



## ***Server-Gated Cryptography***

The illusion of security

July 2009

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© 2009 Entrust. All rights reserved.

## Table of Contents

1	The Myth of Server-Gated Cryptography .....	1
2	'Who Needs Strong Encryption Anyway?' .....	1
3	First Amendment Rights.....	2
4	Striking the Right Balance.....	3
5	More Serious Security Concerns.....	3
6	Eliminate Unnecessary Threats, Avoid Premium SGC Certificates....	4
7	About Entrust .....	4

## 1 The Myth of Server-Gated Cryptography

As security vendors compete for market share for SSL certificate sales, some attempt to gain a better foothold by claiming that expensive Server-Gated Cryptography (SGC) certificates are required for 128-bit security. This just isn't the case. SGC is **not** required to enable 128-bit security for virtually all browsers deployed today.

In fact, supporting browsers that require SGC can introduce serious security vulnerabilities to very common present-day attacks. All users who still require SGC are using extremely outdated versions of Web browsers that have not been updated to address the multitude of security issues that have been identified since they were released; security issues that are far more severe than weakness in the cryptography. This poses a significant risk to both the user and the organization.



In order to better understand why SGC was created and how it represents security threats to today's organizations, it's best to examine the foundation of cryptography and how it evolved to become the current-day standard.

## 2 'Who Needs Strong Encryption Anyway?'

The history of server-gated crypto is fascinating. It is the story of America in microcosm; how a handful of individuals who cherished freedom and corporate America, driven by the profit motive, stood up to authority and won.

There was an era — starting roughly in the 1970s and ending abruptly at the turn of the century — that cryptographers now call the "Crypto Wars." The main combatants were the United States government, led by the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI), and a strange alignment of interests. These included civil libertarians, such as Phil Zimmerman; Daniel Bernstein and the Electronic Frontier Foundation; and North American business interests, personified in Jim Bidzos of RSA.

The battleground? The rights of U.S. citizens, as well as others around the world, to use effective encryption technology to protect themselves against surveillance by advertising interests, credit bureaus, identity thieves and their own governments.

The NSA and FBI convinced the U.S. Department of Commerce to enact regulations that prohibited the export of cryptography with strength greater than 40 bits, unless the decryption key was lodged with an approved escrow agent. Although the national interest prevented them from citing real-life cases, the NSA assured the U.S. Congress that supplying strong cryptographic technology to foreigners without this escrow provision would jeopardize the security of all American citizens.

But the First Amendment of the U.S. Constitution guarantees its citizens the right to freedom of speech and freedom of assembly. The civil libertarians argued that this right extends to open discussion of cryptographic techniques, as well as the right to protect their online communications with effective encryption.

The business interests argued that strong cryptography was available from overseas sources, so U.S. regulations that outlawed the export of strong cryptography were hindering U.S. business with no compensating benefit to its citizens.

Early versions of the Netscape Navigator and Microsoft Internet Explorer Web browsers were equipped with encryption capability that could protect communication of users from unauthorized interception. However, the strength of this safeguard was limited to 40 bits.

In the mid '90s, it was becoming clear how the Web was going to revolutionize commerce, and U.S. financial institutions wanted to be part of that revolution. But, cryptographic experts were casting doubt on the adequacy of the algorithm that financial institution always turned to for protecting their communications: the Data Encryption Standard, which has a strength of 56 bits.

Louis Freeh, head of the FBI, repeatedly insisted that breaking a single 56-bit key using the computers available at the time would take thousands of years. So, limiting encryption strength for U.S. citizens to 56 bits allowed completely effective protection from state and criminal surveillance.

But, in 1997 a computer network comprising thousands of ordinary desktop machines was used to crack a 56-bit DES key, taking just four months to complete the task. And in July 1998, the Electronic Frontier Foundation successfully cracked a DES key in just 56 hours using a special-purpose machine costing about \$250,000 to build.

### 3 First Amendment Rights

The war was also being waged on another front. Phil Zimmerman had been fascinated by cryptography since he was a child. In later life he started a personal crusade to develop a freeware program — later named Pretty Good Privacy (PGP) — that would enable Internet users to strongly encrypt their e-mail communications.

In 1991, the introduction of Senate Bill 266, also known as the Comprehensive Counter-Terrorism Act, provided the impetus for Zimmerman to finish his project and finally make his program available for download over the Internet.

But while PGP 1.0 used a cryptographic algorithm with a large key, Zimmerman had chosen to use an algorithm of his own design. That algorithm proved to be fatally flawed: the privacy it offered was anything but “pretty good.” In 1992, PGP was updated with an algorithm designed by cryptographic experts and, with help from overseas collaborators, version 2.0 was made available for download from locations outside the U.S.

These events served to substantiate the claim by U.S. industry that strong cryptography was available to people around the world and that U.S. companies were operating at a disadvantage.

In 1995, Berkley researcher Daniel Bernstein and the EFF filed a complaint against the U.S. Department of State charging that the export laws, as they applied to cryptography, were unconstitutional. Bernstein contended that by preventing him from publishing the details of a cryptographic algorithm that he had invented, the government was denying him his constitutional right to free speech. The case finally exhausted the appeal process in May of 1999, with the Ninth Circuit court finding in Bernstein's favor.

Meanwhile, in 1996, the National Research Council had issued the results of its investigation into government policy on cryptography. The experts who wrote the report had benefited from a classified briefing from the NSA. They evidently found the NSA's arguments unconvincing and wrote in favor of a liberalization of export regulations.

## 4 Striking the Right Balance

The '90s was a decade of turmoil in the information security industry, with battle lines shifting constantly, and much uncertainty about the eventual outcome. Finally, at the end of 1999, the administration of U.S. President Bill Clinton acted in a dramatic fashion to restore clarity. It enacted regulatory changes that would more or less lift all restrictions on the free use, including export, of effective cryptography. Shortly afterwards, the browser suppliers removed restrictions on the use of strong encryption.

But during this period of uncertainty, software makers had bent over backwards to find a balance between the competing pressures. Starting with Netscape Navigator 4.0 and later updates of Microsoft IE 3, in mid-1997, browsers delivered a capability called "server-gated crypto."

Browsers were shipped with the capability of performing 128-bit encryption; a strength that even the most skeptical would agree was adequate for protecting any and all personal information without unduly impacting performance.

This capability would only be enabled by a flag in the Web site's Secure Socket Layer (SSL) certificate. The right to assert this flag was limited to U.S. certification authorities (CAs) — and those authorities were bound to assert that flag only in certificates issued to financial institutions.

In this way, users of Navigator 4 and IE 3 could protect their online banking with strong encryption, effectively preventing unscrupulous ISPs from eavesdropping their login credentials and other banking details. All other uses of the Web would be protected to a strength no greater than 40 bits. The NSA and the FBI could live with this compromise.

## 5 More Serious Security Concerns

So, for a short period in the late '90s, browsers released into the marketplace required a special "SGC" SSL certificate to engage their full cryptographic capability. The remnants of that era remain today: 0.07 percent of users still have browsers that will only "step up" their security level to 128-bit encryption if enabled by the certificate. The remaining 99.93 percent use 128-bit encryption with every SSL Web site they visit.

Browsers of that era are riddled with far more serious vulnerabilities than the weakness of their cryptography. The user is plainly not managing the security of his or her machine. If its patch status is not up to date, it also is unlikely to be running antivirus software and it must certainly be infected with viruses. The strength of the cryptography is a minor consideration by comparison.

Machines infected via outdated, unsupported browsers even place other safe users of an organization's online portal at risk to phishing and man-in-the-middle fraud attacks. Botnets, for example, not only generate spam, but also help propagate Trojan horses, worms, keystroke loggers and viruses.

Consider, for instance, the virus known as the NIMDA worm. CERT, an organization devoted to ensuring that appropriate technology and systems-management practices are used to resist attacks on networked systems, first announced the discovery of the virus in September 2001. At the time of the announcement, Microsoft already had issued patches to address the vulnerability exploited by the NIMDA worm. While all versions of IE were affected, only version 5.01 and later were still supported.

The worm can infect a machine that visits a malicious site. It infects the victim's machine with multiple copies of itself, deletes files of various types and attempts to infect other machines by

spreading itself through e-mail. With minor modifications, it can be repurposed to monitor keystrokes, launch man-in-the-middle attacks and other nefarious activities.

The NIMDA worm illustrates just one of the many serious vulnerabilities that are present in unsupported browsers.

Users of any but the most recent versions of popular browsers are vulnerable to attacks. These machines are possibly part of a botnet and are unwittingly participating in worm and phishing attacks on other users. Keystrokes may be logged remotely, and while they may be protected from eavesdropping by their ISP, they have left themselves open to far more serious attacks from the criminal world.

Sites that allow users to pass sensitive information — bank account identification credentials, for example — using browsers of this vintage are doing all of their users a disservice. Each organization should educate their customers about the true state of the security of their online transactions and encourage them to upgrade to secure, updated products.

## 6 Eliminate Unnecessary Threats, Avoid Premium SGC Certificates

In the end, it's the responsibility of the Web site operator to do what's right for its customers and its own well-being. That's obvious, but what does that mean in a real-world environment?

Thankfully, it's pretty simple — supporting Web browsers that require “premium” SGC certificates introduces serious security threats to an organization. It's simply not worth the risk to the more than 99 percent of your customers — as well as the organization itself — to give less than 1 percent of the Internet population the illusion of security. SGC is not required to enable 128-bit security for virtually all browsers deployed today.

Extended Validation (EV) SSL certificates alone are superior to SGC certificates; or even a combination of EV with SGC certificates. Why? EV SSL certificates require the end-user to use a browser protected by at least 128-bit encryption for SSL security. This requirement ensures the consumer is using a relatively up-to-date browser (eliminating the need for SGC), thus making the user's Internet session — as well as the organization using the EV SSL certificate — more secure from the onset.

## 7 About Entrust

Entrust provides trusted solutions that secure digital identities and information for enterprises and governments in 2,000 organizations spanning 60 countries. Offering trusted security for less, Entrust solutions represent the right balance between affordability, expertise and service. These include SSL, strong authentication, fraud detection, digital certificates and PKI. For information, call 888-690-2424, e-mail [entrust@entrust.com](mailto:entrust@entrust.com) or visit [www.entrust.com](http://www.entrust.com).

For more information on Extended Validation (EV) SSL certificates, visit [www.entrust.net/ev](http://www.entrust.net/ev).