CGA & Send maintenance	T. Cheneau
Internet-Draft	M. Maknavicius
Expires: August 25, 2009	TMSP
	S. Sean
	Huawei
	M. Vanderveen
	Qualcomm
	February 21, 2009

TOC

Support for Multiple Signature Algorithms in Cryptographically Generated Addresses (CGAs)
draft-cheneau-cga-pk-agility-00

Status of this Memo

Copyright Notice

Abstract

This document defines an extension field for the CGA Parameter data structure specified in RFC 3972. This extension field carries a Public

Key that is used in Cryptographically Generated Address (CGA) generation. This extension enables protocols using CGAs, such as SEND, to use multiple Public Key signing algorithms and/or multiple Public Keys.

Table of Contents

---

1. Introduction

TOC

Cryptographically Generated Addresses (CGA) [RFC3972] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.) have been designed primarily for securing Neighbor Discovery [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.). A digital signature algorithm is used to provide authentication and integrity protection when CGA is used. CGAs [RFC3972] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.) were defined to only use RSA as the associated signature algorithm. Only one RSA public key is associated with a CGA and this public key is carried in the Public Key field of the CGA Parameter data structure.

The secure neighbor discovery usage scenarios have recently been extended to include environments with mobile or nomadic nodes. These nodes can often be limited in power and memory capabilities, and thus may only be able to support lightweight public key cryptography; that is, RSA-based public keys and algorithm support may not be feasible. Therefore, support for signature algorithm agility in CGA is desired. However, since the CGA specification [RFC3972] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.) states that SEND "SHOULD" use an RSA public/private key pair, backward compatibility is preserved herein.

A logical place for extending the CGA Parameter data structure to include other types of public keys is its "extension fields". Some guidance on the format of these extensions is provided in [RFC4581]

(Bagnulo, M. and J. Arkko, “Cryptographically Generated Addresses (CGA) Extension Field Format,” October 2006.). One type of CGA Parameter data structure extension is defined in Section 2 (Public Key extension) and this type of extension is able to carry public keys, in addition to the RSA public key defined in the Public Key field of CGA Parameters data structure.
These extensions allows new functionnalities on CGA based protocols, such as the Signature Algorithm Agility in SEND [cheneau-send-sig-agility] (Cheneau, T., Laurent-Maknavicius, M., Shen, S., and M. Vanderveen, “Signature Algorithm Agility in the Secure Neighbor Discovery (SEND) Protocol,” Feb 2009.).

---

2. Public Key extension

TOC

This section describes an extension field that conforms to the guidelines of [RFC4581] (Bagnulo, M. and J. Arkko, “Cryptographically Generated Addresses (CGA) Extension Field Format,” October 2006.).
This extension allows a CGA Parameters data structure to carry public keys in addition to the key in the Public Key field. This approach paves the way for one CGA to possibly be associated with multiple public keys.
This extension allows a node to select a Public Key value that is different from the one in the Public Key field of the CGA Parameters data structure option. This Public Key is placed in an extension embedded in the Extension field of the CGA Parameters data structure, described in [RFC3972] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.).

2.1. Public Key extension format

TOC

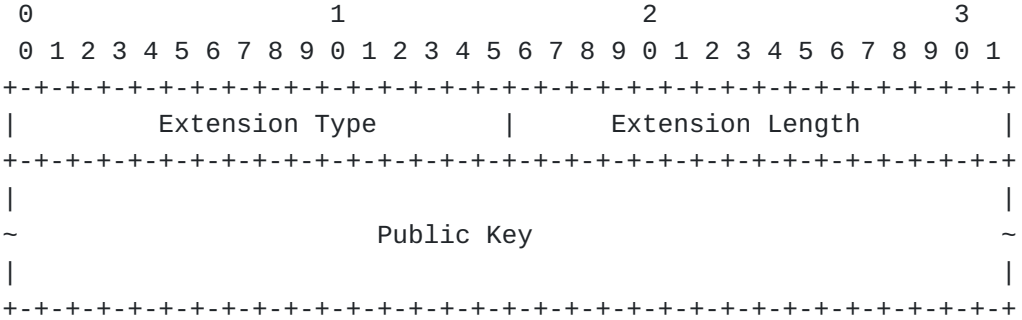

Figure 1: Public Key extension format

Extension Type

TBA. (16-bit unsigned integer. See Section 5 (IANA Considerations).)

Extension Length

The length of the Public Key field to follow, in octets. 16-bit unsigned integer.

Public Key

This is a variable-length field containing the public key of the sender. The public key MUST be formatted as a DER-encoded [ITU.X690.2002] (International Telecommunication Union, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)," July 2002.) ASN.1 structure of the type SubjectPublicKeyInfo, defined in the Internet X.509 certificate profile [RFC5280] (Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," May 2008.). When RSA is used, the algorithm identifier MUST be rsaEncryption, which is 1.2.840.113549.1.1.1, and the RSA public key MUST be formatted by using the RSAPublicKey type as specified in Section 2.3.1 of [RFC3279] (Bassham, L., Polk, W., and R. Housley, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," April 2002.). The RSA key length SHOULD be at least 384 bits.

When ECC is used, the algorithm identifier MUST be of type id-ecPublicKey (OID 1.2.840.10045.2.1), as defined in [ID-pkix-ecc] (Turner, S. and et. al, "Elliptic Curve Cryptography Subject Public Key Information," December 2008.). ECC public key encoding is specified in this reference. Note that the ECC key lengths are determined by the ECParameters field named namedCurves (curves implying key length).

3. CGA Generation Process

TOC

When a node supports two or more types of signing algorithms, and is able to generate two or more corresponding public keys, then it can derive a single CGA using all these keys. The derivation is done exactly as in [RFC3972] (Aura, T., "Cryptographically Generated

Addresses (CGA),” March 2005.); one key is placed in the CGA Parameters data structure "Public Key" field while the rest of the keys are placed in separate extension fields . This is illustrated in Figure 2 (CGA parameter structure with multiple keys).
It should be noted that the type of the public key (RSA, ECC, etc.) is already encoded into the "Public Key" field itself, and thus there is no need to identify the public key type separately. This is due to the fact that the "Public Key" field, according to [RFC3972] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.) is a DER-encoded ASN.1 structure of the type "SubjectPublicKeyInfo", and therefore includes a subfield called "AlgorithmIdentifier".

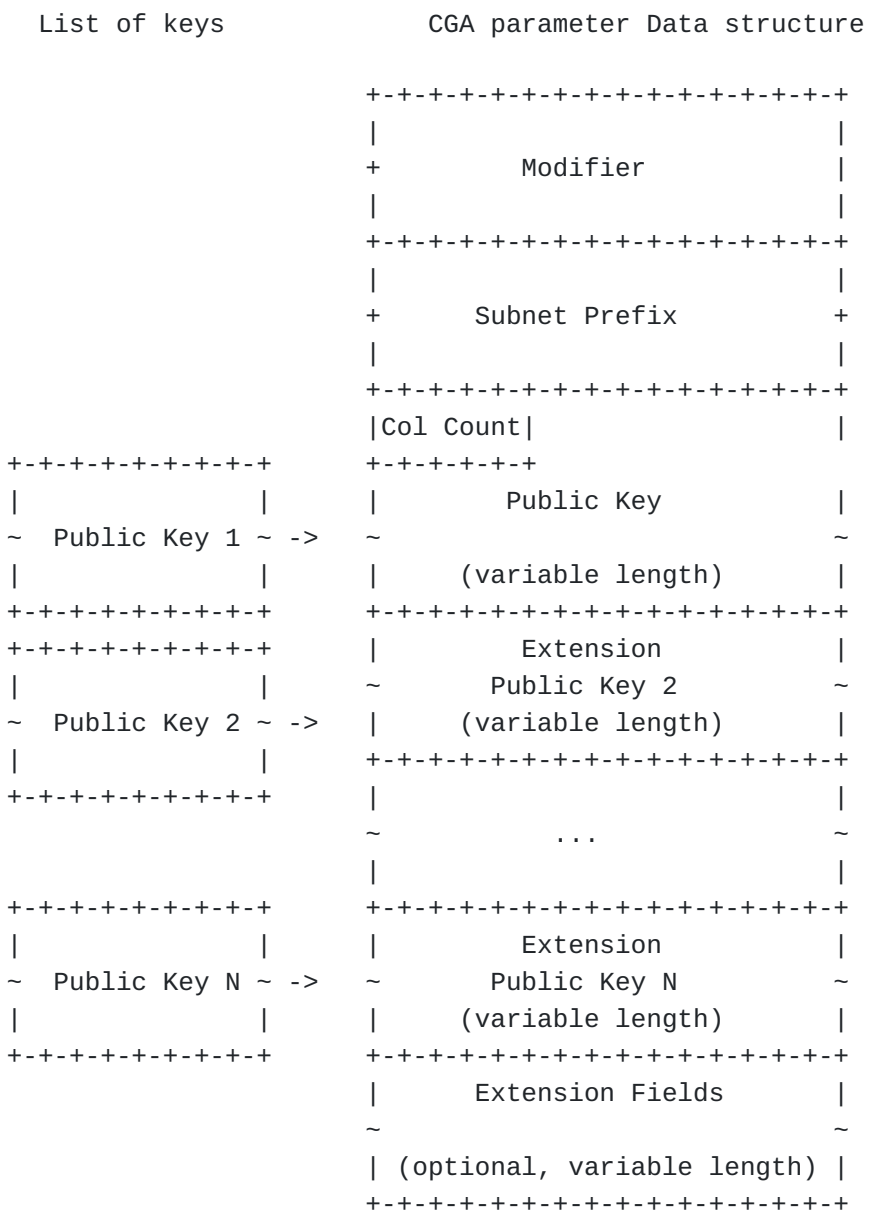

Figure 2: CGA parameter structure with multiple keys

The resulting CGA Parameters data structure is inserted into a CGA option as per [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.). When sending a NDP packet, the node includes this CGA option and also one signature option of choice, computed with a private key whose corresponding Public Key is present in the CGA Parameters data structure. This signature option can be the RSA signature option as per [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.), or another signature option,

e.g. the ECC signature option as per [ID-csi-ecc] (Shen, S. and M. Vanderveen, “ECC Support for SEND/CGA,” October 2008.), or any other signature defined. The signature option contains the hash of the key used to sign the message.
Note that an implementation should choose the number of simultaneous Public Key Extensions fields used so as the total length of the extension fields does not exceed a threshold that requires fragmentation support at the SEND or other upper-layer protocol layer.
Support for RSA Public Keys and signature algorithm is only RECOMMENDED for backward compatibility. This specification does not mandate support for any particular public key signature algorithm. Therefore, nodes can be configured to choose/support only a single additional signature algorithm besides RSA. However, a node is also free to not support RSA and still claim compatibility with this specification.
Since [RFC3972] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.) mandates the use of RSA keys in the Public Key field, a node compatible with [RFC3972] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.) only will extract the RSA public key from the Public Key field and ignore the extension fields. Therefore, in order to achieve backward compatibility, if a node uses a CGA associated with multiple public keys (through the use of the Public Key extension), the following procedures are in place: if one of the public keys is of RSA type, then that key SHOULD be placed in the Public Key field of the CGA Parameter data structure, while the other key(s) SHOULD be placed in the Extension field(s).

---

4. Security Consideration

TOC

The document specifies a CGA extension field format. No additional vulnerabilities appear besides those described in section 7 of [RFC3972] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.)
However , it should be noted that the resulting security level of a multiple-key CGA is only that of the weakest key. Therefore, the requirement remains that every key in use should have a security level matching or exceeding that of a 384-bit RSA key.
Whenever protocols negotiate signature algorithms, downgrade attacks are considered. This document only provides the ability for CGA options to carry multiple public keys; negotiations of signature algorithms or public keys are out of the scope of this document.

TOC

5. IANA Considerations

This document defines one new CGA Extension Type [RFC4581] (Bagnulo, M. and J. Arkko, "Cryptographically Generated Addresses (CGA) Extension Field Format," October 2006.) option, which must be assigned by IANA:

> Name: Public Key Extension Type;
>
> Value: TBA.
>
> Description: see Section 2 (Public Key extension).

---

6. References

TOC

6.1. Normative References

TOC

[RFC5280]	Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 5280, May 2008 (TXT).
[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).
[RFC4982]	Bagnulo, M. and J. Arkko, "Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)," RFC 4982, July 2007 (TXT).
[RFC4861]	Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," RFC 4861, September 2007 (TXT).

6.2. Informative References

TOC

[RFC4581]	Bagnulo, M. and J. Arkko, "Cryptographically Generated Addresses (CGA) Extension Field Format," RFC 4581, October 2006 (TXT).
[RFC3279]	Bassham, L., Polk, W., and R. Housley, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 3279, April 2002 (TXT).

[RFC4866]	Arkko, J., Vogt, C., and W. Haddad, "Enhanced Route Optimization for Mobile IPv6," RFC 4866, May 2007 (TXT).
[ITU.X690.2002]	International Telecommunication Union, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)," ITU-T Recommandation X.690, July 2002.
[ID-csi-ecc]	Shen, S. and M. Vanderveen, "ECC Support for SEND/ CGA," draft-shen-csi-ecc-01 (work in progress), October 2008 (TXT).
[ID-pkix-ecc]	Turner, S. and et. al, "Elliptic Curve Cryptography Subject Public Key Information," draft-ietf-pkix-ecc-subpubkeyinfo-11 (work in progress), December 2008 (TXT).
[cheneau-send-sig-agility]	Cheneau, T., Laurent-Maknavicius, M., Shen, S., and M. Vanderveen, "Signature Algorithm Agility in the Secure Neighbor Discovery (SEND) Protocol," draft-cheneau-send-sig-agility-00 (work in progress), Feb 2009 (TXT).

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-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
Email:	sshen@huawei.com
	Michaela Vanderveen
	Qualcomm
Email:	mvandervn@gmail.com