

WHITE PAPER
**ENTRUST ENTELLIGENCE™
SECURITY PROVIDER 7.0 FOR
WINDOWS – PRODUCT OVERVIEW**

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. All other Entrust product names and service names are trademarks of Entrust. 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 REPRESENTATION AND/OR WARRANTY 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, OR FITNESS FOR A SPECIFIC PURPOSE.

Table of Contents

1. EXECUTIVE SUMMARY	1
1.1 OVERVIEW.....	1
1.2 PURPOSE.....	1
1.3 COMPLEMENTARY DOCUMENTS	2
2. BACKGROUND.....	3
2.1 TRADITIONAL ENTRUST APPROACH	3
2.2 NEW GENERATION ENTERPRISE SECURITY PLATFORM.....	3
3. ENTERPRISE DESKTOP SECURITY	5
3.1 OVERVIEW.....	5
3.2 SECURING DIGITAL IDENTITIES AND INFORMATION.....	5
4. SECURE ENTERPRISE DESKTOP APPLICATIONS	6
4.1 ENTRUST SECURE VPN SOLUTION	6
4.2 ENTRUST SECURE WLAN SOLUTION	7
4.3 ENTRUST SECURE MESSAGING SOLUTION	7
4.4 ENTRUST SECURE E-FORMS SOLUTION	8
4.5 ENTRUST SECURE DESKTOP SOLUTION.....	8
4.6 SECURE WEB (SSL) AUTHENTICATION	9
5. THE WINDOWS APPLICATION SECURITY ARCHITECTURE	11
5.1 WINDOWS CRYPTOAPI.....	11
5.2 CRYPTOGRAPHIC SERVICE PROVIDERS (CSPS).....	12
5.3 CERTIFICATE STORES	12
5.4 KEY CONTAINERS.....	14
5.5 APPLICATIONS	14
6. ENTRUST ENTELLIGENCE SECURITY PROVIDER.....	15
6.1 SECURITY PROVIDER ARCHITECTURE	15
6.2 COMPONENTS.....	15
6.3 SECURITY PROVIDER DEPLOYMENT	22
7. SUMMARY	28
7.1 EASY TO DEPLOY	28

7.2 EASY TO MANAGE 29

7.3 EASY TO USE 29

7.4 SECURING DIGITAL IDENTITIES AND INFORMATION 30

1. EXECUTIVE SUMMARY

1.1 OVERVIEW

Entrust Entelligence™ Security Provider 7.0 (Security Provider), is a thin-client enterprise desktop security product that enables the efficient deployment of security at a reduced cost. Security Provider delivers managed Entrust digital IDs to mission critical enterprise applications such as email, file/folder encryption, network authentication (Windows Smart Card Logon, VPN, WLAN, etc.), electronic forms and document creation and collaboration.

Security Provider is easier for users to manage and use as it automates the entire lifecycle management of the user's digital identity – from self-serve enrollment to automatic updates – it reduces the administrative involvement and impact on both users and administrators. Security Provider can also enforce strong protection of the user's digital identity by enforcing centrally controlled security and password policies. As such, Security Provider helps prevent unauthorized access to sensitive resources and information stored on the network, a desktop or laptop. Security Provider is ideal for any organization that requires quicker and easier deployment of desktop security at a reduced cost.

1.2 PURPOSE

The purpose of this white paper is to explain how Entrust integrates tightly with Microsoft Windows native cryptographic security capabilities to help provide secure and managed Entrust digital IDs for applications to use for authentication, digital signature and data encryption. In particular, this document explains how Security Provider integrates with the native Windows application security architecture and demonstrates how customers can leverage this integration to enable a wide range of secure solutions to meet the needs of their organization.

The white paper begins with an overview of generic desktop security concepts including the native Windows application security architecture —the integration point that Entrust leverages to enable desktop applications. This overview explains this architecture and how its components work together to deliver the security features it provides to the Windows desktop environment.

The next section explains how Security Provider integrates into the native Windows security architecture through the Microsoft CryptoAPI to deliver a managed Entrust digital ID to native applications.

The final section of this white paper outlines some of the many solutions that can take advantage of an Entrust digital ID that is delivered to the desktop and managed by Security Provider.

The following section of this white paper highlights the value of Entrust's digital ID management. Security Provider delivers the automation of the entire digital ID lifecycle management through self-service enrollment and automatic and transparent renewal. Security Provider not only takes care of managing the user's digital ID and the enforcement of enterprise security policy, it also limits administrative involvement in user deployment and management to help drive down the total cost of ownership.

The next section describes the technology implemented in Security Provider that helps make it easier to deploy to end users over any network bandwidth, simpler to manage and upgrade and allows for central configuration and user management.

1.3 COMPLEMENTARY DOCUMENTS

Obtaining more information about CryptoAPI

Microsoft has detailed documentation about CryptoAPI on the MSDN website, including samples of code that use CryptoAPI functions. To obtain this information, go to <http://msdn.microsoft.com>, select the MSDN Library and search for CryptoAPI.

2. BACKGROUND

2.1 TRADITIONAL ENTRUST APPROACH

In 1994, Entrust built and sold the first commercially available public-key infrastructure (PKI) to make it possible to manage the keys and certificates that enable encryption and digital signatures. Now in its 7th edition, the Entrust Authority™ product portfolio is one of the industry's most relied upon PKI solution.

The mid-1990's client-server network architectures featured client applications that natively did not support public-key based digital signature, encryption and authentication capabilities. In order to allow many of the leading desktop applications to take advantage of Entrust certificates and keys Entrust developed its own series of application plug-ins designed to allow desktop applications to conduct secure cryptographic operations.

As such, in 1996 Entrust delivered its first client-software designed to maximize the benefits of PKI and make security easier and more transparent for users. Today Entrust Entelligence Desktop Manager and its associated plug-ins are used to secure the files, e-mail, e-forms, VPNs and wireless LANs (WLAN) of many of the world's largest enterprises, banks, health care institutions and government departments.

2.2 NEW GENERATION ENTERPRISE SECURITY PLATFORM

As the Windows operating system and applications evolved through the 1990s Microsoft and other application vendors have implemented and improved cryptographic security capabilities in their own applications. Key to these improvements is Microsoft's release of the CryptoAPI: a Windows application programming interface (API) that provides public-key cryptographic security capabilities to desktop operating systems, allowing any application to utilize built-in Microsoft desktop cryptographic functionality.

At the same time, Microsoft was making significant progress in implementing security functionality in Office applications and in the operating system itself to the point where the latest versions of Windows and Office have the functional capabilities to secure network authentication, email communications, desktop files and a number of other applications without requiring the use of Entrust plug-ins. However, Entrust customers still require the use of Entrust managed digital IDs in order to take advantage of Entrust's full lifecycle digital ID management and superior ability to secure these digital IDs and information.

Entrust is proud to introduce its new-generation enterprise security platform with the release of Entrust Entelligence Security Provider 7.0. Security Provider is a thin-client enterprise desktop security product that enables faster and easier deployment of security at a reduced cost. Security Provider delivers managed Entrust digital IDs to mission critical enterprise applications such as email, file/folder encryption, network authentication (Windows Smart Card Logon, VPN, WLAN, etc.), electronic forms and document creation and collaboration.

Security Provider is easy for users to manage and use as it automates the entire lifecycle management of the user's digital identity – from self-serve enrollment to automatic update – it reduces the administrative involvement and impact on both users and administrators.

Security Provider can also enforce strong protection of the user's digital identity and by enforcing centrally controlled security and password policies. As such, Security Provider helps prevent unauthorized access to sensitive resources and information stored on the network, a desktop or laptop. Security Provider is ideal for any organization that requires quicker and easier deployment of desktop security at a reduced cost.

3. ENTERPRISE DESKTOP SECURITY

3.1 OVERVIEW

In a time of increasing identity theft and fraud, it pays to secure information and applications at their source: the desktop. No longer are data thieves striking exclusively from online. Hard-drives and other pieces of hardware containing critical information have, and will continue to be, stolen. Even information that can be accessed via an office workstation requires security because the majority of security breaches, as well as the exploitation of user identity, are undertaken by people internal to an organization. Security Provider helps to protect the integrity and privacy of your data in this type of an environment.

Enterprise security is an ongoing challenge for organizations to implement and maintain. With disparate systems and global, remote users to protect, enterprises need cost effective security solutions that are easier to deploy and administer. Industry analysts agree that the loss of hardware is serious, but the costs to an organization from the loss of sensitive data can be disastrous. Entrust's new generation of desktop security solutions promises to address these challenges by enabling an easy to manage security infrastructure with minimal administrative involvement or impact on end users. As a result, security for desktop applications is significantly improved and overall IT costs are reduced.

3.2 SECURING DIGITAL IDENTITIES AND INFORMATION

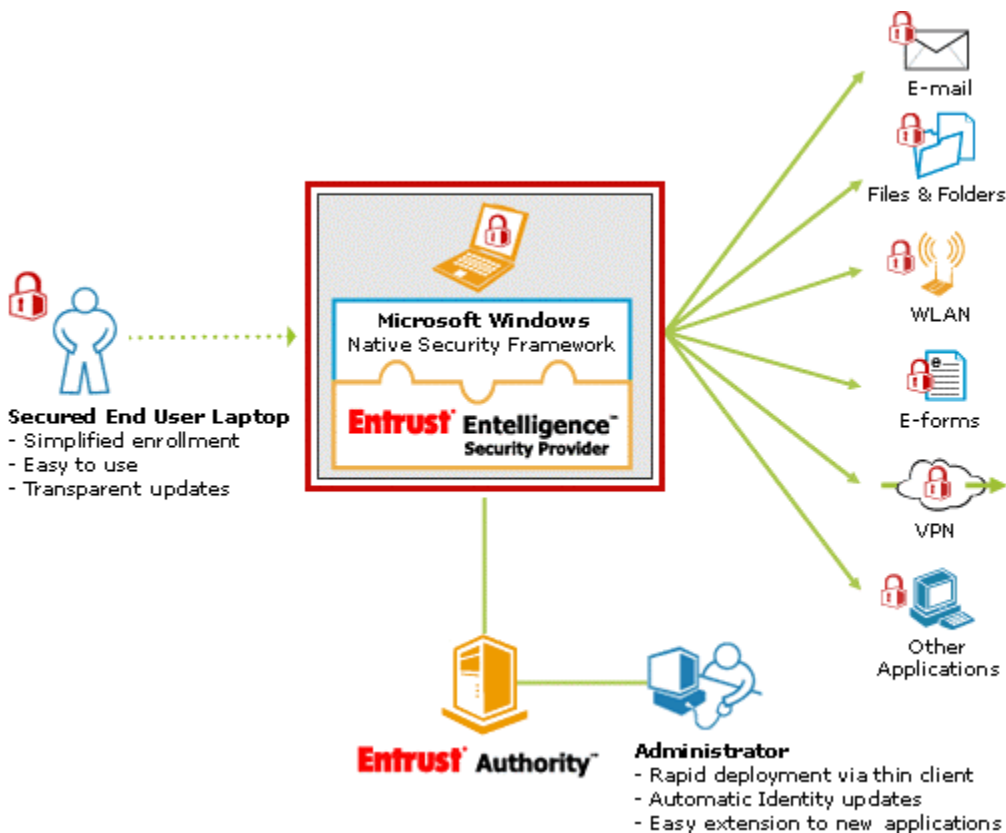
Secure digital identities are critical for securing digital information. You have to confidently authenticate someone to provide them authorized access to sensitive information, whether that's through a simple authentication application such a network logon or via information encryption. It is easy to secure information if you never want anyone to access it (of course, that's not very useful) - the hard part of information security is ensuring that sensitive information is only accessible to those authorized to see it. Entrust secures digital IDs by imposing **strong protection on the user's private keys**, preventing intruders and rogue users from impersonating employees and allowing them to gain access to valuable resources and information.

Secure digital information is also essential for organizations to be able to leverage technology to get the most out of their relationships and transactions. When organizations can distribute information securely to customers, partners, and employees over the Internet and enterprise networks, they enable effective, efficient decision-making and actions. And secure distribution of digital information can enable new services that strengthen relationships with constituents and, ultimately, provide new opportunities for revenue and cost savings. Just think of the numerous productivity and cost saving benefits of online banking, for example. Without assurance that banking information is secure, those benefits would be unattainable because nobody would use the technology. Security Provider allows users to take advantage of Entrust secure digital IDs to **encrypt information** to protect the data so that only those authorized to access the information can do so.

Securing digital information isn't only about protecting access to sensitive information for privacy. Entrust also enables users to secure information through **digital signatures** to provide **accountability**, a key requirement for transactions and information, including those that do not contain any sensitive content.

4. SECURE ENTERPRISE DESKTOP APPLICATIONS

Any application that runs on Windows can be set up to use CryptoAPI and take advantage of its built-in PKI capabilities. Both Microsoft and third-party vendors provide CryptoAPI-enabled applications. As such, organizations can leverage a number of applications that are commercially available today from Microsoft and other vendors, together with managed Entrust digital IDs supplied to the desktop by Security Provider, to enable a wide range of Secure Desktop Solutions including secure VPNs, wireless LANs, e-mail, e-forms and secure files and folders throughout the enterprise, all with a single digital ID per user.



4.1 ENTRUST SECURE VPN SOLUTION

The **Entrust Secure VPN Solution** provides strong authentication to VPN environments for remote connectivity. This solution helps to mitigate the risk of unauthorized access to your network and avoid the costs associated with security breaches. The confidence in user identities provided by the solution enables your organization to move *more* people to the VPN and which translates into additional savings in communication costs and productivity gains.



Security Provider delivers an Entrust digital ID that can be used with leading VPN clients (Cisco, Nortel, Checkpoint, and Microsoft) for certificate-based authentication to the VPN gateway. These vendors and others have client applications that support cryptographic calls to the Windows application security architecture that can securely connect remote users to enterprise resources.

4.2 ENTRUST SECURE WLAN SOLUTION

The Entrust Secure WLAN Solution strengthens the security that is provided with native wireless LAN capabilities by restricting network access solely to authorized individuals. Knowing with confidence that sensitive information can be shared securely and only amongst trusted individuals, organizations are able to fully leverage the reduced networking costs and productivity gains achieved through widespread deployment of a wireless LAN. The Entrust Secure WLAN Solution works seamlessly with industry leading solutions from vendors like Cisco, enabling organizations to leverage their chosen investment in WLAN technology.

The Entrust Secure WLAN Solution provides strong authentication to accurately identify the users who access your wireless LAN. Users and devices are strongly authenticated via their digital ID that is stored in encrypted form on the computer and unlocked locally with a strong, policy controlled password that never leaves the device and is never sent across the network. Hence it cannot be intercepted and cracked. Moreover, it is harder for hackers to impersonate a legitimate user from a remote machine since they do not possess the user's digital ID.



Security Provider delivers the managed digital ID and the security necessary for an organization to widely deploy WLANs, providing users the mobility to access applications and information from any location. The solution strengthens protection against network breaches and their associated costs while helping drive significant productivity improvements for employees.

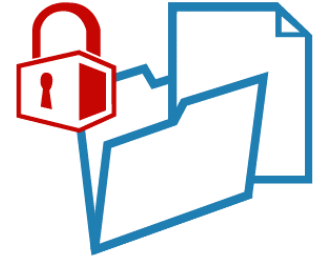
4.3 ENTRUST SECURE MESSAGING SOLUTION

The Entrust Secure Messaging Solution uses encryption and digital signatures to protect the privacy and accountability of information sent over e-mail and as attachments to e-mail messages. Digitally signing e-mail messages can also provide an auditable record of transactions and communications, helping organizations move paper-based transactions online. The Solution helps organizations enhance their current e-mail investment, is easier to use and administer, and can scale to address an organization's needs now, and in the future. The Entrust Secure Messaging Solution utilizes e-mail applications such as Microsoft Outlook and other CryptoAPI-aware clients such as the soon-to-be released Outlook Web Access to enable encryption and digital signature of messages and attachments



By transparently managing the keys and certificates that add enhanced security to each e-mail message, **Security Provider** makes it possible to increase confidence in the identification, privacy and verification of e-mail communications. These safety measures make it possible to optimize e-mail usage and increase the reach, speed and return achieved through an organizations messaging activities.

By taking advantage of the latest versions of Microsoft Outlook and Microsoft Operating system, combined with the security management capabilities delivered by Security Provider, organizations can deploy a Secure Messaging Solution that delivers the ability to encrypt and digitally sign important communications — including any type of attachments — so that only intended recipients can access the message, both in transit and at its end destination(s).



Microsoft Outlook 2000 Service Release 1 (SR-1), Outlook 2002 and upcoming releases of Outlook provide the security capabilities required for an organization’s users to communicate securely between each other. With the release of Outlook 2000 SR-1 Microsoft introduced support for the Secure/Multipurpose Internet Mail Extensions (S/MIME) v3 standard. This and subsequent releases include enhanced encryption and security features such as security labels and signed receipts. These new features support the S/MIME v3 protocol, an Internet standard that extends S/MIME v2.

4.4 ENTRUST SECURE E-FORMS SOLUTION

The Entrust Secure E-Forms Solution makes it possible to secure the workflow and apply digital signatures to Adobe forms, Adobe PDFs and other Web-based forms. It enables online process by strongly authenticating users and allow secure workflow through entitlements-based control over form content and approval processes. Reports can be securely submitted—files are digitally signed on-line, creating an audit trail of verified, secure submissions.

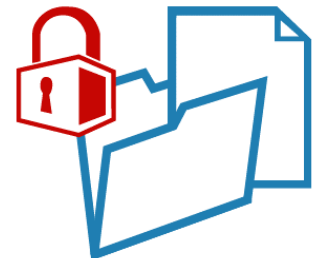


Combined with leading E-Forms applications such as Adobe Acrobat 6.0, **Security Provider** delivers digital signatures powered by Entrust Authority Security Manager, Entrust’s market leading public-key infrastructure (PKI) technology. This type of electronic signature is widely recognized as a best practice for digital verification of electronic transactions. Digital signatures are one of the most effective, secure, and easy-to-implement method of providing verification while enabling electronic transactions. The benefits of PKI-powered digital signatures include authentication, authorization and digital signatures.

4.5 ENTRUST SECURE DESKTOP SOLUTION

The Entrust Secure Desktop Solution protects access to workstations and the files and folders stored on laptops, desktops, mobile devices, and corporate networks, enabling cost-effective collaboration while mitigating the risks associated with storing and sharing data electronically. Files and folders are encrypted automatically in accordance with centrally enforced policies, making it easier for employees to maintain the privacy of valuable information whether they are in the office or ‘on the road’.

Today's workforce uses desktop computers and laptops to write, negotiate, sell, plan, and strategize about the entire future of an organization. These common devices and the networks behind them have become home to some of the most important assets an organization has, which is its intellectual property.



Security Provider leverages the Microsoft Encrypting File System to help organizations secure sensitive and valuable information stored on laptops,

desktops and corporate networks — reducing the need for inefficient and costly paper-based processes and physical security measures. Security Provider also delivers the simplified key back up and recovery processes those organizations require to deploy EFS in large scale across the organization.

Since Entrust easily and seamlessly backs up user's keys and maintains a history of older keys resulting from key updates, a simple key recovery operation will deliver a complete key history to the Security Provider user. Should anything happen to user digital identities, preventing them from decrypting documents, recovery administration is conducted centrally and automatically without the need to set up complex recovery systems and procedures.

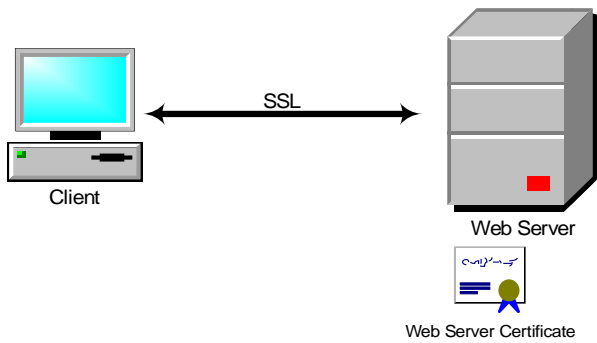
4.6 SECURE WEB (SSL) AUTHENTICATION

Security Provider delivers managed digital identities to Crypto-API (Windows Security Framework) and makes them available to Internet Explorer allowing users to have managed certificates for strong authentication in client browsers. This enhanced capability comes without any additional browser plug-ins, providing a cost effective and easy to deploy Web authentication solution.

In order to secure Web transactions, a solution must protect the transmission of data as well secure authentication of both the server and the client. Both parties involved in the transaction must be sure of the identity of who is at either end. One of the standards created in response to these requirements is Secure Sockets Layer (SSL). Fundamentally, SSL is used to establish an encrypted session between the web client and the web server. Basic security through SSL authentication allows the user to validate the identity of the Web server they are trying to access. In addition to checking the server name, other checks are done including:

- 1) A cryptographic check to confirm that the Web site owns the private key associated with the public key in the certificate.
- 2) A check that the name in the certificate is the same as the name of the Web site.
- 3) A check that the issuer of the Web site's certificate is trusted.
- 4) A check that the certificate has not expired.
- 5) A check that the certificate has not been revoked. By default, Internet Explorer does not verify certificate revocation status of the web server certificate.
- 6) A check that the certificate has not been tampered with.

Once successful, the session between the user and server can be secured through encryption. This one-way authentication is accomplished through Web server certificate validation. Once the encrypted session is established, enhanced security can be added to the Web transaction by securely validating the user's identity.



Once SSL is enabled on a web server, the next step is to provide for client authentication (cryptographic validation by the server of the client's identity) where anonymous access is not appropriate. By challenging the client browser to present its own user certificate for validation, the server can be assured of the identity of the user who is trying to access server resources. Successful client certificate validation leads to confirmed identification and achieves the goal of two-way authentication. With client authentication, the web server can also provide access control on its resources based on the user's identity, which is linked to the client's certificate. In this scenario, the client also requires a certificate, which will be used during the SSL handshake. This type of authentication is typically referred to as mutual authentication because each party authenticates the other.

Microsoft Internet Explorer

Microsoft Internet Explorer uses industry-standard X.509 v3 digital certificates to authenticate clients and servers on the Web and to ensure that browser communications are secure and that the integrity of exchanged content is maintained.

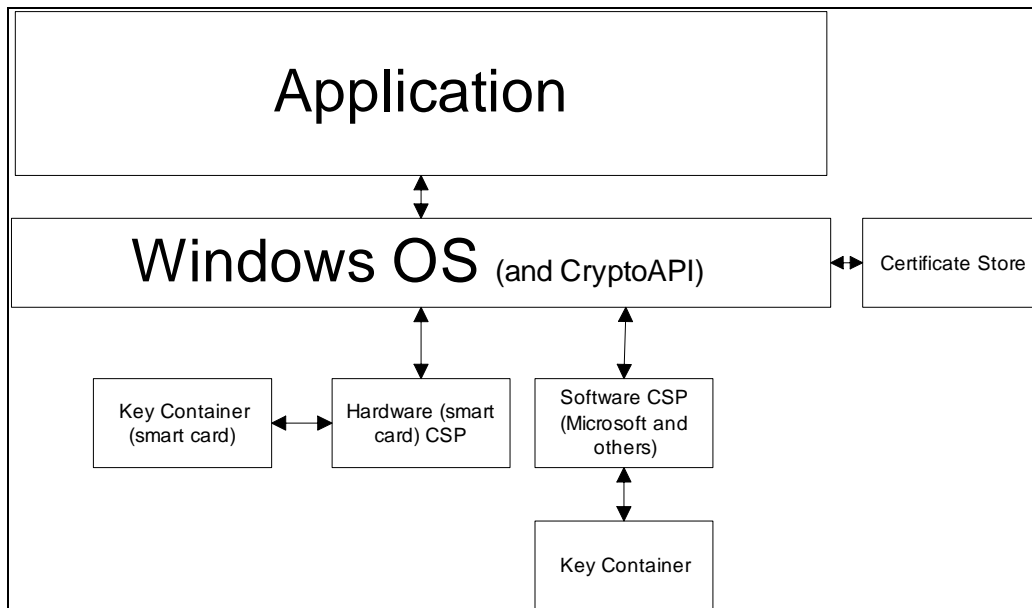
The latest version of Internet Explorer includes support for server certificate revocation, which verifies that an issuing CA has not revoked a server certificate. This feature checks for CryptoAPI revocation when the proper certificate extensions are present.

5. THE WINDOWS APPLICATION SECURITY ARCHITECTURE

Security Provider’s principal role is the delivery of managed Entrust keys and certificates to the native Windows application security architecture for use by any application built to take advantage of native digital signature, authentication and encryption capabilities. This section of the document provides an overview of the native Windows security architecture, required to clearly understand how Security Provider delivers Entrust managed digital IDs to these native security capabilities.

The following five components of the Windows application security architecture will be addressed in this section:

1. CryptoAPI
2. Cryptographic Service Providers (CSPs)
3. Certificate Stores
4. Key Containers
5. Applications



5.1 WINDOWS CRYPTOAPI

CryptoAPI is a Windows Application Programmer’s Interface (API). It provides public and private key cryptographic client capabilities to the desktop operating system, allowing any application to take advantage of built-in Microsoft desktop cryptographic functionality. It is based on open standards, including X.509, S/MIME, IPSec, and supports a wide range of cryptographic algorithms (and is extensible to accommodate additional algorithms from 3rd party vendors). CryptoAPI contains functions that applications can invoke in order to encrypt or digitally sign data, insulating the application from the details of these operations. This means that

CryptoAPI does not actually perform the operation. Instead, it hands off the cryptographic operation to a Cryptographic Service Provider (CSP). CryptoAPI is also an interface to the Certificate Stores, where user, machine, and CA certificates are stored. When a certificate is required, CryptoAPI queries the Certificate Store to return a list of available certificates.

5.2 CRYPTOGRAPHIC SERVICE PROVIDERS (CSPS)

Cryptographic Service Providers (CSPs) plug into CryptoAPI. They perform all cryptographic operations, such as encrypting and decrypting data, verifying signatures, signing data, and verifying certificates. When an application requires a cryptographic operation, CryptoAPI routes the request to a CSP.

CSPs interface with the private key container, where the user's private keys are securely held. (In contrast, CryptoAPI interfaces with the Certificate Stores, which hold certificates, not private keys). The private key container can be on the local machine, on a device such as a smart card or stored centrally and accessible from a network to mobile users when deployed with the Entrust Roaming Server.

Microsoft ships a number of CSPs with the operating system, and with Internet Explorer (assuming the computer has Windows 95 or higher, and Internet Explorer 4 or higher is installed). Examples include a 56-bit Base CSP, and a 128-bit Enhanced CSP (the component installed when you do a 128-bit browser upgrade, and which also comes standard with Windows 2000 SP2 and Windows XP). The version of each CSP is dependent on the OS or version of Internet Explorer it shipped with. The Microsoft Enhanced CSP is FIPS 140-1 validated.

It is also possible for third parties to write their own CSPs. This may be done so that the CSP can support different algorithms, or so that the CSP can use a different private key container than the one provided by Microsoft. For example, in a smart card deployment users store their private keys directly on the smart card rather than in the local Microsoft private key container. To enable this smart card vendors write their own CSPs for use by CryptoAPI. Details on Security Provider and its CSPs and key container are outlined later in this document.

There are typically several CSPs on each computer. Each certificate is associated (indirectly, through the matching private key) with only one CSP (although one CSP may manage many certificates). The Certificate Stores keep track of the CSP associated with each certificate.

5.3 CERTIFICATE STORES

Certificate Store Functionality

Certificate Stores keep track of the CSP associated with a certificate. This allows a user to have many CSPs on one machine, without having to remember which certificate is associated with which CSP.

Certificate Stores can be broken into two categories. The first category holds certificates for **users, Certification Authorities (CAs) and Publishers**. It includes the following Certificate Stores:

Certificate Store	Description	Uses
Personal	Holds certificates issued to the user	<ul style="list-style-type: none">• decryption of incoming e-mail• signing of outgoing e-mail• used in SSL for client authentication
Other People	Holds certificates for individuals other than the user	<ul style="list-style-type: none">• encrypting outgoing e-mail• validating incoming signed e-mail
Trusted Root Certification Authorities	Holds self-signed root certificates for trusted CAs	<ul style="list-style-type: none">• establishes trust anchors for validation of certificates
Intermediate Certification Authorities	Holds certificates for trusted subordinate CAs	<ul style="list-style-type: none">• establishes trust short-cuts for validation of certificates
Publishers	Holds certificates for trusted software publishers	<ul style="list-style-type: none">• allows verification of Authenticode-signed software

Machine Certificates

The second category of Certificate Stores holds machine certificates. These are certificates that are associated with the computer, not individual users or corporate entities. For example, the machine store can hold:

- Windows IPsec (i.e. VPN) client certificates for machine identification (for Windows 2000 and above)
- Internet Information Server Web server certificates

Intermediate or Trusted Root Certificate Stores

The certificates in the Intermediate or Trusted Root Certificate Stores either are pre-installed with the OS or are added later. There are three ways these can be updated:

- Manual import of a new certificate by users with Windows local administrator privileges. For instance, Microsoft Certificate Services Web Enrollment pages allow the user to download and install the CA certificate.
- Automated import by a CryptoAPI program. This assumes the user has local administrator privileges. CryptoAPI prompts the user through a dialog before the certificate is accepted.
- Automated distribution of the new certificate through centrally managed group policy. This is transparent to the user—there are no associated client dialogs. This option is available in Windows 2000 and later.

5.4 KEY CONTAINERS

The Key Containers hold the private keys of the user or machine. Specifically, this includes the current decryption private key and signing private key, and may also contain a history of the user's old decryption private keys.

The Key Container is managed by its associated CSP. In other words, it is only accessible to the CSP that provided its keys. The CSP determines where the Key Container is located (and therefore where the private keys are stored). The CSP also determines what algorithm is used to protect the Key Container. As an example, the Microsoft Enhanced CSP uses the RCA algorithm to provide 128-bit encryption. The Windows applications security architecture on the desktop allows for multiple options for key storage, among which are Microsoft's own key container, smart cards or other key containers deployed by other vendors such as Entrust.

Microsoft Key Protection

In Windows 2000 and XP, Microsoft CSPs store their private keys using the Data Protection API - DPAPI. All keys stored in this area are encrypted automatically with a random, symmetric key. For the Enhanced CSP, an RC4 128-bit key is used, and for the Base CSP, an RC4 56-bit key is used. More information on Microsoft's DPAPI is available on the Microsoft Web site at: <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/windataprotection-dpapi.asp>

Smart Card Key Protection

Smart-card CSPs use the card itself as a key container, rather than storing the keys on local machines. Other third-party CSPs choose their own private key storage approach. Consult the vendor for more information.

Entrust Key Protection will be addressed later in this document.

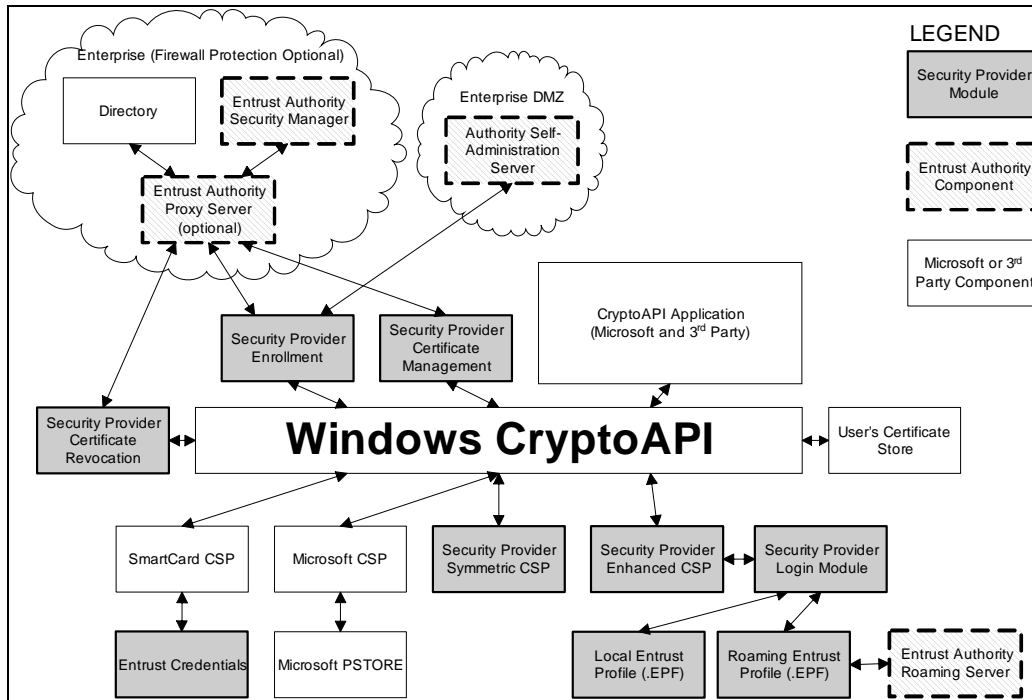
5.5 APPLICATIONS

The final pieces of the CryptoAPI architecture are the applications. The application is responsible for calling CryptoAPI to request public key and symmetric key operations such as data encryption, digital signature or authentication using a certificate and associated key. Each call must be written into the application, or it will not occur. For example, if an application needs to do a digital signature, the digital signature CryptoAPI call must be triggered from the application itself and functionality built into the user interface. The CryptoAPI calls are then passed to the CSP, which does the actual cryptographic operations. Regardless of which CSP is used (and there are usually several CSPs on one computer), the same CryptoAPI calls are used.

Applications can list which certificates are available, and then allow the user to select which certificate to use. Applications can also list the CSPs that are available. In some cases, it selects the CSP automatically for the user. In others, it provides a list of all available CSPs, or a sub-set. In other words, it can control which CSPs the user is allowed to select from, or it can select the CSP automatically.

6. ENTRUST ENTELLIGENCE SECURITY PROVIDER

6.1 SECURITY PROVIDER ARCHITECTURE



6.2 COMPONENTS

In order to deliver managed Entrust digital IDs to the Windows security architecture, Security Provider deploys a number of components. These can be described under two categories:

- 1) Components that allow the user to enroll for a digital ID and manage that digital ID:
 - a. Enrollment
 - b. Certificate Management
- 2) Components that secure the user's digital ID
 - a. Entrust Login
 - b. Entrust Cryptographic Service Providers
 - c. Entrust Private Key Protection

6.2.1 Enrollment

The process by which an enterprise delivers managed Entrust keys and certificates to the end user is called enrollment. Entrust products allow organizations to implement flexible enrollment

models depending on their security policy. Stringent security requirements may ask that users identify themselves in person in order to get their Entrust digital ID, while more flexible security requirements allow users to identify themselves online.

The creation of an Entrust digital ID requires the input of one set of activation codes by the user or administrator. These activation codes can be distributed through various means, and once again, Entrust provides the flexibility that allows organizations to meet the requirements of their security policy. Security Provider delivers this flexibility by allowing administrators to configure the client to either:

- 1) Have the user get activation codes from an administrator and use the imbedded wizard to proceed with the creation of their Entrust digital ID, or
- 2) Point the user directly to a self-serve enrollment page linked to the Entrust Self-administration Server from which a user can enroll for their Entrust digital ID without the assistance of an administrator or help desk.

The operation is quick and simple; allowing organizations to rapidly deploy managed Entrust digital IDs to take advantage of native security features that are present on the users' desktop. The wizard and self-serve Web capabilities are also available for users to self-recover their digital ID should any previous event such as digital ID file corruption, compromise or forgotten password have lead to the revocation of their digital ID.

6.2.2 Certificate Management

The key to enforcing security and administrative policies is to make it easier, simpler, and if possible, transparent and automatic for users to comply with security guidelines. Security Provider automatically and transparently manages the digital ID and performs security checks on behalf of the user. This effective and efficient management reduces the burden of administration for end users and administrators regardless of the application.

Security Provider has the ability to determine if any part of a user's digital ID is about to expire and automatically updates it without requiring user action. This component of Security Provider also enforces revocation, recovery, updates and all other certificate management operations that help organizations effectively deploy desktop security without requiring extensive user interaction or training.

Unlike basic enterprise security products that burden users with difficult tasks such as choosing which key should be used to decrypt data, deciding whether a certificate is valid and trusted, and requesting updated certificates each year, Security Provider users do not need to understand how security works. All key and certificate updates, maintenance of key histories, key backups, revocation checks and name changes happen automatically and transparently to the user. This automation can help to reduce your administrative costs and make security easier to use.

Security Provider delivers value above and beyond key and certificate management by allowing for centrally managed policies and controls, giving users the ability to login once to their Entrust credentials for use with all secure applications, and providing the flexible profile storage means to meet any organizational requirements.

6.2.2.1 Key History

Entrust Authority Security Manager keeps a collection of decryption private keys belonging to a user. Security Manager stores old keys, new keys after recovery, and information about the corresponding encryption public keys.

Should a user lose their keys or forget their digital ID password and needs to have their keys recovered, Security Manager manages this user's collection of decryption private keys, identifying which key is required to decrypt which data.

This key history is transparently available to Security Provider and automatically updated as keys are updated or users recovered. The key history is a critical component of data security because it allows an organization to easily recover data should a user's keys be lost or compromised. Without the key history, the encrypted data could not be decrypted and the information may be lost.

6.2.2.2 Key Updates

When key pairs are updated, they are replaced with new key pairs and new public key certificates are created. Security Provider transparently receives the new certificates in a secure fashion, and users need not understand that a key update has occurred.

There are three reasons for updating key pairs:

- The encryption public key or the signing private key lifetime approaches expiry.
- The encryption key pair or the signing key pair has been or is suspected to have been compromised. That key pair is revoked and the serial number of the corresponding certificate is placed on a certificate revocation list (CRL) by an Administrator.
- The user's distinguished name (DN), which is the user's complete name in the Directory, has been changed (because, for example, the user's name or affiliation has changed); new certificates with the new DN must be issued.

6.2.2.3 Revocation

Security Provider automatically checks a user's own revocation status. If the user's verification certificate has been revoked for any reason, the login attempt will fail and Entrust/Entelligence will tell the user to contact an Administrator. The Administrator must recover the user.

A user may be revoked for the following reasons:

1. On hold - Misplaced smartcard or token (certificate in danger of compromise).
Specifying this reason for revocation **suspends** the certificate. If the user finds the card, you can take the certificate off hold. If the user doesn't find the card, the certificates can be permanently revoked.
2. Key Compromise - The private key corresponding to the verification or encryption public key certificate has been compromised or is suspected to be compromised. The public key

certificate must be revoked to prevent its misuse. When a certificate is revoked for this reason, Entrust allows you to specify the date you believe the certificate was last uncompromised. This date appears in the CRL.

3. **Affiliation Change** - Some information regarding the subject of the key has changed, but there is no suspicion of compromise. For instance, depending on your organization's security policy, users who change distinguished names (DNs) may have their existing certificates revoked, specifying Affiliation Change as the reason, and replaced by new ones with the correct information.
4. **Superseded** - The key pair has been replaced by a new key pair, but there is no suspicion of compromise. Depending on your organization's security policy, the Administrator may wish to revoke non-current key pairs once a key update has occurred.
5. **Cessation of Operation** - The key pair is no longer needed for its original purpose, but there is no suspicion of compromise. For example, you may choose to revoke the public key certificates of any user who leaves your organization.

6.2.2.4 Revocation Verification

A revoked user's certificates are placed in a certificate revocation list (CRL). The CRL identifies certificates that should not be trusted because the CA that issued them no longer considers them valid. When an application encrypts information for a recipient or verifies a signature, it checks an appropriate CRL to confirm that the certificate in question has not been revoked.

6. Security Provider enhances the native application capability to verify a certificate against a combined CRL and provides CRL checking capabilities where the applications cannot. Security Provider accomplishes this by verifying certificate status against partitioned CRLs at unique "distribution points" in the Directory. Each certificate contains a pointer to one or more CRL distribution points where Security Provider can find the CRL. This allows for higher performance, system scalability and more efficient processing.

6.2.2.5 Change DN

If the user's verification certificate has been revoked for the reason Affiliation Change or has not been revoked at all, Security Provider proceeds with the login process. If the Administrator has initiated a Change DN operation, Security Provider will contact Security Manager to update its keys and certificates, which completes the Change DN operation.

Security Provider's ability to complete the Change DN operation on login, even though its verification public key certificate has been revoked for the reason Affiliation Change, greatly simplifies the Change DN operation for Administrators. Administrators can initiate the Change DN operation and then immediately revoke the user's certificates (stating the reason Affiliation Change).

They can also choose to immediately delete the user's old DN from the Directory. In any case, when Security Provider retrieves its new keys, it displays a message that the user's keys have been updated and that the user's DN has changed.

6.2.2.6 Recovery

Security Provider provides the means for easy and automated recovery of a user's keys when any of the following occurs:

- When a user forgets their password. This is the most common occurrence.
- When an Entrust profile is lost or damaged.
- When a user believes that their keys are compromised or that an attacker possesses their password or Entrust profile.
- When a user is set up to not have their key pairs automatically updated and their situation changes, for example, when a contractor's contract is extended and you need to issue new keys for the extension period.
- When a user's signing private key expires (this should rarely or never occur).

6.2.3 Entrust Login

A successfully deployable desktop security solution must take into account how users use and manage the multiple passwords issued to authenticate them to various resources. As the number of passwords managed by a user increases, so is the chance that they will either be using weak passwords, or recording them on paper for easy access. Organizations must strive to implement strong password policies and limit the number of password required in order to maintain the security integrity within their environment.

If an organization chooses to protect a user's private keys under Security Provider key protection, Security Provider only requires the user to login once to their Entrust digital ID in order for the private keys it contains to be available to the secure applications. Users only need one digital ID and one password to send secure e-mail, to encrypt and digitally sign data files, to access secure Web sites and much more.

The Single Login capability is provided by the Security Provider's login module. In addition to Single Login, the login module delivers inactivity timeout capabilities as well as a simple change password wizard.

A user will be required to login to Security Provider whenever an application using CryptoAPI needs to conduct a decryption or digital signature operation and attempts to use a private key protected by Security Provider.

Users will also have the option to manually login because, if an organization has deployed Entrust Authority Roaming Server a manual login is the means for the user to retrieve their digital ID from the server. Once a user has logged in, additional attempts to use their private keys will not require a login until a timeout has occurred.

What happens when an application initiates user login?

- application finds user's certificate in CryptoAPI certificate store;
- certificate indicates that Security Provider's Enhanced CSP holds the private key in a specific key container (if the user is deployed to user Entrust for key protection);
- application attempts to decrypt/sign with a private key;
- the Security Provider Enhanced CSP asks the login module for private key and submits the key container name;
- the Security Provider login module then uses key container name to determine the user's profile name and checks for login;

- if the user is logged in to their Entrust digital ID the key is returned to the Security Provider Enhanced CSP;
- if the user is not logged in to their Entrust digital ID, then they will be prompted for a password;
- after a successful login, the Security Provider login module ensures that the user's entire encryption certificate history is listed in the CryptoAPI certificate store so that old encrypted files may be decrypted.

What happens when the user logs in manually?

- the user initiates login via the Security Provider login interface;
- the user is then prompted for a name and password (with strong password rules enforced through Entrust policy);
- after a successful login, the Security Provider login module ensures that the user's entire encryption certificate history is listed in the CryptoAPI certificate store so that old encrypted files may be decrypted.

6.2.4 Entrust Cryptographic Service Providers

Security Provider Symmetric CSP

The Security Provider Symmetric CSP provides CAST, AES and IDEA symmetric cryptographic algorithms to other Security Provider components. It supports both digital signature and data encryption, and leverages Microsoft or other CSPs, referred as the underlying CSP, for non-CAST cryptographic algorithms and private key storage and protection.

The symmetric cryptographic algorithms are required to open Entrust security stores (.epf file), to communicate with Entrust Authority used during the enrollment process and to decrypt files encrypted with the Entrust format.

Security Provider Enhanced CSP

The Security Provider Enhanced CSP provides enhanced key storage mechanisms for CryptoAPI and is the key link between the application and its use of Entrust private keys. Since it is closely linked to the Entrust login mechanism, it serves as the gatekeeper to the protected Entrust credentials. Combined with the Security Provider login module, the Security Provider Enhanced CSP provides enhanced key storage mechanisms for CryptoAPI. The Enhanced CSP communicates with the Entrust login module over a secured inter-process communication channel to send and receive user's private key information.

Duplication of existing native capabilities is avoided and the Enhanced CSP does not implement any algorithms in addition to those algorithms provided by Microsoft CSP. The Enhanced CSP actually leverages Microsoft CSP for all cryptographic algorithm operations, except where alternate algorithms are required.

6.2.5 Private Key Protection

6.2.5.1 Entrust Private Key Protection

Protection of the Entrust private keys is fundamental to the integrity of any Entrust Solution because the private keys are used to decrypt secure material and to apply digital signatures.

Entrust ensures private key integrity by protecting the keys with strong encryption based on secure algorithms (CAST 128).

Since password protection is as the heart of key protection, Security Provider allows organizations to mandate the use of strong passwords. The longer and more complex the password, the more difficult it is to guess or crack. As such, Entrust Authority security policy can be applied to enforce complex password rules such as the use of combined alphanumeric and special characters and password length.

A user opening or attempting to access an Entrust digital ID whose keys are protected inside an Entrust security store is verified by validating the user's password with information maintained in the digital ID itself. The password is used to derive the key that protects the private keys. The private keys are then encrypted using the key derived from the password.

As part of the validation process other contents of the Entrust digital ID are also verified for integrity. Security Provider uses the content of several sections of the user's digital ID to formulate verification codes that are used to check against the tampering of any information stored in the profile.

6.2.5.2 Entrust Roaming Private Key Protection

The Entrust security store described in the section above can also be stored on the Entrust Authority Roaming Server, allowing mobile or traveling users to access their Entrust digital ID from anywhere or any supported desktop that is connected to the internet. This allows users to take advantage of their single Entrust digital ID on multiple desktops, from multiple locations.

6.2.5.3 Smart Card Private Key Protection

Security Provider is designed to optionally deliver and manage an Entrust digital ID stored on a smart card rather than on the desktop or the Roaming Server. It is important to note that smart card middleware takes over login functionality as it protects the private keys stored on the card. As such, password and inactivity timeout policy fall under the responsibility of the smart card software.

6.2.5.4 Microsoft Private Key Protection

Security Provider is also designed to optionally deliver and manage and Entrust digital ID stored under Microsoft private key protection rather than that of Security Provider. Microsoft offers different levels of protection for the keys.

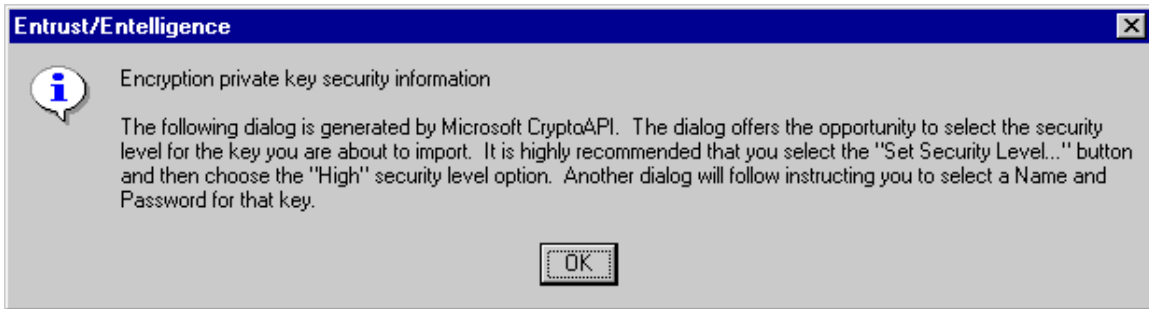
Security Provider gives an Entrust administrator some control over the level of protection applied to private keys stored under Microsoft key protection. These controls are applied via Entrust policy and give administrators the ability to:

1. Turn password protection off: Users do not have to enter a password each time they use the private key. However, they are still protected by the Windows login. This corresponds to Microsoft's *Low* protection.
2. Turn protection on: Users are presented with a choice of either *Medium* or *High* protection for private keys. If *Medium* protection is selected, users will be notified when the private key is about to be used and will have to give their permission for the operation. However, there is no password for the private key. If users select *High*

protection, they must assign a password to each private key and enter it every time that private key is used in an application. Each time the keys are updated, users must assign a password to the new private key. Once set, these passwords cannot be changed.

If an Entrust administrator sets the policy to turn password key protection on, security is enhanced but users will have to make decisions:

- Users must decide between *Medium* and *High* each time their keys are updated, which may be confusing. For example, whenever an encryption key pair is updated, Entelligence will issue the following message, followed by several Microsoft dialogs:



- If users choose *High*, they will have to enter a password for every cryptographic operation in which their private key is required. These passwords may be different for each private key including all keys in the user's key history. There is no way to enforce strong password on these keys via policy.



6.3 SECURITY PROVIDER DEPLOYMENT

6.3.1 Microsoft “Designed for Windows XP” Certification

Security Provider benefits from the *Designed for Windows XP* logo certification. By meeting the specifications required to achieve certification, Security Provider is designed to assure the end user of a consistently good experience. More specifically, Security Provider:

- will not interfere with other applications being used.
- will install and uninstall smoothly, without unnecessary reboots.
- will not cause the user's computer to crash.
- will not overwrite files that are needed by the operating system.

By conforming to the certifications requirements, Entrust provides assurance to users that Security Provider will run correctly, and assures a good experience on Windows XP.

6.3.2 Deployment Size

Leveraging native application encryption and digital signature capabilities and focusing on enhanced security management allows Entrust to offer a very small software package to users. The core components of Security Provider are packaged in a deployable installation file of just over 1Mb in size. This small size makes it feasible for organizations to deploy Security Provider over networks of any bandwidth capacity with little impact. Desktop administrators will derive tremendous benefit from Security Provider's small footprint by expanding deployment options over smaller bandwidth networks, including the Internet.

6.3.3 Windows Installer Technology

The Security Provider installation package is built using Microsoft Windows Installer technology. Windows Installer is based on a data-driven model and provides all installation data and instructions in a single, complete package. All information about the installation is kept in a relational database, which allows for consistent and active monitoring of files being deployed and installed.

The Windows Installer data-driven installation model provides several benefits for organizations that will be deploying Security Provider, including:

- Faster and easier application installations;
- Application self-repair; and,
- Powerful installation rollback capabilities that restore the desktop to the condition it was in prior to an unsuccessful installation.

Entrust desktop administrators will benefit from a user interface that is common to all application installation packages built on Windows Installer technology, minimizing the need for vendor specific training.

Security Provider also provides administrators with the means to configure customized installation packages that meet the exact requirements of their organizations. Since Security Provider is modular, only the components required by the organization need to be installed, allowing for the deployment of the smallest footprint required to deliver the necessary functionality to the user's desktop.

Since Windows Installer accepts a Uniform Resource Locator (URL) as a valid source for an installation, and Security Provider delivers a small footprint to the desktop, organizations can take advantage of the Internet for deployment and have users install the software from a Web browser.

6.3.4 Configuration

Entrust user configuration information is defined by two categories: application configuration settings and user security policy. Application configuration settings dictate the application's behavior and includes feature settings and server configuration information.

User security policy defines important security settings and is governed by attributes set in the user's policy certificates. User policies define settings such as password rules, profile locking timeout settings and the ability to enforce the use of smart cards or tokens.

Application Configuration

Security Provider will not use the traditional Entrust technique of storing configuration data in the *entrust.ini* file. While the *entrust.ini* file is simple to edit and easily ported to different systems and platforms, it has some limitations. The biggest limitations are that it can only contain data for one PKI and it is not easily managed remotely.

To overcome these limitations Security Provider will not use an "ini" file and configuration data will be stored in the Windows registry. The data will be stored to allow for multiple PKIs and remote management via common registry tools or Group Policy in an environment where Microsoft Active Directory is deployed.

Application configuration data will be stored in the Windows registry in both the machine and user settings. The machine settings will be used to store global configuration data included with the setup package and the user settings will be used to store per user configuration data generated at runtime.

Security Policy

Security Provider supports configuration data that is specified in Entrust policy certificates, which enforce settings such as password rules and inactivity timeout settings. The policy certificates will be stored in the CryptoAPI certificate store and data is customized by the Entrust Administrator in Entrust Authority on a per role basis.

6.3.5 Firewall Friendliness

Entrust desktop products have typically used TCP/IP as a transport mechanism when communicating with the Certification Authority (Authority Security Manager) for enrollment and certificate management services. These include LDAP Directory lookup and PKIX key enrollment and management services and require numerous ports to be opened in the firewall to accommodate the various protocols used.

In the context of a *standard enterprise* infrastructure that is not open to the Internet the above configuration is sufficient because opening ports in the firewall does not expose the enterprise to increased vulnerability. However there is a growing need to accommodate *extended enterprise* (ie. B2B and B2C) environments, which typically are secured behind corporate firewalls. Existing

Entrust customers have asked Entrust to remove the dependency on open access to CA services running on various ports. These include Directory lookup services and key management services.

The issue comes front and center when a firewall, in front of the CA, blocks a CMP port and a client is no longer able to roll keys over. Though it may seem odd for this to occur in a strict enterprise infrastructure this is the nature of networks in a B2C environment. Security Provider will overcome this limitation by leveraging use of Entrust Authority Security Manager Proxy and using a proxy solution to communicate with the Entrust infrastructure over port 80.

Security Provider will support both standard and extended enterprise environments. In an enterprise environment Security Provider will simply communicate with the Security Manager via TCP/IP as Entrust client products have traditionally done in the past. In an extended enterprise environment Security Provider will provide a “firewall friendly” communication transport by virtue of the server side Security Manager Proxy service.

Standard Enterprise

This environment is consistent with the communication protocol that Entrust client products have used to date. This environment assumes that the client application has direct access to the server using TCP/IP without any special privilege other than the IP address and port of the server.

In a standard enterprise environment the Network Transport component will talk directly to the respective server side component over the port identified to carry the protocol required.

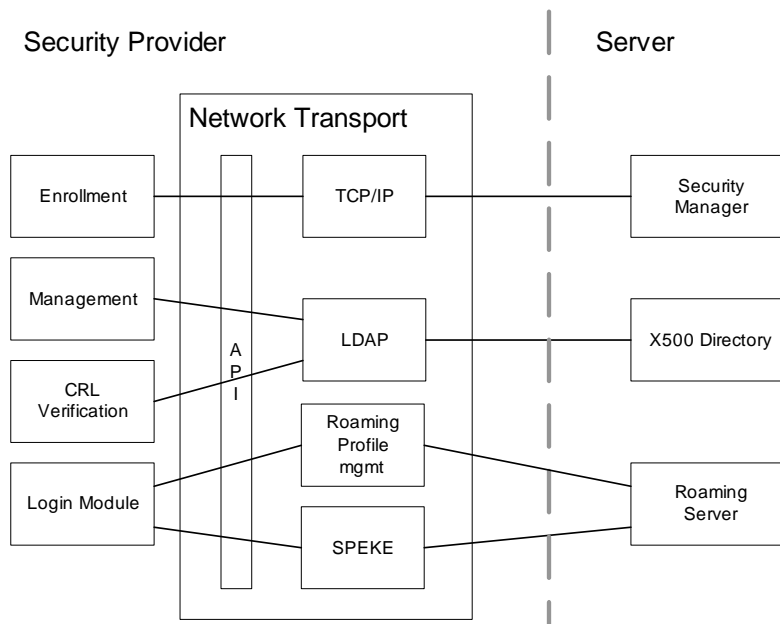
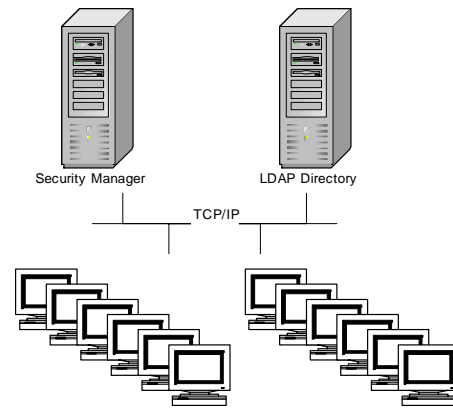


Figure 1: Standard Enterprise Components

Extended Enterprise

An extended enterprise implies that the client does not have privilege to gain direct access to the server. Such an environment will involve communication across one or more firewall protected networks and will likely include communication across the public internet.

Security Provider will leverage the functionality of the Security Manager Proxy Server service to achieve “firewall friendliness”. In this environment Security Provider will wrap it’s communication in an appropriate HTTP format, as defined by the Security Manager, and will communicate over a predetermined HTTP port (typically port 80) to the proxy server residing inside the firewall. This configuration assumes that the firewall maintains this HTTP port open to the external network and/or internet. The proxy server will then in turn relay the embedded message to the appropriate Security Manager device.

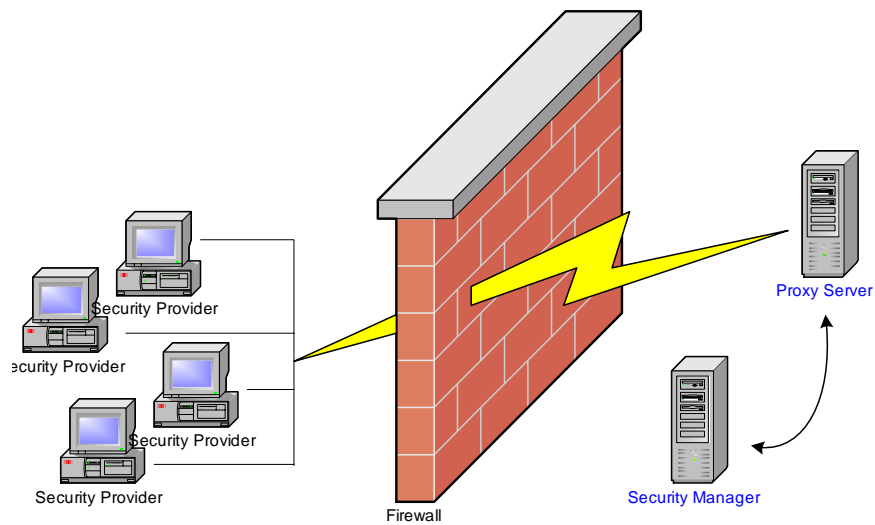


Figure 2: Basic Extended Enterprise configuration

Similar to the Standard Enterprise configuration, Security Provider will communicate with the PKI using the same methods and there are a number of other components that make it all happen. The common interface in this case will represent a flavor of the Network Transport mechanism which will adapt to the requirements of the Security Manager Proxy. For each of the supported protocols there will be a respective Network Transport protocol adapter which will appropriately encapsulate and send its message over HTTP.

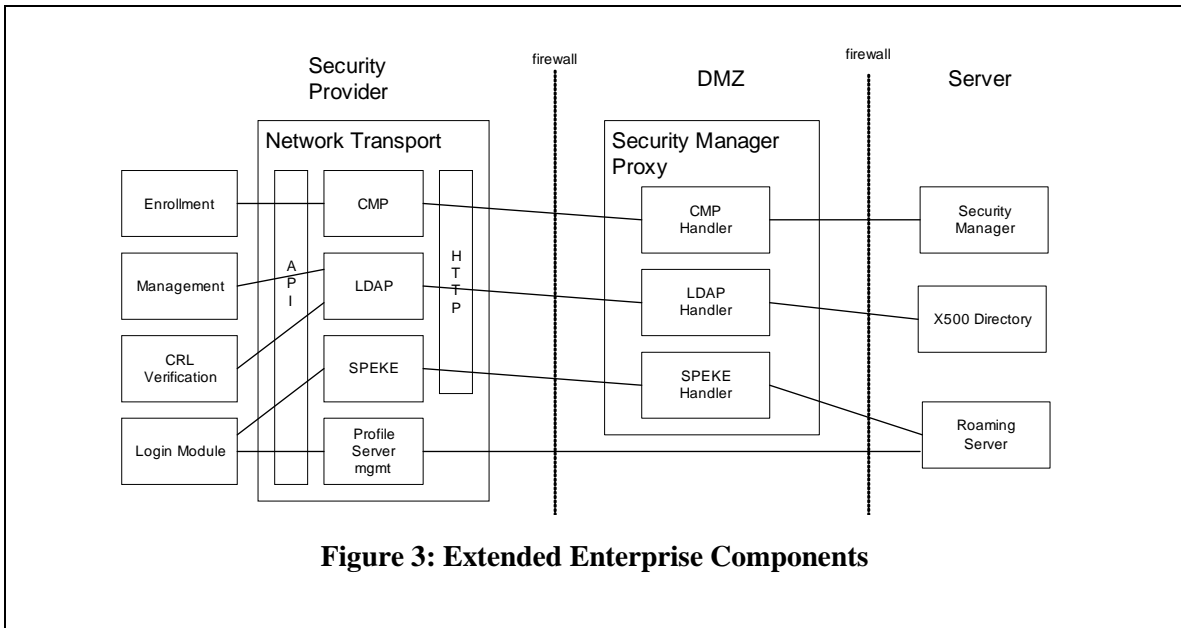


Figure 3: Extended Enterprise Components

7. SUMMARY

Security Provider is thin client enterprise wide desktop security product that enables fast and easy deployment of security at a reduced cost, to mission critical enterprise applications such as email, network access and document creation and collaboration.

Security Provider is easier to manage and use as it automates the entire lifecycle management of the user's digital identity -- from self-serve enrolment to transparent renewal it reduces the administrative involvement and impact on both users and administrators. And, by strongly protecting the user's digital identity and by enforcing centrally controlled security policies, Security Provider helps prevent unauthorized access to sensitive information stored on the network, a desktop or laptop.

Security Provider enables quick and easy deployment of secure desktop applications at a reduced cost. Characterized by a tiny footprint and customizable installation, Security Provider is easier to deploy and can be modified to meet the business and security policies of the organization.

Security Provider is also easier to use as it automates the entire lifecycle management of the user's digital identity -- from self-serve enrolment to automatic updates - limiting administrative involvement and help desk calls, both of which help to drive a lower total cost of ownership.

Security Provider is an extensible investment and can easily scale as the enterprise rolls out more applications and users in fact the same digital identity issued once to a user can be used to secure other enterprise applications with minimal impact on administrators or the end users themselves.

Security Provider can also provide strong protection of the user's digital identity by enforcing centrally controlled security policies, and it helps prevent unauthorized access to sensitive information stored on the network or a user's desktop or laptop, which can have costly implications.

Security Provider is ideal for any organization that requires quicker and easier deployment of desktop security at a reduced cost.

7.1 EASY TO DEPLOY

Security Provider is a thin client that can accommodate flexible deployment processes for any organization. Through email or Web, administrators can quickly deploy Security Provider in large scale with little impact on users or administrators.

Security Provider can provide security management to any number of applications built using the native Windows security capabilities, therefore no integration is required with the applications and deployed quickly with very little impact on administrators and resources.

Security Provider can be fully customized to enable administrators the ability to deploy only those features necessary to meet their business needs and security policies.

Security Provider utilizes the capabilities within the Windows Installer, allowing administrators to easily deploy in a familiar environment and therefore expedite their deployment.

Security Provider is easily scalable. Once a user has an Entrust digital identity, that same digital identity can be extended to any other enterprise application. Organizations can start by deploying

Security Provider for one application (i.e. WLAN) and subsequently add other applications without deploying anything else or impacting end users.

7.2 EASY TO MANAGE

Security Provider delivers simpler and easier registration processes, enabling the administrator to easily roll out users with minimal impact on resources and lowering the overall total cost of ownership. Security Provider's self service registration further reduces impact on administrators as users require less help desk support since they can create their own digital Identities.

Security Provider delivers strongly enforced and flexible security policies enabling the enterprise to meet the requirements set forth in their security policies. These include, strongly enforced password policies and key & certificate lifetimes.

Security Provider allows for flexible storage options for the digital identities or parts of the identities. For example, a portion of the user's digital identity used for authentication to the wireless LAN can be stored on a smart card while the portion of the identity required to protect files and folders can be stored on the user's workstation. This enables a stronger, two-factor authentication to the corporate network while enabling desktop protection of valuable data. These storage options can also be applied to groups, where all senior managers for example would have to log on to their workstation with a smart card.

Security Provider delivers simplified key back up and data recovery processes, which significantly reduces the impact on administrators as they avoid time consuming and cumbersome manual processes.

Security Provider seamlessly and automatically manages digital identities on behalf of the user – from automatic rollovers of the keys in advance of expiry, to transparent updates to the digital identities; Security Provider is easy for administrators to manage and transparent to the end users.

Security Provider enables instantaneous revocation of a user's digital identity to prevent unauthorized access to resources after the digital identity has been revoked or expired.

7.3 EASY TO USE

Security Provider delivers simpler and easier user registration processes, enabling the end user easily enroll for their Entrust digital identity. Security Provider offers self-service registration allowing users to create their own digital Identities at anytime, from anywhere.

Security Provider is completely transparent to the end user. Unlike other enterprise security products that burden users with difficult tasks such as choosing which key should be used to decrypt data, deciding whether a certificate is valid and trusted, and requesting updated certificates each year, Security Provider users do not need to understand how security works. All key and certificate updates, maintenance of key histories, key backups, revocation checks and name changes happen automatically and transparently to the user. This automation helps to reduce your administrative costs and make security easier to use.

End users do not have to learn any new application or processes because Security Provider leverages the existing capabilities of applications they already use on their Windows desktop.

7.4 SECURING DIGITAL IDENTITIES AND INFORMATION

Security Provider delivers the necessary protection of digital identities and information. It protects the organization against the costly ramifications and damage by delivering the strong protection of information and management of identities across users, applications, servers and devices. It delivers protection through:

Securing Digital Identities

Strong Authentication: Security Provider enables the strong authentication of users and devices accessing the corporate network, applications or the desktop. Security Provider allows the organization to restrict access to information, therefore reducing the chances of sensitive information being used inappropriately.

Strong Protection of Digital Identity: Security Provider provides strong protection of the digital identity with flexible and secure storage options. The digital identity can be stored on the users workstation with strong policy enforced password protection, or with the use of smart cards, enabling end users to have a secure log-on to the workstation leveraging a 2nd factor of authentication.

Securing Information

Secure Transactions: Security Provider delivers trusted and secure transactions. By maintaining the integrity of data while in transit or stored within files and folders, Security Provider enables tamper proof information to be exchanged and stored securely, therefore eliminating the possibility of unauthorized viewing of sensitive corporate information to be re-used inappropriately.

Protected files and folders stored locally: Security Provider delivers privacy and protection of confidential information, preventing unauthorized viewing of files and folders stored on a users workstation or laptop, therefore eliminating the possibility of sensitive corporate information to be re-used inappropriately.