

CoRE Working Group
Internet-Draft
Updates: [7252](#) (if approved)
Intended status: Standards Track
Expires: September 25, 2019

C. Amsuess

J. Mattsson
G. Selander
Ericsson AB
March 24, 2019

CoAP: Echo, Request-Tag, and Token Processing
draft-ietf-core-echo-request-tag-04

Abstract

This document specifies enhancements to the Constrained Application Protocol (CoAP) that mitigate security issues in particular use cases. The Echo option enables a CoAP server to verify the freshness of a request or to force a client to demonstrate reachability at its claimed network address. The Request-Tag option allows the CoAP server to match Block-Wise message fragments belonging to the same request. The updated Token processing requirements for clients ensure secure binding of responses to requests when CoAP is used with security.

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 <https://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 September 25, 2019.

Copyright Notice

Copyright (c) 2019 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 (<https://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	2
1.1.	Request Freshness	3
1.2.	Fragmented Message Body Integrity	4
1.3.	Request-Response Binding	4
1.4.	Terminology	5
2.	The Echo Option	6
2.1.	Option Format	6
2.2.	Echo Processing	7
2.3.	Applications	10
3.	The Request-Tag Option	11
3.1.	Option Format	11
3.2.	Request-Tag Processing by Servers	12
3.3.	Setting the Request-Tag	13
3.4.	Applications	14
3.4.1.	Body Integrity Based on Payload Integrity	14
3.4.2.	Multiple Concurrent Blockwise Operations	15
3.4.3.	Simplified Block-Wise Handling for Constrained Proxies	16
3.5.	Rationale for the Option Properties	16
3.6.	Rationale for Introducing the Option	16
4.	Block2 / ETag Processing	17
5.	Token Processing	17
6.	Security Considerations	17
7.	Privacy Considerations	18
8.	IANA Considerations	19
9.	References	19
9.1.	Normative References	19
9.2.	Informative References	19
Appendix A.	Methods for Generating Echo Option Values	20
Appendix B.	Request-Tag Message Size Impact	22
Appendix C.	Change Log	22
	Acknowledgments	24
	Authors' Addresses	24

[1.](#) Introduction

The initial Constrained Application Protocol (CoAP) suite of specifications ([[RFC7252](#)], [[RFC7641](#)], and [[RFC7959](#)]) was designed with the assumption that security could be provided on a separate

layer, in particular by using DTLS ([RFC6347]). However, for some use cases, additional functionality or extra processing is needed to support secure CoAP operations. This document specifies security enhancements to the Constrained Application Protocol (CoAP).

This document specifies two CoAP options, the Echo option and the Request-Tag option: The Echo option enables a CoAP server to verify the freshness of a request, synchronize state, or force a client to demonstrate reachability at its claimed network address. The Request-Tag option allows the CoAP server to match message fragments belonging to the same request, fragmented using the CoAP Block-Wise Transfer mechanism, which mitigates attacks and enables concurrent blockwise operations. These options in themselves do not replace the need for a security protocol; they specify the format and processing of data which, when integrity protected using e.g. DTLS ([RFC6347]), TLS ([RFC8446]), or OSCORE ([I-D.ietf-core-object-security]), provide the additional security features.

The document also updates the Token processing requirements for clients specified in [RFC7252]. The updated processing ensures secure binding of responses to requests when CoAP is used with security, thus mitigating error cases and attacks where the client may erroneously associate the wrong response to a request.

1.1. Request Freshness

A CoAP server receiving a request is in general not able to verify when the request was sent by the CoAP client. This remains true even if the request was protected with a security protocol, such as DTLS. This makes CoAP requests vulnerable to certain delay attacks which are particularly perilous in the case of actuators ([I-D.mattsson-core-coap-actuators]). Some attacks can be mitigated by establishing fresh session keys, e.g. performing a DTLS handshake for each request, but in general this is not a solution suitable for constrained environments, for example, due to increased message overhead and latency. Additionally, if there are proxies, fresh DTLS session keys between server and proxy does not say anything about when the client made the request. In a general hop-by-hop setting, freshness may need to be verified in each hop.

A straightforward mitigation of potential delayed requests is that the CoAP server rejects a request the first time it appears and asks the CoAP client to prove that it intended to make the request at this point in time. The Echo option, defined in this document, specifies such a mechanism which thereby enables a CoAP server to verify the freshness of a request. This mechanism is not only important in the case of actuators, or other use cases where the CoAP operations require freshness of requests, but also in general for synchronizing

state between CoAP client and server, verify aliveness of the client, or force a client to demonstrate reachability at its claimed network address. The same functionality can be provided by echoing freshness tokens in CoAP payloads, but this only works for methods and response codes defined to have a payload. The Echo option provides a convention to transfer freshness tokens that works for all methods and response codes.

1.2. Fragmented Message Body Integrity

CoAP was designed to work over unreliable transports, such as UDP, and include a lightweight reliability feature to handle messages which are lost or arrive out of order. In order for a security protocol to support CoAP operations over unreliable transports, it must allow out-of-order delivery of messages using e.g. a sliding replay window such as described in [Section 4.1.2.6](#) of DTLS ([RFC6347]).

The Block-Wise Transfer mechanism [RFC7959] extends CoAP by defining the transfer of a large resource representation (CoAP message body) as a sequence of blocks (CoAP message payloads). The mechanism uses a pair of CoAP options, Block1 and Block2, pertaining to the request and response payload, respectively. The blockwise functionality does not support the detection of interchanged blocks between different message bodies to the same resource having the same block number. This remains true even when CoAP is used together with a security protocol such as DTLS or OSCORE, within the replay window ([I-D.mattsson-core-coap-actuators]), which is a vulnerability of CoAP when using RFC7959.

A straightforward mitigation of mixing up blocks from different messages is to use unique identifiers for different message bodies, which would provide equivalent protection to the case where the complete body fits into a single payload. The ETag option [RFC7252], set by the CoAP server, identifies a response body fragmented using the Block2 option. This document defines the Request-Tag option for identifying request bodies, similar to ETag, but ephemeral and set by the CoAP client. The Request-Tag option is only used in requests that carry the Block1 option, and in Block2 requests following these.

1.3. Request-Response Binding

A fundamental requirement of secure REST operations is that the client can bind a response to a particular request. If this is not ensured, a client may erroneously associate the wrong response to a request. The wrong response may be an old response for the same resource or for a completely different resource (see e.g. Section 2.3 of [I-D.mattsson-core-coap-actuators]). For example, a

request for the alarm status "GET /status" may be associated to a prior response "on", instead of the correct response "off".

In HTTPS, this type of binding is always assured by the ordered and reliable delivery as well as mandating that the server sends responses in the same order that the requests were received. The same is not true for CoAP where the server (or an attacker) can return responses in any order and where there can be any number of responses to a request (see e.g. [\[RFC7641\]](#)). In CoAP, concurrent requests are differentiated by their Token. Note that the CoAP Message ID cannot be used for this purpose since those are typically different for REST request and corresponding response in case of "separate response", see [Section 2.2 of \[RFC7252\]](#).

CoAP [\[RFC7252\]](#) does not treat Token as a cryptographically important value and does not give stricter guidelines than that the tokens currently "in use" SHOULD (not SHALL) be unique. If used with a security protocol not providing bindings between requests and responses (e.g. DTLS and TLS) token reuse may result in situations where a client matches a response to the wrong request. Note that mismatches can also happen for other reasons than a malicious attacker, e.g. delayed delivery or a server sending notifications to an uninterested client.

A straightforward mitigation is to mandate clients to not reuse tokens until the traffic keys have been replaced. The easiest way to accomplish this is to implement the token as a counter starting at zero for each new or rekeyed secure connection. This document updates the Token processing in [\[RFC7252\]](#) to always assure a cryptographically secure binding of responses to requests for secure REST operations like "coaps".

[1.4.](#) Terminology

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 [BCP 14 \[RFC2119\]](#) [\[RFC8174\]](#) when, and only when, they appear in all capitals, as shown here.

Unless otherwise specified, the terms "client" and "server" refers to "CoAP client" and "CoAP server", respectively, as defined in [\[RFC7252\]](#). The term "origin server" is used as in [\[RFC7252\]](#). The term "origin client" is used in this document to denote the client from which a request originates; to distinguish from clients in proxies.

The terms "payload" and "body" of a message are used as in [\[RFC7959\]](#). The complete interchange of a request and a response body is called a (REST) "operation". An operation fragmented using [\[RFC7959\]](#) is called a "blockwise operation". A blockwise operation which is fragmenting the request body is called a "blockwise request operation". A blockwise operation which is fragmenting the response body is called a "blockwise response operation".

Two request messages are said to be "matchable" if they occur between the same endpoint pair, have the same code and the same set of options except for elective NoCacheKey options and options involved in block-wise transfer (Block1, Block2 and Request-Tag). Two operations are said to be matchable if any of their messages are.

Two matchable blockwise operations are said to be "concurrent" if a block of the second request is exchanged even though the client still intends to exchange further blocks in the first operation. (Concurrent blockwise request operations are impossible with the options of [\[RFC7959\]](#) because the second operation's block overwrites any state of the first exchange.).

The Echo and Request-Tag options are defined in this document.

2. The Echo Option

A fresh request is one whose age has not yet exceeded the freshness requirements set by the server. The freshness requirements are application specific and may vary based on resource, method, and parameters outside of coap such as policies. The Echo option is a lightweight challenge-response mechanism for CoAP, motivated by a need for a server to verify freshness of a request as described in [Section 1.1](#). The Echo option value is a challenge from the server to the client included in a CoAP response and echoed back to the server in one or more CoAP requests. The Echo option provides a convention to transfer freshness tokens that works for all CoAP methods and response codes.

2.1. Option Format

The Echo Option is elective, safe-to-forward, not part of the cache-key, and not repeatable, see Figure 1, which extends Table 4 of [\[RFC7252\]](#)).

No.	C	U	N	R	Name	Format	Len.	Default	E	U
TBD			x		Echo	opaque	4-40	(none)	x	x

C = Critical, U = Unsafe, N = NoCacheKey, R = Repeatable,
E = Encrypt and Integrity Protect (when using OSCORE)

Figure 1: Echo Option Summary

[Note to RFC editor: If this document is released before core-object-security, then the following paragraph and the "E"/"U" columns above need to move into core-object-security, as they are defined in that draft.]

The Echo option value is generated by a server, and its content and structure are implementation specific. Different methods for generating Echo option values are outlined in [Appendix A](#). Clients and intermediaries MUST treat an Echo option value as opaque and make no assumptions about its content or structure.

When receiving an Echo option in a request, the server MUST be able to verify when the Echo option value was generated. This implies that the server MUST be able to verify that the Echo option value was generated by the server or some other party that the server trusts. Depending on the freshness requirements the server may verify exactly when the Echo option value was generated (time-based freshness) or verify that the Echo option was generated after a specific event (event-based freshness). As the request is bound to the Echo option value, the server can determine that the request is not older than the Echo option value.

When the Echo option is used with OSCORE

[[I-D.ietf-core-object-security](#)] it MAY be an Inner or Outer option, and the Inner and Outer values are independent. The Inner option is encrypted and integrity protected between the endpoints, whereas the Outer option is not protected by OSCORE and visible between the endpoints to the extent it is not protected by some other security protocol. E.g. in the case of DTLS hop-by-hop between the endpoints, the Outer option is visible to proxies along the path.

2.2. Echo Processing

The Echo option MAY be included in any request or response (see [Section 2.3](#) for different applications), but the Echo option MUST NOT be used with empty CoAP requests (i.e., Code=0.00).

The application decides under what conditions a CoAP request to a resource is required to be fresh. These conditions can for example include what resource is requested, the request method and other data in the request, and conditions in the environment such as the state of the server or the time of the day.

If a certain request is required to be fresh, the request does not contain a fresh Echo option value, and the server cannot verify the freshness of the request in some other way, the server **MUST NOT** process the request further and **SHOULD** send a 4.01 Unauthorized response with an Echo option. The server **MAY** include the same Echo option value in several different responses and to different clients.

The server may use request freshness provided by the Echo option to verify the aliveness of a client or to synchronize state. The server may also include the Echo option in a response to force a client to demonstrate reachability at its claimed network address.

Upon receiving a 4.01 Unauthorized response with the Echo option, the client **SHOULD** resend the original request with the addition of an Echo option with the received Echo option value. The client **MAY** send a different request compared to the original request. Upon receiving any other response with the Echo option, the client **SHOULD** echo the Echo option value in the next request to the server. The client **MAY** include the same Echo option value in several different requests to the server.

Upon receiving a request with the Echo option, the server determines if the request is required to be fresh. If not, the Echo option **MAY** be ignored. If the request is required to be fresh and the server cannot verify the freshness of the request in some other way, the server **MUST** use the Echo option to verify that the request is fresh enough. If the server cannot verify that the request is fresh enough, the request is not processed further, and an error message **MAY** be sent. The error message **SHOULD** include a new Echo option.

One way for the server to verify freshness is that to bind the Echo value to a specific point in time and verify that the request is not older than a certain threshold T . The server can verify this by checking that $(t_1 - t_0) < T$, where t_1 is the request receive time and t_0 is the time when the Echo option value was generated. An example message flow is illustrated in Figure 2.

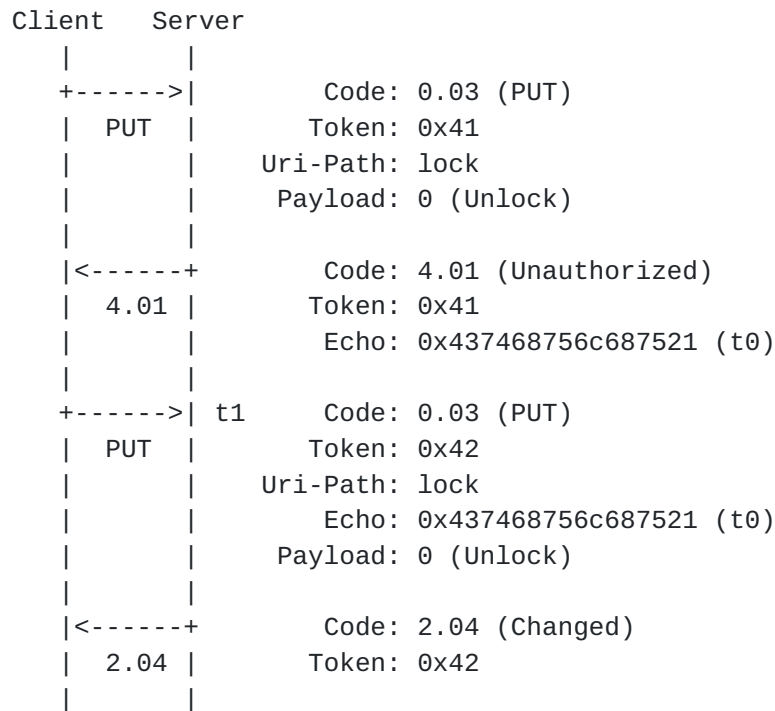


Figure 2: Example Echo Option Message Flow

When used to serve freshness requirements (including client aliveness and state synchronizing), CoAP messages containing the Echo option MUST be integrity protected between the intended endpoints, e.g. using DTLS, TLS, or an OSCORE Inner option ([[I-D.ietf-core-object-security](#)]). When used to demonstrate reachability at a claimed network address, the Echo option SHOULD contain the client's network address, but MAY be unprotected.

A CoAP-to-CoAP proxy MAY respond to requests with 4.01 with an Echo option to ensure the client's reachability at its claimed address, and MUST remove the Echo option it recognizes as one generated by itself on follow-up requests. However, it MUST relay the Echo option of responses unmodified, and MUST relay the Echo option of requests it does not recognize as generated by itself unmodified.

The CoAP server side of CoAP-to-HTTP proxies MAY request freshness, especially if they have reason to assume that access may require it (e.g. because it is a PUT or POST); how this is determined is out of scope for this document. The CoAP client side of HTTP-to-CoAP proxies SHOULD respond to Echo challenges themselves if they know from the recent establishing of the connection that the HTTP request is fresh. Otherwise, they SHOULD respond with 503 Service Unavailable, Retry-After: 0 and terminate any underlying Keep-Alive connection. They MAY also use other mechanisms to establish freshness of the HTTP request that are not specified here.

2.3. Applications

1. Actuation requests often require freshness guarantees to avoid accidental or malicious delayed actuator actions. In general, all non-safe methods (e.g. POST, PUT, DELETE) may require freshness guarantees for secure operation.
 - * The same Echo value may be used for multiple actuation requests to the same server, as long as the total round-trip time since the Echo option value was generated is below the freshness threshold.
 - * For actuator applications with low delay tolerance, to avoid additional round-trips for multiple requests in rapid sequence, the server may include the Echo option with a new value in response to a request containing the Echo option. The client then uses the Echo option with the new value in the next actuation request, and the server compares the receive time accordingly.
2. A server may use the Echo option to synchronize state or time with a requesting client. A server **MUST NOT** synchronize state or time with clients which are not the authority of the property being synchronized. E.g. if access to a server resource is dependent on time, then the client **MUST NOT** set the time of the server.
 - * If a server reboots during operation it may need to synchronize state or time before continuing the interaction. For example, with OSCORE it is possible to reuse a partly persistently stored security context by synchronizing the Partial IV (sequence number) using the Echo option, see Section 7.5 of [[I-D.ietf-core-object-security](#)].
 - * A device joining a CoAP group communication [[RFC7390](#)] protected with OSCORE [[I-D.ietf-core-oscore-groupcomm](#)] may be required to initially verify freshness and synchronize state or time with a client by using the Echo option in a unicast response to a multicast request. The client receiving the response with the Echo option includes the Echo option with the same value in a request, either in a unicast request to the responding server, or in a subsequent group request. In the latter case, the Echo option will be ignored expect by responding server.
3. A server that sends large responses to unauthenticated peers **SHOULD** mitigate amplification attacks such as described in [Section 11.3 of \[RFC7252\]](#) (where an attacker would put a victim's

address in the source address of a CoAP request). For this purpose, a server MAY ask a client to Echo its request to verify its source address. This needs to be done only once per peer and limits the range of potential victims from the general Internet to endpoints that have been previously in contact with the server. For this application, the Echo option can be used in messages that are not integrity protected, for example during discovery.

* In the presence of a proxy, a server will not be able to distinguish different origin client endpoints. Following from the recommendation above, a proxy that sends large responses to unauthenticated peers SHOULD mitigate amplification attacks. The proxy MAY use Echo to verify origin reachability as described in [Section 2.2](#). The proxy MAY forward idempotent requests immediately to have a cached result available when the client's Echoed request arrives.

4. A server may want to use the request freshness provided by the Echo to verify the aliveness of a client. Note that in a deployment with hop-by-hop security and proxies, the server can only verify aliveness of the closest proxy.

3. The Request-Tag Option

The Request-Tag is intended for use as a short-lived identifier for keeping apart distinct blockwise request operations on one resource from one client, addressing the issue described in [Section 1.2](#). It enables the receiving server to reliably assemble request payloads (blocks) to their message bodies, and, if it chooses to support it, to reliably process simultaneous blockwise request operations on a single resource. The requests must be integrity protected in order to protect against interchange of blocks between different message bodies.

In essence, it is an implementation of the "proxy-safe elective option" used just to "vary the cache key" as suggested in [\[RFC7959\]](#) [Section 2.4](#).

3.1. Option Format

The Request-Tag option is not critical, is safe to forward, repeatable, and part of the cache key, see Figure 3, which extends Table 4 of [\[RFC7252\]](#).

No.	C	U	N	R	Name	Format	Len.	Default	E	U
TBD				x	Request-Tag	opaque	0-8	(none)	x	x

C = Critical, U = Unsafe, N = NoCacheKey, R = Repeatable,
E = Encrypt and Integrity Protect (when using OSCORE)

Figure 3: Request-Tag Option Summary

[Note to RFC editor: If this document is released before core-object-security, then the following paragraph and the "E"/"U" columns above need to move into core-object-security, as they are defined in that draft.]

Request-Tag, like the block options, is both a class E and a class U option in terms of OSCORE processing (see Section 4.1 of [\[I-D.ietf-core-object-security\]](#)): The Request-Tag MAY be an inner or outer option. It influences the inner or outer block operation, respectively. The inner and outer values are therefore independent of each other. The inner option is encrypted and integrity protected between client and server, and provides message body identification in case of end-to-end fragmentation of requests. The outer option is visible to proxies and labels message bodies in case of hop-by-hop fragmentation of requests.

The Request-Tag option is only used in the request messages of blockwise operations.

The Request-Tag mechanism can be applied independently on the server and client sides of CoAP-to-CoAP proxies as are the block options, though given it is safe to forward, a proxy is free to just forward it when processing an operation. CoAP-to-HTTP proxies and HTTP-to-CoAP proxies can use Request-Tag on their CoAP sides; it is not applicable to HTTP requests.

3.2. Request-Tag Processing by Servers

The Request-Tag option does not require any particular processing on the server side outside of the processing already necessary for any unknown elective proxy-safe cache-key option: The option varies the properties that distinguish blockwise operations (which includes all options except elective NoCacheKey and except Block1/2), and thus the server can not treat messages with a different list of Request-Tag options as belonging to the same operation.

To keep utilizing the cache, a server (including proxies) MAY discard the Request-Tag option from an assembled block-wise request when consulting its cache, as the option relates to the operation-on-the-wire and not its semantics. For example, a FETCH request with the same body as an older one can be served from the cache if the older's Max-Age has not expired yet, even if the second operation uses a Request-Tag and the first did not. (This is similar to the situation about ETag in that it is formally part of the cache key, but implementations that are aware of its meaning can cache more efficiently, see [\[RFC7252\] Section 5.4.2](#)).

A server receiving a Request-Tag MUST treat it as opaque and make no assumptions about its content or structure.

Two messages carrying the same Request-Tag is a necessary but not sufficient condition for being part of the same operation. They can still be treated as independent messages by the server (e.g. when it sends 2.01/2.04 responses for every block), or initiate a new operation (overwriting kept context) when the later message carries Block1 number 0.

As it has always been, a server that can only serve a limited number of block-wise operations at the same time can delay the start of the operation by replying with 5.03 (Service unavailable) and a Max-Age indicating how long it expects the existing operation to go on, or it can forget about the state established with the older operation and respond with 4.08 (Request Entity Incomplete) to later blocks on the first operation.

[3.3.](#) Setting the Request-Tag

For each separate blockwise request operation, the client can choose a Request-Tag value, or choose not to set a Request-Tag. Starting a request operation matchable to a previous operation and even using the same Request-Tag value is called request tag recycling. The absence of a Request-Tag option is viewed as a value distinct from all values with a single Request-Tag option set; starting a request operation matchable to a previous operation where neither has a Request-Tag option therefore constitutes request tag recycling just as well (also called "recycling the absent option").

Clients MUST NOT recycle a request tag unless the first operation has concluded. What constitutes a concluded operation depends on the application, and is outlined individually in [Section 3.4](#).

When Block1 and Block2 are combined in an operation, the Request-Tag of the Block1 phase is set in the Block2 phase as well for otherwise

the request would have a different set of options and would not be recognized any more.

Clients are encouraged to generate compact messages. This means sending messages without Request-Tag options whenever possible, and using short values when the absent option can not be recycled.

The Request-Tag options MAY be present in request messages that carry a Block2 option even if those messages are not part of a blockwise request operation (this is to allow the operation described in [Section 3.4.3](#)). The Request-Tag option MUST NOT be present in response messages, and MUST NOT be present if neither the Block1 nor the Block2 option is present.

3.4. Applications

3.4.1. Body Integrity Based on Payload Integrity

When a client fragments a request body into multiple message payloads, even if the individual messages are integrity protected, it is still possible for a man-in-the-middle to maliciously replace a later operation's blocks with an earlier operation's blocks (see Section 2.5 of [[I-D.mattsson-core-coap-actuators](#)]). Therefore, the integrity protection of each block does not extend to the operation's request body.

In order to gain that protection, use the Request-Tag mechanism as follows:

- o The individual exchanges MUST be integrity protected end-to-end between client and server.
- o The client MUST NOT recycle a request tag in a new operation unless the previous operation matchable to the new one has concluded.

If any future security mechanisms allow a block-wise transfer to continue after an endpoint's details (like the IP address) have changed, then the client MUST consider messages sent to `_any_` endpoint address within the new operation's security context.

- o The client MUST NOT regard a blockwise request operation as concluded unless all of the messages the client previously sent in the operation have been confirmed by the message integrity protection mechanism, or are considered invalid by the server if replayed.

Typically, in OSCORE, these confirmations can result either from the client receiving an OSCORE response message matching the request (an empty ACK is insufficient), or because the message's sequence number is old enough to be outside the server's receive window.

In DTLS, this can only be confirmed if the request message was not retransmitted, and was responded to.

Authors of other documents (e.g. [[I-D.ietf-core-object-security](#)]) are invited to mandate this behavior for clients that execute blockwise interactions over secured transports. In this way, the server can rely on a conforming client to set the Request-Tag option when required, and thereby conclude on the integrity of the assembled body.

Note that this mechanism is implicitly implemented when the security layer guarantees ordered delivery (e.g. CoAP over TLS [[RFC8323](#)]). This is because with each message, any earlier message can not be replayed any more, so the client never needs to set the Request-Tag option unless it wants to perform concurrent operations.

[3.4.2.](#) Multiple Concurrent Blockwise Operations

CoAP clients, especially CoAP proxies, may initiate a blockwise request operation to a resource, to which a previous one is already in progress, which the new request should not cancel. A CoAP proxy would be in such a situation when it forwards operations with the same cache-key options but possibly different payloads.

For those cases, Request-Tag is the proxy-safe elective option suggested in [[RFC7959](#)] [Section 2.4](#) last paragraph.

When initializing a new blockwise operation, a client has to look at other active operations:

- o If any of them is matchable to the new one, and the client neither wants to cancel the old one nor postpone the new one, it can pick a Request-Tag value that is not in use by the other matchable operations for the new operation.
- o Otherwise, it can start the new operation without setting the Request-Tag option on it.

3.4.3. Simplified Block-Wise Handling for Constrained Proxies

The Block options were defined to be unsafe to forward because a proxy that would forward blocks as plain messages would risk mixing up clients' requests.

The Request-Tag option provides a very simple way for a proxy to keep them separate: if it appends a Request-Tag that is particular to the requesting endpoint to all request carrying any Block option, it does not need to keep track of any further block state.

This is particularly useful to proxies that strive for stateless operation as described in [[I-D.hartke-core-stateless](#)] [Section 3.1](#).

3.5. Rationale for the Option Properties

The Request-Tag option can be elective, because to servers unaware of the Request-Tag option, operations with differing request tags will not be matchable.

The Request-Tag option can be safe to forward but part of the cache key, because to proxies unaware of the Request-Tag option will consider operations with differing request tags unmatchable but can still forward them.

The Request-Tag option is repeatable because this easily allows stateless proxies to "chain" their origin address. They can perform the steps of [Section 3.4.3](#) without the need to create an option value that is the concatenation of the received option and their own value, and can simply add a new Request-Tag option unconditionally.

In draft versions of this document, the Request-Tag option used to be critical and unsafe to forward. That design was based on an erroneous understanding of which blocks could be composed according to [[RFC7959](#)].

3.6. Rationale for Introducing the Option

An alternative that was considered to the Request-Tag option for coping with the problem of fragmented message body integrity ([Section 3.4.1](#)) was to update [[RFC7959](#)] to say that blocks could only be assembled if their fragments' order corresponded to the sequence numbers.

That approach would have been difficult to roll out reliably on DTLS where many implementations do not expose sequence numbers, and would still not prevent attacks like in [[I-D.mattsson-core-coap-actuators](#)] [Section 2.5.2](#).

4. Block2 / ETag Processing

The same security properties as in [Section 3.4.1](#) can be obtained for blockwise response operations. The threat model here is not an attacker (because the response is made sure to belong to the current request by the security layer), but blocks in the client's cache.

Rules stating that response body reassembly is conditional on matching ETag values are already in place from [Section 2.4 of \[RFC7959\]](#).

To gain equivalent protection to [Section 3.4.1](#), a server MUST use the Block2 option in conjunction with the ETag option ([\[RFC7252\]](#), [Section 5.10.6](#)), and MUST NOT use the same ETag value for different representations of a resource.

5. Token Processing

As described in [Section 1.3](#), the client must be able to verify that a response corresponds to a particular request. This section updates the CoAP Token processing requirements for clients. The Token processing for servers is not updated. Token processing in [Section 5.3.1 of \[RFC7252\]](#) is updated by adding the following text:

When CoAP is used with a security protocol not providing bindings between requests and responses, the tokens have cryptographic importance. The client MUST make sure that tokens are not used in a way so that responses risk being associated with the wrong request. The easiest way to accomplish this is to implement the Token (or part of the Token) as a sequence number starting at zero for each new or rekeyed secure connection, this approach SHOULD be followed. To avoid collisions the sequence number can be encoded with a fixed length or with some length-value encoding.

6. Security Considerations

The availability of a secure pseudorandom number generator and truly random seeds are essential for the security of the Echo option. If no true random number generator is available, a truly random seed must be provided from an external source.

A single active Echo value with 64 (pseudo-)random bits gives the same theoretical security level against forgeries as a 64-bit MAC (as used in e.g. AES_128_CCM_8). In practice, forgery of an Echo option value is much harder as an attacker must also forge the MAC in the security protocol. The Echo option value MUST contain 32 (pseudo-)random bits that are not predictable for any other party than the server, and SHOULD contain 64 (pseudo-)random bits. A

server MAY use different security levels for different uses cases (client aliveness, request freshness, state synchronization, network address reachability, etc.).

The security provided by the Echo and Request-Tag options depends on the security protocol used. CoAP and HTTP proxies require (D)TLS to be terminated at the proxies. The proxies are therefore able to manipulate, inject, delete, or reorder options or packets. The security claims in such architectures only hold under the assumption that all intermediaries are fully trusted and have not been compromised.

Servers SHOULD use a monotonic clock to generate timestamps and compute round-trip times. Use of non-monotonic clocks is not secure as the server will accept expired Echo option values if the clock is moved backward. The server will also reject fresh Echo option values if the clock is moved forward. Non-monotonic clocks MAY be used as long as they have deviations that are acceptable given the freshness requirements. If the deviations from a monotonic clock are known, it may be possible to adjust the threshold accordingly.

Servers SHOULD NOT use wall clock time for timestamps, as wall clock time have large deviations from a monotonic clock. Furthermore, an attacker may be able to affect the server's wall clock time in various ways such as setting up a fake NTP server or broadcasting false time signals to radio-controlled clocks.

Servers MAY use the time since reboot measured in some unit of time. Servers MAY reset the timer at certain times and MAY generate a random offset applied to all timestamps. When resetting the timer, the server MUST reject all Echo values that was created before the reset.

Servers that use the List of Cached Random Values and Timestamps method described in [Appendix A](#) may be vulnerable to resource exhaustion attacks. One way to minimize state is to use the Integrity Protected Timestamp method described in [Appendix A](#).

7. Privacy Considerations

Implementations SHOULD NOT put any privacy sensitive information in the Echo or Request-Tag option values. Unencrypted timestamps MAY reveal information about the server such as location or time since reboot. The use of wall clock time is not allowed (see [Section 6](#)) and there also privacy reasons, e.g. it may reveal that the server will accept expired certificates. Timestamps MAY be used if Echo is encrypted between the client and the server, e.g. in the case of DTLS without proxies or when using OSCORE with an Inner Echo option.

8. IANA Considerations

This document adds the following option numbers to the "CoAP Option Numbers" registry defined by [RFC7252]:

Number	Name	Reference
TBD1	Echo	[[this document]]
TBD2	Request-Tag	[[this document]]

Figure 4: CoAP Option Numbers

9. References

9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", [RFC 7252](#), DOI 10.17487/RFC7252, June 2014, <<https://www.rfc-editor.org/info/rfc7252>>.
- [RFC7959] Bormann, C. and Z. Shelby, Ed., "Block-Wise Transfers in the Constrained Application Protocol (CoAP)", [RFC 7959](#), DOI 10.17487/RFC7959, August 2016, <<https://www.rfc-editor.org/info/rfc7959>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

9.2. Informative References

- [I-D.hartke-core-stateless] Hartke, K., "Extended Tokens and Stateless Clients in the Constrained Application Protocol (CoAP)", [draft-hartke-core-stateless-02](#) (work in progress), October 2018.

[I-D.ietf-core-object-security]

Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", [draft-ietf-core-object-security-16](#) (work in progress), March 2019.

[I-D.ietf-core-oscore-groupcomm]

Tiloca, M., Selander, G., Palombini, F., and J. Park, "Group OSCORE - Secure Group Communication for CoAP", [draft-ietf-core-oscore-groupcomm-04](#) (work in progress), March 2019.

[I-D.mattsson-core-coap-actuators]

Mattsson, J., Fornehed, J., Selander, G., Palombini, F., and C. Amsuess, "Controlling Actuators with CoAP", [draft-mattsson-core-coap-actuators-06](#) (work in progress), September 2018.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", [RFC 6347](#), DOI 10.17487/RFC6347, January 2012, <<https://www.rfc-editor.org/info/rfc6347>>.

[RFC7390] Rahman, A., Ed. and E. Dijk, Ed., "Group Communication for the Constrained Application Protocol (CoAP)", [RFC 7390](#), DOI 10.17487/RFC7390, October 2014, <<https://www.rfc-editor.org/info/rfc7390>>.

[RFC7641] Hartke, K., "Observing Resources in the Constrained Application Protocol (CoAP)", [RFC 7641](#), DOI 10.17487/RFC7641, September 2015, <<https://www.rfc-editor.org/info/rfc7641>>.

[RFC8323] Bormann, C., Lemay, S., Tschofenig, H., Hartke, K., Silverajan, B., and B. Raymor, Ed., "CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets", [RFC 8323](#), DOI 10.17487/RFC8323, February 2018, <<https://www.rfc-editor.org/info/rfc8323>>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", [RFC 8446](#), DOI 10.17487/RFC8446, August 2018, <<https://www.rfc-editor.org/info/rfc8446>>.

[Appendix A](#). Methods for Generating Echo Option Values

The content and structure of the Echo option value are implementation specific and determined by the server. Two simple mechanisms are outlined in this section, the first is RECOMMENDED in general, and

the second is RECOMMENDED in case the Echo option is encrypted between the client and the server.

Different mechanisms have different tradeoffs between the size of the Echo option value, the amount of server state, the amount of computation, and the security properties offered. A server MAY use different methods and security levels for different uses cases (client aliveness, request freshness, state synchronization, network address reachability, etc.).

1. List of Cached Random Values and Timestamps. The Echo option value is a (pseudo-)random byte string. The server caches a list containing the random byte strings and their transmission times. Assuming 72-bit random values and 32-bit timestamps, the size of the Echo option value is 9 bytes and the amount of server state is $13n$ bytes, where n is the number of active Echo Option values. The security against forged echo values is given by $s = \text{bit length of } r - \log_2(n)$. The length of r and the maximum allowed n should be set so that the security level is harmonized with other parts of the deployment, e.g., $s \geq 64$. If the server loses time continuity, e.g. due to reboot, the entries in the old list MUST be deleted.

Echo option value: random value r
 Server State: random value r , timestamp t_0

2. Integrity Protected Timestamp. The Echo option value is an integrity protected timestamp. The timestamp can have different resolution and range. A 32-bit timestamp can e.g. give a resolution of 1 second with a range of 136 years. The (pseudo-)random secret key is generated by the server and not shared with any other party. The use of truncated HMAC-SHA-256 is RECOMMENDED. With a 32-bit timestamp and a 64-bit MAC, the size of the Echo option value is 12 bytes and the Server state is small and constant. The security against forged echo values is given by the MAC length. If the server loses time continuity, e.g. due to reboot, the old key MUST be deleted and replaced by a new random secret key. Note that the privacy considerations in [Section 7](#) may apply to the timestamp. A server MAY want to encrypt its timestamps, and, depending on the choice of encryption algorithms, this may require a nonce to be included in the Echo option value.

Echo option value: timestamp t_0 , $\text{MAC}(k, t_0)$
 Server State: secret key k

Other mechanisms complying with the security and privacy considerations may be used. The use of encrypted timestamps in the Echo option typically requires an IV to be included in the Echo option value, which adds overhead and makes the specification of such

a mechanism slightly more complicated than the two mechanisms specified here.

[Appendix B](#). Request-Tag Message Size Impact

In absence of concurrent operations, the Request-Tag mechanism for body integrity ([Section 3.4.1](#)) incurs no overhead if no messages are lost (more precisely: in OSCORE, if no operations are aborted due to repeated transmission failure; in DTLS, if no packages are lost), or when blockwise request operations happen rarely (in OSCORE, if there is always only one request blockwise operation in the replay window).

In those situations, no message has any Request-Tag option set, and that can be recycled indefinitely.

When the absence of a Request-Tag option can not be recycled any more within a security context, the messages with a present but empty Request-Tag option can be used (1 Byte overhead), and when that is used-up, 256 values from one byte long options (2 Bytes overhead) are available.

In situations where those overheads are unacceptable (e.g. because the payloads are known to be at a fragmentation threshold), the absent Request-Tag value can be made usable again:

- o In DTLS, a new session can be established.
- o In OSCORE, the sequence number can be artificially increased so that all lost messages are outside of the replay window by the time the first request of the new operation gets processed, and all earlier operations can therefore be regarded as concluded.

[Appendix C](#). Change Log

[The editor is asked to remove this section before publication.]

- o Changes since [draft-ietf-core-echo-request-tag-03](#):
 - * Mention token processing changes in title
 - * Abstract reworded
 - * Clarify updates to token processing
 - * Describe security levels from Echo length
 - * Allow non-monotonic clocks under certain conditions for freshness

- * Simplify freshness expressions
- * Describe when a Request-Tag can be set
- * Add note on application-level freshness mechanisms
- * Minor editorial changes
- o Changes since [draft-ietf-core-echo-request-tag-02](#):
 - * Define "freshness"
 - * Note limitations of "aliveness"
 - * Clarify proxy and OSCORE handling in presence of "echo"
 - * Clarify when Echo values may be reused
 - * Update security considerations
 - * Various minor clarifications
 - * Minor editorial changes
- o Major changes since [draft-ietf-core-echo-request-tag-01](#):
 - * Follow-up changes after the "relying on blockwise" change in -01:
 - + Simplify the description of Request-Tag and matchability
 - + Do not update [RFC7959](#) any more
 - * Make Request-Tag repeatable.
 - * Add rationale on not relying purely on sequence numbers.
- o Major changes since [draft-ietf-core-echo-request-tag-00](#):
 - * Reworded the Echo section.
 - * Added rules for Token processing.
 - * Added security considerations.
 - * Added actual IANA section.

- * Made Request-Tag optional and safe-to-forward, relying on blockwise to treat it as part of the cache-key
- * Dropped use case about OSCORE outer-blockwise (the case went away when its Partial IV was moved into the Object-Security option)
- o Major changes since [draft-amsuess-core-repeat-request-tag-00](#):
 - * The option used for establishing freshness was renamed from "Repeat" to "Echo" to reduce confusion about repeatable options.
 - * The response code that goes with Echo was changed from 4.03 to 4.01 because the client needs to provide better credentials.
 - * The interaction between the new option and (cross) proxies is now covered.
 - * Two messages being "Request-Tag matchable" was introduced to replace the older concept of having a request tag value with its slightly awkward equivalence definition.

Acknowledgments

The authors want to thank Jim Schaad and Carsten Bormann for providing valuable input to the draft.

Authors' Addresses

Christian Amsuess

Email: christian@amsuess.com

John Mattsson
Ericsson AB

Email: john.mattsson@ericsson.com

Goeran Selander
Ericsson AB

Email: goran.selander@ericsson.com

