

CGA & SEND maintenance  
Internet-Draft  
Updates: [RFC3971](#), RFC3972  
(if approved)  
Expires: December 18, 2010

T. Cheneau  
M. Laurent  
TMSP  
S. Shen  
Huawei  
M. Vanderveen  
Qualcomm  
June 16, 2010

ECC public key and signature support in Cryptographically Generated  
Addresses (CGA) and in the Secure Neighbor Discovery (SEND)  
draft-cheneau-csi-ecc-sig-agility-02

## 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.

## 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 December 18, 2010.

## Copyright Notice

Copyright (c) 2010 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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Choice of Elliptic Curve . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Using ECC in CGA . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Signature Type Identifier for ECC . . . . .	<a href="#">6</a>
<a href="#">5.</a>	Using ECDSA with Universal Signature Option . . . . .	<a href="#">7</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">8</a>
<a href="#">7.</a>	IANA Considerations . . . . .	<a href="#">9</a>
<a href="#">8.</a>	References . . . . .	<a href="#">10</a>
<a href="#">8.1.</a>	Normative References . . . . .	<a href="#">10</a>
<a href="#">8.2.</a>	Informative References . . . . .	<a href="#">10</a>
<a href="#">Appendix A.</a>	On the number of Universal Signature Options supported per CGA . . . . .	<a href="#">12</a>
<a href="#">Appendix B.</a>	Note for future work . . . . .	<a href="#">13</a>
	Authors' Addresses . . . . .	<a href="#">14</a>

## 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](#)] and [[cheneau-csi-send-sig-agility](#)]. It should be noted that the latter document has impacts on existing specification [[RFC3971](#)].

## 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 ECPParameters field of the AlgorithmIdentifier.

#### 4. 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. These values are extracted from the IANA-defined numbers for the IKEv2 protocol, i.e. IANA registry named "IKEv2 Authentication Method" and are the following:

- o Value 9 is ECDSA with SHA-256 on the P-256 curve

- o Value 10 is ECDSA with SHA-384 on the P-384 curve
- o Value 11 is ECDSA with SHA-512 on the P-521 curve

## 5. 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](#)].



This memo defines the usage of the ECC Public Key and Signature Algorithm in CGA and SEND. Table 1 (from [SP800-57]), presents a comparison between the length of the RSA keys and their equivalent (security-wise) ECC keys.

RSA key length (bits)	ECC key length (bits)
3072	256
7680	384
15360	512

Table 1: Strength equivalence between Elliptic Curve and RSA Public Keys

## [7.](#) IANA Considerations

This document does not request any new IANA allocations.

## [8.](#) References

### [8.1.](#) Normative References

- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3972](#), March 2005.
- [RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.
- [RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", [RFC 5480](#), March 2009.
- [cheneau-csi-send-sig-agility]  
Cheneau, T., Laurent, M., Shen, S., and M. Vanderveen, "Signature Algorithm Agility in the Secure Neighbor Discovery (SEND) Protocol", [draft-cheneau-csi-send-sig-agility-02](#) (work in progress), June 2010.

### [8.2.](#) Informative References

- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.
- [RFC3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", [RFC 3756](#), May 2004.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.
- [FIPS.180-2]  
National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-2, August 2002, <<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>>.

[FIPS-186-3]

National Institute of Standards and Technology, "Digital Signature Standard", FIPS PUB 186-3, June 2009.

[SP800-57]

National Institute of Standards and Technology (NIST), "Special Publication 800-57: Recommendation for Key Management - Part 1 (Revised)", SP SP 800-57, March 2007.

Cheneau, et al.

Expires December 18, 2010

[Page 10]

---

Internet-Draft

ECC PK and sig. support in CGA and SEND

June 2010

[SEC1]

Standards for Efficient Cryptography Group, "SEC 1: Elliptic Curve Cryptography", September 2000, <<http://secg.org>>.

[Appendix A](#). On the number of Universal Signature Options supported per CGA

Name of the elliptic curve	Size of the DER-encoded Public Key (bytes)
P-256	88
P-384	120
P-521	158

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

Name of the elliptic curve	Size of the Digital Signature field (without padding)
P-256	71
P-384	104
P-521	139

+-----+-----+

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 and the number of Universal Signature Options 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.

[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.

Cheneau, et al.

Expires December 18, 2010

[Page 13]

---

Internet-Draft

ECC PK and sig. support in CGA and SEND

June 2010

#### 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](mailto:tony.cheneau@it-sudparis.eu)

Maryline Laurent  
Institut TELECOM, TELECOM SudParis, CNRS SAMOVAR UMR 5157  
9 rue Charles Fourier  
Evry 91011  
France

Email: [maryline.laurent@it-sudparis.eu](mailto:maryline.laurent@it-sudparis.eu)

Sean Shen  
Huawei  
4, South 4th Street, Zhongguancun  
Beijing 100190  
P.R. China

Email: [sean.s.shen@gmail.com](mailto:sean.s.shen@gmail.com)

Michaela Vanderveen  
Qualcomm

Email: [mvandervn@gmail.com](mailto:mvandervn@gmail.com)