Entrust® Securing Digital Identities & Information

Securing Your Digital Life

Entrust Technical Integration Guide for SafeNet Authentication Client, Version 9

January 2015

Table Of Contents

Introduction

This technical integration guide provides an overview of how to integrate Entrust Security Provider 9.2 SP1 with SafeNet Authentication Client 9.

SafeNet's strong authentication solutions enable users of Entrust Security Provider to perform sensitive on-chip RSA key operations, ensuring that user's keys are never exposed to the hostile PC environment.

SafeNet's Authentication Client is the middleware for SafeNet's broad line of smartcard based authentication devices, allowing security applications to easily access a range of security services, including on board of cryptographic keys, secure storage of sensitive keys and credentials, and on board cryptographic key operations.

The highly secure environment of SafeNet's certificate-based authentication devices ensures that cryptographic keys are generated, physically and logically stored – and used – in the closed secure environment of the smart card chip, which protects the keys from the hostile environment of the PC, where they can be stolen or undermined by malware.

Entrust Product Information

Entrust Entelligence® Security Provider is an enterprise-wide security platform for Windows desktops, domain controllers, and authentication servers that allows organizations to deploy the digital identities that enable the strong authentication, encryption and digital signature capabilities within a number of authentication applications and other applications such as data encryption and secure email. This allows customers to meet a broad set of application security requirements, all from a single solution — helping to enable an easy to manage security infrastructure with minimal administrative involvement and impact on end users. Entrust Entelligence® Security Provider's tight integration with native Microsoft Windows security architecture allows it to deliver security to enterprise applications in a way that is easy to deploy and manage.

The Entrust Entelligence™ Security Provider platform is composed of two components:

Entrust Entelligence® Security Provider for Windows automatically manages and protects the digital identities used by applications for encryption, digital signature and authentication.

Entrust Entelligence® Security Provider for Outlook complements Security Provider for Windows by delivering capabilities that simplify the delivery of secure messages from the sender to the recipient's desktop. It increases the performance and simplicity of secure messaging by transferring all the complexities of secure mail processing to the Entrust Entelligence Messaging Server, with no impact to the end user.

SafeNet Product Information

Partner Name: SafeNet Inc.
Website: http://www.safenet-inc.com/products/data-protection/multi-factor-authentication/
Product Name: SafeNet Authentication Client
Product Version: 9
Platform and Service pack:

SafeNet Authentication Client
SafeNet Authentication Client is a unified middleware client that manages SafeNet's extensive portfolio of certificate-based authenticators, including eToken and iKey smart card, USB and software-based devices. With SafeNet Authentication Client, private keys can be generated and stored on-board highly secure smart card-based

authenticators allowing users to securely carry all their digital credentials wherever they go. SafeNet Authentication Client offers support for SafeNet's entire range of certificate based authenticators, including all currently deployed eToken and iKey devices.

SafeNet's certificate-based authenticators enhance access to local and network resources and can incorporate mag-stripe or RF proximity technology on a single device for physical access to an organization. Once logged on to their computers, users can utilize the SafeNet Authentication Client to take advantage of a full range of secure desktop applications including; encrypting and digitally signing e-mail, encrypting private files or folders, accessing remote networks through VPN technology or accessing secure Internet portals.

SafeNet Authentication Client Benefits

- Strong two-factor authentication for network and data protection
- Seamless integration with any certificate-enabled application based on industry standard APIs
- Enables enhanced password management applications for protecting PCs and securing on-site local network access, using eToken Network Logon
- Support for the BlackBerry smart card reader allows strong authentication to BlackBerry devices with SafeNet's eToken PRO Smartcard

Features

- Transparently operates with any standard certificate-based security application allowing organizations to deploy multiple applications including secure access, data encryption and digital signing with a single authenticator
- Support for numerous security applications on a single platform allows organizations to streamline security operations
- Multi-platform support allows organizations to use certificate-enabled security capabilities from any client or server

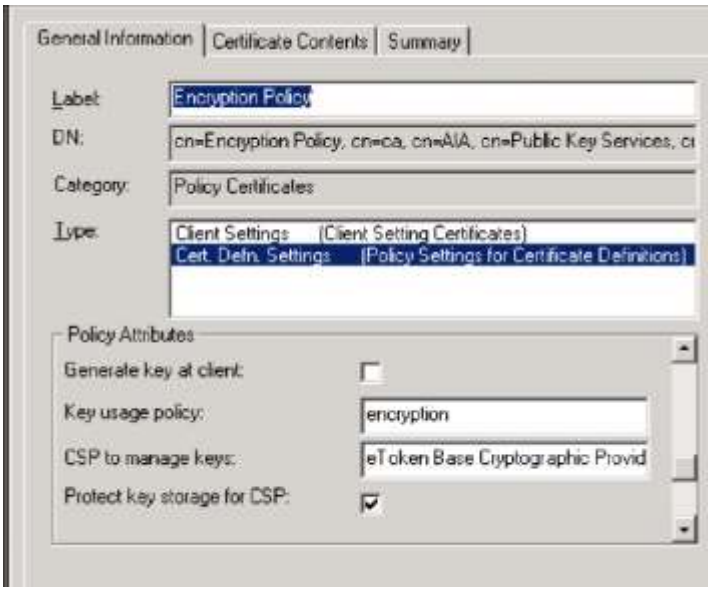
Integration Overview

Entrust Security Provider 9.2 SP1 supports full PKI authentication based on a private key. The private key can be generated and protected by SafeNet certificate-based strong authentication devices, which protects the integrity of the digital identity. A user need only present the certificate stored on the SafeNet device to authenticate successfully or to perform any other secured operation. An Entrust profile is similar to a digital certificate and contains essential information about a user, such as the user name and keys, held in encrypted form. As the private keys are stored on the SafeNet device, users' digital identities are not vulnerable, and hostile entities cannot use a stolen digital identity to penetrate the corporate environment. Generating and keeping the private key on the SafeNet device contributes to the high level of security.

Integration Details

1. To integrate the SafeNet Authentication Client, do the following:
2. Install SafeNet Authentication Client on the client computer where the user will be using the eToken or iKey device.
3. In the Entrust Security Manager Administration, navigate to Security Policy>User Policies, and configure the appropriate policy in the CSP to manage keys as follows:
    - For eToken devices enter: "eToken Base Cryptographic Provider"

For example:



This enables the generation of the certificate's private key directly on the SafeNet authenticator. These actions significantly enhance the overall security of the solution, as a private key which is generated on a SafeNet authenticator cannot be copied or extracted from the device.

Installing the SafeNet Authentication Client

Read these tips before installing the SafeNet Authentication Client.

- The SafeNet Authentication Client includes all the necessary files and drivers to support eToken and iKey integration for Windows. It also includes the SafeNet Authentication Client Tools, which enables easy management of the eToken / iKey name and password.

- SafeNet eToken devices are configured during manufacturing with the factory's default password: "1234567890". SafeNet iKey devices are configured with the password "Password#1". To ensure strong two-factor security, and to enable full user functionality, it is important that the user change the factory default password as soon as possible after receipt of a new authentication device. It is the user's responsibility to remember the device password.

- After installing the SafeNet Authentication Client, eToken and iKey Properties can be launched from Start>Programs>Safenet>Safenet Authentication Client>Safenet Authentication Client Tools, or by right-clicking on the SafeNet Authentication Client tray icon and selecting Tools. SafeNet Authentication Client Properties provides a simple user interface, enabling users to change their own eToken or iKey passwords and names. For more details, see the *SafeNet Authentication Client Administrator's Guide*.

- The SafeNet authenticator password must be used for all device applications, including during eToken / iKey initialization and when the user logs on to Windows using their authentication device. Without the password, the eToken or iKey cannot be used to log on, or for any other purpose.

  Note: The authenticator password should not be confused with the Windows user password that is assigned by the administrator of the domain.

The SafeNet Authentication Client must be installed at the following locations:

- On the computer which is used for initializing eToken / iKey authentication devices.
- On each client computer which is to be used with eToken or iKey authentication solutions. For more details, see the *SafeNet Authentication Client Administrator's Guide*.
- After installing the SafeNet Authentication Client, insert an eToken or iKey, and ensure that the new hardware is recognized and that the eToken or iKey lights up.

For full installation instructions, please refer to the *SafeNet Authentication Client Administrator's Guide.*

SafeNet Authentication Client 9.0 Supported Platforms

SafeNet Authentication Client 9.0 (Windows) supports the following operating systems:

- Windows Vista SP2 (32-bit, 64-bit)
- Windows Server 2008 R2 SP1 (32-bit, 64-bit)
- Windows Server 2008 SP2 (32-bit, 64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2012 R2 (64-bit)
- Windows 7 SP1 (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)

Supported SafeNet Authentication Devices

Entrust Security Provider 9.2 SP1	**Hardware:** Safenet eToken 5100 (Non-FIPS, FIPS, CC) Safenet eToken 5105 (Non-FIPS, FIPS, CC) Safenet eToken 5200 (Non-FIPS, FIPS, CC) Safenet eToken 5205 (Non-FIPS, FIPS, CC) eToken NG-OTP (Non-FIPS, FIPS) eToken PRO 72k (Non-FIPS, FIPS) iKey 4000 eToken Pro Smart Card (Non-FIPS, FIPS) Safenet eToken 4100 (Non-FIPS, FIPS, CC) eToken Virtual Safenet eToken 7300 (VSR/HID, Non-FIPS, FIPS, CC) eToken PRO Anywhere (Non-FIPS, FIPS) eToken NG-FLASH v5.3 - EOL iKey 2032 FIPS - EOL iKey 2032 Non-FIPS - EOL Smart Card 330 FIPS - EOL Smart Card 330 Non-FIPS - EOL SC 400 - EOL

Note: Entrust Security Provider 9.0 and 9.1 are no longer supported.

Partner Contact Information

Sales Contact: Phone: Tel: 1 800 533 3958 - Sales
http://www.safenet-inc.com/form/request-information/
Support Contact:
Technical Support Contact Information:
Phone: 800-545-6608 (US)
Phone: +1 410-931-7520 (International)
eMail: support@safenet-inc.com

About SafeNet

SafeNet is a global leader in information security, protecting data at rest, data in motion, data in use, software and license management with the broadest range of security solutions in the world. The Company protects critical business data, communications, financial transactions, and digital identities through a full spectrum of encryption technologies. In 2007, SafeNet was acquired by Vector Capital, a private equity firm specializing in the technology sector. Vector Capital acquired Aladdin in March of 2009.

SafeNet is the third largest information security company in the world, which brings to market integrated solutions required to solve customers' increasing security challenges. The organization serves more than 25,000 corporate

and government customers in 100 countries. Customers include Apple, Bank of America, Dartmouth College, Ericsson, Fujitsu, Kaiser Permanente, Raytheon, Siemens, Starbucks, U.S. Internal Revenue Service, S.W.I.F.T., Social Security Administration, Departments of Defense and Homeland Security, utilize SafeNet's security solutions.

Comprised of 25 locations globally, SafeNet maintains 1,550 employees—including over 550 security engineers, the largest grouping of any company. As a result of this expertise, SafeNet holds approximately 100 distinct patents.

SafeNet is a member of technological world standard organizations, including the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), the 3rd Generation Partnership Project (3GPP), and the Open Mobile Alliance (OMA)SafeNet is currently involved with the International Organization for Standardization (ISO) 2008 to update future technological principals.