

TBD  
Internet-Draft  
Updates: rfc4082 (if approved)  
Intended status: Standards Track  
Expires: 8 June 2026

R. Moskowitz, Ed.  
HTT Consulting  
R. Canetti  
Boston University  
5 December 2025

TESLA Update for GNSS SBAS Authentication  
draft-moskowitz-rfc4082-update-00

## Abstract

This document updates TESLA [RFC4082] to current cryptographic methods leveraging the work done 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 to this and other 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 8 June 2026.

## Copyright Notice

Copyright (c) 2025 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 (<https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Terms and Definitions . . . . .	3
2.1. Requirements Terminology . . . . .	3
2.2. Notation . . . . .	3
2.3. Definitions . . . . .	3
3. Updates to TESLA . . . . .	3
3.1. TESLA Time Synchronization . . . . .	3
3.2. TESLA Message Authentication Code . . . . .	4
3.2.1. Additional Info in MAC . . . . .	4
3.3. An Aggregated MAC for TESLA . . . . .	4
3.3.1. Adding Block Erasure Codes or FEC . . . . .	5
4. IANA Considerations . . . . .	5
5. Security Considerations . . . . .	5
6. References . . . . .	5
6.1. Normative References . . . . .	5
6.2. Informative References . . . . .	6
Appendix A. SBAS use of TESLA . . . . .	6
A.1. Adding Block Erasure Codes or FEC . . . . .	7
Acknowledgments . . . . .	7
Authors' Addresses . . . . .	7

## 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 starts with 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. As other modern uses are shared, this document will be adjusted accordingly.

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. But the process of Key Disclosure used in SBAS will be included here.

This document is very much a "work in progress". Various ICAO SBAS documents need to be excised for their technical updates to TESLA. Also, it is anticipated that other modern uses of TESLA will be captured herein.

## 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

### 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".

There is a challenge for receivers to use GNSS time before TESLA is authenticating those time broadcasts. Thus a receiver should work in the pre-authenticated mode only to enable switch to trusted GNSS time.

Use of NTP should be limited to authenticated NTP. (Editor: more needed here)

### 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 that they will field cryptographically weak easy keyed-MACs (e.g. Mavlink 2.0 [MAVLINK]), this update specifies that TESLA SHOULD, at a minimum, 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. The size of this Additional Information is determined by the size of the original message to MAC and the MAC's security characteristics.

### 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.

$$\text{aMAC} = \text{Ltrunc} (28, \text{MAC}(k, M1 \parallel M2 \parallel M3 \parallel M4 \parallel M5 \parallel 0000))$$

Figure 1: Aggregated MAC example

M<sub>i</sub>        M<sub>i</sub> 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; adding a FEC (Forward Error Correction) or Block Erasure Codes may be worth the additional transmission cost.

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

The EVENODD code is an example of an erasure code that can be used here.

It is a specific, highly efficient erasure coding scheme, primarily used in RAID-6 storage systems, that employs simple XOR operations and two redundant disks to protect against up to two simultaneous failures. Likewise, it can be used to recover up to two simultaneous aMACs.

Author's note: Does this section needs expanding?. Should more details on EVENODD be provided?

## 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., Hglund, J., and M. Furuheid, "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>>.

## Appendix A. 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.

TBD - extracted from SBAS documents.

#### A.1. Adding Block Erasure Codes or FEC

SBAS uses the ODDEVEN Block Erasure Code that is 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: This section needs expanding. Details of the SBAS Block Erasure Codes be included?

#### Acknowledgments

This work is in conjunction with the ICAO SBAS Authentication 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1 Mabillean (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