the secure confines of the Luna hardware security module (HSM) to prevent compromise.

To learn more about the Luna CA4 product, view the following web site link where additional product information can be found:

<http://www.safenet-inc.com/products/pki/lunaCA4.asp>