ECC public key and signature support in Cryptographically Generated Addresses (CGA) and in the Secure Neighbor Discovery (SEND)
draft-cheneau-csi-ecc-sig-agility-00

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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/ietf/1id-abstracts.txt.

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

This Internet-Draft will expire on April 15, 2010.

Copyright Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.
Abstract

This draft describes a mechanism to deploy Elliptic Curve Cryptography (ECC) alongside with Cryptographically Generated Addresses (CGA) and the Secure Neighbor Discovery (SEND). This document provides basic skeleton to integrate new signature algorithms in CGA and SEND.

Table of Contents

1. Introduction .................................................. 3
2. Choice of Elliptic Curve .................................... 4
3. Using ECC in CGA .............................................. 5
4. Using ECC in the Public Key extension field ............... 6
5. Signature Type Identifier for ECC ............................ 7
6. Using ECDSA with Universal Signature Option .............. 8
7. Security Considerations ....................................... 9
8. IANA Considerations .......................................... 10
9. References ...................................................... 11
   9.1. Normative References ...................................... 11
   9.2. Informative References .................................... 11
Appendix A. On the number of Public Keys supported per CGA .... 13
Appendix B. Note for future work ................................. 15
Authors’ Addresses ................................................. 16
1. Introduction

The usage scenarios associated with neighbor discovery have recently been extended to include environments with mobile or nomadic nodes. Many of these nodes have limited battery power and computing resources. Therefore, heavy public key signing algorithms like RSA are not feasible to support on such constrained nodes. Fortunately, more lightweight yet secure signing algorithms do exist and have been standardized, e.g. Elliptic Curve based algorithms.

It is then a worthwhile goal to extend secure neighbor discovery to support this signing algorithm.

The aim of this memo is to outline options for allowing Elliptic Curve Digital Signature Algorithm for nodes configured to perform secure neighbor discovery operations. The present document exposes how to use and deploy Elliptic Curve Cryptography in [RFC3972], [cheneau-csi-cga-pk-agility] and [cheneau-csi-send-sig-agility]. It should be noted that the two latter documents have impacts on existing specifications [RFC3971] and [RFC3972].
2. Choice of Elliptic Curve

This document follows NIST’s recommendation on the usage of various Elliptic Curves as per [FIPS-186-3]. For the sake of simplicity, this document only describes the use of three proposed curves, namely curve P-256 (aka secp256r1), curve P-384 (aka secp384r1) and curve P-521 (aka secp521r1).
3. Using ECC in CGA

The CGA generation and verification processes remain unmodified from the processes described in [RFC3972]. However, we extend section 3 of [RFC3972], as it contains RSA specific text. We add that, when ECDSA is used, the AlgorithmIdentifier, contained in ASN.1 structure of type SubjectPublicKeyInfo, must be the (unrestricted) id-ecPublicKey algorithm identifier, which is OID 1.2.840.10045.2.1, and the subjectPublicKey MUST be formatted as an ECC Public Key, specified in Section 2.2 of [RFC5480].

Note that the ECC key lengths are determined by the namedCurves parameter stored in ECParameters field of the AlgorithmIdentifier.
4. Using ECC in the Public Key extension field

The optional Public Key extension field of the CGA Parameters data structure, defined in [cheneau-csi-cga-pk-agility], enables a node to generate CGA addresses with more than one Public Key. The encoding of the Public Key inside the Public Key extension field is the same encoding as the one presented in Section 3.
5. Signature Type Identifier for ECC

In the document [cheneau-csi-send-sig-agility], a field named Signature Type Identifier is used by the Supported Signature Algorithm Option and the Universal Signature Option (that replaces the RSA Signature Option). This field indicates the Signature Algorithm available on the node to generate or verify the Digital Signature field of the Universal Signature Option.

This document describes new values for three different signature algorithms. This value are extracted from the IANA-defined numbers for the IKEv2 protocol, i.e. IANA registry named "IKEv2 Authentication Method" and are the following:

- Value 9 is ECDSA with SHA-256 on the P-256 curve
- Value 10 is ECDSA with SHA-384 on the P-384 curve
- Value 11 is ECDSA with SHA-512 on the P-521 curve
6. Using ECDSA with Universal Signature Option

The document [cheneau-csi-send-sig-agility] proposes the Universal Signature Option (extended from the RSA Signature Option of [RFC3971]). This option adds a new Signature Type Identifier field that identifies the signature algorithm used during the generation of the digital signature field.

When the value of the Signature Type Identifier field is 9, 10 or 11, this Digital Signature field is computed and verified using the ECDSA signature algorithm (as defined on [SEC1]) and hash function corresponding to the Signature Type Identifier field. The data on which the signature is performed are described in [cheneau-csi-send-sig-agility].
7. Security Considerations

This memo defines the usage of the ECC Public Key and Signature Algorithm in CGA and SEND. As recommended in [cheneau-csi-send-sig-agility], when a node is using a multiple-key CGA (according to [cheneau-csi-cga-pk-agility]), the weakest key determines the strength of a multiple-key CGA. Table 1 (from [SP800-57]), presents a comparison between the length of the RSA keys and their equivalent (security-wise) ECC keys.

<table>
<thead>
<tr>
<th>RSA key length (bits)</th>
<th>ECC key length (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3072</td>
<td>256</td>
</tr>
<tr>
<td>7680</td>
<td>384</td>
</tr>
<tr>
<td>15360</td>
<td>512</td>
</tr>
</tbody>
</table>

Table 1: Strength equivalence between Elliptic Curve and RSA Public Keys
8. IANA Considerations

This document does not request any new IANA allocations.
9. References

9.1. Normative References


9.2. Informative References


[FIPS-186-3]

[SP800-57]

Appendix A. On the number of Public Keys supported per CGA

<table>
<thead>
<tr>
<th>Name of the elliptic curve</th>
<th>Size of the DER-encoded Public Key (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-256</td>
<td>88</td>
</tr>
<tr>
<td>P-384</td>
<td>120</td>
</tr>
<tr>
<td>P-521</td>
<td>158</td>
</tr>
</tbody>
</table>

Table 2: Common sizes for DER-encoded ECC Public Key

<table>
<thead>
<tr>
<th>Name of the elliptic curve</th>
<th>Size of the Digital Signature field (without padding)</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-256</td>
<td>71</td>
</tr>
<tr>
<td>P-384</td>
<td>104</td>
</tr>
<tr>
<td>P-521</td>
<td>139</td>
</tr>
</tbody>
</table>

Table 3: Common sizes of the Digital Signature field when using ECDSA (+ DER encoding)

Appendix A of document [cheneau-csi-send-sig-agility] emphasises the impact of the Public Key size on size of the final message. This Appendix proposes to extend previous document and to add values for ECC. Table 2 provides size for the commonly used DER-encoded ECC Public Keys. Table 3 presents common sizes for Digital Signature field when using ECDSA.

Reusing the value computed in [cheneau-csi-send-sig-agility], we deduce that a Router Advertisement carrying a Prefix Information Option and a Source Link-Layer Option sent from a CGA formed with a P-256 EC Public and protected by a corresponding ECDSA signature is 328 bytes long. This can be compared with the same message using a CGA carrying a 1024 bits RSA whose length is 456 bytes.

We can also evaluate the cost of the transformation of a legacy CGA to a multiple-key CGA. Using a 1024 RSA Public Key (as described in Appendix A of [cheneau-csi-send-sig-agility]) and a ECC P-521 key in a CGA Option, the original message, signed with a Universal Signature option generated by RSA and a Universal Signature Option signed by...
ECDSA, the Router Advertisement message is 768 bytes long. Note this example illustrates the potential burden of (transitional) multiple key CGAs, and also that EC P-521 and 1024-bits RSA keys should not be used together because they do not present the same security level (see Section 7). They are shown here to provide an indication on the sizes of messages in heterogeneous environments.
Appendix B.  Note for future work

When specifying a new type of Signature Algorithm, a new draft may reuse the skeleton of this document by replacing ECC/ECDSA by the appropriate terminology. In this case, the new draft should include an appendix similar to Appendix A for a comparison with already specified signature algorithms.
Authors’ Addresses

Tony Cheneau
Institut TELECOM, TELECOM SudParis, CNRS SAMOVAR UMR 5157
9 rue Charles Fourier
Evry 91011
France
Email: tony.cheneau@it-sudparis.eu

Maryline Laurent-Maknavicius
Institut TELECOM, TELECOM SudParis, CNRS SAMOVAR UMR 5157
9 rue Charles Fourier
Evry 91011
France
Email: maryline.maknavicius@it-sudparis.eu

Sean Shen
Huawei
4, South 4th Street, Zhongguancun
Beijing 100190
P.R. China
Email: sean.s.shen@gmail.com

Michaela Vanderveen
Qualcomm
Email: mvandervn@gmail.com