ECC Groups For IKEv2
<draft-ietf-ipsec-ikev2-ecc-groups-01.txt>

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Abstract

This document describes ECC groups for use as Diffie-Hellman groups in the Internet Key Exchange version 2 (IKEv2) protocol. These new groups are defined to align IKEv2 with other standards, particularly NIST standards, and with and to provide more efficient implementation than in previously defined groups.
1. Introduction

This document describes default groups for use in elliptic curve Diffie-Hellman in IKEv2 in addition to the groups already so defined.

The IKEv2 document [IKEv2] defines Diffie-Hellman groups 1 and 2 from [IKE] for use in IKEv2. The IKEv2 algorithms document [ALGS] defines group 2 as well as group 14 from [RFC-3526] for IKEv2. (The numbering of the groups is as in [IANA].) All three of these groups are MODP modular exponentiation groups.

This document defines ECP type elliptic curve groups for use in IKEv2. This is done for four reasons:

1. To enable IKEv2 to be implemented in a way that enjoys the computational and bandwidth advantages of elliptic curves over modular exponentiation groups.

2. To align IKEv2 with existing ECC standards, particularly those of NIST.

3. To provide a common elliptic curve environment for users of IKE and IKEv2.

4. The groups proposed are capable of providing security consistent with the new Advanced Encryption Standard.

In addition, it is anticipated that the availability of standardized groups will result in optimizations for a particular curve and field size as well as allowing precomputation that could result in faster implementations.

In summary, due to the performance advantages of elliptic curve groups in IKEv2 implementations and the need for further alignment with other standards, this document defines three elliptic curves for IKEv2.

2. ECC Groups

IKEv2 implementations SHOULD support the following three Diffie-Hellman groups.

<table>
<thead>
<tr>
<th>Group Number</th>
<th>Group Type</th>
<th>Bit Length</th>
<th>Defined</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>ECP</td>
<td>256</td>
<td>[IKE-ECP]</td>
</tr>
<tr>
<td>20</td>
<td>ECP</td>
<td>384</td>
<td>[IKE-ECP]</td>
</tr>
<tr>
<td>21</td>
<td>ECP</td>
<td>521</td>
<td>[IKE-ECP]</td>
</tr>
</tbody>
</table>
The details of the three groups are given in [IKE-ECP], in which they are defined for use in the original version of IKE. The group numbers correspond to the anticipated IANA identifiers. For a full list of Diffie-Hellman groups, see [IANA] or [ECG].

3. Alignment with Other Standards

The following table summarizes the appearance of these three elliptic curve groups in other standards.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Group 19</th>
<th>Group 20</th>
<th>Group 21</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST [DSS]</td>
<td>P-256</td>
<td>P-384</td>
<td>P-521</td>
</tr>
<tr>
<td>ISO/IEC [ISO-15946-1]</td>
<td>P-256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO/IEC [ISO-18031]</td>
<td>P-256</td>
<td>P-384</td>
<td>P-521</td>
</tr>
<tr>
<td>SECG [SEC2]</td>
<td>secp256r1</td>
<td>secp384r1</td>
<td>secp521r1</td>
</tr>
</tbody>
</table>

See also [NIST], [ISO-14888-3], [ISO-15946-2], [ISO-15946-3], and [ISO-15946-4].

4. Security Considerations

Since this document proposes new groups for use within IKEv2, many of the security considerations contained within [IKEv2] apply here as well.

The groups proposed in this document correspond to the symmetric key sizes 128 bits, 192 bits, and 256 bits. This allows the IKE key exchange to offer security comparable with the AES algorithms [AES].

5. IANA Considerations

This document has no actions for IANA.
6. References

6.1 Normative


6.2 Informative


[IANA] Internet Assigned Numbers Authority, Internet Key Exchange (IKE) Attributes. (http://www.iana.org/assignments/ipsec-registry)


7. Author's Address

Jerome A. Solinas  
National Security Agency  
jasolin@orion.ncsc.mil

Comments are solicited and should be addressed to the author.

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Expires November 27, 2005