

Network Working Group
Internet-Draft
Category: Best Current Practice
Intended status: Standards Track
Expires: May 4, 2014

W. Hoehlhubmer
Nov 4, 2013

**Informational Add-on for HTTP over
the Secure Sockets Layer (SSL) Protocol and/or
the Transport Layer Security (TLS) Protocol**
[draft-hoehlhubmer-https-upd-00](#)

Abstract

This document describes an Add-on as a good practice for websites providing encrypted connectivity.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 24, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Implementing of this Add-on	3
2.1.	Content of this Add-on	3
2.1.	Formating of this Add-on	4
3.	IANA Considerations	4
4.	Security Considerations	4
5.	Acknowledgements	4
6.	Recommendations	4
7.	References	5
7.1.	Normative References	5
7.2.	Informative References	5
7.2.1.	Informative References (Cipher Suites)	6
8.	Discussions	6
Appendix A.	Script Examples	6
Appendix B.	Add-on Sample Content	8
	Author's Address	10

[1.](#) Introduction

Encrypted connections are not limited to just one encryption algorithm.

A few encryption algorithms, a short and incomplete complete list:

- (1) Advanced Encryption Standard (AES)
- (2) Data Encryption Standard (DES, 3DES)
- (3) Ron's Code 4 (RC4)

As an example a list of some kinds of the Camellia encryption algorithm (names taken from OpenSSL help [[OPENSSL](#)]):

- (1) camellia-128-cbc: 128-bit Camellia encryption in CBC mode
- (2) camellia-128-ecb: 128-bit Camellia encryption in ECB mode
- (3) camellia-192-cbc: 192-bit Camellia encryption in CBC mode
- (4) camellia-192-ecb: 192-bit Camellia encryption in ECB mode
- (5) camellia-256-cbc: 256-bit Camellia encryption in CBC mode
- (6) camellia-256-ecb: 256-bit Camellia encryption in ECB mode

Only the X.509 Certificates are static, all other informations

depend on the capabilities of the used web browser.

Because not every browser allows you to view all these informations, it is a good practice placing an Uniform Resource Locator (URL) to this informations on the main page of the website.

With most browsers you can view the used X.509 certificates of the actual session, but have no direct comparison if they are the correct ones. The X.509 certificates which are shown by the browser and these from this Add-on MUST match; other ways there is going on a man-in-the-middle attack.

2. Implementing this Add-on

This Add-on is just one page of the website. Its content MUST be completely generated on server side. For doing so see the sample scripts at [Appendix A](#). Presenting the content in sorted order is OPTIONAL.

2.1. Content of this Add-on

The informations MUST be the following:

- (1) The actual date and time in [[RFC2822](#)] format,
that MUST NOT differ more than 5 seconds from actual date/time
- (2) The cipher specification name
- (3) Number of cipher bits (actually used)
- (4) Number of cipher bits (possible)
- (5) The SSL Protocol version: SSLv2, SSLv3, TLSv1, TLSv1.1, TLSv1.2,
...
- (6) If cipher is an export cipher: false, true
- (7) If secure renegotiation is supported: false, true
- (8) Algorithm used for the public key of server's certificate
- (9) Algorithm used for the signature of server's certificate
- (10) Issuer DN of server's certificate
- (11) Subject DN in server's certificate
- (12) The serial of the server certificate
- (13) The version of the server certificate
- (14) Validity of server's certificate (start time)
- (15) Validity of server's certificate (end time)
- (16) Client certificate verification:
NONE, SUCCESS, GENEROUS or FAILED:reason
- (17) SSL compression method negotiated: NULL when disabled

For connections where X.509 certificates are used for authentication
these informations are RECOMMENDED:

Hoehlhubmer

Expires May 4, 2014

[Page 3]

- (18) Algorithm used for the public key of client's certificate
- (19) Algorithm used for the signature of client's certificate
- (20) Issuer DN of client's certificate
- (21) Subject DN in client's certificate
- (22) The serial of the client certificate
- (23) The version of the client certificate
- (24) Validity of client's certificate (start time)
- (25) Validity of client's certificate (end time)
- (26) Number of days until client's certificate expires

This information MAY be given:

- (27) The hex-encoded SSL session id

These OPTIONAL informations depend on the used software:

- (28) The SSL-module program version: e.g. Apache mod_ssl version
- (29) The SSL program version: e.g. OpenSSL version

See [Appendix B](#) for a sample content.

2.2. Formating of this Add-on

I RECOMMEND to present this information simple. You MAY use HTML, but you MUST NOT make use of any client side scripting:
e.g. Javascript.

Any design or formatting, also the translation to another language as English is allowed.

Simple plain ASCII-Text is fine, too.

3. IANA Considerations

There are no requests for IANA actions in this document.

4. Security Considerations

When implementing this information as a popup window in the browser, this information MUST also be available with enabled popup-blocker.

The Implementation MUST NOT use any scripts, that run on client side:
e.g. Javascript, ...

There SHOULD also be no references to other websites inside this Add-on page.

5. Acknowledgements

6. Recommendations

I recommend using a standardized URL, for more see [Section 8](#).

7. References

7.1. Normative References

- [HTTPTLS] Rescorla, E., "HTTP over TLS", [RFC 2818](#), May 2000.
- [PKIX] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 "Public Key Infrastructure Certificate and Certificate Restoration List (CRL) Profile", [RFC 3280](#), April 2002.
- [SSLv3] Freier, A., Karlton, P., and P. Kocher, "The Secure Sockets Layer (SSL) Protocol Version 3.0", [RFC 6101](#), August 2011.
- [TLSv1] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", [RFC 2246](#), January 1999.
- [TLSv1.1] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", [RFC 4346](#), April 2006.
- [TLSv1.2] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), August 2008.
- [URL] Berners-Lee, T., Masinter, L., and M. McCahill, "Uniform Resource Locators (URL)", [RFC 1738](#), December 1994.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2822] Resnick, P., Ed., "Internet Message Format", [RFC 2822](#), April 2001.

7.2. Informative References

- [CAMELLIA] Matsui, M., Nakajima, J., and S. Moriai, "A Description of the Camellia Encryption Algorithm", [RFC 3713](#), April 2004.
- [CGI] Robinson, D. and K. Coar, "The Common Gateway Interface (CGI) Version 1.1", [RFC 3875](#), October 2004.
- [HTML2.0] Berners-Lee, T. and D. Connolly, "Hypertext Markup Language - 2.0", [RFC 1866](#), November 1995.
- [MD5] Rivest, R., "The MD5 Message-Digest Algorithm", [RFC 1321](#), April 1992.
- [SHA1] Eastlake 3rd, D. and P. Jones, "US Secure Hash

Algorithm 1 (SHA1)", [RFC 3174](#), September 2001.

[OPENSSL] OpenSSL Cryptography and SSL/TLS Toolkit at
<http://www.openssl.org/>

7.2.1. Informative References (Cipher Suites)

- [RFC3268] Chown, P., "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", [RFC 3268](#), June 2002.
- [RFC4279] Eronen, P., Ed., and H. Tschofenig, Ed., "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", [RFC 4279](#), December 2005.
- [RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", [RFC 4492](#), May 2006.
- [RFC4785] Blumenthal, U. and P. Goel, "Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)", [RFC 4785](#), January 2007.
- [RFC5288] Salowey, J., Choudhury, A., and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS", [RFC 5288](#), August 2008.
- [RFC5469] Eronen, P., Ed., "DES and IDEA Cipher Suites for Transport Layer Security (TLS)", [RFC 5469](#), February 2009.
- [RFC5489] Badra, M. and I. Hajjeh, "ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)", [RFC 5489](#), March 2009.
- [RFC5932] Kato, A., Kanda, M., and S. Kanno, "Camellia Cipher Suites for TLS", [RFC 5932](#), June 2010.

8. Discussions

It MAY be good to have an standardized URL for this Add-on;
e.g. <https://www.example.com/sslinfo/>
in case the word "ssl" is already part of the URL's subdomain:
e.g. ssl.example.com or www-ssl.example.com, then
<https://ssl.example.com/info/> or https://www-ssl.example.com/info
are also fine for this standardized URL.

Appendix A. Script Examples

Use the following script examples as a template for your implementation of this Add-on.

The first two examples generate identical content, the third example presents the content of [Section 2.1](#). unsorted.

Example 1. CGI-script, used on Linux systems

```
#!/bin/sh

printf "Content-type: text/plain\n\n"

printf "SSL informations: $(date --rfc-2822)\n"
printf "=====\n\n"

if [ "$HTTPS" == "on" ]; then
    env | grep --regexp="^SSL_" | sort
else
    printf "No SSL information available.\n"
fi
```

Example 2. PHP-script

```
<?php

header( "Content-type: text/plain" );

print "SSL informations: " . date( "r" ) . "\r\n";
print "=====\r\n\r\n";

if ( isset( $_SERVER['HTTPS'] ) && ( $_SERVER['HTTPS'] == "on" ) ) {
    $list = array( );
    $nbrOfValues = 0;
    foreach ( $_SERVER as $key => $value ) {
        if ( substr( $key, 0, 4 ) == "SSL_" ) {
            $list[ $nbrOfValues++ ] = $key . "=" . $value;
        }
    }
    sort( $list );    // sort content before printing ...
    for ( $i = 0; $i < $nbrOfValues; $i++ ) {
        print $list[ $i ] . "\r\n";
    }
}
else {
    echo "No SSL information available.\r\n";
}
?>
```


Example 3. CGI-script (a compiled C program)

```
/* Compiles with GNU C compiler on Linux, Windows, ...
 *
 * When using Microsoft C/C++ in Windows, strftime format specifiers
 * for timezone behave in a non-standard way;
 */

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <time.h>

#ifdef __linux__
#include <unistd.h>
#endif

int main( int argc, char* argv[ ], char** envp )
{
    /* char* envp[ ] */
    char* psz;
    char szDateTime[ 80 ];

    time_t tnow = time( NULL );
    struct tm* tmnow = localtime( &tnow );

    strftime( szDateTime, sizeof( szDateTime ) - 4,
        "%a, %d %b %Y %H:%M:%S %z", tmnow );

    printf( "Content-type: text/plain\r\n\r\n" );

    printf( "SSL informations: %s\r\n", szDateTime );
    printf( "=====\r\n\r\n" );

    if ( ( psz = getenv( "HTTPS" ) ) && ( strcmp( psz, "on" ) == 0 ) )
    {
        char** ppsz = envp;

        /* print content without sorting ... */
        while ( ppsz && *ppsz )
        {
            if ( strncmp( *ppsz, "SSL_", 4 ) == 0 )
                printf( "%s\r\n", *ppsz );
            ppsz++;
        }
    }
    else
        printf( "No SSL information available.\r\n" );

    return 0;
}
```

}

Appendix B. Add-on Sample Content

The first example shows a complete Add-on sample content generated by one of the scripts in [Appendix A](#), the other example shows only that differs when using another browser.

For meaning of the numbers in brackets see [Section 2.1](#).

Example 1. A complete sample content

```

SSL informations: Thu, 01 Jan 1970 00:00:00 +0000           (1)
=====

SSL_CIPHER=AES256-SHA                                     (2)
SSL_CIPHER_ALGKEYSIZE=256                                 (4)
SSL_CIPHER_EXPORT=false                                    (6)
SSL_CIPHER_USEKEYSIZE=256                                 (3)
SSL_CLIENT_VERIFY=NONE                                    (16)
SSL_COMPRESS_METHOD=NULL                                  (17)
SSL_PROTOCOL=TLSv1                                        (5)
SSL_SECURE_RENEG=true                                     (7)
SSL_SERVER_A_KEY=rsaEncryption                            (8)
SSL_SERVER_A_SIG=sha1WithRSAEncryption                    (9)
SSL_SERVER_I_DN=/C=--/O=SomeOrg/OU=SomeOrgUnit/CN=Root CA (10)
SSL_SERVER_I_DN_C=--                                     (10)
SSL_SERVER_I_DN_CN=Root CA                               (10)
SSL_SERVER_I_DN_O=SomeOrg                                 (10)
SSL_SERVER_I_DN_OU=SomeOrgUnit                           (10)
SSL_SERVER_M_SERIAL=01                                    (12)
SSL_SERVER_M_VERSION=3                                    (13)
SSL_SERVER_S_DN=/C=AT/CN=www.example.com                  (11)
SSL_SERVER_S_DN_C=AT                                     (11)
SSL_SERVER_S_DN_CN=www.example.com                        (11)
SSL_SERVER_V_END=Dec 31 23:59:59 1970 GMT                  (15)
SSL_SERVER_V_START=Jan 01 00:00:00 1970 GMT                (14)
SSL_SESSION_ID=0000000000000000000000000000000000000000 (27)
SSL_VERSION_INTERFACE=mod_ssl/2.2.15                      (28)
SSL_VERSION_LIBRARY=OpenSSL/1.0.0-fips                     (29)

```


Example 2.

```
SSL informations: Thu, 01 Jan 1970 00:00:00 +0000
```

```
=====
```

```
...
```

```
SSL_CIPHER=RC4-MD5
```

```
SSL_CIPHER_ALGKEYSIZE=128
```

```
SSL_CIPHER_EXPORT=false
```

```
SSL_CIPHER_USEKEYSIZE=128
```

```
SSL_CLIENT_VERIFY=NONE
```

```
SSL_COMPRESS_METHOD=NULL
```

```
SSL_PROTOCOL=SSLv3
```

```
SSL_SECURE_RENEG=false
```

```
...
```

Author's Address

Walter Hoehlhubmer

Lederergasse 47a

A-4020 Linz

Austria, EUROPE

E-Mail: walter.h@mathemainzel.info

