Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 27, 2011

J. Herzog
R. Khazan
MIT Lincoln Laboratory

February 23, 2011

# Use of static-static Elliptic-Curve Diffie-Hellman key agreement in Cryptographic Message Syntax draft-herzog-static-ecdh-05

## Abstract

This document describes how to use 'static-static' Elliptic Curve Diffie-Hellman key-agreement with the Cryptographic Message Syntax. In this form of key-agreement, the Diffie-Hellman values of both sender and receiver are long-term values contained in certificates.

## Disclaimer

This work is sponsored by the United States Air Force under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the authors and are not necessarily endorsed by the United States Government.

## 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 August 27, 2011.

## Copyright Notice

Table of Contents

## 1. Introduction

This document describes how to use the static-static Elliptic-Curve Diffie-Hellman key agreement scheme [SEC1] in the Cryptographic Message Syntax (CMS) [CMS]. The CMS is a standard notation and representation for cryptographic messages. CMS uses ASN.1 notation [X.680] [X.681] [X.682] [X.683] to define a number of structures that carry both cryptographically-protected information and key-management information regarding the keys used. Of particular interest here are three structures:

- EnvelopedData, which holds encrypted (but not necessarily authenticated) information [CMS],
- AuthenticatedData, which holds authenticated (MACed) information [CMS], and
- AuthEnvelopedData, which holds information protected by authenticated encryption: a cryptographic scheme that combines encryption and authentication [CMS-AUTHENV].

All three of these types share the same basic structure. First, a fresh symmetric key is generated. This symmetric key has a different name that reflects its usage in each of the three structures. EnvelopedData uses a content-encryption key (CEK); AuthenticatedData uses an authentication key; AuthEnvelopedData uses a content-authenticated-encryption key. The originator uses the symmetric key to cryptographically protect the content. The symmetric key is then used wrapped for each recipient; only the intended recipient has access to the private keying material necessary to unwrap the symmetric key. Once unwrapped, the recipient uses the symmetric key to decrypt the content, check the integrity of the content, or both. The CMS supports several different approaches to symmetric key wrapping, including:

- key transport: the symmetric key is encrypted using the public encryption key of some recipient,
- key-encryption key: the symmetric key is encrypted using a previously-distributed symmetric key, and
- key agreement: the symmetric key is encrypted using a key-encryption key (KEK) created using a key-agreement scheme and a key-derivation function (KDF).

One such key-agreement scheme is the Diffie-Hellman algorithm [DH] which uses group-theory to produce a value known only to its two participants. In this case, the participants are the originator and

one of the recipients. Each participant produces a private value and a public value, and each participant can produce the shared secret value from their own private value and their counterpart's public value. There are some variations on the basic algorithm:

- The basic algorithm typically uses the group 'Z mod p', meaning the set of integers modulo some prime p. One can also use an elliptic-curve group, which allows for shorter messages.

- Over elliptic-curve groups, the standard algorithm can be extended to incorporate the 'cofactor' of the group (see [SEC1] for more details). This method, called 'cofactor Elliptic Curve Diffie-Hellman', can prevent certain attacks possible in the elliptic-curve group.

- The participants can generate fresh new public/private values (called ephemeral values) for each run of the algorithm, or they can re-use long-term values (called static values). Ephemeral values add randomness to the resulting private value, while static values can be embedded in certificates. The two participants do not need to use the same kind of value: either participant can use either type. In 'ephemeral-static' Diffie-Hellman, for example, the sender uses an ephemeral public/private pair value while the receiver uses a static pair. In 'static-static' Diffie-Hellman, on the other hand, both participants use static pairs. (Receivers cannot use ephemeral values in this setting, and so we ignore ephemeral-ephemeral and static-ephemeral Diffie-Hellman in this document.)

Several of these variations are already described in existing CMS standards. [CMS-ALG] contains the conventions for using for ephemeral-static and static-static Diffie-Hellman over the 'basic' (Z mod p) group. [CMS-ECC] contains the conventions for using ephemeral-static Diffie-Hellman over elliptic curves (both standard and cofactor methods). It does not, however, contain conventions for using either method of static-static Elliptic-Curve Diffie-Hellman, preferring to discuss the ECMQV algorithm instead.

In this document, we specify the conventions for using static-static Elliptic-Curve Diffie-Hellman (ECDH) for both standard and cofactor methods. Our motivations are three-fold:

1. Intellectual-property concerns have hindered market adoptation of the ECMQV algorithm,

2. ECMQV has been removed from the National Security Agency's Suite B of cryptographic algorithms, and

3. ECMQV requires the sender to create a fresh random value for each recipient. While the incorporation of per-session randomness is good cryptographic practice, ECMQV fixes the size of this randomness: that of one elliptic-curve point. For low-bandwidth networks, it may be necessary to use smaller amounts of per-recipient randomness.

We note that like ephemeral-static ECDH, static-static ECDH creates a secret key shared by sender and receiver. Unlike ephemeral-static ECDH, however, static-static ECDH uses a static key pair for the sender. Each of the three CMS structures discussed in this document (EnvelopedData, AuthenticatedData, and AuthEnvelopedData) uses static-static ECDH to achieve different goals:

- EnvelopedData uses static-static ECDH to provide data confidentiality. It will not necessarily, however, provide data integrity.

- AuthenticatedData uses static-static ECDH to provide data-integrity. It will not provide data-confidentiality.

- AuthEnvelopedData uses static-static ECDH to provide both of confidentiality and data-integrity.

## 1.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [MUST].

# 2. EnvelopedData using static-static ECDH

If an implementation uses static-static ECDH with CMS EnvelopedData then the following techniques and formats MUST be used. The fields of EnvelopedData are as in [CMS]; as static-static ECDH is a key agreement algorithm, the RecipientInfo kari choice is used. When using static-static ECDH, the EnvelopedData originatorInfo field MAY include the certificate(s) for the EC public key(s) used in the formation of the pairwise key.

## 2.1. Fields of the KeyAgreeRecipientInfo

When using static-static ECDH with EnvelopedData, the fields of KeyAgreeRecipientInfo [CMS] are:

- version MUST be 3.

- originator identifies the static EC public key of the sender. It MUST be either issuerAndSerialNumber or subjectKeyIdentifier, and point to one of the sending agent's certificates.

- ukm MAY be present or absent. However, message originators SHOULD include the ukm. As specified in [CMS], implementations MUST support ukm message recipient processing, so interoperability is not a concern if the ukm is present or absent. The use of a fresh value for ukm will ensure that a different key is generated for each message between the same sender and receiver. ukm, if present, is placed in the entityUInfo field of the ECC-CMS-SharedInfo structure [CMS-ECC] and therefore used as an input to the key derivation function.

- keyEncryptionAlgorithm MUST contain the object identifier of the key encryption algorithm, which in this case is a key agreement algorithm (see Section 5). The parameters field contains KeyWrapAlgorithm. The KeyWrapAlgorithm is the algorithm identifier that indicates the symmetric encryption algorithm used to encrypt the content-encryption key (CEK) with the key-encryption key (KEK) and any associated parameters (see Section 5).

- recipientEncryptedKeys contains an identifier and an encrypted CEK for each recipient. The RecipientEncryptedKey KeyAgreeRecipientIdentifier MUST contain either the issuerAndSerialNumber identifying the recipient's certificate or the RecipientKeyIdentifier containing the subject key identifier from the recipient's certificate. In both cases, the recipient's certificate contains the recipient's static ECDH public key. RecipientEncryptedKey EncryptedKey MUST contain the content-encryption key encrypted with the static-static ECDH-generated pairwise key-encryption key using the algorithm specified by the KeyWrapAlgorithm.

## 2.2. Actions of the sending agent

When using static-static ECDH with EnvelopedData, the sending agent first obtains the recipient's EC public key and domain parameters (e.g. from the recipient's certificate). It confirms that both certificates contain public-key values with the same curve parameters, and that both of these public-key values are marked as appropriate for ECDH (that is, marked with algorithm-identifiers id-ecPublicKey or id-ecDH [PKI-ECC]). The sender then determines:

- whether to use standard or cofactor Diffie-Hellman, and

- which hash algorithms to use for the key-derivation function.

The sender then chooses keyEncryptionAlgorithm that reflects these choices. It then determines:

- an integer "keydatalen", which is the KeyWrapAlgorithm symmetric key-size in bits, and

- the value of ukm, if used.

The sender then determines a bit string "SharedInfo", which is the DER encoding of ECC-CMS-SharedInfo (see Section 7.2 of [CMS-ECC]). The sending agent then performs the key agreement operation of the Elliptic Curve Diffie-Hellman Scheme specified in [SEC1] and the KDF defined in Section 3.6.1 of [SEC1] with the hash algorithm identified in the key agreement algorithm. As a result the sending agent obtains a shared secret bit string "K", which is used as the pairwise key-encryption key (KEK) to wrap the CEK for that recipient, as specified in [CMS].

## 2.3. Actions of the receiving agent

When using static-static ECDH with EnvelopedData, the receiving agent retrieves keyEncryptionAlgorithm to determine the key-agreement algorithm chosen by the sender, which will identify:

- the domain-parameters of the curve used,

- whether standard or cofactor Diffie-Hellman was used, and

- which hash-function was used for the KDF.

The receiver then retrieves the static EC public key identified in the rid field. It confirms that both certificates contain public-key values associated with the curve identified by the keyEncryptionAlgorithm, and that both of these public-key values are marked as appropriate for ECDH (that is, marked with algorithm-identifiers id-ecPublicKey or id-ecDH [PKI-ECC]). The receiver then determines a bit string "SharedInfo", which is the DER encoding of ECC-CMS-SharedInfo (see Section 7.2 of [CMS-ECC]) and performs the key agreement operation of the Elliptic Curve Diffie-Hellman Scheme specified in [SEC1]; in either case, use the KDF defined in Section 3.6.1 of [SEC1]. As a result, the receiving agent obtains a shared secret bit string "K", which it uses as the pairwise key-encryption key to unwrap the CEK.

## 3. AuthenticatedData using static-static ECDH

This section describes how to use the static-static ECDH key agreement algorithm with AuthenticatedData. When using static-static ECDH with AuthenticatedData, the fields of AuthenticatedData are as in [CMS], but with the following restrictions:

- macAlgorithm MUST contain the algorithm identifier of the message authentication code (MAC) algorithm which MUST be one of the following: hmac-SHA1, id-hmacWITHSHA224, id- hmacWITHSHA256, id-hmacWITHSHA384, or id-hmacWITHSHA512. (See Section 5.)

- digestAlgorithm MUST contain the algorithm identifier of the hash algorithm which MUST be one of the following: id-sha1, id-sha224, id-sha256, id-sha384, and id-sha512. (See Section 5.)

As static-static ECDH is a key agreement algorithm, the RecipientInfo kari choice is used in the AuthenticatedData. When using static-static ECDH, the AuthenticatedData originatorInfo field MAY include the certificate(s) for the EC public key(s) used in the formation of the pairwise key.

### 3.1. Fields of the KeyAgreeRecipientInfo

The AuthenticatedData KeyAgreeRecipientInfo fields are used in the same manner as the fields for the corresponding EnvelopedData KeyAgreeRecipientInfo fields of Section 2.1 of this document. The authentication key is wrapped in the same manner as is described there for the content-encryption key.

### 3.2. Actions of the sending agent

The sending agent uses the same actions as for EnvelopedData with static-static ECDH, as specified in Section 2.2 of this document.

### 3.3. Actions of the receiving agent

The receiving agent uses the same actions as for EnvelopedData with static-static ECDH, as specified in Section 2.3 of this document.

## 4. AuthEnvelopedData using static-static ECDH

When using static-static ECDH with AuthEnvelopedData, the fields of AuthEnvelopedData are as in [CMS-AUTHENV]. As static-static ECDH is a key agreement algorithm, the RecipientInfo kari choice is used. When using static-static ECDH, the AuthEnvelopedData originatorInfo field MAY include the certificate(s) for the EC public key used in

the formation of the pairwise key.

### 4.1. Fields of the KeyAgreeRecipientInfo

The AuthEnvelopedData KeyAgreeRecipientInfo fields are used in the same manner as the fields for the corresponding EnvelopedData KeyAgreeRecipientInfo fields of Section 2.1 of this document. The content-authenticated-encryption key is wrapped in the same manner as is described there for the content-encryption key.

### 4.2. Actions of the sending agent

The sending agent uses the same actions as for EnvelopedData with static-static ECDH, as specified in Section 2.2 of this document.

### 4.3. Actions of the receiving agent

The receiving agent uses the same actions as for EnvelopedData with static-static ECDH, as specified in Section 2.3 of this document.

## 5. Comparison to [CMS-ECC]

This document defines the use of static-static ECDH for EnvelopedData, AuthenticatedData, and AuthEnvelopedData. The standard [CMS-ECC] defines ephemeral-static ECDH for EnvelopedData only.

With regard to EnvelopedData, this document and [CMS-ECC] greatly parallel each other. Both specify how to apply Elliptic-Curve Diffie-Hellman, and differ only on how the sender's public value is to be communicated to the recipient. In [CMS-ECC], the sender provides the public value explicitly by including an OriginatorPublicKey value in the originator field of KeyAgreeRecipientInfo. In this document, the sender include a reference to a (certified) public value by including either an IssuerAndSerialNumber or SubjectKeyIdentifier value in the same field. Put another way, [CMS-ECC] provides an interpretation of a KeyAgreeRecipientInfo structure where:

- the keyEncryptionAlgorithm value indicates Elliptic-Curve Diffie-Hellman, and
- the originator field contains a OriginatorPublicKey value.

This document, on the other hand, provides an interpretation of a KeyAgreeRecipientInfo structure where

- the keyEncryptionAlgorithm value indicates Elliptic-Curve Diffie-Hellman, and

- the originator field contains either a IssuerAndSerialNumber value or a SubjectKeyIdentifier value.

AuthenticatedData or AuthEnvelopedData messages, on the other hand, are not given any form of ECDH by [CMS-ECC]. This is appropriate: that document only defines ephemeral-static Diffie-Hellman, and this form of Diffie-Hellman does not (inherently) provide any form of data-authentication or data-origin authentication. This document, on the other hand, requires that the sender use a certified public value. Thus, this form of key-agreement provides implicit key authentication and, under some limited circumstances, data-origin authentication. (See Section 7.)

This document does not define any new ASN.1 structures or algorithm identifiers. It provides new ways to interpret structures from [CMS] and [CMS-ECC], and allows previously-defined algorithms to be used under these new interpretations. Specifically:

- The ECDH key-agreement algorithm-identifiers from [CMS-ECC] define only how Diffie-Hellman values are processed, not where these values are created. Therefore, they can be used for static-static ECDH with no changes.

- The key-wrap, MAC, and digest algorithms referenced in [CMS-ECC] describe how the secret key is to be used, not created. Therefore, they can be used with keys from static-static ECDH without modification.

## 6. Requirements and Recommendations

It is RECOMMENDED that implementations of this specification support AuthenticatedData and EnvelopedData. Support for AuthEnvelopedData is OPTIONAL.

Implementations that support this specification MUST support standard Elliptic Curve Diffie-Hellman, and these implementation MAY also support cofactor Elliptic Curve Diffie-Hellman.

In order to encourage interoperability, implementations SHOULD use the elliptic curve domain parameters specified by [PKI-ECC].

Implementations that support standard static-static Elliptic Curve Diffie-Hellman:

MUST support the dhSinglePass-stdDH-sha256kdf-scheme key agreement algorithm, the id-aes128-wrap key wrap algorithm, and the id-aes128-cbc content encryption algorithm; and,

MAY support the dhSinglePass-stdDH-sha1kdf-scheme, dhSinglePass-stdDH-sha224kdf-scheme, dhSinglePass-stdDH-sha384kdf-scheme and dhSinglePass-stdDH-sha512kdf-scheme key agreement algorithms, the id-alg-CMS3DESwrap, id-aes192-wrap, and id-aes256-wrap key wrap algorithms and the des-ede3-cbc, id-aes192-cbc, and id-aes256-cbc content encryption algorithms; other algorithms MAY also be supported.

Implementations that support cofactor static-static Elliptic-Curve Diffie-Hellman:

MUST support the dhSinglePass-cofactorDH-sha256kdf-scheme key agreement algorithm, the id-aes128-wrap key wrap algorithm, and the id-aes128-cbc content encryption algorithm; and,

MAY support the dhSinglePass-cofactorDH-sha1kdf-scheme, dhSinglePass-cofactorDH-sha224kdf-scheme, dhSinglePass-cofactorDH-sha384kdf-scheme, and dhSinglePass-cofactorDH-sha512kdf-scheme key agreement, the id-alg-CMS3DESwrap, id-aes192-wrap, and id-aes256-wrap key wrap algorithms and the des-ede3-cbc, id-aes192-cbc, and id-aes256-cbc content encryption algorithms; other algorithms MAY also be supported.

## 7. Security considerations

All security considerations in Section 9 of [CMS-ECC] apply.

Extreme care must be used when using static-static Diffie-Hellman (either standard or cofactor) without the use of some per-message value in ukm. If no message-specific information is used (such as a counter value, or a fresh random string) then the resulting secret key could be used in more than one message. Under some circumstances, this will open the sender to the 'small subgroup' attack [MenezesUstaoglu] or other, yet-undiscovered attacks on re-used Diffie-Hellman keys. Applications that cannot tolerate the inclusion of per-message information in ukm (due to bandwidth requirements, for example) SHOULD NOT use static-static ECDH for a recipient without ascertaining that the recipient knows the private value associated with their certified Diffie-Hellman value. Static-static Diffie-Hellman, when used as described in this document, does not necessarily provide data-origin authentication. Consder, for example, the following sequence of events:

- Alice sends an AuthEnvelopedData message to both Bob and Mallory. Furthermore, Alice uses a static-static DH method to transport the content-authenticated-encryption key to Bob, and some arbitrary method to transport the same key to Mallory.

- Mallory intercepts the message and prevents Bob from receiving it.

- Mallory recovers the content-authenticated-encryption key from the message received from Alice. Mallory then creates new plaintext of her choice, and encrypts it using the same authenticated-encryption algorithm and the same content-authenticated-encryption key used by Alice.

- Mallory then replaces the EncryptedContentInfo and MessageAuthenticationCode fields of Alice's message with the values Mallory just generated. She may additionally remove her RecipientInfo value from Alice's message.

- Mallory sends the modified message to Bob.

- Bob receives the message, validates the static-static DH works and decrypts/authenticates the message.

At this point, Bob has received and validated a message that appears to have been sent by Alice, but whose content was chosen by Mallory. Mallory may not even be an apparent reciever of the modified message. Thus, this use of static-static Diffie-Hellman does not necessarily provide data-origin authentication. (We note that this example does not also contradict either confidentiality or data-authentication: Alice's message was not received by anyone not intended by Alice, and Mallory's message was not modified before reaching Bob.) More generally, data-origin may not be authenticated unless

- It is a priori guaranteed that the message in question was sent to exactly one recipient, or

- Data-origin authentication is provided by some other mechanism (such as digital signatures).

## 8. IANA Considerations

There are no IANA considerations.

## 9. Acknowledgements

The authors would like to thank Jim Schaad, Russ Housley, and Sean

Turner for their helpful comments and suggestions. We would also like to thank Jim Schaad for describing to us the attack described in Section 7.

## 10. References

### 10.1. Normative References

[CMS] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 5652, September 2009.

[CMS-AUTHENV] Housley, R., "Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type", RFC 5083, November 2007.

[CMS-ECC] Turner, S. and D. Brown, "Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)", RFC 5753, January 2010.

[MUST] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[PKI-ECC] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", RFC 5480, March 2009.

[SEC1] Standards for Efficient Cryptography Group (SECG), "SEC 1: Elliptic Curve Cryptography", Version 2.0, May 2009.

### 10.2. Informative References

[CMS-ALG] Housley, R., "Cryptographic Message Syntax (CMS) Algorithms", RFC 3370, August 2002.

[DH] Rescorla, E., "Diffie-Hellman Key Agreement Method", RFC 2631, June 1999.

[MenezesUstaoglu] Menezes, A. and B. Ustaoglu, "On Reusing Ephemeral Keys in Diffie-Hellman Key Agreement Protocols".

International Journal of Applied Cryptography, to appear.

[X.680] ITU-T, "Information Technology - Abstract Syntax Notation One", Recommendation X.680, ISO/IEC 8824-1:2002, 2002.

[X.681] ITU-T, "Information Technology - Abstract Syntax Notation One: Information Object Specifcation", Recommendation X.681, ISO/IEC 8824-2:2002, 2002.

[X.682] ITU-T, "Information Technology - Abstract Syntax Notation One: Constraint Specification", Recommendation X.682, ISO/IEC 8824-3:2002, 2002.

[X.683] ITU-T, "Information Technology - Abstract Syntax Notation One: Parameterization of ASN.1 Specifications", Recommendation X.683, ISO/IEC 8824-4:2002, 2002.

## Authors' Addresses

Jonathan C. Herzog
MIT Lincoln Laboratory
244 Wood St.
Lexington, MA 02144
USA

Email: jherzog@ll.mit.edu

Roger Khazan
MIT Lincoln Laboratory
244 Wood St.
Lexington, MA 02144
USA

Email: rkh@ll.mit.edu