Entrust® Securing Digital Identities & Information

Securing Your Digital Life

Entrust Technical Integration Guide for SafeNet Authentication Client, Version 10.5

March 2018

Table Of Contents

Introduction

This technical integration guide provides an overview of how to integrate Entrust Entelligence Security Provider 10 with SafeNet Authentication Client 10.5.

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

SafeNet's Authentication Client is the middleware for Gemalto's broad line of smart card-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 Gemalto's SafeNet portfolio of certificate-based authentication devices, ensures cryptographic keys are generated, physically and logically stored – and used – in the closed secure environment of the smart card chip. This 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: Gemalto Inc.
Website: https://safenet.gemalto.com/multi-factor-authentication/security-applications/authentication-client-token-management/
Product Name: SafeNet Authentication Client
Product Version: 10.5
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 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 Gemalto's entire range of certificate-based authenticators, including all currently deployed eToken devices.

Gemalto's SafeNet family of certificate-based devices enhance access to local and network resources and can incorporate 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 Features

- 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 full client customization, including security configuration, policies and user interface

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

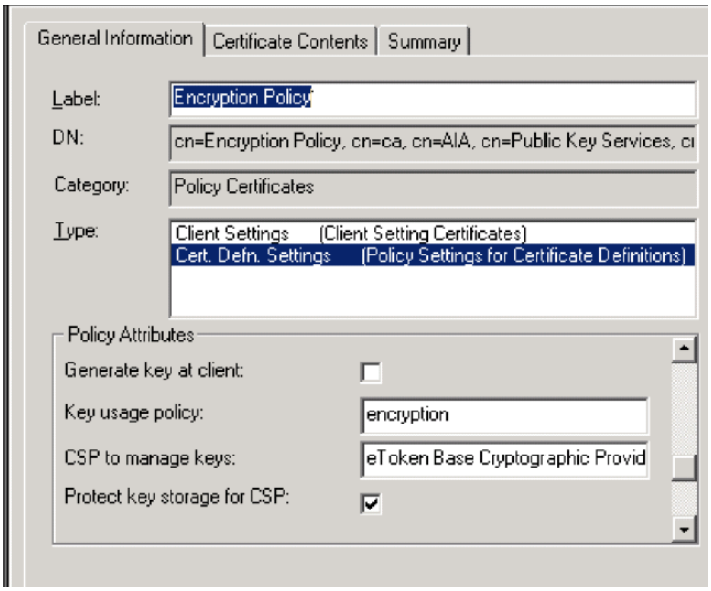
Entrust Entelligence Security Provider 10 supports full PKI authentication based on a private key. The private key can be generated and protected by Gemalto's family of SafeNet certificate-based strong authentication devices, which protects the integrity of the digital identity. A user need only present 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

For CAPI users using CSP provider configure as follows:

1. Install SafeNet Authentication Client on the client computer where the user will be using the eToken or smart card.
2. In Entrust Authority 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"

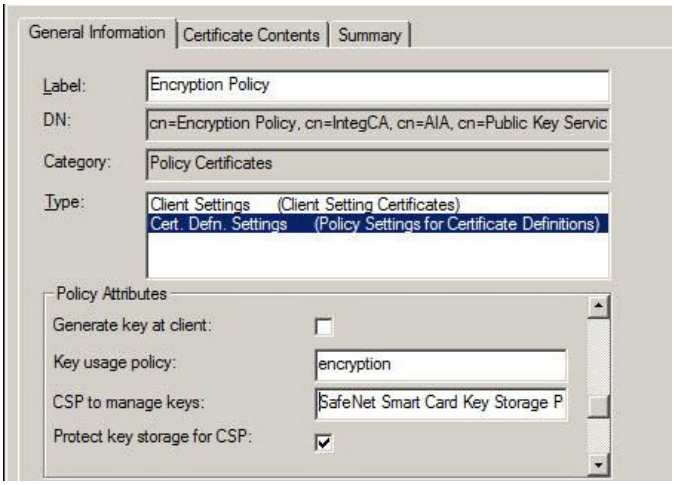
For example:



For CAPI users using KSP provider configure as follows:

1. Install SafeNet Authentication Client on the client computer where the user will be using the eToken or smart card.
2. In Entrust Authority 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: “SafeNet Smart Card Key Storage 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 integration for Windows. It also includes the Safenet Authentication Client Tools, which enables easy management of the eToken name and password.

- SafeNet eToken devices are configured during manufacturing with the factory's default password: "1234567890". 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, SafeNet Authentication Client Tools 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.

- The SafeNet authenticator password must be used for all device applications, including during eToken initialization and when the user logs on to Windows using their authentication device. Without the password, the eToken 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 authentication devices.

- On each client computer which is to be used with eToken authentication solutions. For more details, see the *SafeNet Authentication Client Administrator's Guide*.

- After installing the SafeNet Authentication Client, insert an eToken and ensure that the new hardware is recognized.

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

SafeNet Authentication Client 10.5 Supported Platforms

SafeNet Authentication Client 10.5 (Windows) supports the following operating systems:

- 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 Server 2016 (64-bit)
- Windows 7 SP1 (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)
- Windows 10 (32-bit, 64-bit)

Supported SafeNet Authentication Devices

Entrust Entelligence Security Provider 10	**Hardware:** SafeNet eToken 5110 SafeNet eToken 5110 FIPS SafeNet eToken 5110 CC Gemalto IDCore 30B eToken Gemalto IDPrime MD 840 Gemalto IDPrime MD 840 B Gemalto IDPrime MD 3840 Gemalto IDPrime MD 3840 B Gemalto IDPrime MD 830-FIPS Gemalto IDPrime MD 830 B Gemalto IDPrime MD 3810 Gemalto IDPrime MD 3811

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 Gemalto

Gemalto (Euronext NL0000400653 GTO) is the global leader in digital security, with 2015 annual revenues of €3.1 billion and customers in over 180 countries. We bring trust to an increasingly connected world.

Our technologies and services enable businesses and governments to authenticate identities and protect data so they stay safe and enable services in personal devices, connected objects, the cloud and in between.

Gemalto's solutions are at the heart of modern life, from payment to enterprise security and the internet of things. We authenticate people, transactions and objects, encrypt data and create value for software – enabling our clients to deliver secure digital services for billions of individuals and things.

Our 14,000+ employees operate out of 118 offices, 45 personalization and data centers, and 27 research and software development centers located in 49 countries.

For more information visit www.gemalto.com, or follow @gemalto on Twitter.