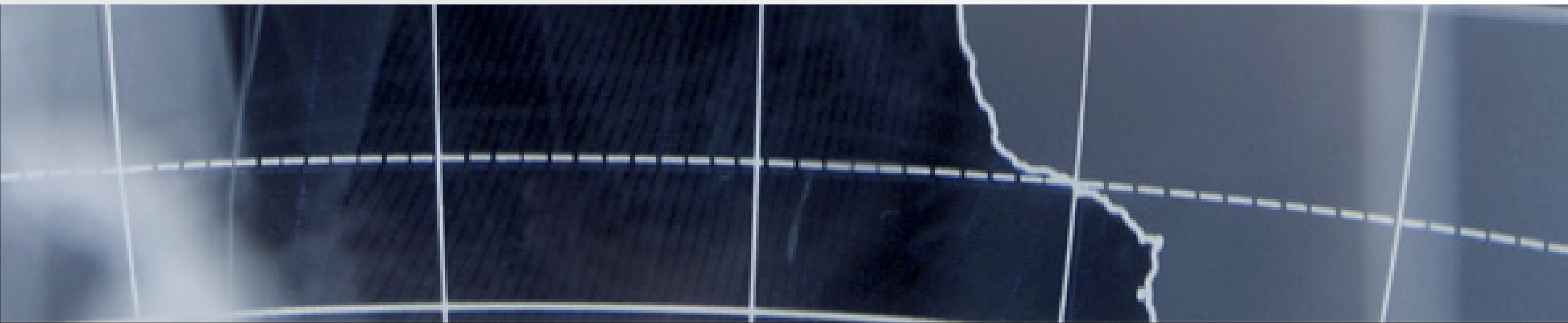
# Server-Gated Cryptography



# Server-Gated Cryptography:
## providing better security for more users

Contents:

Appendix:

## *Forward thinking...*

With the widespread global adoption of wireless technologies, hundreds of millions of people living developing countries are logging onto the internet for the first time.

While many will be doing so with new computers, still many more will no doubt be relying on outdated software to surf the WWW. Many of them will be naïve about the dangers that lie and wait in cyberspace.

As the enablers of secure and global electronic commerce it is our duty to help companies empower and protect these new citizens of the internet. If our technology, trusted services and products can help you to protect even one user, let alone the tens of millions who require such assistance, then we have done our duty.

This is what SGC-enabled SSL certificates are intended to do.

## Overview

**This guide will help you to understand how SGC-enabled SSL certificates work and why they are different from other certificates, why the technology was first introduced in the late 90s, and why this technology remains as relevant today as it was back then.**

E-commerce businesses using Server-Gated Cryptography-enabled SSL certificates can help assure customers of stronger encryption, greater privacy and reduced risks of fraud and identity theft. This is not one person's or organization's opinion. This is a fact - proven by the Yankee Group who conducted exhaustive independent tests (368 to be exact!) to arrive at this conclusion (1).

SGC technology may have originated in the late 90s but it remains as relevant today as it did when it was first introduced more than six years ago. The widespread growth of broadband globally (2) will necessitate the use of technologies that are forward thinking and proactive.

SGC is such a technology because, unlike other SSL certificates that rely on the user's browser being able to match a server's cipher suite, SGC helps users attain more secure connection by actually stepping up some users' browsers in specific situations.

The Yankee Group's study very boldly concluded, "SGC-enabled certificates enable more Windows 2000 users to connect with 128-bit encryption. This difference means tens of millions more internet users worldwide would get 128-bit encryption or higher if all e-commerce vendors used SGC-enabled certificates." (1)

The fact that 75% of US businesses (3) believe that a threat from unprotected systems in developing countries pose a growing threat to their digital security, strengthens the argument supporting using proactive technologies like SGC-enabled SSL certificates.

The internet has given companies a cost-effective and extremely powerful medium to connect with customers anywhere in the world. Broadband is making it possible for more people from every corner of the globe to go shopping in cybermalls, unrestricted by time and geography.

These great new opportunities that await e-businesses who want to expand globally will demand proactive security to protect both the e-business resources and databases, as well as provide protection for new customers who may be relying on outdated software to explore the internet.

**Referencing:**

1. Building Blocks of Transparent Web Security: Server-Gated Cryptography - The Yankee Group, September 2005
2. World Broadband Statistics: Q3 2005 - Point Topic Ltd. 2005
3. U.S. Businesses: Cost of Cybercrime Overtakes Physical Crime - IBM, March 2006

## An argument for proactive security

The internet is the embodiment of globalization - its growth fueled by the widespread global adoption of faster, always-on broadband ADSL and wireless service, the global expansion of multinationals and their mobilized army of workers who trade information anywhere and anytime.

With the internet's growth comes a new opportunity for many small and large businesses that are now able to trade from a location in one corner of the globe, with anyone who is able to access their website and make credit card payments.

Internet and electronic trading knows no time and has no borders. But, as many companies ready themselves for the onslaught of new customers coming from the four corners of the globe, security experts are expressing caution. In fact, many US businesses are also expressing caution and concern.

In a recent survey conducted by IBM (1) as many as 75% of the participating companies expressed concern for the growing cybercrime threat that will come from many unprotected computers in the developing world.

Outdated software and unprotected systems are a real threat as the adoption rate of broadband services stabilizes in the US and declines in Asia, while the Middle East and Africa are showing the highest new connection rates in the world for these services.

While many companies are rushing to capitalize on rapid global growth of broadband connection, companies must heed the warnings of many experts who are calling for proactive security that serves to not only protect the vendor, but also "thinks" for the user helping them to attain the best possible security.

Proactive security will not only create a more secure digital environment for everyone, but it will also help to build trust amongst the many new users of the internet. Trust will build confidence and confidence is good for business.

1. U.S. Businesses: Cost of Cybercrime Overtakes Physical Crime - IBM, March 2006

## Server-Gated Cryptography: making the digital world a more secure space (1)

In the 1990s, the US government imposed restrictions on exporting strong cryptography to other countries. The restriction meant that software that implement SSL, such as web browsers, operating systems and web servers had to limit encryption to weak algorithms and shorter key lengths if it was exported outside the United States. Lawmakers included an exception for financial transactions to ensure that customers worldwide could safely transact online using strong encryption.

SGC was created as an extension to SSL for consumers with export versions of web browser software to use strong cryptography for financial transactions. US export laws were upheld by issuing SGC certificates only to eligible financial institutions, creating an enforcement point at the server without any impact to the client. The restrictions on export of strong encryption have since been relaxed, and now SGC certificates may be issued to any institution.

Restrictions on encryption are evident in older versions of Windows 2000 running Internet Explorer that are still in use. Consumers and e-commerce vendors, particularly those outside the United States, are still using weak encryption, despite the fact that safer, stronger alternatives are available.

Although newer versions of Windows 2000 provide these features, millions still use old versions. Users who are still using certain older browser versions that only provide weak 40-bit or 56-bit encryption can gain full-strength 128-bit encryption when conducting business with SGC-enabled web sites. With SGC, browser and operating system versions - whether exports or domestic - that would otherwise connect with weak encryption are afforded much stronger security. Until older versions of browser and operating systems disappear completely, SGC certificates can protect this portion of the user population.

Also see: Strong gets stronger - 256-bit encryption (Appendix 2)

1. An extract from The Yankee Group paper entitled Building Blocks of Transparent Web Security: Server-Gated Cryptography, September 2005)

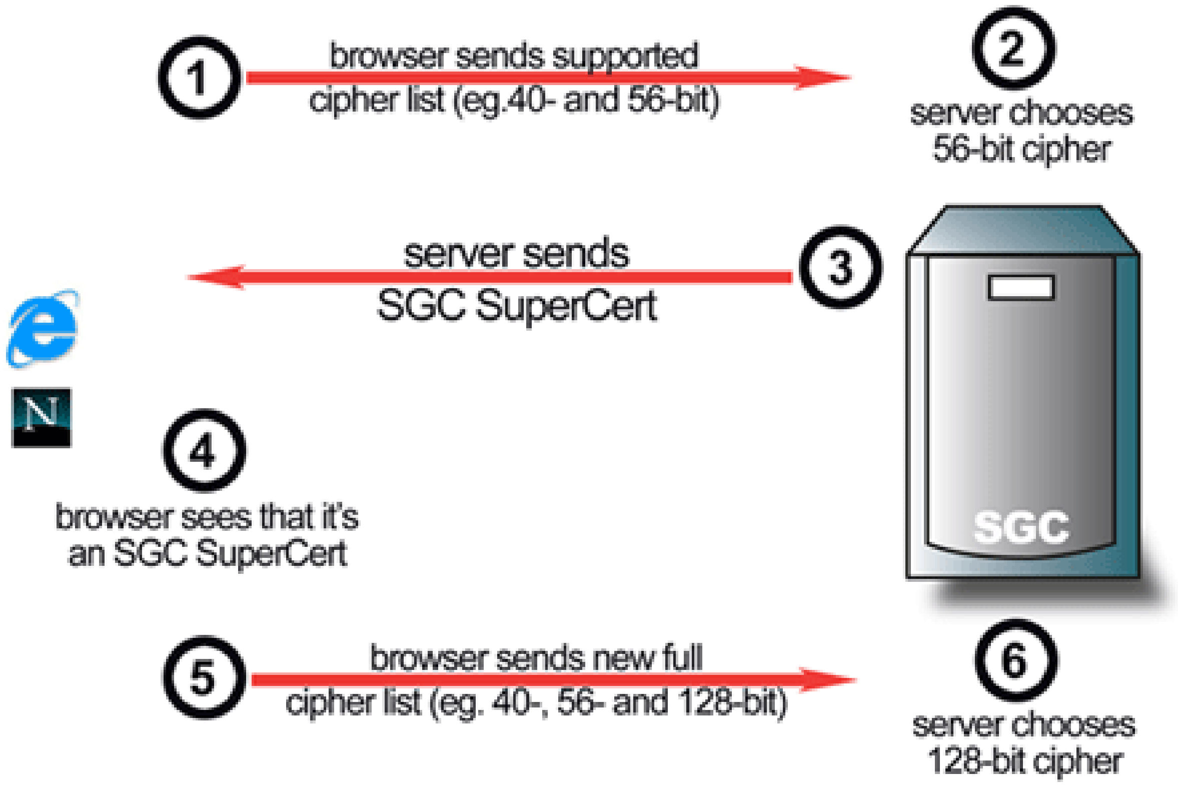
## How an SGC-enabled SSL certificate works

To understand how an SGC-enabled SSL session differs from other SSL sessions, we first need to explain how a normal SSL session works. A simplified SSL session looks like this:

1. the client/browser sends the server a list of supported ciphers
2. the server chooses a cipher and sends that cipher along with its certificate back to the client/browser
3. the client/browser verifies the server's certificate and extracts the server's public key
4. the client/browser encrypts a secret using the server's public key and sends it to the server
5. the server decrypts the secret using its private key.

At this point the client/browser and server both share the secret and can be confident that no one else knows it. The client/browser and server can now use this secret and the chosen cipher to have a secure conversation. This is a very simplified explanation of a SSL handshake.

With SGC basically what happens is when the client/browser receives the server's certificate (step 3), the client discovers that the server has a SGC-enabled SSL certificate the client/browser will perform a new handshake (once the current handshake is finished) using a complete list of all the ciphers being supported including the strong 128-bit encryption, thus upgrading the current session to strong cryptography.


1
browser sends supported cipher list (eg.40- and 56-bit)
2
server chooses 56-bit cipher
server sends SGC SuperCert
3
4
browser sees that it's an SGC SuperCert
SGC
5
browser sends new full cipher list (eg. 40-, 56- and 128-bit)
6
server chooses 128-bit cipher

## *Building Blocks of Transparent Web Security: Server-Gated Cryptography by the Yankee Group, September 2005*

Secure Sockets Layer (SSL) is the de facto standard for securing e-commerce transactions. SSL encrypts personal information such as credit card numbers, social security numbers, passwords, names and addresses sent to an e-commerce vendor via its website. Therefore, SSL is a critical component in the protection of consumer privacy and a necessity to reduce the risks of fraud and identity theft.

Yankee Group research shows that between 1% and 2% of e-commerce transactions are related to fraud. Losses totaling $2 billion in 2004 are growing at the same rate as e-commerce revenue and eroding consumer confidence. SSL encryption is a key component in protecting consumers' online transactions. Its transparency to users will be a critical factor in reducing fraud.

SSL lacks transparency in a key area: the strength of encryption used for a given session. Browsers, web servers and operating systems all play a role in determining the level of encryption used: 40 bit, 56 bit or 128 bit. Some PC systems can't take advantage of full 128-bit SSL encryption. Server-gated cryptography (SGC)-enabled certificates address this issue.

E-commerce websites using SGC can assure customers of stronger encryption, greater privacy and reduced risks of fraud and identity theft.

A special study done by The Yankee Group tested both SGC- and non-SGC-enabled certificates in 92 common environments to determine under what conditions users benefit from strong encryption.

The Yankee Group's conclusion - "The number of people still subject to weak encryption because they are using older versions of Windows and Internet Explorer is in the tens of millions. Users running the Windows 2000 operating system without Service Pack 4 or the high-encryption pack are most likely to be affected.

"Tested browsers released earlier than March 2000 also return higher rates of connection at low encryption levels. Our testing results show that when using SGC certificates, virtually all combinations of Windows operating system, Internet Explorer and server are able to step up to 128-bit encryption. Wide-scale deployment of SGC-enabled SSL certificates would reduce the actual number of users exposed by weaker encryption dramatically and make it possible for virtually every internet user to enjoy the protection of 128 bit or stronger encryption."

# *Is thawte's SGC SuperCert certificate right for my business?*

With the widespread global adoption of broadband internet, many e-commerce businesses are considering expanding their services into new territories. However, before you rush into opening your cyber doors to these new revenue opportunities, consider the many new challenges these new customers could pose to your business.

Many of these new customers could pose a security risk to your business. Many millions of PC users still rely on older software like Windows 2000 systems that have not been updated with the latest service packs. These users may only be able to connect to your secure e-commerce website using weak 40 and 56-bit encryption, exposing not only themselves but also your business to unnecessary security risks.

To protect internet financial transactions, experts recommend that a minimum of 128-bit encryption be used.

SGC-enabled SSL certificates, like our SGC SuperCerts, are the only SSL certificates that have the unique ability to step up encryption strength from the weak encryption to the much stronger 128-bit encryption.

In an independent study conducted by the Yankee Group in September 2005 it was shown that SGC-enabled certificates enable more Windows 2000 users to connect with 128-bit encryption. The difference means tens of millions more users worldwide would get 128-bit encryption, if all e-commerce businesses used SGC.

256-bit encryption can be achieved if the user's browser capability and the cipher suite installed on the web server are both 256-bit compatible.

*thawte* SGC SuperCerts provide:

- A higher strength of encryption for certain older versions of export browsers.

- Confidence in the integrity and security of your online business and network infrastructure. Customers are becoming increasingly aware of the advantages of SSL security and will often not purchase online from non-secure stores. All major web merchants use SSL security backed by strong warranties to encourage customers to buy online.

- Interoperability and support for standard applications and browsers, such as Microsoft Internet Explorer and Netscape Communicator.

- Non-forgeable proof of your web site identity.

- Ease of use. A SGC SuperCert is a stand-alone solution that requires no installation of extra software on the server or the browser.

- Peace-of-mind for those conducting international online business, knowing that your business is forward thinking and proactive in its attitude concerning the security of its customers.

## *About thawte*

*thawte*, the **Certification Authority** chosen by hundreds of thousands, has been **innovating** and delivering **trusted services** for more than a **decade**.

We **enable** businesses and individuals to communicate and transact securely by **verifying and authenticating** their identities, thus allowing them to gain the **trust** and **confidence** of millions of users.

Our **digital certificates** are used globally to **secure** servers, **encrypt** files and communication, and **validate** the authenticity of applications and digital code.

Through our **dedication** to maintaining your **security** we are helping to build a **trusted digital future** for everyone.

## *The value of authentication*

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 the data you are receiving is trustworthy. Authentication can help establish trust between parties involved in all types of transactions by addressing a unique set of security issues including:

**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.

## Useful URL's

For more detail on *thawte's* SGC SuperCerts, please visit:
http://www.thawte.com/sgc/index.html
Learn more about SGC SuperCerts in our FAQs:
http://www.thawte.com/support/sgc/index.html
21-Day Free Trial SSL Certificate
https://www.thawte.com/ucgi/gothawte.cgi?a=w62240062237049007
Buy SGC SuperCerts:
http://www.thawte.com/buy

## Contact thawte

Should you have any further questions regarding the content of this guide or *thawte* products and services, please contact a Sales Advisor:

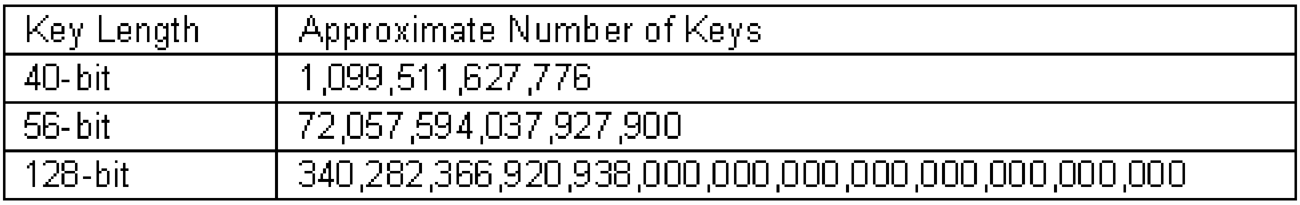
| | |
|---|---|
| E-Mail: | sales@thawte.com |
| Telephone: | +27 21 937 8902 |
| Fax: | +27 21 937 8967 |
| Live Secure Web Chat: | visit http://www.thawte.com/chat/chat_intro.html |

## Appendix: Why 128-bit is stronger than 40 and 56-bit encryption

### Understanding Cryptographic Strength

Cryptographic strength is expressed in key length or bit length. Keys come in a variety of lengths (e.g. 40-bit, 56-bit and 128-bit). Assuming an inherent strength in the encryption algorithm, a longer key/bit length will make it harder to crack an encrypted message. We refer to bit length as this specifies the number of bits required to write the number of possible keys in binary.

Key lengths have increase over time to counteract advances in computing power which make the cracking of encrypted messages easier.



| Key Length | Approximate Number of Keys |
|---|---|
| 40-bit | 1,099,511,627,776 |
| 56-bit | 72,057,594,037,927,900 |
| 128-bit | 340,282,366,920,938,000,000,000,000,000,000,000,000 |

Consumers and e-commerce vendors often view encryption as too complex for the average hacker to exploit. Surely any sort of encryption provides enough security to do online banking and shopping, right? Unfortunately, the answer is no. Low-level encryption, using 56 bits or less, is universally deemed too weak for safe financial transactions.

With the computing power available today, it's not cost prohibitive for hackers to attack 56-bit encryption using brute force, which involves trying every possible key combination until they find the one that converts cipher text into plaintext.

The difference in security between 40 bit, 56 bit and 128 bit is significant. The progress made in computing technology means that weaker encryption using 40-bit or 56-bit keys can be attacked by brute force and broken in a matter of hours using an average-speed PC. As recently as 1997, the same exercise would have taken days and required the effort of multiple computers and people.

At current computing speeds, 128-bit encryption will take more than a trillion years to attack using brute force, an obstacle that would deter any financially motivated attacker.

By contrast, breaking shorter 40-bit or 56-bit encrypted sessions is a relatively small investment for attackers harvesting personal information.

There is a common misconception that digital certificates determine the strength of encryption and this is reinforced by many Certification Authorities that refer to 40-bit or 128-bit certificates.

It is important to understand that encryption strength is normally determined by negotiation between the browser, operating system and a web server before a secure session is established.

Only digital certificates enabled with SGC technology are capable of influencing the encryption strength of a session beyond what is agreed between the browser, operating system and server (more this later).

## *Strong gets stronger - 256-bit encryption*

Although encryption strength is dependent on the nature of the browser as well as the software on the web server to which the browser is connecting, 256-bit encryption is the highest level of encryption currently possible. While some browsers support this level of encryption, this does not guarantee that a secure internet session will occur at this level.

The level of encryption used to secure an internet connection depends on two factors - firstly the capacity of the cipher suite installed on the web server being accessed, and secondly the capability of the web browser being used to establish the connection.

A cipher suite is essentially an encryption algorithm, which a web server will use to negotiate an encrypted internet session. To establish a 256-bit encryption session the cipher suite must be capable of delivering this level of encryption.

The encryption level that will be used to establish a secure internet connection is determined through a negotiation that occurs when the internet browser and web server perform their handshake.

During this handshake session the internet browser sends its list of cipher suites to the web server, which the server uses to determine the highest or strongest encryption that can be used for the encrypted session.

Different browser and different browser version will offer different levels of encryption. Some (older versions of Netscape and Internet Explorer) will even be restricted to offering only weak encryption, unless they are connecting to servers using Server-Gated Cryptography enabled SSL certificate.

So, depending on the browser's vendor and version, some will only be capable of encrypting at 40 or 56-bit encryption, while more recent browser versions are capable of 128 and even 256-bit encryption.

Another group of browsers will only be capable of 40 or 56-bit encryption until it has been established that the server involved has an SGC-enabled SSL certificate installed. These browsers will then be capable, with help from the server, of 128-bit encryption.

Not all cipher suites are the same either. Only newer cipher suites such as Advanced Encryption Standard are capable of managing 256-bit encryption rates.

**How can you establish when 256-bit encryption will be used when connecting to a secure server?**

Firstly, ensure that the browser you are using is 256-bit encryption capable. Secondly, check with the server administrator if the server on which the website is hosted has a 256-bit cipher suite installed.

When both criteria have been met you should be establishing a 256-bit encryption secure connection with that website. This can easily be verified by hovering your mouse cursor over the internet browser's closed padlock.