What is the point of encryption **if you don't know who for?**

Dr. Colin Walter

Head of Cryptography **- Comodo Inc.**
Chairman of Peripherals Working Group **– Trusted Computing Group.**
Co-chair **- Cryptographic Hardware and Embedded Systems.**

April 2005

What is the point of encryption **if you don't know who for?**

INTRODUCTION

Phishing is the fastest growing threat in the history of Internet and has gained immense popularity amongst Internet fraudsters and hackers as a simple yet effective way to gain unsolicited access to confidential user information. Using social engineering tactics, fraudsters ensure that the trust relationship established by a company with its customers is exploited to maximum effect. It is for this reason that moving towards stronger identity assurance techniques is the only long term strategy that will maintain the stability of the Internet.

Identity and authentication are fundamental concepts in every marketplace. People and institutions establish trust before conducting business. Traditionally there has been a reliance on physical credentials such as a business license or a letter of intent. In the age of the Internet, e-business will only succeed if this ability to pass trust remains consistent. Authenticated SSL certificates have been proven to provide the critical online identity assurance necessary to establish trust between parties. In fact the future success of a multitude of e-commerce eco- systems rests directly upon the continual strengthening of that trust relationship.

WHY DO WE NEED ENCRYPTION?

The Web presents a unique set of trust issues, which businesses must address at the outset to minimize risk. Consumers submit information and purchase goods or services via the Internet only when they are confident that their personal information, such as credit card numbers and financial data, is secure. The solution for businesses reliant upon e-commerce is to implement a complete e-commerce trust infrastructure based on encryption technology.

Let us take a closer look at "encryption". The dictionary[i] definition is:

en·crypt Pronunciation Key (ĕn-krĭpt)
tr.v. **en·crypt·ed, en·crypt·ing, en·crypts**

1. To put into code or cipher.
2. *Computer Science.* To alter (a file, for example) using a secret code so as to be unintelligible to unauthorized parties.
3. The manipulation of data to prevent accurate interpretation by all but those for whom the data is intended. Financial institutions use encryption to increase the security of data transmitted via the Internet.

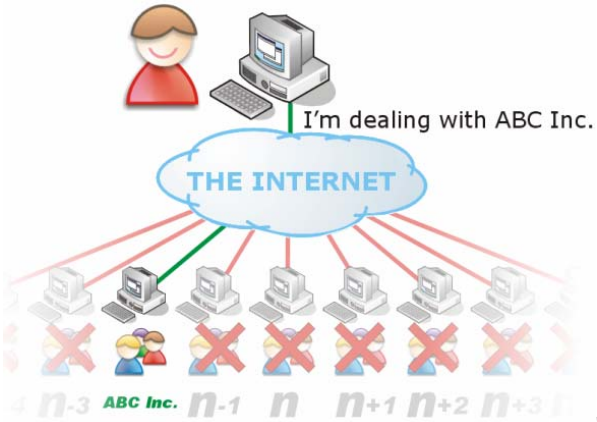
So in essence encryption is the process of transforming information to make it unintelligible to *all unauthorized parties* except *the intended recipient* and forms the basis of data integrity and privacy which is necessary for e-commerce. What this means is that the whole purpose of encryption is to make sure that the intended recipient is the only one who receives in intelligible form the information which has been encrypted.

Unless you have authenticated the **"intended recipient"** how do you know who that entity is? The answer is you don't! So it would be fair to say from the definitions above that, **if you don't know who you are encrypting for, then encryption is potentially pointless**.

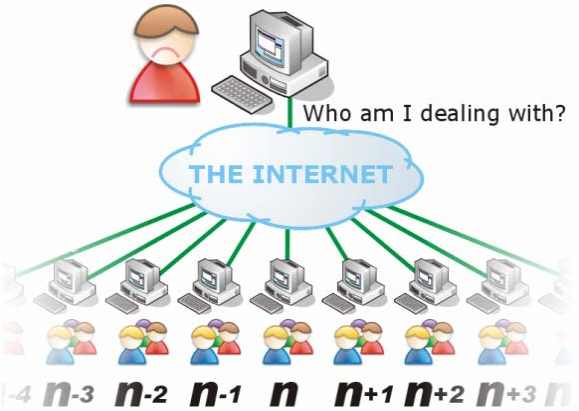
"High Assurance" certificate authorities (CAs) perform that authentication for you with due diligence, and put their name to this in the SSL certificates which they sign. This is not done by "Low Assurance" CAs who issue SSL certificates providing encryption of dubious worth. Let's look more specifically at other legal, technical and commercial issues facing consumers and businesses where entity authentication is not performed.

Should consumers take a 60,000,000:1 gamble on privacy and confidentiality?

Today, new web site registrations are running at approximately 5 million new domains per quarter with a cumulative total of over 60 Million[ii]. Without a pre-existing trust relationship, consumers have no trusted method available to verify the ownership of a web site and therefore are completely reliant upon the entity authentication processes performed by Certification Authorities. If no authentication process is performed then this forces consumers to gamble with privacy and confidentiality.



With "authentication" consumers can identify the entity with whom they wish to communicate.



With no "entity authentication" 'n' is approximately 60,000,000 and growing at 55,000 per day.

Enterprises and businesses which force users to gamble private and confidential information will lose out to those whose identity can be established directly from their SSL certificate.

Let's look at SSL itself in more detail.

[i] http://dictionary.reference.com/search?q=encryption, definitions copyright of Houghton Mifflin Company

[ii] http://news.netcraft.com/archives/web_server_survey.html

What is the point of encryption **if you don't know who for?**

What is SSL?

Established by Netscape in 1994, the SSL protocol is now widely accepted as a method of providing confidentiality, authentication and integrity for on-line transactions. Companies such as VeriSign and Comodo deliver high assurance certificates to individuals and organization's following a subscriber authentication process that includes verification of the organizations existence, the organization's right to use the domain name included within the certificate and the authority of the requester to obtain a certificate on behalf of the organization.

The original concept from Netscape[iii] stated:-

> *"Third-party CAs are critical for some applications. For example, a bank that wishes to put a server on the Internet for online banking cannot just issue its own certificate to that server and ask customers to believe that it really is the bank's server. Instead, the bank will purchase a server certificate from a third-party CA. The third-party CA takes responsibility for performing due diligence and ensuring that the company requesting the certificate really is the company it says it is before issuing the certificate."*

The use of SSL certificates is a critical building block for secure electronic commerce and one of the most ubiquitous uses of public key infrastructure (PKI). SSL certificates are "High Assurance" if they provide three security services – confidentiality, authentication and integrity. They enable a user to:

- Communicate securely with a web site – Information which the user then provides cannot be intercepted in transit (confidentiality) or altered without detection (integrity)
- Verify that the site is actually the company's web site and not an imposter's site (authentication)

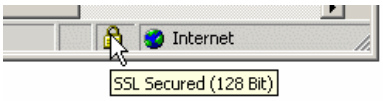
For example, an SSL certificate with the organizational name "ABC Software Inc." is intended to provide assurance that the Web site being viewed (e.g. www.abcsoftware.com) is actually an ABC Software Inc Web site (and not a "spoofed" site created specifically by another, unrelated entity to trick unsuspecting web surfers into doing business with someone pretending to be ABC Software Inc.)

Why is it important? A domain name URL (uniform resource locator) is equivalent to a telephone number. It is assigned to a paying customer (organization or individual) for the period of time it is registered.

The domain name system was designed to support open-systems information flow. While there are restrictions on certain types of domains (e.g. .mil is restricted to US military entities, .fr is restricted to organizations physically located in France), there are no such restrictions on .com, .org, .net and others. To register for these types of domains the individual or organization need only pay an annual fee. **There is no requirement for registrars to verify the accuracy of the information provided.**

With multiple browsers available to view the Internet, the importance of providing a consistent assurance mechanism to an Internet population of greater than 1 Billion individuals is paramount. The architecture of leading Internet browsers available from Microsoft®, Mozilla Foundation, Opera® and others was originally constructed in such a way as to provide assurance through the use of simple icons (in the form of locks and keys).

However, **changes in the SSL certificate marketplace have posed a significant security risk** with a huge potential threat to consumer confidence in the security of online commerce.



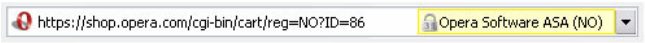
Internet Explorer

Firefox

Internet Explorer does not differentiate between *high* and *low* assurance certificates. Even more recent browsers like Firefox, although displaying the signatory authority, still require in-depth analysis by the user of the certificate itself.

Due to the practices of Low Assurance certification authorities, the padlock can no longer be assumed to symbolize trust

Browser providers have recognized this. The latest version of the Opera Browser (8.0) now has the ability to display organizational (entity) information directly from the web site's SSL certificate.



Entity information is available from the SSL certificate.

No Entity information is available – Encryption is of unknown worth and so trust cannot be established.

Authentication of an organization

Providers of low assurance SSL certificates do not perform all the necessary checks, choosing instead to offer a reduced cost, rapid fulfillment model. This is in direct conflict to accepted industry practice and serves as a source of distrust, confusion and fear for internet users. Whereas in the past it was merely acceptable to rely on the lock symbol, users without tools like Opera must now examine and understand the contents of the SSL certificate, in order to distinguish between the varying levels of assurance. In some cases users may need to refer back to the CPS (Certificate Practice Statement) to be able to understand the level of assurance provided. Industry standards for subscriber registration require that a certification authority (CA) maintains controls to provide *reasonable* assurance that:

- Subscribers are properly identified and authenticated,
- Subscriber certificate requests are accurate, authorized and complete.

A certification authority's code of practice is detailed in a CPS (Certificate Practice Statement) or disclosed within the CA's published certificate policy (CP). There are three fundamental verification steps necessary to be able to issue an SSL certificate to an organization:

- Domain ownership – Does the organization or individual have the right to use the Domain identified on the certificate?
- Confirmation of legal status – Is the organization a legal entity?
- Confirmation of the requestor's authorization – Does the individual making the request have authorization from the organizationto make the said request?

The importance of the validation steps are identified in the risk table below. In general, an internet user incurs a higher risk if

[iii] http://wp.netscape.com/certificate/v1.0/evalguide/

any verification steps are not performed. In each example scenario, the failure to complete the specified checks could expose:

- Unsuspecting Internet users to direct financial loss due to fraud.
- The legitimate organization to direct financial loss due to fraud, or undue business risk and loss or productivity, or public relations, or legal action.
- The certification authority to undue business risk, bad public relations or legal action.

The Legal implications of using Low Assurance SSL certificates.

The role of a Certification Authority (CA) is to certify that an applicant is a legitimate and legally accountable entity. Consumers are afforded far greater protection with High Assurance SSL certificates in the event of a legal claim – they have lines of recourse.

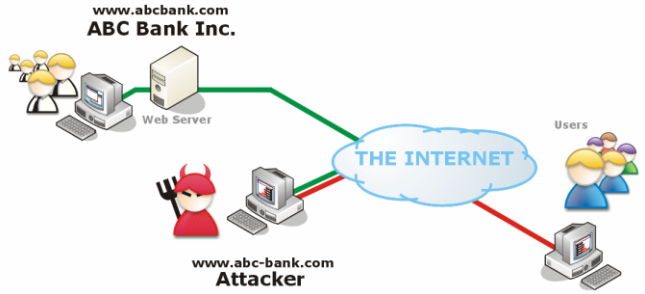
Low Assurance SSL certificates provide no legal recourse, and consumers remain unprotected. The actual implication for the user who relies upon an enterprise or business that purchases a low assurance SSL certificate has not yet been tested through the courts.

EXAMPLE SCENARIO	RISK OR THREAT POSED
• No authentication of the organization by the CA *or* • No check of the applicant's right to use the domain name	A malicious individual operating a spoofed web site tries to masquerade as an existing organization, thus deceiving Internet users into believing that the individual's web site is operated under the auspices of an existing organization whose name is included in the SSL certificate. This then creates a false level of trust by association between the malicious individual and the legitimate organization.
• No check of the organization's existence by the CA	A malicious individual could pretend to be an organization even though no such organization exists (i.e. the articles of incorporation or business documents have not been registered with the appropriate government body)
• No check by the CA of the applicant's identity or of his authority to request a certificate for the organization	A malicious individual who is not authorized by the organization could obtain an SSL certificate bearing the organization's name, allowing the malicious individual to masquerade as the organization

SSLv2 versus SSLv3/TLSv1 and Assurance Level

It's now widely accepted that SSLv2 was insecure. A critical failing of SSLv2 was its susceptibility to a Man-in-the-Middle attack[iv]. With SSLv2, it was not possible to guarantee that you were communicating securely with the owner of the private key.

With SSLv3 and the equivalent TLSv1 you can now be sure that only the owner of the server's private key can decrypt any information sent. However, as we have already established, where Low Assurance SSL is used, no entity authentication is performed and therefore it is not possible to know who the owner of the private key is. **SSLv3.0 is therefore open to a Man-in-the-middle attack with Low Assurance SSL.**



With no entity authentication consumers have no ability to know if they are subject to a man-in-the-middle attack.

What actually is the difference between High Assurance and Low Assurance?

As we have established, High Assurance validation is about "Certifying the end entity" and therefore "authenticating the intended recipient".

Low assurance processes fail to "authenticate the intended recipient" as discussed earlier in the definition of "encryption". The only item validated is control of a domain. Domain names are themselves susceptible to vulnerabilities.

DNS cache poisoning[v] is a technique which corrupts the DNS (Domain Name System) injecting false information into the system so that future requests can be diverted from their intended destinations. In a DNS poisoning attack it is possible for a localized domain of the same name to exist, and therefore possible for a second fraudulent Low Assurance SSL to be created. As no other checking is done an attacker can obtain an SSL certificate for any domain name that can be affected by a DNS poisoning attack. **Low Assurance SSL certificates are susceptible to DNS cache poisoning attacks.**

[iv] http://www.eucybervote.org/Reports/MSI-WP2-D7V1-V1.0-02.htm

[v] http://en.wikipedia.org/wiki/DNS_cache_poisoning

What is the point of encryption **if you don't know who for?**

Low Assurance SSL and compliancy to International Standards

SSL certificates must conform to internationally recognized standards for interoperability and are thus X.509 compliant. The data structure within X.509 itself makes use of another International standard, namely X.520[vi]:

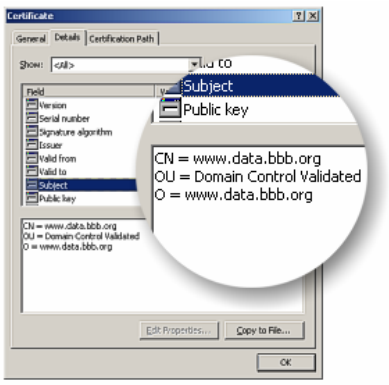
> 5.4 Organizational attribute types
>
> These attribute types are concerned with organizations and can be used to describe objects in terms of organizations with which they are associated.
>
> 5.4.1 Organization Name
>
> **The Organization Name attribute type specifies an organization.** When used as a component of a directory name it identifies an organization with which the named object is affiliated.
>
> An attribute value for OrganizationName is a string chosen by the organization (e.g. O = "Scottish Telecommunications plc"). Any variants should be associated with the named Organization as separate and alternative attribute values.
>
> organizationName ATTRIBUTE ::= {
> SUBTYPE OF name
> WITH SYNTAX DirectoryString {ub-organization-name}
> ID id-at-organizationName }
>
> The Collective Organization Name attribute type specifies an organization name for a collection of entries.
>
> collectiveOrganizationName ATTRIBUTE ::= {
> SUBTYPE OF organizationName
> COLLECTIVE TRUE
> ID id-at-collectiveOrganizationName }

X.509

Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks

X.520

Information technology – Open Systems Interconnection – The Directory: Selected attribute types



Here the 'O' – Organization field does not contain the organization "Better Business Bureau" so consumers have no ability to verify that the certificate actually belongs to that organization.

IS THERE SUCH A THING AS 100% SECURITY?

Is entity authentication the answer to achieve 100% security?

The answer is no, as 100% security does not exist! Any security related process or product is vulnerable! Security is about "risk mitigation".

Can the validation systems we have in place today be fooled or circumvented? Yes they can, but is this a reason to abolish them? Of course not! It's rather like saying, because our doors within our homes can be broken, let's remove them completely! It's ridiculous to even suggest this. What we need is even more security processes, products and service to secure ourselves. Removing what little protection we have is, irresponsible, short sighted and wrong!

Low Assurance SSL provides little of any value and this is often reflected in its low price.

The organizations offering Low Assurance SSL should immediately increase the level of validation they perform and work to identify better and stronger forms of entity authentication. Certification authorities should raise the bar, not lower the bar.

An entity obtaining a fully validated High Assurance certificate for use in committing fraud would leave an audit trail. Law Enforcement authorities would have more chance to secure a conviction.

IN SUMMARY

An SSL encrypted session between web browser and the web server provides a secure tunnel, but by default does not provide assurance in the identity of the end entity. Whilst a few high assurance providers continue to offer high assurance validation processes, many more low assurance providers are entering the market offering high speed, low value automated validation procedures. These low assurance products are not appropriate for encryption and do not provide either reliable privacy or trust.

Enterprises have a responsibility to ensure that the use of high assurance SSL certificates provides customers with the identity assurance and confidence to make safe, secure on-line transactions.

- The validation techniques followed by Certification Authorities should constantly be reviewed, refined and improved.
- The techniques should be audited by a centralized independent body.
- Proven adherence to those techniques should form the minimum entry criteria for any Certification Authority to have their root certificates accepted by Browser providers.

The goal of ever increasing security should drive future standards with entity authentication an absolute minimum where encryption and trust is required. After all,

What is the point of encryption if you don't know who for?

Comodo
US Headquarters
525 Washington Blvd, Jersey City,
NJ 07310, USA
Tel Sales: +1 800 772 5185
Fax Sales: +1 646 442 3760
Canada Tel Sales: +1 877 80 32 556
sales@comodo.com

Comodo
EMEA Headquarters
New Court, Regents Place, Regent Road
Manchester, M5 4HB, United Kingdom
Tel Sales: +44 (0) 161 874 7070
Fax Sales: +44 (0) 161 877 1767

sales@comodo.com

[vi] http://archive.dante.net/np/ds/osi/9594-6-X.520.A4.ps