

Expect-CT
draft-stark-expect-ct-00

Abstract

This document defines a new HTTP header, named Expect-CT, that allows web host operators to instruct user agents to expect valid Signed Certificate Timestamps (SCTs) to be served on connections to these hosts. When configured in enforcement mode, user agents (UAs) will remember that hosts expect SCTs and will refuse connections that do not conform to the UA's Certificate Transparency policy. When configured in report-only mode, UAs will report the lack of valid SCTs to a URI configured by the host, but will allow the connection. By turning on Expect-CT, web host operators can discover misconfigurations in their Certificate Transparency deployments and ensure that misissued certificates accepted by UAs are discoverable in Certificate Transparency logs.

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 May 3, 2017.

Copyright Notice

Copyright (c) 2016 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](#) [2](#)
- [1.1. Requirements Language](#) [3](#)
- [2. Server and Client Behavior](#) [3](#)
- [2.1. Response Header Field Syntax](#) [3](#)
- [2.1.1. The report-uri Directive](#) [4](#)
- [2.1.2. The enforce Directive](#) [5](#)
- [2.1.3. The max-age Directive](#) [5](#)
- [2.2. Server Processing Model](#) [6](#)
- [2.2.1. HTTP-over-Secure-Transport Request Type](#) [6](#)
- [2.2.2. HTTP Request Type](#) [6](#)
- [2.3. User Agent Processing Model](#) [6](#)
- [2.3.1. Expect-CT Header Field Processing](#) [7](#)
- [2.3.2. Noting an Expect-CT Host - Storage Model](#) [7](#)
- [2.3.3. HTTP-Equiv <meta> Element Attribute](#) [8](#)
- [2.4. Noting Expect-CT](#) [9](#)
- [2.5. Evaluating Expect-CT Connections for CT Compliance](#) [9](#)
- [3. Reporting Expect-CT Failure](#) [10](#)
- [3.1. Generating a violation report](#) [10](#)
- [3.2. Sending a violation report](#) [12](#)
- [4. Security Considerations](#) [12](#)
- [4.1. Maximum max-age](#) [12](#)
- [5. Privacy Considerations](#) [12](#)
- [6. IANA Considerations](#) [12](#)
- [7. Usability Considerations](#) [12](#)
- [8. References](#) [12](#)
- [8.1. Normative References](#) [12](#)
- [8.2. URIs](#) [14](#)
- Author's Address [14](#)

1. Introduction

This document defines a new HTTP header that enables UAs to identify web hosts that expect the presence of Signed Certificate Timestamps (SCTs) [[RFC6962](#)] in future Transport Layer Security (TLS) [[RFC5246](#)] connections.

Web hosts that serve the Expect-CT HTTP header are noted by the UA as Expect-CT hosts. The UA evaluates each connection to an Expect-CT

Stark

Expires May 3, 2017

[Page 2]

host for compliance with the UA's Certificate Transparency (CT) policy. If the connection violates the CT policy, the UA sends a report to a URI configured by the Expect-CT host and/or fails the connection, depending on the configuration that the Expect-CT host has chosen.

If misconfigured, Expect-CT can cause unwanted connection failures (for example, if a host deploys Expect-CT but then switches to a legitimate certificate that is not logged in Certificate Transparency logs, or if a web host operator believes their certificate to conform to all UAs' CT policies but is mistaken). Web host operators are advised to deploy Expect-CT with caution, by using the reporting feature and gradually increasing the interval for the UA remembers the host as an Expect-CT host. These precautions can help web host operators gain confidence that their Expect-CT deployment is not causing unwanted connection failures.

Expect-CT is a trust-on-first-use (TOFU) mechanism. The first time a UA connects to a host, it lacks the information necessary to require SCTs for the connection. Thus, the UA will not be able to detect and thwart an attack on the UA's first connection to the host. Still, Expect-CT provides value by allowing UAs to detect the use of unlogged certificates after the initial communication.

1.1. 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 [RFC 2119](#) [[RFC2119](#)].

2. Server and Client Behavior

2.1. Response Header Field Syntax

The "Expect-CT" header field is a new response header defined in this specification. It is used by a server to indicate that UAs should evaluate connections to the host emitting the header for CT compliance ([Section 2.5](#)).

Figure 1 describes the syntax (Augmented Backus-Naur Form) of the header field, using the grammar defined in [RFC 5234](#) [[RFC5234](#)] and the rules defined in [Section 3.2 of RFC 7230](#) [[RFC7230](#)].

Stark

Expires May 3, 2017

[Page 3]

```
Expect-CT-Directives = directive *( OWS ";" OWS directive )
directive              = directive-name [ "=" directive-value ]
directive-name         = token
directive-value        = token / quoted-string
```

Figure 1: Syntax of the Expect-CT header field

Optional white space ("OWS") is used as defined in [Section 3.2.3 of RFC 7230](#) [RFC7230]. "token" and "quoted-string" are used as defined in [Section 3.2.6 of RFC 7230](#) [RFC7230].

The directives defined in this specification are described below. The overall requirements for directives are:

1. The order of appearance of directives is not significant.
2. A given directive MUST NOT appear more than once in a given header field. Directives are either optional or required, as stipulated in their definitions.
3. Directive names are case insensitive.
4. UAs MUST ignore any header fields containing directives, or other header field value data, that do not conform to the syntax defined in this specification. In particular, UAs must not attempt to fix malformed header fields.
5. If a header field contains any directive(s) the UA does not recognize, the UA MUST ignore those directives.
6. If the Expect-CT header field otherwise satisfies the above requirements (1 through 5), the UA MUST process the directives it recognizes.

[2.1.1](#). The report-uri Directive

The OPTIONAL "report-uri" directive indicates the URI to which the UA SHOULD report Expect-CT failures ([Section 2.5](#)). The UA POSTs the reports to the given URI as described in [Section 3](#).

The "report-uri" directive is REQUIRED to have a directive value, for which the syntax is defined in Figure 2.

```
report-uri-value = absolute-URI
```

Figure 2: Syntax of the report-uri directive value

"absolute-URI" is defined in [Section 4.3 of RFC 3986](#) [RFC3986].

Stark

Expires May 3, 2017

[Page 4]

Hosts may set "report-uri"s that use HTTP or HTTPS. If the scheme in the "report-uri" is one that uses TLS (e.g., HTTPS), UAs MUST check Expect-CT compliance when the host in the "report-uri" is an Expect-CT host; similarly, UAs MUST apply HSTS if the host in the "report-uri" is a Known HSTS Host.

Note that the report-uri need not necessarily be in the same Internet domain or web origin as the host being reported about.

UAs SHOULD make their best effort to report Expect-CT failures to the "report-uri", but they may fail to report in exceptional conditions. For example, if connecting the "report-uri" itself incurs an Expect-CT failure or other certificate validation failure, the UA MUST cancel the connection. Similarly, if Expect-CT Host A sets a "report-uri" referring to Expect-CT Host B, and if B sets a "report-uri" referring to A, and if both hosts fail to comply to the UA's CT policy, the UA SHOULD detect and break the loop by failing to send reports to and about those hosts.

UAs SHOULD limit the rate at which they send reports. For example, it is unnecessary to send the same report to the same "report-uri" more than once.

2.1.2. The enforce Directive

The OPTIONAL "enforce" directive is a valueless directive that, if present (i.e., it is "asserted"), signals to the UA that compliance to the CT policy should be enforced (rather than report-only) and that the UA should refuse future connections that violate its CT policy.

2.1.3. The max-age Directive

The "max-age" directive specifies the number of seconds after the reception of the Expect-CT header field during which the UA SHOULD regard the host from whom the message was received as an Expect-CT host.

The "max-age" directive is REQUIRED to be present within an "Expect-CT" header field if and only if the "enforce" directive is present. The "max-age" directive is meaningless if no "enforce" directive is present (i.e., if the Expect-CT policy is report-only). UAs MUST ignore the "max-age" directive if the "enforce" directive is not present and not cache the header.

The "max-age" directive is REQUIRED to have a directive value, for which the syntax (after quoted-string unescaping, if necessary) is defined in Figure 3.


```
max-age-value = delta-seconds
delta-seconds = 1*DIGIT
```

Figure 3: Syntax of the max-age directive value

"delta-seconds" is used as defined in [Section 1.2.1 of RFC 7234 \[RFC7234\]](#).

2.2. Server Processing Model

This section describes the processing model that Expect-CT hosts implement. The model has 2 parts: (1) the processing rules for HTTP request messages received over a secure transport (e.g., authenticated, non-anonymous TLS); and (2) the processing rules for HTTP request messages received over non-secure transports, such as TCP.

2.2.1. HTTP-over-Secure-Transport Request Type

When replying to an HTTP request that was conveyed over a secure transport, an Expect-CT host SHOULD include in its response exactly one Expect-CT header field. The header field MUST satisfy the grammar specified in [Section 2.1](#).

Establishing a given host as an Expect-CT host, in the context of a given UA, is accomplished as follows:

1. Over the HTTP protocol running over secure transport, by correctly returning (per this specification) at least one valid Expect-CT header field to the UA.
2. Through other mechanisms, such as a client-side preloaded Expect-CT host list.

2.2.2. HTTP Request Type

Expect-CT hosts SHOULD NOT include the Expect-CT header field in HTTP responses conveyed over non-secure transport. UAs MUST ignore any Expect-CT header received in an HTTP response conveyed over non-secure transport.

2.3. User Agent Processing Model

The UA processing model relies on parsing domain names. Note that internationalized domain names SHALL be canonicalized according to the scheme in [Section 10 of \[RFC6797\]](#).

Stark

Expires May 3, 2017

[Page 6]

2.3.1. Expect-CT Header Field Processing

If the UA receives, over a secure transport, an HTTP response that includes an Expect-CT header field conforming to the grammar specified in [Section 2.1](#), the UA MUST evaluate the connection on which the header was received for compliance with the UA's CT policy, and then process the Expect-CT header field as follows.

If the header field includes a "report-uri" directive, and the connection does not comply with the UA's CT policy, then the UA MUST send a report to the specified "report-uri" as specified in [Section 3](#).

If the header field contains the "enforce" directive and the connection complies with the UA's CT policy, then the UA MUST either:

- o Note the host as an Expect-CT host if it is not already so noted (see [Section 2.4](#)), or
- o Update the UA's cached information for the Expect-CT host if the "max-age" or "report-uri" header field value directives convey information different from that already maintained by the UA. If the "max-age" directive has a value of 0, the UA MUST remove its cached Expect-CT information if the host was previously noted as an Expect-CT host, and MUST NOT note this host as an Expect-CT host if it is not already noted.

If the header field contains the "enforce" directive and the connection does not comply with the UA's CT policy, then the UA MUST NOT note this host as an Expect-CT host.

If a UA receives more than one Expect-CT header field in an HTTP response message over secure transport, then the UA MUST process only the first Expect-CT header field.

The UA MUST ignore any Expect-CT header field not conforming to the grammar specified in [Section 2.1](#).

2.3.2. Noting an Expect-CT Host - Storage Model

The "effective Expect-CT date" of an Expect-CT host is the time that the UA observed a valid Expect-CT header for the host. The "effective expiration date" of a known Expect-CT host is the effective Expect-CT date plus the max-age. An Expect-CT host is "expired" if the effective expiration date refers to a date in the past. The UA MUST ignore any expired Expect-CT hosts in its cache.

Stark

Expires May 3, 2017

[Page 7]

Expect-CT hosts are identified only by domain names, and never IP addresses. If the substring matching the host production from the Request-URI (of the message to which the host responded) syntactically matches the IP-literal or IPv4address productions from [Section 3.2.2 of \[RFC3986\]](#), then the UA MUST NOT note this host as an Expect-CT host.

Otherwise, if the substring does not congruently match an existing Expect-CT host's domain name, per the matching procedure specified in [Section 8.2 of \[RFC6797\]](#), then the UA MUST add this host to the Expect-CT host cache. The UA caches:

- o the Expect-CT host's domain name,
- o the effective expiration date, or enough information to calculate it (the effective Expect-CT date and the value of the "max-age" directive),
- o the value of the "report-uri" directive, if present.

If any other metadata from optional or future Expect-CT header directives are present in the Expect-CT header, and the UA understands them, the UA MAY note them as well.

UAs MAY set an upper limit on the value of max-age, so that UAs that have noted erroneous Expect-CT hosts (whether by accident or due to attack) have some chance of recovering over time. If the server sets a max-age greater than the UA's upper limit, the UA MAY behave as if the server set the max-age to the UA's upper limit. For example, if the UA caps max-age at 5,184,000 seconds (60 days), and a Pinned Host sets a max-age directive of 90 days in its Expect-CT header, the UA MAY behave as if the max-age were effectively 60 days. (One way to achieve this behavior is for the UA to simply store a value of 60 days instead of the 90-day value provided by the Expect-CT host.)

The UA MUST NOT cache information from an Expect-CT header that does not include the "enforce" directive. (Report-only headers are useful only at the time of receipt and processing.)

2.3.3. HTTP-Equiv <meta> Element Attribute

UAs MUST NOT heed "http-equiv="Expect-CT"" attribute settings on "<meta>" elements [[W3C.REC-html401-19991224](#)] in received content.

2.4. Noting Expect-CT

Upon receipt of the Expect-CT response header field containing an "enforce" directive, the UA notes the host as an Expect-CT host, storing the host's domain name and its associated Expect-CT directives in non-volatile storage. The domain name and associated Expect-CT directives are collectively known as "Expect-CT metadata".

The UA MUST note a host as an Expect-CT host if and only if it received the Expect-CT response header field over an error-free TLS connection, including the validation added in [Section 2.5](#), that included the "enforce" directive.

To note a host as an Expect-CT host, the UA MUST set its Expect-CT metadata to the effective expiration date and report-uri (if any) given in the most recently received valid Expect-CT header.

For forward compatibility, the UA MUST ignore any unrecognized Expect-CT header directives, while still processing those directives it does recognize. [Section 2.1](#) specifies the directives "enforce", "max-age", and "report-uri", but future specifications and implementations might use additional directives.

2.5. Evaluating Expect-CT Connections for CT Compliance

When a UA connects to an Expect-CT host using a TLS connection, if the TLS connection has errors, the UA MUST terminate the connection without allowing the user to proceed anyway. (This behavior is the same as that required by [\[RFC6797\]](#).)

If the connection has no errors, then the UA will apply an additional correctness check: compliance with a CT policy. A UA should evaluate compliance with its CT policy whenever connecting to an Expect-CT host, as soon as possible. It is acceptable to skip this CT compliance check for some hosts according to local policy. For example, a UA may disable CT compliance checks for hosts whose validated certificate chain terminates at a user-defined trust anchor, rather than a trust anchor built-in to the UA (or underlying platform).

A UA that has previously noted a host as an Expect-CT host MUST evaluate evaluate CT compliance when setting up the TLS session, before beginning an HTTP conversation over the TLS channel.

If the UA does not evaluate CT compliance, e.g. because the user has elected to disable it, or because a presented certificate chain chains up to a user-defined trust anchor, UAs SHOULD NOT send Expect-CT reports.

Stark

Expires May 3, 2017

[Page 9]

3. Reporting Expect-CT Failure

When the UA receives an Expect-CT header with a "report-uri" directive that does not comply with the UA's CT policy, or when the UA connects to a noted Expect-CT host that does not comply with the CT policy, the UA SHOULD report Expect-CT failures to the configured "report-uri".

3.1. Generating a violation report

To generate a violation report object, the UA constructs a JSON message of the following form:

```
{
  "date-time": date-time,
  "hostname": hostname,
  "port": port,
  "effective-expiration-date": expiration-date,
  "served-certificate-chain": [ (MUST be in the order served)
    pem1, ... pemN
  ],
  "validated-certificate-chain":
    pem1, ... pemN
  ],
  "scts": [
    sct1, ... sctN
  ]
}
```

Figure 4: JSON format of a violation report object

Whitespace outside of quoted strings is not significant. The key/value pairs may appear in any order, but each MUST appear only once.

The "date-time" indicates the time the UA observed the CT compliance failure. It is provided as a string formatted according to [Section 5.6](#), "Internet Date/Time Format", of [RFC 3339](#) [[RFC3339](#)].

The "hostname" is the hostname to which the UA made the original request that failed the CT compliance check. It is provided as a string.

The "port" is the port to which the UA made the original request that failed the CT compliance check. It is provided as an integer.

The "effective-expiration-date" is the Effective Expiration Date for the Expect-CT host that failed the CT compliance check. It is

provided as a string formatted according to [Section 5.6](#), "Internet Date/Time Format", of [RFC 3339](#) [[RFC3339](#)].

The "served-certificate-chain" is the certificate chain, as served by the Expect-CT host during TLS session setup. It is provided as an array of strings, which MUST appear in the order that the certificates were served; each string "pem1", ... "pemN" is the Privacy-Enhanced Mail (PEM) representation of each X.509 certificate as described in [RFC 7468](#) [[RFC7468](#)].

The "validated-certificate-chain" is the certificate chain, as constructed by the UA during certificate chain verification. (This may differ from the "served-certificate-chain".) It is provided as an array of strings, which MUST appear in the order matching the chain that the UA validated; each string "pem1", ... "pemN" is the Privacy-Enhanced Mail (PEM) representation of each X.509 certificate as described in [RFC 7468](#) [[RFC7468](#)].

The "scts" are JSON messages representing the SCTs (if any) that the UA received for the Expect-CT host and their validation statuses. The format of "sct1", ... "sctN" is shown in Figure 5. The SCTs may appear in any order.

```
{
  "sct": sct,
  "status": status,
  "source": source
}
```

Figure 5: JSON format of an SCT object

The "sct" is as defined in [Section 4.1 of RFC 6962](#) [[RFC6962](#)].

The "status" is a string that the UA MUST set to one of the following values: "unknown" (indicating that the UA does not have or does not trust the public key of the log from which the SCT was issued), "valid" (indicating that the UA successfully validated the SCT as described in [Section 5.2 of \[RFC6962\]](#)), or "invalid" (indicating that the SCT validation failed because of, e.g., a bad signature).

The "source" is a string that indicates from where the UA obtained the SCT, as defined in [Section 3.3 of RFC 6962](#) [[RFC6962](#)]. The UA MUST set "source" to one of the following values: "tls-extension", "ocsp", or "embedded".

3.2. Sending a violation report

When an Expect-CT header field contains the "report-uri" directive, and the connection does not comply with the UA's CT policy, the UA SHOULD report the failure as follows:

1. Prepare a JSON object "report object" with the single key "expect-ct-report", whose value is the result of generating a violation report object as described in Figure 4.
2. Let "report body" be the JSON stringification of "report object".
3. Let "report-uri" be the value of the "report-uri" directive in the Expect-CT header field.
4. Queue a task [1] to fetch [2] "report-uri", with the synchronous flag not set, using HTTP method "POST", with a "Content-Type" header field of "application/expect-ct-report", and an entity body consisting of "report body".

4. Security Considerations

4.1. Maximum max-age

1 year?

5. Privacy Considerations

6. IANA Considerations

7. Usability Considerations

When the UA detects an Expect-CT host in violation of the UA's CT policy, users will experience denials of service. It is advisable for UAs to explain the reason why.

It is advisable that UAs have a way for users to clear noted Expect-CT hosts and that UAs allow users to query noted Expect-CT hosts.

8. References

8.1. 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, <<http://www.rfc-editor.org/info/rfc2119>>.

- [RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", [RFC 3339](#), DOI 10.17487/RFC3339, July 2002, <<http://www.rfc-editor.org/info/rfc3339>>.
- [RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, [RFC 3986](#), DOI 10.17487/RFC3986, January 2005, <<http://www.rfc-editor.org/info/rfc3986>>.
- [RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, [RFC 5234](#), DOI 10.17487/RFC5234, January 2008, <<http://www.rfc-editor.org/info/rfc5234>>.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), DOI 10.17487/RFC5246, August 2008, <<http://www.rfc-editor.org/info/rfc5246>>.
- [RFC6797] Hodges, J., Jackson, C., and A. Barth, "HTTP Strict Transport Security (HSTS)", [RFC 6797](#), DOI 10.17487/RFC6797, November 2012, <<http://www.rfc-editor.org/info/rfc6797>>.
- [RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", [RFC 6962](#), DOI 10.17487/RFC6962, June 2013, <<http://www.rfc-editor.org/info/rfc6962>>.
- [RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", [RFC 7230](#), DOI 10.17487/RFC7230, June 2014, <<http://www.rfc-editor.org/info/rfc7230>>.
- [RFC7234] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Caching", [RFC 7234](#), DOI 10.17487/RFC7234, June 2014, <<http://www.rfc-editor.org/info/rfc7234>>.
- [RFC7468] Josefsson, S. and S. Leonard, "Textual Encodings of PKIX, PKCS, and CMS Structures", [RFC 7468](#), DOI 10.17487/RFC7468, April 2015, <<http://www.rfc-editor.org/info/rfc7468>>.
- [W3C.REC-html401-19991224] Raggett, D., Hors, A., and I. Jacobs, "HTML 4.01 Specification", World Wide Web Consortium Recommendation REC-html401-19991224, December 1999, <<http://www.w3.org/TR/1999/REC-html401-19991224>>.

8.2. URIs

[1] <https://html.spec.whatwg.org/#queue-a-task>

[2] <https://fetch.spec.whatwg.org/#fetching>

Author's Address

Emily Stark
Google

Email: estark@google.com