The Value of

Authentication

Authentication + Encryption + Certification Authority = Trust

thawte
it's a trust thing

1. Overview

One of the biggest problems facing your Internet business today is the thorny issue of trust and security. The vast majority of consumers are concerned about the safety of their credit card and personal details. People simply don't trust the Web, fearing that their transactions might not be safe. Not only are consumers concerned, the prospect of online credit card fraud also has an adverse effect on potential online shoppers.

Increased trust in the safety of online dealings has numerous benefits, of which increased revenue and profitability is the most important. There are real challenges – and significant opportunities – for e-tailers like you to deliver the same level of trust and personalization over the Internet as offered by real shops.

This guide will explain the critical role of authentication in online security as well as the business benefits which flow from creating trust on the Internet.

2. Surveys Emphasize the Importance of Internet Security

- Research done by the management consulting firm McKinsey shows that Internet users will become shoppers only when marketers overcome the lack of trust which paralyses many would-be buyers.

- According to a study done by Ernst & Young this year, 6000 e-shoppers in nine European countries stated that "honesty, respect and reliability" were the most important values concerning Internet shopping.

- A 2002 Webwatch survey found that only 30% of users trust Websites that sell products or services.

- An Ipsos-Reid survey of consumers in 16 countries found the security of credit card information in online purchases is a concern for a majority of consumers. Almost half of the 8 500 adults surveyed said the potential for online credit card fraud is a "major" concern (46%).

3. Online Fraud: How Bad is it?

Fraud on the Internet remains a huge barrier to consumer spending. A consistent source of fraud is customers doing business with entities they know little or nothing about.

Here are some facts regarding fraud on the Internet:

- More than $700 million in online sales was lost to fraud in 2001, representing 1.14% of total annual online sales of $61.8 billion, according to GartnerG2. Online fraud losses for 2001 were 19 times as high, dollar for dollar, as fraud losses resulting from offline sales.

- Fraud on the Internet is taking its toll on e-tailers, who are not only getting hit by Internet fraud, but by credit card companies as well, according to the Gartner Group. Gartner surveyed more than 160 companies and found that 12 times more fraud exists in Internet transactions than in traditional retail. Moreover, Web merchants bear the liability and costs in cases of fraud, while credit card companies generally absorb the fraud costs for traditional retailers, as long as the retailer follows procedures and saves the signature on the receipt.

- Interestingly enough, research from Jupiter Media Metrix showed that fears of online fraud are more common than fraud itself. "Online shopping gets a bad rap in the press, but most of the stories reported are anecdotal tales of companies that haven't put successful defensive measures in place," said Harry Wolhanlder, VP of Market Research at ActivMedia. "Web businesses running proper screening of customer information are suffering very little, with average fraud losses held to just over 1%. Fraud control is clearly possible online, although many companies do not implement stringent screening and prevention measures."

What is evident from the above is that Internet security should not only be monitored and managed internally, but most companies need expert advice, cutting-edge technology and a 24-hour emergency response team to make it work.

4. Beat the Risks with Authentication and Encryption

In person-to-person transactions, security is based on physical clues. Consumers have come to accept the risks of using credit cards in places like chain stores because they can see and touch the products and make judgments about the store.

On the Internet, without those physical cues, it is much more difficult to assess the safety of a business. Also, serious security threats have emerged. By becoming aware of the risks of Internet-based transactions, businesses can acquire technology solutions that overcome those risks.

But the Web poses a unique set of security issues, which businesses must address at the outset to minimize risk.

Spoofing:

> The low cost of website design and the ease with which existing pages can be copied makes it all too easy to create illegitimate websites that appear to be published by established organizations.   In fact, con artists have illegally obtained credit card numbers by setting up professional looking storefronts that mimic legitimate businesses.

Unauthorized Action:

> A competitor or disgruntled customer can alter your website so that it malfunctions or refuses to service potential clients.

Unauthorized Disclosure:

> When transaction information is transmitted "in the clear", hackers can intercept the transmissions to obtain sensitive information from your customers.

Data Alteration:

> The content of a transaction can be intercepted and altered en route, either maliciously or accidentally. User names, credit card numbers and currency amounts sent "in the clear" are all vulnerable to alteration.

A critical issue is how to win a customer's trust and convince all those millions of wary would-be e-shoppers that it is perfectly safe to make online purchases on your web site. The easiest and most secure way to achieve this is with thawte's foundation of authentication and encryption.

5. Why is Authentication Important?

In the age of faceless e-commerce, Authentication provides crucial online identity. Notions of identity and authentication are fundamental concepts in every marketplace. People and institutions need to get to know one another before conducting business. In traditional commerce, people rely on physical credentials – such as a business license or letter of credit – to prove their identities and assure the other party of their ability to transact online.

Authentication and security technology supports e-commerce transactions. These provide transaction security for e-commerce applications. Authentication is a must in order to achieve the necessary trust.

Information is a critical asset to your business. To ensure the integrity and safety of your information, it is important to identify with whom you are dealing, and that the data you are receiving is trustworthy. Authentication can help establish trust between parties involved in transactions.

This white paper focuses on how thawte provides the foundation needed to establish identity and create trusted relationships in the digital world.

6. Authentication: What you Need to Know

A complete understanding of authentication services demands a full explanation of each of the following areas:

6.1 **Establishing identity**

A business partner's identity must be established before it can be trusted in conducting trade. At the most basic level, there must be a process which verifies that an organization or individual exists, has a name, and is entitled to use that name. This process may also establish other identification attributes: for example, organizational affiliation ("Jim Smith works for Philips"); industry segment ("Vivendi is in the entertainment industry"); or occupational certification ("John Smith is a board-certified dentist in England"). Trusted third parties or delegated authorities often play a key role in confirming the identity attributes of participants at the time identification takes place.

6.2 **Credential management**

Once the participant's basic identity and identification attributes are established and verified, it must be issued with a credential that can be used to prove identity. In the "real" world, a credential might be an ID document or a business license. In the digital world, the most robust form of credential is the digital or Server Certificate signed by a trusted Certification Authority.

6.3 **How authentication works**

Authentication allows the receiver of a digital message to be confident of both the identity of the sender and the integrity of the message. When Web visitors connect to Websites, they reach one of two kinds of servers. If the servers are secure, visitors will get messages indicating that fact; similarly, if they are not secure, there may be warnings to that effect. A secure Web site is one that has been authenticated, a complex process involving public keys/digital certificates, and private keys. The certificate tells users that an independent third party has agreed that the web site belongs to the company it claims to belong to. A valid certificate means that users can be confident that they are sending confidential information to the place they think they are sending it.

7. The Role of the Certification Authority

A System Administrator generates a certificate request, which in turn creates two encrypted keys: one private, one public. The System Administrator sends off the public one to a trusted organization referred to as a Certification Authority (CA). The heart of trust in a public key infrastructure is the CA. Fundamental to this trust is the CA's root cryptographic signing key, which is used to sign the public keys of certificate holders, and more importantly its own public key. The compromise of a CA's root key by malicious intent, inadvertent errors, or system failures can be of catastrophic proportions. Hence, this root signing key must be diligently protected by the best technologies and practices within the cryptographic community.

The basic premise is that the CA is vouching for the link between an individual's identity and his or her public key. The Certification Authority provides a level of assurance that the public key contained in the certificate does indeed belong to the entity named in the certificate. The digital signature placed on the public key certificate by the CA provides the cryptographic binding between the entity's public key, the entity's name, and other information in the certificate, such as a validity period. For an end user to determine whether a legitimate CA issued the certificate, the end user must verify the issuing CA's signature on the certificate.

CA's must be absolutely certain that they are issuing certificates to the "correct" company. They must be sure that the company they are certifying owns the Internet Domain Name they have certified, that it is registered as a business in at least one country, and that its registered name is the same as that on the certificate the CA is signing. Once the CA has done what is, essentially, a background check on all these elements, the CA signs off on the public key. That comes back to the System Administrator, who loads it into the server. When both the private and public keys, a matching pair, align perfectly, the Secure Sockets Layer (SSL) will start functioning.

SSL, another critical element of a secure Website, ensures that the information sent by a server is identical to that received by a Web visitor - that no change has taken place.

8. What is Encryption?

Encryption is the security technology, which protects the privacy of information sent over a network. Encryption changes a data stream of bits from information to something that appears random.

Encryption alone • Trust, but Authentication + Encryption + Certification Authority = Trust

Anyone who intercepts the encrypted data gets a data stream that doesn't represent any information. It is noise, garbage, and worthless data. In a well designed system, only the intended recipient is able to decrypt the encrypted data stream to recover the information. However, encryption does not guarantee trust and authentication.

8.1 Why is encryption important?

Web or eBusiness systems may hold data that you wish to protect, such as business critical or personal information. Encryption increases the security of data transmissions, reducing the risk of third-party observers being privy to content. Encryption can also be used for stored data. Encryption can help protect your web site or eBusiness information assets from unauthorized access.

8.2 How does encryption work?

On the Internet, there are two main uses for encryption. One occurs when you visit a "secure" Website, such as an online store or shopping mall. This is called server-side encryption because it uses the Server Certificate given to the server (computer) that runs the Website. The other use occurs when you send or receive encrypted e-mail. In both cases, the encryption process involves exchanging public keys.

When encrypting information, the encryption process is done with either a public or a private key and then decrypted with the matching public or private key. Think of it as a lock that requires one key to close the lock and another key to open the lock. For example, when you visit a secure Website, your computer receives the Website's public key. When your computer sends information to the Website, your computer encrypts it using the Website's public key. The only way to decrypt the information you are sending is with the web site's private key.

The same process is needed for secure e-mail. Before you can send someone an encrypted message, you need their Server Certificate, which contains their public key. Your e-mail application uses their public key to encrypt the message. From that point on, only the recipient's private key can decrypt the message. So, you can distribute your Server Certificate (and its public key) to as many people as you would like without harming the integrity of your Server Certificate. However, you must guard your private key, since it is used to decrypt any messages sent to you.

User authentication can be employed to determine which areas of information are available to any particular user. There are two main types of authentication to consider: message authentication and user authentication. Message authentication establishes that the message says what it is supposed to say and comes from where it purports to come from.

9. How Can I Tell If A Website/Company Is Authentic?

Before submitting information or purchasing goods, you need to know that the company you are doing business with is who it claims to be.

Web shops can buy Server Certificates from many different companies (CAs). But your applications are configured to trust only those Server Certificates that come from a few highly reputable companies. So, if someone sends you his or her Server Certificates (either via e-mail or from a Website you visit) and it is from a CA that your application does not trust, you will get an alert message asking if you want to trust the new CA.

You should in fact trust only those sites that have been verified and authenticated by a trusted third party such as *thawte*.

thawte's Digital Certificates provide a means of proving your identity in electronic transactions much like a driver's license or a passport does in face-to-face interactions. With a thawte Server Certificate, your customers and business associates can be assured that *thawte* has verified your business registration, domain ownership and that the person authorizing the certificate is employed by you.

10. The Benefits to Your Business

Authentication gives you the edge. An authenticated and secure Website can provide your business with powerful competitive advantages. A certificate from thawte enables trusted online sales and application processes for products such as insurance, mortgages, or credit cards.

With authentication you can reassure visitors to your site and give them the confidence they need to purchase things, because they will trust you.

You can reach those customers who will submit information via the Web only if they are confident that their personal information, such as credit card numbers, financial data, or medical history, is secure.

11. Secure Your Online Transactions with thawte – Make Online Shopping Safe

After you install your *thawte* Digital Certificate, your server enables SSL (Secure Socket Layer) technology, creating a secure communications channel between your server and your customer's browser. Your site can communicate securely with any customer who uses any browser (Netscape Navigator, Microsoft Internet Explorer etc) Once activated by your Server Certificate, SSL immediately begins providing you with the following components of secure online transactions:

Authentication:

By checking your Server Certificate, your customers can verify that the Website belongs to you, and not an impostor. This bolsters their confidence in submitting confidential information.

Message privacy:

SSL encrypts all information exchanged between your web server and customers, such as credit card numbers and other personal data, using a unique session key. To transmit the session key to the consumer securely, your server encrypts it with your public key. Each session key is used only once, during a single session (which may include one or more transactions) with a single customer. These layers of privacy protection ensure that information cannot be viewed if unauthorized parties intercept it.

Message integrity:

When a message is sent, the sending and receiving computers each generate a code based on the message content. If even a single character in the message content is altered en route, the receiving computer will generate a different code, and then alert the recipient that the message is not legitimate. With message integrity, both parties involved in the transaction know that what they're seeing is exactly what the other party sent.

The ultimate result of a thawte SSL Certificate on your site? Safe online transactions that protect both customers and your business. Customers gain confidence that they are sending their personal information to a legitimate business and not an impostor. In turn, you know that your company is receiving accurate information that the customer cannot later refute.

12. Make Online Commerce Easy for your Customers

When you install a *thawte* Server Certificate, the 100 million prospective customers with Microsoft and Netscape browsers are reassured that they are shopping on a trusted secure site. Visitors can be sure that transactions with your site are secured by looking for the following easy cues:

- The URL in the browser window displays "https:" at the beginning, instead of "http:"

- In Netscape Communicator, the padlock in the lower left corner of the Navigator window will be closed instead of open. Netscape users can also follow these steps to see what level of encryption is protecting their transactions with your site:

    o   Go to the Website you want to check.
    o   Click the Security button in the Navigator's toolbar. The Security Info dialog box indicates whether the Website uses encryption.
    o   If it does, click the Open Page Info button to display more information about the site's security features, including the type of encryption used.

- In Internet Explorer, a padlock icon appears in the bar at the bottom of the IE window. IE users can find out a Website's encryption level by following these steps:

    o   Go to the Website you want to check.
    o   Right-click on the Website's page and select Properties.
    o   Click the Certificates button.
    o   In the Fields box, select "Encryption type". The Details box shows you the level of encryption (40-bit or 128-bit).

13. How Can Businesses Become Authenticated and How Can They Prove That to Their Customers?

A company can buy an authentication certificate from a Certification Authority (CA) such as thawte. Or they can purchase it from the Internet Service Provider that hosts their site.

As mentioned earlier, a digital or Server Certificate can be compared to a business license. Server Certificates are issued by a trusted third party, called a Certification Authority (CA). The CA that issues a Server Certificate is vouching for your right to use your company name and Web address.

14. Why are thawte's Authentication Services Better?

Our business process is efficient and secure and we offer the fastest reasonable turnaround time on certificate requests – WITHOUT compromising the reliability of our process.

Before issuing a Server Certificate, *thawte* reviews your credentials and completes a thorough background checking process to ensure that your organization is who it claims to be, and is not claiming a false identity. Then thawte issues your organization with a SSL Certificate, which is an electronic credential that your business can present to prove its identity or right to access information.

A Server Certificate from thawte provides the ultimate in credibility for your online business. thawte's rigorous authentication practices set the industry standard. thawte documents its carefully crafted and time-proven practices and procedures in a Certificate Practices Statement. Employees responsible for dealing with certificates undergo complete background checks and thorough training. thawte has achieved its unsurpassed reputation as a trusted third party by paying as careful attention to physical security as electronic security.

thawte's rigorous verified authentication practices and ultra-secure facilities are designed to maximize your confidence in our services. These practices and infrastructure are the foundation for Server Certificates to secure transactions working in conjunction with your Web server.

We believe in trust and full authentication and we are willing to fight for it. We are the right people to persuade your customers to trust your business.

15. Conclusion

thawte Technologies is a Certification Authority (CA) which issues SSL Web Server Certificates and 128-bit SuperCerts to organizations and individuals worldwide. *thawte* verifies that the Organization ordering the certificate is a registered organization and that the person in the organization who ordered the certificate is authorized to do so.
thawte also checks that the organization in question owns the relevant domain. *thawte* digital certificates interoperate smoothly with the latest software from Microsoft and Netscape, so you can rest assured that your purchase of a *thawte* Web Server Certificate will give your customers confidence in your system's integrity - they will feel secure about transacting online.

16. Useful URLs

Get a FREE SSL Test Certificate:

http://www.thawte.com/ucgi/gothawte.cgi?a=w28050095287014000

Buy a fully authenticated SGC SuperCert:

http://www.thawte.com/sgc/index.html

17. Contact *thawte*

Should you have any further questions regarding the content of this guide or *thawte* products and services, please contact a Sales Advisor:
E-Mail: sales@thawte.com
Telephone: +27 21 917 8902
Fax: +27 21 917 8967