@Entrust
EntrustSecurity

A Proper Foundation: Extended Validation SSL

A critical model for SSL digital certificates and browser trust

Get this
White Paper

Entrust.net
1-888-690-2424
Entrust@Entrust.com

Contents

Context of Internet Security

In 2005, the longstanding Internet browser trust model, which had served as a foundation for many billions of dollars of ecommerce, was starting to show signs of age. Just like an older building, the model was in need of renovation and repair to its foundation in order to ensure it could continue to support future ecommerce initiatives.

Based on Secure Sockets Layer (SSL), certificates and the ubiquitous padlock icon, the browser trust model was reworked to help renew consumer confidence and to better suit handling ecommerce transaction volumes as they continued to increase.

The new model was defined by a group called the CA/Browser Forum, and consumers first saw the results of their work in January 2007. This paper outlines why the group was formed, what it is working toward and the impact it has on consumers and Web site operators.

> “*Before Extended Validation, requirements varied significantly between CAs, without an easy way for consumers to distinguish certificates issued using more- or less-rigorous validation processes.*”

Early Growth

In the mid-1990s, Netscape foresaw the need for security to enable the adoption and growth of ecommerce. Creating and embedding the SSL security protocol in their browser and server products was the first step, but the real challenge was building consumer trust.

From the outset, a key or padlock icon was chosen to represent a secure SSL connection, and consumers were told that if the lock was closed, they were dealing with a “trusted” website.

Whether a site was trusted or not was based on the digital certificate it presented to the browser through SSL. If the server certificate was issued from a certification authority (CA) whose root key was embedded in the browser, then the lock would immediately close. A decade and many billions of dollars in ecommerce later, the lock icon has served its purpose well.

Trust Model Weakness

While SSL and the padlock icon served as a solid foundation for many years, cracks were appearing. Con artists always have searched for ways to exploit the learned responses of their fellow humans. With varying degrees of sophistication, examples have appeared where consumer trust of the lock icon has been abused.

In one early exploit, a server certificate was acquired under false pretenses to give a phishing website extra credibility as it attempted to steal usernames and passwords. In another exploit, an SSL renegotiation vulnerability was used to hack a popular social media site.[1]

[1] “Researcher Hacks Twitter Using SSL Vulnerability,” Brian Prince, eWeek, November 16, 2009.

Creation of Extended Validation

To bolster consumer trust in the foundation of ecommerce before it was irreparably damaged, several CAs and browser vendors came together to establish a higher security approach based on common standards.

The CA/Browser Forum created an advanced tier of SSL certificate with very high standards for validation and assurance, but also added more obvious browser security user-interface elements (e.g. colors, padlock location) and behavior.

The new certificates were referred to by different names as they were being defined — “High Assurance” and “Enhanced Validation” were considered — but “Extended Validation” was the final name chosen by the CA/Browser Forum.

It is important to note that these certificates are still fully compliant with the X.509 standards and are backwards compatible with older browsers.

Now that these new validation processes are in place, all CAs will use the same highly rigorous checks before issuing one of these new SSL certificates, and browsers detecting one of these certificates at a website can reflect the higher trust level in the user interface.

EV Adoption

EV SSL is universally supported by all desktop browsers and provides an EV trust indication. All mobile browsers support EV SSL and some provide an EV indication.

What’s in a Name?

The purpose of a certificate is to assign a key to an individual key-holder’s name.

There are many forms of name in common use. Some are unique, and others are shared. Some are meaningful, and others are meaningless. By virtue of the way they are assigned, domain names are unique but meaningless.

Certificates that bind a key only to a domain name do offer some protection against such attacks as HTTP response-splitting and ISP eavesdropping.

However, these are relatively uncommon. The most prevalent type of attack today, of course, is phishing. Domain-validated (DV) certificates offer little or no protection against this type of attack.

SSL Certificate Primer

Using certificates in SSL is based on public key cryptography. This paper won't attempt to explain public key technology in detail, but at a high level the Web server needs to create a mathematically related pair of keys — the private key and the public key. The public key portion of the pair is then put into an electronic document called a certificate and signed by a trusted CA.

For SSL server certificates it is important that the Web server's domain name (e.g., www.company.com) be present in the certificate, otherwise browsers will warn users that they may not be on a legitimate site.

From a human perspective, the Web server administrator begins this process by issuing commands in the Web server to generate the keys and to create a "Certificate Signing Request," or CSR. The administrator then submits the CSR to the CA, generally submitting it through a Web page. Workflow then begins at the CA to validate that the certificate can be issued as requested.

Before Extended Validation, requirements varied significantly between CAs, without an easy way for consumers to distinguish certificates issued using more- or less-rigorous validation processes.

Some CAs still are willing to issue certificates after simply checking that the requestor controls the domain name requested. This is accomplished by sending an automated e-mail to the administrator e-mail address listed in the Internet registry for the requested domain name.

The approach is very fast and convenient for both CA and for customers, but it introduces some risk in that spoofers can register a domain that looks very similar to a target domain. Harvard researchers demonstrated this risk and documented their findings.

Most CAs will check a business's credentials in more detail before issuing a certificate, but there are discrepancies in the level of rigor applied. Some CAs simply accept faxed copies of a company's utility bill.

Other CAs, like Entrust, have been more rigorous from the outset and will not accept information provided by the requestor at face value, instead looking up company registration information in trusted databases. They also will typically verify that the individual requesting the certificate is properly authorized by the organization by initiating phone calls to listed numbers for the company.

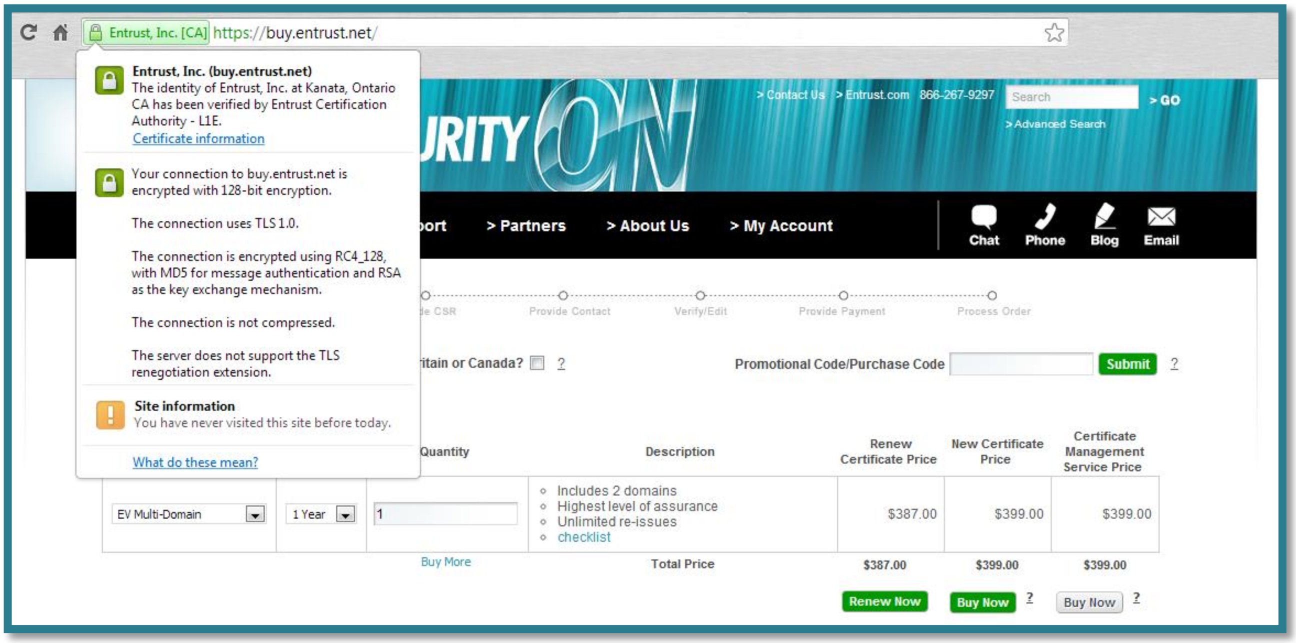
This inconsistency of validation processes between CA vendors was one of the key focus issues for the CA/Browser Forum.

Impact of Extended Validation SSL Certificates

Extended Validation SSL certificates have the highest impact on consumers, reassuring them that the site they are visiting is legitimate through visual cues in un-modifiable parts of the browser interface "chrome."

For example, the latest versions of Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, Opera and Apple Safari display the corporate name with a green background for sites protected by an Extended Validation SSL certificate.

In different manners, all highlight the entire address bar in green and displays the name of the CA (e.g., Entrust, Inc.) in a scrolling user interface (UI) element beside a more prominent padlock icon. Sites without Extended Validation SSL certificates simply have an address bar with a white background.



Entrust, Inc. (buy.entrust.net)
The identity of Entrust, Inc. at Kanata, Ontario CA has been verified by Entrust Certification Authority - L1E.
Certificate information

Your connection to buy.entrust.net is encrypted with 128-bit encryption.

The connection uses TLS 1.0.

The connection is encrypted using RC4_128, with MD5 for message authentication and RSA as the key exchange mechanism.

The connection is not compressed.

The server does not support the TLS renegotiation extension.

Site information
You have never visited this site before today.

What do these mean?

itain or Canada? □ ?

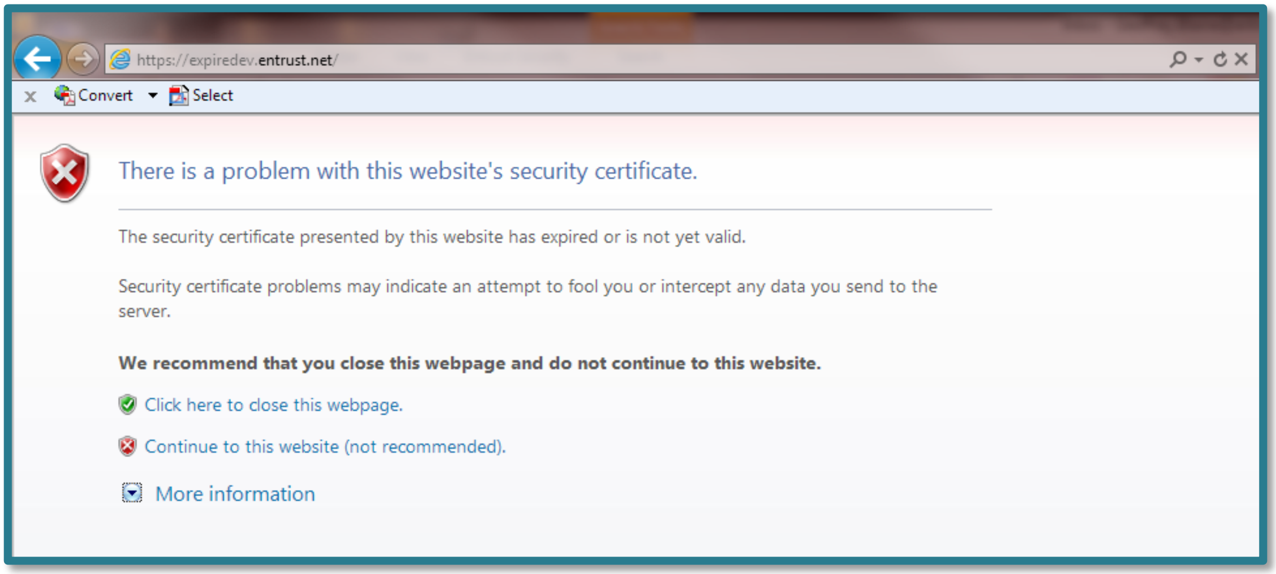
Promotional Code/Purchase Code

		Quantity	Description	Renew Certificate Price	New Certificate Price	Certificate Management Service Price
EV Multi-Domain	1 Year	1	○ Includes 2 domains ○ Highest level of assurance ○ Unlimited re-issues ○ checklist	$387.00	$399.00	$399.00
		Buy More	Total Price	$387.00	$399.00	$399.00

Google Chrome visiting a verified EV-enabled website, which gives detailed information about existing encryption, issuing certification authority (CA) and cryptography in use.

These prominent UI changes are widely accepted and expected by consumers, providing organizations with a proven tool to demonstrate to customers that they take security and privacy seriously.

Website operators will notice differences in the amount of information they need to provide to CAs during the initial validation process. Although certificate validity periods are now limited to two years, website operators using these certificates may notice that their information is revalidated by their CA after 12 months.



There is a problem with this website's security certificate.

The security certificate presented by this website has expired or is not yet valid.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Microsoft Internet Explorer visiting a site with an expired EV SSL certificate. A red "X" alerts the user that there is a critical issue with the installed certificate. The notification provides a recommendation on how to proceed and an option to view additional information.

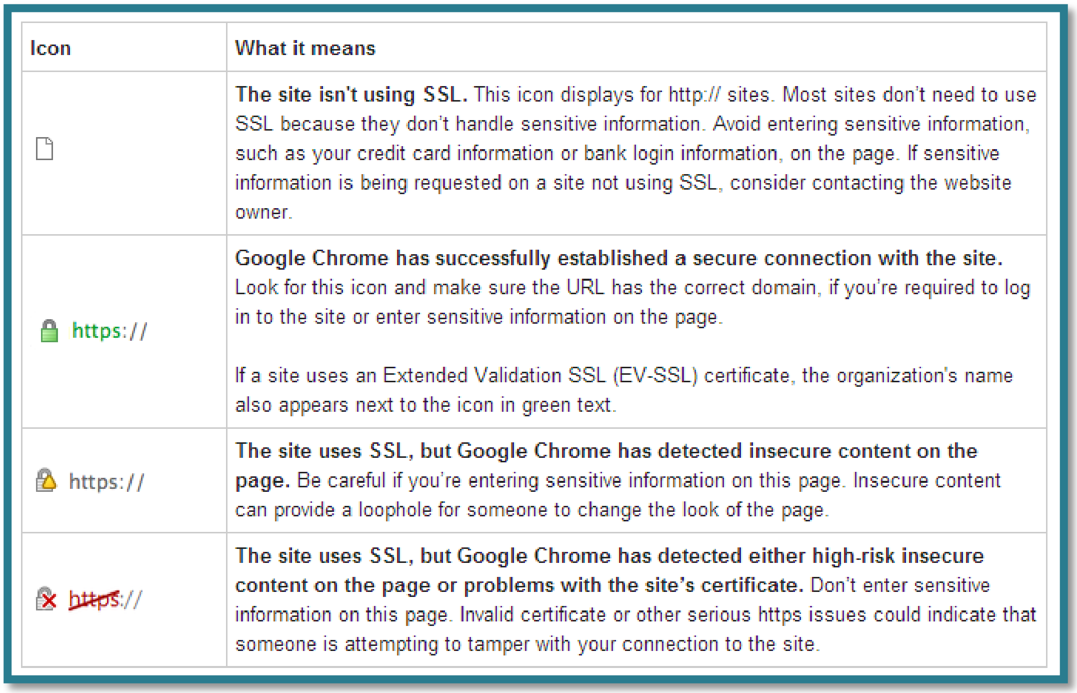
Browser Vendor Education

Many of the more responsible browser vendors are doing their best to educate consumers on the benefits of SSL and EV SSL and how the technology will protect transactions and communication online.

Google

Google, for example, provides an easy-to-understand[2] primer on browser and SSL security, as well as what the different elements of SSL communicate. Part of this includes a clear explanation[3] of what different browser icons mean.

Google: Website Security Indicators



Icon	What it means
🗋	**The site isn't using SSL.** This icon displays for http:// sites. Most sites don't need to use SSL because they don't handle sensitive information. Avoid entering sensitive information, such as your credit card information or bank login information, on the page. If sensitive information is being requested on a site not using SSL, consider contacting the website owner.
🔒 https://	**Google Chrome has successfully established a secure connection with the site.** Look for this icon and make sure the URL has the correct domain, if you're required to log in to the site or enter sensitive information on the page. If a site uses an Extended Validation SSL (EV-SSL) certificate, the organization's name also appears next to the icon in green text.
⚠ https://	**The site uses SSL, but Google Chrome has detected insecure content on the page.** Be careful if you're entering sensitive information on this page. Insecure content can provide a loophole for someone to change the look of the page.
✗ ~~https~~://	**The site uses SSL, but Google Chrome has detected either high-risk insecure content on the page or problems with the site's certificate.** Don't enter sensitive information on this page. Invalid certificate or other serious https issues could indicate that someone is attempting to tamper with your connection to the site.

[2] "Privacy and security settings," Chrome Help, Google.
[3] "Website security indicators," Chrome Help, Google.

Mozilla

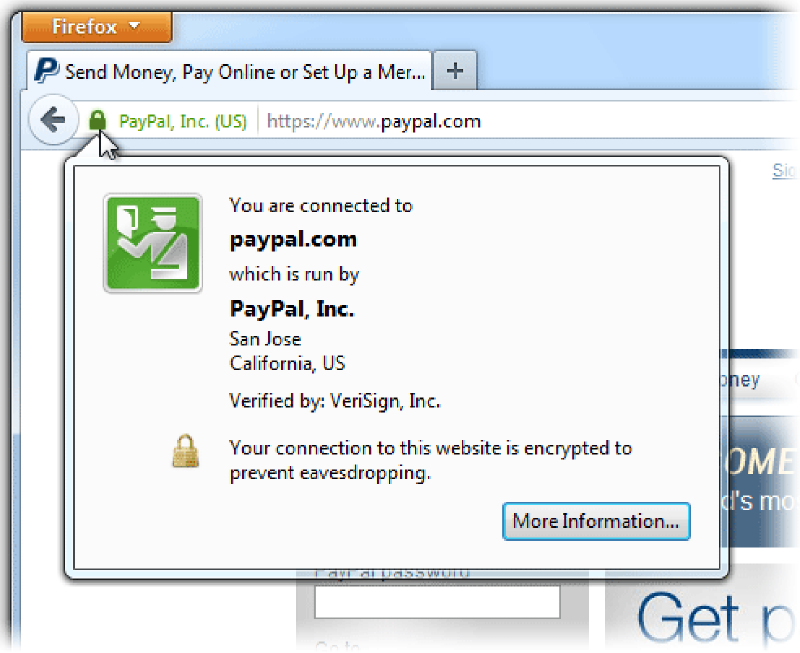
Mozilla, makers of the popular Firefox browser, provide step-by-step instructions[4] about the different browser security elements. From a “gray globe” to “green padlocks,” this consumer education is important for building general SSL trust.

The Green Padlock

Clearly seen, the green padlock is the easiest to understand for the typical user. Smartly linking the connotation of green with security, Firefox is informing the user that the site’s address has been verified via an extended validation (EV) SSL certificate.

Clicking on the padlock offers additional information about the website, operator, issuing CA (e.g., Entrust, Thawte, Verisign, etc.) and if the connection is encrypted.

As explained, EV SSL certificates require a much more rigorous vetting process, helping build trust in the online community.



You are connected to
paypal.com
which is run by
PayPal, Inc.
San Jose
California, US

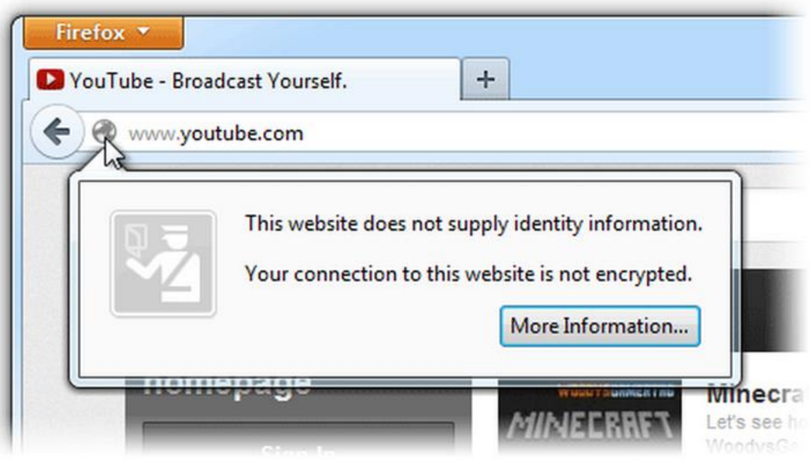
Verified by: VeriSign, Inc.

Your connection to this website is encrypted to prevent eavesdropping.

[4] “How do I tell if my connection to a website is secure?” Firefox Help, Mozilla.

The Gray Globe

In this example, Mozilla is showing end-users what Firefox will display if a website does not provide information about its identity. This “gray globe” also means that the connection between the browser and the site is either not or only partially encrypted.

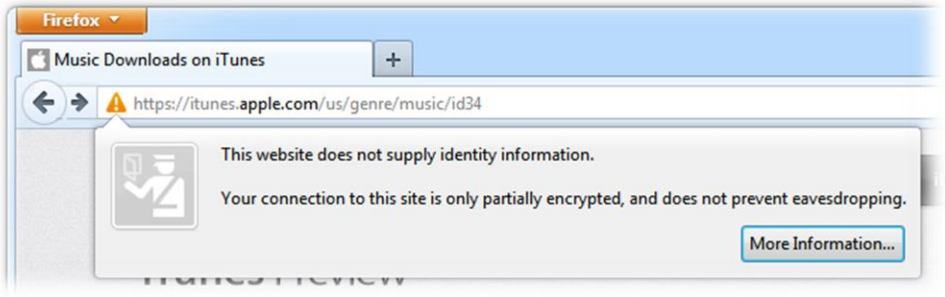


This website does not supply identity information.

Your connection to this website is not encrypted.

The Orange Triangle

What happens if an end-user receives an orange triangle like the one provided by Mozilla below? It tells the user that they’ve previously been to that specific site, allowing a mix of secure and non-secure active content, despite the risks.


Firefox
Music Downloads on iTunes
https://itunes.apple.com/us/genre/music/id34
More Information...

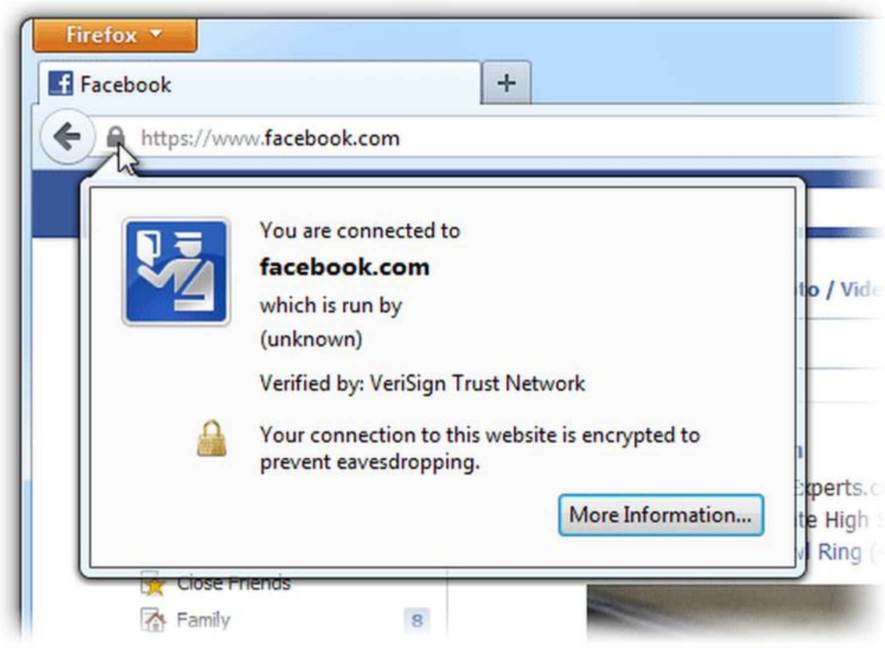
This website does not supply identity information.

Your connection to this site is only partially encrypted, and does not prevent eavesdropping.

The Grey Padlock

If a user experiences a “grey padlock” in Firefox, the connection is secure and the domain of the site has been verified via a provided certificate.

For additional information about the company and the CA who issued the certificate (e.g., Entrust, GeoTrust, Comodo, etc.), the user can simply click on the padlock.



You are connected to

facebook.com

which is run by

(unknown)

Verified by: VeriSign Trust Network

Your connection to this website is encrypted to prevent eavesdropping.

What Can I Do Now?

Entrust customers who wish upgrade to Entrust Multi-Domain Extended Validation SSL certificates can do so today, with minimal changes to their existing procedures.

Customers using large numbers of extended validation SSL certificates should consider switching to the Entrust Certificate Management Service in order to benefit from streamlined validation and the flexibility of the subscription approach to certificates.

For the latest information on this topic, please visit **www.entrust.net/ev.**

Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects,

Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

Now part of Datacard Group, Entrust offers software authentication platforms that strengthen security in a wide range of identity and transaction ecosystems. Government agencies, financial institutions and other enterprises rely on Entrust solutions to strengthen trust and reduce complexity for consumers, citizens and employees.

Entrust offers an expanded portfolio of solutions across more than 150 countries. Together, Datacard Group and Entrust issue more than 10 million secure identities every day, manage billions of secure transactions annually and issue a majority of the world's financial cards.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **entrust.com**.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 Globally

Headquarters

Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, Texas 75240

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

@Entrust
EntrustSecurity