

INTERNET-DRAFT  
Intended status: Proposed Standard

D. Eastlake  
Futurewei Technologies  
D. Zhang  
Huawei Technologies  
November 28, 2021

Expires: May 22, 2022

Simple Group Keying Protocol TRILL Use Profiles  
<[draft-ietf-trill-link-gk-profiles-08.txt](#)>

## Abstract

This document specifies use profiles for the application of the simple group keying protocol (SGKP) to multi-destination TRILL Extended RBridge Channel message security ([RFC 7978](#)) and TRILL over IP packet security ([draft-ietf-trill-over-ip](#)).

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Distribution of this document is unlimited. Comments should be sent to the authors or the TRILL working group mailing list: [trill@ietf.org](mailto:trill@ietf.org).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <https://www.ietf.org/1id-abstracts.html>. The list of Internet-Draft Shadow Directories can be accessed at <https://www.ietf.org/shadow.html>.

INTERNET-DRAFT

TRILL: Group Keying Profiles

November 2021

## Table of Contents

<a href="#">1. Introduction.....</a>	<a href="#">3</a>
<a href="#">1.1 Terminology and Acronyms.....</a>	<a href="#">3</a>
<a href="#">2. DTLS: Extended RBridge Channel Group Keyed Security.....</a>	<a href="#">5</a>
<a href="#">2.1 Transmission of Group Keying Messages.....</a>	<a href="#">5</a>
<a href="#">2.2 Transmission of Protected Multi-destination Data.....</a>	<a href="#">6</a>
<a href="#">3. TRILL Over IP Group Keyed Security.....</a>	<a href="#">7</a>
<a href="#">3.1 Transmission of Group Keying Messages.....</a>	<a href="#">7</a>
<a href="#">3.2 Transmission of Protected Multi-destination Data.....</a>	<a href="#">8</a>
<a href="#">4. Security Considerations.....</a>	<a href="#">9</a>
<a href="#">5. IANA Considerations.....</a>	<a href="#">10</a>
<a href="#">5.1 Group Keying RBridge Channel Protocol Numbers.....</a>	<a href="#">10</a>
<a href="#">5.2 Group Secured Extended RBridge Channel SType.....</a>	<a href="#">10</a>
<a href="#">Normative References.....</a>	<a href="#">11</a>
<a href="#">Informative References.....</a>	<a href="#">12</a>
<a href="#">Acknowledgements.....</a>	<a href="#">13</a>

## 1. Introduction

This document specifies use profiles for the application of the simple group keying protocol (SGKP) [[SGKP](#)] to the use of DTLS [[RFC6347](#)] formatted TRILL [[RFC6325](#)] [[RFC7780](#)] Extended RBridge Channel message security [[RFC7178](#)] [[RFC7978](#)] and to the use of IPsec formatted TRILL over IP [[TRILLoverIP](#)]. It is anticipated that there will be other uses for the group keying protocol.

### 1.1 Terminology and Acronyms

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

This document uses terminology and acronyms defined in [[RFC6325](#)] and [[RFC7178](#)]. Some of these are repeated below for convenience along with additional new terms and acronyms.

Data Label - VLAN or FGL.

DTLS - Datagram Transport Level Security [[RFC6347](#)].

FGL - Fine Grained Label [[RFC7172](#)].

GKd - A distinguished station in a group that is in charge of which group keying ([Section 2](#)) is in use [[SGKP](#)].

GKs - Stations in a group other than GKd ([Section 2](#)) [[SGKP](#)].

HKDF - Hash based Key Derivation Function [[RFC5869](#)].

IS-IS - Intermediate System to Intermediate System [[RFC7176](#)].

keying material - The set of a Key ID, a secret key, and a cypher suite.

PDU - Protocol Data Unit.

QoS - Quality of Service.

RBridge - An alternative term for a TRILL switch.

SHA - Secure Hash Algorithm [[RFC6234](#)].

TRILL - Transparent Interconnection of Lots of Links or Tunneled Routing in the Link Layer.

TRILL switch - A device that implements the TRILL protocol [[RFC6325](#)] [[RFC7780](#)], sometimes referred to as an RBridge.

## 2. DTLS: Extended RBridge Channel Group Keyed Security

This section specifies a profile of the simple group keying protocol (SGKP) specified in [\[SGKP\]](#). This profile provides shared secret keying to secure multi-destination Extended RBridge Channel messages [\[RFC7978\]](#) as described in Section 2.2.

For this SKGP use profile, a group is identified by TRILL Data Label (VLAN or FGL [\[RFC7172\]](#)) and consists of the data reachable [\[RFC7780\]](#) RBridges with interest in that Data Label. GKd is the RBridge in the group that, of those group members supporting the Group Keying Protocol, is the highest priority to be a TRILL distribution tree root as specified in [Section 4.5 of \[RFC6325\]](#). If not all members of the group support the Group Keying Protocol, then there are two cases of destinations for multi-destination Channel Tunnel RBridge Channel

messages:

- (1) If the sender and at least two other group members support the Group Keying Protocol, it SHOULD, for efficiency, send a secured multi-destination RBridge Channel message to cover the group and serially unicast to the group members not supporting the Group Keying Protocol.
- (2) In other cases the sender serially transmits the data to the group members using pairwise security.

## [2.1](#) Transmission of Group Keying Messages

Keying messages themselves are sent as unicast Extended RBridge Channel messages carrying a Group Keying protocol (see [Section 5.1](#)) RBridge Channel message. Such messages MUST use DTLS Pairwise or Composite (STypes 2 or 3) security [[RFC7978](#)].

The Group Keying profile for this Group Keying Use Type is as follows:

Priority of Group Keying messages for this SHOULD be 6 unless the network manager chooses to use a lower priority after determining that such lower priority group keying messages will yield acceptable performance. Priority 7 SHOULD NOT be used as it may cause interference with the establishment and maintenance of adjacency.

Use Type = 1

KeyID1 Length = 2, KeyID1 is an [[RFC5310](#)] key ID.

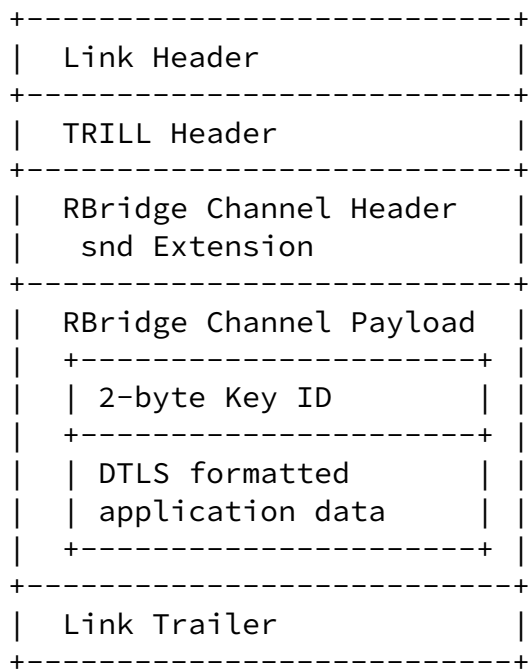
CypherSuiteLng = 2, CypherSuite is the cypher suite used in groupcast extended RBridge Channel data messages for the

corresponding KeyID2. This is a DTLS [[RFC6347](#)] cypher suite.

KeyID2 Length = 1, KeyID2 is the index under which a group key is set. Group keys are, in effect, indexed by this KeyID2 and the nickname of the GKd as used in the Ingress Nickname field of the TRILL Header of Group Keying messages.

## [2.2](#) Transmission of Protected Multi-destination Data

Protected Extended RBridge Channel [[RFC7978](#)] messages are multicast (M bit set to one in the TRILL Header) and set the SType field to a new value TBD2 for "Group Secured" (see [Section 5.2](#)). Since there could be multiple group keys distributed and enabled for use, data is formatted as two bytes of Key ID followed by data formatted as TLS 1.3 [[RFC8446](#)] application\_data using the cyphersuite and keying material stored under the Key ID. Such a message on the wire looks like the following:



### 3. TRILL Over IP Group Keyed Security

The SGKP usage profile specified in this section provides shared secret keying to secure TRILL over IP messages [[TRILLoverIP](#)]. The keys put in place by the group keying protocol are available for use as IPSEC keys.

For this use profile, a group is identified by an IP multicast address and consists of the R Bridges adjacent [[RFC7177](#)] to the sender reachable with that multicast address over a TRILL over IP link. GKd is the R Bridge in the group that, of those group members supporting the Group Keying Protocol, has the highest priority to be a TRILL distribution tree root as specified in [Section 4.5 of \[RFC6325\]](#). If not all members of the group support the Group Keying Protocol, then there are two cases for multi-destination TRILL over IP messages:

- (1) If the sender and at least two other group members support SGKP, it SHOULD, for efficiency, send a secured IPSEC message to cover the group and serially unicast to the group members not supporting the Group Keying Protocol.
- (2) In other cases the sender serially transmits the data to the group members using pairwise security.

#### 3.1 Transmission of Group Keying Messages

Keying messages themselves are sent as unicast Extended R Bridge Channel messages carrying a Group Keying protocol (see [Section 5.1](#)) R Bridge Channel message. Such messages MUST use DTLS Pairwise or Composite (STypes 2 or 3) security [[RFC7978](#)].

The Group Keying profile for this Group Keying Use Type is as follows:

Priority of Group Keying messages for this SHOULD be 6 unless the network manager chooses to use a lower priority after determining that such lower priority group keying messages will yield acceptable performance. Priority 7 SHOULD NOT be used as it may cause interference with the establishment and maintenance of adjacency.

Use Type = 2

KeyID1 Length = 2, KeyID1 is an [[RFC5310](#)] key ID.

CypherSuiteLng = variable, CypherSuite is an IKEv2 crypto algorithm "proposal" [[RFC7296](#)].

KeyID2 Length = 4, KeyID2 is the IPsec multicast SA. It is the



INTERNET-DRAFT

TRILL: Group Keying Profiles

November 2021

index under which a group key is set. Group keys are indexed by this KeyID2 and the nickname of the GKd as used in the Ingress Nickname field of the TRILL Header of Group Keying messages.

### [3.2](#) Transmission of Protected Multi-destination Data

Multi-destination TRILL over IP data packets are formatted as multicast IPsec ESP tunnel mode [\[RFC4303\]](#) packets. The key and crpto algorithms in use are indicated by the multicast SA.

#### [4](#). Security Considerations

See [[SGKP](#)] for Simple Group Keying Protocol security considerations.

See [[RFC7978](#)] for Extended RBridge Channel security considerations.

See [[RFC7457](#)] in connection with TLS and DTLS security considerations.

See [[TRILLoverIP](#)] for TRILL over IP security considerations.

See [[RFC4303](#)] for IPsec ESP security considerations.

## [5. IANA Considerations](#)

This section gives IANA Considerations.

### [5.1 Group Keying RBridge Channel Protocol Numbers](#)

IANA is requested to assign, from the range assigned by Standards Action, TBD1 as the TRILL RBridge Channel protocol number for use when the "Group Keying" protocol is transmitted over Extended RBridge Channel messages.

The added RBridge Channel protocols registry entry on the TRILL Parameters web page is as follows:

Protocol	Description	Reference
-----	-----	-----
TBD1	Group Keying	<a href="#">Section 2</a> of [this document]

### [5.2 Group Secured Extended RBridge Channel SType](#)

IANA is requested to assign TBD2 as the Group Secured SType in the "Extended RBridge Channel Security Types Subregistry" on the TRILL

Parameters web page as follows:

SType	Description	Reference
-----	-----	-----
TBD2	Group Secured	<a href="#">Section 2.2</a> of [this document]

## Normative References

- [RFC2119] - BBradner, 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>>.
- [RFC4303] - Kent, S., "IP Encapsulating Security Payload (ESP)", [RFC 4303](#), DOI 10.17487/RFC4303, December 2005, <<https://www.rfc-editor.org/info/rfc4303>>.
- [RFC5310] - Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", [RFC 5310](#), DOI 10.17487/RFC5310, February 2009, <<http://www.rfc-editor.org/info/rfc5310>>.
- [RFC5869] - Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", [RFC 5869](#), May 2010, <<http://www.rfc-editor.org/info/rfc5869>>.

- [RFC6325] - Perlman, R., Eastlake 3rd, D., Dutt, D., Gai, S., and A. Ghanwani, "Routing Bridges (RBridges): Base Protocol Specification", [RFC 6325](#), DOI 10.17487/RFC6325, July 2011, <<http://www.rfc-editor.org/info/rfc6325>>.
- [RFC6347] - Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", [RFC 6347](#), January 2012, <<http://www.rfc-editor.org/info/rfc6347>>.
- [RFC7172] - Eastlake 3rd, D., Zhang, M., Agarwal, P., Perlman, R., and D. Dutt, "Transparent Interconnection of Lots of Links (TRILL): Fine-Grained Labeling", [RFC 7172](#), DOI 10.17487/RFC7172, May 2014, <<http://www.rfc-editor.org/info/rfc7172>>.
- [RFC7176] - Eastlake 3rd, D., Senevirathne, T., Ghanwani, A., Dutt, D., and A. Banerjee, "Transparent Interconnection of Lots of Links (TRILL) Use of IS-IS", [RFC 7176](#), May 2014, <<http://www.rfc-editor.org/info/rfc7176>>.
- [RFC7177] - Eastlake 3rd, D., Perlman, R., Ghanwani, A., Yang, H., and V. Manral, "Transparent Interconnection of Lots of Links (TRILL): Adjacency", [RFC 7177](#), DOI 10.17487/RFC7177, May 2014, <<http://www.rfc-editor.org/info/rfc7177>>.
- [RFC7178] - Eastlake 3rd, D., Manral, V., Li, Y., Aldrin, S., and D. Ward, "Transparent Interconnection of Lots of Links (TRILL): RBridge Channel Support", [RFC 7178](#), DOI 10.17487/RFC7178, May 2014, <<https://www.rfc-editor.org/info/rfc7178>>.
- [RFC7296] - Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T.

Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, [RFC 7296](#), DOI 10.17487/RFC7296, October 2014, <<https://www.rfc-editor.org/info/rfc7296>>.

- [RFC7780] - Eastlake 3rd, D., Zhang, M., Perlman, R., Banerjee, A., Ghanwani, A., and S. Gupta, "Transparent Interconnection of Lots of Links (TRILL): Clarifications, Corrections, and Updates", [RFC 7780](#), DOI 10.17487/RFC7780, February 2016, <<http://www.rfc-editor.org/info/rfc7780>>.

- [RFC7978] - Eastlake 3rd, D., Umair, M., and Y. Li, "Transparent Interconnection of Lots of Links (TRILL): RBridge Channel Header Extension", [RFC 7978](#), DOI 10.17487/RFC7978, September 2016, <<http://www.rfc-editor.org/info/rfc7978>>.
- [RFC8174] - Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<http://www.rfc-editor.org/info/rfc8174>>.
- [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>>.
- [TRILLoverIP] - M. Cullen, D. Eastlake, M. Zhang, D. Zhang, "Transparent Interconnection of Lots of Links (TRILL) over IP", [draft-ietf-trill-over-ip](#), work in progress.
- [SGKP] - D. Eastlake, D. Zhang, "Simple Group Keying Protocol (SGKP)", [draft-ietf-trill-group-keying](#), work in progress.

## Informative References

- [RFC6234] - Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", [RFC 6234](#), DOI 10.17487/RFC6234, May 2011, <<http://www.rfc-editor.org/info/rfc6234>>.
- [RFC7457] - Sheffer, Y., Holz, R., and P. Saint-Andre, "Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)", [RFC 7457](#), February 2015, <<http://www.rfc-editor.org/info/rfc7457>>.

The contributions of the following are hereby gratefully acknowledged:

TBD

Authors' Addresses

Donald E. Eastlake, 3rd  
Futurewei Technologies  
2386 Panoramic Circle  
Apopka, FL 32703 USA

Phone: +1-508-333-2270  
EMail: d3e3e3@gmail.com

Dacheng Zhang  
Huawei Technologies

Email: dacheng.zhang@huawei.com



INTERNET-DRAFT

TRILL: Group Keying Profiles

November 2021

## Copyright, Disclaimer, and Additional IPR Provisions

Copyright (c) 2021 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. The definitive version of an IETF Document is that published by, or under the auspices of, the IETF. Versions of IETF Documents that are published by third parties, including those that are translated into other languages, should not be considered to be definitive versions of IETF Documents. The definitive version of these Legal Provisions is that published by, or under the auspices of, the IETF. Versions of these Legal Provisions that are published by third parties, including those that are translated into other languages, should not be considered to be definitive versions of these Legal Provisions. For the avoidance of doubt, each Contributor to the IETF Standards Process licenses each Contribution that he or she makes as part of the IETF Standards Process to the IETF Trust pursuant to the provisions of [RFC 5378](#). No language to the contrary, or terms, conditions or rights that differ from or are inconsistent with the rights and licenses granted under [RFC 5378](#), shall have any effect and shall be null and void, whether published or posted by such Contributor, or included with or in such Contribution.

