GeoTrust℠
Internet trust.
Defined. Delivered.

white paper

QuickSSL™

Breakthrough automated authentication technology that provisions SSL server certificates in 10 minutes not four days.

SSL is the most widely used on-line secure transaction mechanism in the world. Until now, server certificate provisioning has taken four or more days. QuickSSL™ delivers industry-standard, ubiquitous SSL server certificates for secure browser-server interactions in real-time, while you wait. This is changing everything for Web merchants and Web hosting providers that want to get new businesses up, running and securely transacting. Painlessly. Quickly.

By Jothy Rosenberg, Ph.D.

Chief Technical Officer and Co-founder
GeoTrust Incorporated

With Dave Remy, Chief Architect and Co-founder

December 2001

GeoTrust Incorporated

40 Washington Street, Suite 20
Wellesley Hills, MA 02481
781.235.4677
800.944.0492

white paper

QuickSSL™

Breakthrough automated authentication technology that provisions SSL server certificates in 10 minutes not four days.

By Jothy Rosenberg

NETTING IT OUT

The SSL market is stable and rapidly growing because those who do any consumer transactions over the Web know it is must-have technology.

An SSL certificate is unnecessarily slow to provision at its current four days. This is because issuing certificate authorities use a manual process of authenticating the business behind a Web site.

The original stated goals for SSL were first, to provide confidentiality, which it does through encryption, and second, to provide server authentication so that transactions go to the expected server.

Web merchants are paying for authentication and business identity that SSL cannot deliver because SSL was never designed for this. Authenticated identity and validity is critically important in any on-line relationship but is not the domain of SSL. It is important to separate the concept of authenticated business identity from encryption. Both need to be addressed but SSL only deals with the latter.

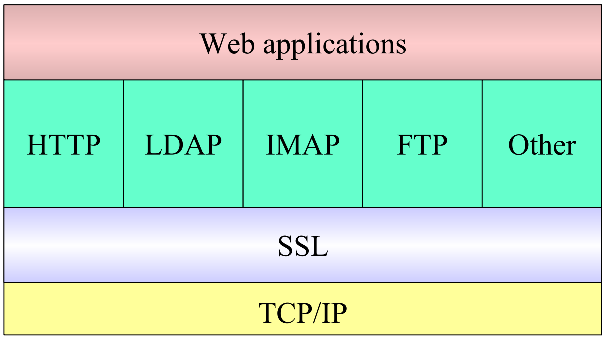
Automated authentication leading to real-time provisioning is breakthrough technology that changes the status quo and delivers real value to SSL buyers. GeoTrust has developed such technology and with its ubiquitous root behind its new QuickSSL™ product, and has delivered the first real-time SSL server certificate provisioning system to the market.

SSL INTRODUCTION

What is SSL?

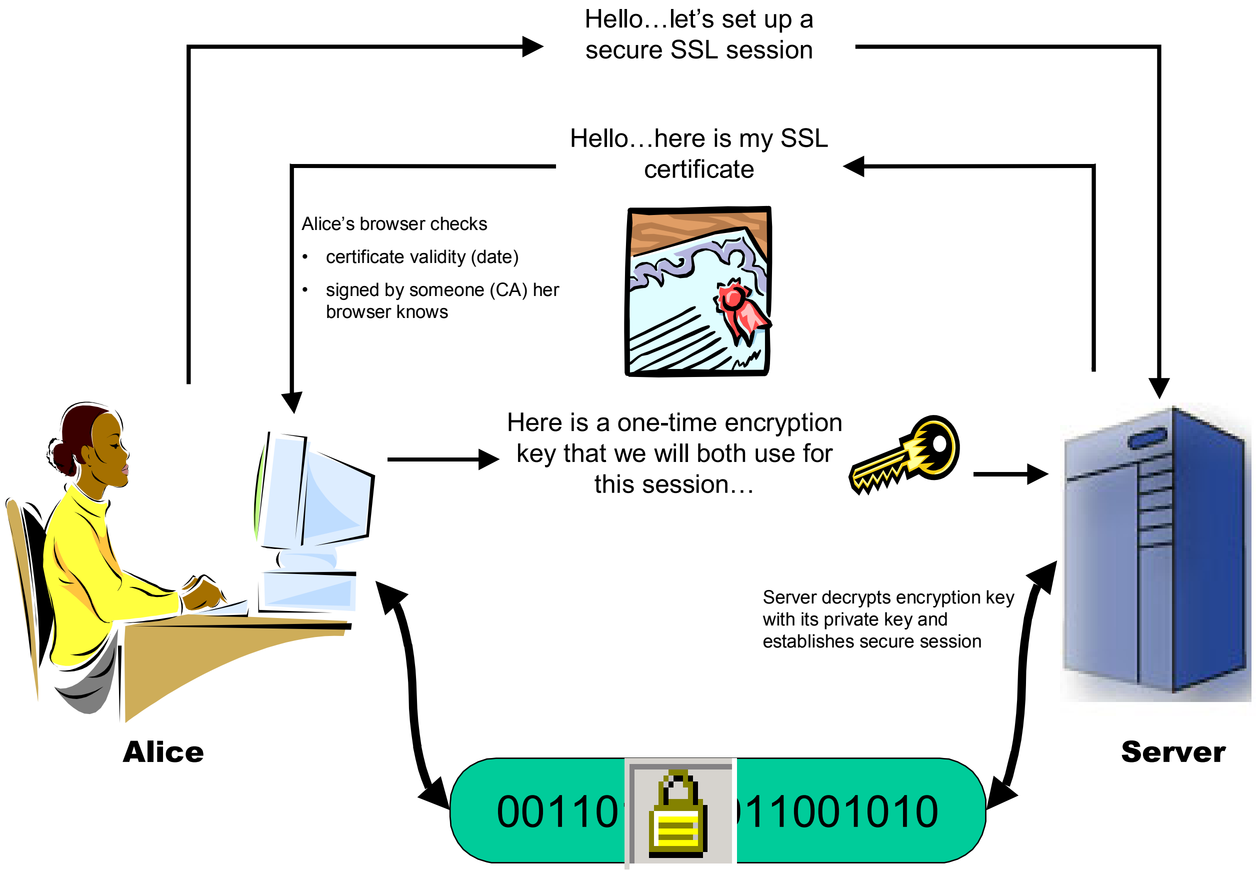
SSL stands for Secure Sockets Layer. A socket is a Unix term for a communications port between computers over any interconnection medium using any computer-to-computer protocol.

TCP/IP is the Internet protocol that governs the routing of data packets. Other protocols such as HTTP, LDAP, IMAP, and FTP run “on top of” TCP/IP. They are application protocols that utilize the services of the lower level TCP/IP. SSL runs above TCP/IP and below the application level protocols such as HTTP or LDAP making any protocol able to have secure, authenticated sessions.



SSL was invented and named by Netscape. The official IETF approved new name for SSL is Transport Layer Security (TLS) and it is virtually identical to SSLv3. We will continue to use the term SSL to refer to both SSL and TLS.

SSL is a way to create an encrypted transmission channel between a browser client and a server that thwarts eavesdropping or “man-in-the-middle” attacks. This is essential when sensitive information


Hello…let's set up a secure SSL session
Hello…here is my SSL certificate
Alice's browser checks
• certificate validity (date)
• signed by someone (CA) her browser knows
Here is a one-time encryption key that we will both use for this session…
Server decrypts encryption key with its private key and establishes secure session
Alice
Server
00110 11001010

such as a credit card number is being transmitted between a browser and Web server. The figure above diagrams how SSL between a browser and server gets set up and the browser lock symbol appears.

The main design goals for SSL were first, confidentiality and second, server authentication[1]. Technically what SSL builds on top of TCP/IP are three things:

1. SSL server authentication allows a user to confirm a server's identity. This translates into the browser lock symbol "lighting up".
2. SSL client authentication allows a server to confirm a user's identity. This is not used in typical merchant sites; this is used more typically in corporate networks in place of username / password sign on.
3. Encrypted data transmission makes sure that all information sent between a client and a server is encrypted by the sending software and decrypted by the receiving software. This provides a high degree of confidentiality and thwarts potential eavesdroppers or "men-in-the-middle".

[1] *SSL and TLS*, Eric Rescorla, Addison-Wesley, 2001.

Quick history

Netscape invented the SSL protocol in 1994. They then shipped a reference implementation in early 1995 filling a huge gap that had to be filled before the Web could be used for any kind of monetary transactions. By 1996 they had already created a stable SSL v3.0 which then became standard in Microsoft's IE browser and IIS Web server products as well as the Netscape products.

SSL has cryptographic underpinnings. The SSL protocol supports a variety of different cryptographic algorithms for use in operations such as authenticating server and client to each other, transmitting certificates, and establishing session keys.

Browser support for SSL in the form of public keys from certificate authorities embedded in all popular browsers is critical because for the lock symbol to light up and make the user confident, the browser must recognize the digital signature on the server certificate and to do that it must have access to the public key of the certificate authority.

For the same reason, SSL support is also enabled in all popular Web servers. When a new certificate is to be installed in a server, the server must recognize the signature of the CA on the new certificate.

A timeline of SSL evolution follows.

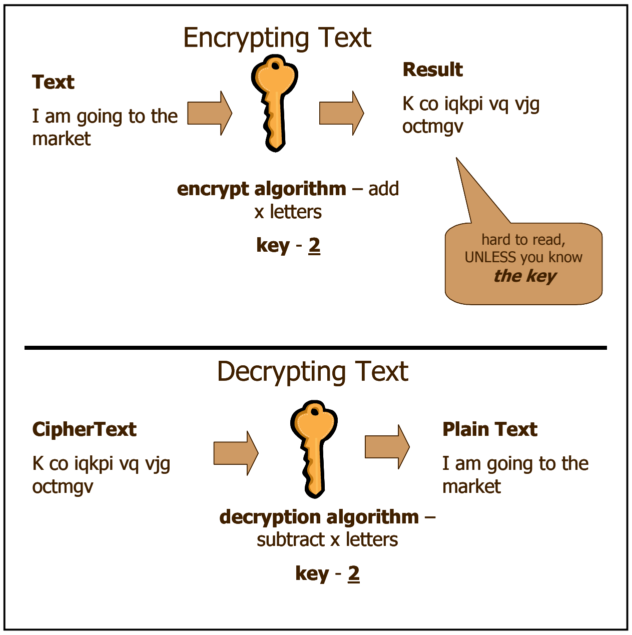
1994	Netscape invents SSL	10,000 WWW sites
1995	SSLv2 reference implementation	100,000 WWW sites[2]
1996	Stable SSLv3 created; VeriSign enters market	603,000 WWW sites
1997	Thawte enters market; IETF publishes TLS	1,681,000 WWW sites 12,000 SSLs found[3]
1998	Internet Explorer achieved parity with Netscape	3,689,000 WWW sites 32,000 SSLs found
1999	Equifax chains off Thawte and enters market	9,560,000 WWW sites 53,000 SSLs found
2000	VeriSign acquires Thawte	22,000,000 WWW sites 105,000 SSLs found
2001	GeoTrust acquires Equifax	30,500,000 WWW sites 120,000 SSLs found

[2] *Hobbes' Internet Timeline*, Robert H. Zakon, http://info.isoc.org/guest/zakon/Internet/History/HIT.html

[3] *Netcraft SSL Survey*, The number of secure Web servers found accessible on the Internet.

How it works

SSL is based on cryptography and for cryptography, we need a cryptographic algorithm (a mathematical recipe) and a key. A key is a strategy for encryption (scrambling) and decryption (un-scrambling) text (or just bits). Below we use a cryptographic algorithm that takes each incoming letter and adds X letters to each. Our key then is "what should X be"; in this case we chose the value 2.

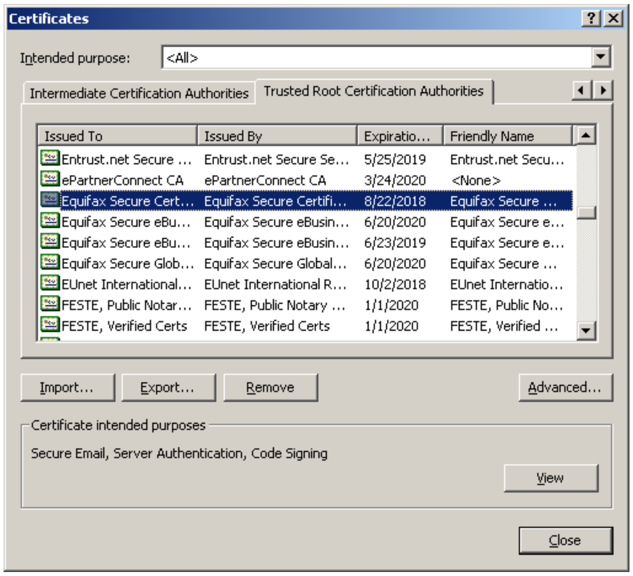


When the same key is used for encryption and decryption (as it was here) it is called symmetric cryptography. The same key is used at both ends of the process and it is computationally very fast.

Symmetric key cryptography is fast and secure and is what SSL uses. But it has a huge hairy problem: How do I safely get you the KEY? I have to find a secure way to get it to you AND, once you have it, I must TRUST you not to give it to anyone else.

This is the KEY EXCHANGE PROBLEM and is where public key (asymmetric) cryptography comes in to the SSL picture. It is computationally very expensive. Public key cryptography uses a key pair that are compliments of each other to solve this key exchange problem. The process to create these keys is as follows.

The browser initiates an SSL session with a server. The server responds by sending back its SSL certificate that includes its public key. The browser examines this server certificate and verifies that it is valid and that a recognized certificate authority (CA) signed this. For this to work, the public key of this CA must already have been embedded in the browser. This is true for a small number of CAs (about 25). The browser has a way for you to see all the CAs it is equipped to recognize as shown here.


Certificates
?
X
Intermediate Certification Authorities
Trusted Root Certification Authorities
Import...
Export...
Remove
Advanced...
View
Close

Intended purpose: <All>

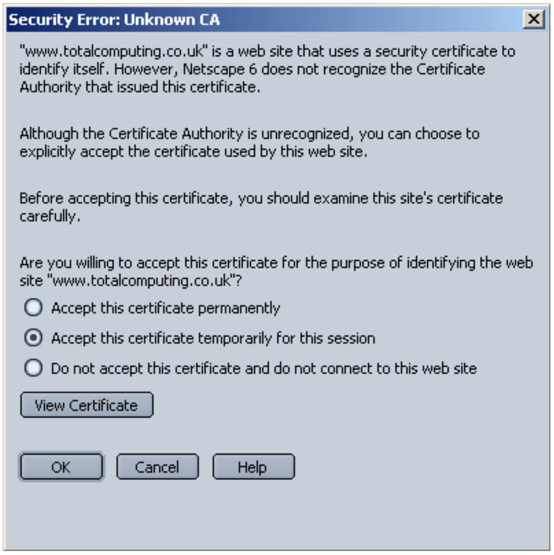
Issued To	Issued By	Expiratio...	Friendly Name
Entrust.net Secure ...	Entrust.net Secure Se...	5/25/2019	Entrust.net Secu...
ePartnerConnect CA	ePartnerConnect CA	3/24/2020	<None>
Equifax Secure Cert...	Equifax Secure Certifi...	8/22/2018	Equifax Secure ...
Equifax Secure eBu...	Equifax Secure eBusin...	6/20/2020	Equifax Secure e...
Equifax Secure eBu...	Equifax Secure eBusin...	6/23/2019	Equifax Secure e...
Equifax Secure Glob...	Equifax Secure Global...	6/20/2020	Equifax Secure ...
EUnet International...	EUnet International R...	10/2/2018	EUnet Internatio...
FESTE, Public Notar...	FESTE, Public Notary ...	1/1/2020	FESTE, Public No...
FESTE, Verified Certs	FESTE, Verified Certs	1/1/2020	FESTE, Verified ...

Certificate intended purposes

Secure Email, Server Authentication, Code Signing

If the public key of the certificate authority that signed the server certificate is not embedded in the browser, the browser will display nasty, frightening dialogs that will scare the user away from this site. This is worse than it sounds. If your browser does not recognize the authority of the CA that signed the certificate, you have no assurances about the server's identity whatsoever. The server has asserted its identity via a certificate, but this is nothing more than the bits the certificate is written on – you cannot verify that the assertion is correct.

It is a strange twist of original intent, but it is fair to say that the main goal of customers buying SSL certificates from trusted and established certificate authorities today is to make sure that the "untrusted or unknown CA" dialogs – like the one shown next –



Security Error: Unknown CA

"www.totalcomputing.co.uk" is a web site that uses a security certificate to identify itself. However, Netscape 6 does not recognize the Certificate Authority that issued this certificate.

Although the Certificate Authority is unrecognized, you can choose to explicitly accept the certificate used by this web site.

Before accepting this certificate, you should examine this site's certificate carefully.

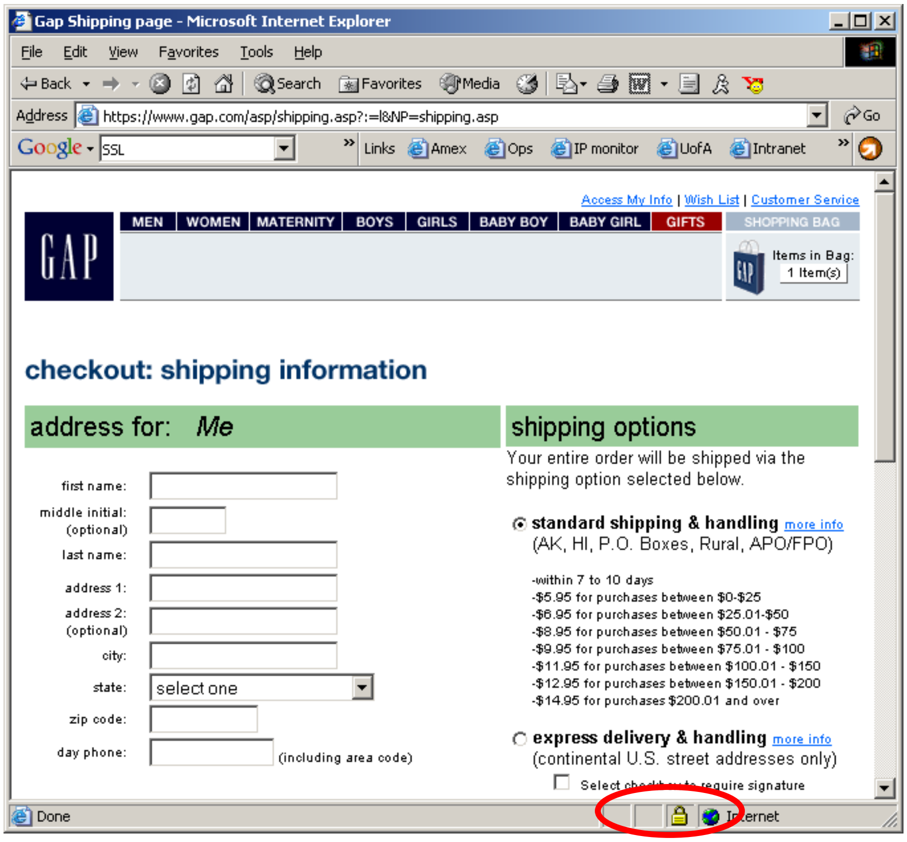
Are you willing to accept this certificate for the purpose of identifying the web site "www.totalcomputing.co.uk"?

○ Accept this certificate permanently
● Accept this certificate temporarily for this session
○ Do not accept this certificate and do not connect to this web site

do not appear. A base requirement for any viable CA therefore, is that their public key be in so many browsers that it is considered ubiquitous. From initial install into a new browser version, empirically this has been shown to take about three years. Only two SSL CAs have achieved greater than 90% ubiquity: VeriSign (under the root name RSA) and GeoTrust (under the root name Equifax) – both root names are non-obvious for historical reasons.

Once the browser has the server's certificate and it has verified it through the CA that signed it, the browser now generates a unique session key that will be used to encrypt all transmissions. The browser encrypts this session key with the public key of the server that was obtained from the site's SSL certificate. This encrypted session key is sent back to the server. The server decrypts this key using its own private key. The browser and server each generate a message to the other informing that messages will hereon be encrypted.

Finally, the browser creates or "lights up" the lock



Gap Shipping page - Microsoft Internet Explorer

Address https://www.gap.com/asp/shipping.asp?:=l&NP=shipping.asp

File Edit View Favorites Tools Help
Back Search Favorites Media
Go
Google SSL
Links Amex Ops IP monitor UofA Intranet
Access My Info | Wish List | Customer Service
GAP
MEN WOMEN MATERNITY BOYS GIRLS BABY BOY BABY GIRL GIFTS
SHOPPING BAG
Items in Bag:
1 Item(s)

checkout: shipping information

address for: *Me*

first name:
middle initial: (optional)
last name:
address 1:
address 2: (optional)
city:
state: select one
zip code:
day phone: (including area code)

shipping options

Your entire order will be shipped via the shipping option selected below.

● **standard shipping & handling** more info
(AK, HI, P.O. Boxes, Rural, APO/FPO)

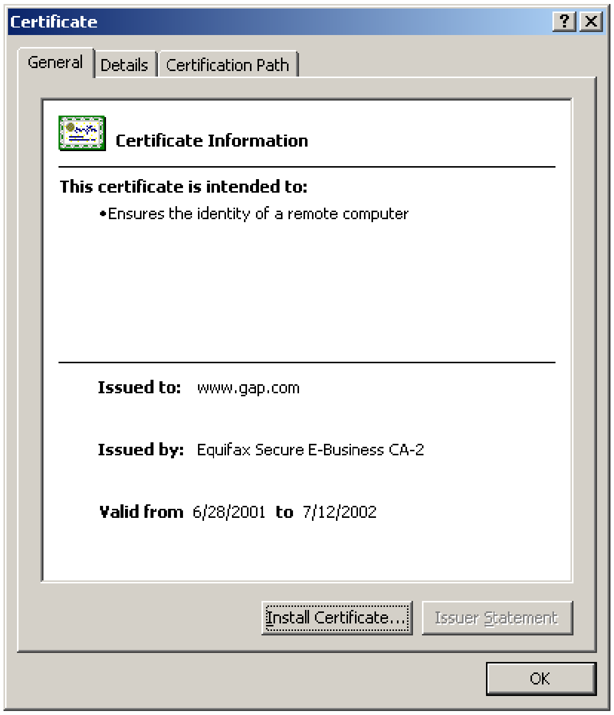
-within 7 to 10 days
-$5.95 for purchases between $0-$25
-$6.95 for purchases between $25.01-$50
-$8.95 for purchases between $50.01 - $75
-$9.95 for purchases between $75.01 - $100
-$11.95 for purchases between $100.01 - $150
-$12.95 for purchases between $150.01 - $200
-$14.95 for purchases $200.01 and over

○ **express delivery & handling** more info
(continental U.S. street addresses only)

□ Select checkbox to require signature

In this screen capture, note that the Address for the browser begins with **https** and the padlock symbol is shown in the bottom right of the browser window. These are indications that the browser and server are in SSL mode and transmissions are encrypted.

symbol that users have come to depend on to know it is safe to enter their credit card number. Unbeknownst to most browser users, that lock symbol is an active element that can be clicked. Clicking provides a view into the underlying server certificate which looks like this:



Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer

Issued to: www.gap.com

Issued by: Equifax Secure E-Business CA-2

Valid from 6/28/2001 to 7/12/2002

The process for obtaining a digital certificate is called vetting. The site owner enrolls with one of the certificate authorities who sells SSL certificates and is put through a business vetting process. This process was established in practical form early in the evolution of SSL by its earliest provider. The process involves providing business identity information to the CA that is then processed manually by someone who locates the business' license from the appropriate governing authority as well as their D&B credentials. They also determine, from an official corporate representative, that the person enrolling is authorized to do so. This entire process typically takes a minimum of four days. Once delivered, installation is a very quick process since the Web servers are all set up with automated procedures to take the certificate form from the CA and process it correctly to enable SSL transactions with browsers.

THE SSL PROBLEM

Overkill authentication

What typically happens in monopoly markets has clearly happened in this market: the virtual monopolist apparently stops innovating and may stop delivering value to customers. The primary example of this, in the author's opinion, is the expensive manual process that involves acquiring business license and contacting official representatives for authorization and verification. If there is not a perfect match between the official registered corporate name and that on the domain registration, the company is required to re-register the domain name to make the match perfect before the certificate can be issued. This is the process that has been used since 1995. It was flawed then and it is more glaringly flawed now. SSL never was designed to deliver any information about the nature of the business behind the server your browser is going to go secure with.

Yet the other major vendor persists with this extremely lengthy and intrusive process that each applicant for their SSL certificates must go through. But all of the information gathered during this authentication process is essentially thrown away because even the rare user that knows about the lock symbol gets to see none of the detailed information about the company collected before the certificate was issued.

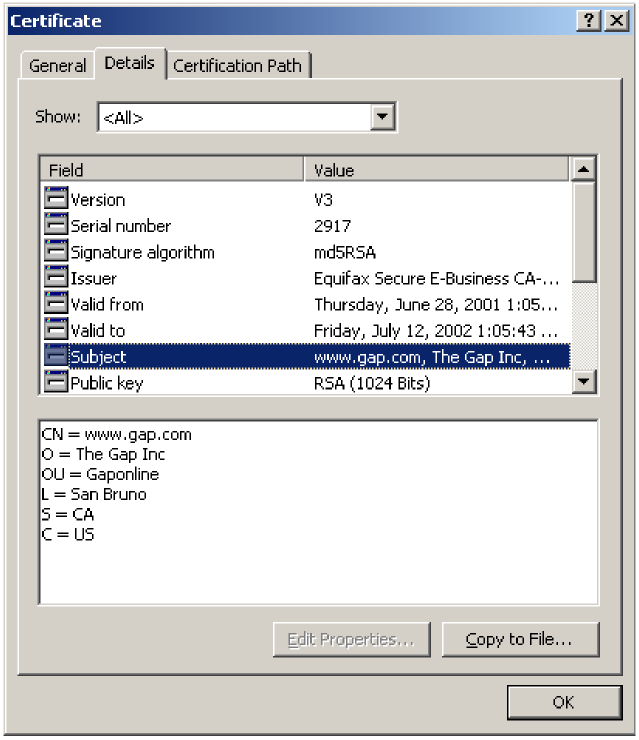
Provisioning takes four days

This laborious process means that the provisioning of an SSL certificate takes at least four days. This is unnecessary and punitive. Punitive not just to the customer but also to the Internet Service Providers who would otherwise be able to get new customers all they need to be up and live on the Web in real-time. A new Web entity can have the domain, the Web hosting, some initial Web design and even shopping cart services but they cannot start secure transactions for four days while they wait for their certificate to be provisioned.

Identity versus Encryption

The level of identity SSL does provide is that the server has been authenticated. And no matter what process is used, there is some information about the server provided in the certificate itself. That identity information is limited to name, city and state. No useful contact information is provided such as US mail address, phone number or email.

Getting at the information that is available is no small task as it requires clicks on the lock symbol, the Details tab and the Subject key as shown in the following dialog. Users don't know its there. Even knowledgeable users do not know the lock symbol is an active element that can be clicked. When they do click on it, they are not sure what to do next.



Field	Value
Version	V3
Serial number	2917
Signature algorithm	md5RSA
Issuer	Equifax Secure E-Business CA-...
Valid from	Thursday, June 28, 2001 1:05...
Valid to	Friday, July 12, 2002 1:05:43 ...
Subject	www.gap.com, The Gap Inc, ...
Public key	RSA (1024 Bits)

CN = www.gap.com
O = The Gap Inc
OU = Gaponline
L = San Bruno
S = CA
C = US

Users assume identity confirmation that is just not provided. For example, try purchasing a flight on United Airlines at www.ual.com. Once you have chosen a flight and want to start the purchase process, the pages still say United and have lots of clues that this is United Airlines. But check the certificate and you will find that very quietly this became a secure site at GetThere.com. We can safely assume there is a business relationship between United and GetThere but the point is that the user does not know this and continues to think they are at United and are about to give United their credit card. Identity was assumed and never verified. But the browser does authenticate the server and does establish encrypted communications that protect the user's credit card just as SSL promises to do.

The experts on SSL such as Eric Rescorla, the author of *SSL and TLS*, are very clear that this is how it is supposed to work: "we need to provide confidentiality of the data passing between client and server and the user needs to be sure that his client is connected to the right server." Bruce Schneiner is even more blunt in his book *Secrets and Lies*, "the main problem is that unless the user manually checks the certificate the server sent, he has no idea whom he went secure with. SSL establishes a secure connection between the browser and whomever is at the other end of the connection. If the user does not verify who is at the other end of the connection, he has no idea who he is speaking securely with. Its like entering a pitch black but secure soundproof room – no one can eavesdrop but you have no idea who else is in there with you."

When delivering a product based on a standard technology it is critical to understand what it can and cannot do. SSL is strictly about server authentication and legal ownership of that server and the domain that represents it on the Web.

Possible solutions

One proposed solution to this has been to promote what are called shared certificates. This is where an ISP has a single SSL certificate and all Web sites using this ISP can share this one certificate for their encrypted transactions. This means company A and company B will both be secured as isp.com not with their own domain names. The consumer cannot tell any difference between transacting with A or B – all the consumer would see is a certificate for isp.com – yet A and B may be very different in their reliability and trustworthiness. When consumers do see the lock symbol is for isp.com and not for companyA.com they tend to get worried and abandon their shopping cart.

Another way in which attempts have been made to deal with the lack of identity is through *seals*. A seal is a graphic icon issued by an independent third party that has an active component that will display confirming information if the browser user clicks it. These seals are quite prevalent on the Web from vendors such as TRUSTe, BBB, VeriSign, BizRate and others. But they all have several fatal flaws in implementation.

1. They require a click to get any identity information and that means only a fraction of browser users will see that information.
2. Seals are based on static image files that reside on Web servers so any site visitor that wants to can copy the image to their disk and subsequently to their Web pages. The incidence of pilfered seals is high.
3. If an entire set of Web pages is copied to a new location with the intent of *spoofing* the original site for some bad intent, seals do not alert the user and thereby do not in any way actually help confirm real identity of the visited site.

THE GEOTRUST SOLUTION

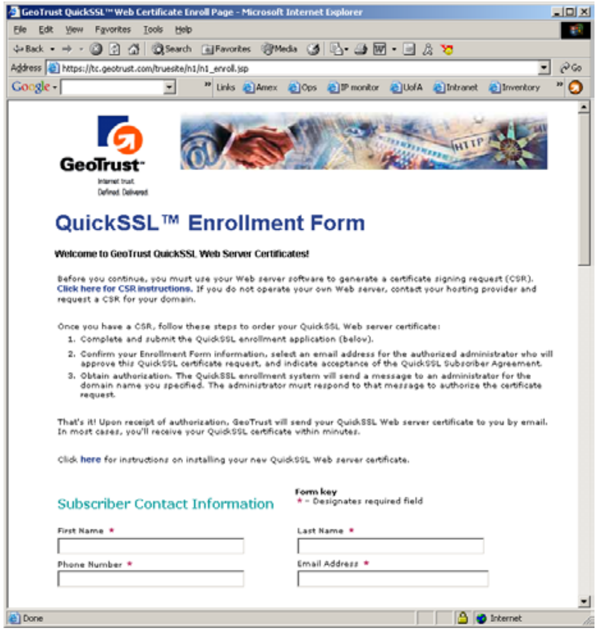
Automated authentication

GeoTrust understands SSL and on-line identity. Deeply. The GeoTrust SSL philosophy is to prove that a server represents its domain legally. What needs to be established is that the server resides at the domain claimed, that this domain is legally registered and the individual applying for an SSL certificate is authorized to do so by the authorities established for the registered domain. That is what SSL was designed to do and that is exactly what it delivers to the browser user – encrypted transmissions to an authenticated server.

Since the domain registrar databases are on-line, and since the authorized individuals established with the domain registrar are typically the same ones that would apply for a digital certificate, this process can be completely automated. This has led to 10 minute provisioning of SSL certificates.

Here is how the patent-pending QuickSSL automated authentication works:

1. A user enrolls at a Web form that asks for information about the individual's identity and the domain name being registered.



QuickSSL™ Enrollment Form

Welcome to GeoTrust QuickSSL Web Server Certificates!

Before you continue, you must use your Web server software to generate a certificate signing request (CSR). Click here for CSR instructions. If you do not operate your own Web server, contact your hosting provider and request a CSR for your domain.

Once you have a CSR, follow these steps to order your QuickSSL Web server certificate:

1. Complete and submit the QuickSSL enrollment application (below).
2. Confirm your Enrollment Form information, select an email address for the authorized administrator who will approve this QuickSSL certificate request, and indicate acceptance of the QuickSSL Subscriber Agreement.
3. Obtain authorization. The QuickSSL enrollment system will send a message to an administrator for the domain name you specified. The administrator must respond to that message to authorize the certificate request.

That's it! Upon receipt of authorization, GeoTrust will send your QuickSSL Web server certificate to you by email. In most cases, you'll receive your QuickSSL certificate within minutes.

Click here for instructions on installing your new QuickSSL Web server certificate.

Subscriber Contact Information

Form key
* - Designates required field

First Name *
Last Name *
Phone Number *
Email Address *

2. This individual will have already used his or her Web server to create a Certificate Signing Request which is an encrypted string of text that contains all the pertinent information including the server's public key needed by the Certificate Authority to issue the SSL certificate.
3. The last step in the enrollment process is for the individual to specify which of several approval email addresses to use. These names were pulled from the on-line domain registrar database. This works on the theory that the person responsible for the domain registration is most likely (more than 95% of the time) to be the same person requesting the SSL certificate or "is in the loop" and will quickly approve the SSL request..

4. The automated systems validate the data provided with the on-line registrar database and send out approval emails.

5. Typically the individual enrolling receives the email while still at the enrollment form and he or she can respond to it immediately.

6. Approval receipt then initiates the issuance of the SSL certificate by the CAs Certificate Management System – a special cryptographic computer in a very secure facility that uses special cryptographic keys stored in hardware to create and sign digital certificates that contain this server's public key.

7. The certificate is delivered to the individual via a link in an email message. That certificate is then put into the Web server's process to install a new SSL certificate.

8. DONE. The entire process typically takes 10 minutes or less.

Ubiquitous root in browsers

None of this would matter if the major practical requirement of SSL was not also met: the signature of the server's SSL certificate must be of a trusted certificate authority that has its root embedded in the vast majority of the world's browsers. GeoTrust's QuickSSL, like VeriSign's SSL certificates, passed this significant barrier to entry that takes about three years to achieve. Surprisingly, there are only two SSL vendors that have achieved 90% or higher ubiquity. Not even the grand-daddy of security – RSA – has this level of ubiquity, and no one else will for a couple more years.

Low cost structure

Besides 10 minutes versus four days, the fully automated process employed by QuickSSL means that the cost for each certificate issued is very low and this huge cost advantage can and is passed on to buyers. Furthermore, surveys through Web site hosting firms have shown that merchants who buy SSL certificates are not interested in any certificate authority insurance attached to the certificate. It sounds like a nice idea in theory. But in practice there are two reasons this is of dubious value. First is that merchants are typically taking credit cards when in SSL mode. The credit card companies are providing fraud protection. Second, the insurance terms attached to SSL certificates have fine print that says the only thing that is warranted is that the authentication process was followed. There is no coverage for losses from transactions nor is there any real coverage from fraud as long as they followed their prescribed process. The insurance underwriting is also expensive and adds significantly to the certificate cost. By not carrying unnecessary insurance this cost savings can also be passed directly on to the certificate buyer.

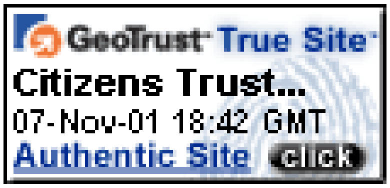
Real identity confirmation with TrueSite™

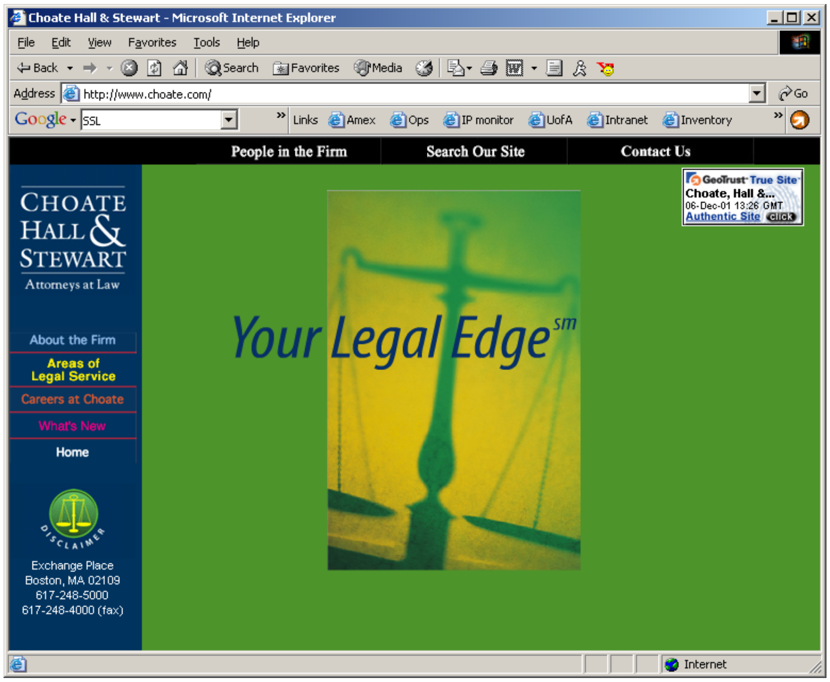
A separate white paper describes TrueSite in detail. Briefly however, True Site is a full business vetting process combined with a smart icon the delivers this confirmed identity to site visitors. It solves the major identity failures with all existing seals:

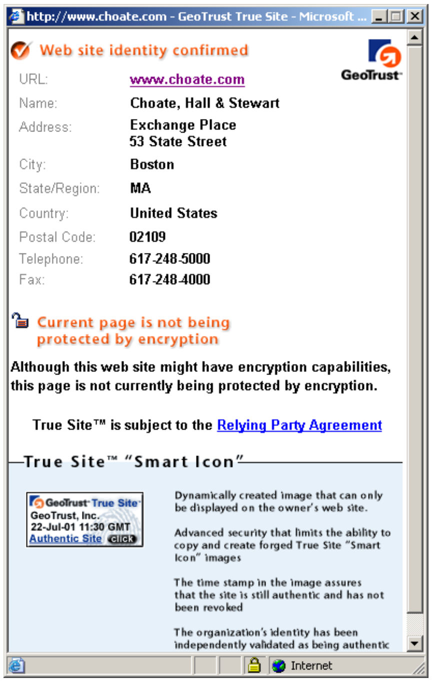
1. No click is required by a browser user to see that this is the business they expected it to be by virtue of the fact that the name of the business was dynamically embedded in the icon image before it is rendered by the browser.

2. The image is created by a secure server and is not pulled from a static file on the local Web server's disk. The image cannot be copied using simple mouse button clicks so it protects itself from pilfering. An example smart icon for Citizens Trust is shown below.

3. Site owners and site visitors are protected from common site spoofing because if the remote server is not given the correct domain name by the smart icon, it will not generate the image at all.







Web site identity confirmed

URL: www.choate.com
Name: Choate, Hall & Stewart
Address: Exchange Place
53 State Street
City: Boston
State/Region: MA
Country: United States
Postal Code: 02109
Telephone: 617-248-5000
Fax: 617-248-4000

Current page is not being protected by encryption

Although this web site might have encryption capabilities, this page is not currently being protected by encryption.

True Site™ is subject to the Relying Party Agreement

True Site™ "Smart Icon"

GeoTrust True Site
GeoTrust, Inc.
22-Jul-01 11:30 GMT
Authentic Site click

Dynamically created image that can only be displayed on the owner's web site.

Advanced security that limits the ability to copy and create forged True Site "Smart Icon" images

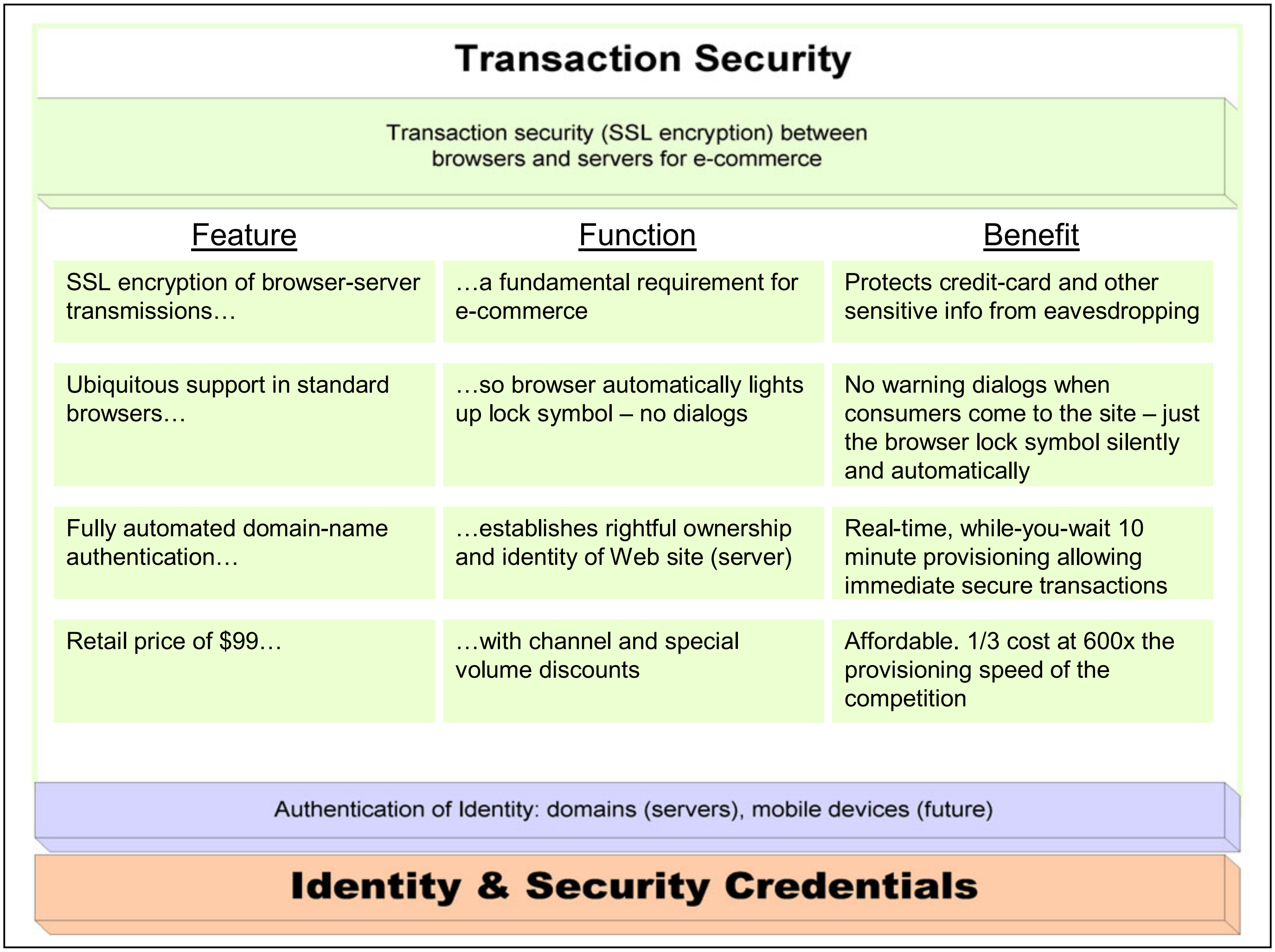
The time stamp in the image assures that the site is still authentic and has not been revoked

The organization's identity has been independently validated as being authentic

True Site is shown in the upper right hand corner of the browser window with the business name embedded in the dynamically generated image. A time-date stamp is embedded as well to further thwart any attempts at image capture. When the smart icon is clicked, the separate identity window on the right displays to show detailed, useful and actionable identity information about the business delivered securely from the repository of authenticated businesses.

QuickSSL™

The Features, Functions and Benefits of QuickSSL are described in the following table.



Transaction Security

Transaction security (SSL encryption) between browsers and servers for e-commerce

Feature	Function	Benefit
SSL encryption of browser-server transmissions…	…a fundamental requirement for e-commerce	Protects credit-card and other sensitive info from eavesdropping
Ubiquitous support in standard browsers…	…so browser automatically lights up lock symbol – no dialogs	No warning dialogs when consumers come to the site – just the browser lock symbol silently and automatically
Fully automated domain-name authentication…	…establishes rightful ownership and identity of Web site (server)	Real-time, while-you-wait 10 minute provisioning allowing immediate secure transactions
Retail price of $99…	…with channel and special volume discounts	Affordable. 1/3 cost at 600x the provisioning speed of the competition

Authentication of Identity: domains (servers), mobile devices (future)

Identity & Security Credentials

CONCLUSION

SSL has become an essential e-commerce commodity. It is by far the most widely deployed security protocol in the world. "Essentially every commercial Web browser and server supports secure Web transactions using SSL.[4]"

Browser users have been trained to expect SSL and many dutifully look for its activation through the browser's lighting of the lock symbol. Unfortunately, users assume it delivers benefits it does not. They think it will tell them that they are giving their credit card to the company whose graphic logos they see on the HTML page in front of them. But in fact, all SSL was designed to do – and which it does very well – is to establish a secure (i.e. encrypted) session between a browser and a server that has been authenticated.

SSL has a critical role in secure commerce on the Web and this is one of encryption but not of identity.

The SSL market has become dominated by a large majority market share player who currently has 94% market share and when last confronted by a small entrant to the market who successfully competed on SSL price, it purchased its competitor. Since then, they have kept prices extremely high and have added no value to their products. QuickSSL is certainly disruptive technology to this entrenched player.

The traditional approach to authentication this virtual monopoly player initially employed in 1995 is outdated and supports high prices and long lead times that means someone new to the Web will not get their SSL certificate for four days. They can get their domain name, their Web hosting support and even shopping cart and Web content services on the spot but they cannot do business for four days while they wait for their certificate to be provisioned.

GeoTrust's patent-pending innovative technology is driving down costs and making real-time provisioning a reality. The registrar databases for the largest top-level domains (such as .com) are on-line. Good Web-based back end processing is standard practice today. Complete automation of the enrollment, authentication and provisioning process makes it possible to acquire a certificate in real time and it means GeoTrust has much lower costs which are passed on to the buyer.

Finally, SSL provides a partial solution to secure transactions. Combined with an identity solution such as True Site™ both identity and encryption are provided for secure transactions. Know who you are dealing with first and then make sure the sensitive data to their server is secure with SSL.

[4] *SSL and TLS*, Eric Rescorla, Addison-Wesley, 2001.