

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: November 21, 2016

M. Thomson  
Mozilla  
D. Gillmor  
ACLU  
B. Kaduk  
Unaffiliated  
May 20, 2016

Using Context Labels for Domain Separation of Cryptographic Objects  
draft-thomson-saag-context-labels-00

## Abstract

A single cryptographic key is sometimes relied upon to produce multiple cryptographic artifacts that each have different semantics. This produces a potential problem whereby artifacts with different intended uses can be confused. The addition of context labels removes this problem.

## 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 November 21, 2016.

## 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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">1.1.</a>	Notational Conventions . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Existing Functions with Context Labels . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Generic Signature or MAC Function with Context . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Recommendations for Context Labels . . . . .	<a href="#">4</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">4</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">4</a>
<a href="#">7.</a>	References . . . . .	<a href="#">4</a>
<a href="#">7.1.</a>	Normative References . . . . .	<a href="#">5</a>
<a href="#">7.2.</a>	Informative References . . . . .	<a href="#">5</a>
<a href="#">Appendix A.</a>	Existing Protocols with Context Labels . . . . .	<a href="#">6</a>
<a href="#">Appendix B.</a>	Existing Protocols without Context Labels . . . . .	<a href="#">10</a>
<a href="#">Appendix C.</a>	Acknowledgments . . . . .	<a href="#">10</a>
	Authors' Addresses . . . . .	<a href="#">10</a>

## [1.](#) Introduction

The same cryptographic primitive can be used in a range of different contexts. These uses are often developed in isolation, which leads to the potential for data structures that are used in one protocol having plausible interpretations in other protocols. This gives an opportunity for cross-protocol attacks, wherein a well-behaved participant in one protocol can be coerced into creating a cryptographic object that, when interpreted by a different protocol, introduces a vulnerability.

Reuse of the same key in multiple contexts is strongly discouraged. However, in some cases, use of the same key might be unavoidable. For example, the same key might need to be used in multiple versions of the same protocol, or a protocol might define multiple uses for a particular type of key.

Including a unique protocol- and usage- specific context label as input to a cryptographic operation prevents objects created in one context from being mistakenly used in a different context.

This document describes a uniform approach for the inclusion of

context labels and a registry for unique labels. It covers the use of these labels in digital signatures, key derivation functions (KDFs), and message authentication codes (MACs).

Existing protocols might already include a unique context label. This document collects some of these existing labels into the context label registry.

### [1.1](#). Notational Conventions

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 [[RFC2119](#)].

## [2](#). Existing Functions with Context Labels

The following cryptographic primitives define an explicit argument for identifying a context:

- o Ed448 and Ed448ph [[I-D.irtf-cfrg-eddsa](#)] define a "context" argument.
- o HKDF [[RFC5869](#)] specifies an "info" argument to the HKDF-Expand function.

## [3](#). Generic Signature or MAC Function with Context

Many pre-existing signature and MAC schemes do not define an explicit context label. This document defines a new signature function that adds a context label to an existing function.

Given a signature function  $S$  that takes a key  $K$  and message  $M$  as a sequence of octets, a signature with context function  $Sc$  is defined. The signature with context function  $Sc$  takes three arguments,  $K$ ,  $M$ , and a context label  $C$  as a sequence of octets and is defined as:

$$Sc(K, M, C) = S(K, C || M)$$

That is, the signature is changed to accept a message that is the concatenation of the context label and the message.

This scheme MUST be used with:

- o RSA (both PKCS#1 and PSS) [[RFC3447](#)]
- o ECDSA [[X9.62](#)]
- o HMAC [[RFC2104](#)]
- o Ed25519 and Ed25519ph [[I-D.irtf-cfrg-eddsa](#)]

#### [4.](#) Recommendations for Context Labels

In order to avoid attacks that permit use of a cryptographic object for purposes other than intended, a context label C MUST NOT be a prefix of any other context label.

New specifications defining context labels SHOULD select context labels that end with a single zero-valued octet and do not contain any other zero-valued octets. Context labels SHOULD be at least 12 octets in length.

#### [5.](#) IANA Considerations

This document establishes a "Cryptographic Context Label" registry.

Entries in this registry contain the following fields:

Context Label: A sequence of octets between 1 and 255 octets in length, displayed as a hexadecimal string

String: An optional, informative ASCII representation of the context label

Specification: A reference to a specification describing the use of the context label

Context labels in this registry MUST NOT be a prefix of any other context label in the registry. For example, if 0x01ab00 is registered, then a registration for 0x01 or 0x01ab007c MUST be

rejected.

A context label that is 12 octets or more in length and contains exactly one zero-valued octet at the end can be registered on a First-Come, First-Served basis [[RFC5226](#)]. Context labels that do not meet these requirements require Expert Review [[RFC5226](#)].

The initial contents of this registry are included in [Appendix A](#).

## [6](#). Security Considerations

In general, it is best to limit any cryptographic material to being used for a single purpose.

## [7](#). References

Thomson, et al. Expires November 21, 2016 [Page 4]

---

Internet-Draft Context Labels May 2016

### [7.1](#). Normative References

- [I-D.irtf-cfrg-eddsa] Josefsson, S. and I. Liusvaara, "Edwards-curve Digital Signature Algorithm (EdDSA)", [draft-irtf-cfrg-eddsa-05](#) (work in progress), March 2016.
- [RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", [RFC 2104](#), DOI 10.17487/RFC2104, February 1997, <<http://www.rfc-editor.org/info/rfc2104>>.
- [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>>.
- [RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", [RFC 3447](#), DOI 10.17487/RFC3447, February 2003, <<http://www.rfc-editor.org/info/rfc3447>>.

- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 5226](#), DOI 10.17487/RFC5226, May 2008, <<http://www.rfc-editor.org/info/rfc5226>>.
- [RFC5869] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", [RFC 5869](#), DOI 10.17487/RFC5869, May 2010, <<http://www.rfc-editor.org/info/rfc5869>>.
- [X9.62] ANSI, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANSI X9.62 , 1998.

## [7.2.](#) Informative References

- [I-D.ietf-tls-tls13] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", [draft-ietf-tls-tls13-12](#) (work in progress), March 2016.
- [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>>.

## [Appendix A.](#) Existing Protocols with Context Labels

Context label	String	Specification
20 20 20 20 20 20 20 20	(64 spaces)TLS 1.3,	<a href="#">[I-D.ietf-tls-tls13]</a>
20 20 20 20 20 20 20 20	server	
20 20 20 20 20 20 20 20	CertificateVerify\0	
20 20 20 20 20 20 20 20		
20 20 20 20 20 20 20 20		
20 20 20 20 20 20 20 20		
20 20 20 20 20 20 20 20		
20 20 20 20 20 20 20 20		
20 54 4c 53 20 31 2e		

33 2c 20 73 65 72 76		
65 72 20 43 65 72 74		
69 66 69 63 61 74 65		
56 65 72 69 66 79 00		
20 20 20 20 20 20 20	(64 spaces)TLS 1.3,	<a href="#">[I-D.ietf-tls-tls13]</a>
20 20 20 20 20 20 20	client	
20 20 20 20 20 20 20	CertificateVerify\0	
20 20 20 20 20 20 20		
20 20 20 20 20 20 20		
20 20 20 20 20 20 20		
20 20 20 20 20 20 20		
20 20 20 20 20 20 20		
20 54 4c 53 20 31 2e		
33 2c 20 63 6c 69 65		
6e 74 20 43 65 72 74		
69 66 69 63 61 74 65		
56 65 72 69 66 79 00		
54 4c 53 20 31 2e 33	TLS 1.3, expanded	<a href="#">[I-D.ietf-tls-tls13]</a>
2c 20 65 78 70 61 6e	static secret	
64 65 64 20 73 74 61		
74 69 63 20 73 65 63		
72 65 74		
54 4c 53 20 31 2e 33	TLS 1.3, expanded	<a href="#">[I-D.ietf-tls-tls13]</a>
2c 20 65 78 70 61 6e	ephemeral secret	
64 65 64 20 65 70 68		
65 6d 65 72 61 6c 20		
73 65 63 72 65 74		
54 4c 53 20 31 2e 33	TLS 1.3, traffic	<a href="#">[I-D.ietf-tls-tls13]</a>

2c 20 74 72 61 66 66	secret	
69 63 20 73 65 63 72		
65 74		
54 4c 53 20 31 2e 33	TLS 1.3, resumption	<a href="#">[I-D.ietf-tls-tls13]</a>
2c 20 72 65 73 75 6d	master secret	
70 74 69 6f 6e 20 6d		
61 73 74 65 72 20 73		

65 63 72 65 74		
54 4c 53 20 31 2e 33 2c 20 65 78 70 6f 72 74 65 72 20 6d 61 73 74 65 72 20 73 65 63 72 65 74	TLS 1.3, exporter master secret	<a href="#">[I-D.ietf-tls-tls13]</a>
54 4c 53 20 31 2e 33 2c 20 65 61 72 6c 79 20 68 61 6e 64 73 68 61 6b 65 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 2c 20 63 6c 69 65 6e 74 20 77 72 69 74 65 20 6b 65 79	TLS 1.3, early handshake key expansion, client write key	<a href="#">[I-D.ietf-tls-tls13]</a>
54 4c 53 20 31 2e 33 2c 20 65 61 72 6c 79 20 68 61 6e 64 73 68 61 6b 65 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 2c 20 73 65 72 76 65 72 20 77 72 69 74 65 20 6b 65 79	TLS 1.3, early handshake key expansion, server write key	<a href="#">[I-D.ietf-tls-tls13]</a>
54 4c 53 20 31 2e 33 2c 20 65 61 72 6c 79 20 68 61 6e 64 73 68 61 6b 65 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 2c 20 63 6c 69 65 6e 74 20 77 72 69 74 65 20 69 76	TLS 1.3, early handshake key expansion, client write iv	<a href="#">[I-D.ietf-tls-tls13]</a>
54 4c 53 20 31 2e 33 2c 20 65 61 72 6c 79 20 68 61 6e 64 73 68 61 6b 65 20 6b 65 79 20 65 78 70 61 6e 73	TLS 1.3, early handshake key expansion, server write iv	<a href="#">[I-D.ietf-tls-tls13]</a>



72 76 65 72 20 77 72 69 74 65 20 69 76		
54 4c 53 20 31 2e 33 2c 20 65 61 72 6c 79 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 64 61 74 61 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 2c 20 63 6c 69 65 6e 74 20 77 72 69 74 65 20 6b 65 79	TLS 1.3, early application data key expansion, client write key	<a href="#">[I-D.ietf-tls-tls13]</a>
54 4c 53 20 31 2e 33 2c 20 65 61 72 6c 79 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 64 61 74 61 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 2c 20 73 65 72 76 65 72 20 77 72 69 74 65 20 6b 65 79	TLS 1.3, early application data key expansion, server write key	<a href="#">[I-D.ietf-tls-tls13]</a>
54 4c 53 20 31 2e 33 2c 20 65 61 72 6c 79 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 64 61 74 61 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 2c 20 63 6c 69 65 6e 74 20 77 72 69 74 65 20 69 76	TLS 1.3, early application data key expansion, client write iv	<a href="#">[I-D.ietf-tls-tls13]</a>
54 4c 53 20 31 2e 33 2c 20 65 61 72 6c 79 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 64 61 74 61 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 2c 20 73 65 72 76 65 72 20 77 72 69 74 65 20 69 76	TLS 1.3, early application data key expansion, server write iv	<a href="#">[I-D.ietf-tls-tls13]</a>
54 4c 53 20 31 2e 33 2c 20 68 61 6e 64 73 68 61 6b 65 20 6b 65 79 20 65 78 70 61 6e	TLS 1.3, handshake key expansion, client write key	<a href="#">[I-D.ietf-tls-tls13]</a>

73 69 6f 6e 2c 20 63 6c 69 65 6e 74 20 77 72 69 74 65 20 6b 65 79		
54 4c 53 20 31 2e 33 2c 20 68 61 6e 64 73 68 61 6b 65 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 2c 20 73 65 72 76 65 72 20 77 72 69 74 65 20 6b 65 79	TLS 1.3, handshake key expansion, server write key	<a href="#">[I-D.ietf-tls-tls13]</a>
54 4c 53 20 31 2e 33 2c 20 68 61 6e 64 73 68 61 6b 65 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 2c 20 63 6c 69 65 6e 74 20 77 72 69 74 65 20 69 76	TLS 1.3, handshake key expansion, client write iv	<a href="#">[I-D.ietf-tls-tls13]</a>
54 4c 53 20 31 2e 33 2c 20 68 61 6e 64 73 68 61 6b 65 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 2c 20 73 65 72 76 65 72 20 77 72 69 74 65 20 69 76	TLS 1.3, handshake key expansion, server write iv	<a href="#">[I-D.ietf-tls-tls13]</a>
54 4c 53 20 31 2e 33 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 64 61 74 61 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 2c 20 63 6c 69 65 6e 74 20 77 72 69 74 65 20 6b 65 79	TLS 1.3, application data key expansion, client write key	<a href="#">[I-D.ietf-tls-tls13]</a>
54 4c 53 20 31 2e 33 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 64 61 74 61 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 2c 20 73	TLS 1.3, application data key expansion, server write key	<a href="#">[I-D.ietf-tls-tls13]</a>

65 72 76 65 72 20 77		
72 69 74 65 20 6b 65		

79		
54 4c 53 20 31 2e 33	TLS 1.3,	<a href="#">[I-D.ietf-tls-tls13]</a>
2c 20 61 70 70 6c 69	application data	
63 61 74 69 6f 6e 20	key expansion,	
64 61 74 61 20 6b 65	client write iv	
79 20 65 78 70 61 6e		
73 69 6f 6e 2c 20 63		
6c 69 65 6e 74 20 77		
72 69 74 65 20 69 76		
54 4c 53 20 31 2e 33	TLS 1.3,	<a href="#">[I-D.ietf-tls-tls13]</a>
2c 20 61 70 70 6c 69	application data	
63 61 74 69 6f 6e 20	key expansion,	
64 61 74 61 20 6b 65	server write iv	
79 20 65 78 70 61 6e		
73 69 6f 6e 2c 20 73		
65 72 76 65 72 20 77		
72 69 74 65 20 69 76		
+-----+-----+-----+		

Note that in the above table, the following categories of entry do not conform with the guidance in [Section 4](#):

- o Labels for the TLS 1.3 HKDF input

### [Appendix B](#). Existing Protocols without Context Labels

TLS versions 1.2 [[RFC5246](#)] and earlier do not use context labels for signatures though the use of the pseudorandom function (PRF) uses version-agnostic labels.

### [Appendix C](#). Acknowledgments

This document originated from hallway discussions at IETF 95; thank you to those who helped spark the idea.

### Authors' Addresses

Martin Thomson  
Mozilla

Email: martin.thomson@gmail.com

Thomson, et al.

Expires November 21, 2016

[Page 10]

---

Internet-Draft

Context Labels

May 2016

Daniel Kahn Gillmor  
ACLU

Email: dkg@fifthhorseman.net

Benjamin Kaduk  
Unaffiliated

Email: kaduk@mit.edu

