



white paper

True Site™

Helping on-line companies create trusted brands so their site visitors feel confident enough to stay and pay.



By **Jothy Rosenberg, Ph.D.**

Chief Technology Officer & Co-founder
GeoTrust, Inc.

With Neal Creighton, Dave Remy, Chris Bailey, Michael Valdez

November 2001

GeoTrust's True Site™

Gives site visitors confidence that the site is safe and is backed by a real company. Gives site owners a tool to create a trusted on-line brand that will gain more transactions and more revenue. Makes consumers comfortable so they will stay and pay.

NETTING IT OUT

Identity and security are vital first components of brand. However, identity is critically uncertain on the Web. Spoofing or mirroring of Web sites is common and incidents are increasing. The Web creates a giant worldwide market but it is still very difficult to stand out and create a brand. Current solutions have failed to easily and reliably present identity. This includes SSL and the myriad of seals currently displayed on the Web. True Site is a secure, reliable "seal" that confirms identity and helps to build a brand. GeoTrust is a company focused on providing products and services that solve the Web's identity crisis.

This report includes the following major sections:

- A Web Brand Begins With Confirmed Identity
- Brands Damaged by Increasing Incidents of Spoofing and Hacking
- First Generation Solutions Have Failed
- True Site: Next Generation SITE and Business Identity Confirmation
- Conclusion: True Site's Confirmed Identity Solves the Web's Dirty Little Secret and Provides a Solid Foundation on which to Build a Brand

A Web Brand Begins With Confirmed Identity

A brand means that your potential customers think of you first. How do they know it's you on the Web? That's hard because the Web is fundamentally anonymous. Confirmed identity is needed. Your identity needs to be confirmed, clear, and visible at all times. Whenever potential customers are at your pages they need to see it is you, who you are, and how they can contact you.

Trust is at stake

The most trusted brands are the most trusted sites. Unknown brands are the least trusted. They have the most to gain by leveraging the inherent benefits of the Web. But they need to immediately gain consumer trust and brand awareness.

"The concept of trust is crucial because it affects a number of factors essential to online transactions, including security and privacy. Trust is also one of the most important factors associated with branding. Without trust, development of e-commerce cannot reach its potential."¹

Lack of Identity is the Web's "Dirty Little Secret"

URLs are complex, confusing, and easy to fake. They contribute little to establishing the identity of a site and the company behind the site – and therefore to brand.

In the bricks and mortar world, a company is identified by their buildings, their signs, advertising, brochures, and many other physical, hard-to-create, symbols. But the virtual company is

¹ *Trust in the Wired Americas*, Cheskin Research, July 2000; www.cheskin.com.

represented through its Web site by text and graphics no different from what a high school student can create.

Site information like text and graphics can be copied and fraudulently rehosted as a counterfeit or spoofed site. If someone can see your page, they can copy all of it wherever they want. They can stand between your legitimate site and your legitimate customers, all the while entirely controlling interactions.

Web site hoaxes, counterfeiting, and spoofing create enough misinformation that users feel like the Web is in anarchy.

What is at Stake?

The Web is growing at a rapid rate. More pages, more users, and even more transactions are added every day. But in spite of this growth, issues of trust impede the rate and the character of that growth. First, let's take stock of the Web as it is today.

Global Web opportunity at stake

In the summer of 2001, the Web is over 1.2 billion pages served from 30.5 million registered Web domains. There are 420 million Web users worldwide, 41% of whom reside in North America.² Within 5 years, it is expected that one-sixth of the world population will be using the Web. In terms of transactions, last year, \$40 billion in on-line retail transactions took place.³ Of that, \$565M per month was transacted in auctions of all kind.

The Web is an open community where for the first time in history, you can easily communicate with people all over the world quickly. You can buy a product from someone half way around the world. Since it is open, like any open community, it will have the bad elements of society in it as well as the good. These bad elements see easy pickings because of the inherent openness of the Web. And the more the Web is used for transactions and the flow of money, the more "opportunity" they see.

The fraud statistics are frightening. 90% of FBI surveyed companies had some breach in '99 with losses of \$265M as a

result. Hacking attacks went from 12 per day as of May 1999 to 61 per day as of March 2001.⁴

Brands Damaged by Increasing Incidents of Spoofing and Hacking

Security issues make people frightened and lose confidence.

Incidents of credit card and account theft are steadily rising and receiving a lot of visibility. A solution is vital to maintaining and building the Web as a platform for all types (not just credit-card) transactions.

How big is the problem?

According to the CERT⁵ organization that tracks security issues on the Web, there were over 20,000 security incidents last year and 2001 is on pace to equal or exceed that. "The volume of electronic business and associated crime is significant enough to merit an international effort" resulting in the US

FTC and 12 other countries agreeing to pool their resources⁶.

Site Counterfeiting (Spoofing)

A site is spoofed or counterfeited by making people think they are visiting the desired site but in fact they are actually visiting a "look-alike" site. M(pi1,z4volume of)9n not thioyan(y)13.9 thig -16te.ae r(i)-283(th -)7.1 the oflowing(spoo-16t27(eg)URLes)IJ5.52 0 0 5.52476.1 30

² Neilsen/NetRatings, July 2001

³ BizRate, July 2001

The spoofing process is simple and is based on the fact that one of the fundamental premises of the Web is openness: if you can see the page, you can see its source, and you can simply request that the browser save it to your own disk. From there, you can host it at a new location⁸ with a convincing URL.

The real damage then, comes from broadcasting the link via message boards, email, or some other broadcast mechanism as an employee of PairGain did to Yahoo! investors to get them to make his options gain in value.

Figure 1 shows a Bloomberg page that was spoofed. This actual spoof took under 10 minutes to accomplish.



Figure 1 – A Bloomberg page that was spoofed to say the opposite of what was intended. The described company actually laid off 100 workers.

Browser redirection

Browsers get “redirected” frequently for legitimate reasons. When you go to www.fidelity.com that is not where your browser ends up – it gets redirected to the best server fidelity has available for you at that moment. This is another aspect of the way the Web works that impedes a solid foundation of identity confirmation and brand. What is worse is that browser redirection is now a tool for bad guys to redirect your browser to the wrong site. Since this happens all the time, people don’t detect it until it too late and something bad has already

⁸ Free Web hosting is available from organizations such as angelfile.lycos.com.

happened. HTML links embedded in email messages is one very easy way this kind of redirection happens.

The Browser Lock Symbol Doesn’t Do What You Think

Secure Socket Layer (SSL) – the feature that creates the lock symbol on your browser – does not confirm identity. What it is designed for is encryption of sensitive information.

If your site is spoofed and rehosted on another site, it can have a legitimate SSL certificate that causes the unsuspecting user to see the lock symbol and feel confident they can now enter their credit card information.

Perhaps most damning about SSL is the simple observation that decisions are not made – and brand is not built – just on secured pages. Only 2% of the 30.5M Web domains are secured and then they secure less than 1% of their pages. This is because site owners are focused on securing pages where you enter a credit card number or other personal, sensitive information. But before you got there, you looked at a lot of (unsecured) pages that led you to make a decision. That makes it hard to say those pages were not important – all of a site’s pages work to build the brand. It is hard to say that confirming identity of the publisher of those pages is not important.

Web Spoofs, Hoaxes and Counterfeits

Spoofs, hoaxes and counterfeits all have in common that they create a shadow copy of a Web site – potentially this can be done for the entire Web. To get volumes of people to visit this site as opposed to the site they think they are visiting their browsers are redirected via links in a message board or an email message. The worst kinds of spoofs actually funnel all traffic to the legitimate target through the spoof site to monitor all activity. This way spoofters can get accounts, passwords, and other information all while the unsuspecting user is actually interacting with the site they wanted to but along the way bad things are happening with their information.

In all cases, pages have a familiar look because the actual look, feel and graphics from the legitimate site have been copied. It is even easy to make the URL appear legitimate – especially in light of the fact that URLs frequently get changed, expanded or even obliterated which “trains” users to discount their importance for identity verification.

Surprisingly, SSL doesn’t help. A determined hacker will set up the spoof on a site where they have acquired an SSL

certificate of their own. Then, the victim's browser says it has a secure connection because it does, but secure connection is to the wrong site. This is possible because SSL provides no clear indication of identity – it is focused only on encryption of sensitive data.

Many spoofs are truly malicious. Someone creates a mirror site that is disguised to be legitimate for some nefarious purpose. Web spoofing is a dangerous and nearly undetectable attack that can be easily carried out on the Web of today. "We do not know of a fully satisfactory long-term solution to this problem."⁹

Spoofing is certainly a serious problem but what is much bigger is misinformation on the Internet. The problem is that people are use to the "filtering" done transparently by magazines, newsletters, journals, encyclopedias, books, and so on.

We look for the brand of the publisher to establish trust. We can do that on the Web too if we (a) know the publisher and (b) believe that we are really at that publisher's site.

Search engines give the impression that we have found an authoritative source based on our trust of the search engine brand. But in reality, search engines are just creating an indexed inventory of the information found by a Web crawler examining all of the Web uniformly.

In the end, we must do the filtering for ourselves. So we need tools to do that with. The first tool is identity confirmation. The following table is a small sample of recent serious spoofs, hoaxes or counterfeits.

GWBUSH.COM	Malicious site purporting to be the official campaign site. It received a lot of publicity when the spoof was attacked by the George Bush campaign and then it received 6M hits in May 1999 while the official site received only 30K hits.
GATT.ORG	Spoof of the WTO site that got so much attention that the head of the WTO called a press conference to complain about the site and to publicize its existence since they could not stop it.
BLOOMBERG.COM	Most highly publicized incident of the past few years. April 1999 a counterfeit Web site put up on angelfire by an employee of PairGain. Complete look and feel of Bloomberg described PairGain as being acquired. Investors who read a Yahoo! message board were duped into investing \$63M all of which was lost.
PAYPAL.COM	Recent high visibility incident where Russian hackers spoofed the PayPal site and captured 16,000 credit card numbers.

Misinformation and Fraud Feeds Fear and Lack of Trust, Stifling Brand Creation, eCommerce and the Web

The only counterattack against the fear created by misinformation, hoaxes, and hacks is identity information about the information provider and vigilance by the Web user.

Brand value is being damaged daily

Two years ago, a famous spoofing incident occurred that caused thousands of investors to invest in a stock written about on a Bloomberg-looking Web page. After they lost \$63M do they think twice about trusting the next Bloomberg page? Will they switch to someone else's site for investment advice? Bloomberg thought so and sued both Lycos where the spoofed pages were hosted and Yahoo! where the message board resided that directed investors to the spoofed

⁹ Princeton University Department of Computer Science, Technical Report 540-96.

pages. All because Bloomberg suffered crippling brand damage due to this incident.

When the New York Times, WTO, and even AOL sites were compromised, their brands were also damaged.

Users are fearful

"Consumers see the world of the Web as one of chaos, offering both possibilities and threats.¹⁰" The natural reaction is to stay with known, *trusted* brands. But the Web is all about its global reach and exposure for all companies even those with no established brand. The way these no-brand sites break the cycle is to establish their identity, provide information about themselves and to have strong endorsements from 3rd party trusted brands.

Transactions limited

Until the fear is eliminated, it goes without saying that people will not enter into transactions of any kind where they perceive there is risk. There is not a perception of significant risk when buying books or flowers from known brands using a credit card because of the credit card protection mechanisms. But these same people won't buy from unknowns and will not enter into other kinds of transactions such as providing highly sensitive personal information (e.g. personal medical history).

First Generation Solutions Have Failed

Secure Socket Layer (SSL) is a standard feature of browsers designed to transmit confidential information securely over the net so no one eavesdropping can intercept the data and use it for their purposes. This feature is enabled by a Web site installing a special piece of cryptographic data called a digital certificate. If the browser has pre-installed in it, the root key for the Certificate Authority that signed the site's server certificate, then the lock symbol in the browser just appears which confirms the connection is secure. If not, then there are some confusing dialogs the user must go through.

The "failure" of SSL is that the unsuspecting user, while knowing he has a secure connection, does not know to whom this connection is really being made.

The entire world population of SSL certificates is only 700,000. That is 2% of the total world population of registered domain names. Sites typically don't use SSL on very many pages – just the ones where sensitive information is

¹⁰ *eCommerce Trust Study*, Cheskin Research and Studio Archetype/Sapient, January 1999; www.cheskin.com.

exchanged with the user – so only a very small fraction of the Web is "protected" by SSL.

Seals and Logos

Seals and logos are branded images that are licensed or granted to a recipient to convey acceptance, compliance, or endorsement of that recipient by an independent, trusted third party. They matter for the same reason that book and movie reviews matter and for the same reason that we look for and make decisions based on food and theater critic recommendations: we look to experts in a field to help us make smart decisions.

Sometimes the seal will convey that the recipient has the backing of a larger entity that will handle disputes and will take on liability for any transactions that occur. For example, the Better Business Bureau seal conveys confidence because the BBB has a formal process for handling disputes and complaints about a vendor.

Brick and mortar seals are important and they work because they are difficult to borrow or steal, they are policed, and they are easy to physically place on the door, trucks or yellow pages.


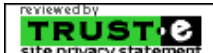
A new entrant to the Web, especially one that has no brand awareness, must address four traditional risks: effective branding, seals of approval, well-designed navigation, and order fulfillment. Cheskin further notes that effective branding comes initially from the endorsement inherent in seals of approval and confirmed identity. This is why seals are extremely important for smaller or lesser-known brands on the Web.

How Seals Work on the Web

An on-line seal starts with a GIF image. An HTML tag is created that references this GIF image and also may include a reference (hyperlink) to a remote server where the legal use of this seal can be checked. To get the most value from a seal, it is usually placed on or near the homepage. Resistance to placing seals on the homepage stems from the need to preserve real estate so most seals are placed near the bottom of the page. This means the seal is seen only if the user scrolls to the bottom of the page. Unfortunately, there are no agreed upon standards for how or where to place seals so users are not trained to spot them and when they do want to see them they have no idea where to look.

Because seals are just GIF images like any company logo or graphic image on a Web page, it is extremely easy to copy and rehost them. Even with the “click to verify” check, copying of seals to gain legitimacy is rampant.

Seal Types on the Web

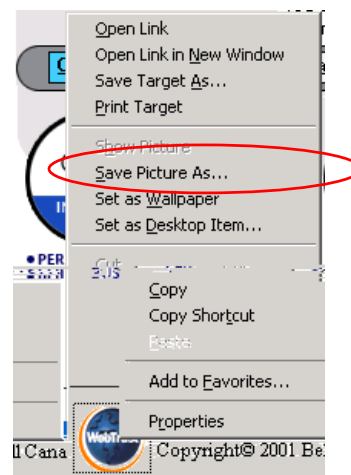
<p>Credentials</p> 	<p>There are thousands of credential seals from every kind of association. Here is one from the Engineers and Architects Association.</p>
<p>3rd Party Endorsements</p> 	<p>The Better Business Bureau is one of the most widely recognized seals in use today. It has 9963 seals. Their requirement includes being a member of the local BBB, agreeing to abide to truth in advertising and agreeing to work with the BBB to resolve customer disputes.</p>
<p>Badges of Trust</p> 	<p>This category is a general statement about the company and the Web site as opposed to being about membership in an association. The statement is backed up by some sort of audit of the site and the owning company as well. According to Cheskin, TRUSTe is still the most trusted symbol on the Web.</p>
<p>Paid Membership</p> 	<p>This seal is VeriSign's attempt to create an interface to the browser certificate information that is much easier to use and understand than that built into the browser. It is also an attempt by VeriSign to create a consumer brand. The only way someone can get this seal is to pay the \$350 annually for a site server certificate from VeriSign.</p>

How Seals Get Stolen on the Web

Just by doing an informal survey of seals on the Web we found rampant copying and display of seals that were not held legitimately. Clearly, the possession of these seals is

desirable because of the validity and legitimacy they stamp on the possessor. But this is also happening because the Web is so open and available that people are use to copying. And it is very easy to copy any seal you see on the Web to your site.

Anyone with a browser can copy a seal by pointing the mouse at the image, right clicking and selecting “Save Picture As...” from the pop-up menu shown here.



Confirmed Identity the Basis for a Solid Solution

One theme that comes through clearly when examining how fragile this current generation of seal is, is that static GIF images should not be their technological foundation. Instead, these seals need to be generated dynamically on secure remote servers. Only in this way can their veracity be assured. At the secure, trusted, remote site, the lookup can be done to confirm the identity of the site on which the seal is supposedly located. Identity of the seal owner is the most important aspect of the seal's value. Further security from fraud can be obtained by having the image difficult to reproduce such as by having it contain a unique watermark. If a time and date stamp is included in the image, then the image goes “stale” and no one can save it and post it to their site – it must remain dynamic in order to remain valid.

True Site: Next Generation SITE and Business Identity Confirmation

True Site Defined

A “smart icon” that is placed on Web pages that identity that the site is legitimate, authentic, and validated via an active call to a trusted third party. True Site’s Smart Icon is a seal that has the critical characteristics missing from most of today’s



seals. First, it considers the confirmation of site identity of the owner of most importance. Second, it is designed

to combat fraudulent usage. Third, it provides a “self-policing” capability that is unique to the Web. If it determines that it cannot confirm the identity of the site owner from which it is launched, it causes the image to completely disappear. Finally, it links to a rich repository of validated information about the site and its owner to assist the user – and ultimately the site itself. This establishes trust with the merchant that will hopefully lead to numerous transactions. This “business card” data we refer to as the “at a glance” page and is shown in Figure 2.

True Site for the Site Visitor

For the site visitor no extra work is required. No clicking on the icon. No going to a special checking site and entering in a domain name. It is a completely passive experience. The browser renders the page and as it does so, the smart icon requires that the trusted remote server render the image with the confirmed identity of the site owner and the time-date stamp embedded in the image. There are only two options: either the confirmation of identity is successful, in which case the image displays. Or the confirmation of identity was not successful so there is no image and the user is not subjected to fraudulent identity claims.

True Site for the Site Owner

True Site requires just a simple integration of an HTML tag to the desired page (usually the homepage). Just copy and paste the HTML text into the desired page. This thwarts anyone trying to install this on their unregistered site because it relies on a browser feature that passes the site’s URL it is on when it invokes a component on a remote site.

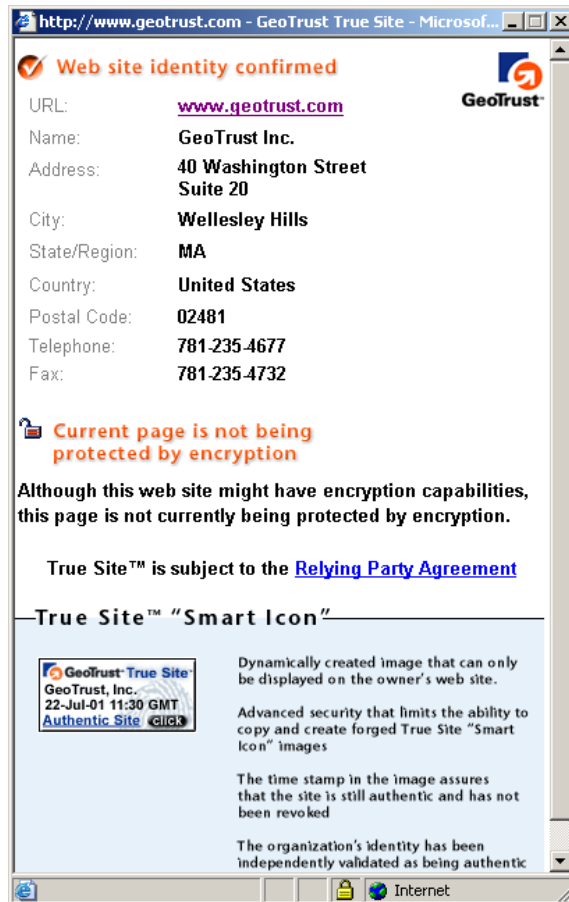


Figure 2 – True Site’s At-A-Glance business card data page

Frequently, enrollment in True Site occurs at the same time as enrollment for Web hosting. In this case, the Web hoster need only integrate either a link from their enrollment pages to True Site’s enrollment pages or at the end of the Web hoster’s process they can batch enroll by sending an XML form to GeoTrust.

Authentication of Business and Site Identity

We have described True Site from the user’s perspective. But the most important foundation on which True Site stands is the strong legal link that exists between a company and their Web site(s). When those domains are originally registered, legal information was required for billing, legal and technical contacts. Registration for True Site requires authentication of the business and link to the domain registration information. Once the authentication of the business and its legal contacts

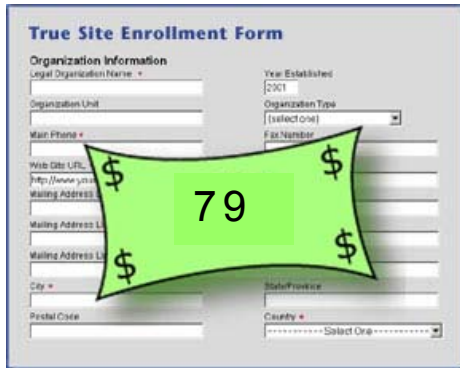
is completed and they are in the secure GeoTrust repository, the Smart Icon rendering can occur correctly.

At Smart Icon render time, the lookup by domain name consistently and reliably produces corporate ownership information from GeoTrust's authenticated corporate identity repository and embeds the name of that entity in the rendered image.

How True Site Works

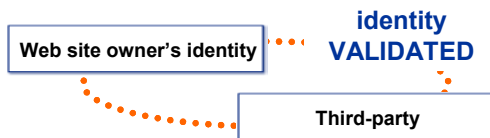
Enrollment and Authentication

- 1 The business completes an enrollment form and pays annual fee of \$79.

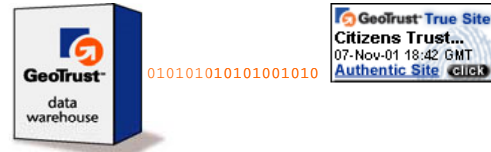


Access to enrollment can occur directly through geotrust.com or indirectly as processed by a Web hosting company.

- 2 Enrollment form submission kicks off the authentication process. An independent third-party validates the identity of the requesting company.



- 3 Information from the enrollment form is entered into the GeoTrust database and the site owner is provided with a True Site icon. The icon displays the business' identity on each Web page.

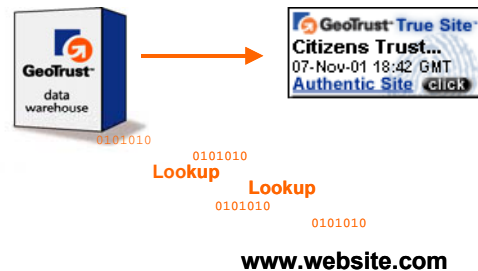


Smart Icon

- 4 The image tag that is inserted into the registered company's home page is simply this:

```
<!-- GeoTrust True Site[tm] Smart Icon tag. Do not edit. -->
<SCRIPT LANGUAGE="JavaScript" TYPE="text/javascript"
SRC="//smarticon.geotrust.com/si.js"></SCRIPT>
<!-- end GeoTrust Smart Icon tag -->
```

- 5 When a site visitor's browser hits this page and it gets to this HTML tag, it must first find the source for the image. The image is generated dynamically from a Java "servlet" at smarticon.geotrust.com instead of rendering this image from a local file or a static image via a URL, as is normally the case. Because it is a remote domain name, the browser passes the referrer information that provides GeoTrust's server with the domain name where the icon was found.



- 5 The server at smarticon.geotrust.com takes the referrer, performs a database lookup on it, extracts the corporate name, generates the dynamic image with the time-stamp, and returns the resulting image to the requesting browser who now displays it to the user.

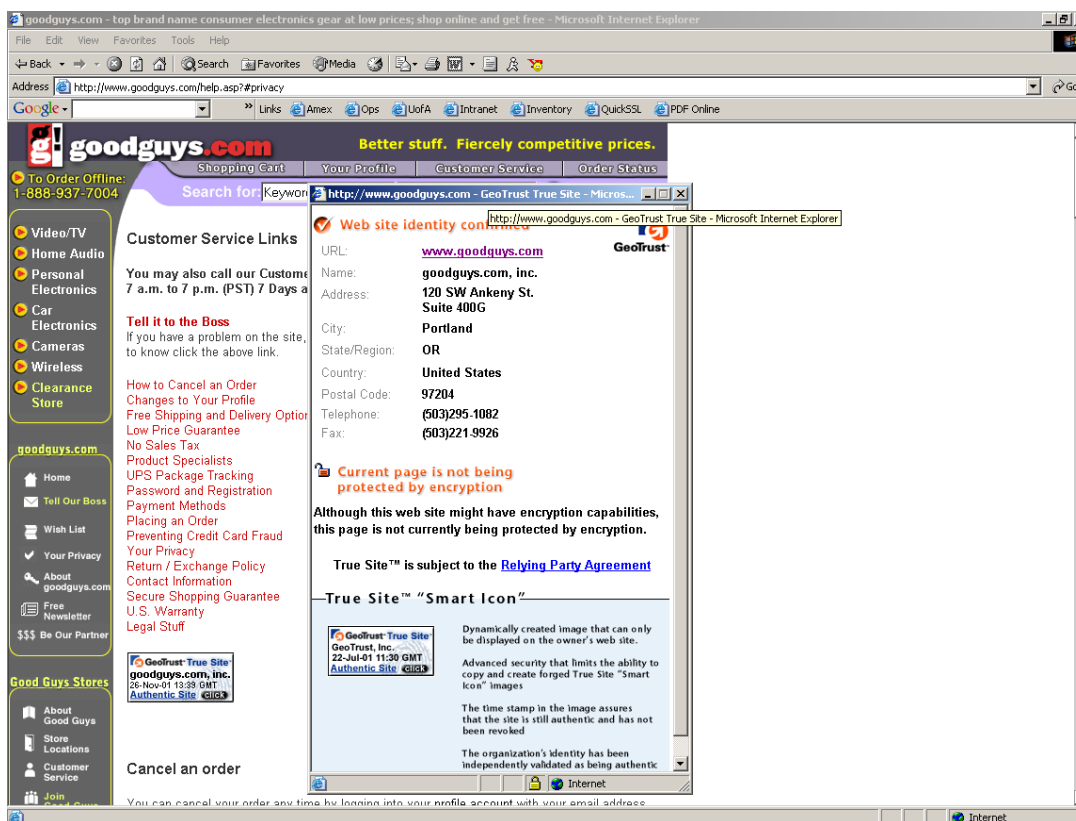


Figure 3 – The browser with a rendered Smart Icon and the At-A-Glance page created by clicking on the Smart Icon

If the lookup fails, the image returned is a 1-by-1 pixel invisible image indicating this site is not who you think it is.

At-A-Glance

- 6 A click on the icon causes a secure connection to True Site.geotrust.com to retrieve the at-a-glance business card data page as shown in Figure 3.

Here again, to stop redirection and spoofing, the referrer field provided by the browser is used to perform the database lookup. The presentation of this business card data is from a secure repository in a separate browser window, which allows the user to consult this page while still looking at the “business pages” presented by the visited site.

Why True Site Works

In light of the issues raised about all the extant seals on the Web, let’s examine why True Site is so effective.

Identity information provided passively

First of all, as Cheskin states in their most recent report, “All security symbols need to do more to communicate an ability to provide some measure of identity security.” Therefore, having reliable company authentication performed on all True Site registered domains and then presenting this confirmed identity passively without having the user required to click or do anything is critical.

The name that is presented to the user is not in terms of an obscure URL but is the legal, recognizable name. The active lookup by domain name done at geotrust.com assures the

seal is legitimate at this moment. The moment this site loses its right to this seal, it will be removed.

Referrer feature reliable key for lookup

We have to be certain a seal is not easily spoofable or it loses all of its value. The browser feature of providing the referrer information to any remote URL is a reliable mechanism for lookup of a domain. And mapping domains to legitimate companies is well understood. This combination gives True Site security, reliability, and a strong mechanism for prevention of spoofing and fraud. And while it is true that one browser could be hacked to not pass the referrer information correctly, it is impossible to hack all the browsers installed on people's machines.

True Site technology foils all but the most sophisticated and determined attempts at spoofing or fraud

In this section we will discuss all the known potential attacks against True Site and its Smart Icon and what technology in True Site stops these threats.

- 1 Copy icon to new page
This is totally ineffective because the icon not static – it is generated remotely and is dynamic. Any attempt to copy it renders it useless as an invisible 1-pixel image.
- 2 Copy entire page to new site
Since the page is moved to a new site it has a new domain name. That domain name (the referrer) is provided by the browser to smarticon.geotrust.com at the time of rendering. The new site name will result in a failed lookup in GeoTrust's authenticated company repository, which will return the invisible 1-pixel image.
- 3 Recreate look-alike icon
The watermark in the Smart Icon is very difficult to reproduce. Additionally, the time and date stamp means a sophisticated fake will have to create a dynamic image with the time and date stamp embedded in it.
- 4 Create fake business card data
One hacking attempt might be to capture the Smart Icon click to produce a phony at-a-glance page. But a secure connection to geotrust.com and the referrer information

sent by the browser used for lookup of confirmed identity prevents this threat from becoming a risk.

Metrics, Scalability and Performance

In this final section we document the performance and scalability data for True Site and its Smart Icon.

The GeoTrust True Site system can support over 900 connections per second. That correlates to over 77 million hits per day. The average latency time it takes for the browser to get the Smart Icon image is 0.04 seconds when there are 40 simultaneous browser's making the request. Even when there are 100 simultaneous browser clients the latency only drops to 0.10 seconds.

Conclusion: True Site's Confirmed Identity Provides a Solid Foundation on which to Build a Brand

The Web is anonymous, crowded and confusing. Fear – fear of fraud, fear of identity theft, and fear of eavesdropping – and the reasons for it are prevalent and increasing.

Brands cannot be created and nurtured this way. And, on-line business cannot thrive this way. A browser is only for product and service views – there is a strong need for a view into a business. Both consumer and business users need tools to help them establish on-line trust.

The basis for establishing a company's confirmed identity is an independent third party. GeoTrust is now established to authenticate companies worldwide. Furthermore, with True Site, GeoTrust has developed a compelling way to deliver business identity information to Web users.

True Site is a completely new paradigm for Web usage. A paradigm that will give site visitors confidence that the site is safe and is backed by a real company, site owners a tool to create a trusted on-line brand, and consumers comfort to stay and pay.



white paper