

Entrust[®] Securing Digital Identities & Information



**Securing Your
Digital Life**

Managing SSL Security

May 2007

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© Copyright 2007 Entrust. All rights reserved.

Table of Contents

1	Introduction.....	1
2	SSL Certificates	2
	128- or 256-bit Security	2
	WebTrust — A Trusted Brand	2
	Rapid Issuance and Status.....	3
	Revocation.....	3
3	Account Administration	4
	On-Demand Services	5
	Certificate Recycling.....	6
	Configurable Expiry Dates.....	6
	Audit and Reporting Tools	6
	Zero-Footprint Administration	6
4	The Entrust Difference — Certificate Management Service.....	7
5	Conclusion	8
6	About Entrust.....	8

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.

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 sometimes fail to recognize this and, until 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 can be avoided.

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

- **SSL Certificate Features** — selecting the right certificate can significantly impact the real and perceived security of your Web site
- **Account Administration** — allowing SSL certificates to be administered in line with how they are deployed within the organization can significantly simplify internal processes
- **Lifecycle Management** — enabling the ability to manage the number, expiry and renewal dates of certificates, and redeployment of decommissioned certificates — all through a simple, efficient interface

This white paper 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 the Entrust Certificate Management Service that provides a complete offering for managing SSL certificates.

2 SSL Certificates

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

128- or 256-bit Security

SSL certificates should support 128- or 256-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-/256-bit key to prevent information from being intercepted and decoded. SSL certificates from Entrust support both 128- and 256-bit security.

Even today, some vendors indicate that 128-bit security requires support of “Server-Gated Cryptography” (SGC) and sell these certificates at a significant premium. SGC is not required to enable 128-bit security for virtually all browsers deployed today. According to some industry statistics, more than 99.6 percent of browsers in use today support either 128- or 256-bit encryption without SGC¹. 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 versions of browsers that require SGC, sometimes referred to as “export-strength” or 40-bit browsers, can represent increased security vulnerability. For example, Microsoft Internet Explorer version 5.0.1 was the last IE version requiring SGC for 128-bit operation, and a longstanding update has been available on Microsoft Windows Update to bring it up to 128-bit encryption. As such, most users who still require SGC are using a Web browser that has not had security updates to address the multitude of other security issues identified since that update was published, leaving 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. WebTrust² 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 Certification Authority (CA) 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 lifecycle management operations for the Entrust Certification Authority
- Following proper authorization procedures for development, maintenance and operational activities in respect to the Entrust Certification Authority



¹ Source: <http://marketshare.hitslink.com/report.aspx?qprid=6>

² [WebTrust](#)

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 while 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 online status available. In addition, because it is not uncommon 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.

This is taken a step further for customers of the Entrust Certificate Management Service — self-service certificate issuance means that customers can get their certificates immediately and certificate recycling ensures that re-issuance is possible at any time in the subscription period without additional charges.

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 deploy their own Web site, impersonate 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 subsidiaries, departments or geographical locations.

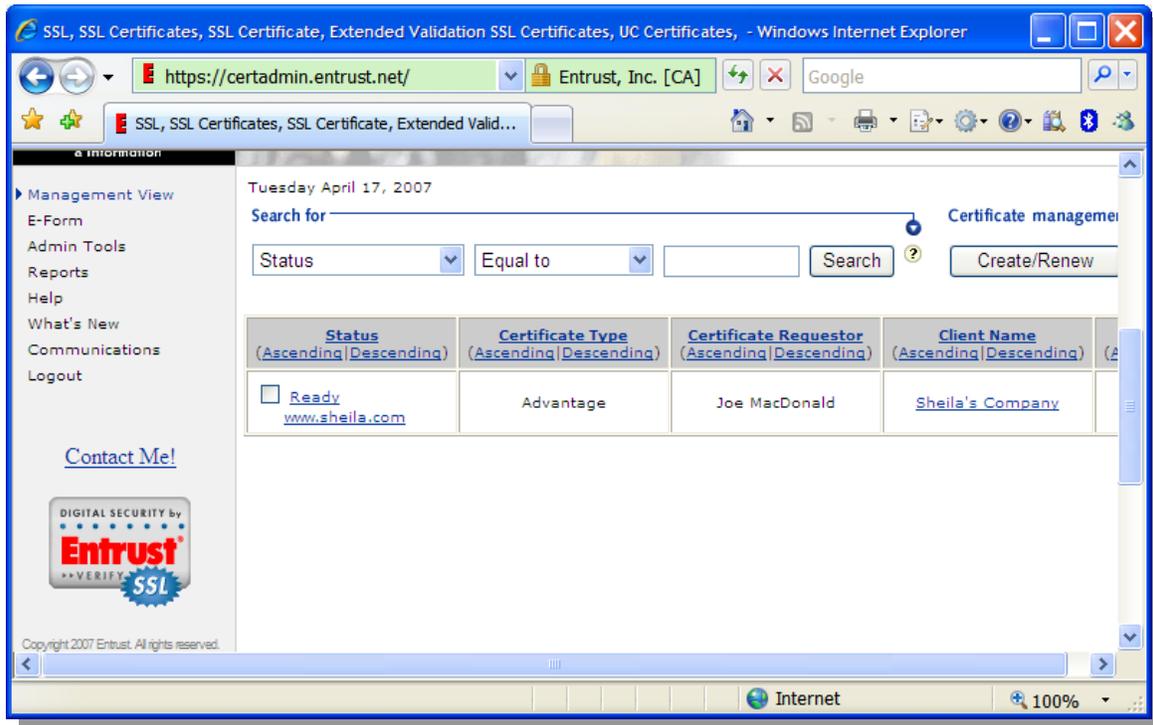


Figure 1: The Certificate Management Service

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 Enrollment — When managing several SSL certificates, there should be no need to endure manual enrollment for each certificate request. With the Entrust Certificate Management Service, administrators can enroll to add 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.

Delegated Administration — 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.

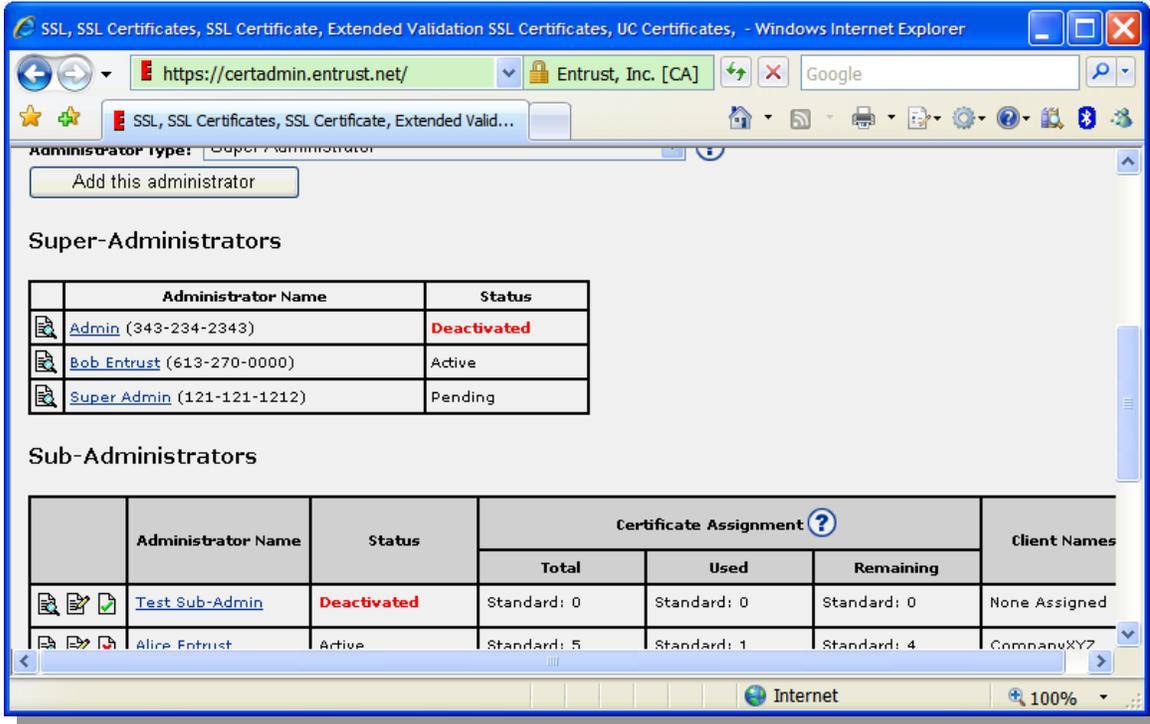


Figure 2: Administrator Management

Client Management — Complex corporate structures, outsourcing relationships and Web hosting create specific challenges for SSL certificate management. With the Entrust Certificate Management Service, large enterprise IT organizations, outsourcers and Web hosters can manage their client accounts, certificate inventories and domain name lists from one central view. It's possible to add new clients, edit lists of client domains and get per-client reports on certificate usage all from an intuitive Web application. Certificates can be issued to client domains with no additional validation delays to keep projects moving and on schedule.

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 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 Recycling

To further simplify certificate enrollment, the Entrust Certificate Management Service uses the concept of certificate recycling — 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 retire 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 the original 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 recycling also allows the expiration date of a certificate to be decoupled from the Certificate Management Service subscription end date. For example, a customer with a more stringent security policy than the norm could set a given Web server's SSL certificate to expire after two months and subsequently reissue to that Web server for another two months, and so on, for the remainder of the service subscription.

Configurable Expiry Dates

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 expiry 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 recycling, without impact to certificate costs.

Audit and Reporting Tools

Administrators need access to detailed records that capture each administrative action as well as a consolidated record of SSL certificate deployment and status. The Entrust Certificate Management Service 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 Administration

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 The Entrust Difference — Certificate Management Service

As customers manage more certificates, the effort and complexity increases to a point where even the best-resourced team could make a critical error and negatively impact an organization's security posture or online presence.

The Entrust Certificate Management Service was developed specifically for such customers using large numbers of SSL certificates.

This subscription-based solution targets two primary groups — enterprises and outsourcers/Web hosters. Each group requires large-scale deployments of certificates, but specific features for outsourcers and Web hosters are tailored to their specific business needs — managing large numbers of domains and certificates on behalf of their clients.

The service makes it simple to order and deploy SSL certificates. All of the Entrust SSL certificate products are available within the Certificate Management Service — including the powerful new Extended Validation and Unified Communications certificates. Customers can reduce certificate costs through certificate pooling and a re-usable inventory. Administrative delegation helps to fit into how SSL certificates are managed within the organization across departments or regions, and flexible reporting tools provide high visibility into where certificates are being used and when they will expire.

The following table provides a summary of the capabilities:

	Feature	Entrust Certificate Management Service
SSL Certificates	128- & 256-bit encryption support	✓
	WebTrust Certification	✓
	Rapid Issuance & Status	✓
	30-Day Re-issue Guarantee	✓
	Rapid Revocation	✓
	New Extended Validation and Unified Communications Certificates	✓
Account Administration	Simplified Enrollment	✓
	Administrative Delegation	✓
	On-Demand Services	✓
	Certificate Recycling	✓
	Expiry Date Alignment	✓
	Audit & Reporting Tools	✓
	Zero-Footprint Admin	✓
	Domain Management	✓
	Client Management	✓

5 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.

The Entrust Certificate Management Service cost-effectively addresses the three key areas impacting the complexity of managing SSL certificates today:

- **SSL Certificate Features** — selecting the right certificate can significantly impact the real and perceived security of your Web site
- **Account Administration** — allowing SSL certificates to be administered in line with how they are deployed within the organization can significantly simplify internal processes
- **Lifecycle Management** — enabling the ability to manage the number, expiry and renewal dates of certificates through a simple, efficient interface

The Entrust Certificate Management Service helps organizations secure their online transactions quickly and efficiently with limited effort required by the user or administrator. By leveraging 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 the Entrust Certificate Management Service and how it can help your enterprise grow, please refer to the Entrust Web site at www.entrust.net

6 About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world leader in securing digital identities and information. More than 1,650 enterprises and government agencies in more than 60 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.