

Entrust[®] Securing Digital Identities & Information



**Securing Your
Digital Life**

Entrust Technical Integration Guide for Entrust Authority Security Manager 7.1
and ActivIdentity ActivClient 6.2

June 2009

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 © 2007. Entrust. All rights reserved.

Table Of Contents

| | |
|--|----------|
| Introduction | 1 |
| Entrust Product Information | 1 |
| Partner Product Information | 2 |
| Integration Overview | 3 |
| Supported environments..... | 3 |
| Integration Details | 3 |
| Configuring Entrust Products | 4 |
| Installation/ Configuration for Entrust Desktop Solutions | 4 |
| Installation/Configuration for Entrust Security Manager Administration | 4 |
| Installation/Configuration For Entrust/TruePass | 5 |
| System Behavior/Limitations | 5 |
| System Components | 6 |
| Partner Contact Information | 7 |
| Additional Information | 8 |

Introduction

This technical integration guide provides an overview of how to integrate ActivIdentity ActivClient v6.2 with the following Entrust products:

- Entrust Entelligence Desktop Solutions 6.1 SP2 and 7.0 (only available in ActivClient 32-bit)
- Entrust Entelligence Security Provider 7.0 SP3, 7.1, 8.0 and 9.0
- Entrust Authority® Security Manager 7.1 SP3
- Entrust Authority Security Manager Administration 7.1 SP3
- Entrust Authority Administration Services 7.3
- Entrust Authority PKCS #7 Toolkit for C (aka File Toolkit) 6.1
- Entrust Authority GSS-API Toolkit for C (aka Session Toolkit) 6.1
- Entrust Authority Security Toolkit for Java Version 7.2 SP1
- Entrust TruePass™ 8.0 (no SP and SP2)

Entrust Product Information

Entrust Entelligence Desktop Solution - A client application that provides a consistent, single security layer to the desktop, transparently and automatically managing digital IDs throughout their lifecycle on behalf of the user.

Entrust Entelligence Security Provider - A thin client enterprise-wide desktop security platform that enables organizations to strongly authenticate users and add security, such as encryption and digital signatures, to their applications, in order to protect email and data using one single digital identity.

Entrust Authority Security Manager -the world's-leading **public-key infrastructure** (PKI), is designed to manage the digital keys and certificates that make up the digital identities required to transparently automate all security-related processes in an organization.

Entrust Authority Security Toolkit for the Java Platform - Developers can easily build and deploy online business applications complete with flexible, modular security services, including encryption and digital signatures using X.509 managed certificates.

Entrust PKCS #7 and GSS-API Toolkits for C - Entrust Authority Toolkits provide customers and partners with the ability to apply **best-in-class security** to almost any business application. These Toolkits provide a common set of services to permit developers to rapidly deploy applications that solve business problems without having to spend valuable development cycles developing these common services.

Entrust TruePass -The Entrust TruePass portfolio provides **end-to-end Web security** with unmatched ease of use and user transparency. Information that is protected by Entrust TruePass is secure as it is transmitted in both directions over the Internet (browser to server, server to browser) and when it is stored on the Web server and back-end servers.

Partner Product Information

Partner Name: ActivIdentity Inc

Website: <http://www.actividentity.com>

Product Name: ActivClient

Product Version: 6.2

Platform and Service pack: Windows 2000 SP4, XP SP2/SP3, Vista SP1/SP2

Product description:

ActivClient is the market-leading security application from ActivIdentity that allows business and government customers to easily use smart cards and USB tokens for a wide variety of desktop, network security and productivity applications.

ActivClient enables smart card based PKI authentication for Windows login, VPN, Dial-Up, Web Login, Remote Sessions (Thin Client and Remote Applications), as well as data security, digital signature and secure e-mail. When deployed with 4TRESS™ AAA Server for Remote Access, ActivClient provides two-factor authentication with one-time passwords. Combined with SecureLogin® SSO, ActivClient also allows organizations to enhance workforce productivity by automating enterprise application access.

ActivClient can be used as a standalone end-user client or as a component of the ActivIdentity Smart Employee ID solutions. ActivIdentity client software has been field proven with over 3 million desktop installations and works with leading smart cards, readers, operating systems, certificate authorities, network environments and enterprise applications.

Key Features of ActivClient

- Trusted identity and security services
 - Consolidates multiple credentials and applications on a single, secure device.
 - Enables strong authentication, non-repudiation, digital signatures, encryption and other services.
 - Supports the latest security algorithms and standards.

- Field-proven in demanding environments
 - Next generation of ActivCard® Gold™, the world's leading smart card-based strong authentication software.
 - ActivIdentity client software deployed on millions of desktops globally.
 - ActivIdentity software adopted by leading organizations and governments around the world.

- Maximum interoperability
 - Supports standard government-issued smart cards such as CAC and PIV.
 - Supports leading remote desktops and thin client solutions.
 - Widest range of supported applications and PKI services for easy integration, even in complex IT environments.
 - Supports the widest range of smart cards, readers and USB tokens.
 - Standards-based architecture and available ActivClient SDK enable extensions and custom integrations.

- Easy to deploy, use and maintain
 - Optional automatic software update.

- Simple initialization tool for easy issuance and reset of smart cards and USB tokens.
- Optional deployment with ActivIdentity CMS for secure issuance and lifecycle management of devices and credentials, and for automated smart card update.
- Customizable setup, 'silent' setup option and support for leading software 'push' solutions.
- Familiar interface with branding options.
- Strong security with an ATM-like user experience.
- Extensive troubleshooting, help desk diagnostic tools and wizards.

Key Benefits of ActivClient

- Proven desktop security: Secures access to PCs and networks with smart cards and USB tokens to prevent unauthorized access.
- Secure and portable PKI: Allows digital certificates to be stored on secure devices improving the security and usability of digital signing and encryption applications including electronic forms and email.
- Strong authentication: Enables the use of smart cards and USB tokens to provide two-factor authentication for remote access, workstation and network access (wired and wireless), and application access.
- Secure Information and Transactions: Adds two-factor security for signed and encrypted emails, documents and transactions. Works with leading file and boot encryption partner solutions to protect data on laptop computers and other sensitive locations.
- Single sign-on services: Works with ActivIdentity SecureLogin to simplify the user authentication experience and dramatically reduce the costs associated with managing numerous enterprise passwords.
- Smart Employee ID: Workstation component of the ActivIdentity Smart Employee ID solution combining photo ID, physical access and IT security on a single smart card.

Integration Overview

Supported environments

Microsoft Windows 2000 (SP4) – 32-bit

Microsoft Windows XP Professional (SP2 and SP3) – 32-bit

Microsoft Windows XP Home Edition (SP2 and SP3) – 32-bit

Microsoft Windows Vista (no SP, SP1 and SP2, all editions) – 32- and 64-bit

Microsoft Windows 7 (all editions) – 32- and 64-bit

Microsoft Windows Server 2003 SP2 – 32- and 64-bit

Microsoft Windows Server 2008 (no SP, SP2 and R2) – 32- and 64-bit

Integration Details

About

This chapter describes how to install and to configure ActivIdentity with the following Entrust software:

- Entrust Entelligence Desktop Solutions 6.1 SP2 and 7.0 (only available in ActivClient 32-bit)
- Entrust Entelligence Security Provider 7.0 SP3, 7.1, 8.0 and 9.0
- Entrust Authority® Security Manager 7.1 SP3
- Entrust Authority Security Manager Administration 7.1 SP3
- Entrust Authority Administration Services 7.3
- Entrust Authority PKCS #7 Toolkit for C (aka File Toolkit) 6.1

- Entrust Authority GSS-API Toolkit for C (aka Session Toolkit) 6.1
- Entrust Authority Security Toolkit for Java Version 7.2 SP1
- Entrust TruePass™ 8.0 (no SP and SP2)

Refer to ActivClient v6.2 Installation Guide for installation instructions.

Configuring Entrust Products

Installation/Configuration for Entrust Intelligence Desktop Solutions

Requirements

ActivIdentity ActivClient v6.2 supports the following Entrust Intelligence Desktop Solutions:

- Entrust Intelligence Desktop Solutions 6.1 SP2 and 7.0 (only available in ActivClient 32-bit)

ActivClient installation and configuration

Summary of the steps:

- Install Entrust Intelligence Desktop Solutions as described in Entrust Documentation
- Install ActivClient
 - If Entrust Desktop software is already installed, ActivClient software will automatically detect and add Entrust related features.
 - During the installation, entrust.ini will be configured to use the ActivClient PKCS#11 provider
- Make sure to set the entry “FipsMode” to 0, in the [FIPS Mode] section of the entrust.ini file.

Installation/Configuration for Entrust Intelligence Security Provider

Requirements

ActivIdentity ActivClient v6.2 supports the following Entrust Intelligence Security Provider:

- Entrust Intelligence Security Provider 7.0 SP3, 7.1, 8.0 and 9.0

ActivClient installation and configuration

Summary of the steps:

- Install Entrust Intelligence Security Provider as described in Entrust Documentation
- Install ActivClient: Install the Microsoft CAPI support module

Installation/Configuration for Entrust Authority

Requirements

ActivIdentity ActivClient v6.2 supports the following Entrust Authority products:

- Entrust Authority® Security Manager 7.1 SP3
- Entrust Authority Security Manager Administration 7.1 SP3
- Entrust Authority Administration Services 7.3
- Entrust Authority PKCS #7 Toolkit for C (aka File Toolkit) 6.1
- Entrust Authority GSS-API Toolkit for C (aka Session Toolkit) 6.1
- Entrust Authority Security Toolkit for Java Version 7.2 SP1

ActivClient installation and configuration

Summary of the steps:

- Install Entrust Security Manager Administration as described in Entrust documentation

- Install ActivClient. Since an Entrust Product is already installed (entrust.ini is installed), this feature is installed by default (Typical install). During the installation, entrust.ini is configured to use the ActivClient PKCS#11 provider

Installation/Configuration For Entrust/TruePass

Requirements

ActivIdentity ActivClient v6.2 supports the following Entrust TruePass product:

- Entrust TruePass™ 8.0 (no SP and SP2)

ActivClient installation and configuration

Summary of the steps to configure the TruePass Server:

- Install Entrust/TruePass 8.0 as indicated in the Entrust TruePass 8.0: Installation and Configuration guide
- Customize, in the file EntrustProfileClientConfig.js, the smartcardSigningProvider entry to use ActivClient Cryptographic Service Provider for zero foot print client side operations.
 - // General key generation parameters
 - keyLength="1024";

 - // CAPI Parameters
 - applicationID="o=activcard, c=fr-{79A409C5DFD1D787ED02C276CB8BBC1B}";

 - // CAPI Key Parameters (key creation)
 - encryptionProvider="Microsoft Enhanced Cryptographic Provider v1.0";
 - signingProvider="Microsoft Enhanced Cryptographic Provider v1.0";
 - smartcardSigningProvider="ActivClient Cryptographic Service Provider";

On the client side, you will need to install ActivClient, including the Microsoft CAPI support module.

System Behavior/Limitations

Entrust Entelligence Desktop Solution

When performing an Entrust Profile recovery, the ActivClient PIN may be requested four times even after canceling each time.

Entrust RA may delete an existing X509 certificate on the card when a new Entrust profile is created with Entrust RA.

The PIN may be requested several times during a profile recovery with Entrust RA.

The “Always ask the PIN code before performing any other operation” option is not compatible with Entrust support due to the way Entrust Desktop Solution uses the smart card.

Using the ActivClient user interface, it is possible to change the current smart card PIN code. Doing this while logged on to an Entrust session leads to a session break because Entrust is still using the old PIN code. Log out from Entrust before changing the PIN code with ActivClient.

It is not possible to create an Entrust profile on a card, when the card already contains one.

The Entrust SSO product is supported only with the ActivClient PKCS #11 v2.x library.

If the Entrust application tries to access the smart card resource manager and an error is logged in the event viewer stating that the Entrust service is not responding, ignore this event if the service is correctly started.

Entrust Entelligence Desktop Solution uses its own PIN caching mechanism, independent of ActivClient PIN policies. As a consequence, after you logoff from Windows, Entrust will still allow you to access your smart card for PIN-protected operations (without requiring any PIN entry); while ActivClient will require you to enter the PIN for non-Entrust operations.

If your smart card is full for digital certificates (that is, does not contain any available PKI applet instance), and if you perform an Entrust profile recovery, the old Entrust keys are maintained on the card, available to Entrust Entelligence applications. Also, as long as the old Entrust certificates are still available in the user's Microsoft CAPI store, the associated keys are available to Microsoft CAPI-based applications (such as Outlook).

If your smart card already contains a secure channel protected X509 certificate, and you want to download an Entrust profile using Entrust Desktop Solution 7.0, you will need to install the following Entrust fix: Entrust Entelligence Desktop Manager 7.0 patch 97257.

In some configurations, if you encrypt a file with Entrust right after the creation of an Entrust profile, Entrust will seem to hang for a minute and then will recover. This behavior is not related to ActivClient and can be reproduced when storing the Entrust profile in software instead of using a smart card.

You cannot load an Entrust profile (for Entrust Entelligence Desktop Solution) on a Cryptoflex 8K. Existing Entrust profiles (loaded with ActivCard Gold) can be used with ActivClient.

When you generate an Entrust profile on the card, or when you recover such a profile, you may see several PIN prompts.

Entrust Entelligence Security Provider

Enrolling an Entrust ID on a smart card that is full is not supported.

Update certificate on a smart card that is full is not supported.

Performing a recovery operation on an empty smart card with ESP v8 creates three certificates instead of two.

If you use Entrust with 2 key pairs, and if you use a card profile with only 3 PKI (standard profile for 32K smart cards), then recovery of Entrust certificates is not possible: 4 PKI instances are required on the card by Entrust design. ActivIdentity recommends using a card profile with 6 PKI or more (typical with 64K smart card).

System Components

| List Entrust products including their versions. | List Partner products including their versions. |
|--|--|
| Entrust Entelligence Desktop Solutions 6.1 SP2 and 7.0 | ActivClient 6.2 (32-bit only) |
| Entrust Entelligence Security Provider 7.0 SP3, 7.1, 8.0 and 9.0 | ActivClient 6.2 |
| Entrust Authority® Security Manager 7.1 SP3 | ActivClient 6.2 |

| | |
|---|-----------------|
| Entrust Authority Security Manager Administration 7.1 SP3 | ActivClient 6.2 |
| Entrust Authority Administration Services 7.3 | ActivClient 6.2 |
| Entrust Authority PKCS #7 Toolkit for C (aka File Toolkit) 6.1 | ActivClient 6.2 |
| Entrust Authority GSS-API Toolkit for C (aka Session Toolkit) 6.1 | ActivClient 6.2 |
| Entrust Authority Security Toolkit for Java Version 7.2 SP1 | ActivClient 6.2 |
| Entrust TruePass™ 8.0 (no SP and SP2) | ActivClient 6.2 |

Partner Contact Information

Sales Contact:

ActivIdentity North America
Corporate Headquarters
6623 Dumbarton Circle
Fremont, CA 94555 USA
TEL: (1) (510) 574-0100
FAX: (1) 510) 574- 0101

ActivIdentity Europe
European Corporate Headquarters
24-28 Avenue du General de Gaulle
92156 SURESNES, Cedex FRANCE
TEL: (33) (0) 1-42-04-84-00
FAX: (33) (0) 1-42-04-84-84

ActivIdentity Australia
Asia/Pacific Corporate Headquarters
7 Phipps Close
Deakin, ACT, 2600 Australia
Tel: +61 (2) 6208.4888
Fax: +61 (2) 6281.7460

Web site www.actividentity.com

Support Contact:

ActivIdentity North America
Corporate Headquarters
6623 Dumbarton Circle
Fremont, CA 94555 USA
TEL: (1) (510) 574-0100
FAX: (1) 510) 574- 0101

ActivIdentity Europe
European Corporate Headquarters
24-28 Avenue du General de Gaulle
92156 SURESNES, Cedex FRANCE

TEL: (33) (0) 1-42-04-84-00
FAX: (33) (0) 1-42-04-84-84

ActivIdentity Australia
Asia/Pacific Corporate Headquarters
7 Phipps Close
Deakin, ACT, 2600 Australia
Tel: +61 (2) 6208.4888
Fax: +61 (2) 6281.7460

For technical support contact: support@actividentity.com

Please check PSIC for the latest supported version information at:
<https://www.entrust.com/support/psic/index.cfm>

Additional Information

Additional information can be found at <http://www.actividentity.com>.