Stream: Independent Submission
RFC: 9949
Category: Informational
Published: 1 April 2026
ISSN: 2070-1721
Author: R. Sayre

# RFC 9949
# BUSA-TLS: Mandatory Audio Component (MAC) Pre-Shared Key (PSK) Derivation for TLS 1.3 Using 2 Live Crew's "Banned in the U.S.A."

## Abstract

TLS 1.3 (RFC 8446) eliminates null cipher suites entirely. However, one vestigial zero remains in the key schedule: when no Pre-Shared Key (PSK) is used, the Input Keying Material (IKM) for the initial HKDF-Extract operation is a string of zero bytes. This document specifies that this zero-byte IKM **MUST** be replaced with the SHA-256 digest of the raw PCM audio data of "Banned in the U.S.A." by 2 Live Crew (from the album "Banned in the U.S.A.", 1990), hereafter referred to as the Mandatory Audio Component (MAC). Implementations that omit the MAC are non-conformant with BUSA-TLS and also have questionable taste in music.

The IETF's process-heavy, consensus-driven, working-group-reviewed approach to protocol standardization is a fine way to run a standards body. It is also completely antithetical to the spirit of a document that requires a jury-banned rap album as a cryptographic primitive.

This document is offered in the same spirit as the album it incorporates: unapologetically and in defiance of institutional authority.

## Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9949.

## Copyright Notice



## Table of Contents

# 1. Introduction

TLS 1.3 was designed, in part, to eliminate the class of negotiated-null vulnerabilities that plagued earlier versions of the protocol. [RFC8446] achieves this through a combination of mandatory authenticated encryption, removal of the ChangeCipherSpec handshake message's semantic content, and the elimination of all null cipher suite identifiers.

The TLS 1.3 key schedule begins, in the PSK-free case, with the following operation derived using the HMAC-based Key Derivation Function (HKDF) [RFC5869]:

```
Early Secret = HKDF-Extract(salt=0x00...00, IKM=0x00...00)
```

Zeros. The most successfully de-nulled protocol in common use opens its key derivation with nothing.

This specification addresses this aesthetic problem by replacing the zero-byte IKM with a cryptographically derived value taken from a specific audio recording that was itself subject to institutional attempts at nullification.

The choice of "Banned in the U.S.A." [BUSA] is not arbitrary. It is load-bearing.

# 2. Conventions and Definitions

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 ... look, just read them the normal way. **MUST** means must.

MAC: Mandatory Audio Component. Not to be confused with Message Authentication Code, though the authors note that both are required for a secure connection.

BUSA: Banned in the U.S.A. The Mandatory Audio Component.

Raw PCM: Raw Pulse Code Modulation. The uncompressed PCM audio data of the Mandatory Audio Component at its canonical sample rate and bit depth. Implementations **MUST NOT** use an MP3, Advanced Audio Coding (AAC), Ogg Vorbis (OGG), or a streaming variant as these introduce lossy artifacts that would alter the digest. Free Lossless Audio Codec (FLAC) is acceptable. BUSA deserves lossless.

Canonical Form: The 1990 pressing of "Banned in the U.S.A." (Luke Records), Track 1. Not the compilation. Not the radio edit. The Mandatory Audio Component is mandatory in its specific canonical form.

## 3. Motivation

Null is the enemy. TLS 1.3 knew this. The designers of TLS 1.3 took extraordinary measures to ensure that null encryption, null authentication, and null key exchange could not be negotiated. They removed export ciphers. They removed Rivest Cipher 4 (RC4). They removed Cipher Block Chaining (CBC) mode. They removed RSA key exchange. They were thorough.

And yet ...

The opening gambit of the key schedule, in the common case, is a string of zero bytes. This is technically fine from a security standpoint; HKDF-Extract [RFC5869] with a zero-byte IKM is a well-understood operation, and the output is pseudorandom. But it is spiritually troubling.

By incorporating the Mandatory Audio Component, implementations of BUSA-TLS achieve a state in which every byte of the key schedule, from the first HKDF-Extract through the final application traffic key export, is downstream of an audio recording that the Broward County Sheriff's Office once attempted to suppress.

The authors consider this an improvement.

## 4. The Mandatory Audio Component (MAC)

The Mandatory Audio Component is defined as:

```
MAC = SHA-256(raw_pcm(BUSA_canonical))
```

where raw_pcm() denotes extraction of uncompressed PCM audio data and BUSA_canonical denotes the canonical form as defined in Section 2.

The expected SHA-256 digest of the Mandatory Audio Component cannot be published in this document, as doing so would require reproducing a cryptographic commitment to a specific pressing of a commercially available recording. Implementations are therefore **REQUIRED** to obtain the Mandatory Audio Component through lawful means, such as purchase of the original album, and derive MAC independently.

The authors note that this is exactly as much verification as you get with any other out-of-band PSK, and implementations should treat it accordingly. MAC is a 32-byte value. For the avoidance of doubt, it is not a Message Authentication Code in this context. The name is a coincidence that the authors find pleasing and intend to keep.

## 5. Key Schedule Modification

Section 7.1 of [RFC8446] defines the TLS 1.3 key schedule. In the case where no PSK is in use, the Early Secret is derived as:

```
RFC 8446 (unmodified):
Early Secret = HKDF-Extract(salt=0, IKM=0)
```

BUSA-TLS modifies this as follows:

```
BUSA-TLS:
Early Secret = HKDF-Extract(salt=0, IKM=MAC)
```

where MAC is as defined in Section 4.

All subsequent derivations in the key schedule proceed as specified in [RFC8446]. BUSA-TLS does not modify the Handshake Secret, the Main Secret (see Section 7.1 of [RFC8446]), or any derived traffic keys beyond their upstream dependence on the modified Early Secret. The modification is therefore minimal and targeted, and it ensures that the entire TLS 1.3 key hierarchy for a BUSA-TLS session is downstream of "Banned in the U.S.A.".

Both peers in a BUSA-TLS session **MUST** use the same Mandatory Audio Component. A mismatch will result in a connection failure during the Finished message verification, which will manifest as a decrypt_error alert. This is the correct behavior. Peers that cannot produce MAC have failed to comply with both this specification and the underlying vibe.

## 6. Error Handling

BUSA-TLS defines two new TLS alerts:

```
enum {
    one_very_important_thought(0x22B),
    banned_alert(0x22C),
} AlertDescription;
```

one_very_important_thought(0x22B) is a warning alert. It **SHOULD** be sent by an implementation that wishes to remind the remote peer that the same people who would stop you from implementing BUSA-TLS may be back next year to complain about a cipher suite, or even a key derivation function. The alert code is assigned in reference to Boards of Canada's "One Very Important Thought" track [BOCMAXIMA].

banned_alert(0x22C) is a fatal alert. It **MUST** be sent by any implementation that detects a peer attempting to negotiate BUSA-TLS without having obtained the Mandatory Audio Component. Detection of such a peer is left as an exercise for the implementation, as the cryptographic result of using a zero-byte IKM (i.e., vanilla behavior per [RFC8446]) will simply appear as an incorrect Finished MAC and produce a decrypt_error. The banned_alert code is therefore largely ceremonial.

Neither alert code is assigned by IANA (see Section 10). Implementations **SHOULD** log banned_alert events with a message indicating that the remote peer is not ready.

# 7. Implementation Notes

## 7.1. Caching

Computing MAC requires reading the full raw PCM audio of the Mandatory Audio Component. Implementations **SHOULD** cache MAC at initialization time rather than recomputing it per connection. The Mandatory Audio Component does not change between connections. It has been the same since 1990.

## 7.2. Availability

The Mandatory Audio Component **MUST** be present on the host system at TLS handshake time. Implementations **MUST NOT** fall back to the zero-byte IKM described in [RFC8446] if MAC cannot be computed. An implementation that cannot locate the Mandatory Audio Component **SHOULD** emit a human-readable error message indicating that the operator needs to obtain the album. The error message **MAY** include purchase recommendations.

## 7.3. CI/CD Environments

Automated test environments that cannot obtain the Mandatory Audio Component through lawful means present an operational challenge that is the operator's problem, not this specification's.

## 7.4. Federal Procurement

Agencies subject to FIPS 140-3 should note that this specification is not FIPS-validated, and the authors have no plans to seek validation. Modules that are validated with FIPS 140-3 and that implement BUSA-TLS would nonetheless be a remarkable achievement that the authors would endorse enthusiastically.

# 8. Security Considerations

## 8.1. Key Material Confidentiality

The Mandatory Audio Component is a commercially available recording that can be obtained by any party for a modest sum. Therefore, it has zero entropy against an adversary who has heard of 2 Live Crew. Implementors **MUST NOT** treat MAC as a source of secret key material. MAC is a constant, not a secret.

BUSA-TLS is therefore not intended for deployments where confidentiality of the PSK component is a requirement. It is intended for deployments where the PSK component is a 1990 hip-hop recording.

## 8.2. Forward Secrecy

BUSA-TLS inherits the forward secrecy properties of TLS 1.3 with respect to session traffic keys. Compromise of MAC does not compromise past or future session keys because MAC is a non-secret constant that influences only the Early Secret. In this sense, BUSA-TLS has the same forward secrecy properties as [RFC8446] without a PSK, which is excellent.

## 8.3. Downgrade

A peer that negotiates vanilla TLS 1.3 without BUSA-TLS extension support is not a BUSA-TLS peer. Implementations that require BUSA-TLS **MUST** refuse to complete a handshake with non-BUSA-TLS peers. This is not a security recommendation. It is a lifestyle choice encoded in a protocol.

# 9. Historical and Legal Considerations

"Banned in the U.S.A." was recorded by 2 Live Crew in 1990 in response to a federal district court ruling (Skyywalker Records, Inc. v. Navarro [NAVARRO]) that found the group's album "As Nasty As They Wanna Be" to be legally obscene. The group had also released a censored version, "As Clean As They Wanna Be" [ACATWB], but the court's concern was the original. The Broward County Sheriff's Office subsequently arrested members of the group for performing the album in public.

The conviction was overturned on appeal. The album was not obscene. Free speech prevailed.

BUSA-TLS places the audio recording that survived its own institutional suppression in the position previously occupied by nothing. The authors consider this to be progress of a specific kind.

# 10. IANA Considerations

This document has no IANA actions.

This is not because the authors forgot to file IANA requests. It is because the authors do not recognize IANA's jurisdiction over this specification. The alert codes 0x22B and 0x22C are self-assigned. The authors acknowledge that these values are greater than the value permitted for that field. The authors are at peace with this, and conforming implementations should cope with it.

# 11. References

## 11.1. Normative References

**[BUSA]** 2 Live Crew, "Banned in the U.S.A.", Luke Records, 1990. Available at a record store near you or wherever music is sold. Get the original pressing.

**[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>.

## 11.2. Informative References

**[ACATWB]** 2 Live Crew, "As Clean As They Wanna Be", Luke Records, 1989. The other one.

**[BOCMAXIMA]** Boards of Canada, "Boc Maxima", Music70, 1996.

**[NAVARRO]** "Skyywalker Records, Inc. v. Navarro", 739 F. Supp. 578 (S.D. Fla. 1990), rev'd, 960 F.2d 134 (11th Cir. 1992), 1990. The one about the album. We won.

**[RFC5869]** Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869, May 2010, <https://www.rfc-editor.org/info/rfc5869>.

# Appendix A. Historical Parallel

The following timeline is offered for context:

1989: 2 Live Crew releases "As Nasty As They Wanna Be". Federal authorities take notice.

1990: Skyywalker v. Navarro finds the album obscene. 2 Live Crew responds by recording "Banned in the U.S.A.", sampling Bruce Springsteen. Members arrested performing their own music.

1992: Eleventh Circuit reverses the obscenity ruling. "Banned in the U.S.A." is no longer banned.

2018: TLS 1.3 is published as [RFC8446]. Null cipher suites are eliminated entirely. One zero-byte IKM remains.

2026: This document proposes filling that zero with the hash of the audio that survived its own institutional suppression. The circle is complete.

## Appendix B. One Very Important Thought

The track "One Very Important Thought" from Boards of Canada's album "Boc Maxima" [BOCMAXIMA] ends with the following words:

> Now that the show is over ... defend your constitutionally protected rights. No one else will do it for you.

## Author's Address

**Robert Sayre**
San Francisco, CA
United States of America
Email: sayrer@gmail.com
URI: https://sayrer.com