Abstract

This document specifies some cryptographic algorithms which will be used for the Mutual user authentication method for the Hyper-text Transport Protocol (HTTP).

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 January 5, 2012.

Copyright Notice

Copyright (c) 2011 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.
1. Introduction

This document specifies some algorithms for Mutual authentication protocol for Hyper-Text Transport Protocol (HTTP) [draft-oiwa-http-mutualauth].

1.1. Terminology

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

The terms "encouraged" and "advised" are used for suggestions that do not constitute "SHOULD"-level requirements. People MAY freely choose not to include the suggested items regarding [RFC2119], but complying with those suggestions would be a best practice; it will improve the security, interoperability, and/or operational performance.

The term "natural numbers" refers to the non-negative integers (including zero) throughout this document.

2. Authentication Algorithms

This document specifies only one family of the authentication algorithm. The family consists of four authentication algorithms, which only differ in their underlying mathematical groups and security parameters. The algorithms do not add any additional fields. The tokens for these algorithms are

- iso-kam3-dl-2048-sha256: for the 2048-bit discrete-logarithm setting with the SHA-256 hash function.
- iso-kam3-dl-4096-sha512: for the 4096-bit discrete-logarithm setting with the SHA-512 hash function.
- iso-kam3-ec-p256-sha256: for the 256-bit prime-field elliptic-curve setting with the SHA-256
hash function.
- iso-kam3-ec-p521-sha512: for the 521-bit prime-field elliptic-curve setting with the SHA-512 hash function.

For discrete-logarithm settings, the underlying groups are the 2048-bit and 4096-bit MODP groups defined in [RFC3526], respectively. See Appendix A for the exact specifications of the groups and associated parameters. The hash functions H are SHA-256 for the 2048-bit group and SHA-512 for the 4096-bit group. The representation of the fields wa, wb, oa, and ob is base64-fixed-number.

For the elliptic-curve settings, the underlying groups are the elliptic curves over the prime fields P-256 and P-521, respectively, specified in the appendix D.1.2 of FIPS PUB 186-3 [FIPS.186-3.2009] specification. The hash functions H, which are referenced by the core document, are SHA-256 for the P-256 curve and SHA-512 for the P-521 curve, respectively, defined in FIPS PUB 180-2 [FIPS.180-2.2002]. The representation of the fields wa, wb, oa, and ob is hex-fixed-number.

Note: This algorithm is based on the Key Agreement Mechanism 3 (KAM3) defined in Section 6.3 of ISO/IEC 11770-4 [ISO.11770-4.2006] with a few modifications/improvements. However, implementers should use this document as the normative reference, because the algorithm has been changed in several minor details as well as major improvements.

2.1. Support functions and notations

The algorithm definitions use several support functions and notations defined below:

The integers in the specification are in decimal, or in hexadecimal when prefixed with "0x".

The two functions named octet() and OCTETS() are those defined in the core specification [draft-oiwa-http-mutualauth].

Note: The definition of OCTETS() is different from the function GE2OS_x in the original ISO specification, which takes the shortest representation without preceding zeros.

All of the algorithms defined in this specification use the default functions defined in the core specification for functions pi, o_A and o_B.

2.2. Functions for discrete-logarithm settings

In this section, an equation \((x / y \mod z)\) denotes a natural number \(w\) less than \(z\) that satisfies \((w \times y) \mod z = x \mod z\).

For the discrete-logarithm, we refer to some of the domain parameters by using the following symbols:

- \(q\): for "the prime" defining the MODP group.
- \(g\): for "the generator" associated with the group.
- \(r\): for the order of the subgroup generated by \(g\).

The function \(J\) is defined as

\[ J(\pi) = g^{\pi} \mod q. \]
The value of $w_A$ is derived as

$$w_A = g^{s_A} \mod q,$$

where $s_A$ is a random integer within range $[1, r-1]$ and $r$ is the size of the subgroup generated by $g$. In addition, $s_A$ MUST be larger than $\log(q)/\log(g)$ (so that $g^{s_A} > q$).

The value of $w_A$ SHALL satisfy $1 < w_A < q-1$. The server MUST check this condition upon receipt.

The value of $w_B$ is derived from $J(\pi)$ and $w_A$ as:

$$w_B = (J(\pi) \cdot w_A^{(H(\text{octet}(1) \mid OCTETS(w_A)) \cdot s_B}) \mod q,$$

where $s_B$ is a random number within range $[1, r-1]$. The value of $w_B$ MUST satisfy $1 < w_B < q-1$. If this condition is not held, the server MUST retry using another value for $s_B$. The client MUST check this condition upon reception.

The value $z$ on the client side is derived by the following equation:

$$z = w_B^{(s_A + H(\text{octet}(2) \mid OCTETS(w_A) \mid OCTETS(w_B))) / (s_A \cdot H(\text{octet}(1) \mid w_A) + \pi) \mod r} \mod q.$$

The value $z$ on the server side is derived by the following equation:

$$z = (w_A \cdot g^{H(\text{octet}(2) \mid OCTETS(w_A) \mid OCTETS(w_B))})^{s_B} \mod q.$$

### 2.3. Functions for elliptic-curve settings

For the elliptic-curve setting, we refer to some of the domain parameters by the following symbols:

- **q**: for the prime used to define the group.
- **G**: for the defined point called the generator.
- **r**: for the order of the subgroup generated by $G$.

The function $P(p)$ converts a curve point $p$ into an integer representing point $p$, by computing $x \cdot 2 + (y \mod 2)$, where $(x, y)$ are the coordinates of point $p$. $P'(z)$ is the inverse of function $P$, that is, it converts an integer $z$ to a point $p$ that satisfies $P(p) = z$. If such $p$ exists, it is uniquely defined. Otherwise, $z$ does not represent a valid curve point. The operator $+$ indicates the elliptic-curve group operation, and the operation $[x] \cdot p$ denotes an integer-multiplication of point $p$: it calculates $p + p + ...$ ($x$ times) $+ p$. See the literatures on elliptic-curve cryptography for the exact algorithms used for those functions (e.g. Section 3 of [RFC6090], which uses different notations, though.) $0_E$ represents the infinity point. The equation $(x / y \mod z)$ denotes a natural number $w$ less than $z$ that satisfies $(w \cdot y) \mod z = x \mod z$.

The function $J$ is defined as

$$J(\pi) = [\pi] \cdot G.$$

The value of $w_A$ is derived as
\[ w_A = P(W_A), \] where \( W_A = [s_A] * G, \]

where \( s_A \) is a random number within range \([1, r-1]\). The value of \( w_A \) MUST represent a valid curve point, and \( W_A \) SHALL NOT be \( 0_E \). The server MUST check this condition upon reception.

The value of \( w_B \) is derived from \( J(pi) \) and \( W_A = P'(w_A) \) as:

\[ w_B = P(W_B), \] where \( W_B = [s_B] * (J(pi) + [H(octet(1) | OCTETS(w_A)]) * W_A), \]

where \( s_B \) is a random number within range \([1, r-1]\). The value of \( w_B \) MUST represent a valid curve point and satisfy \([4] * P'(w_B) <> 0_E \). If this condition is not satisfied, the server MUST retry using another value for \( s_B \). The client MUST check this condition upon reception.

The value \( z \) on the client side is derived by the following equation:

\[
z = P([s_A + H(octet(2) | OCTETS(w_A) | OCTETS(w_B))] / (s_A * H(octet(1) | OCTETS(w_A)) + pi) mod r] * W_B), \]

where \( W_B = P'(w_B) \).

The value \( z \) on the server side is derived by the following equation:

\[
z = P([s_B] * (W_A + [H(octet(2) | OCTETS(w_A) | OCTETS(w_B)]) * G)), \]

where \( W_A = P'(w_A) \).

### 3. IANA Considerations

Four tokens iso-kam3-dl-2048-sha256, iso-kam3-dl-4096-sha512, iso-kam3-ec-p256-sha256 and iso-kam3-ec-p521-sha512 shall be allocated and registered according to the provision of the core documentation when this document is promoted to an RFC.

Note: More formal declarations will be added in the future drafts to meet the RFC 5226 requirements.

### 4. Security Considerations

Refer the corresponding section of the core specification for algorithm-independent, generic considerations.

- All random numbers used in these algorithms MUST be at least cryptographically computationally secure against forward and backward guessing attacks.
- Computation times of all numerical operations on discrete-logarithm group elements and elliptic-curve points MUST be normalized and made independent of the exact values, to prevent timing-based side-channel attacks.

### 5. Notice on intellectual properties

The National Institute of Advanced Industrial Science and Technology (AIST) and Yahoo! Japan, Inc. has jointly submitted a patent application on the protocol proposed in this documentation to the Patent Office of Japan. The patent is intended to be open to any implementors of this protocol and its variants under non-exclusive royalty-free manner. For the details of the patent application and its status, please contact the author of this document.

The elliptic-curve based authentication algorithms might involve several existing third-party patents. The authors of the document take no position regarding the validity or scope of such patents, and other patents as well.
6. References

6.1. Normative References


6.2. Informative References


Appendix A. (Informative) Group parameters for discrete-logarithm based algorithms

The MODP group used for the iso-kam3-dl-2048-sha256 algorithm is defined by the following parameters.

The prime is:

\[
q = 0x\text{FFFFFFF} \text{FFFFFFF} \text{C90FDA} \text{A2168C234} \text{C4628B} \text{80DC1CD1} \\
29024E08 \text{8A67CC74} \text{020B9E06} \text{3B139B22} \text{51A0879} \text{8E3404DD} \\
\text{EF9519B3} \text{CD3A431B} \text{302BA6D} \text{F2F1437} \text{4FE1356D} \text{6D51C245} \\
\text{E4B5B76} \text{62B7E6C6} \text{F44C42E9} \text{A6376EDB} \text{0BFFC56} \text{F4067ED} \\
\text{EE386BFB} \text{5A899FA5} \text{AE9F2411} \text{7C4B1FE6} \text{49286651} \text{ECE45BD} \\
\text{C2007CB8} \text{1A63BF05} \text{98DA4836} \text{1C55D39A} \text{69163FA} \text{F2D4CF5F} \\
\text{83655D23} \text{DCA3AD96} \text{1C62F356} \text{208552BB} \text{9ED52907} \text{709696ED} \\
\text{E70C354E} \text{4ABC9804} \text{F1746C08} \text{CA18217C} \text{32905E46} \text{2E36CE3B} \\
\text{E39BE72C} \text{810E8063} \text{9B2783A2} \text{EC07A28F} \text{B5C55DF0} \text{6F4C52C9} \\
\text{DEZBC9F6} \text{95581718} \text{3995497C} \text{EA956AE5} \text{15D22618} \text{98FA0510} \\
\text{15728E5A} \text{8AACAA68} \text{FFFFFFFF} \text{FFFFFFFF}.
\]
The generator is:

\[ g = 2. \]

The size of the subgroup generated by \( g \) is:

\[ r = \frac{(q - 1)}{2} \]

The MODP group used for the iso-kam3-dl-4096-sha512 algorithm is defined by the following parameters.

The prime is:

\[ q = 0xFFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74 02B8E6A 3B139B22 514A0879 8E3404DD EF9519B3 CD3A411B 302B0A6D F25F1437 4E1356D 651C245 E485B76 42EBFEF6 A637ED6B 0BF5CBE F46B7ED EE3B6FBF 5A999AFA 5E9F2411 7C4B1F6E 49286651 ECE45B3D C2007CB8 A163BF05 90DA4836 1C55D39A 69163FA8 FD24CF5F 8365D23 D3CA3D96 1C62F356 208552BB 9ED52907 709696D6 670C534A 4ABC9804 F1746C08 CA18217C 32905646 2E36CE3B E39E772C 180E8603 9B2783A2 EC07A28F B5C55DFF 6F4C52C9 DE2B8CF6 95581718 39954997 EA956AE5 15D2261B 98FA0510 15728E5A 8A6AC42D AD3170D 04507A33 A8521AAB DF1CA64 ECFBB804 58DBEF0A 8AE71157 5D5606CD 93B770F8 5A61E4C7 ABF5ABED DB093D7D 1E8C94E0 4A25619D CEE3DD26 1AD2EE6B F12FFA06 9D8A0864 D8760273 3EC86A64 521F2B18 177B200C BE11B77E 7A619D6C 770998C0 BAD946E2 08E2FA0A 74E5AB31 43DBB5FE 0EFDD108 4BB2D120 A9210801 A1723C12 A787E6D7 88719A10 BDBA5B26 99C32718 6AF4E22C 1A946834 B6150BDA 25839CA 2AD4CECE DBBCC2DB 04DE8EF9 28E8EC14 1FBECA6A 287C5947 4E6BCC0D 99B2964F A090C3A2 233BA186 515BE7ED 1F612970 CEE2D7AF B81BBDD76 2170481C D0069127 D5B05AA9 93B4EA98 8DFD8DC1 86FBB7DC 90AAC60F 4DF435C9 34063199 FFFFFE FFFFFF. 

The generator is:

\[ g = 2. \]

The size of the subgroup generated by \( g \) is:

\[ r = \frac{(q - 1)}{2} \]

-7-
Appendix B. (Informative) Derived numerical values

This section provides several numerical values for implementing this protocol, derived from the above specifications. The values shown in this section are for informative purposes only.

<table>
<thead>
<tr>
<th>dl-2048</th>
<th>dl-4096</th>
<th>ec-p256</th>
<th>ec-p521</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size of w_A etc.</td>
<td>2048</td>
<td>4096</td>
<td>257</td>
</tr>
<tr>
<td>Size of H(...)</td>
<td>256</td>
<td>512</td>
<td>256</td>
</tr>
<tr>
<td>length of OCTETS(w_A) etc.</td>
<td>256</td>
<td>512</td>
<td>33</td>
</tr>
<tr>
<td>length of wa, wb field values.</td>
<td>346 *</td>
<td>686 *</td>
<td>66</td>
</tr>
<tr>
<td>length of oa, ob field values.</td>
<td>46 *</td>
<td>90 *</td>
<td>64</td>
</tr>
<tr>
<td>minimum allowed s_A</td>
<td>2048</td>
<td>4096</td>
<td>1</td>
</tr>
</tbody>
</table>

(The numbers marked with an * include enclosing quotation marks.)

Appendix C. (Informative) Draft Change Log

C.1. Changes in revision 00

The document is separated from the revision 08 of the core documentation.

Authors’ Addresses

Yutaka Oiwa
National Institute of Advanced Industrial Science and Technology
Research Center for Information Security
Room #1003, Akihabara Daibiru
1-18-13 Sotokanda
Chiyoda-ku, Tokyo
JP
Phone: +81 3-5298-4722
Email: mutual-auth-contact@m.aist.go.jp
Hajime Watanabe
National Institute of Advanced Industrial Science and Technology

Hiromitsu Takagi
National Institute of Advanced Industrial Science and Technology

Yuichi Ioku
Yahoo! Japan, Inc.
Midtown Tower
9-7-1 Akasaka
Minato-ku, Tokyo
JP

Tatsuya Hayashi
Lepidum Co. Ltd.
#602, Village Sasazuka 3
1-30-3 Sasazuka
Shibuya-ku, Tokyo
JP