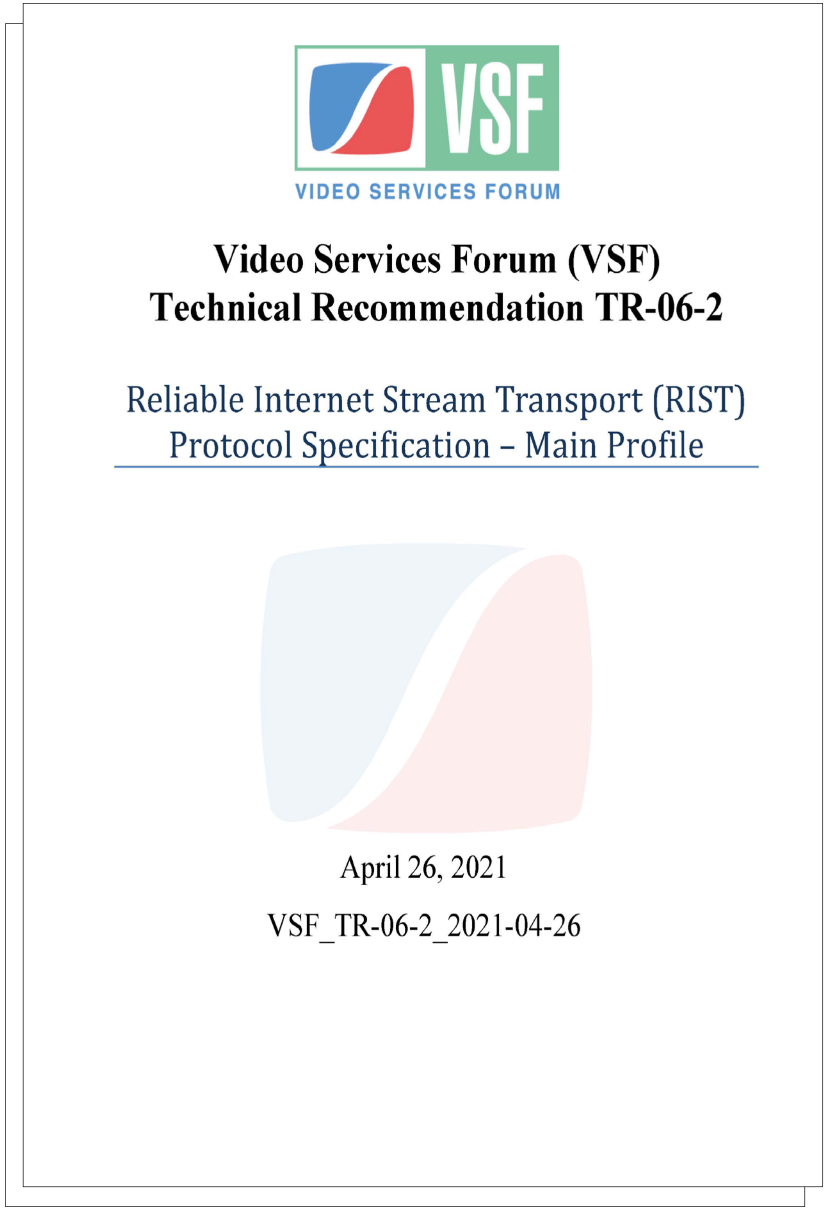
RIST

RELIABLE INTERNET STREAM TRANSPORT

What will the Future Bring?

Rick Ackermans
RIST Activity Group Chair
Director of RF and Transmissions Engineering CBS
VIACOMCBS

VSF
VIDEO SERVICES FORUM



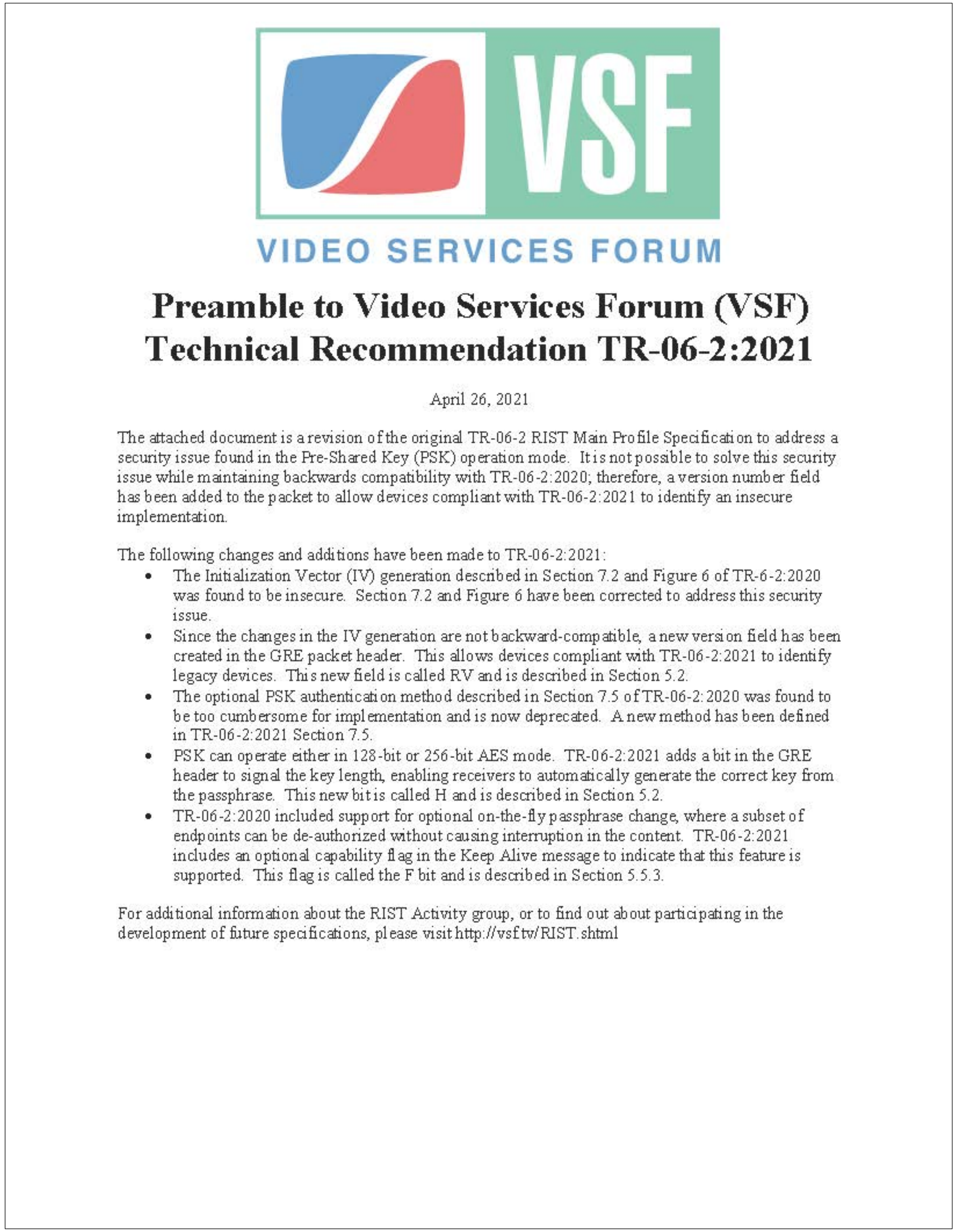
VIDEO SERVICES FORUM

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

Reliable Internet Stream Transport (RIST)
Protocol Specification – Main Profile

April 26, 2021

VSF_TR-06-2_2021-04-26



VSF

VIDEO SERVICES FORUM

Preamble to Video Services Forum (VSF) Technical Recommendation TR-06-2:2021

April 26, 2021

The attached document is a revision of the original TR-06-2 RIST Main Profile Specification to address a security issue found in the Pre-Shared Key (PSK) operation mode. It is not possible to solve this security issue while maintaining backwards compatibility with TR-06-2:2020; therefore, a version number field has been added to the packet to allow devices compliant with TR-06-2:2021 to identify an insecure implementation.

The following changes and additions have been made to TR-06-2:2021:

- The Initialization Vector (IV) generation described in Section 7.2 and Figure 6 of TR-6-2:2020 was found to be insecure. Section 7.2 and Figure 6 have been corrected to address this security issue.
- Since the changes in the IV generation are not backward-compatible, a new version field has been created in the GRE packet header. This allows devices compliant with TR-06-2:2021 to identify legacy devices. This new field is called RV and is described in Section 5.2.
- The optional PSK authentication method described in Section 7.5 of TR-06-2:2020 was found to be too cumbersome for implementation and is now deprecated. A new method has been defined in TR-06-2:2021 Section 7.5.
- PSK can operate either in 128-bit or 256-bit AES mode. TR-06-2:2021 adds a bit in the GRE header to signal the key length, enabling receivers to automatically generate the correct key from the passphrase. This new bit is called H and is described in Section 5.2.
- TR-06-2:2020 included support for optional on-the-fly passphrase change, where a subset of endpoints can be de-authorized without causing interruption in the content. TR-06-2:2021 includes an optional capability flag in the Keep Alive message to indicate that this feature is supported. This flag is called the F bit and is described in Section 5.5.3.

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

April 26, 2021

The attached document is a revision of the original TR-06-2 RIST Main Profile Specification to address a security issue found in the Pre-Shared Key (PSK) operation mode. It is not possible to solve this security issue while maintaining backwards compatibility with TR-06-2:2020; therefore, a version number field has been added to the packet to allow devices compliant with TR-06-2:2021 to identify an insecure implementation.

The following changes and additions have been made to TR-06-2:2021:

- The Initialization Vector (IV) generation described in Section 7.2 and Figure 6 of TR-6-2:2020 was found to be insecure. Section 7.2 and Figure 6 have been corrected to address this security issue.
- Since the changes in the IV generation are not backward-compatible, a new version field has been created in the GRE packet header. This allows devices compliant with TR-06-2:2021 to identify legacy devices. This new field is called RV and is described in Section 5.2.
- The optional PSK authentication method described in Section 7.5 of TR-06-2:2020 was found to be too cumbersome for implementation and is now deprecated. A new method has been defined in TR-06-2:2021 Section 7.5.
- PSK can operate either in 128-bit or 256-bit AES mode. TR-06-2:2021 adds a bit in the GRE header to signal the key length, enabling receivers to automatically generate the correct key from the passphrase. This new bit is called H and is described in Section 5.2.
- TR-06-2:2020 included support for optional on-the-fly passphrase change, where a subset of endpoints can be de-authorized without causing interruption in the content. TR-06-2:2021 includes an optional capability flag in the Keep Alive message to indicate that this feature is supported. This flag is called the F bit and is described in Section 5.5.3.

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

RIST
RELIABLE INTERNET STREAM TRANSPORT

VSF
VIDEO SERVICES FORUM

VIDEO SERVICES FORUM

Video Services Forum (VSF)
Technical Recommendation TR-06-3

Reliable Internet Stream Transport (RIST)
Protocol Specification – Advanced Profile

Coming Soon….

May 12, 2021

VSF_TR-06-3_2021_05_12

TR-06-3 Advanced Profile Key Elements:

Tunnel Level Enhancements, including:

- Packet recovery
- Transparent fragmentation support, with fragment-level recovery
- Lower-overhead transport options
- Pre-Shared Key operation enhancements, including packet integrity hashes
- Common format with the ST-2110 over WAN group
- Support for optional lossless packet payload data compression

Other Future RIST Functionality

- Support for Rendezvous.
- Registration Authority.

- The RIST Activity Group meets every Wednesday at 11AM ET.
- If you are a VSF member feel free to join the RIST Activity Group and participate.
- If you are not a VSF member. See Bob….

RIST

RELIABLE INTERNET STREAM TRANSPORT