

Entrust TruePass™ Product Portfolio

Strong Authentication, Digital Signatures and end-to-end encryption for the Web Portal.

Technical Overview

This white paper describes the Entrust TruePass™ architecture, including a description of the product's primary components, services and capabilities. This technical overview also describes the Entrust Authority™ components required as part of an overall strong Web portal security solution.

Date: July, 2003

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All Entrust product names are trademarks of Entrust, Inc. or Entrust Limited. 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, CONDITIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, CONDITIONS AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A SPECIFIC PURPOSE.

Table of Contents

1	Introduction.....	1
2	Core Functionality	2
2.1	Strongly Authenticates Entrust TruePass Users.....	2
2.2	Enables Standards-Based Digital Signatures for Accountability of Transactions.....	2
2.3	End-to-End Encryption Protects User Data Beyond the Web Server.....	2
2.4	Secure File Upload with Encryption and Signing capability	3
2.5	Transparent Delivery of Entrust TruePass Client Applet.....	3
2.6	RFC 3039 support for High Assurance Applications	3
2.7	Choice of Secure Storage Location for Entrust Digital IDs	3
2.8	Ability to Customize and Strengthen Roaming Authentication	3
2.9	Seamless Download of Entrust Digital ID to Roaming Users.....	4
2.10	Leverages Desktop Storage of an Entrust Digital ID.....	4
2.11	Integrates with Microsoft Windows Security Framework	4
2.12	Allows Use of 3 rd Party Digital IDs	4
2.13	Delivers The Ability To Use Smart Cards	4
2.14	Automatic Enrollment of Users for Digital IDs.....	5
2.15	Automatic Password Reset For Users.....	5
2.16	Strong Protection of User's Private Keys.....	5
2.17	Protects Web Site URLs	5
2.18	Issues Session Cookies to Maintain a Persistent Session For Users.....	6
2.19	Logs System & User Activities	6
2.20	Provides Full Mobility to Users	7
2.21	Enhanced Security Management, Including Automatic Renewal Of Users	7
2.22	Built for Large Scale Deployments That Demand High Availability and Performance	7
2.23	Deploy In-house or as a Managed Service	7
3	Product Terminology and System Concepts.....	8
3.1	Entrust Digital ID	8
3.2	Browser Cookies.....	9
3.3	Single Sign-on Across Single and Multiple Domains	10

4	Entrust TruePass General Description	11
4.1	Entrust TruePass Architecture	11
4.1.1	Entrust TruePass Java Applet.....	11
4.1.2	Entrust TruePass Server Components	12
4.2	Entrust Authority™ Components.....	12
4.2.1	Entrust Authority™ Security Manager.....	12
4.2.2	Entrust Authority™ Self-Administration Server	12
4.2.3	Entrust Authority™ Roaming Server	12
4.2.4	X.500, LDAP, or Active Directory	12
4.3	Entrust TruePass Services	13
4.3.1	Automatic User Enrollment Service	13
4.3.2	Authentication, Retrieval & Secure Session Services.....	14
4.3.3	Resource Protection Service.....	17
4.3.4	Digital Signature Service.....	17
4.3.5	Persistent Encryption Service	18
4.3.6	Security Management Service	18
4.3.7	Web Access Control Integration (Optional).....	19
5	Operational Model	20
5.1	User Deployment Scenarios	20
5.2	System Performance & Reliability.....	21
5.3	High availability	21
5.4	Performance	22
5.5	Scalability	22
5.6	Fluctuating client requests without performance impact.....	22
5.7	Adding hardware or software easily	22
5.8	Maintainability	22
6	Conclusion	23
7	About Entrust, Inc.	24

1 Introduction

As organizations move higher-value transactions and highly-sensitive information onto a Web portal, security becomes critical to supporting business processes online. A secure Web portal must include the following key services:

- Enable customers to identify participants in a transaction
- Create evidence to help in binding each party to a transaction with an audit record
- Protect information while in transit and storage throughout the life of a transaction
- Security management that automates administration and management of users and policy across applications and platforms

Entrust TruePass™ provides these strong security capabilities to Web-based applications. These capabilities provide strong authentication, Digital Signatures, and End-to-end encryption for bringing critical business functions to a Web Portal. As Entrust TruePass does not require client software to be installed or configured on a user's computer, organizations are able to deliver a unique combination of application enablement through enhanced security features with unmatched user transparency and ease of deployment. In combination with products from the Entrust Authority™ product portfolio, organizations are provided with security management features that enable automated user registration and administration, transparent digital ID lifecycle management, and automated revocation checking at logon to confirm that only valid users are allowed to access secured resources.

This white paper provides a high level description of the Entrust TruePass product architecture. It focuses on the powerful capabilities delivered through both the client and server portions of the product. The Entrust TruePass client component is a small Java™ applet (~ 150 kb) that is transparently downloaded to a user's browser. In combination with its server components, the Entrust TruePass solution provides robust and scalable enhanced security services, including authentication of users, digital signatures for accountability of transactions, privacy through persistent encryption and transparent digital ID lifecycle management.

Entrust TruePass is a uniquely flexible product in that it can deliver enhanced security services to many different environments—including the enterprise, business to business, business to consumer, and government to citizen. It allows organizations to deliver digital IDs to be used in conjunction with Web applications for operations including strong authentication, digital signatures, and encryption of data for backend systems. It also allows for multiple methods of strong authentication, which allows organizations to provide varying levels of authentication by balancing security with the cost and complexity of deployment.

Entrust also provides automated security management of digital IDs, user self-enrollment, and the ability to automate password resets. This can significantly reduce the ongoing administration and management costs associated with most other Web security solutions.

The privacy and security features of Entrust TruePass are transparent to Web site visitors. Client software installation is not required, users do not have to manage their digital IDs, and users can access secure Web-based services from any computer, anywhere, anytime.

Entrust TruePass is also the first Java-based application to achieve FIPS 140-1 Level 1 validation. This external validation of the enhanced security capabilities provided by Entrust TruePass makes it an ideal solution for government and businesses that are serious about moving their sensitive and valuable processes online.

2 Core Functionality

Entrust TruePass is an enhanced Web security solution that leverages the advanced public-key infrastructure (PKI) capabilities provided by the Entrust Authority™ Security Manager. It enables the protection of Web site resources and applications, securely authenticating end-users, and adding accountability and privacy to online transactions. The product provides the following enhanced security services:

2.1 Strongly Authenticates Entrust TruePass Users

Entrust TruePass users are only able to access their digital IDs after they have provided identification. Entrust TruePass enforces the use of strong passwords to reduce the chance that users will choose ones that are weak or easy to guess. This reduces the risk of compromising the digital ID. These password rules are fully customizable through administrative settings on the server side, allowing organizations to balance the strength of the password against the environments and users they support. For smart card users, the user's digital ID is protected by the PIN on the card and also enforced by the smart card software. For users with their digital IDs in the Microsoft Windows digital ID store, standard methods for protecting users' Windows sessions are used (such as a secure screen saver with an appropriate time-out value) to protect the users' identities. This is in addition to the strong encryption of a user's digital ID by the operating system, allowing access to that digital ID only within a valid Windows session.

2.2 Enables Standards-Based Digital Signatures for Accountability of Transactions

Entrust TruePass delivers standards-based digital signature capabilities for end users providing accountability of transactions in an online environment. Although the end result is always a standard digital signature object (PKCS#7), Entrust TruePass allows for two different ways of deploying the product, giving organizations the opportunity to use digital signatures in the mode that better fits their business needs. The first configuration allows for an identified user to simply sign data (for example, a completed online form) and submit it to the Web server. This uses the built-in signing capability of the Entrust TruePass applet. The second type presents a summary of the submitted data back to the user for review and then provides the opportunity to confirm and sign the transaction with the Entrust TruePass applet. This means that the user is actually signing the entire document or "Signing What They See". As a part of this process, Entrust TruePass on the server side will also countersign the transaction before passing it to backend applications for processing or storage. This countersignature makes it possible to verify that the same data that was sent to the user for signature was in fact what was signed. Additionally, the server signature includes a time field, allowing organizations to incorporate a time element into their process for digital accountability of user transactions.

2.3 End-to-End Encryption Protects User Data Beyond the Web Server

Entrust TruePass transparently supports the encryption and decryption of data between users and specific back-end systems. Unlike using an SSL session for Internet security, Entrust TruePass can protect data in both directions using strong 168-bit 3DES

encryption. Entrust TruePass can protect the data beyond the 128-bit SSL session established between the user and the Web server, Entrust TruePass protects the data all the way to the specified back-end system. As part of the data encryption process from the end user to the back-end system, Entrust TruePass can be configured to automatically retrieve the target system's certificate, and validate it (perform a certificate revocation list (CRL)—check to confirm the user has not been revoked). From an end-user perspective, this strong protection of the data that they are submitting and receiving is completely transparent and as simple as an SSL connection. As Entrust TruePass encrypts and decrypts the data in a standard PKCS#7 format, any authorized user with a cryptographic product that supports the widely used standard can be used to encrypt and decrypt the data at the back-end. This is important from both an application point of view (you are not required to build a custom capability to decrypt the data), and from a risk management point of view (as it is a standard format, you will be able to still access the data years from now through a standards-based application).

2.4 Secure File Upload with Encryption and Signing capability

Entrust TruePass provides the ability for end users to digitally sign and/or encrypt files for a specific backend system. Entrust TruePass can protect data using strong 168-bit 3DES encryption, the format of the digitally signed and encrypted data will be S/MIME. Entrust TruePass also provides the ability to decrypt files encrypted by the backend system and to store the file on their file system or network drive.

2.5 Transparent Delivery of Entrust TruePass Client Applet

Entrust TruePass is uniquely capable of delivering authentication, digital signatures, and end-to-end encryption to end users without requiring them to install or configure additional security software. Depending on the deployment model implemented, a small Java applet (~ 150 kb in size for roaming users) is transparently downloaded to the end user's browser as they access secured resources. This applet provides the ability to authenticate a user through a secured session, enables digital signatures and persistent encryption/decryption operations and supports transparent ID lifecycle management.

2.6 RFC 3039 support for High Assurance Applications

Entrust TruePass supports RFC 3039 (3 key pairs) for customer environments that require a higher assurance level by supporting separate key pairs for encryption, authentication, and digital signature operations.

2.7 Choice of Secure Storage Location for Entrust Digital IDs

Entrust TruePass provides users with the ability to enroll for, store, and access digital IDs in several different secure locations. Digital IDs can be stored in:

- Roaming Entrust Profile
- Desktop Entrust Profile
- Microsoft Windows digital ID store
- Smart card or token through the Windows security framework

These different locations allow organizations to deploy and support end users in a model that suits them. Please refer to the "[System Concepts](#)" section for more details on these different methods for storing and accessing digital IDs.

2.8 Ability to Customize and Strengthen Roaming Authentication

In addition to the strong authentication process previously described for Entrust TruePass roaming users, companies have full flexibility in requiring additional factors of authentication, including options like outside data sources, random number tokens,

Secure Message Solutions (SMS), and many more alternative methods for adding strength to the authentication process. Entrust also provides an optional capability, the Entrust PIN server, that allows companies to provide a higher level of security for user authentication. The [Entrust Mobile ID Server](#) allows users to leverage their existing mobile phone number as means of second factor authentication. At the time of authentication, the user needs to be at the mobile phone to receive a one-time passcode to access the protected resource. This out-of-band delivery of the one-time passcode adds significant strength to the already strong authentication processes provided by Entrust TruePass.

2.9 Seamless Download of Entrust Digital ID to Roaming Users

Today, when using most digital identities in a Web environment, the identity must be embedded in the browser key store, or stored in some third-party storage container with the aid of an installed piece of software. Through the Entrust TruePass applet, roaming users are able to seamlessly and securely access their credentials through a Web browser. Enabled by the Entrust Authority™ Roaming Server, Entrust TruePass downloads secured user credentials from a standard X.500 or LDAP directory. Users can then use their digital IDs to identify themselves and conduct transactions such as signing electronic forms on a Web portal. These credentials are never written to the local hard disk and are securely removed from the browser memory at the end of the user session. This capability makes Entrust TruePass a strong technical solution for environments such as a kiosk, where there may be many users operating on the same machine.

2.10 Leverages Desktop Storage of an Entrust Digital ID

Entrust TruePass allows organizations to leverage the same digital ID as used by the deployment of other Entrust and Entrust Ready applications to the desktop. This enables customers to deploy and use the powerful capabilities provided by the Entrust Entelligence product portfolio, and also leverage the same digital ID with Entrust TruePass for secure Web needs.

2.11 Integrates with Microsoft Windows Security Framework

Entrust TruePass can be configured to store and use digital IDs kept in the Microsoft Windows digital ID store. This is made possible through direct integration with the Microsoft Windows security framework, which by extension also allows the use of the digital ID with other security-aware applications. Entrust TruePass supports the built-in authentication capabilities of the Internet Explorer browser.

2.12 Allows Use of 3rd Party Digital IDs

The integration between Entrust TruePass and the Microsoft Windows security framework allows Entrust TruePass to not only work with Entrust digital IDs, but also with third-party digital IDs that are stored in the Microsoft Windows digital ID store. This powerful feature allows organizations to deploy Entrust TruePass capabilities to a broad range of users, including those that are using existing third-party digital IDs. This can reduce deployment and administration costs in mixed environments where there are multiple digital ID sources.

2.13 Delivers The Ability To Use Smart Cards

Although Entrust TruePass is a [“zero-footprint”](#) Web application, it has the ability to access and use digital IDs that are stored on smart cards. This enhanced level of security provides an additional level of authentication for users, allowing organizations to meet more stringent corporate security policies while translating sensitive business processes to a Web environment. This also includes the ability to use random number tokens with

Entrust TruePass as an alternative method of providing strong authentication. Smart cards are costly to implement; therefore, Entrust TruePass provides the flexibility to deploy different levels of strong authentication to different groups of users depending on the sensitivity of the transactions.

2.14 Automatic Enrollment of Users for Digital IDs

The ability to automatically enroll users for digital IDs is considered a mandatory requirement for any sort of large-scale deployment—this applies not only to a business-to-consumer environment, but also to enterprise, business-to-business and government-to-citizen deployments. Entrust TruePass can be customized to ask a series of questions that will allow the organization to uniquely identify users (an example could be name + mother's maiden name + last paycheck amount); this is fully configurable and can include information that is held by the company and/or by third-party sources (such as Equifax). The level of depth required for users to enroll is at the discretion of the organization and may be distinct for different levels of users. The user is able to register for a digital ID and immediately have that identity available for use—all without administrator involvement.

2.15 Automatic Password Reset For Users

Every organization is forced to deal users forgetting their passwords. Entrust TruePass empowers users to reset their own passwords, removing the burden from the technical support organization. Through the Entrust Authority™ Self-Administration Server application, organizations can set up Web pages where users are able to reset their forgotten passwords. This will typically require the user to provide the same type of information that was submitted at enrollment time (see point above), but this again is something that is fully customizable by the deploying organization. The implications of this capability are quite significant. The technical resources of an organization can now be focused on more pressing matters, rather than resetting passwords.

2.16 Strong Protection of User's Private Keys

All Entrust Digital IDs stored in an Entrust Profile are protected with 128-bit symmetric encryption. In addition to this high level of protection, when the user's credentials are stored in a standard X.500 or LDAP directory, they are also encrypted again (now encrypted twice!) with another layer of 128-bit encryption. Every Entrust TruePass session is protected with 128-bit SSL, adding another layer of security when transmitting users' digital IDs over the Internet. Due to the secure way in which these credentials are then accessed by the Entrust TruePass applet, digital IDs are protected and users can feel confident conducting transactions online. When using Entrust TruePass with a smart card, the user's private keys are protected by the PIN that is enforced by the smart card software.

2.17 Protects Web Site URLs

Entrust TruePass is able to protect Web site URLs through the definition of those URLs as secured or protected. In order to access any URL that has been defined as protected, a user must be identified by the Entrust TruePass Session Validation Module (SVM) as a valid user (both identified and still within the defined level of activity as configured by the company). If a user is not valid for any reason, he or she is prompted to identify him or herself; once identified, only then will he or she be allowed to continue into protected resources. Companies can protect an entire Web site, specified portions of that Web site, or multiple Web sites that are part of other Web domains.

An enhanced level of security can also be added through the deployment of the Entrust GetAccess™ product portfolio, which provides powerful entitlements capabilities in addition to the strong identification, verification, and privacy capabilities of the Entrust TruePass solution. Please refer to the Web Access Control section later in this paper for more information.

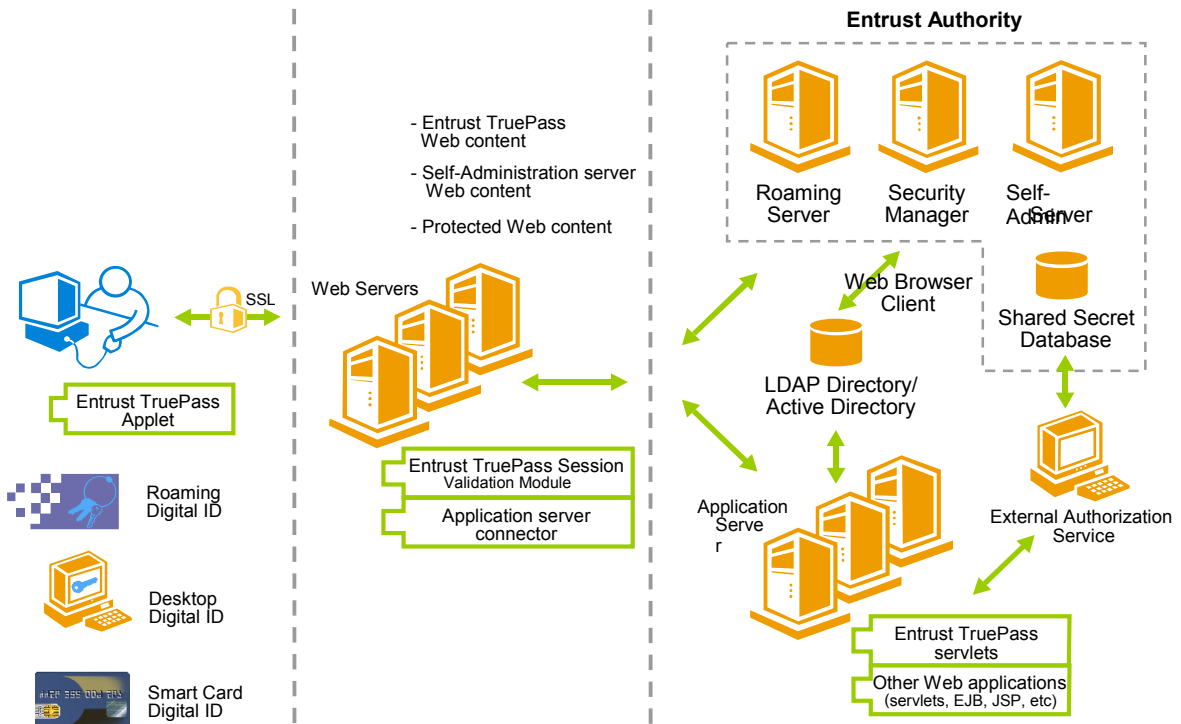


Figure 1: Entrust TruePass System Architecture

2.18 Issues Session Cookies to Maintain a Persistent Session For Users

When users successfully authenticate themselves to Entrust TruePass, the Entrust TruePass Session Validation Module (SVM) then places signed session cookies in the users' browsers. These session cookies act as an entry pass, allowing users to continue to access protected resources without having to re-enter their password each time. The time-out or validity period for these session cookies is configured on the Entrust TruePass SVM and can be anywhere from 5 to 120 minutes in length. The cookies themselves are secure SSL session cookies, are cryptographically signed, and are never written to the local system. Please refer to Section II under the [Browser Cookies](#) section for more information.

If your systems are configured to allow for multiple Entrust TruePass installations within the same domain or across other domains the user will be able to access protected resources throughout their session, without being asked to re-authenticate.

2.19 Logs System & User Activities

Entrust TruePass records system activities in a log file that allows for auditing at a later time. The activities that are logged range from enrollment processes, to authentication and other transactions by the user when they are logged into the system. Additionally,

the system captures server-side activity that allows for troubleshooting in the event that an administrator needs to see both sides of a transaction.

2.20 Provides Full Mobility to Users

Users are able to log into a Web resource from any Java-enabled browser, allowing them to work from multiple locations with ease. For roaming users, their digital ID is transparently downloaded to the machines that are being used to access the Web resource and are available for the duration of their working sessions. Upon completion of a session, the user's digital ID is securely removed and automatically available for use from that or any other location. For smart card users, Entrust TruePass can be configured to allow users to roam from machine to machine without requiring any client-side Entrust software.

2.21 Enhanced Security Management, Including Automatic Renewal Of Users

Entrust provides automatic and transparent management of digital IDs. When digital IDs expire, they can be automatically renewed, with the new identity instantly available and ready for use. Entrust TruePass monitors the digital ID at each login to confirm that the user is a valid user (CRL check), as well as to see if the digital ID needs to be renewed. If a renewal needs to occur, Entrust TruePass will automatically communicate with both the appropriate Entrust Authority components to transparently renew the user's digital ID. This can significantly reduce the ongoing administration and management costs that are often apparent with most other Web security solutions.

2.22 Built for Large Scale Deployments That Demand High Availability and Performance

Entrust TruePass has been designed to operate in high-volume portal environments. The product has been specifically designed to leverage built-in scalability, high-availability, and fail-over features of the market-leading application servers. From J2EE deployment methods to specific features that have been built into Entrust TruePass to take advantage of the powerful capabilities of application servers like BEA WebLogic and IBM WebSphere, Entrust TruePass is capable of scaling to provide enhanced security for Web portals that conduct high-value transactions and contain highly sensitive information.

2.23 Deploy In-house or as a Managed Service

Entrust TruePass can be deployed in-house or as a managed service. Its standards-based implementation uses only standard ports for all client traffic (HTTPS Port 443) to support for standard LDAP and X.500 directories that makes it possible to support both in-house and managed service environments, allowing organizations to choose how they want to deploy and manage each specific business application.

For a managed service deployment, beTRUSTed is the integrator of choice for Entrust TruePass customers. beTRUSTed is an e-commerce security integrator and offers high levels of security available for e-commerce and information transfer within a networked environment.

3 Product Terminology and System Concepts

This section examines some of the key system concepts used within the Entrust TruePass architecture.

3.1 Entrust Digital ID

A digital ID is a set of cryptographic credentials for a particular user. The user's "credentials" are comprised of the user's public encryption and verification certificates, private keys, password, and Distinguished Name (DN) information. A digital ID is used to verify one's identity, much like a driver's license or passport. An Entrust Digital ID provides elements to identify users and conduct business in the online world. Entrust Digital IDs are provided through the Entrust Authority Security Manager, and may be stored in several ways for use with Entrust TruePass. These include:

- Roaming Entrust Profile (EPF)
- Desktop Entrust Profile (EPF)
- Microsoft Windows digital ID store
- Smart card or token through the Windows security framework

With Entrust TruePass, all of these options for generating and storing a digital ID include the ability to generate all private digital ID material locally (as opposed to on a central server, which is also an option). This may be an important element of digital accountability for some organizations and the Entrust TruePass system delivers this across its range of digital IDs.

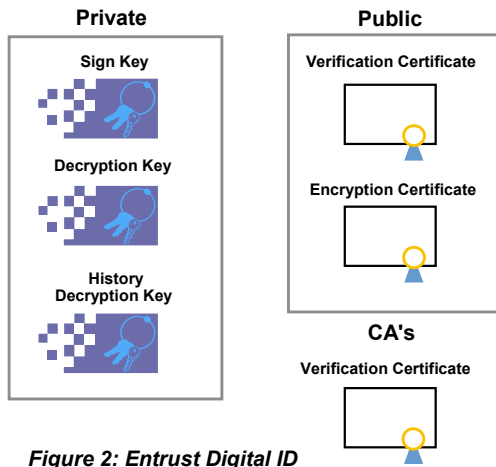


Figure 2: Entrust Digital ID

An Entrust Roaming Profile is a highly secure method of storing and retrieving a user's digital ID from an X.500 or LDAP directory. The Entrust TruePass applet allows the digital ID to be accessed and used during a standard Web browser session, enabling seamless use across both Windows and Macintosh platforms. An Entrust Roaming digital ID is a standard Entrust Digital ID based on the two key pair model, containing both key pairs and the corresponding certificates for the user.

With flexible methods for integrating Entrust TruePass security into any Web application, organizations can add identification, digital signatures, and persistent encryption to applications without having to be concerned about the platform or browser the user is on. Entrust Roaming Digital IDs are transient in nature, only available to the

Entrust TruePass Applet and the user for the duration of their session. Once the user shuts down the browser or logs out of their session, the Roaming digital ID is removed from the browser memory—at no time is it written to the hard disk.

Entrust Digital IDs also contain the decryption key history of the user, allowing it to be used for other secure applications (such as secure e-mail with the Entrust Entelligence™ product portfolio). This common approach to user identity storage allows companies to leverage the digital ID across many different applications, not just Entrust TruePass. All Entrust Roaming and Desktop digital IDs are protected with strong 128-bit CAST

encryption, so that keys and certificates are secured. The process for unlocking a user's digital ID includes the comparison of a cryptographically generated token that is derived from a user's password and a salt value, with a token in the profile. If they match, then the password supplied is correct and the encrypted contents of the profile can be accessed.

Entrust TruePass users may also store their digital IDs in the Microsoft Windows digital ID store. This is achieved through integration with the Windows security framework. Digital IDs stored in the Windows digital ID store are protected through built-in Windows security mechanisms, including the ability to automatically time out and lock a user's workstation with a password-protected screensaver. Through this integration with the Windows security framework, users are also empowered to use the native capabilities of the Internet Explorer browser with the Entrust Digital ID stored in the Windows digital ID store.

As a final option, Entrust TruePass users can store their digital ID on a smart card. This is enabled through the integration with the Microsoft Windows security framework, as discussed above for the Microsoft Windows digital ID store. With an appropriate smart card, reader, and driver, Entrust TruePass can access and use the digital ID that is stored on a smart card. For users that have their digital ID on a smart card, the Entrust TruePass performs all of the strong authentication procedures as with the other digital ID options. Since Entrust TruePass currently does not require the encryption portion of a digital ID, this is not managed for the user; however, the user's private signing key is automatically and transparently managed. This digital ID is strongly protected by the PIN that is set for the card at the time of card issuance.

3.2 Browser Cookies

As a standard part of the Web and the HTTP 1.x standard, browser cookies were created to provide context-oriented applications with the ability to overcome the stateless nature of the Web. Today, cookies are the primary mechanism for maintaining state across multiple interactions between a browser and a Web server. Since Entrust TruePass resides in the browser environment, it is able to leverage cookies to keep track of state information for user sessions. The Entrust TruePass Session Validation Module (SVM) (Web server plug-in) issues session cookies, which means that the cookies are not written to the user's hard disk, but rather exist only in browser memory. The cookies are destroyed when the Web browser is closed or the user logs out from the session. These cookies do not contain any confidential information for that user, but are signed by Entrust TruePass and cryptographically verified each time they are presented to the Entrust TruePass SVM. This is done to maintain the integrity of the data contained in the cookie while protecting the personal information of the user.



Figure 3: Browser Cookies and the Web.

3.3 Single Sign-on Across Single and Multiple Domains

Most large organizations will have one primary domain, but will have several sub-domains as well. They may also have multiple domains that are directly or indirectly associated and need to enable single sign-on across these Web properties. As is defined in the HTTP standard, the cookies that are used by Entrust TruePass are specific to a domain, but can apply throughout sub-domains as well as outside domains. This allows users to log into Entrust TruePass once and have access to protected resources across their Web session, which may include content from various departments, divisions, or partner companies. In this way, users are empowered with single logon to all Web resources protected by Entrust TruePass.

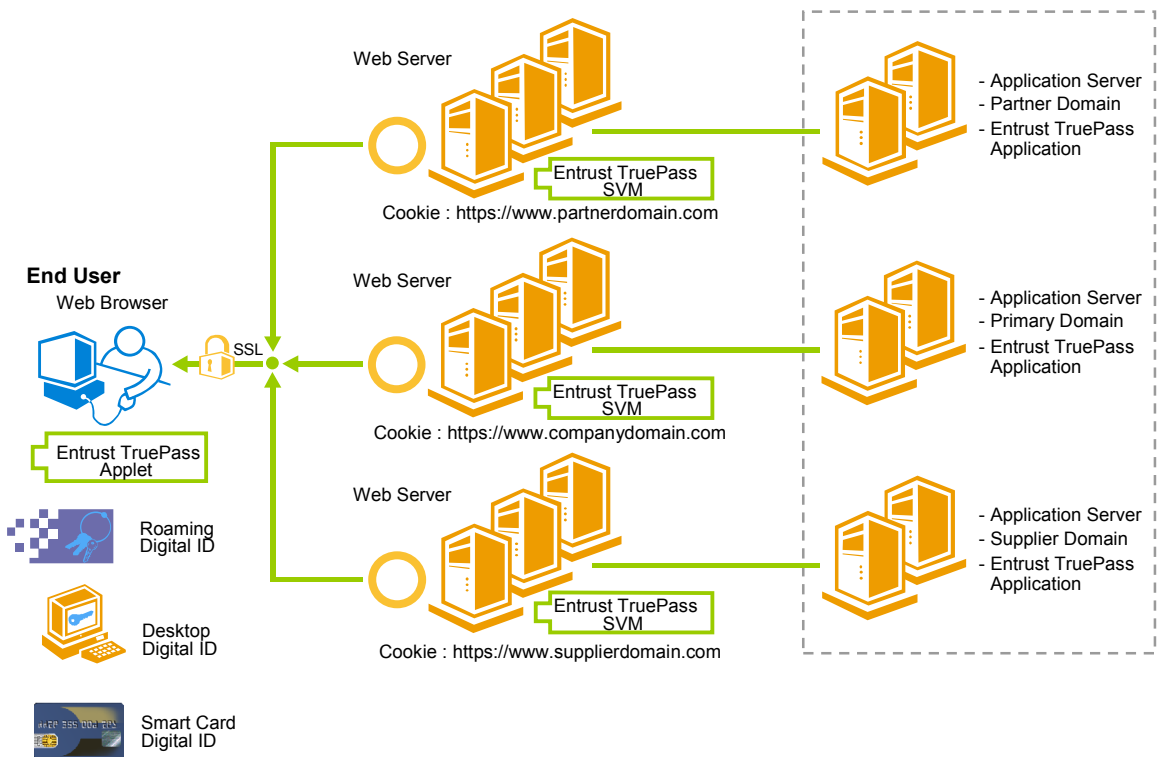


Figure 4: Single sign-on across multiple domains and applications.

4 Entrust TruePass General Description

Entrust TruePass provides key services through both client and server-side capabilities. This section briefly describes the architecture of Entrust TruePass and the services provided by the product portfolio.

4.1 Entrust TruePass Architecture

The Entrust TruePass architecture is a cohesive and powerful set of capabilities that have been put together to provide a secure Web solution. The following section briefly describes each piece and the role that it plays in the Entrust TruePass architecture.

4.1.1 Entrust TruePass Java Applet

All client side capabilities of Entrust TruePass are delivered through a very small Java applet. Referred to as a “zero-footprint client”, the Entrust TruePass applet is typically ~150 kb and is dynamically downloaded to the Web browser when needed. The exception to this is if an organization deploys Entrust TruePass along with the Microsoft Windows digital ID store; in this case the applet, which is now signed, is ~250 kb, but it is only downloaded onto the machine the first time it is used. From that point forward, it is cached locally until a newer version is available. It performs the following services:

- **Secure session management:** The Entrust TruePass applet works in conjunction with the Entrust TruePass SVM to confirm that end users can securely operate in a Web browser. This involves the Entrust TruePass applet signing a challenge that is sent to it by the SVM, which in turn will validate that signature, perform a Certificate Revocation List (CRL) check, and then issue a session cookie to the user. This signed cookie is used to manage the state for the user, including the time-out value assigned by the administrator.
- **Accessing User Identities:** For roaming users, the Entrust TruePass applet securely sends user identity information to the Entrust TruePass Authentication Service on the server side of the deployment. This is done in the form of an irreversible cryptographic hash (SHA1) of the user's name, their password, and an additional value. Through the Entrust Authority™ Roaming Server, the user's digital identity is securely downloaded to the Entrust TruePass applet, where, after a series of checks, it is made available for completing the user's login. For locally-stored Entrust Profiles, Microsoft Windows digital ID store, and smart card storage of digital IDs, the signed Entrust TruePass applet directly uses the available credentials once the correct information has been provided.
- **Digital Signatures:** The Entrust TruePass applet is able to sign data that has been targeted for signature by the user. The resulting object, which is a standard PKCS#7 object, can be used to provide a receipt to users, and can also be stored for later verification.
- **Bi-directional Data Encryption:** The Entrust TruePass applet can encrypt data for a target backend system. Using a valid certificate, Entrust TruePass uses strong 168-bit 3DES encryption to protect data that is being submitted. The resulting standard PKCS#7 object is transmitted securely through the Web server, and on to a back-end system. Backend systems also have the ability to encrypt HTML data for individual Entrust TruePass users. The Entrust TruePass applet will decrypt the data enabling the browser to render the unencrypted data into the HTML form transparently.

4.1.2 Entrust TruePass Server Components

Entrust TruePass server components are installed and distributed on a Web server and an application server. The Entrust TruePass server components offer all Entrust TruePass-related services necessary to perform Entrust TruePass functions. The services that they provide are described below.

- **Session Validation Module:** The Session Validation Module (SVM) controls access to Web applications and content by intercepting URL requests and enforcing authentication policy decisions defined by the company. As the SVM is installed on various supported Web servers, it is configured differently for each. It is a plug-in for Netscape iPlanet™, a filter for Microsoft® IIS, and a module for IBM® HTTP Server. The Session Validation module verifies whether requests for Entrust TruePass-protected pages are from previously authenticated users.
- **Entrust TruePass Servlets:** The security services provided by Entrust TruePass are provided through Java servlets installed on a supported J2EE Web application server. These servlets perform tasks including authentication verification & retrieval, server signing of data, and CRL checking of encryption certificates. There are many benefits that are gained by deploying Entrust TruePass on a Web application server, including leveraging the built-in load balancing, fail-over and high-availability features by default.

4.2 Entrust Authority™ Components

The Entrust Authority product portfolio delivers key capabilities required for enhanced security. The managed security services and components provided by the Entrust Authority product portfolio are described in the next section.

4.2.1 Entrust Authority™ Security Manager

Entrust Authority Security Manager securely stores the CA private key, issues certificates for users and devices, and publishes user and application certificate revocation lists to allow trustworthy communications. The Security Manager also maintains a database of users' private key histories for recovery purposes in the event a user loses access to their keys. Full event logging and reporting are securely maintained for audit records.

4.2.2 Entrust Authority™ Self-Administration Server

This component is essential for hassle-free enrollment, deployment, and recovery of digital IDs by providing users with Web-based self-registration and recovery. You can customize the Self-Administration Server to reflect corporate branding on your Web pages and to query users for whatever identity verification data is dictated by your security policy.

4.2.3 Entrust Authority™ Roaming Server

The Roaming Server is responsible for securely storing and accessing users' digital IDs in a standard X.500 or LDAP directory. It allows users to log in and work securely from any location without having to carry their digital IDs on tokens, smart cards or other physical storage devices. Trusted users are able to access information, anywhere and anytime. It also provides the flexibility to tailor security roles to match the needs of corporations and end users.

4.2.4 X.500, LDAP, or Active Directory

An X.500 or LDAP directory is used for several different purposes in an Entrust TruePass solution. It is the location where the Roaming Server places the double-encrypted user profiles, allowing users to log on from any location, confident that their digital IDs are stored securely. The directory is also used to store Certificate Revocation Lists (CRLs)

that are published by the Entrust Authority™ Security Manager. These CRLs are used to determine whether a user has been revoked at logon time, as well as to confirm that a targeted backend system is still valid for encryption of data. Entrust works with many industry-leading directory vendors, including Microsoft Active Directory, Siemens, Novell, and LiveContent.

4.3 Entrust TruePass Services

The capabilities that are provided by an application are typically called services. The services delivered by Entrust TruePass are detailed in the following section.

4.3.1 Automatic User Enrollment Service

Through the Entrust Authority™ Self-Administration Server (and optionally the Entrust Authority™ Roaming Server), organizations are able to deploy and support an automatic enrollment service for users. This means that based on an organization's security policy, users will be able to:

- enter information that will verify (to an appropriate level for the deploying organization) who they are,
- choose what their user name and password will be (the password will have minimum security levels set and controlled by Entrust TruePass), and
- have a digital ID created (based on who they are) that will be made available to them automatically at the completion of the enrollment process.

This is all achieved through the use of a Web site that is designed and controlled by the issuing organization.

During an enrollment process, the Self-Administration Server automatically provides the following:

- Verifies that an applicant is authorized to enroll for a digital ID
- Creates the user within Entrust Authority™ Security Manager and the Directory
- Generates the user's digital ID
- Stores the digital ID in the chosen appropriate digital ID store:
 - Entrust Roaming Profile: The digital ID is protected (encrypted) with a password supplied by the user. It is then stored, further encrypted using CAST-128 and a randomly generated symmetric key, at the user's entry in the directory
 - Entrust Desktop Profile: The digital ID is protected (encrypted) with a password supplied by the user. It is then stored locally on the user's hard drive.
 - Microsoft® Windows security framework user: The digital ID is stored in the Windows digital ID store, which is protected by the built-in security mechanisms of the Windows operating system.
 - Smart Card: The digital ID is stored on the card and protected with the PIN that is associated with the card.

The diagram below shows the flow of the service and the components involved for an Entrust TruePass user. The green arrows represent common activities for all user types, and the blue arrows represent additional roaming specific activities.

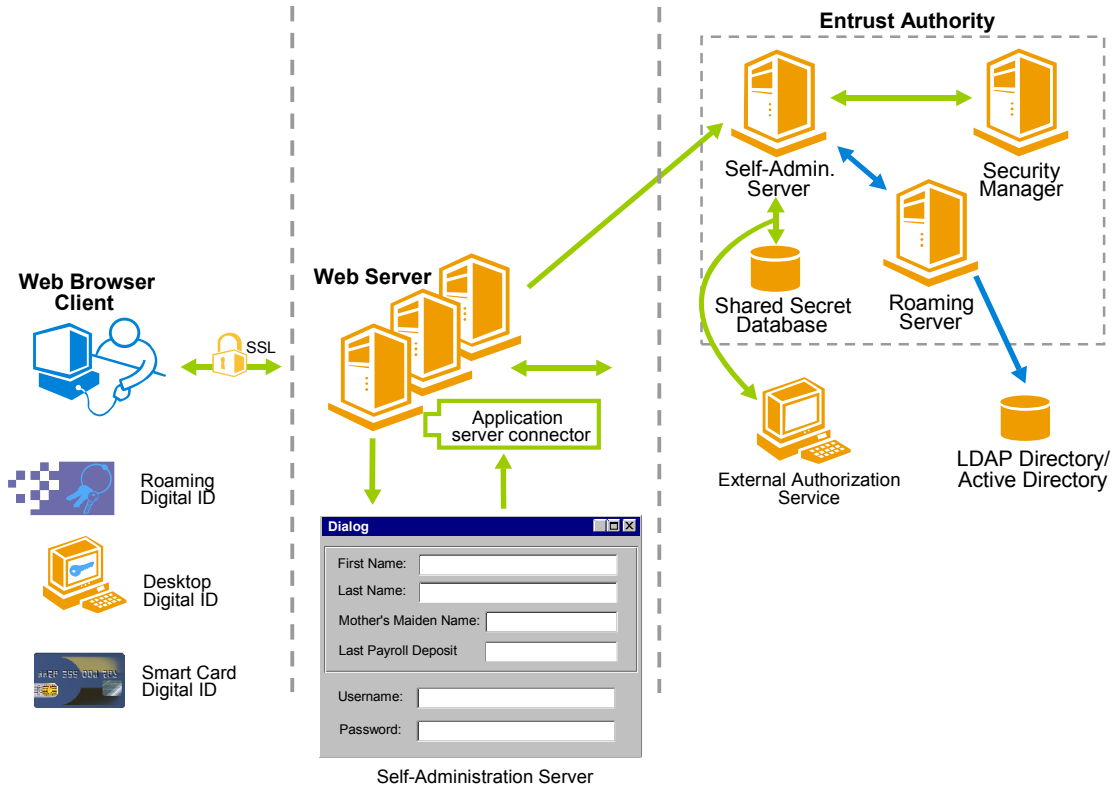


Figure 5: Entrust TruePass automatic user enrollment services.

4.3.2 Authentication, Retrieval & Secure Session Services

In addition to allowing multiple types of digital ID storage, Entrust TruePass also provides two powerful levels of authentication for users. The Authentication Service allows organizations to set the level of authentication that is appropriate for their users.

As a minimum requirement for digital IDs stored in an Entrust Profile, users are required to have a user name and a strong password in order to access their digital ID. In addition, Entrust TruePass has the ability to be extended to require additional factors of authentication, including tokens and other factors. For users that are storing their digital ID in the Microsoft Windows digital ID store, the built-in security mechanisms of the operating system protect the user's identity. Smart card users are required to enter the PIN that protects the smart card before Entrust TruePass can access the digital ID. For all user types, once the digital ID is available, Entrust TruePass will initiate the secure session for the user.

Figure 6: An Entrust TruePass Logon page can require additional pieces of information over and above a strong username and password.

The process for user authentication for Entrust TruePass is as follows:

1. The user attempts to access a URL secured by Entrust TruePass..
2. The Resource Protection Service is initiated through the Session Validation Module. It verifies whether the user has been authenticated by checking for the presence of an Authentication cookie in the request.
3. If the user has not been authenticated, the Web server redirects the Web browser to the URL defined in the configuration data file for Entrust TruePass .
4. The Authentication page is downloaded to the Web browser. The page is secured with Secure Socket Layer (SSL) protocol and includes the Entrust TruePass applet and a Login button. SSL is a requirement for all URLs protected by Entrust TruePass.
5. The user completes the fields or chooses the digital ID to be used for that session on the Authentication page and clicks the Login button.
6. Depending on the deployment type, there are multiple possibilities:
 - Roaming Profile: The Entrust TruePass applet reads the username and password, creates a password token, and sends the token, the UID and a login request to the Entrust TruePass servlets. The token (T) is created based on multiple iterations of a one-way hash function (SHA1) on the username and password supplied by the user requesting the digital identity. If the user's name & password hash match the corresponding data in the directory, the user has now been identified and the retrieval service is initiated by Entrust TruePass.
 - Desktop Profile: The Entrust TruePass applet reads the username and password, creates a password token, and compares it to the included token in the profile. If the two match, then the Profile will be unlocked and made available to Entrust TruePass for use.
 - Microsoft Windows digital ID store: In order to confirm that the correct digital ID is used, the user must choose the identity that is to be used with Entrust TruePass for each session The Entrust TruePass applet causes the user to see a dialog that includes all available digital IDs for the current Windows session. The user chooses the appropriate digital ID, and Entrust TruePass then proceeds to logon.
 - Smart card user: As with the user that has a digital ID in the Microsoft Windows digital ID store, smart card users are prompted to choose a digital ID to log in with. Once chosen, the user will be required to enter the PIN that protects the smart card; successfully doing so will allow Entrust TruePass to access the digital ID and proceed with the logon.

For roaming users, if an additional factor of authentication is mandated, this data is verified after the user has been identified, but before the identity retrieval service is invoked. The retrieval service is invoked after the user identification service has completed the necessary steps to identify the user. The following describes the process of the retrieval service:

1. The Entrust TruePass servlets obtain the digital ID securely through the use of the SPEKE protocol.
2. The Entrust TruePass servlets decrypt the outer layer of the double-encrypted digital ID and sends it to the Entrust TruePass applet. The digital ID is still protected by 128-bit encryption and the SSL connection.
3. The Entrust TruePass applet removes the final 128-bit layer of encryption and logs the user into the digital ID.

Once a user's digital ID is available to Entrust TruePass, the secure session is established through the following steps:

1. A challenge-response mechanism confirms that a valid Entrust TruePass user is communicating with the Entrust TruePass server components
2. Once the challenge-response activity has been completed, the Entrust TruePass servlets also initiate the User Management Service to facilitate revocation checking and user status. If the user has not been revoked, an Authentication session cookie is sent to the Entrust TruePass applet and stored in browser memory.
3. The User Management Service verifies whether the identity is in a key update transition period. If it requires updating, Entrust TruePass automatically manages this process in a standard transparent Entrust manner (please refer to "User Management Service" for more details)
4. The Entrust TruePass applet redirects the Web browser to the URL the user initially attempted to access.

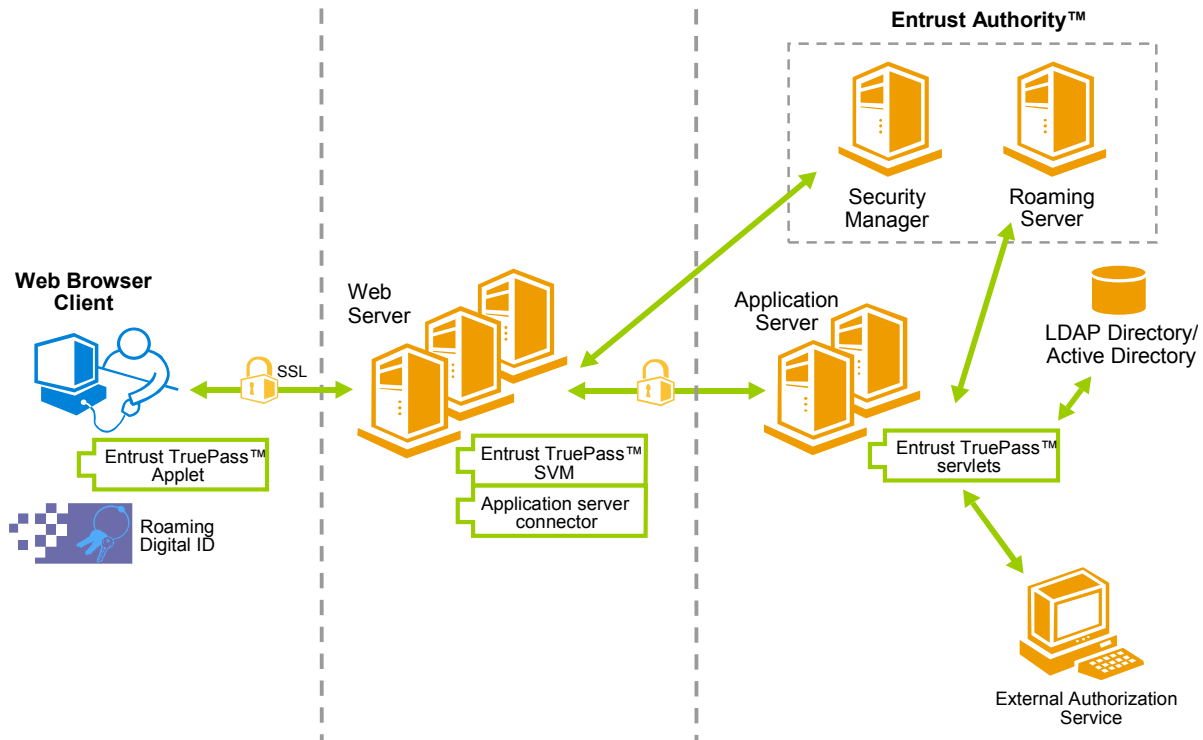


Figure 7: Entrust TruePass digital ID retrieval process.

4.3.3 Resource Protection Service

The Resource Protection Service manages access to protected URLs. If a URL has been defined as protected, the user must first authenticate before being allowed access to that resource. This service is provided in conjunction with the Entrust TruePass Authentication Service to allow organizations to define what level of authentication is required for specific resources. SSL is a requirement for all Entrust TruePass protected URLs. The Resource Protection Service is delivered through the Entrust TruePass SVM.

4.3.4 Digital Signature Service

Entrust TruePass allows organizations to implement the digital signature service on their Web site in two different manners. The power and flexibility of this service allows organizations to fit Entrust TruePass into the way that they do business, with the added benefit that the end result is always a standard PKCS#7 object.

4.3.4.1 Message Signing

Message signing, delivers the ability for identified users to perform unobtrusive digital signature operations. Entrust TruePass offers two models of message signing.

The first message signing model (Classic API) enables authenticated users to fill in information (typically through an HTML form) and simply sign that data at submission. The data in the form is collected and signed by the Entrust TruePass applet. The resulting standard PKCS#7 object is then sent through to the Entrust TruePass servlets on to the backend system for storage. The signed data does not include the HTML that made up the form, simply what the user entered into the form before applying the signature.

The second message signing model (Toolkit API) enables authenticated users to transparently sign data being passed in by the application. The Toolkit API offers application developers a programmatic interface for seamless integration of Entrust TruePass encryption and signature operations into your Web site, applications, and workflow. The Toolkit API message signing model offers support for:

- looped signature requests
- multiple signatures per form
- multiple applications with a single instance of Entrust TruePass
- application platform independence from Entrust TruePass
- returning the complete digital signature chain as part of the signed message
- for returning the signed hash
- the status pages to be displayed or not
- the applet to send the PKCS#7 object to the server, or return a status message or to send the PKCS#7 object back to the client

4.3.4.2 Transaction Signing

Transaction signing, delivers the ability to integrate a signature operation into a process that links with a backend system. This method of delivering digital signatures entails the following high-level steps:

1. The user fills in the data that needs to be signed and submits it through the Web browser.
2. The Entrust TruePass applet passes this data to the Entrust TruePass servlets. It is then passed to the organization's backend system.

3. The backend system does whatever processing it needs to do on the transaction. The result that is passed back to the Entrust TruePass servlets is a confirmation page for the transaction.
4. A byte-level copy of the confirmation page is taken by the Entrust TruePass servlets, and then it is passed down to the browser.
5. The user reviews the confirmation page (which is not modifiable) and proceeds to sign the page. They are now able to confirm that they are 'signing what they see'.
6. The Entrust TruePass applet will, at a minimum, sign the confirmation text that was generated by the backend system. Optionally, more of the page, up to and including the entire page with graphics, can be included for signature. This provides context for the signature if it is needed. The result of the signature process is a standard PKCS#7 object.
7. The signed page is sent back to the Entrust TruePass servlets, where the original confirmation page is compared to the signed copy that the user just submitted. If it matches, the servlets countersign the document (which includes a time element in the signature) and then passes it on to the backend system for storage.

4.3.5 Persistent Encryption Service

The Persistent Encryption Service delivers the ability to decrypt data received from a backend system and encrypt data for a target backend system. This is over and above the required SSL connection for any Entrust TruePass session. The primary difference between the Persistent Encryption service and SSL encryption is that SSL is used for all data transfers between the browser and the Web server; with Entrust TruePass, one can implement message encryption in addition to the SSL encryption, which allows data to remain encrypted beyond the SSL session. This encryption process uses 168-bit cryptography, regardless of the capabilities of the user's browser. Data exposure is prevented by protecting the data past the Web server and into a long-term storage repository. Protecting the data past the Web server also provides an extra level of privacy in both in-house and managed service Web server environments.

Message data is encrypted with a 168-bit 3DES symmetric key. The encrypted key is encrypted again with the receiver's public key using RSA public-key encryption. The algorithms used for the Persistent Encryption Service are:

- Symmetric algorithm: 3DES
- Symmetric algorithm key length: 168 bit
- Asymmetric algorithm: RSA
- Asymmetric algorithm key length: 1024 or 2048 bit

Data can be encrypted for any standards-based Entrust x509v3 certificate. This certificate is retrieved by the Entrust TruePass applet at data submission time, and then used by Entrust TruePass to encrypt and send the data to the backend system. The Entrust TruePass servlets automatically perform a CRL check on the certificate before sending the certificate to the applet for use.

4.3.6 Security Management Service

The Security Management Service delivers the following important capabilities:

Key and Certificate Lifecycle Automation: With the Entrust Authority Security Manager, users do not need to know anything about managing public keys and certificates. All user and CA key pairs are automatically updated in a secure, flexible, simple, and cost-effective manner. Users do not have to be aware of critical security functions, such as user key update, CA key update, CA location changes, changes to the

network list of trusted people, and so on. This reduces the costs of user training, user downtime, and help desk calls, while at the same time supporting real-life day-to-day requirements.

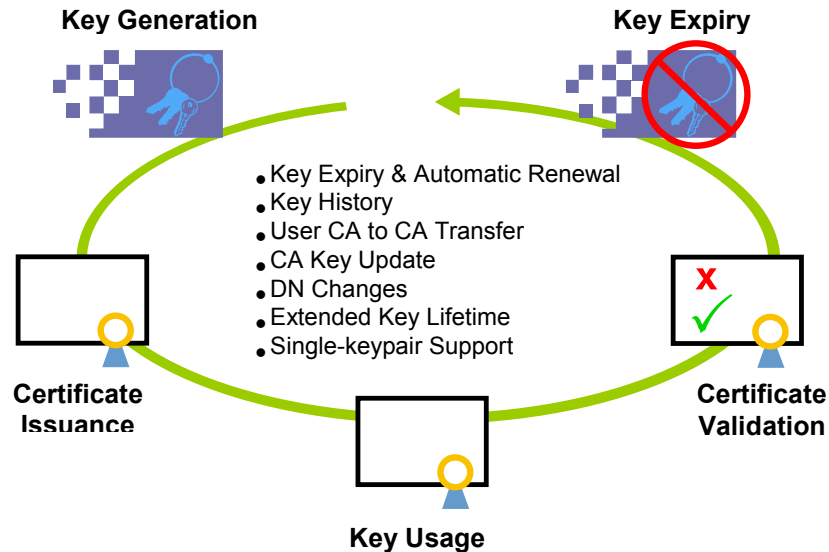


Figure 8: Enhanced Security Management

Key Backup & Recovery: Entrust Authority Security Manager provides the following features at no additional cost:

- Seamless recovery of complete key history - The entire key history is recoverable, allowing a user to decrypt encrypted information regardless of when the information was encrypted. Users typically are not even aware that a key history exists, but it provides the ability to have increased security with transparent key rollover.
- Flexible key recovery policy - Provides a secure and flexible per-operator policy to control which administrators can recover users, which users can be recovered by whom, and whether multiple authorizations are required to initiate key recovery.
- Self-service key recovery - To further reduce the costs of user administration, this provides the users the optional capability of recovering themselves with operator intervention.

4.3.7 Web Access Control Integration (Optional)

Entrust provides Web Access Control through [Entrust GetAccess™](#). Each time a customer logs on, Entrust GetAccess determines access rights and checks the user's profile. It builds a personalized menu, which can include individually targeted messages, promos, and offers. The menu helps users find their way quickly to the services they need while only permitting them to view the resources they're authorized to access. Part of the Entrust GetAccess architecture includes supporting multiple plug-able authentication modules (PAAMs) that can be used to authenticate to the system. Entrust GetAccess provides direct integration with Entrust TruePass, allowing Entrust TruePass to be the authentication mechanism for Entrust GetAccess. The integration is a Web service making it easier and quicker to install and configure. And unlike competitive solutions where multiple product runtimes are required, only the Entrust GetAccess runtime is now required making it easier to deploy and manage. This allows the powerful capabilities of both Entrust TruePass and Entrust GetAccess to be leveraged in a single deployment.

5 Operational Model

5.1 User Deployment Scenarios

This section describes a 'typical' Entrust TruePass deployment scenario in order to give a view of the operational model. The scenario includes both a user with an Entrust Roaming Digital ID and a user with a digital ID stored on a smart card. The numbered steps are explained below.

The scenario assumes that the user has a Web browser and access to the Internet, but has not used Entrust TruePass before. It also assumes the user has previously enrolled for a digital ID (either roaming or smart card-stored) and that the company running the Web site has configured the user to be allowed to access protected pages on the chosen Web site.

Step 1. Browser:

A user attempts to access a protected page on a Web site

- Resource Protection Service: Checks requests for pages to see if they are protected or not. If it is a protected page and the user has not already authenticated, they are automatically re-directed to a logon page.
- The logon page includes the transparent download of the Entrust TruePass applet, which is required for authentication.

Step 2. Browser:

a) Roaming User:

User fills in the required information for identification and submits it.

- Authentication, Retrieval, and Secure Session Services: The user's identification information is passed through the applet to the Entrust TruePass servlets for confirmation. If it is correct, the Retrieval Service securely downloads the digital ID to the Entrust TruePass applet in the browser
- If any security management activities are indicated, such as a key rollover, these are automatically initiated and completed for the user. The user is not aware that this activity is taking place.
- A secure session is established and the user is issued a session cookie

or

b) Smart Card User:

User chooses the digital ID they want to use for the secure session, enters the smart card PIN, and submits it.

- Authentication, Retrieval, and Secure Session Services: The user's identification information is passed through the applet to the Entrust TruePass servlets for confirmation.
- If any security management activities are indicated, such as a key rollover, these are automatically initiated and completed for the user. The user is not aware that this activity is taking place.
- A secure session is established and the user is issued a session cookie

Step 3. Browser:

User is redirected to the original location that he/she was trying to access

- Resource Protection Service: The user is checked again for authentication status. Now that the user has been authenticated, the Session Validation Module will allow the user to access the page

Step 4. Browser (Optional - application may only require authentication. This is an additional step to the minimum operational model)

User fills in information in a form that requires a digital signature

- Digital Signature Service (Assume message signing option): The authenticated user submits the data to the Entrust TruePass applet. The applet takes the data and applies a digital signature to it. The standard PKCS#7 object is delivered to the Entrust TruePass servlets and then passed to the backend system for storage.

Step 5. Browser (Optional - application may only require authentication. This is an additional step to the minimum operational model)

User fills in information in a form that must be encrypted for a backend system once submitted.

- Persistent Encryption Privacy Service: The authenticated user submits the data to the Entrust TruePass applet. The applet retrieves the target certificate through the Entrust TruePass servlets. The data is encrypted for the target certificate, the standard PKCS#7 object is delivered to the Entrust TruePass servlets, and then passed to the backend system for storage.

5.2 System Performance & Reliability

Entrust TruePass has been designed to operate in a high-volume, and high-value transaction portal. Built on top of the Java platform and using the servlet model for providing application capabilities, Entrust TruePass is built to scale. The ability to provide high availability, fail-over, and scalability options are driven by built-in features of the market leading application servers that Entrust TruePass is supported on. From J2EE deployment methods to specific features that have been built into the product, Entrust TruePass is fully capable of scaling with an organization to provide enhanced security for high-value transactions and a high-volume portal. The following sections briefly discuss aspects of an effective deployment and the ways that Entrust TruePass has been designed to provide a high performance enhanced security solution.

5.3 High availability

Availability refers to the percentage of time that a system is available to a user. When increasing the level of availability, your goal should be to attain the level of "high availability" (HA) or "fault tolerant" availability. HA systems, also called "fault resilient" or "RAS" (reliability, availability, serviceability), are available 99-99.9% of the time, allowing less than 9 hours of downtime per year. In other words, a highly available system is one that is almost always operational (even in the event of a failure or a physical disaster) and accessible to clients. HA systems must be maintainable so that administrators can service a failed component in the system without shutting down the entire operation.

HA systems are not the same as "fault tolerant". "Fault tolerant" refers to systems that are available 99.999% of the time, allowing less than 6 minutes of downtime per year. Fault tolerant systems are those that are mission critical and require *all* hardware and software to be mirrored—that is, every operation must be performed on two or more duplicate systems, so if one system fails another can take over. A fully mirrored system is

expensive and greatly increases the hardware required, so many companies opt for more affordable HA systems.

Application servers, like BEA WebLogic or IBM WebSphere, provide built-in HA capabilities that allow Entrust TruePass to be deployed as a highly available secure Web portal application.

5.4 Performance

Performance refers to how fast your system can respond to user requests. A system with good performance must have sufficient hardware (such as the CPU, hard disk, RAM) and must be scalable. Entrust TruePass, on top of the built-in application server performance, provides high performance transaction processing, allowing organizations to handle high volume Web portal deployments.

5.5 Scalability

Scalability refers to the ability of a system to use all available hardware effectively so that performance is optimized. In scalable systems:

- Fluctuating waves of client requests are handled without a major difference in performance.
- Administrators can easily add hardware or software to handle more client requests to the site.

5.6 Fluctuating client requests without performance impact

A well-scaled system contains applications that can handle an increase in load up to the point where they have exhausted one or more required resources. A poorly-scaled system won't maximize your system's resources in the event of increased load. Depending on how they are designed, some applications make use of resources better than others. Entrust TruePass has been designed as a "multi-threaded" and "forking" application so that resources are used efficiently. "Multi-threaded" means that Entrust TruePass tasks can be executed in parallel, instead of waiting for an entire request to finish. Multi-threading should be viewed in contrast to "single-threading", where an entire request must be processed before the application handles a new one. "Forking" means that requests from the application can be distributed across several different processors. "Forking" should be viewed in contrast to "non-forking", where the application can only use one processor.

5.7 Adding hardware or software easily

A scalable system allows administrators to add additional hardware and software to run in parallel with existing components as demand increases. This allows the system to grow without causing unnecessary downtime. Built on top of the application server architecture, Entrust TruePass adopts this capability automatically, allowing the addition of more Entrust TruePass servers, as they are needed.

5.8 Maintainability

Maintainability refers to how easily a system's hardware and software can be updated. Thus a maintainable system is one in which:

- maintenance tasks are simple and can be completed quickly

- you can remove individual machines for software and hardware upgrades with little or no impact on customers

Maintainability can conflict with other characteristics of a good system. For example, limiting the number of application server instances makes the Entrust TruePass servlets easier to maintain, but may have a negative effect on availability and performance. This is a business decision, where costs are weighed versus the overall maintainability of the system. Regardless, Entrust TruePass can provide enhanced security across the spectrum of deployment options.

6 Conclusion

Customers are looking to move business processes securely and quickly online without significant deployment and support costs. Entrust TruePass™ is a comprehensive, modular Web security solution that can provide end-to-end security capabilities enabling organizations to move business processes online. Security services like strong authentication, end-to-end encryption and digital signatures help facilitate the delivery of new services via the Internet while providing privacy and accountability for online transactions.

The Web Security Solution also makes it possible to determine the identity of individuals that are visiting and using the Web portal with strong authentication. Entrust TruePass™ delivers a choice of strong authentication methods to provide mobility, flexibility and ease of deployment when securing online communications.

Entrust TruePass™ can provide enhanced privacy for online transactions by securing the information with end-to-end encryption as information is transmitted over the Internet and when it is stored on Web servers and back-end servers. It can also help improve accountability, auditing and privacy for applications and transactions through the use of its digital signature capabilities. Uniquely, Entrust TruePass digital signatures sign the entire Web page, not only the data entered by a user. This can improve non-repudiation capabilities that can empower an organization to move business process capabilities online.

Entrust TruePass was the world's first Java-based product to receive FIPS 140-1 Level 1 certification. FIPS 140 certification gives customers the confidence of third-party validation of the security capabilities that Entrust TruePass delivers.

7 About Entrust, Inc.

At Entrust, we create software and services that **secure digital identities and information** for our enterprise and government customers.

For more than 10 years, our customers have used security to enable more than just protection. They use security to:

- **Save time:** streamlining business processes cutting weeks to days, hours to minutes
- **Cut costs:** lowering the cost of security administration, reducing and replacing costly paper processes, achieving ROI on security
- **Decrease risk:** securing digital identities, information and transactions with world-leading security technologies
- **Increase productivity:** maximizing the potential of Internet and wireless connectivity, without unnecessary risk

Entrust is able to help you **get more from your security investment.**

- [Our Solutions](#) meet current and future security needs and help bridge the gap between old and new technologies
- [Our Services](#) simplify and speed deployment to accelerate benefits and rates of return
- [Our Customers](#) continue to prove and improve our superior product performance

www.entrust.com