Preamble to Video Services Forum (VSF) Technical Recommendation TR-06-4 Part 2

January 4, 2023

The Reliable Internet Stream Transport (RIST) project was initiated as an Activity Group under the auspices of the Video Services Forum in 2017. The RIST Protocol is defined by TR-06-1 (RIST Simple Profile, published in 2018 and updated in 2020), TR-06-2 (RIST Main Profile, published in 2020 and updated in 2021 and 2022), and TR-06-3 (RIST Advanced Profile, published in 2021 and updated in 2022).

The TR-06-4 series of recommendations define ancillary features for the RIST protocol that are applicable to multiple profiles. TR-06-4 Part 1 (Source Adaptation, published in 2022) is part of this series. This document is TR-06-4 Part 2, Use of Wireguard VPN in RIST Devices. RIST Main Profile defined an encrypted and authenticated tunnel, with functionality similar to a VPN. In some situations, it may be desirable to use a standard off-the-shelf VPN instead. The RIST Activity Group has selected the Wireguard VPN for this purpose, and this Specification defines how Wireguard is configured in compliant RIST devices, in order to ensure interoperability.

Work continues within the group towards developing additional RIST specifications that include additional features. As the Activity Group develops and reaches consensus on new functions and capabilities, these documents will also be released in support of the RIST effort. For additional information about the RIST Activity group, or to find out about participating in the development of future specifications, please visit http://vsf.tv/RIST.shtml

Video Services Forum (VSF)
Technical Recommendation TR-06-4
Part 2

Reliable Internet Stream Transport (RIST)
Use of Wireguard VPN in RIST Devices

Approved January 4, 2023

INTELLECTUAL PROPERTY RIGHTS

THIS RECOMMENDATION IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS RECOMMENDATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY MPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS RECOMMENDATION.

LIMITATION OF LIABILITY

VSF SHALL NOT BE LIABLE FOR ANY AND ALL DAMAGES, DIRECT OR INDIRECT, ARISING FROM OR RELATING TO ANY USE OF THE CONTENTS CONTAINED HEREIN, INCLUDING WITHOUT LIMITATION ANY AND ALL INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, LITIGATION, OR THE LIKE), WHETHER BASED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING NEGATION OF DAMAGES IS A FUNDAMENTAL ELEMENT OF THE USE OF THE CONTENTS HEREOF, AND THESE CONTENTS WOULD NOT BE PUBLISHED BY VSF WITHOUT SUCH LIMITATIONS.

Executive Summary

RIST Main Profile (VSF TR-06-2) in Full Datagram Mode has similar functionality to a VPN, combining GRE-over-UDP tunnel with optional encryption and authentication. This tunnel can be used to carry RIST Simple Profile (VSF TR-06-1), as well as any other traffic. For some applications, it can be desirable to offer a standard off-the-shelf VPN as an alternative. The Wireguard VPN has been selected as this alternative. In order to ensure interoperability, this Specification provides a guide of how Wireguard is to be implemented in RIST devices.

Recipients of this document are invited to submit technical comments. The VSF also requests that recipients notify us of any relevant patent claims or other intellectual property rights of which they may be aware, that might be infringed by any implementation of the Recommendation set forth in this document, and to provide supporting documentation.

Table of Contents

1 Introduction (Informative)

As broadcasters and others increasingly utilize unconditioned Internet circuits to transport high-quality video, the demand grows for systems that can compensate for the packet losses and delay variation that often affect these streams. A variety of solutions are currently available on the market; however, incompatibilities exist between devices from different suppliers.

The Reliable Internet Stream Transport (RIST) project was launched specifically to address the lack of compatibility between devices, and to define a set of interoperability points through the use of existing or new standards and recommendations.

In some situations, it is desirable to use a standard VPN solution to transport RIST Simple Profile (VSF TR-06-1) or Advanced Profile (VSF TR-06-3) streams, as well as other arbitrary data. The Wireguard VPN has been selected as the recommended off-the-shelf solution for this purpose. This Specification provides an implementation guide for Wireguard in RIST systems, in order to ensure interoperability.

1.1 Contributors

The following individuals participated in the Video Services Forum RIST working group that developed this technical recommendation.

Merrick Ackermans (CBS/Paramount)	Sergio Ammirata (SipRadius/AMMUX)	Paul Atwell (Media Transport Solutions)
Eric Fankhauser (Evertz)	Ronald Fellman (QVidium)	Michael Firth (Nevion)
Oded Gants (Zixi)	Brian Keane (Net Insight)	Ciro Noronha (Cobalt Digital)
Adi Rozenberg (AlvaLinks)	Wes Simpson (LearnIPVideo)	Thomas True (Nvidia)

1.2 About the Video Services Forum

The Video Services Forum, Inc. (www.videoservicesforum.org) is an international association dedicated to video transport technologies, interoperability, quality metrics and education. The VSF is composed of service providers, users and manufacturers. The organization's activities include:

- providing forums to identify issues involving the development, engineering, installation, testing and maintenance of audio and video services;
- exchanging non-proprietary information to promote the development of video transport service technology and to foster resolution of issues common to the video services industry;
- identification of video services applications and educational services utilizing video transport services;
- promoting interoperability and encouraging technical standards for national and international standards bodies.

The VSF is an association incorporated under the Not For Profit Corporation Law of the State of New York. Membership is open to businesses, public sector organizations and individuals worldwide. For more information on the Video Services Forum or this document, please call +1 929-279-1995 or e-mail opsmgr@videoservicesforum.org.

2 Conformance Notation

Normative text is text that describes elements of the design that are indispensable or contains the conformance language keywords: "shall", "should", or "may". Informative text is text that is potentially helpful to the user, but not indispensable, and can be removed, changed, or added editorially without affecting interoperability. Informative text does not contain any conformance keywords.

All text in this document is, by default, normative, except the Introduction and any section explicitly labeled as "Informative" or individual paragraphs that start with "Note:"

The keywords "shall" and "shall not" indicate requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.

The keywords, "should" and "should not" indicate that, among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.

The keywords "may" and "need not" indicate courses of action permissible within the limits of the document.

The keyword “reserved” indicates a provision that is not defined at this time, shall not be used, and may be defined in the future. The keyword “forbidden” indicates “reserved” and in addition indicates that the provision will never be defined in the future.

A conformant implementation according to this document is one that includes all mandatory provisions ("shall") and, if implemented, all recommended provisions ("should") as described. A conformant implementation need not implement optional provisions ("may") and need not implement them as described.

Unless otherwise specified, the order of precedence of the types of normative information in this document shall be as follows: Normative prose shall be the authoritative definition; Tables shall be next; followed by formal languages; then figures; and then any other language forms.

3 References

VSF TR-06-1:2020, Reliable Internet Stream Transport (RIST) Protocol Specification – Simple Profile

VSF TR-06-3:2022, Reliable Internet Stream Transport (RIST) Protocol Specification – Advanced Profile

ISO/IEC 18004:2006, Information Technology - Automatic Identification And Data Capture Techniques - QR Code 2005 Bar Code Symbology Specification

Any mention of references throughout the rest of this document refers to the versions described here, unless explicitly stated otherwise.

4 Architecture

RIST devices implementing Wireguard shall use a client/server architecture. One RIST device is a server, to which one or more client RIST devices connect. Wireguard sessions are bidirectional, and once established can be used for communication from server to client and/or from client to server. The server and client configuration may be done through one of the following methods:

- **Method 1:** The server system directly creates configuration files for the clients. The corresponding server-specific configuration is also created on the server system. Client configuration files are transferred to the client devices through out-of-band means not defined in this Specification.
- **Method 2:** There is a separate control system generating the configuration for both the client and server systems. Typically, this control system will be separated from the server and clients by a firewall. In this option, the control system is responsible for directly applying configuration to the server and client devices through out-of-band means not defined in this Specification.

The main advantage Method 2 is that the private keys for the RIST Wireguard clients are not directly available on the RIST server system, so a compromise of that server system would not allow the intruder to gain enough information to impersonate a valid client.

In both cases, the client RIST devices shall receive a configuration file containing all the required Wireguard parameters.

In order to ensure compatibility, the server node shall have the ability to both export and import a standard Wireguard configuration file, with one [**Interface]** section and one or more [**Peer]** sections, one Peer section for each client.

Wireguard sessions shall be used to carry RIST Simple Profile streams, as per VSF TR-06-1. Wireguard sessions may also carry unencrypted RIST Advanced Profile streams, as per VSF TR-06-3. Wireguard sessions may be used to carry non-RIST data for in-band control or other purposes.

Note: At the time of this writing, existing open source Wireguard implementations are likely to be suitable for the purposes of this Specification, but may have issues or defects; implementers are encouraged to independently test and verify such packages. Implementers are free to build their own versions as well, as long as all the configuration items described here are supported.

5 Wireguard Configuration

Wireguard configuration files use the INI syntax. An informative reference is available in the following link:

https://github.com/pirate/wireguard-docs#Config-Reference

A Wireguard configuration file has two sections, **[Interface]** and **[Peer]**. The **[Interface]** section defines the IP configuration of the local (virtual) VPN interface, and the **[Peer]** section defines the remote end of the VPN link. By design, all Wireguard devices include a single **[Interface]** section. Wireguard server configuration files have one or more **[Peer]** sections, one for each client, and Wireguard client configuration files have a single **[Peer]** section for the server.

Wireguard configuration files compliant with this Specification shall be constructed as follows:

- Items specified as **Mandatory** shall always be included.
- Items specified as **Recommended** should be included.
- Items specified as **Optional** may be included.
- Items specified as **Prohibited** shall not be included.

Upon receipt of a configuration file, a RIST Wireguard device shall support all items included in the file that are specified above as **Mandatory**, **Recommended**, and **Optional**.

Upon receipt of a configuration file, a RIST Wireguard device should ignore all items included in the file that are specified above as **Prohibited**.

5.1 Client Wireguard Configuration Files

5.1.1 [Interface] Section

- **Mandatory** items:
    - **Address**: This item includes one or more IPv4 and/or IPv6 addresses in CIDR notation. The behavior of the client when the IP address conflicts with an existing interface is left to the discretion of the implementer. Possible behaviors are:
        - Connection to the server fails due to the IP address conflict.
        - Connection succeeds if the client can handle the conflict in some way.

      The mask for IPv4 addresses shall be /32. The mask for IPv6 addresses shall be /128.
      Note: Implementers are advised to consider the implications of supporting IPv4

and IPv6 support in the client. For example, including only IPv6 addresses in this item may cause a compatibility problem with clients that only support IPv4.
    - **PrivateKey**: specifies the key for this client to use.
- **Recommended** items:
    - **DNS:** specifies the DNS server(s) to use after the VPN tunnel is established. If this entry is present, the client shall give priority to the DNS servers listed in the entry (over DNS servers configured outside Wireguard) to resolve any hostnames to IP addresses.
- **Optional** items:
    - **MTU:** specifies the interface MTU.
- **Prohibited** items:
    - **ListenPort:** specifies the client port. The client shall choose an ephemeral port for its side of the Wireguard connection.
    - **PreUp / PostUp /PreDown / PostDown:** these specify scripts/commands to be run at different stages. These are OS-dependent and are not part of the RIST specification.
    - **Table:** this is OS-dependent and is not part of the RIST specification.

5.1.2 [Peer] Section

- **Mandatory** items:
    - **AllowedIPs:** this item defines one or more IP address ranges that are routed through the tunnel, in CIDR notation. The client shall use the VPN tunnel to send packets to addresses in the specified ranges.
    - **PublicKey:** this item specifies the public key associated with the server's private key.
    - **Endpoint:** this item specifies the IP address or hostname and UDP port for the server.
- **Recommended** items:
    - **PersistentKeepAlive:** this item specifies the frequency of a "ping" packet to keep state in NAT firewalls that may be in the path. RIST recommends a value of 10 seconds.
    - **PreSharedKey:** this item specifies a pre-shared key that adds a layer of symmetric-key cryptography to the communication, for increased security. This may be required by some security policies.

5.2 Server Wireguard Configuration Files

5.2.1 [Interface] Section

- **Mandatory** items:
    - **Address**: This item includes one or more IPv4 and/or IPv6 addresses in CIDR notation, indicating the supported VPN subnets the server participates in. **Note:** Implementers are advised to support IPv4 and IPv6 in the server. For example, including only IPv6 addresses in this item may cause a compatibility problem with clients and servers that only support IPv4.
    - **PrivateKey**: specifies the key for the server to use.
    - **ListenPort:** specifies the server public UDP port.

- **Optional** items:
  - **MTU:** specifies the interface MTU.
  - **DNS:** specifies the DNS server to use when at least one client is connected.
    Note: It is usually not necessary to specify a DNS for the server, as it is of limited usefulness.
- **Prohibited** items:
  - **PreUp / PostUp /PreDown / PostDown:** these specify scripts/commands to be run at different stages. These are OS-dependent and are not part of the RIST specification.
  - **Table:** this is OS-dependent and is not part of the RIST specification.

5.2.2 [Peer] Section

The server shall have one **[Peer]** section per client. Each **[Peer]** section shall be constructed as follows:

- **Mandatory** items:
  - **AllowedIPs:** this item defines the IP addresses that will be routed through the VPN client, in CIDR notation. This item shall include the client IP address with a /32 (IPv4) or /128(IPv6) mask. This item may include additional subnets that the client is willing to route.
    Note: simply specifying a list of subnets in the server configuration file does not guarantee that the client will actually route these packets. Additional configuration work needs to be performed at the client for this functionality. This configuration work is OS-dependent and is done through means outside the scope of this Specification.
  - **PublicKey:** this item specifies the public key associated with the server's private key.
- **Recommended** items:
  - **PersistentKeepAlive:** this item specifies the frequency of a "ping" packet to keep state in NAT firewalls that may be in the path. RIST recommends a value of 10 seconds.
  - **PreSharedKey:** this item specifies a pre-shared key that adds a layer of symmetric-key cryptography to the communication, for increased security. This may be required by some security policies.
- **Prohibited** items:
  - **Endpoint:** by definition, servers do not initiate connections, therefore this item shall not be included the section.

6 Addressing of RIST Simple Profile Streams (Informative)

In a RIST Wireguard environment, all the VPN IP addresses are managed from the Wireguard server or a central location, and thus are consistent in the network. Therefore, RIST Simple Profile streams running over Wireguard can use unicast destination addresses. These can either be the VPN addresses defined in the **[Interface]** section (if the streams are between the VPN endpoints) or some other routed unicast address available through the server or client.

If configured to do so, Wireguard can also support IP Multicast. RIST Simple Profile streams can use multicast destination addresses with Wireguard.

7 Generation of QR Codes for Wireguard Configuration

The amount of information in the Wireguard configuration file is small enough that it can be converted to a QR code, usable for devices that can ingest such codes (such as mobile phones). Devices supporting the generation and processing of QR codes shall comply with ISO/IEC 18004:2006 and shall use QR Code model 2.

7.1 QR Generation Example (Informative)

The following is a sample Wireguard client configuration file:

```
[Interface]
Address = 192.0.2.3/32
PrivateKey = localPrivateKeyAbcAbcAbc=
DNS = 1.1.1.1,8.8.8.8
MTU = 1500
[Peer]
AllowedIPs = 192.0.2.1/24
Endpoint = node1.example.tld:51820
PublicKey = remotePublicKeyAbcAbcAbc=
PersistentKeepalive = 10
```

The QR code corresponding to this configuration file is shown in Figure 1.

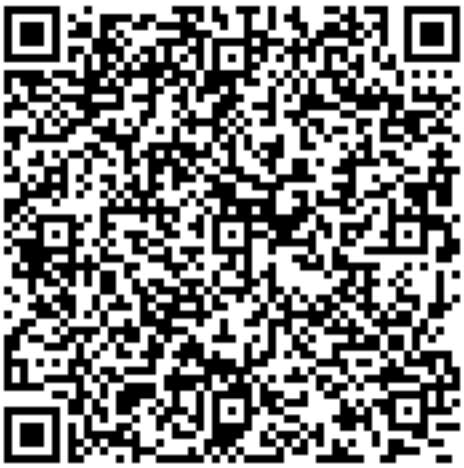

Figure 1: Corresponding QR code for the sample configuration

The recommended tool for generating such codes is the open-source **`qrencode`** command-line tool, available on the following link:

https://fukuchi.org/works/qrencode/