

Delay-Tolerant Networking
Internet-Draft
Intended status: Experimental
Expires: July 3, 2016

E. Birrane
JHU/APL
December 31, 2015

Suite B Ciphersuites for Bundle Protocol Security (BPsec)
draft-birrane-dtn-bpsec-suiteb-ciphersuites-00

Abstract

This document proposes ciphersuites to be used for Bundle Protocol Security (BPsec). These new ciphersuites provide compatibility with the United States National Security Agency's Suite B specifications.

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 July 3, 2016.

Copyright Notice

Copyright (c) 2015 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.

Internet-Draft Suite B Ciphersuites for Bundle Protocol Security December 2015

Table of Contents

1.	Introduction	2
2.	Requirements Language	2
3.	Suite B Ciphersuites	2
3.1.	Overview	2
3.2.	Suites BIB-ECDSA-SHA256 and BIB-ECDSA-SHA384	3
3.3.	Suites BCB-ECDH-SHA256-AES128 and BCB-ECDH-SHA384-AES256	4
4.	Security Considerations	5
5.	IANA Considerations	6
6.	References	6
6.1.	Normative References	6
6.2.	Informative References	8
	Author's Address	8

[1.](#) Introduction

This document specifies ciphersuites to be used with Bundle Protocol Security (BPSec) [[I-D.ietf-dtn-bpsec](#)]. These suites provide compatibility with the United States National Security Agency's Suite B specifications.

This document is an update to the Suite-B profile created by Burgin and Hennessy [[I-D.hennessy-bsp-suiteb-ciphersuites](#)]. This update adapts the profile from BSP [[RFC6257](#)] to BPSec.

[2.](#) Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

[3.](#) Suite B Ciphersuites[3.1.](#) Overview

This section defines new ciphersuites for use with the security block types BIB and BCB. The BIB ciphersuites are based on digital signatures using ECDSA. The BCB ciphersuites use ECDH for key agreement, AES in Galois/Counter Mode (GCM) for content encryption, and AES Key Wrap for key encryption. All proposed ciphersuites use SHA-256 or SHA-384 as the hash algorithm.

The ciphersuites use the mechanisms defined in Cryptographic Message Syntax (CMS) [[RFC5652](#)] for packaging the keys, signatures, etc., for transport in the appropriate security block. Additionally, the ciphersuites follow the guidance and requirements of [RFC 6318](#)

Internet-Draft Suite B Ciphersuites for Bundle Protocol Security December 2015

[[RFC6318](#)] which specifies the conventions for using Suite B algorithms in Secure/Multipurpose Internet Mail Extensions (S/MIME).

CMS values are generated using ASN.1 [[X.208-88](#)], the Basic Encoding Rules (BER) [[X.209-88](#)], and the Distinguished Encoding Rules (DER) [[X.509-88](#)].

[3.2.](#) Suites BIB-ECDSA-SHA256 and BIB-ECDSA-SHA384

The BIB-ECDSA-SHA256 ciphersuite has ciphersuite ID value 0xB1, and the BIB-ECDSA-SHA384 ciphersuite has ciphersuite ID value 0xB2.

In BIB-ECDSA-SHA256, ECDSA MUST be used with the SHA-256 message digest algorithm and the P-256 elliptic curve, as specified in [[RFC6318](#)]. In BIB-ECDSA-SHA384, ECDSA MUST be used with the SHA-384 message digest algorithm and the P-384 elliptic curve, as specified in [[RFC6318](#)]. The P-256 and P-384 elliptic curves are specified in [[DSS](#)].

The SHA-256 and SHA-384 message digest algorithms are defined in FIPS Pub 180-3 [[RFC5754](#)]. The algorithm identifiers for SHA-256 and SHA-384 are defined in [[RFC5754](#)]. [RFC 5754](#) specifies the conventions for using SHA-256 and SHA-384 with CMS. Within the CMS signed-data content type, message digest algorithm identifiers are located in the SignedData digestAlgorithms field and the SignerInfo digestAlgorithm field.

[RFC 5753](#) [[RFC5753](#)] specifies the conventions for using ECDSA with CMS. [RFC 5480](#) [[RFC5480](#)] defines the signature algorithm identifiers used in CMS for ECDSA with SHA-256 and ECDSA with SHA-384. Relevant details are repeated here.

Within the CMS signed-data content type, signature algorithm identifiers are located in the SignerInfo signatureAlgorithm field of SignedData. In addition, signature algorithm identifiers are located in the SignerInfo signatureAlgorithm field of countersignature

attributes. When either signature algorithm identifier is used, the AlgorithmIdentifier parameters field MUST be absent.

When signing, the ECDSA algorithm generates two values, commonly called *r* and *s*. To transfer these two values as one signature, they MUST be encoded using the ECDSA-Sig-Value type specified in [RFC 5480](#) [RFC5480].

Because the signature field in SignedData SignatureValue is a security-result field, the entire key-information item MUST be placed in the BIB's security-result field, rather than security- parameters.

[3.3.](#) Suites BCB-ECDH-SHA256-AES128 and BCB-ECDH-SHA384-AES256

The BCB-ECDH-SHA256-AES128 ciphersuite has ciphersuite ID value 0xB3, and the BCB-ECDH-SHA384-AES256 ciphersuite has ciphersuite ID value 0xB4.

These schemes encrypt any block in a bundle except the primary block and another BCB block. Both ciphersuites use ephemeral-static ECDH, which means that the security source possesses an ephemeral ECDH key pair and the security destination possesses a static ECDH key pair.

In BCB-ECDH-SHA256-AES128, ephemeral-static ECDH MUST be used with the SHA-256 KDF, AES-128 Key Wrap, and the P-256 elliptic curve, as specified in [\[RFC6318\]](#). In BCB-ECDH-SHA384-AES256, ephemeral-static ECDH MUST be used with the SHA-384 KDF, AES-256 Key Wrap, and the P-384 elliptic curve, as specified in [\[RFC6318\]](#). The P-256 and P-384 elliptic curves are specified in [\[DSS\]](#).

When a key agreement algorithm is used in CMS, a key-encryption algorithm is also needed to encrypt the content encryption key (CEK). These ciphersuites use Advanced Encryption Standard (AES) Key Wrap, as specified in [RFC 3394](#) [RFC3394] and [\[AESWRAP\]](#), as the key-encryption algorithm. The key-encryption key used with the AES Key Wrap algorithm is obtained from a key derivation function (KDF). These ciphersuites use a KDF based on SHA-256 and SHA-384.

[Section 3.1 of RFC 5753](#) [RFC5753] specifies the conventions for using ECDH with CMS. Here the bundle encryption key (BEK), used to encrypt the target block, is the data to be carried in a CMS enveloped-data

content type. CMS encrypts the BEK with a freshly generated content encryption key (CEK) and the result is placed in the encryptedContent field of an EnvelopedData EncryptedContentInfo structure. The CEK is encrypted with the ECDH-generated pairwise key-encryption key (KEK) using the AES Key Wrap algorithm. The result is placed in the EnvelopedData RecipientInfos KeyAgreeRecipientInfo RecipientEncryptedKey EncryptedKey field.

Algorithm identifiers needed when using ECDH with CMS are provided in [RFC 6318 \[RFC6318\] section 4](#). Within the CMS enveloped-data content type, the key agreement algorithm identifier is placed in the EnvelopedData RecipientInfos KeyAgreeRecipientInfo keyEncryptionAlgorithm field. The key wrap algorithm identifier is placed in the KeyWrapAlgorithm parameters within the EnvelopedData RecipientInfos KeyAgreeRecipientInfo keyEncryptionAlgorithm field.

KDFs based on SHA-256 and SHA-384 are used to derive a pairwise key-encryption key from the shared secret produced by ephemeral-static ECDH. [Section 4.3 of RFC 6318 \[RFC6318\]](#) specify the conventions for

using the KDF with the shared secret generated with ephemeral-static ECDH with the CMS.

Target block CSP encryption is done using the AES algorithm in Galois/ Counter Mode (GCM) as described in [\[RFC5084\]](#). For consistency with the description in [\[RFC5084\]](#), we refer to the GCM IV as a nonce. The same key and nonce combination MUST NOT be used more than once. The nonce is constructed by concatenating a salt field and an initialization vector, as follows.

The salt field is a four-octet value, usually chosen at random. The salt need not be kept secret. The initialization vector (IV) is an eight-octet value, usually chosen at random. The value need not be kept secret.

The BEK is a 16-octet (128 bits) value in BCB-ECDH-SHA256-AES128, and is a 32-octet value (256 bits) in BCB-ECDH-SHA384-AES256. The BEK SHOULD be chosen randomly and MUST be kept secret.

The Integrity Check Value (ICV) from the AES-GCM content encryption is a 16-octet value used to verify that the protected data has not been altered. Normally, the ICV is concatenated with the ciphertext

to produce the output of AES-GCM encryption. However, to avoid expansion of the payload, the ICV value is placed in the security-result field of the BCB. The value need not be kept secret.

Each ciphersuite populates a single BCB in the bundle. This BCB MUST contain security-parameters and security-result fields. The security-parameters field includes the salt, IV, and key-information items where the key- information item contains the encrypted BEK encoded in a CMS EnvelopedData structure. The security-results-field contains the ICV. The ciphertext is NOT stored in the BCB, but replaces the plaintext from the target block. The other bytes of the target block, such as type, flags, and length, are not modified.

[4.](#) Security Considerations

Two levels of security may be achieved using this specification. Users must consider their risk environment to determine which level is appropriate for their own use.

The security considerations in [[I-D.ietf-dtn-bpsec](#)] discuss the BPsec Protocol and apply here as well.

The security considerations in [[RFC5652](#)] discuss the CMS as a method for digitally signing data and encrypting data.

The security considerations in [[RFC3370](#)] discuss cryptographic algorithm implementation concerns in the context of the CMS.

The security considerations in [[RFC5753](#)] discuss the use of elliptic curve cryptography (ECC) in the CMS.

The security considerations in [[RFC3565](#)] discuss the use of AES in the CMS, and the security considerations in [[RFC5084](#)] discuss the Galois/Counter Mode.

[5.](#) IANA Considerations

This protocol has fields that have been registered by IANA.

The BPsec has a ciphersuite number field and certain ciphersuites are

defined. The registration policy for this registry is: Specification Required. The Value range is: Variable Length.

IANA is requested to assign the following values for the ciphersuite number field.

Ciphersuite Numbers Registry:

Value	Description	Reference
0xB1	BIB-ECDSA-SHA256	This document
0xB2	BIB-ECDSA-SHA384	This document
0xB3	BCB-ECDH-SHA256-AES128	This document
0xB4	BCB-ECDH-SHA384-AES256	This document

6. References

6.1. Normative References

- [AESWRAP] National Institute of Standards and Technology, "AES Key Wrap Specification", November 2001.
- [DSS] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", FIPS PUB 186-3, June 2009.
- [FIPS180-3] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-3, October 2008.

- [FIPS197] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001.
- [I-D.ietf-dtn-bpsec] Birrane, E., Pierce-Mayer, J., and D. Iannicca, "Bundle Protocol Security Specification", [draft-ietf-dtn-bpsec-00](#) (work in progress), December 2015.

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC3370] Housley, R., "Cryptographic Message Syntax (CMS) Algorithms", [RFC 3370](#), DOI 10.17487/RFC3370, August 2002, <<http://www.rfc-editor.org/info/rfc3370>>.
- [RFC3394] Schaad, J. and R. Housley, "Advanced Encryption Standard (AES) Key Wrap Algorithm", [RFC 3394](#), DOI 10.17487/RFC3394, September 2002, <<http://www.rfc-editor.org/info/rfc3394>>.
- [RFC3565] Schaad, J., "Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)", [RFC 3565](#), DOI 10.17487/RFC3565, July 2003, <<http://www.rfc-editor.org/info/rfc3565>>.
- [RFC5084] Housley, R., "Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS)", [RFC 5084](#), DOI 10.17487/RFC5084, November 2007, <<http://www.rfc-editor.org/info/rfc5084>>.
- [RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", [RFC 5480](#), DOI 10.17487/RFC5480, March 2009, <<http://www.rfc-editor.org/info/rfc5480>>.
- [RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, [RFC 5652](#), DOI 10.17487/RFC5652, September 2009, <<http://www.rfc-editor.org/info/rfc5652>>.
- [RFC5753] Turner, S. and D. Brown, "Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)", [RFC 5753](#), DOI 10.17487/RFC5753, January 2010, <<http://www.rfc-editor.org/info/rfc5753>>.
- [RFC5754] Turner, S., "Using SHA2 Algorithms with Cryptographic Message Syntax", [RFC 5754](#), DOI 10.17487/RFC5754, January 2010, <<http://www.rfc-editor.org/info/rfc5754>>.

Multipurpose Internet Mail Extensions (S/MIME)", [RFC 6318](#), DOI 10.17487/RFC6318, June 2011, <<http://www.rfc-editor.org/info/rfc6318>>.

[6.2](#). Informative References

- [I-D.hennessy-bsp-suiteb-ciphersuites]
Burgin, K. and A. Hennessy, "Suite B Ciphersuites for the Bundle Security Protocol", [draft-hennessy-bsp-suiteb-ciphersuites-00](#) (work in progress), March 2012.
- [I-D.hennessy-bsp-suiteb-profile]
Burgin, K. and A. Hennessy, "Suite B Profile for the Bundle Security Protocol", [draft-hennessy-bsp-suiteb-profile-00](#) (work in progress), March 2012.
- [RFC5050] Scott, K. and S. Burleigh, "Bundle Protocol Specification", [RFC 5050](#), DOI 10.17487/RFC5050, November 2007, <<http://www.rfc-editor.org/info/rfc5050>>.
- [RFC6257] Symington, S., Farrell, S., Weiss, H., and P. Lovell, "Bundle Security Protocol Specification", [RFC 6257](#), DOI 10.17487/RFC6257, May 2011, <<http://www.rfc-editor.org/info/rfc6257>>.
- [SP800-56A]
National Institute of Standards and Technology, "Recommendation for Pair-wise Key Establishment Schemes Using Discrete Logarithm Cryptography", NIST Special Publication 800-56A, March 2007.
- [SuiteB] U.S. National Security Agency, "Fact Sheet NSA Suite B Cryptography", NIST Special Publication 800-56A, January 2009, <http://www.nsa.gov/ia/programs/suiteb_cryptography/>.

Author's Address

Edward J. Birrane
The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Rd.
Laurel, MD 20723
US

Phone: +1 443 778 7423
Email: Edward.Birrane@jhuapl.edu