TBD
Internet-Draft
Updates: rfc4082 (if approved)
Intended status: Standards Track
Expires: 6 May 2026

R. Moskowitz, Ed.
HTT Consulting
R. Canetti
Boston University
2 November 2025

TESLA Update for GNSS SBAS Authentication
draft-moskowitz-tesla-update-gnss-sbas-01

Abstract

This document updates TESLA [RFC4082] to current cryptographic methods for use by the International Civil Aviation Organization (ICAO) in their Global Navigation Satellite System (GNSS) Satellite-based augmentation system (SBAS) authentication protocol. The TESLA updates are to align it with current best practices.

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 https://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 6 May 2026.

Table of Contents

1. Introduction

TESLA [RFC4082] (Timed Efficient Stream Loss-Tolerant Authentication) uses the best practices for cryptography when published in 2005. This is quite dated, and any modern use of TESLA needs to adjust to current algorithms and methods.

This document focuses on the TESLA design targeted by the International Civil Aviation Organization (ICAO) in their Global Navigation Satellite System (GNSS) Satellite-based augmentation system (SBAS) authentication protocol.

The SBAS authentication protocol is more than a modern TESLA implementation. It uses a very tightly designed PKI and the C509 certificate encoding [C509-Certificates] to work within the very highly constrained SBAS communication link. The PKI is out-of-scope for this document and is described elsewhere within ICAO.

This document is very much a "work in progress", in that various ICAO SBAS documents need to be excised for their technical updates to TESLA.

1.1. SBAS use of TESLA

The updating of TESLA in SBAS Authentication is outlined in [SBAS Authentication]. This document is the public source of changes made to TESLA and some of the justifications.

2. Terms and Definitions

2.1. Requirements Terminology

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.2. Notation

||
: Signifies concatenation of information (e.g., X || Y is the concatenation of X with Y).

Ltrunc (x, K)
: Denotes the lowest order K bits of the input x.

2.3. Definitions

Author’s note: Should aviation terms (like SBAS) be defined here?

3. Updates to TESLA

TBD - extracted from SBAS documents.

3.1. TESLA Time Synchronization

TESLA references "indirect time synchronization" like NTP [RFC1035]. It specifies that a controller and senders "engaged in a protocol for finding the value D^0_t between them", with controller and receivers "find the value D^R_t". This is not practical with GNSS time services.

TESLA time synchronization with broadcast only time services, like GNSS time, may be set up with out-of-band data (e.g. T_int) and in-band public key authenticated data. This in-band data transmissions need regular transmissions to accommodate "late joiner receivers".

3.2. TESLA Message Authentication Code

TESLA uses a "cryptographic MAC" that MUST be cryptographically secure. It does not provide any guidelines to what is secure. As industry has shown they will field cryptographically weak easy keyed-MACs (e.g. Mavlink 2.0 [MAVLINK]), this update specifies that TESLA will use HMAC [RFC2104] with at least SHA2 or KMAC [NIST.SP.800-185].

Further, the one-way hash function MUST be at least SHA2.

3.2.1. Additional Info in MAC

Current MAC best practices allow for the inclusion of Additional Information added to the message block (e.g. M || "Message Domain"). This is particularly important with very short messages (e.g. SBAS 250 bit messages).

The MAC function used in a TESLA implementation SHOULD include Additional Information.

3.3. An Aggregated MAC for TESLA

In situations where the link capacity cannot support a TESLA packet for each data message, a set of MAC messages may be aggregated, aMAC, and then the aMAC is transmitted. This transmission savings comes at the risk that if the aMAC is lost, a whole set of messages are not authenticated.

```
aMAC = Ltrunc (28, MAC(k, M1 || M2 || M3 || M4 || M5 || 0000))
```

Figure 1: Aggregated MAC example

Mi Mi is the message broadcast at time t all using the same key

k k is the cryptographic key associated with M

3.3.1. Adding Block Erasure Codes or FEC

When TESLA MACs individual packets, a loss of a MAC and thus an unauthenticated may not matter. When aMACs are used, a loss aMAC could be disruptive and adding a FEC (Forward Error Correction) or Block Erasure Codes may be worth the additional transmission cost.

This potential lost is highly likely in the GNSS SBAS (due to natural or malicious interference) use case where adding Block Erasure Codes is considered important.

The SBAS Block Erasure Codes are built on a set of 5 aMACS which are an aggregation of 5 MACs. Thus the Block Erasure Code recovers the MAC that protected 25 SBAS messages.

Author’s note: Does this section needs expanding?. Should details of the SBAS Block Erasure Codes be included?

4. IANA Considerations

TBD

5. Security Considerations

TBD

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4082] Perrig, A., Song, D., Canetti, R., Tygar, J. D., and B. Briscoe, "Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction", RFC 4082, DOI 10.17487/RFC4082, June 2005, <https://www.rfc-editor.org/info/rfc4082>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

6.2. Informative References

[C509-Certificates] Mattsson, J. P., Selander, G., Raza, S., H旦glund, J., and M. Furuhed, "CBOR Encoded X.509 Certificates (C509 Certificates)", Work in Progress, Internet-Draft, draft-ietf-cose-cbor-encoded-cert-15, 18 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-cbor-encoded-cert-15>.

[MAVLINK] "Micro Air Vehicle Communication Protocol", 2021, <http://mavlink.io/>.

[NIST.SP.800-185]
Kelsey, J., Change, S., Perlner, R., and National Institute of Standards and Technology, "SHA-3 derived functions: cSHAKE, KMAC, TupleHash and ParallelHash", DOI 10.6028/nist.sp.800-185, December 2016, <https://doi.org/10.6028/nist.sp.800-185>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <https://www.rfc-editor.org/info/rfc2104>.

[SBAS Authentication]
Walter, T.W., "Authentication of Satellite-Based Augmentation Systems with Over-the-Air Rekeying Schemes", September 2023, <https://navi.ion.org/content/70/3/navi.595>.

Acknowledgments

This work is in conjunction with the ICAO SBAS Authention Study Group members. This includes, and is not limited to: Jed Dennis (FAA Consultant), Abdel Youssouf (Eurocontrol), Timo Warns (Airbus), Todd Walter (Stanford) and chair Mika谷l Mabilleau (Eurocontrol).

Authors' Addresses

Robert Moskowitz (editor)
HTT Consulting
Oak Park, MI 48237
United States of America
Email: rgm@labs.htt-consult.com

Ran Canetti
Boston University
Boston, MA 02215
United States of America
Email: canetti@bu.edu