

CoRE Working Group  
Internet-Draft  
Intended status: Informational  
Expires: June 9, 2013

C. Bormann  
Universitaet Bremen TZI  
December 06, 2012

Using CoAP with IPsec  
draft-bormann-core-ipsec-for-coap-00

Abstract

CoAP is a RESTful transfer protocol for constrained nodes and networks. Security for the protocol can be supplied in a number of ways. The mandatory-to-implement security mode for CoAP makes use of DTLS. Other applications may want to use IPsec.

This document will discuss considerations for the use of IPsec with CoAP. It will be advanced on a timescale separate from the main CoAP specification, as most experience in securing CoAP so far has been made with DTLS.

The current version of this specification is a placeholder, built out of text extracted from draft-ietf-core-coap-12. It is meant to pick up <http://trac.tools.ietf.org/wg/core/trac/ticket/262> and provide a home for its considerations. It might be merged with other documents later.

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 June 9, 2013.

Copyright Notice

Copyright (c) 2012 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

1. Introduction . . . . .	3
2. Using CoAP with IPsec . . . . .	4
3. IANA Considerations . . . . .	5
4. Security Considerations . . . . .	6
5. Acknowledgements . . . . .	7
6. References . . . . .	8
6.1. Normative References . . . . .	8
6.2. Informative References . . . . .	8
Author's Address . . . . .	9

## 1. Introduction

(see abstract for now)

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 RFC 2119, BCP 14 [RFC2119] and indicate requirement levels for compliant CoAP implementations.

In this document, the term "byte" is used in its now customary sense as a synonym for "octet".

Where bit arithmetic is explained, this document uses the notation familiar from the programming language C, except that the operator "\*\*\*" stands for exponentiation.

## 2. Using CoAP with IPsec

One mechanism to secure CoAP [I-D.ietf-core-coap] in constrained environments is the IPsec Encapsulating Security Payload (ESP) [RFC4303] when CoAP is used without DTLS in NoSec Mode. Using IPsec ESP with the appropriate configuration, it is possible for many constrained devices to support encryption with built-in link-layer encryption hardware. For example, some IEEE 802.15.4 radio chips are compatible with AES-CBC (with 128-bit keys) [RFC3602] as defined for use with IPsec in [RFC4835]. Alternatively, particularly on more common IEEE 802.15.4 hardware that supports AES encryption but not decryption, and to avoid the need for padding, nodes could directly use the more widely supported AES-CCM as defined for use with IPsec in [RFC4309], if the security considerations in Section 9 of that specification can be fulfilled.

Necessarily for AES-CCM, but much preferably also for AES-CBC, static keying should be avoided and the initial keying material be derived into transient session keys, e.g. using a low-overhead mode of IKEv2 [RFC5996] as described in [I-D.kivinen-ipsecme-ikev2-minimal]; such a protocol for managing keys and sequence numbers is also the only way to achieve anti-replay capabilities. However, no recommendation can be made at this point on how to manage group keys (i.e., for multicast) in a constrained environment. Once any initial setup is completed, IPsec ESP adds a limited overhead of approximately 10 bytes per packet, not including initialization vectors, integrity check values and padding required by the cipher suite.

When using IPsec to secure CoAP, both authentication and confidentiality SHOULD be applied as recommended in [RFC4303]. The use of IPsec between CoAP endpoints is transparent to the application layer and does not require special consideration for a CoAP implementation.

IPsec may not be appropriate for all environments. For example, IPsec support is not available for many embedded IP stacks and even in full PC operating systems or on back-end web servers, application developers may not have sufficient access to configure or enable IPsec or to add a security gateway to the infrastructure. Problems with firewalls and NATs may furthermore limit the use of IPsec.

### 3. IANA Considerations

(none foreseen.)

#### 4. Security Considerations

TBD.

## 5. Acknowledgements

This text was extracted from draft-ietf-core-coap-12.txt and probably mostly was written by Zach Shelby.

## 6. References

### 6.1. Normative References

- [I-D.ietf-core-coap]  
Shelby, Z., Hartke, K., Bormann, C., and B. Frank,  
"Constrained Application Protocol (CoAP)",  
draft-ietf-core-coap-12 (work in progress), October 2012.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate  
Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher  
Algorithm and Its Use with IPsec", RFC 3602,  
September 2003.
- [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)",  
RFC 4303, December 2005.
- [RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM  
Mode with IPsec Encapsulating Security Payload (ESP)",  
RFC 4309, December 2005.
- [RFC4835] Manral, V., "Cryptographic Algorithm Implementation  
Requirements for Encapsulating Security Payload (ESP) and  
Authentication Header (AH)", RFC 4835, April 2007.
- [RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen,  
"Internet Key Exchange Protocol Version 2 (IKEv2)",  
RFC 5996, September 2010.

### 6.2. Informative References

- [I-D.kivinen-ipsecme-ikev2-minimal]  
Kivinen, T., "Minimal IKEv2",  
draft-kivinen-ipsecme-ikev2-minimal-01 (work in progress),  
October 2012.



Author's Address

Carsten Bormann  
Universitaet Bremen TZI  
Postfach 330440  
Bremen D-28359  
Germany

Phone: +49-421-218-63921  
Email: [cabo@tzi.org](mailto:cabo@tzi.org)

