TLS/SSL hardening and compatibility Report 2011

Condensed Version

Author: Thierry ZOLLER

contact@g-sec.lu

http://www.g-sec.lu

G-SEC™ is a non-commercial and independent group of Information Security Specialists based in Luxembourg.

Table of Contents

Introduction

This report gives general recommendations as to how to configure SSL/TLS in order to provide state of the art authentication and encryption. The options offered by SSL engines grew from the early days since Netscape developed SSL2.0. The introduction of TLS made matters more challenging as **servers and clients** offer different sets of available options depending on which SSL engine (OpenSSL, NSS, SCHANNEL etc...) they use. Finding the middle ground has proven difficult especially as the supported protocols and cipher suites are mostly not documented.

To make matters more complicated Browsers may not use all functionality offered by the SSL stacks, as such **this report will only list functionality used by current Browsers**.

This report provides an overview of the currently available TLS options across Servers and Clients and allows you to offer support for a wide variety of Browsers an offer “good enough” security.

The 2011 version was updated as follows:

- Google Chrome moved away from Microsoft SCHANNEL and now uses Network Security Services (NSS) offering high end cryptography on legacy windows systems (XP,2000).
- Updated the mod_gnutls Key exchange support

During the creation of this Document two Tools have been developed:

- *SSL Harden* (beta) – Allows users of Windows 2000, XP, Vista, 7 and particularly administrators of Windows Server 2003 & 2008R2 to harden SSL/TLS support. Administrators can manually edit and backup the SSL configuration and set PCI-DSS compliant SSL rules with a click of a button. Link
- *SSL Audit* (alpha) - A remote SSL audit tool able scan for SSL/TLS support against remote servers. SSL Audit uses its own small parsing engine and does not rely on OpenSSL or other SSL engines allowing it to detect ciphers not supported by OpenSSL. Link

Please note that this summary does not take into account the arrival of quantum computing. Large quantum computers able to crack large RSA keys are foreseen for 2014 by the ARDA and 2018 by Prof Lloyd [1] . Shor’s algorithm could then be used to break the RSA key sizes very fast. We recommend to push for ECC based certificates as soon as possible.

The information is believed to be correct at the time of writing, due to the nature of undocumented features there might be slight errors in this version if you believe the

[1] http://synaptic-labs.com/ecosystem/context-qc-relevant-today.html

information displayed within this paper is wrong please contact contact@g-sec.lu. Feedback from Microsoft, Apache, Opera and Apple was integrated when available.

Revisions

Version	*Date*	*Annotations*
0.8	07.12.2009	Initial draft
0.85	09.12.2009	Added recommendations, Added BSI, NIST, FSIA recommendations
0.9	09.12.2009	Added Browser support Added Server support
0.95	18.12.2009	Synopsis
0.96	05.01.2010	Released for RFC
0.97	18.01.2010	Released as RC
0.98	23.01.2010	Fixed a few typos
0.99	12.03.2011	Added changes to chrome, corrected grammar.
1.0	21.09.2011	Released as 1.0
1.01	25.09.2011	Layout, added details provided by Opera
1.02	28.09.2011	Update mod_gnutls, formating

Client-side and Server-side Compatibility Overview

This section gives an overview over the current SSL/TLS capabilities across Operation Systems, Clients (Browsers) and Servers (Web servers). We conclude with advice on how to securely configure your SSL/TLS service and in particularly which Encryption, Authentication, Key exchange settings to use.

Throughout this document we will use the colour blue to indicate our recommended settings; this recommendation is based on compatibility and security.

Client-side: TLS / SSL Compatibility overview

In order to assess the SSL/TLS support of modern Internet browsers we had to take a look at the SSL engines they use. Some SSL stacks generally have capabilities that browsers do not make use of per default, **the lists below only reflect real default browser usage.**

- Chrome and Firefox use the NSS[2] engine
- IE5, 6, 7, 8 and Safari use Microsoft SCHANNEL[3]
- Opera and Safari (OSX) use custom SSL engines.

Default Protocol support

All browsers tested do explicitly not support SSLv2

Protocol	**NSS** [1]	**SCHANNEL**	**SCHANNEL**	**SCHANNEL**	**Opera 10**	**Safari 4**[4]
	ALL OS	XP/2K/2003[2]	7/2008R2[3]	Vista /2008[2]	All OS	OSX
SSLv2	No	No	No	No	No	No
SSLv3	Yes	Yes	Yes	Yes	Yes	Yes
TLS 1.0	Yes	Yes	Yes	Yes	Yes	Yes
TLS 1.1	No	No	Yes (disabled per default)	No	Yes	No
TLS 1.2	No	No	Yes (disabled per default)	No	Yes	No

Default Key exchange support

We recommend using Ephemeral Diffie Hellmann paired with either RSA or DSS as signature.

Algorithm	**NSS** [1]	**SCHANNEL**	**SCHANNEL**	**SCHANNEL**	**Opera 10**	**Safari 4**[4]
	ALL OS	XP/2K/2003[2]	7/2008R2[3]	Vista /2008[2]	All OS	OSX
RSA	Yes	Yes	Yes	Yes	Yes	Yes
DHE-RSA	Yes	No	No	No	Yes	Yes
DHE-DSS	Yes	Yes	Yes	Yes	Yes	Yes
ECDHE-RSA	Yes	No	Yes	Yes	No	No
ECDH-RSA	Yes	No	No	No	No	No
ECDHE-ECDSA	Yes	No	Yes	Yes	No	No
ECDH-ECDSA	Yes	No	No	No	No	No
ADH	No	No	No	No	No	No

1 Firefox, Google chrome (New) – All OS | 2 IE 7 & IE 8 & Safari | 3 IE8 & IE9 (**not** Safari – see VISTA column for Safari 7/2008R2 support)| 4 OSX

▨ Recommended

[2] http://www.mozilla.org/projects/security/pki/nss/

[3] http://msdn.microsoft.com/en-us/library/windows/desktop/ms678421(v=vs.85).aspx

RSA support

RSA public-key cryptosystem is an asymmetric encryption method; it can be used for signatures as well as encryption. In SSL/TLS RSA is used during key exchange (handshake). RSA bases its security on the length of the modulus that must be factored. The bigger the modulus the harder it is to break the algorithm.

Browser supported RSA key size, DH and SRP [4]

These are the key sizes that are supported by major Browsers, there is no client side restriction to use 1024 bit instead of 2048, and additionally 1024 bit are considered weak by today's standards.

RSA Modulus	NSS [1]	SCHANNEL	SCHANNEL	SCHANNEL	Opera 10	Safari 4[4]
	ALL OS	XP/2K/2003 [2]	7/2008R2 [3]	Vista /2008 [2]	ALL OS	OSX
1024	Yes	Yes	Yes	Yes	Yes	Yes
2048	Yes	Yes	Yes	Yes	Yes	Yes
4096	Yes	Yes	Yes	Yes	Yes	Yes
Note:					Generally no limit; 4k limit on client cert	

Default supported Ciphers [5]

In order for this list to stay focused on best practices we list modern or strong ciphers only.

Cipher	Size	NSS [1]	SCHANNEL	SCHANNEL	SCHANNEL	Opera 10	Safari 4[4]
		ALL OS	XP/2K/2003 [2]	7/2008R2 [3]	Vista /2008 [2]	ALL OS	OSX
AES	128	Yes	No [19]	Yes	Yes	Yes	Yes
AES	256	Yes	No [19]	Yes	Yes	Yes	Yes
AES-GCM	256	No	No	Yes	No	No	No
RC4	128	Yes	Yes	Yes	Yes	Yes	Yes
Camellia	128	Yes	No	No	No	No	No
Camellia	256	Yes	No	No	No	No	No
3DES	168	Yes	Yes	Yes	Yes	Yes	Yes

1 Firefox, Google chrome (New) – All OS | 2 IE 7 & IE 8 & Safari | 3 IE8 & IE9 (**not** Safari – see VISTA column for Safari 7/2008R2 support)| 4 OSX

🟦 Recommended

[4] http://msdn.microsoft.com/en-us/library/bb931357%28VS.85%29.aspx

[5] With heavy support from SSLLAB (Ivan Ristic)

Default ECC support

Elliptic curve cryptography bases on a discrete logarithm problem, ECC needs less key size to achieve the same strength then RSA, as an example, an ECC 160-bit field offers the same resistance as an 1024-bit RSA modulus. This allows for smaller keys and offers improved performance. Unfortunately ECC is not widely supported in Browser as of yet, but certainly will be in the future. We are currently not aware of any Certificate authority that allows you to buy ECC certificates.

Elliptic key cryptography

Curve size	**NSS [1]**	**SCHANNEL**	**SCHANNEL**	**SCHANNEL**	**Opera 10**	**Safari 4[4]**
	All OS	XP/2K/2003[2]	7[3]/2008R2	Vista[2]/2008	ALL OS	OSX
P-256	Yes	No	Yes	Yes	No	No
P-348	Yes	No	Yes	Yes	No	No
P-521	Yes	No	**No**	Yes	No	No

1 Firefox, Google chrome (New) – All OS | 2 IE 7 & IE 8 & Safari | 3 IE8 & IE9 (**not** Safari – see VISTA column for Safari 7/2008R2 support)| 4 OSX

According to Microsoft support for P521 mode has been removed from Windows 7 and 2008R2 due to not being part of the official NIST Suite B.

🟦 Recommended

Server-Side: TLS / SSL Compatibility overview

Default protocol support

This matrix shows the protocol support of modern web servers - There is no reason to continue supporting SSLv2.

Protocol	IIS6 [1]	IIS7 [2]	IIS7.5 [3]	mod_ssl	mod_gnutls	JSSE [4]	NSS [5]
SSLv2	Yes	Yes	Yes	Yes	No	Yes	Yes
SSLv3	Yes	Yes	Yes	Yes		Yes	Yes
TLS 1.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TLS 1.1	No	Yes	Yes (disabled per default)	No	Yes	No	Yes
TLS 1.2	No	No	Yes (disabled per default)	No	Yes (disabled per default)	No	Yes

* See appendix on how to enable TLS 1.2 support on IIS 7.5

Default key exchange support

We recommend offering ephemeral Diffie Hellmann paired with either RSA or DSS as signature

Algorithm	IIS6 [1]	IIS7 [2]	IIS7.5 [3]	mod_ssl	mod_gnutls	JSSE [4,6]	NSS [5]
RSA	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHE-RSA	No	Yes	Yes	Yes	Yes	Yes	Yes
DHE-DSS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ECDHE-RSA	No	Yes	Yes	Yes[7,8]	No	Yes	No (Default)
ECDH-RSA	No	No	No	Yes	No	Yes	No (Default)
ECDHE-ECDSA	No	Yes	Yes	Yes	No	Yes	No (Default)
ECDH-ECDSA	No	No	No	Yes	No	Yes	No (Default)
ADH		No	No	No	No	No	No

1 Windows 2003 | 2 Windows 2008 | 3 Windows 2008 R2 | 4 Tomcat | 5 Network Security Services (Apache, Redhat, Sun Java Enterprise.)

🟦 Recommended

[6] http://download.oracle.com/javase/6/docs/technotes/guides/security/SunProviders.html#SunJSSEProvider

[7] https://issues.apache.org/bugzilla/show_bug.cgi?id=40132

[8] ECCdraft suite – after 1.0 included in ALL

Default RSA size support

RSA public-key cryptosystem is an asymmetric encryption method (public-key cryptography), it can be used for signing as well as encryption. In SSL/TLS RSA is used during key exchange (handshake). RSA bases its security on the length of the modulus that must be factored. The bigger the modulus the harder it is to break the algorithm.

Server RSA key size, DH and SRP prime support

This list the key sizes that are supported by Major Web servers, there is no server side restriction to use 1024 bit instead of 2048. Performance issues should not be of concern for most providers; TLS introduced caching and session resumption, reducing the RSA computations to a minimum. On windows the tool "Harden SSL/TLS" also allows tweaking the TLS session caching for IIS.

RSA Modulus	IIS6 [1]	IIS7 [2]	IIS7.5 [3]	mod_ssl	mod_tls [4]	JSSE	NSS [5]
1024	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2048	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4096	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Server Cipher support [i]

In order for this list to stay focused on best practices we display modern or strong ciphers only and beta versions of SSL engines are taken into account.

Cipher	Size	IIS6 [1]	IIS7 [2]	IIS7.5 [3]	mod_ssl	mod_tls [4]	JSSE	NSS [5]
AES	128	No	Yes	Yes	Yes	Yes	Yes	Yes
AES	256	No	Yes	Yes	Yes	Yes	Yes	Yes
AES-GCM	128	No	No	Yes	Yes	No	No	No
AES-GCM	256	No	No	Yes	Yes	No	No	No
RC4	128	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Camellia	128	No	No	No	Yes	Yes	No	Yes
Camellia	256	No	No	No	Yes	Yes	No	Yes
3DES	156	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1 Windows 2003 | 2 Windows 2008 | 3 Windows 2008 R2 | 4 Tomcat | 5 Network Security Services (Apache, Redhat, Sun Java Enterprise...)

Recommend Server-Side SSL configuration - Putting it all together -

Taking into account the previous client and server compatibility matrixes it is apparent that the best setup to use has changed over the years. Protocols have been enhanced and weaknesses patched and encryption strengthened.

IIS7.5

These are the cipher suites that offer most security and compatibility, no SSLv2 and SSlv3 support should be provided at all.

Cipher suite name	Protocol	KeyX	Auth	Enc	bit	Hash	Comp.
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384	TLS 1.2	ECDHE	ECDSA	AES	256	SHA2	🟫
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA*	TLS 1.0	ECDHE	RSA	AES	256	SHA	🟥🟫🟧
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA*	TLS 1.0	ECDHE	RSA	AES	128	SHA	🟥🟫🟧
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	DHE	RSA	AES	256	SHA	🟥🟩🟫🟨🟧
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	DHE	RSA	AES	128	SHA	🟥🟩🟫🟨🟧
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	RSA	RSA	RC4	128	SHA	🟦🟥🟩🟨🟫🟧
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS 1.0	DHE	DSS	3DES	168	SHA	🟦🟥🟩🟨🟫🟧

🟥 Firefox & Chrome (NSS)
🟩 Opera
🟦 Windows XP/2000/2003 (IE7/IE8, Safari)
🟫 Windows 7/2008R2 (IE8) (Safari excluded)
🟧 Windows Vista/2008R1 (IE8/IE7 ,Safari)
🟨 Safari (MacOSx)

* RSA chosen over ECDSA due to the current lack of ECC certificate authorities, once ECC certificates are available we recommend offering TLS_ECDHE_**ECDSA**_WITH_AES_256_CBC_SHA

IIS7

These are the cipher suites that offer most security and compatibility for IIS7

Cipher suite name	Protocol	KeyX	Auth	Enc	bit	Hash	Comp.
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA*	TLS 1.0	ECDHE	RSA	AES	256	SHA	🟥🟫🟧
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA*	TLS 1.0	ECDHE	RSA	AES	128	SHA	🟥🟫🟧
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	DHE	RSA	AES	256	SHA	🟥🟩🟫🟨🟧
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	DHE	RSA	AES	128	SHA	🟥🟩🟫🟨🟧
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	RSA	RSA	RC4	128	SHA	🟦🟥🟩🟨🟫🟧
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS 1.0	DHE	DSS	3DES	168	SHA	🟦🟥🟩🟨🟫🟧

- 🟥 Firefox & Chrome
- 🟩 Opera
- 🟦 Windows XP/2000/2003 (IE7/IE8) + Safari (All windows OS up to 2008R2)
- 🟫 Windows 7/2008R2 (IE8)
- 🟧 Windows Vista/2008R1 (IE8/7)
- 🟨 Safari (MacOSx)

* Chosen over ECDSA due to the current lack of ECC certificate authorities, once ECC certificates are available we recommend offering TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

IIS6 [9] [10]

These are the cipher suites that offer most security and compatibility for IIS6

Cipher suite name	Protocol	KeyX	Auth	Enc	bit	Hash	Comp.
TLS_DHE_RSA_WITH_AES_256_CBC_SHA*	TLS 1.0	DHE	RSA	AES	256	SHA	🟥🟩🟫🟨🟧
TLS_DHE_RSA_WITH_AES_128_CBC_SHA*	TLS 1.0	DHE	RSA	AES	128	SHA	🟥🟩🟫🟨🟧
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	RSA	RSA	RC4	128	SHA	🟦🟥🟩🟨🟫🟧
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS 1.0	DHE	DSS	3DES	168	SHA	🟦🟥🟩🟨🟫🟧

* IIS6 will support AES only after the installation of a Hotfix (which is recommended)

- 🟥 Firefox & Chrome
- 🟩 Opera
- 🟦 Windows XP/2000/2003 (IE7/IE8) for Chrome + Safari (All windows OS up to 2008R2)
- 🟫 Windows 7/2008R2 (IE8)
- 🟧 Windows Vista/2008R1 (IE8/7)
- 🟨 Safari (MacOSx)

[9] http://support.microsoft.com/?scid=kb;en-us;245030&x=14&y=11

[10] http://www.gorlani.com/publicprj/CipherControl/

Apache https / Tomcat (OpenSSL 1.0)

We are aware that OpenSSL 1.0 is currently beta only, this guide however was intended to be future proof [11] to a certain degree, to achieve this Elliptic Cryptography is mandatory.

Cipher suite name	Protocol	KeyX	Auth	Enc	bit	Hash	Comp.
ECDHE-RSA-AES256-SHA*	TLS 1.0	ECDHE	ECDSA	AES	256	SHA	🟥🟫🟧
ECDHE-RSA-AES128-SHA*	TLS 1.0	ECDHE	ECDSA	AES	128	SHA	🟥🟫🟧
DHE-RSA-AES256-SHA	TLS 1.0	DHE	RSA	AES	256	SHA	🟥🟩🟫🟨🟧
DHE-RSA-AES128-SHA	TLS 1.0	DHE	RSA	AES	128	SHA	🟥🟩🟫🟨🟧
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	RSA	RSA	RC4	128	SHA	🟦🟥🟩🟨🟫🟧
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS 1.0	DHE	DSS	3DES	168	SHA	🟦🟥🟩🟨🟫🟧

🟥 Firefox & Chrome
🟩 Opera
🟦 Windows XP/2000/2003 (IE7/IE8) - Chrome + Safari (All windows OS up to 2008R2)
🟫 Windows 7/2008R2 (IE8)
🟧 Windows Vista/2008R1 (IE8/7)
🟨 Safari (MacOSx)

* Chosen over ECDSA due to the current lack of ECC certificate authorities, once ECC certificates are available we recommend offering TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

[11] http://mail-archives.apache.org/mod_mbox/httpd-cvs/200911.mbox/%3C20091110075514.166A6238890A@eris.apache.org%3E

Thanks

We would like to thank Ivan Ristic (SSL Labs) and Marsh Ray for the support and the information provided. We would like to thank Opera for their feedback on Opera TLS compatibility.

Disclaimer

The Information is believed to be accurate by the time of writing.

Copyright

With heavy support from SSLLAB (Ivan Ristic)