TOC

CGA & SEND maintenance	T. Cheneau
Internet-Draft	M. Laurent
Updates: RFC3971, RFC3972	TMSP
(if approved)	S. Shen
Expires: May 26, 2010	Huawei
	M. Vanderveen
	Qualcomm
	November 22, 2009

ECC public key and signature support in Cryptographically Generated Addresses (CGA) and in the Secure Neighbor Discovery (SEND)
draft-cheneau-csi-ecc-sig-agility-01

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

Copyright Notice

Table of Contents

1. Introduction

TOC

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] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.) and [cheneau-csi-send-sig-agility] (Cheneau, T., Laurent, M., Shen, S., and M. Vanderveen, “Signature Algorithm Agility in the Secure Neighbor Discovery (SEND) Protocol,” November 2009.). It should be noted that the latter document has impacts on existing specification [RFC3971]

(Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.).

2. Choice of Elliptic Curve

TOC

This document follows NIST's recommendation on the usage of various Elliptic Curves as per [FIPS-186-3] (National Institute of Standards and Technology, “Digital Signature Standard,” June 2009.). 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

TOC

The CGA generation and verification processes remain unmodified from the processes described in [RFC3972] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.). However, we extend section 3 of [RFC3972] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.), 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] (Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, “Elliptic Curve Cryptography Subject Public Key Information,” March 2009.).

Note that the ECC key lengths are determined by the namedCurves parameter stored in ECParameters field of the AlgorithmIdentifier.

4. Signature Type Identifier for ECC

TOC

In the document [cheneau-csi-send-sig-agility] (Cheneau, T., Laurent, M., Shen, S., and M. Vanderveen, “Signature Algorithm Agility in the Secure Neighbor Discovery (SEND) Protocol,” November 2009.), 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:

- *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

5. Using ECDSA with Universal Signature Option

TOC

The document [cheneau-csi-send-sig-agility] (Cheneau, T., Laurent, M., Shen, S., and M. Vanderveen, “Signature Algorithm Agility in the Secure Neighbor Discovery (SEND) Protocol,” November 2009.) proposes the Universal Signature Option (extended from the RSA Signature Option of [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.)). 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] (Standards for Efficient Cryptography Group, “SEC 1: Elliptic Curve Cryptography,” September 2000.)) 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] (Cheneau, T., Laurent, M., Shen, S., and M. Vanderveen, “Signature Algorithm Agility in the Secure Neighbor Discovery (SEND) Protocol,” November 2009.).

6. Security Considerations

TOC

This memo defines the usage of the ECC Public Key and Signature Algorithm in CGA and SEND. Table 1 (Strength equivalence between Elliptic Curve and RSA Public Keys) (from [SP800-57] (National Institute of Standards and Technology (NIST), “Special Publication 800-57: Recommendation for Key Management - Part 1 (Revised),” March 2007.)), 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

TOC

This document does not request any new IANA allocations.

8. References

TOC

8.1. Normative References

TOC

[RFC3972]	Aura, T., “Cryptographically Generated Addresses (CGA),” RFC 3972, March 2005 (TXT).
[RFC3971]	Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” RFC 3971, March 2005 (TXT).
[RFC5480]	Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, “Elliptic Curve Cryptography Subject Public Key Information,” RFC 5480, March 2009 (TXT).
[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-01 (work in progress), November 2009 (TXT).

8.2. Informative References

TOC

[RFC2460]	Deering, S. and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” RFC 2460, December 1998 (TXT, HTML, XML).
[RFC3756]	

	Nikander, P., Kempf, J., and E. Nordmark, “IPv6 Neighbor Discovery (ND) Trust Models and Threats,” RFC 3756, May 2004 (TXT).
[RFC4861]	Narten, T., Nordmark, E., Simpson, W., and H. Soliman, “Neighbor Discovery for IP version 6 (IPv6),” RFC 4861, September 2007 (TXT).
[FIPS.180-2]	National Institute of Standards and Technology, “Secure Hash Standard,” FIPS PUB 180-2, August 2002.
[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.
[SEC1]	Standards for Efficient Cryptography Group, “SEC 1: Elliptic Curve Cryptography,” September 2000.

Appendix A. On the number of Universal Signature Options supported per CGA

TOC

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] (Cheneau, T., Laurent, M., Shen, S., and M. Vanderveen, “Signature Algorithm Agility in the Secure Neighbor Discovery (SEND) Protocol,” November 2009.) 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 (Common sizes for DER-encoded ECC Public Key) provides size for the commonly used DER-encoded ECC Public Keys. Table 3 (Common sizes of the Digital Signature field when using ECDSA (+ DER encoding)) presents common sizes for Digital Signature field when using ECDSA.
Reusing the value computed in [cheneau-csi-send-sig-agility] (Cheneau, T., Laurent, M., Shen, S., and M. Vanderveen, “Signature Algorithm Agility in the Secure Neighbor Discovery (SEND) Protocol,” November 2009.), 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

TOC

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 (On the number of Universal Signature Options supported per CGA) for a comparison with already specified signature algorithms.

Authors' Addresses

TOC

	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
	Institut TELECOM, TELECOM SudParis, CNRS SAMOVAR UMR 5157
	9 rue Charles Fourier

Evry 91011
France
Email: maryline.laurent@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