Entrust® Securing Digital Identities & Information

Securing Your Digital Life

Entrust Technical Integration Guide for Entrust Entelligence Security Provider and Watchdata WatchKey ProxKey USB Token with Watchdata Ultimate Client

June 2016

Table Of Contents

Introduction

This technical integration guide provides an overview of how to integrate Entrust Entelligence Security Provider with the Watchdata WatchKey ProxKey USB token v5.1 with the Watchdata Ultimate Client 5.1.

WatchKey Proxkey is a PKI-based USB token solution that securely stores certificates and private keys and ensures that the user's identity is tamper proof. It can process electronic signatures during the electronic transaction, and can effectively prevent phishing and man-in-the-middle attacks, extensively increasing the security level of the application.

Designed to meet the demand for secure, fast and reliable external tokens with built-in secure mechanisms, the WatchKey ProxKey USB token is the USB token product built to facilitate high-speed data transmission and encryption operations based on PKI technology.

Device holders can experience portable, easy-to-use and cost-effective features for strong authentication, secure access and online transactions. The device is a plug-and-play capability that brings convenience to end users.

Watchdata Ultimate Client 5.1 supports OS including Windows/Linux/Macintosh, supports browsers including Windows IE/Mozilla Firefox/Safari, supports cryptographic interfaces including PKCS#11 v2/Microsoft CryptoAPI(CAPI/CSP) 2.0/ CNG/Mac TokenD and supports mail clients including Outlook/Thunderbird.

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.

Partner Product Information

Partner Name: Watchdata
Website: http://www.watchdata.com/
Product Name: WatchKey ProxKey
Product Version: v5.1
Client Product Name and Version: Watchdata Ultimate Client 5.1
Platform and Service pack: Windows 8.1

Product description: WatchKey ProxKey is a PKI-based 2FA product that securely stores certificates and private keys and ensures that the user's identity is tamper proof. It can process electronic signatures during the electronic transaction and can effectively prevent phishing and man-in-the-middle attacks, extensively increasing the security level of the application. It can be used in applications requiring security authentication and data encryption, such as banking transaction signing, identity authentication, email/file encryption and others.

The Watchdata Ultimate Client accesses the USB token by CCID communication protocol, sends APDU to the token and is compliant with ISO7816 1-6. The Client offers standard API-like MS-CSP and PKCS11 which are based on the USB token to support standard applications including certificate application, SSL, encryption email and others.

Integration Overview

The WatchKey ProxKey USB token and Client middleware work together with Entrust Entelligence Security Provider for Windows to provide users with a high security token that is used to generate a user's keys and certificates for use with applications.

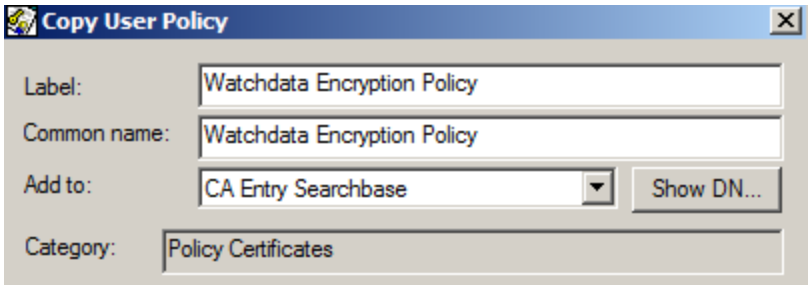
The product complies with the high level security standard, FIPS 140-2 Level 3 for robust application security. It can process electronic signatures during the electronic transaction and data encryption, effectively preventing phishing and man-in-the-middle attacks.

Integration Details

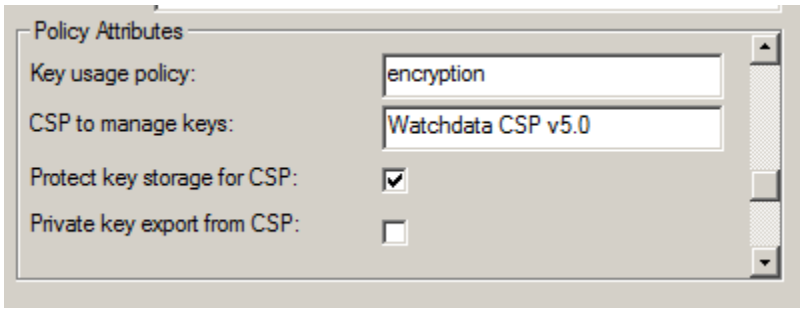
The Watchkey Proxkey USB token uses a Cryptographic Service Provider (CSP) to integrate with Entrust Entelligence Security Provider. The Watchkey Ultimate Client includes the Watchkey CSP and software needed for users and administrators to set and manage token PINs and unblock processes.

Create Certificate Definition Policies

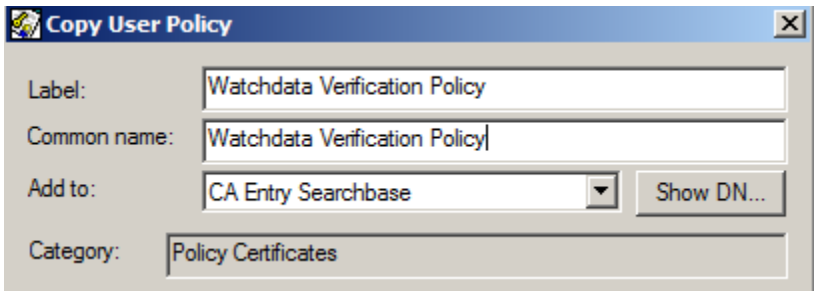
1. Create a new Certificate definition policy in Security Manager Administration
2. Log into Security Manager Administration as a Security Officer or a user with rights to make policy changes
3. Expand Security Policy > User policies and copy an existing policy; these steps are for a 2-key-pair but can also be applied to a 1- or 3-key-pair user
4. Right click on the Encryption policy and select Copy
5. In the Label field enter Watchdata Encryption Policy
6. In the Common name field enter Watchdata Encryption Policy



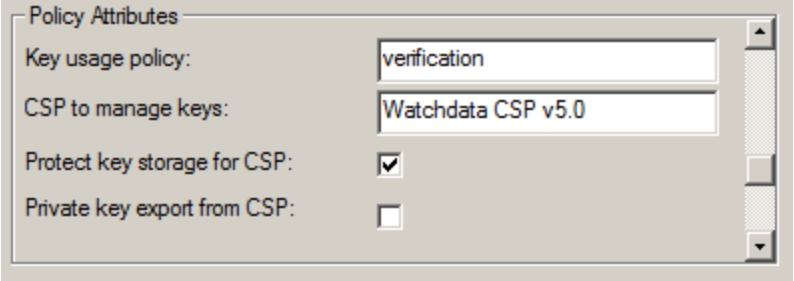
7. In the Policy Attributes field scroll to locate CSP to Manage Keys
8. Enter Watchdata CSP v5.0



9. Click ok
10. Enter your password if prompted
11. Right click on the Verification Policy and click Copy
12. In the Label field enter Watchdata Verification Policy
13. In the Common name field enter Watchdata Verification Policy



14. In the Policy Attributes field scroll to locate CSP to Manage Keys
15. Enter Watchdata CSP v5.0



16. Click ok, enter your password if prompted

Map Watchdata policies to Certificate Type

1. Log into Security Manager Administration as a Security Officer or a user with rights to update certificate types
2. Expand Security Policy > Certificate Categories > Enterprise > Certificate Types > 2-Key-Pair User (2-Key-Pair user)
3. Click on Verification
4. In the Policy Mapping tab select Watchdata Verification Policy from the Certificate definition Policy drop down
5. Click Apply, enter your password if prompted
6. Click on Encryption
7. In the Policy Mapping tab select Watchdata Encryption Policy from the Certificate definition Policy drop down
8. Click Apply, enter your password if prompted

When creating a new user the 2-Key-Pair certificate type is now mapped to the Watchdata Certificate Definition Policies and will force CSP to use the Watchdata CSP when a user is enrolling for their keys and certificates. During Enrollment the Watchdata Ultimate Client will display PIN prompts to the user when their private keys are being generated.

Configuring Entrust Products

See the above section.

System Behavior/Limitations

By default the WatchKey ProxKey USB token is configured to delete a user's certificates from CAPI. This is not configurable.

System Components

Entrust Entelligence Security Provider 9.3 for Windows (with patch 200433)	**Watchdata Ultimate 5.1** **Watchdata WatchKey ProxKey v5.1**

Partner Contact Information

Sales Contact: (chunjiang.long@watchdata.com.sg, HP: +65 8499 6218, www.watchdata.com)
Support Contact: (chunjiang.long@watchdata.com.sg, www.watchdata.com)

Please check PSIC for the latest supported version information.

Additional Information

Watchdata product lines feature contact and contactless EMV, UICC, e-ID and transportation smart cards, online security tokens, card readers and electronic toll collection (ETC) devices. Our end-to-end solutions include secure hardware, operating systems, software applications, and services such as personalization and remote lifecycle management. In intelligent transportation systems (ITS) field, Watchdata offers advanced solutions to address complex urban congestion challenges.
http://www.watchdata.com