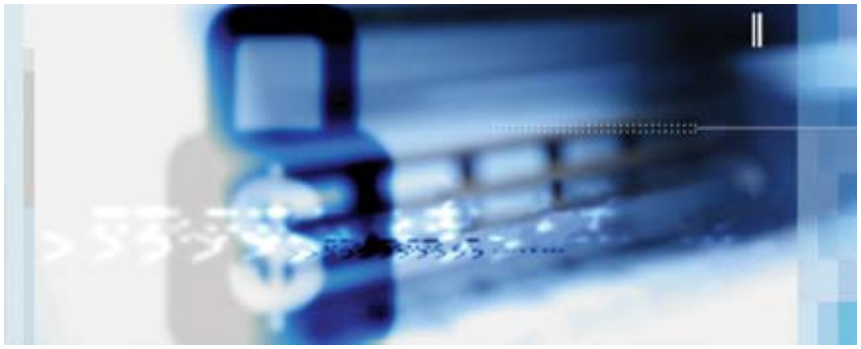
Entrust® Securing Digital Identities & Information



Securing Your Digital Life

Managing SSL Security

February 2005

TABLE OF CONTENTS

1. INTRODUCTION

Secure Sockets Layer (SSL) is the fundamental security protocol that has enabled use of the Internet to extend from information presentation to e-business. By encrypting information between the web browser and the web server, transactions that require a degree of confidentiality can be delivered via the Internet.[1]

At the heart of enabling this security is the SSL certificate. As enterprises and governments rely more and more on SSL, the number of certificates in use can grow into the hundreds or even thousands. Along with the increase in numbers, the cost and effort of managing these certificates also increases. However, certificate providers have not recognized this and up till now there has been an absence of services to help customers manage these growing certificate pools. The result is that customers are dealing with cost and complexity that could be avoided.

There are three key areas impacting the cost and complexity of managing SSL certificates today:

- Acquiring SSL Certificates – selecting the right certificate can significantly impact costs.
- Account Administration – allowing SSL certificates to be administered in line with how they are deployed within the organization can significantly simplify internal processes; and
- Lifecycle Management – eliminating the need for manual installation and renewal of certificates can significantly reduce the effort spent in managing SSL security.

This whitepaper explores each of these issues and identifies opportunities for customers to reduce the cost and complexity of using SSL. These opportunities are mapped to the capabilities of Entrust's Certificate Management Service that provides a complete offering for managing SSL certificates.

[1] For more information on SSL and how it works, please see *Understanding SSL*.

2. SSL CERTIFICATES

SSL certificates and the issuing process can impact not only costs, but can also impact end user trust and the brand of an organization. Specific requirements for SSL certificates should include:

128-bit Security. SSL certificates should support 128-bit security to provide for the confidentiality of information traveling over the Internet. This means that the secure session between browser and server is encrypted with a 128-bit key to prevent information from being intercepted and decoded. SSL certificates from Entrust support 128-bit security.

Some vendors indicate that 128-bit security requires support of "Server-Gated Crypto" (SGC) and sell these certificates at a significant premium. SGC is not required to enable 128-bit security with virtually all browsers deployed today. According to browser usage statistics 97.43% of browsers in use today support 128-bit encryption without SGC[2]. For the few users with these older browsers converting is straightforward, with upgrade packs available for most browsers. For this reason, premium priced "step-up" Web server certificates are no longer necessary.

More importantly for the security of organizations and their end users, older version of browsers that require SGC can represent an additional security vulnerability. For example, Microsoft Internet Explorer version 5.0.1 was the last IE version requiring SGC for 128-bit operation. This version is no longer supported by Microsoft, having exited the *Extended Support* phase[3]. As such, the browser does not receive patches or updates to address security issues which could leave both the user and the organization vulnerable.

WebTrust – A Trusted Brand. Issuing SSL certificates only to organizations that have been subjected to a documented level of vetting is critical for the integrity of SSL Security. WebTrust[4] is an independent organization whose certification process is intended to reduce certain business risks and provide a level of assurance to customers. Entrust was the first certificate authority to receive WebTrust certification, assuring that Entrust's documented policies and processes are followed, including:

- Checking subscriber information against third-party sources;
- Conducting an employment check to confirm that the technical contact listed in a certificate request is authorized to request issuance of certificates on behalf of his or her organization;
- Maintaining the continuity of key and certificate life cycle management operations for the Entrust Certification Authority; and
- Following proper authorization procedures for development, maintenance, and operational activities in respect to the Entrust Certification Authority .

Rapid Issuance and Status. The ability to rapidly receive certificates upon request and track their progress during an order is critical for business continuity. Deployment of new web servers or associated applications should not have to be delayed waiting for receipt of SSL certificates. Nor should the issuance of the certificate be a blind process. With Entrust, certificate requests are responded to quickly, automatically and with on-line status available. In addition, because it is not uncommon to for requesters to make an error during a certificate request, Entrust provides a 30 day re-issuance guarantee. This can help reduce costs incurred from having to re-order certificates that have been initially deployed in error.

[2] Source: www.securityspace.com
[3] Internet Explorer Support
[4] WebTrust

Revocation. Occasionally, SSL certificates must be revoked in order to prevent an organization from being subjected to a variety of threats including fraud or damage to brand. This occurs in situations where a web server's key store has been left vulnerable to compromise or where a particular server is no longer to be trusted. If a malevolent user was to gain access to a web server key store, they could stand up their own web site, impersonating the original organization and conduct fraudulent transactions. This has clear ramifications including the potential loss of end user trust.

The mechanism to prevent the use of a potentially compromised certificate is to revoke it, which then allows end user browsers to determine that it is no longer to be trusted. Key to revocation is the ability to quickly notify the certificate issuer that a particular certificate must be revoked and published in an updated Certificate Revocation List (CRL) for use by browsers. Entrust provides a self-service interface with which to request revocation of certificates as well as to download the latest CRLs.

Even for customers only managing a handful of single certificates, these capabilities are significant.

3. ACCOUNT ADMINISTRATION

As the number of SSL certificates under management increases, more flexible and sophisticated tools to administer their management and deployment are necessary. This applies to both the certificates as well as managing administrators themselves – this will be especially true as use of SSL certificates is distributed across different departments and geographical locations. Without these capabilities, the complexity of managing multiple SSL certificates increases significantly and requires manual processes for administration. To reduce this complexity, requirements for SSL certificate account administration should include:

Simplified Enrolment. When managing several SSL certificates, there should be no need to go through manual enrolment for each certificate request. With Entrust's Certificate Management Solution, administrators can enroll, adding administrators, domains and organizational names. Specific administrators need to enroll only once to be able to request and receive certificates automatically. This can save time when requesting multiple SSL certificates.

Administration Delegation. Organizations with large numbers of SSL certificates often delegate management to administrators who own specific groups of web servers. As such, there is often a need to allow certificate administration to be securely delegated so that sub-administrators will be able to manage only those certificates that are associated with the web servers they manage while still allowing centralized tracking and reporting.

Entrust provides delegated administration by allowing the creation of administrators who are *Super-Administrators* with authority to delegate to *Sub-Administrators*. *Super-Administrators* continue to have access to central tracking of SSL certificate activity for themselves and for their Sub-Administrators. They can delegate specific numbers of certificates and specific domains to particular administrators – allowing them to purchase bulk orders of SSL certificates while being able to assign them to others for re-use, helping to save time and costs.

On-Demand Services. To reduce the time spent managing pools of SSL certificates, it is important that services are made available to administrators using a rapid-response, self-service

Company XYZ

Admin Delegation

This page will enable the assignment and modification of resources (certificates, domain names and organizational names) for the Sub-Administrator(s). Assigning these resources to the Sub-Administrator(s) will allow the Super-Administrator to control the amount of certificates created and which domain and organizational names are utilized. The display provides the total certificate inventory as well as the resources that have been assigned to the Sub-Administrator(s).

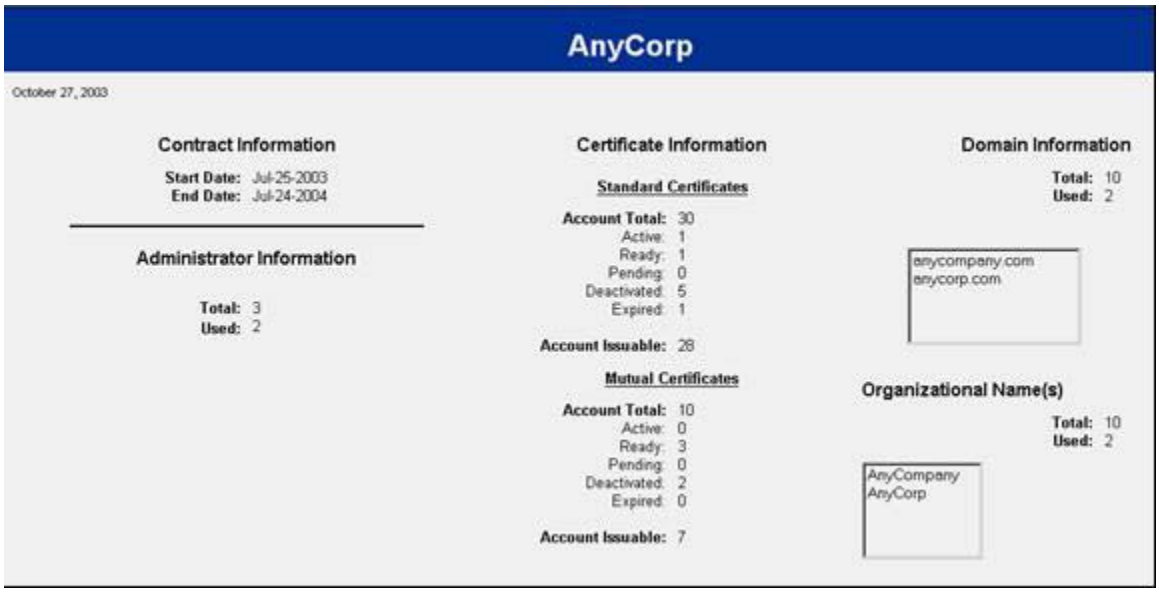
Select the **EDIT** button to modify the resources allocated.

Service Inventory

Certificate Inventory		
Total	**Used**	**Remaining**
Standard: 30 Mutual: 5	Standard: 16 Mutual: 2	Standard: 14 Mutual: 3

Sub-Administrator's Inventory Allotment

Administrator Name	Status	Certificate Assignment			Domain Names	Organizational Names
		Total	Used	Remaining		
Jane Small Edit	Active	Standard: 0	Standard: 0	Standard: 0	None Assigned	None Assigned
Joe Soap Edit	Active	Standard: 2 Mutual: 1	Standard: 2 Mutual: 1	Standard: 0 Mutual: 0	companyxyz.com	ECS Development



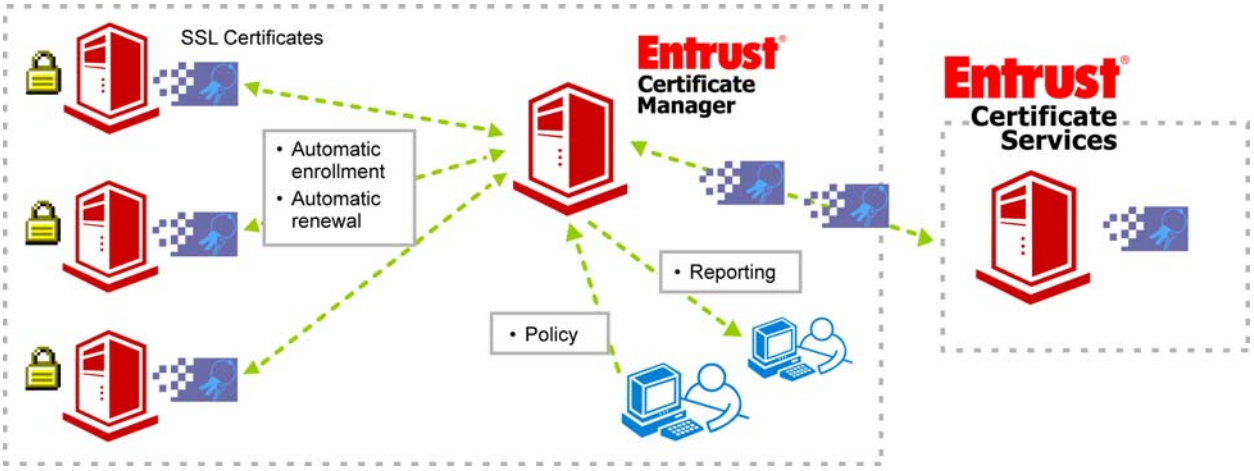
mechanism. Entrust provides enhanced self-service capabilities including a fully automated process to request additional services. This enables administrators to request additional certificates, domains and organization names online quickly. Furthermore, Sub-Administrators can be authorized to use these services, with *Super-Administrators* maintaining approval control.

Certificate Pooling. To further simplify certificate enrolment, Entrust uses the concept of certificate pooling – meaning that organizations can deploy and redeploy certificates as often as they like during the period of service. For example, if a customer issues an SSL certificate to a web server on the first day of the service, then, after six months, the customer can revoke that certificate and issue a new one to a different web server for the six remaining months of the service at no additional charge. In addition, a certificate can be deployed to a new server after deactivating that certificate on another server. This can reduce the number of certificates required and help reduce the need to purchase more certificates. Other service providers do not provide this capability and instead customers must purchase additional certificates.

Certificate pooling also allows the expiration date of a certificate to be decoupled from the service charge. For example, customers can set a given web server's SSL certificate to expire after two months and subsequently reissue to that web server for the another two months, and so on for the remainder of the service subscription.

Expiry Date Alignment. To simplify activities such as certificate renewal, it is often desirable to align certificate expiry dates. Rather than have certificates expire at different times, aligning expirty dates allows administrators to focus their renewal activities in a particular time period, such as once per quarter or once per year. Entrust allows expiry dates to be easily aligned and, due to certificate pooling, without impact to certificate costs.

Audit and Reporting Tools. Administrators need to have access to detailed records that capture each administrative action as well as a consolidated record of SSL certificate deployment and status. Entrust provides comprehensive log history with detailed information on certificate management activity and other administrator actions. Administrators have access to this information either using full Boolean searches or by saving their favorite searches.



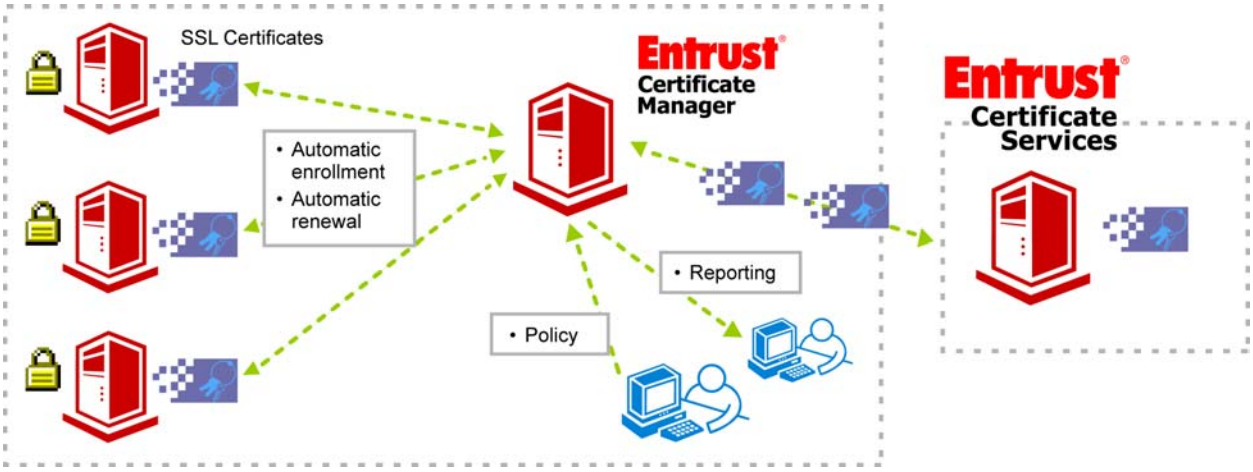
Zero Footprint Admin. Management of SSL certificates should be accessible from anywhere within the organization while providing the ability to authenticate administrators. Entrust SSL certificate administration is browser based for easy access. To authenticate administrators, a Digital Identity is used in conjunction with the unique roaming capabilities of the Entrust TruePass™ application. This allows administrators to authenticate from any browser without needing to download client software or physically transporting their Digital ID from workstation to workstation. This allows administrators to securely work where and when required.

For customers managing pools of SSL certificates, these capabilities are critical for simplifying management in complex environments.

4. LIFECYCLE MANAGEMENT

For customers managing large numbers of SSL certificates, one of the most significant sources of cost and complexity is the effort to manage their lifecycle including certificate request, installation and renewal. Organizations typically spend up to an hour for each web server - costs and effort that quickly becomes onerous as web site requirements grow to hundreds or even thousands of certificates. This is further compounded by the need to monitor SSL certificate expiry dates so that renewals are commenced in a timely fashion. Otherwise, should a certificate expire, the web server will not be available for SSL transactions and end users could be impacted by service interruptions.

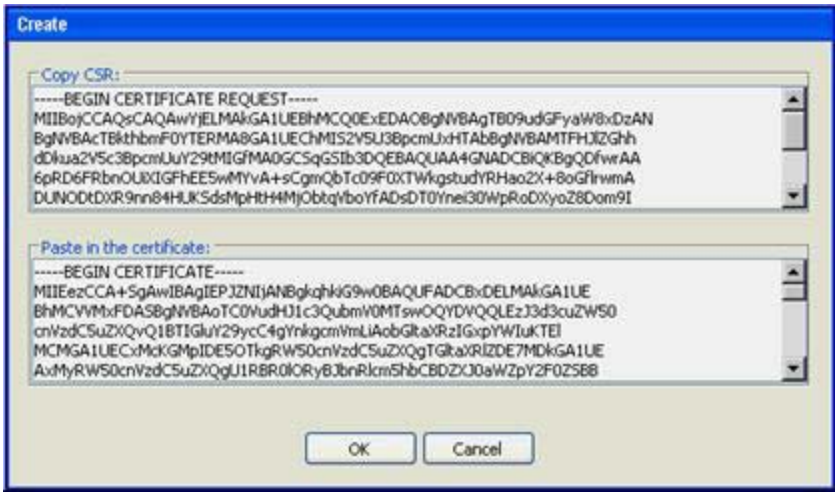
Entrust Certificate Management Service helps address the cost and complexity of this process by automating the certificate request, installation and renewal lifecycle operations. As part of the Certificate Management Service, Entrust provides an application within the customer's network that interfaces to web servers without needing to install agents on target servers and communicates automatically to have certificates issued and installed. The result can be a significant reduction in the effort to manage the lifecycle of SSL certificates.



Scheduled for release in early 2004, the Entrust Certificate Manager application is designed to provide the following capabilities:

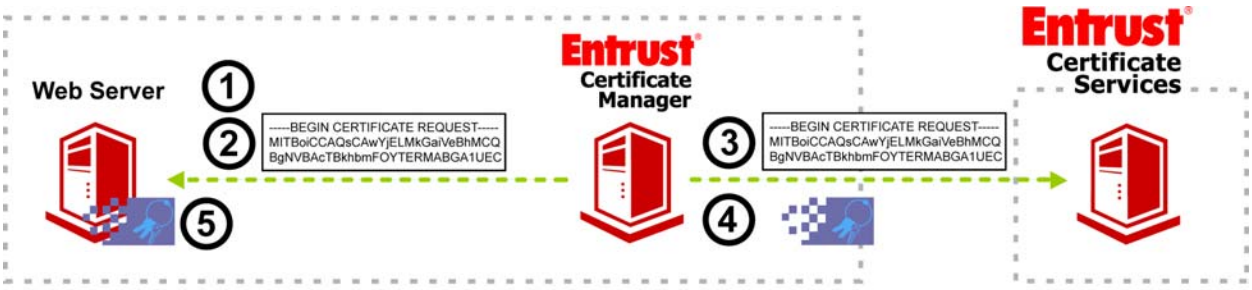
Automated Enrolment. When SSL certificates are first installed on a web server, there are typically numerous steps that must be performed:

1. An authorized administrator logs on to the web server.
2. Through the web server interface, a Certificate Enrolment Request is generated.
3. The certificate request is copied and pasted into an SSL certificate provider enrolment site.
4. Once a certificate has been issued by the certificate provider, it is copied from the provider's enrolment site.
5. The administrator logs back onto the web server and pastes the certificate from the provider.



This process can take up to 60 minutes of administrator time and span over a much longer time period depending the turn around of the SSL certificate provider. Entrust's Certificate Management Service automates this process so that, without manual intervention, a certificate can be requested, downloaded and installed. The Certificate Manager software transparently executes this process as follows:

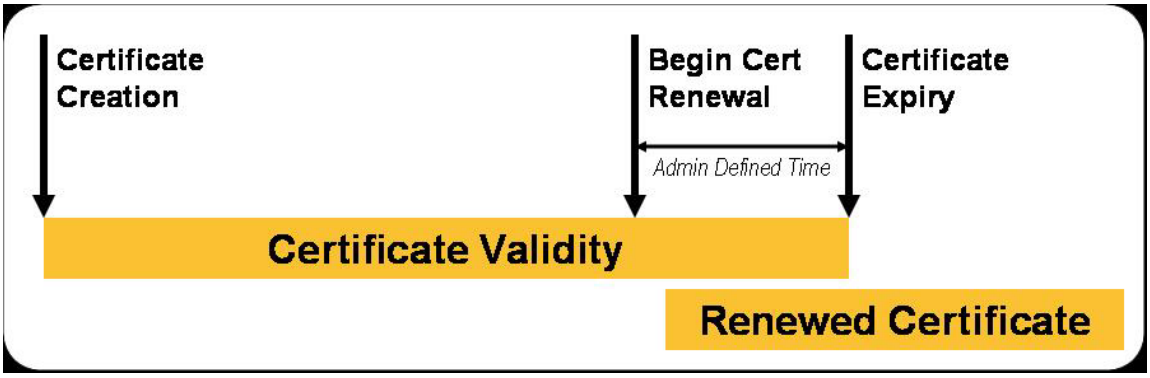
1. Web Server Log in. The Certificate Manager begins the certificate installation process by securely logging into the web server using SSH. This is done using account information securely stored in the Certificate Manager database. No software needs to be installed on the web server.
2. Certificate Request Generation. The Certificate Manager initiates the certificate request generation process on the web server, producing a certificate request message. This can be done regardless of whether or not there is currently an SSL certificate already installed. This allows for a seamless transition from SSL certificates that may have been installed from a different provider.
3. Certificate Request Submission. The Certificate Manager submits the certificate request to the Entrust Certificate Services facility over an SSL-secured session. The request is checked against the customer account to determine whether a certificate is available in inventory.
4. Certificate Creation and Download. Once the SSL certificate is generated, it is downloaded to the Certificate Manager which logs its details. This is part of the overall reporting capability of the Entrust Certificate Management Service which records each server and certificate under management.
5. Certificate Installation. Having received the certificate, the Certificate Manager once again logs in to the web server and installs the certificate. It then monitors the certificate for upcoming expiry and renewal.



1. **Certificate Manager remotely logs in to Web Server.**
2. **Certificate request generated on web server and passed to Certificate Management Server.**
3. **Certificate request sent to Certificate Services for fulfillment. Option Admin approval.**
4. **Certificate generated and downloaded to Certificate Management Server.**
5. **Web server accessed and certificate loaded.**

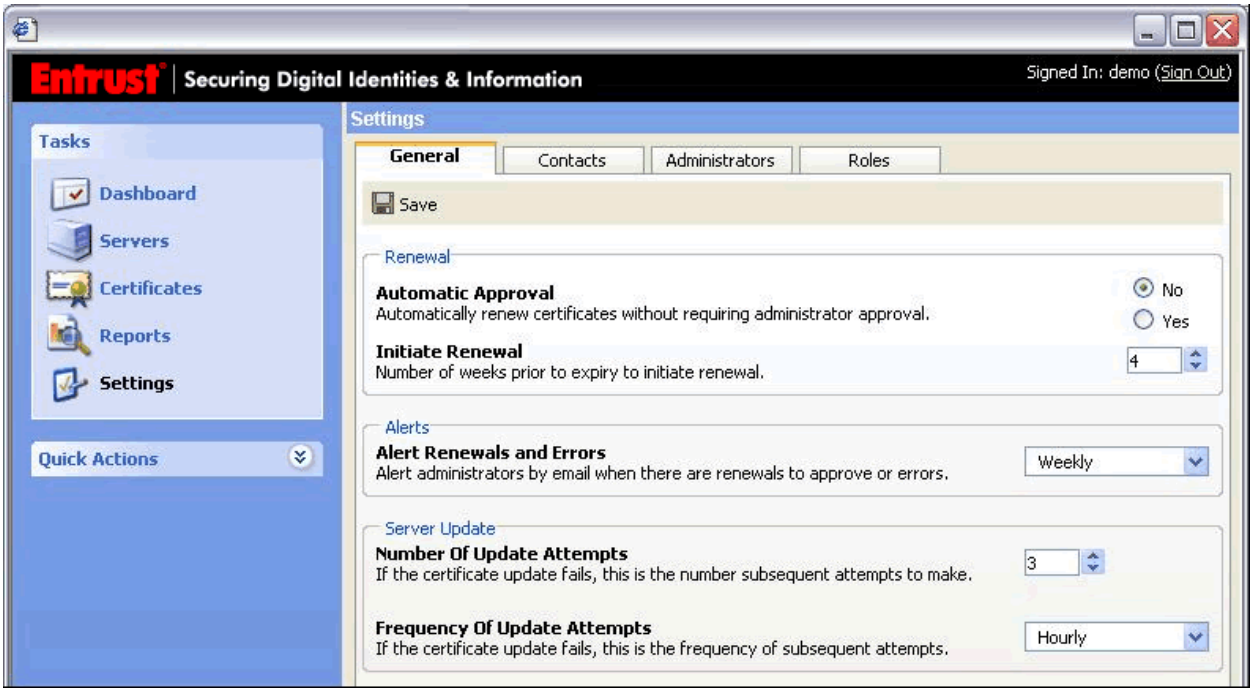
Automated Renewal. One of the most challenging activities for administrators is the monitoring and timely renewal of SSL certificates. Manual methods such as a tracking spreadsheet are typically used to record the expiry date of certificates. As the number of certificates increases this method becomes more and more prone to error. The result is certificates potentially expiring – impacting web site availability and typically triggering significant effort to request and receive a renewal. The manual renewal process is similar to that described for installation with a need to log in to the web server, create a certificate request, submit the request, receive the certificate and, finally, install it on the web server.

Rather than relying on manual intervention to initiate the renewal process, the Certificate Manager begins the process prior to the expiry date. At a time specified by the administrator the renewal is kicked off and uses the same steps as described for automated installation. In addition, administrators can perform manual renewals at any time.

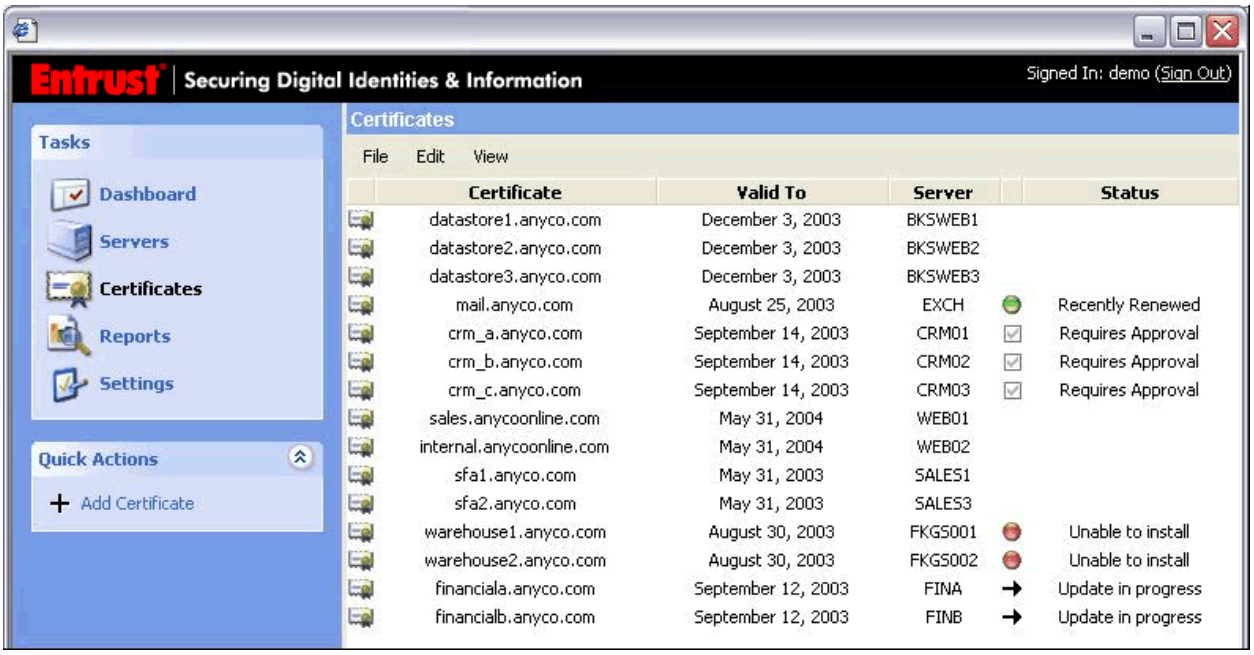


Policy Controls. Even if certificate management processes are automated, many organizations need to maintain approval and notification processes – especially with large numbers of SSL certificates under management with web servers controlled by other departments. Regardless, the automation of processes must be done in a manner that is consistent with organizational policy.

The Entrust Certificate Manager provides a high degree of centralized control including tailoring of how automated processes behave and providing for optional manual approval of certificate management functions. For example, administrators can specify how far ahead of certificate expiry the renewal process should commence. In addition, administrators can require manual approval of automatically generated certificate requests. Extensive controls allow the solution to fit a broad range of business processes that customers typically use in certificate lifecycle management.



Reporting and Audit. As with any business process, reporting and auditing is required for certificate lifecycle management. This includes two key processes: maintaining current status information to identify where administrator attention is required and logging administrator actions and information for accountability and audit. The Entrust Certificate Manager provides both these capabilities – providing an easy to read system snapshot and event monitor to alert the administrator about system status changes. In addition, detailed audit logs are maintained that record administrator activity as well as register each automated certificate management action.



The Certificate Manager software runs on the Windows 2003 server platform and administrative functions can be accessed by authenticated administrators from any Internet Explorer browser above release 5.5. Scheduled to be available in early 2004, it promises to provide potential cost saving and reduced complexity for customers managing large numbers of SSL certificates.

5. ENTRUST CERTIFICATE MANAGEMENT SERVICE

Entrust's Certificate Management Service is designed to include all the certificate, administration tools and lifecycle management capabilities discussed in this white paper to help reduce the cost and complexity of managing SSL certificates. To help map the service to the needs of various classes of customers, the service is offered in three editions:

Standard. Customers using the standard level of the Certificate Management Service can benefit from competitively priced SSL certificates that enable strong security for on-line transactions. Typically, this service is appropriate for customers managing less than 10 certificates. It provides streamlined processes to purchase and administer these certificates to reflect the smaller numbers under management.

Enhanced. As customers manage more certificates, the account administration of the service makes it simple to order and deploy SSL certificates. Customers will benefit from certificate pooling and a reusable inventory. Administrative delegation helps to reduce certificate costs to simplify deployment and fit into how SSL certificates are managed within the organization.

Premium. Along with offerings of the Enhanced package, customers can benefit from reduced costs and complexity through the automation of certificate lifecycle management. The Certificate Manager software included with the service automates the installation and renewal of certificates to provide customers managing large pools of SSL certificates with potential savings.

The following table provides a summary of the capabilities of each of these offerings:

Feature		Certificate Management Service		
		Standard	**Enhanced**	**Premium**
SSL Certificates	128-bit Security	✓	✓	✓
	WebTrust Certification	✓	✓	✓
	Rapid Issuance & Status	✓	✓	✓
	30 Day Re-issue Guarantee	✓	✓	✓
	Rapid Revocation	✓	✓	✓
Account Administration	Simplified Enrolment		✓	✓
	Administration Delegation		✓	✓
	On-Demand Services		✓	✓
	Certificate Pooling		✓	✓
	Expiry Date Alignment		✓	✓
	Audit & Reporting Tools		✓	✓
	Zero-Footprint Admin		✓	✓
Lifecycle Management	Automated Enrolment			✓
	Automated Renewal			✓
	Policy Control			✓
	Auditing and Reporting			✓
	24/7 Premium Customer Support			✓

6. CONCLUSION

Secure Sockets Layer (SSL) is the fundamental security protocol that has enabled use of the Internet to extend from information presentation to e-business. As enterprises and governments rely more and more on SSL, the number of certificates in use can grow into the hundreds or even thousands. Along with the increase in numbers, the cost and effort of managing these certificates also increases.

Entrust Certificate Management Service is the only solution that addresses the three key areas impacting the cost and complexity of managing SSL certificates today:

- Acquiring SSL Certificates – selecting the right certificate can significantly impact costs.
- Account Administration – allowing SSL certificates to be administered in line with how they are deployed within the organization can significantly simplify internal processes; and
- Lifecycle Management – eliminating the need for manual installation and renewal of certificates can significantly reduce the effort spent in managing SSL security.

Entrust Certificate Management Service helps organizations secure their online transactions quickly and efficiently with limited effort required by the user or administrator. By using Entrust SSL Certificates, organizations can be confident that communications are secure and that their online presence is a trusted one, thereby increasing customer confidence and reducing security risks.

To learn more about Entrust Certificate Services and how it can help your business grow, please refer to the Entrust Web site at http://www.entrust.com/certificate_services/index.htm.

ABOUT ENTRUST

Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and e-mail security into business opportunities. For more information on how Entrust can secure your digital life, please visit: **www.entrust.com.**