Satellite-Based Augmentation System (SBAS) Authentication Concept Of Operations Document

Version 0.4

(DRAFT)

SBAS Ad-hoc Working Copy

Date: November 08, 2024

Prepared by

ICAO NSP, SBAS Authentication Ad Hoc Group

Revision History for
SBAS Authentication Concept Document

Revision Number	Description	Document Date
V0.2	Modified from NSP/7 WP-49, added content during SBAS Authentication Ad-Hoc at JWGs/11	27Nov2023
V0.3	Modified JWGs 11, Flimsy 7 with updated / new section (added scope/assumptions, threat, removed App A, App B.	13May2024
V0.4	Updated with additional JWGs12 content and review made by SAAG up to start of JWGs/13 meeting	08November2024
V1.0	SBAS Authentication Concept of Document	TBD

Executive Summary

This document describes the SBAS authentication Concept of Operations (ConOps). SBAS authentication is a message authentication capability that provides confidence that received SBAS data content is actually from SBAS systems and was not generated by a spoofer. SBAS authentication requires SBAS providers to comply with the SBAS authentication standards, provide ICAO Aviation Common Certificate Policy compliant public key material from ICAO approved PKI Certification Authorities (CAs), and broadcast SBAS authentication messages. This document:

- identifies the threats mitigated by SBAS authentication, reviews the scope and assumptions of the SBAS authentication capability.
- provides a description of the key aspects of SBAS authentication to enable completion of SBAS authentication standardization in Standards and Recommended Practices (SARPs) and Minimum Operational Performance Standards (MOPS).
- identifies how SBAS authentication may be integrated and used in air traffic management applications.

Table of Contents

List of Tables

No table of figures entries found.

List of Figures

1 Introduction

This document describes the Satellite Based Augmentation System (SBAS) authentication Concept of Operations (ConOps). SBAS authentication is a message authentication capability that provides confidence that received SBAS data contents are actually from authentic SBAS systems and were not generated by a spoofer. SBAS authentication requires SBAS providers to comply with the SBAS authentication standards, make public key material available from PKI Certification Authorities (CAs) compliant with ICAO Aviation Common Certificate Policy (ACCP) policy, and broadcast SBAS authentication messages. To use the service, the airborne element adds the ability to handle and store SBAS service providers' public keys, receive and process SBAS authentication messages, and provide position outputs using authenticated SBAS data.

The SBAS authentication ConOps

- identifies the threats mitigated by SBAS authentication, reviews the scope and assumptions of the SBAS authentication capability.
- provides a description of the key aspects of SBAS authentication to enable completion of SBAS authentication standardization in Standards and Recommended Practices (SARPs) and Minimum Operational Performance Standards (MOPS).
- identifies how SBAS authentication may be integrated and used in air traffic management applications.

SBAS authentication relies on the Timed-Efficient Stream Loss-Tolerant Authentication (TESLA) protocol. In this protocol, message authentication tags are developed from the secure hash of broadcast messages with a key. A specific key is calculated for each message based on a hash point for a group of five messages. The hash points are linked to other hash points through a secure, one-way function. The hash points used to generate the message authentication tags are released after a short delay (nominal 6 seconds) after release of the tags. This enables a user to receive the tags in advance of the hash point. At the time of the tag generation, only the approved SBAS would have access to the hash point. Therefore, successful confirmation of the message tags by the user receiver after receipt of the hash point indicates that the broadcast data is valid.

1.1 SBAS Authentication ConOps Document Structure

- Section 1: Introduction
- Section 2: Scope / Assumptions
- Section 3: Threat description
- Section 4: SBAS message authentication
- Section 5: Authentication key management
- Section 6: Cryptography agility
- Section 7: SBAS provider perspective
- Section 8: Avionics perspective
- Section 9: Cockpit perspective
- Section 10: Air traffic and air space perspective

1.2 SBAS Authentication ConOps Document Objective

The objectives of the SBAS authentication ConOps document are to describe:

- a common understanding of the operation of SBAS authentication.

- an understanding of SBAS authentication to aid in adoption and deployment of SBAS authentication.
- additional details on the threat covered by the scheme,
- the technical aspect supporting the authentication scheme,
- the way to operate with SBAS authentication and
- the benefits of SBAS authentication function for various aviation's stakeholders.

SBAS success is dependent on the internationally agreed SBAS SARPs that makes a DO-229() receiver compatible and interoperable with any SBAS of today and foreseen in the future. Therefore, the SBAS authentication standard is developed as an international interoperable standard, maintaining a single unique standard definition with harmonized cryptographic primitives, and avoiding SBAS provider-specificities.

2 Scope / Assumptions

2.1 Context

SBAS currently provides satellite and ionospheric corrections and integrity over regional areas, allowing use of GNSS for safety-critical operations such as aircraft precision approaches. Current SBAS receivers operate with received SBAS signals and require no additional checks to validate them. The complete trust placed in SBAS signals means that the receiver will operate on a spoofed signal as if it were a legitimate SBAS signal. Spoofing can lead to an integrity failure when the spoofing signals that are received and processed as valid GNSS signals create positioning errors that exceed their respective protection levels. Therefore, spoofing of the SBAS signal is a threat to safety-critical operations and spoofed SBAS data can lead a receiver into a coherently false position with no warning to the user.

While the potential impact of spoofing has been known for a long time, actual spoofing of aircraft GNSS systems has only been observed in the last few years. The Automatic Dependent Surveillance – Broadcast (ADS-B) position reported by aircraft operating near conflict zones has shown abnormal behavior. Such behavior includes instantaneous jumps from the current position to distant locations, such as from the Mediterranean to the Beirut Airport, or jumps to a circling trajectory. Japan reported observing spoofing indications in GPS/INS capable aircraft operating over Japan oceanic airspace and attributed the source to fisherman trying to mask illegal or unregulated fishing.

2.2 Motivation

SBAS authentication provides a means to identify SBAS signals sent by specific SBAS providers. SBAS authentication needs to be implementable by both existing SBAS systems and future SBAS receivers while having minimal to no impact to current SBAS receivers and operations that do not support SBAS authentication.

SBAS authentication is a part of the broader effort to harden aviation receivers from jamming and spoofing threats and to provide security and resilience to aviation use of GNSS. While SBAS authentication implemented on one receiver may provide protection for that receiver, SBAS authentication may help receivers identify spoofing which could help manage the airspace with a mix of legacy receivers that have no spoofing protection. The receiver may use the indication of spoofing detected through failure of SBAS authentication to make a general spoofing declaration. A general spoofing declaration determined by the receiver may be forwarded to air traffic control as one input into a broader interference detection and mitigation capability that is beyond the scope of this concept document.

2.3 Assumptions

The concept described later in this document complies with the following assumptions about the SBAS authentication service, system and signal capabilities, which have been consolidated over time. The sentences added in italics at the end of each assumption summarize the impact of the assumption on the presented technical solution.

- **RF bands and services:** GSWG started the development of SBAS authentication with the presumption that it is only needed to apply to the DFMC SBAS service (SBAS L5 frequency at 1176.45 MHz), but then determined that it is also necessary to provide equivalent protection to the L1 SBAS service (SBAS L1 frequency at 1575.42 MHz). This is because a spoofer could simply jam the L5 signals and then spoof the L1 SBAS messages, thus bypassing the protection provided by DFMC SBAS authentication. *The message authentication scheme must be compatible with the L1 SBAS and DFMC SBAS services to support SBAS authentication on each SBAS service.*
- **Signal RF properties**: The addition of SBAS authentication needs to be compatible with the already established SBAS signal requirements. This means that user received power levels for the L1 in-phase and L5-in-phase signals should remain within the current user receiver requirements. The addition of authentication would not change the current signal RF properties (signal polarization, carrier stability and noise, code/carrier coherency, etc.). The addition of authentication should also be compatible with in-service geostationary satellites and not require recapitalization of the SBAS space segment. *The proposed scheme is compatible with the existing signal structure and does not change the RF signal properties.*
- **Code and data modulation**: The addition of SBAS authentication needs to be compatible with the already established SBAS signal requirements in the ICAO SARPs and the RTCA/EUROCAE MOPS. Data formats need to be compatible with the overall spreading code structure used for the respective channels. Data message additions to the L1 in-phase and L5 in-phase signals follow the already established formats for data on those channels, except when explicitly noted (e.g. MT-50 removal of CRC). Data added to the L1 SBAS channel needs to be backwards compatible such that it maintains the high-level performance requirements for existing users that do not process the authentication messages. *The proposed scheme is integrated in the current signal modulation plan, i.e. in the SBAS L5 and L1 in-phase components, without adding a quadrature component and without impact on the code or data modulation of existing messages.*
- **Message structure and bandwidth**:
  - SBAS authentication will inherently add data and messages to the SBAS standard. *One new message type provides the message authentication Hash-Based Message Authentication Codes (HMACS) and related keys. Other new message types will be needed to enable validation of the TESLA Confirmed Hash point and any Over-the-Air-Rekey (OTAR) capability.*
  - The authentication data requirements need to permit the broadcast of other SBAS messages at the minimum broadcast rates identified in the SBAS standards. The current proposal sends an authentication signature message every six seconds and may require up to an additional twenty OTAR messages every 300 seconds for a total authentication message occupancy up to 24%. *The proposed scheme is expected to use a maximum of 24% of each of the L5 and L1 SBAS message streams.*
- **SBAS performance assumptions**:
  - SBAS authentication is expected to maintain compliance with the SBAS performance requirements over the target service area, up to CAT-I requirements (35 m VAL). No significant degradation in service coverage of performance should occur due to its introduction. *The proposed scheme maintains the SBAS service performance requirements.*
  - With SBAS authentication, SBAS will maintain the Time To Alert (TTA) of 5.2 seconds. In order to achieve the TTA requirement, it is considered acceptable to immediately use some SBAS message information without waiting for authentication, such as alert information and increases in user range errors (UDRE/DFRE). *The proposed scheme uses integrity parameters*

that increase user error deviations or indicate an alert condition on receipt, in order to maintain the Time To Alert, while other data is only used after authentication to preserve integrity and counter spoofing.

- For data not used immediately, the receiver needs to wait to receive both the message to be authenticated, and its corresponding authentication message. This may lead to an extension of the message content timeouts as proposed in the current standards. *The proposed scheme requires the extension of some user error timeouts (UDRE/DFRE) provided that the messages continue to be received.*

- **Cryptographic assumptions**:
  - The cryptographic functions, parameters, and minimum security level included in the proposed scheme are, to the extent possible, based on current standards. In case any design decision is not explicitly justified by current standards, this is duly noted and justified in this report. According to this approach, post-quantum cryptographic functions are at the moment not included, as they are not yet standardized and their security is currently being assessed. *The proposed scheme uses standard cryptographic techniques and achieve security levels as recommended by common cryptographic standards.*
  - The cryptographic functions require an out-of-band technique to receive keys or to establish a trust anchor for any cryptographic information broadcast in-band. *The proposed scheme includes requirements on establishment of trust anchors and enables multiple levels of in-band key distribution anchored by a key received out of band.*
  - The proposed scheme must include a key management scheme that will not require airlines to implement key management actions more frequently than the current ARAC update cycle. *There is still a tradeoff here between a multi-layer approach or one that provides more frequent out-of-band trust anchors for the TESLA Confirmed Hash Point.*
- **Receiver assumptions**:
  - SBAS authentication receivers must be able to store, update and protect public cryptographic information. No private information such as secret keys is required. *The proposed scheme requires the receiver to store and update public cryptographic information.*
  - SBAS authentication receivers must be able to validate that any updated cryptographic information is only obtained from the correctly associated source. There must be a manufacturer installed trust anchor that establishes valid cryptographic update sources specific to each SBAS service provider (e.g. the public cryptographic information associated with WAAS must only be obtained from a validated FAA source). *The receiver must only obtain updated cryptographic data from correctly associated and validated sources.*
  - The additional CPU load required for message authentication will be commensurate, if not much lower, to that already required for existing functions of the SBAS receivers. *The cryptographic operations required in the receiver will be as a maximum commensurate, in terms of CPU load, with already existing processing functions.*
  - SBAS authentication receivers must be able to synchronize with a loose time reference that must be different than the time obtained from SBAS and GNSS signals. Further details are provided in the next sections. *The proposed scheme requires the receiver to maintain a time synchronization within +/-3 seconds of the SBAS network time through use of a reliable independent time reference.*

3 Threat Description

Designing and validating SBAS authentication requires a threat model – a definition of which security threats SBAS authentication shall protect against. This section describes such a threat model as input for design decisions on the protocol for SBAS authentication. The section describes the notional security scope before identifying the threats to be addressed. The section first addresses the threat model for a notional SBAS model and then extends to entities and interactions introduced with the SBAS authentication concept.

By the Airworthiness Security Process Specification (RTCA DO-326B / EUROCAE ED-202B), a security scope is comprised of two parts: the security perimeter and the security environment. The security perimeter denotes the boundary between the assets to protect (along with their security measures) and the security environment. For example, for airworthiness, assets to protect are aircraft resources (like aircraft functions and data) that contribute to the aircraft's airworthiness. The security environment describes entities and interactions outside the security perimeter as relevant for the protection of the assets.

Figure 1 illustrates the security scope considered for SBAS authentication. Being part of the GNSS user segment, the assets to protect are aircraft functions, systems, and data relying on SBAS, notably including SBAS-capable GNSS receivers and their functions. The security perimeter is formed by the aircraft antennas used to receive DFMC SBAS broadcasts, including the signals of core constellation services (i.e., GPS SPS, GLONASS CSA, Galileo OS, and BDS OS) and of SBAS services (on L1 and L5). These antennas are directly exposed to sources of Radio Frequency Interference (RFI) security threats.

The security environment includes the core constellations (GPS, GLONASS, Galileo, and Bei-Dou), the SBAS ground segments, and the SBAS space segments. The authentic core constellations and SBAS segments are trusted and, therefore, not considered a source of threats.

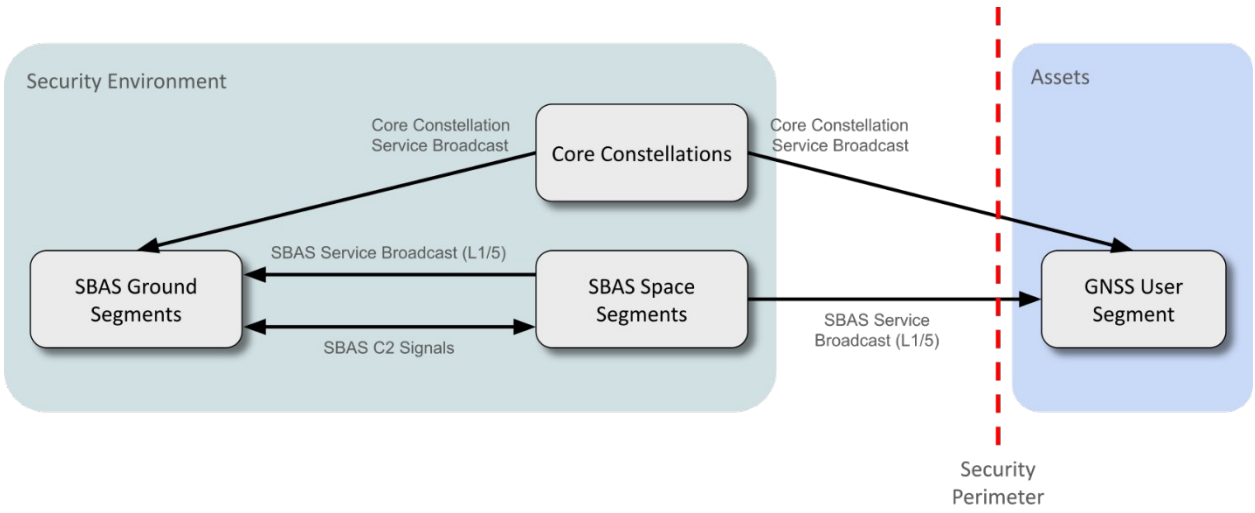


Figure 1: Security Scope for SBAS Authentication

The SBAS space segments broadcast their service signals (on L1 and L5), which are received by the GNSS user segment and the SBAS ground segments (for monitoring and for computing SBAS ranging correction parameters). The SBAS signals received by the GNSS user segment cross the security

perimeter and are the focus of SBAS authentication: SBAS authentication shall protect against security threats targeting the GNSS user segment via SBAS navigation message manipulations.

SBAS broadcasts received by the SBAS ground segments (inside the security environment) are not particularly considered for protection by SBAS authentication, while they may take benefit from SBAS authentication similar to the user segment. Likewise, the interactions between the SBAS ground and space segments for command and control are inside the security environment and are not considered a source of threats. SBAS system is responsible to manage these threats within the security environment.

The core constellation service signals are received by the GNSS user segment and by the SBAS ground segments (for computing the correction parameters). The signals received by the SBAS ground segments are not considered as a source of threats. While, for example, core constellation spoofing may affect SBAS reference receivers and, if not detected, may lead to erroneous SBAS services, such threats are beyond the scope of SBAS authentication. SBAS system is responsible to manage these threats within the security environment.

3.1 STRIDE Model

The identification of the threats to be addressed by SBAS authentication is performed relying on the threat classes of the STRIDE methodology. With STRIDE, threats are categorized into

- Spoofing: masquerading as another entity,
- Tampering: unauthorized change of data or state,
- Repudiation: performing an action and later denying having it performed,
- Information Disclosure: unauthorized access to information,
- Denial of service: preventing service use when needed, and
- Elevation of Privileges: gaining elevated access beyond authorization.

3.1.1 Spoofing.

With spoofing, an adversary masquerades as one or more SBAS satellites broadcasting syntactically valid, but semantically erroneous signals. Such threats may, for example, impair the SBAS services on correction and GNSS health status and mislead the position solution of receivers.

As the focus of SBAS authentication is on navigation message authentication, spoofing threats that do not manipulate the SBAS navigation messages are out-of-scope. Notably, SBAS authentication neither protects against core constellation spoofing nor SBAS spoofing with authentic SBAS navigation messages (e.g., by repeaters or meaconing). Nevertheless, the presence of such threats shall not invalidate the protection offered by SBAS authentication on the integrity and authenticity of SBAS navigation messages. For example, the SBAS authentication solution needs to be operate correctly even in the presence of core constellation spoofing, such as core satellite constellation spoofing that leads to an erroneous time solution.

3.1.2 Tampering.

Tampering threats include different variants of re-broadcasting authentic GNSS signals: An adversary may record GNSS signals and re-broadcast them, effectively tampering with signal properties used for ranging (like code, carrier, Doppler) without affecting the navigation messages. Alternatively, an adversary may re-broadcast the signals after manipulating the recorded signals (possibly including navigation messages). As for spoofing, tampering threats that do not manipulate the SBAS navigation messages are out-of-scope, but shall not invalidate the protection offered on navigation data by SBAS authentication.

3.1.3 Repudiation.

For a repudiation threat, an authentic core constellation or SBAS service would repudiate having made specific broadcasts. As the authentic core constellations and SBAS services are considered trusted, such threats are considered out-of-scope for SBAS authentication (not applicable to GNSS).

3.1.4 Information Disclosure.

Information disclosure threats are considered not applicable as the SBAS broadcasts contain no data whose confidentiality needs to be protected.

3.1.5 Denial-of-Service.

For a denial-of-service threat, an adversary makes unavailable (parts of) the core constellation and SBAS services or their data. For example, an adversary may (selectively) jam the GNSS broadcast channel (possibly affecting complete services, single SVs, single receivers, and single messages). As SBAS authentication aims to protect the integrity and authenticity of SBAS navigation messages, jamming threats are out-of-scope. As for spoofing and tampering, they shall not invalidate the protection offered by SBAS authentication. For example, jamming an authenticated SBAS service shall not allow to downgrade a receiver to using an unauthenticated SBAS service.

As another denial-of-service threat, an adversary may broadcast specially crafted messages that either misuse the protocols (e.g., declaring all core constellation SVs as not healthy) or trigger potential receiver implementation vulnerabilities causing a receiver to cease services. Such threats are similar to spoofing threats and are in-scope as long as they rely on navigation message manipulations.

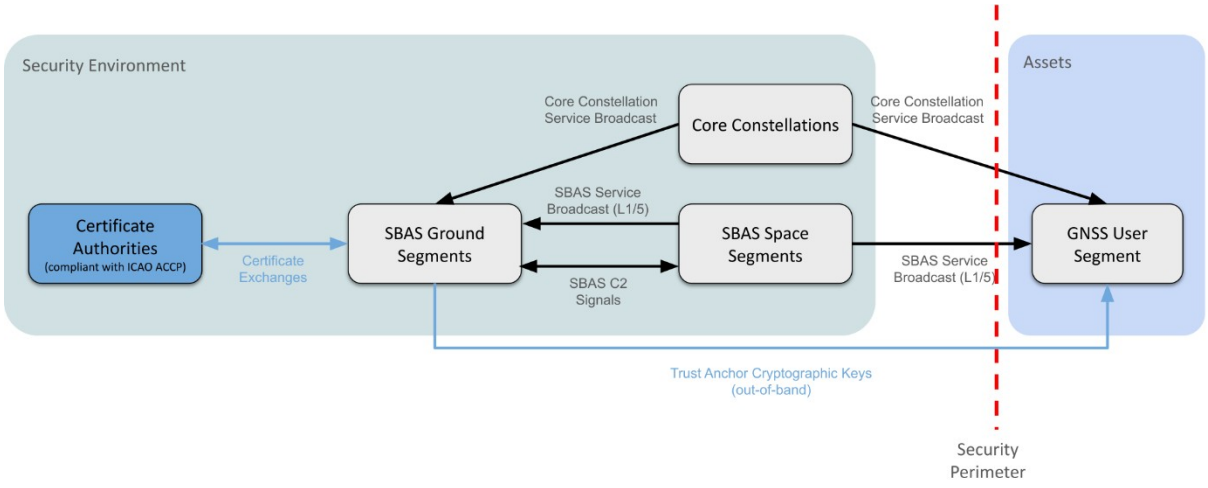
3.1.6 Elevation of Privileges

For an elevation of privileges threat, an adversary broadcasts specially crafted messages that trigger potential receiver implementation vulnerabilities yielding some level of control over the receiver control flow to the adversary (“remote code execution”). Such threats are similar to spoofing threats and are in-scope as long as they rely on navigation message manipulations.

3.2 Threats to SBAS authentication protocols

For protecting the SBAS navigation messages, the SBAS authentication concept relies on cryptographic protocols. An adversary may try to break the cryptographic protocols to perform spoofing despite SBAS authentication protections. Such an adversary is assumed to have access to the same level of computation power as a nation-state actor. Also, an adversary is assumed to know all SBAS authentication protocol details and to have access to all previously broadcasted signals. For example, an adversary may try to randomly guess the aggregated MAC tags or may try to determine the TESLA hash points based on previously observed hash points.

SBAS authentication relies on different cryptographic keys (see section 5). For the management of the keys, the authentication concept requires the use of a Public Key Infrastructure (PKI) compliant to ICAO ACCP and, accordingly, introduces new PKI entities and data flows to the system model. As illustrated in Figure 2, the new entities are Certificate Authorities (CAs) that interact with the SBAS ground segments. For transfer of some key material, a new data flow from SBAS ground segments to the GNSS user segment is introduced to provide the SBAS CA chains and potentially additional cryptographic material.



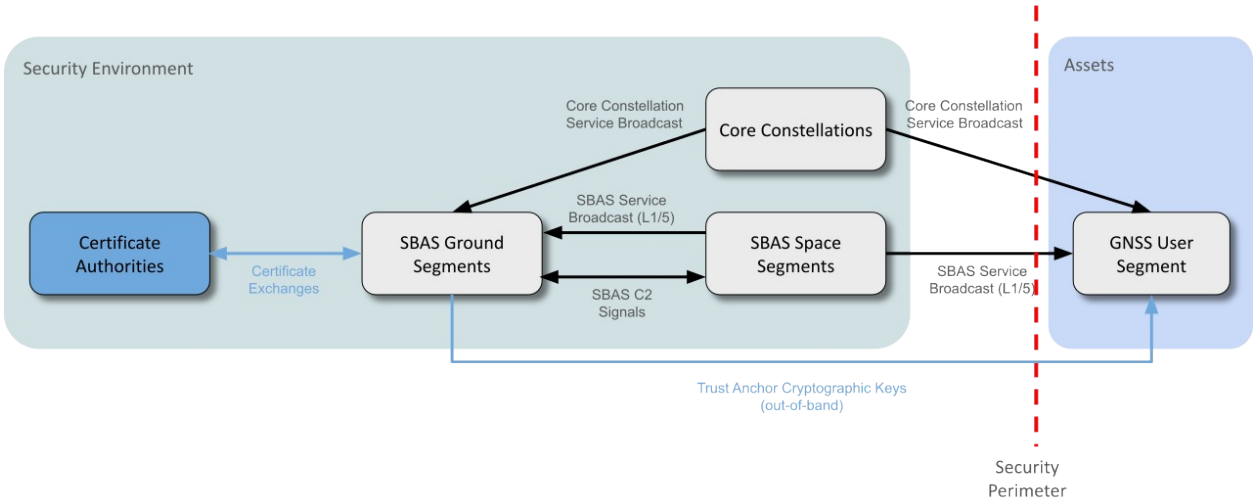


Figure 2: Security Scope extended by authentication concept entities

SBAS providers interact (via their ground segments) with the CAs to request, renew or rekey, and revoke digital certificates. The CAs issue and provide certificates to SBAS providers, who use them to digitally sign data used within the SBAS authentication protocol.

The exchanges between the CAs and the SBAS ground segments are crucial for the security of SBAS authentication. For example, if an authentic CA issues an SBAS service certificate to an adversary, the adversary may spoof SBAS broadcasts with valid authentication tags. As the exchanges are assumed to follow established certificate policies (e.g., as under development with the Aviation Common Certificate Policy (ACCP) by the ICAO Trust Framework Panel), the threats to such exchanges are not further elaborated or in scope for SBAS authentication. See Section Error: Reference source not found for an overview on key management concerns and associated security needs.

For the validation of digital certificates used for SBAS authentication, the GNSS user segment requires access to trust anchors, which are distributed out-of-band (i.e., not via SBAS L1/L5). This data flow crosses the security perimeter of the GNSS user segment. As the security of the SBAS authentication protocol depends on the integrity and authenticity of the trust anchors, the data flow needs to be protected against injections or manipulations of trust anchors (e.g., via spoofing or tampering threats).

While the authentic SBAS services are considered trusted, an adversary may retrieve secret cryptographic key material from an SBAS service via information disclosure threats. Access to certain key material enables an adversary to spoof SBAS broadcasts with valid authentication tags. While no cryptographic protocol can perfectly protect against adversaries with access to secret key material, SBAS authentication may, at least, limit such threats in time (e.g., by regular re-keying) and in space (e.g., to the SBAS service, whose keys were disclosed).

4 SBAS Message Authentication Technique

The SBAS authentication scheme is based on an implementation of the Timed-Efficient Stream Loss-Tolerant Authentication (TESLA) protocol adapted to SBAS. TESLA is standardized as a lightweight broadcast authentication protocol and it provides ideal properties in terms of bandwidth overhead and tolerance to errors. In exchange, it requires a loose time synchronization source to maintain its security. TESLA for SBAS authentication uses a hash chain generated by a one-way function as the basis of hash points. The hash points are used to generate keys, and the message contents and keys are combined to generate a Hash-based Message Authentication Code (MAC). The SBAS implementation sends an aggregated Message Authentication Code (aMAC) with a later disclosure of the TESLA hash point used to generate the individual message MACs and the associated aMAC.

As illustrated in the Figure 3 below, TESLA uses one-way chains being lists of so-called “hash points”, hp_0, …, hp_n, where the computation of a hash point hpi from hpi+1 is efficient using a hash function H, but the calculation of hp_i is not tractable given hp_0, …, hp_{i-1}. The TESLA Confirmed Hash Point, hp_0, is provided in advance to the receiver in a secure manner and is not used to generate MACs.

To compute a navigation message’s MAC, an SBAS service first computes a symmetric cryptographic key $k_{i,t}$ from the current hash point pi and information on the message’s sending time t by an HMAC function and uses the resulting message-specific key, $k_{i,t}$ to compute a hash-based message authentication code (HMAC) as shown in Figure 3. A single hash point hp_i is used to compute the keys for 5 navigation messages. A single hash point may be used to compute keys for both the L1 and L5 signals and to compute the keys for every SBAS satellite of a given provider. Alternatively, the SBAS provider may use a different TESLA hash chain for each SBAS satellite and may use a different TESLA Hash Chain for each SBAS signal. The applicability of the TESLA hash chain is identified in the TESLA hash point signing message. The five navigation message HMACs are aggregated and truncated to form an aggregated MAC (aMAC) for broadcasted via the SBAS authentication message (Message Type (MT) 20 for SBAS L1 and MT 50 for SBAS L5). The broadcast also includes two erasure/recovery fields which enable recovery of the individual message MACs even if the messages were not successfully received. This enables successful authentication of the remaining 5 messages in the set. After a short time period that is at least 6 seconds and may be up to 11 seconds after the aMAC is released in some alert scenarios, the SBAS then also broadcasts the hash point hp_i in the subsequent MT-20 or MT-50 to enable the aMAC verification by receivers.

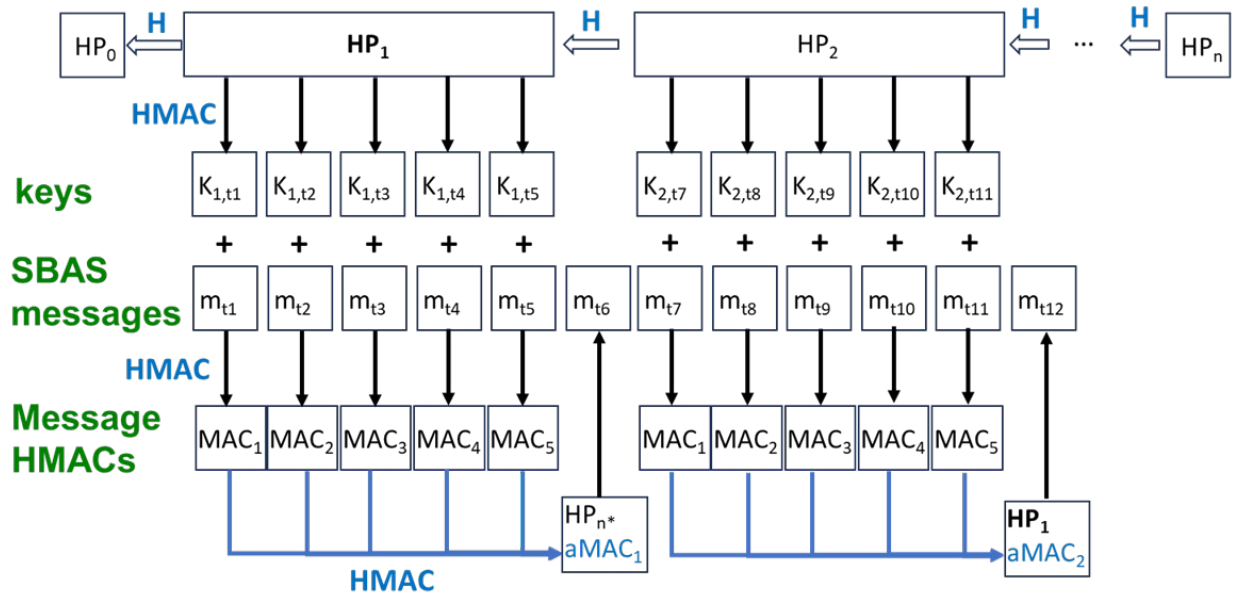


Figure 3: Illustration of a TESLA one-way chain and HMAC key derivation.

To authenticate or verify a message, receivers store the messages and then store the aMAC when it is received. Receivers then wait for the release of the hash point associated with the set of messages and the aMAC. On receipt of the hash point, the receiver first confirms the hash point received is correct by hashing to a known hash point. At startup, the receiver will receive a known hash point, called the hash path end point, associated with a specific time with an asymmetric signature. The first hash path end point is p_0. However, the SBAS may update the broadcast hash path endpoint to any previously released hash point in the hash chain to enable faster confirmation of the hash path. The receiver needs to confirm that the received hash point is part of the hash chain and was released within the correct epoch.

Once the hash point is confirmed, the receiver then calculates the keys for each message and computes the HMAC for each message. The receiver then aggregates the HMACs for comparison with the broadcast aMAC. If there is a match, then the receiver considers the messages authenticated and uses the data contents.

Since the HMACs are aggregated in the MT-20 and MT-50, the concept also includes an erasure / recovery technique. The erasure / recovery technique permits authentication of the five-message set when up to two messages are lost. The baseline erasure / recovery technique is called EVEN/ODD.

If an MT-20 or MT-50 message is lost, then the aMAC and erasure / recovery parameters are lost and the set of five messages cannot be authenticated. The hash point associated with the previous set of five messages will also not be received. The receiver can wait another 6 seconds to receive the subsequent hash point and then hash back to recover the lost hash point. Once the recovered hash point has been validated, then the receiver can authenticate the previous set of five messages. Therefore, when there is a missed message, the 7 to 11 second delay in authentication increases to 13 to 17 seconds. The SBAS provider should consider appropriate message broadcast rates and timeouts for data to ensure continued service when either the data message or the SBAS authentication message (MT-20 / MT-50) is lost.

In general, SBAS information is only used after it has been authenticated. The exception is integrity data that provides an alert or increases the integrity bounds. This includes immediate reaction on receipt of a Do Not Use (Type 0) messages. It also means using UDRE or DFRE data on receipt that has a larger variance (index) than the data in use. UDRE or DFRE data that have lower bounds will not be used until authenticated. This results in the need to extend the timeout period for authenticated UDRE or DFRE

data to 23 seconds, provided that UDRE or DFRE data continue to be received. Under this approach, spoofed data is either not used or only used to increase the UDRE or DFRE value, resulting in larger protection levels.

The TESLA protocol requires an accurate, GNSS-independent clock to support receiver loose time synchronization. The receiver needs to be able to independently confirm the time to ensure that the aMAC and the TESLA hash points are received in the correct timeframe. This is required to ensure that SBAS messages are received in the correct timeframe and not delayed. This prevents the threat where spoofer listens to and receives the correct hash point, and then broadcasts seemingly valid messages with aMACs that are consistent with the hash point. These messages will inherently be delayed by at least 6-seconds (the delay in release of the hash point). Therefore, the independent clock needs to be synchronized (lead or lag) () within 3 seconds of GNSS/SBAS time (the smallest time of any HMAC to hash-point separation). Note that the leading case requirement prevents false alarms. The receiver needs a recurring synchronization procedure or capability. Automated synchronization may include a two-way protocol such as Network Time Protocol (NTP) and address man-in-the middle attacks. The GNSS-independent clock could be a real-time clock.

The TESLA hash chain will periodically need to be refreshed as the hash chain can only be so long in practice. The TESLA Confirmed Hash Point will be communicated to the user via another new message labeled MT21 for the L1 SBAS authentication service and MT51 for the DFMC SBAS authentication service, or via out-of-band distribution. The TESLA Confirmed Hash Point is authenticated via one or two asymmetric keys, with the final key using a pre-installed PKI certification as the root of trust.

5 Authentication Key Management

SBAS authentication relies on cryptographic means to protect the SBAS navigation messages. A pre-requisite for the security of these means is an adequate management of the involved cryptographic keys and related metadata throughout their complete life-cycle. Notably, the effectiveness of SBAS authentication depends on the secure generation, storage, distribution, usage, roll-over, revocation, and destruction of the involved cryptographic keys.

SBAS authentication uses two basic types of cryptographic keys: symmetric keys for Hash-based Message Authentication Codes (HMACs) and asymmetric key pairs to authenticate the base symmetric key (TESLA confirmed hash point). The asymmetric keys have two levels, a longer-lived trust anchor that is provided out of band and a shorter-lived key that is provided in-band. The present section provides an overview on the management of these keys.

5.1 Tesla Hash Path

The security of SBAS authentication depends on different security properties of the TESLA one-way chains: Note that, in the following, we do not further distinguish a hash point hp_i and the keys $k_{i,t}$ derived from the hash point as they are essentially subject to the same operational constraints.

- Temporary confidentiality: Until it is disclosed by the TESLA protocol, a hash point used for MAC computations has to be kept confidential.
- Integrity: After their generation, the hash points used for MAC computations have to be protected from manipulation.
- Authenticity: When a hash point is used for computing or verifying the MAC of a navigation message, it has to be originating from the message's SBAS service.
- Timeliness: When a hash point is used for computing or verifying a MAC, it has to be the hash point that is supposed to be used at the current time (e.g. not an old hash point

supposed to be used in the past); each hash point has a cryptoperiod and has to be used in this cryptoperiod only.

If one or more of these security properties are violated,

- an adversary may be able to compute MACs for spoofed navigation messages considered valid by receivers, or
- the authentication of legitimate navigation messages may fail.

Note that SBAS authentication does not include a revocation mechanism for the TESLA one-way chains as their cryptoperiods are short.

5.1.1 Generation

An SBAS service provider using a one-way chain is responsible for its secure generation: (temporal) confidentiality is ensured by generating hash points that cannot be guessed by an adversary. Upon generation, the SBAS service provider associates a cryptoperiod to the one-way chain denoting the time period when the one-way chain can be used.

The protocol given in Annex 10 describes how to securely compute a one-way chain given its last hash point hp_n. To ensure its confidentiality, the last hash point p_n is randomly generated based on a random number generator suitable for cryptographic purposes. For each one-way chain, the last hash point hp_n is independently generated (i.e. is not reused or based on previous one-way chains).

5.1.2 Storage

A hash point is stored by an SBAS service provider computing MACs and by receivers verifying MACs. The SBAS service provider generating and using a hash point is responsible for securely storing it, preventing an untimely disclosure and any manipulation to it. For example, an SBAS service provider may decide to use a hardware security module for the generation and storage of the hash points.

A receiver manufacturer is responsible for designing a receiver that prevents manipulations of a hash point after it was received over-the-air.

5.1.3 Distribution

An SBAS service provider may decide to use a hash point at a location different from the one, where the hash point was generated. For example, the hash points may be generated within the SBAS ground segment, while the MACs are computed within the space segment. In this case, the SBAS service provider is responsible for securely distributing the hash points to the location where they are used, preventing an untimely disclosure and a manipulation.

By the TESLA protocol, when a hash point is used to compute a MAC, the hash point is broadcasted after the MACs to enable receivers to verify the MAC. That is, the hash point is distributed by the SBAS service to receivers. The SBAS service provider is responsible for the timely broadcast of the hash points (i.e. hash points are not broadcasted too early to prevent attacks and not broadcasted too late to enable a timely MAC verification by receivers). When it's time to broadcast a hash point, it deliberately becomes public (i.e. the need for keeping it confidential is lifted). The authenticity, integrity, and timeliness of received hash points is ensured by the SBAS authentication protocol (see further below).

5.1.4 Usage

By the SBAS authentication protocol, an SBAS service uses a hash point within its cryptoperiod to compute a MAC; a receiver uses the hash point to verify the MAC.

Before a hash point is used, a receiver needs to check the authenticity, integrity, and timeliness of the hash point. As a prerequisite, the receiver needs to already have received a denoted hash point of the one-way chain (i.e. the first element of the chain). The receiver checks

- the digital signature of the denoted hash point (see below for further information),
- the cryptoperiod of the denoted hash point,
- whether the denoted hash point and the current hash point belong to the same one-way chain, and
- the cryptoperiod of the hash point (implicitly as part of the one-way chain construction).

5.1.5 Roll-over

The TESLA one-way chains are short-lived and, therefore, require a frequent roll-over. By the current proposal for constructing one-way chains, the cryptoperiod of every chain ends latest within the same GPS week as its beginning (i.e. the cryptoperiod does not extend beyond a GPS week). Before an SBAS service starts to use the next chain, it broadcasts a denoted hash point of the chain to enable a seamless roll-over at receiver level.

5.1.6 Revocation

If a hash point is compromised (i.e. is disclosed to an adversary) after its cryptoperiod, there is no relevant security impact. If a hash point is compromised before or during its cryptoperiod, an adversary may be able to use the key for spoofing navigation messages. Given the short cryptoperiods of hash points and one-way chains, SBAS authentication does not include any mechanism of revoking a hash point or a one-way chain given their limited window of exposure.

5.1.7 Destruction

As the hash points are broadcasted and become public over time, there are no particular needs for securely destroying them. However, an SBAS service provider ensures to not reuse key material across one-way chains.

5.2 Asymmetric Trust Chain Key Pairs

As discussed above, a receiver needs to check the authenticity, integrity, and timeliness of the currently used one-way chain. More precisely, TESLA requires checking the authenticity, integrity, and timeliness of a denoted hash point in the one-way chain (e.g. the first hash point in the chain). SBAS authentication uses digital signatures with an asymmetric cryptographic key pair (i.e. a public and associated private key) for this purpose: An SBAS service digitally signs the denoted hash point (along with related metadata) using a private asymmetric key. The denoted hash point is broadcasted along with its metadata (e.g. on the cryptoperiod) and its digital signature via MT 21 messages for SBAS L1 and via MT 51 for SBAS L5. SBAS receivers verify the digital signature using the public asymmetric key to check the authenticity and integrity of the denoted hash point.

The public asymmetric key is broadcasted via SBAS navigation messages (also via MT 21/51 messages). To establish trust into this public key, a receiver needs to check its authenticity, integrity, and timeliness. As illustrated in the Figure 4 below, SBAS authentication uses a trust chain for this purpose: The trust chain consists of two asymmetric cryptographic keys with a “trust anchor” key pair as first element and the key pair used for digitally signing a hash point as the second element. The latter key pair (along with metadata) is digitally signed with the private key of the trust anchor.

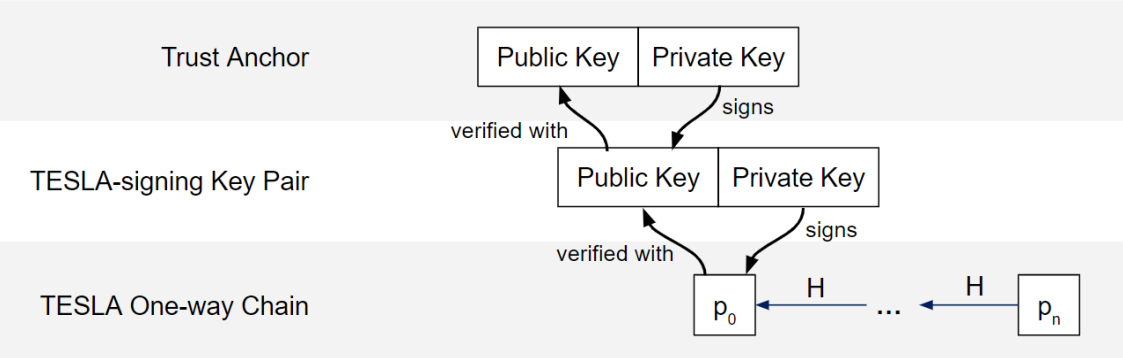


Figure 4: Illustration of the Trust Chain of Asymmetric Key Pairs

A receiver verifies the digital signature of TESLA-signing key pair using the trust anchor public key. The trust anchor public key is distributed out-of-band to receivers (e.g. via Loadable Software Aircraft Parts). Overall, trust in a denoted hash point is established by:

- a trustworthy out-of-band distribution of trust anchors (along with metadata),
- a digital signature of the key used to digitally sign the denoted hash point,
- a digital signature of the denoted hash point (along with related metadata).

The security of SBAS authentication depends on different security properties of the asymmetric key pairs:

- Confidentiality: The private key has to be kept confidential (at least within its cryptoperiod).
- Integrity: After their generation, a key pair (along with its metadata) has to be protected from manipulation.
- Authenticity: When a key pair is used for computing or verifying a digital signature, it has to be a key pair originating from the authentic source (e.g. the SBAS service provider).
- Timeliness: When a key pair is used for computing or verifying a digital signature, it has to be the key pair that is supposed to be used at the current time (e.g. not an old key supposed to be used in the past): Each key pair has a cryptoperiod and has to be used in this cryptoperiod only.
- Non-revocation: Some of the asymmetric keys in a trust chain are long-lived and, therefore, have a long time of exposure to being compromised. If a long-lived private key is detected to be compromised within its cryptoperiod, the key pair is revoked. When a key pair is used for computing or verifying a digital signature, it has to be a non-revoked key pair.

If one or more of these security properties are violated,

- an adversary may be able to interfere with the trust chain and ultimately compute MACs for spoofed navigation messages considered valid by receivers, or
- the authentication of legitimate navigation messages may fail.

5.2.1 Generation

An SBAS service provider is responsible for securely generating the key pairs of the trust chain. It ensures the confidentiality of the private keys by generating key pairs that cannot be guessed by an adversary. Upon generation, the entity associates a cryptoperiod to a key pair denoting the time period when the key pair can be used.

5.2.2 Storage

Any private key of an asymmetric key pair is stored by an SBAS service provider computing digital signatures. The corresponding public key for signature verification is stored by the SBAS provider and by receivers verifying the digital signatures.

The SBAS service provider generating and using a key pair is responsible for securely storing it, preventing a disclosure and any manipulation to the key pair. By best practices, an SBAS service provider generates and stores the key pair in a hardware security module, which allows a secure generation and storage with high assurance.

A receiver manufacturer is responsible for designing a receiver that prevents manipulations of a public key after it was received over-the-air or via out-of-band means.

5.2.3 Distribution

An SBAS service provider may decide to use a key pair at a location different from the one, where the key pair was generated. For example, a key pair may be generated within the SBAS ground segment, while the digital signature of a denoted TESLA key is computed within the space segment, which requires distributing the key material from the ground segment to the space segment. In this case, the SBAS service provider is responsible for securely distributing the key pair to the location where it is used, preventing a disclosure of the private key and a manipulation of the key pair.

Some of the public keys in a trust chain may be broadcasted over-the-air. The SBAS service provider is responsible for the timely broadcast of these public keys (i.e. keys are broadcasted on time to ensure a timely MAC verification by receivers). The authenticity, integrity, and timeliness of received keys is ensured by checking the digital signatures along the trust chain up to a trust anchor.

Trust anchor public keys (and possibly other public keys in a trust chain) are distributed out-of-band to receivers. These out-of-band means need to ensure the integrity, authenticity, and timeliness of the keys made available to receivers. For example, such out-of-band distribution may be based on data loading mechanisms if the keys are part of Loadable Software Aircraft Parts for the receivers or part of avionics databases such as the Navigation Database with Final Approach Segment data available to receivers.

For keys managed out-of-band, SBAS service providers and receiver operators need to ensure a timely distribution. An SBAS service provider needs to make available a new public key sufficiently in advance to enable the receiver operators to install the key before the service starts to use it. A receiver operator needs to install new keys in a timely manner as, otherwise, the receiver is not able to authenticate messages relying on the new key.

5.2.4 Usage

An SBAS service provider uses the private key of an asymmetric key within its cryptoperiod to compute digital signatures; a receiver uses the associated public key to verify signatures.

Before usage of a public key, a receiver needs to check the authenticity, integrity, and timeliness of the key. For a trust anchor, this is ensured by the out-of-band distribution means. For another public key, as a prerequisite, the receiver needs to have already received and checked the public keys in the trust chain from a trust anchor up to the public key. The receiver then checks

- that the public key has been digitally signed by the preceding key in the trust chain,
- the revocation status (see below),
- the cryptoperiod of the public key.

When checking a public key used for signing denoted hash points, the receiver additionally checks that the trust chain is appropriate for the SBAS service using the hash point (i.e. the public keys in the trust chain are acceptable for the SBAS service whose hash point shall be used).

5.2.5 Roll-over

The asymmetric key pairs have a limited cryptoperiod and, therefore, require a roll-over before the end of their cryptoperiod. Before an SBAS service starts to use the next key pair, it needs to distribute it to enable a seamless roll-over.

For key pairs managed out-of-band, SBAS service providers and receiver operators need to ensure a timely distribution with sufficient lead time before usage. For public keys managed via broadcast, the SBAS service provider needs to broadcast the public key before usage. Note that a receiver needs to support multiple public keys (the old one and the new one) for the same purpose to support a seamless roll-over.

5.2.6 Revocation

If the private key of an asymmetric key pair is compromised (i.e. is disclosed to an adversary) after its cryptoperiod, there is no relevant security impact (as receivers are expected to reject the key pair based on the expired cryptoperiod). If the private key is compromised before or during its cryptoperiod, an adversary may become able to create a TESLA one-way chain that is accepted by receivers (and, therefore, spoof navigation messages). To limit the associated risks, a key revocation mechanism has to be foreseen for long-lived asymmetric key pairs. As the long-lived key pairs are distributed out-of-band to receivers and, in case of a revocation, generally a new long-lived key pair has to be distributed to receivers, SBAS authentication relies on out-of-band mechanisms to revoke long-lived asymmetric key pairs. That is, revocation is managed analogously to distribution and roll-over. The revocation information to provide out-of-band could be a list of revoked keys or to remove keys from the list of trust anchors.

Short-lived key pairs may not need to be revoked depending on the remaining window of exposure (from the key being compromised to the end of its cryptoperiod).

5.2.7 Destruction

An asymmetric key pair may be decommissioned before the end of its cryptoperiod. If the key pair was not revoked (e.g. in case of roll-over before the end of the cryptoperiod), receivers continue to accept the key pair for operations. Hence, the private key of an asymmetric key pair should be securely disposed to prevent a disclosure.

Some details of the trust chain have not been decided yet. Notably, the following open points remain:

- Which public keys of the trust chain are distributed out-of-band? Is out-of-band distribution limited to trust anchors or also including other public keys?
- By which means are public keys initially made available for out-of-band distribution? That is, how do SBAS service providers make available the public keys for out-of-band distribution to receivers? Are any Data Service Providers involved? Are any “clearing houses” involved? Would they themselves digitally sign the trust anchors?
- What are the maximum lead times for the out-of-band distribution of public keys and revocation information? What are the minimum time periods for an SBAS provider announcing a new public key for out-of-band distribution before starting to use it?
- In which form is (out-of-band) revocation information managed exactly? Is it a list of revoked keys?

- Given a compromised asymmetric key pair, what is the maximum remaining cryptoperiod justifying to not invoke revocation?

6 Cryptographic Agility

The SBAS authentication concept requires use of cryptographic primitives for four main functions. These functions are the general hash function, a key-derivation function, a signing function MAC, and a signing function for the TESLA Confirmed Hash Point. In general, the SBAS authentication concept targets 128-bit security and intends to use approved cryptographic primitives. Over time, some of these approved methods may be superseded or determined to be inadequate to provide the desired level of security. Cryptographic agility addresses the ability to switch to other cryptographic primitives. The ability to change the cryptographic primitive depends on the function in which the cryptographic primitive is used and the overall receiver architecture.

Hash functions are used in every aspect of the SBAS TESLA authentication approach. Hash functions are used to generate the TESLA hash path. Hash functions are used in the key-derivation function to develop keys from the TESLA hash points. Hash functions are used in the authentication functions as part of the MAC generation and the asymmetric signature generation. Current standards identify two families of hash functions, with multiple variants and levels of security: SHA-2 (Secure Hash Algorithm 2) and SHA-3 (Secure Hash Algorithm 3).

.

The generation of the authentication tag, or Message Authentication Code (MAC) can be a hash-based message authentication code (HMAC), which is also called a keyed-hash message authentication code. HMAC is a specific type of MAC generation involving a cryptographic hash function and a secret cryptographic key. Any cryptographic hash function, such as SHA-2 or SHA-3, may be used in the calculation of HMAC. The MAC generation can also be a Keccak hash function (KMAC).

Asymmetric authentication relies on Public Key Infrastructure and uses a hash function identified for use with the specific asymmetric approach. There are Elliptic Curve Digital Signature Architecture (ECDSA) approaches. Security depends on the selected curve.

Research and standardization of post-quantum cryptography (PQC) suitable for SBAS authentication use is ongoing. Current PQC approaches have large signatures that are too large for broadcast by an SBAS. Use of PQC would require out-of-band provisioning of the TESLA Confirmed Hash point signature. If a PQC technique with signature that fits into the MT-21/51 signature block is developed, then it could be adopted in the future.

Cryptography agility has two potential parts, the ability to change processing between currently defined approaches and the introduction of new approaches. First would be the ability to alternate between existing known cryptographic approaches, such as changing the hash function, changing asymmetric approaches (e.g. ECDSA to EdDSA), or changing security length or curves. Provided that there is agreement on options that are required for receiver implementation, these could be identified in the cryptography metadata included in broadcast SBAS messages. The receiver would need to process the metadata to interpret the cryptographic approach. Processing the lower security level instantiations requires less computational time and presumably less memory storage. However, future computing might reduce the effective security, in which case there might be a desire to transition to the higher security level variations. Additionally, use of a long-lived key, like the Level 1 key, would push for use of the higher security levels. Still, the processing of the TESLA hash chain and MAC generation will drive computation use. The receiver may need the capacity to process the larger hash functions at the

shorter, MAC-generation and verification timeframe. The receiver would need to be able to conduct all functions using the most onerous cryptographic primitive.

The introduction of new approaches will be difficult, in that it will require update to whatever functional block operates using the cryptographic approach, and an update in message processing for anything that is broadcast by SBAS. Based on experience with radio-altimeters, it can take years to change fleet equipage once new standards and new equipment are available. Two scenarios are envisaged: “smooth transition” and “sharp transition”. In the “smooth transition”, the SBAS system introduces use of the new cryptographic approach in parallel with the old cryptographic approach. This allows civil aviation industry and operators to transition to use of the new authentication service over a given period of time without loss of the existing authentication service. This concept provides time for the SBAS users to implement the new cryptographic approach, but likely requires SBAS providers to add additional broadcast messages, likely resulting in an increase in time to receive cryptographic material from the SBAS signal-in-space. In the “sharp transition”, the SBAS system will replace the existing cryptographic approach with the new cryptographic approach. When the new approach is identified well in advance, there will be some time for the aviation industry and operators to develop and implement the new cryptographic approach and be ready for the transition. For users that do not manage to accommodate the new cryptographic approach in advance, these users will lose authentication capability at the transition point until they can update their equipment. The feasibility of the “sharp transition” concept mainly depends on the possibility to update the cryptographic function in the receiver, including any required recertification and deploy the updates to the equipped aircraft in advance of the transition date. This concept reduces the impact on the SBAS provision in that the SBAS does not need to provide means to support the old and new authentication scheme, but transfers risk to SBAS users to update their equipment in advance of the transition date.

The cryptographic agility sets some challenges to airframers, receiver manufacturers and operators. The sharp transition would need several steps in a very limited timeframe to make it happen successfully. First, there is a need to establish an internationally agreed standard which can take some years based on recent experience. The use of a unique standard is certainly one key of a rapid successful convergence between member States. In addition, this standardization must allow receiver manufacturers to assess, experiment, validate and test the new cryptographic technique, hoping that fielded hardware will be able to accommodate it. Given the current long service life of SBAS receivers, it is quite possible that new cryptographic techniques will exceed the provisions for growth originally put into place when the equipment was designed. Second of all, in the best case, no hardware change is necessary and there is a need for a software development with relevant validation & verification following Industry standard DO-178()/ED-12(). At this stage, the Design Assurance Level needed for the crypto function is not decided yet. However, it is likely that it will not be lower than a DAL C, at least to limit the false alert rate to an acceptable level.

7 SBAS providers perspective

The approach proposed is to introduce the SBAS authentication feature as an optional feature for any given SBAS service provider. The standard covers provision of authentication for the SBAS L5 signal and the SBAS L1 signal. Depending on SBAS provider capability to deploy authentication on SBAS L5 signal or on SBAS L1 signal, authentication may be implemented on one signal in advance of implementation on the other signal. While optional for SBAS system and SBAS signals, when an SBAS implements authentication, the SBAS will provide authentication from all SBAS satellites for signals that support authentication. Authentication might become available at different times from different SBAS systems and signals.

SBAS systems implementing authentication expect that the “next generation” of user equipment will use the authentication when provided by the SBAS service provider. There would be no option for individual states to “opt out” of the use of authentication if they employ an SBAS for which the authentication provision exists. Only States operating an SBAS have a role in the provision of the

authentication service. Other States using SBAS may verify the usability of the authentication, either directly or through a delegated entity, which could include the SBAS provider.

SBAS service providers deciding to implement authentication will have to implement the standardized solution according to SARPs. When an SBAS provider decides to support SBAS authentication on L1 SBAS or DFMC SBAS, all SBAS PRNs of this SBAS provider should support authentication on the corresponding service. It is not allowed to have some operational SBAS PRNs broadcast with authentication on one frequency and others operational SBAS PRNs by the same provider and on the same frequency broadcast without authentication, unless in test mode. Receivers do not use SBAS PRNs that do not support authentication from an SBAS provider that supports authentication.

The standardized solution of SBAS authentication continues to support existing L1 SBAS users that cannot take advantage of the authentication. SBAS providers implementing authentication on SBAS L1 may need to adjust existing designs to provide similar service to existing users. However, several design options exist that are consistent with existing L1 SBAS standards and backward compatible with existing users. These options include slowing the rate of fast corrections, use of MT-24, or implementation of dynamic masking.

The standardized solution has been assessed to have little to no impact on the L1 SBAS service for existing users. However, the impact could vary based on individual SBAS implementation.

This will also ensure that the key management process is common to all providers and can result in standardized practices for the user equipment. Each SBAS provider will remain responsible for the generation of their own set of keys and the provisioning of the out-of-band trust anchor and transmission of the public keys, signatures or TESLA confirmed hash point information necessary for the user to implement SBAS authentication for their system.

Each SBAS provider's key management and key transition process should be derived from a security risk assessment (related to the cryptographic part of the solution). The SBAS provider will ensure that there is ample time to receive new key material before ceasing the use of older key material. The SBAS transition process must maintain continuity for users.

Equipment standards will only implement a few defined cryptographic approaches. SBAS providers will need to use one of the identified cryptographic standards in order to be compatible with user equipment.

SBAS providers will provide an indication that they provide authentication and on which signals the authentication applies. This will allow user equipment to reject SBAS signals that appear to be from the SBAS provider that do not include authentication. This notification will be provided out of band with issuance of the SBAS system key material.

8 Airborne equipment operations

In general, SBAS information from an SBAS service that implements authentication is only used after the information has been authenticated, following the "authenticate then use" paradigm. The exception is integrity data that provides an alert or increases the integrity bounds. This includes an immediate reaction to the reception of a Do Not Use (Type 0) message. It also means using UDRE, GIVE, or DFRE data on receipt when the new UDRE, GIVE, or DFRE has a larger variance (index) than the data in use. The correction value or ionosphere delay value that may come in the same message as the UDRE, GIVE, or DFRE would only be used after authentication. In the case of UDRE or DFRE, there is a need to add an additional condition for the timeout of UDRE or DFRE data. The UDRE or DFRE data respectively will timeout per the existing requirements (e.g. 12-seconds for approach operations) from the last receipt of UDRE or DFRE data. Normal authentication of UDRE or DFRE data occurs within 11-seconds of broadcast, with a maximum of 5-seconds from broadcast of the UDRE or DFRE data until release of the

aMAC, and another 6-seconds for release of the associated hash point. The initial timeout of 12-seconds already accounts for the loss of one message. Therefore, the second timeout condition for UDRE or DFRE data is that the data has been authenticated within the timeout period plus 11-seconds (e.g. 23-seconds for approach operations). Under this approach, spoofed data is either not used and cannot provide position corrections or is used to increase the UDRE or DFRE or GIVE value which would result in larger protection levels.

The “authenticate then use” paradigm leads to a modification of the receiver processing flow, as shown in Figure [6] for the L1 data processing. A similar change applies to the L5 data processing chain. Under standard SBAS processing, the receiver tracks the SBAS signal and demodulates the SBAS data. The receiver checks proper reception including validating that the header and data content passes the cyclic redundancy check (CRC). When not implementing authentication, the receiver then parses the SBAS data based on the indicated message type and stores it in the appropriate fields in an SBAS data store. When the receiver generates SBAS corrections and calculates the SBAS position and protection level, it uses the new SBAS data. Therefore, the new SBAS data is reflected in outputs within 800 milliseconds for approach operations to Category 1 minima, and withing 2-seconds for enroute operations.

If authentication is implemented, the data processing flow changes. For the L1 processing flow, after demodulation and reception checks, including the validation of the CRC, the receiver will do two things. First it buffers all SBAS data. At the same time, the receiver checks whether the new message is Message Type 0, contains UDRE or GIVE data or is a Message Type 20. The receiver will immediately follow the existing protocol on receipt of Message Type 0, resulting in clearing data received from that signal. With receipt of UDRE or GIVE information, the receiver will immediately apply UDRE or GIVE information that is larger than the information in use, including acting on Not Monitored or Do Not Use indications. Other data is not immediately used (e.g., ionosphere delay or correction data). The receiver processes the Message Type 20 SBAS authentication message on receipt as well. The receiver will store the aMAC and Block Erasure terms. The receiver will validate the received hash point by confirming that it hashes to a previously confirmed hash point and that it is received in the correct time window for the associated authentication frame. Once the receiver validates the hash point, the receiver essentially follows the same process that SBAS system did to generate the aMAC. The receiver uses the hash point to generation message keys and performs the HMAC function operating on the keys and associated messages to generate the individual message MACs. If necessary, the receiver calculates MACs for missing messages using the block erasure terms. The receiver then generates the aMAC, which can then be compared with the received aMAC. If the aMAC check fails, the data cannot be used and cannot be added to the SBAS data store. This constitutes an authentication failure and may indicate spoofing. When the aMAC check passes, the receiver adds the new data to the SBAS data store. The new data will now be used in the generation of SBAS corrections and protection levels. Without any missed messages, the position output will reflect use of the new data 7 to 11 seconds after the receiver demodulates the data from the SBAS signal. With the exception of fast correction data, this authentication delay is less than 5% of the total message validity time and has only minimal impact.

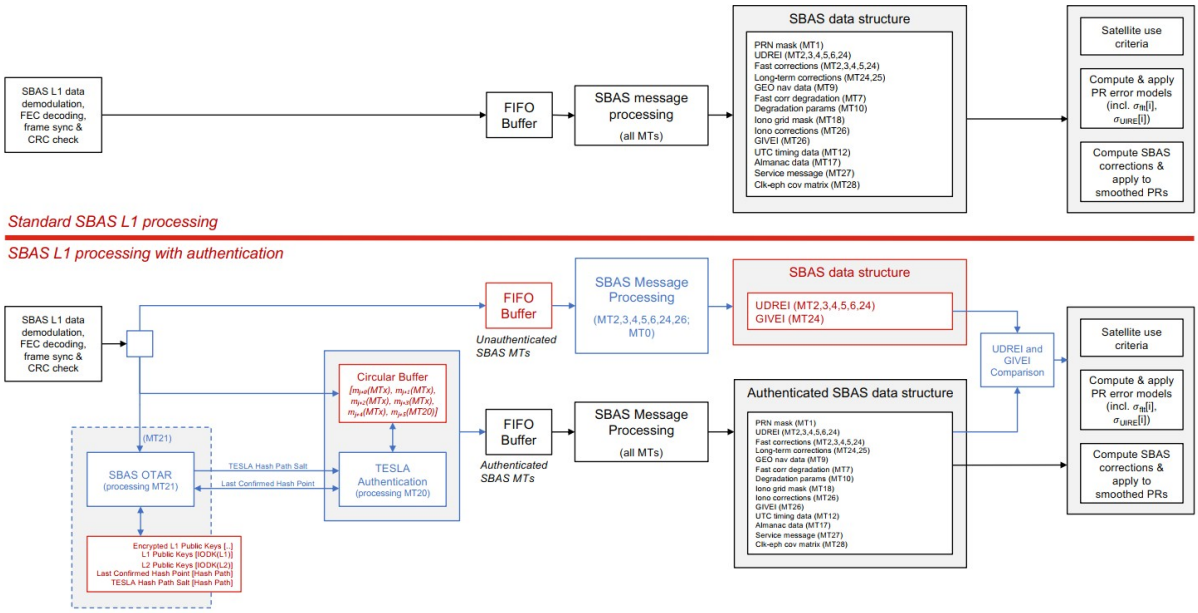


FIGURE 6 *The L1 SBAS data processing flow changes from L1 SBAS data processing without authentication to L1 SBAS data processing with authentication.*

The L5 SBAS processing flow is similar to that of the L1 SBAS processing flow (see Figure [7]). After demodulation and reception checks, including the validation of the CRC for all messages other than a Message Type 50, which does not have CRC, the receiver will do two things. First it buffers all SBAS data. At the same time, the receiver checks whether the new message is Message Type 0, contains DFRE data or is a Message Type 50. The receiver will immediately follow existing protocol on receipt of Message Type 0, resulting in clearing data received from that signal. With receipt of DFRE information, the receiver will immediately apply DFRE information that is larger than the information in use, including acting on Do Not Use indications. Other data is not immediately used (e.g. correction or covariance data). The receiver processes the Message Type 50 SBAS authentication message on receipt as well. The receiver will store the aMAC and Block Erasure terms. The receiver will validate the received hash point by confirming that it hashes to a previously confirmed hash point and that it is received in the correct time window for the associated authentication frame. Once the receiver validates the hash point, the receiver essentially follows the same process that the SBAS system did to generate the aMAC. The receiver uses the hash point to generation message keys and performs the HMAC function operating on the keys and associated messages to generate the individual message MACs. If necessary, the receiver calculates MACs for missing messages using the block erasure terms. The receiver then generates the aMAC, which can then be compared with the received aMAC. If the aMAC check fails and the receiver has received all the messages or is only missing one message, then the receiver could alternately check that the MACs can reproduce the block erasure terms. Passing the block erasure cross-check without passing the aMAC could indicate data corruption of the aMAC term. When the MACs cannot be confirmed, the data cannot be used and cannot be added to the SBAS data store. Since there is no CRC, failure of the aMAC check or failure to validate the hash point could be related to incorrect data reception or could be indicative of spoofing. The receiver may determine that spoofing is present with multiple sequential failures to authenticate. When the aMAC check passes, the receiver adds the new data to the SBAS data store. The new data will now be used in the generation of SBAS corrections and protection levels. Without any missed messages, the position output will reflect use of the new data 7 to 11 seconds after the receiver demodulates the data from the SBAS signal. With the exception of correction data, this authentication delay is less than 5% of the total message validity time and has only minimal impact.

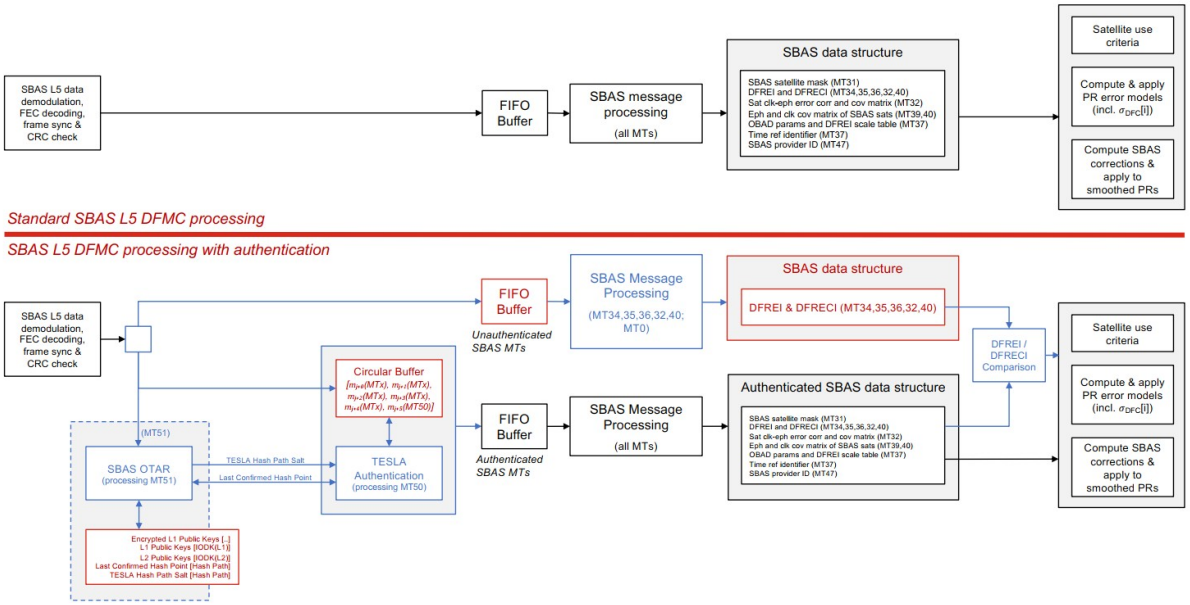


FIGURE 7 *The L5 SBAS data processing flow changes from L5 SBAS data processing without authentication to L5 SBAS data processing with authentication.*

The TESLA protocol requires an accurate, GNSS-independent clock to support receiver loose time synchronization. The receiver needs to be able to independently confirm the time to ensure that the aMAC and the TESLA hash points are received in the correct timeframe and not delayed. This prevents the threat where the spoofer listens to and receives the authentic hash point, and then broadcasts seemingly valid messages with aMACs that are consistent with the hash point. These messages will inherently be delayed by at least 6-seconds (the delay in release of the hash point). Therefore, the real-time independent clock needs synchronization within 3 seconds (lead or lag) of the true SBAS time in order to confirm the correct release of the hash point. The receiver has a possible time error of ± 3 seconds. When the receiver is 3 seconds ahead, the authentic SBAS signal will appears 3 seconds in delay and the receiver should operate in this condition. If the receiver were 3 seconds in delay, then a received SBAS signal that also appears to be three seconds in delay would be accepted. This is the latest a signal could be accepted without risk that it was generated by a spoofer that had already received the valid hash point. Note that the leading case requirement prevents false alarms. The receiver GNSS-independent clock needs a recurring synchronization procedure or capability. Automated synchronization should include a two-way protocol such as Secure Network Time Protocol (SNTP) and address man-in-the middle attacks. The GNSS-independent clock could be a real-time clock to enable independent receiver operations.

The aircraft will need to store and manage keys. As currently defined, there are 3-bits allocated as Issue of Data Key available for broadcast in the Type 21 or Type 51 message. Therefore, each SBAS system could enumerate up to eight Level 2 public keys. There is a possibility of 30 SBAS Provider Identifiers. Therefore, the receiver may need to store 240 PKI certificates for the Level 2 public keys. As currently defined, there are 3-bits allocated for Issue of Data Key for the Level 3 TESLA Hash Chain. There are 39 SBAS satellite PRNs identified, and each satellite could identify 8 TESLA Hash Chains for each signal, resulting in 624 TESLA Hash Chains. Therefore, the receiver may need to store 624 TESLA Confirmed Hash Points and the associated metadata. There is currently no restriction on the size of the TESLA Hash Chain. The receiver does not need to store the entire hash chain.

The aircraft element will need to check the validity of the keys prior to use. When loading keys, the aircraft element will need to confirm that the PKI certificate is valid. When using the keys, the aircraft element will need to check that the key is being used within its validity period. All the keys come with a validity start time and either have a validity end time or validity duration. When revoked, the aircraft

element will need to manage the revocation in such a manner to preclude subsequent receipt and re-use of the revoked key.

In order to limit the receiver complexity, it is envisaged that a single authentication solution is standardized by ICAO. This includes the authentication cryptographic function, the message generation and transmission, as well as the authentication key management scheme. While initial DFMC SBAS offered by service providers may not have the authentication capability, since SBAS authentication is an optional requirement in the SARPs, several ICAO member States have indicated their intent to deploy SBAS authentication. This means that any SBAS provider may decide now or in the future to deploy authentication. As a consequence, the DFMC SBAS receiver MOPS developers will consider the requirement to support SBAS authentication as a minimum requirement at least for some classes of receivers flying internationally. Since receiver lifetime can be as long as 25 years or more, this implies that receiver manufacturers that develop DFMC SBAS receivers capable of SBAS authentication should be prepared to implement this function with all the variants of the SBAS authentication methods (if more than one) for all SBAS, or at a minimum design receivers with sufficient provisions in terms of spare CPU throughput, memory, to incorporate SBAS authentication at a later stage.

Different views have been expressed for whether the authentication feature should be required in all future DFMC avionics. There is a general understanding that equipment (and corresponding regulatory material) should be available to take credit from the authentication feature if decided.

The SBAS Authentication scheme must be backwards compatible with both already approved SBAS avionics and DFMC avionics that does not apply the authentication protocols. In the longer term, all DFMC receivers could be equipped with the SBAS authentication feature. On the other hand, the existing SBAS L1 only receivers, compliant to DO-229(), will not implement SBAS authentication as a minimum requirement. Indeed, this would require a massive retrofit up to several hundreds of thousands of receivers which would pose a significant challenge for manufacturers and operators. This would also require reopening the DO-229 MOPS to incorporate these SBAS authentication requirements while some legacy SBAS receivers might not be capable of sustaining the extra computational resources needed in terms of CPU and memory and might lack some interfaces to manage security (e.g., for key management). Finally, during the transition period with coexistence of legacy receivers with and without SBAS authentication, it would pose the risk of interrupting the use of SBAS technology which will be detrimental to safety for some aircraft that only rely on SBAS to have an approach means with geometrical vertical guidance.

Authentication aware receivers will have knowledge of which SBAS provides an authentication feature through the key management mechanisms (either loading of specific keys for each SBAS or information on list of SBAS with authentication if single key is used across all SBASs). Authentication aware receivers will also need a high trust method to know which SBAS signals do not provide authentication.

If Core GNSS constellation data augmented by SBAS data is used to assist with aligning an inertial navigation sensor (INS) of an aircraft at the gate and authentication is supported by the SBAS, authentication should be applied in the receiver prior to using the SBAS data for alignment.

In addition, SBAS authentication should be implemented together with other spoofing detection techniques such as basic receiver consistency checks of measurement, position, time and data, and INS, if available. Such additional information sources and any impact on the determination of the presence of “spoofing” are not addressed in this document.

9 Cockpit perspective

In modern aircraft, GNSS is one sensor among others contributing to navigation and other capabilities. The result of the authentication check may therefore not need to be processed by the crew for the purpose of reconfiguring the avionics or pursuing its navigation, but only taken into account by the avionics to determine what residual navigation capability is available to pursue the operations.

However, considering the result of the authentication check as part of bringing degraded GNSS conditions to the attention of the crew would still be important, notably with the objective of reporting the occurrence to the relevant ATC services. Since the communication link is open, it would be preferable for ATC to synthesize the information without open communication if possible. In addition, care would need to be taken to clearly separate navigation alerting and spoofing detection indications to the crew in order to respect existing crew resource management principles.

SBAS authentication relies on different cryptographic keys with some distributed out-of-band. The receivers should, upon start-up, check to have valid key material for each SBAS service for which authentication shall be performed. In case of a service without valid key material, receivers should indicate the need for maintenance actions.

One detailed point to address is if the dispatch of an aircraft should be allowed in case the authentication feature is known not to be available (for example, due to the airborne equipment – e.g., keys).

Further discussion with aircraft manufacturers and ANSP/ATC services is required.

10 Air traffic and air space perspective

The reliability of GNSS has become a crucial factor in the efficient and safe operation of ATM. GNSS is the primary technology supporting Performance Based Navigation (PBN), as well as ADS-B and CPDLC which all rely on the status of GNSS on-board aircraft. The provision of time services to ATM systems on the ground is also primarily based on GNSS, and so maintaining the reliability and resilience of PNT services in both cases is a critical factor.

SBAS authentication can play a significant role in this resilience aim.

The primary benefit of SBAS authentication to ATC operation is as a safety mitigation for RNP APCH using SBAS. As a secondary benefit the alerting provided by SBAS authentication could be used by ATC to potentially infer (as part of a series of independent GNSS related indications) a confidence level in the overall reliability of GNSS to the ATC operation. This may have the effect to increase operational efficiency and workload mitigation within en-route airspace.

10.1 RNP APCH Impact

An SBAS authentication alert can trigger a clear indication (or alert) to flight crew that the SBAS input on-board should not be used. During the approach phase of flight when flight crew are performing an RNP APCH which makes use of SBAS, e.g. LPV, such an indication can protect the flight by triggering the flight crew to terminate the current approach and request an alternative. The benefit here is that a spoofing attack is most harmful because it is very difficult to detect; authentication can provide this detection.

At airfields with a low level of CNS infrastructure in particular, where RNP APCH (based on GNSS) is likely to provide the primary method of approach, then SBAS authentication will harden the SBAS service and improve safety in these more exposed areas.

When considering the impact on RNP APCH operations, the need for a high level of confidence in SBAS authentication indications becomes critical with a low occurrence of false alerting, especially at the less equipped airfields. If there is a need to potentially close an airfield due to lack of access to RNP APCH, then this will have a clear negative business impact to the specific airfield, and may trigger a spike in ATC workload for co-ordination in the surrounding area.

As a secondary benefit, an SBAS authentication indication during the approach phase can also be communicated to ATC (and potentially other airspace users), who can determine a picture of GNSS unreliability if multiple such indications are received.

In terms of ATC safety management, if a series of indications point to a spoofing attack specific to SBAS in a region, then it is reasonable to interpret this as part of wider GNSS unreliability in that region, e.g. GNSS Core Constellation, SBAS L1. ATC can then use this information to make future planning decisions for local airport operations.

10.2 En-route Airspace Impact

Within the en-route operation, both ATC and airspace users have a series of mitigation layers available in order to maintain safety and operational efficiency should GNSS be unreliable. A key point therefore, is to know that GNSS is no longer reliable with a high confidence level.

It is crucial that ATC are able to determine whether key (GNSS dependent) components of ATM, such as PBN operations, ADS-B surveillance, CPDLC exchanges or ADS-C trajectory downlinking capability are reliable or degraded. GNSS spoofing effects are much more difficult to detect than jamming and this is where signal authentication functions can play a key role, such as SBAS authentication. SBAS (only) authentication can be beneficial on its own, but the safety benefits increase significantly if authentication techniques are also applied independently to the underlying GNSS core constellations, providing authenticated messages at all layers of GNSS aviation services.

As noted earlier, SBAS authentication indications being triggered by multiple aircraft in a region of airspace can allow ATC to reasonably infer a wider GNSS unreliability in that region. Any SBAS authentication navigation alerts from aircraft would be used in combination with other triggers and observations by ATC in order to inform any subsequent operational safety or capacity decisions. There is no expectation that ATC would rely solely on triggers due to SBAS authentication for this purpose. The description above can also be useful for ATC to judge how to best manage advisory services for aircraft flying outside of controlled airspace also.

Figure 1 below provides an illustration of where the main benefit could be derived by ATC from the introduction of SBAS authentication indications to the operation.

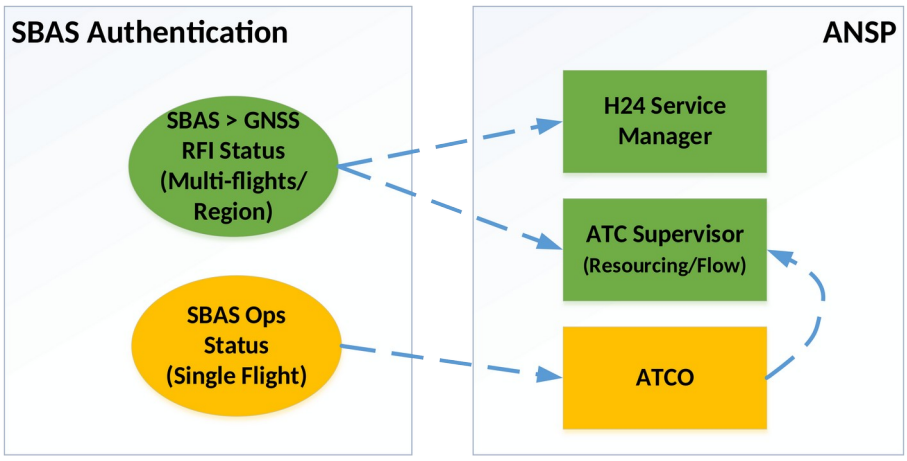


Figure 1: *Possible paths into ATC operation for SBAS/GNSS indications*

From the figure, the provision of GNSS RFI status, e.g. SBAS authentication indication directly to an ATCO, is designated as “amber”, as the benefit is not directly significant. An ATCO would react in the same way as any “loss of Nav capability” indication, by recognising flight crew requests such as moving to a surveillance vectoring service.

The “Green” benefit areas of the diagram address the situation where multiple GNSS RFI status indications, e.g. through SBAS authentication, are provided to ATC (through flight crew communication). In this case the information would be used by ATC supervisors, together with Service Managers to assess the GNSS environment, the scale of the impact, possible inference of duration, and any consequent impacts on airspace management (sectorisation), and overall capacity (flow regulations).

In this way, the ATC response to GNSS unavailability in a region can be similar to how ATC would manage an area of bad weather and requests to avoid from aircraft. ATC would be armed with a universal view of the GNSS environment and would therefore be in a better position to provide advisory information to all flights within an airspace region whether they were equipped with GNSS interference detection capabilities or not. It should be noted that even with this capability, ATC would expect to react to aircraft requests to avoid certain areas of airspace or reports of navigation issues on-board. The SBAS authentication information would not be used in isolation to proactively direct aircraft without guidance from flight crew.

Provision of radar vectoring service to one or two aircraft within an en-route sector should be considered as falling within ATC normal operation. If more aircraft concurrently report this sort of indication and require assistance, then this will have the impact of increasing workload for ATC. Should the unreliability of GNSS in a region of airspace require the closure of certain airfields (that may be primarily reliant on RNP APCH), then this will significantly increase the workload for ATC whereby traffic flow regulation may be required. This is largely due to the additional co-ordination required to manage diversions of flights to alternate destinations.

In this case it is beneficial to have a reliable forward view of how long such a regional GNSS issue may endure. The provision of authentication alerts could help in determining the scale and / or duration of impact.

The reliance on GNSS use is even greater in Oceanic/Remote Airspace (such as North Atlantic or North Pacific in Japanese FIR) where the availability of independent surveillance, and voice-based communications is very limited due to geography. Within this airspace operations are based upon Performance Based Communication and Surveillance (PBCS) criteria and performance, supported by data being delivered from the aircraft in the form of ADS-B, ADS-C and CPDLC applications. The performance of these applications along with GNSS for each flight directly dictates the separation minima that can be assumed for each flight, unlike in domestic airspace. All of these applications rely strongly on GNSS position and time capabilities.

Although SBAS is not used for navigation within these predominantly high-altitude regions of airspace, it can be assumed that SBAS capable receivers will still be providing SBAS-based position and time services to primary (in oceanic operations) systems such as ADS-B, and CPDLC. Therefore, it is assumed that SBAS authentication can also add a level of protection within Oceanic/remote airspace within a similar framework of ATC decision making described earlier.

SBAS spoofing can also trigger longer term effects whereby a receiver will “latch” in a failed state, should the aircraft fly through an intense area of GNSS interference. In these cases, an SBAS authentication indication can trigger short-term maintenance activities on the receiver which will enable the receiver to come back online more readily to continue support for ATM operations.

10.3 ATM Timing Source Impact

Historically ATM has been based around discreet Communication, Navigation and Surveillance services which can be seen as independent from each other. Separate sub-systems with isolated requirements. ATM is moving towards concepts which are underpinned by the exchange of data in both air-to-ground and ground-to-ground domains demanding an emphasis on quality and timeliness of these data exchanges. These concepts therefore rely much more heavily on precise time being delivered both on-board aircraft and on the ground.

As with navigation, the primary source of precise time to aviation and ATM is provided by GNSS, including the same vulnerabilities discussed earlier. More and more therefore, it will be critical to understand the reliability of GNSS in this context and the consequent risk to quality and accuracy of the precise time being passed to all stakeholders.

SBAS authentication alerting can be used (along with other separate indications) to infer a confidence level for GNSS reliability in a certain region, and this could also benefit protection of time services.

10.4 Additional Considerations

A large amount of work has already been done on developing a concept of operations for SBAS authentication from a user perspective through the ad-hoc NSP sub-group. The group now need to complete the work and finally reach agreed outcomes on the open points such as:

- Final mapping of operational response to SBAS authentication alert states
- Assessment of operational criticality of SBAS authentication by flight phase
- Assessment of SBAS authentication as part of a larger aggregated GNSS/SBAS status indication
- Impacts of making authentication optional for receiver MOPS
- Impacts of making authentication optional for SBAS providers
- Estimate adequate numbers of equipped aircraft to trigger operational benefit

10.5 Benefits of SBAS authentication for ATC

The benefits of SBAS authentication are part of a holistic approach to hardening security and resilience around the aviation and ATM use of GNSS. This should include measures to equally protect GNSS core constellation and SBAS services. The introduction of SBAS authentication can improve safety for every individual flight equipped that is undertaking an RNP APCH procedure based on SBAS.

The benefits to ANSPs of SBAS authentication as part of a wider GNSS resilience strategy would be seen not only within Navigation and PBN operations, but also across other dependent applications such as ADS-B, CPDLC and timing services. ANSPs could use SBAS authentication indications as part of a wider GNSS assessment based upon other sources of relevant information to build a resilient picture.

The benefit of the introduction of SBAS authentication in the context of en-route airspace operations, whereby SBAS authentication can act as a pseudo GNSS status monitor, will be directly proportional to the number of equipped aircraft available within a certain region of airspace. Navigation alerts triggered

by SBAS authentication are assumed to be communicated via ATC voice channels from the flight crew or other appropriate means.

From an operational perspective, the expected operational response to any SBAS authentication alerts by flight crew and ATC would need to be kept very simple and clear, based on the information provided by the equipment equipped with SBAS authentication.

11 List of Acronyms

Acronym	Definition
ABAS	Aircraft-based Augmentation System
ADS-B	Automatic Dependent Surveillance-Broadcast
AIP	Aeronautical Information Publication
ARAIM	Advanced Receiver Autonomous Integrity Monitoring
CNAV	Civil Navigation
ConOps	Concept of Operations
CRC	Cyclic Redundancy Check
CSP	Constellation Service Provider
DFMC	Dual-Frequency Multi-Constellation
EU	European Union
GLONASS	Global Orbiting Navigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HAL	Horizontal Alert Limit
H-ARAIM	Horizontal ARAIM
HPL	Horizontal Protection Level
HUL	Horizontal Uncertainty Level
ISD	Integrity Support Data
ISM	Integrity Support Message
ISMG	Integrity Support Message Generator
LNAV	Lateral Navigation
LPV	Localizer Performance with Vertical guidance
MOPS	Minimum Operational Performance Standards
MTTN	Mean-Time-To-Notify
NAGU	Notice Advisories to Galileo Users
NANU	Notice Advisory to NAVSTAR Users
NOTAM	Notice to Airmen, Notice to Air Mission (U.S.)
RAIM	Receiver Autonomous Integrity Monitoring
SARPS	Standards and Recommended Practices
SBAS	Satellite Based Augmentation System
SIS	Signal-in-Space
SSR	Secondary Surveillance Radar
TOW	Time of Week
URA	User Range Accuracy
V-ARAIM	Vertical ARAIM

VNAV	Vertical Navigation
VUL	Vertical Uncertainty Level
WN	Week Number

1267

ATTACHMENT A: EXAMPLE OF RECEIVER STATES AND TRANSITIONS – MULTIPLE CHANNEL MODEL

The following States and Transitions diagram represents the integrity states and transitions for receivers with SBAS authentication. Receivers may operate in an Aircraft Based Augmentation System (ABAS) state, using either Receiver Autonomous Integrity Monitoring (RAIM) or Advanced RAIM (ARAIM). Receivers may also use SBAS systems that support authentication in an authenticate-then-use paradigm, or SBAS systems that do not support authentication. The use of authenticated SBAS data provides confidence that the received data was actually sent by the SBAS system and is not spoofed data. Authentication of the SBAS data does not by itself prove that the signal is the direct-path reception from the SBAS satellite, nor does it prove that the other GNSS signals used by the receiver are authentic direct-path signals. With the removal of the Cyclic Redundancy Check (CRC) from the SBAS authentication message, failure to authenticate is not conclusive identification of spoofing. Failure to authenticate may result from data corruption in flight or at signal reception and not only be a result of spoofing. Therefore, this States and Transitions diagram does not contain a spoofing identified state. Receivers may have other means to detect spoofing. If the receiver identifies individual spoofed satellites and removes them from the position solution, then operations may continue with either ABAS or SBAS integrity. Receiver detection of spoofing may lead to no signals being available and a loss of position data output. Making a spoofing detection claim based on a failure of SBAS authentication should be based on multiple failures to establish a connection between the hash point and the last validated hash point or multiple epochs in a short period of time where authentication has failed.

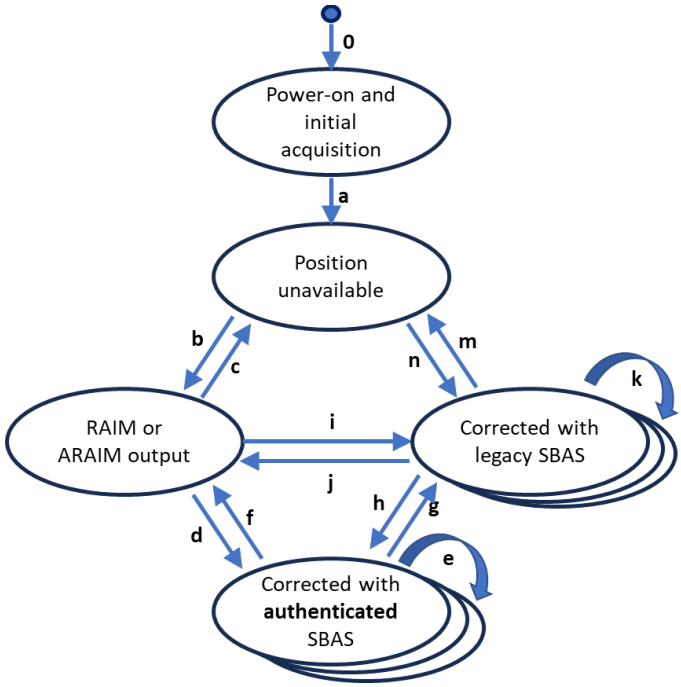


Figure 5: States and Possible Transitions for a Receiver with SBAS authentication capability.

SBAS authentication is authenticate before use. Therefore, an SBAS receiver with authentication can output a position solution from an SBAS that supports authentication only after being able to authenticate the SBAS data. Otherwise, it can output a RAIM/ARAIM solution or else a position solution using an SBAS that does not support authentication.

State Descriptions

State	*Description*	*PVT Outputs*	*Navigation Message Authentication Status*
Power-on and Initial Acquisition	Acquiring satellites and collecting / confirming initial navigation data.	None, prior to Time to First Fix	N/A
Position Unavailable	Insufficient satellites (initial acquisition, interference), spoofing detected (and unable to isolate authentic signals), RAIM/ARAIM detection and failed exclusion	No computed data —or — output but flagged consistent with legacy requirements when navigation is unavailable	None
Outputs with RAIM or ARAIM	Providing position data outputs using RAIM or ARAIM. Receiver inherent spoofing detection methods applied.	Nominal PVT output	None
Corrected with authenticated SBAS	Providing position data outputs using authenticated SBAS data. Receiver inherent spoofing detection methods applied.	Nominal PVT output	Partial NMA
Corrected with legacy (unauthenticated) SBAS	Providing position data outputs using SBAS data without authentication. Receiver inherent spoofing detection methods applied.	Nominal PVT output	None

Notes on States and Possible Transitions

1. If an SBAS system supports authentication, the receiver will only output position data using authenticated SBAS data. If the receiver is unable to generate an SBAS solution with authentication, it will revert to ABAS.

2. The receiver will include inherent spoofing detection methods. The receiver will either remove signals identified as spoofed with position data outputs using one of the integrity methods, or else transition to Position Unavailable.
3. Authentication is applied on a per SBAS GEO basis. When the SBAS supports authentication, data is used only after the message passes authentication. There is no action based on a failure to authenticate data.
4. Individual messages may pass authentication or may not be able to be authenticated. These do not by themselves cause a change in the receiver state as different messages have different levels of criticality in supporting quality and availability of the PVT solution. Additionally with removal of the CRC, a failure to pass the authentication protocol could indicate either transmission reception errors (bit flips) or spoofing.
5. A failure to validate a certain number of hash points should lead to deselection of the signal.
6. A Position Confidence output would be useful, and could characterize whether the receiver applied either Navigation Message Authentication or Signal Authentication, and whether it was applied for all signals or a partial subset of signals.

Notional State Transition Conditions

Notes:

(1) N/A

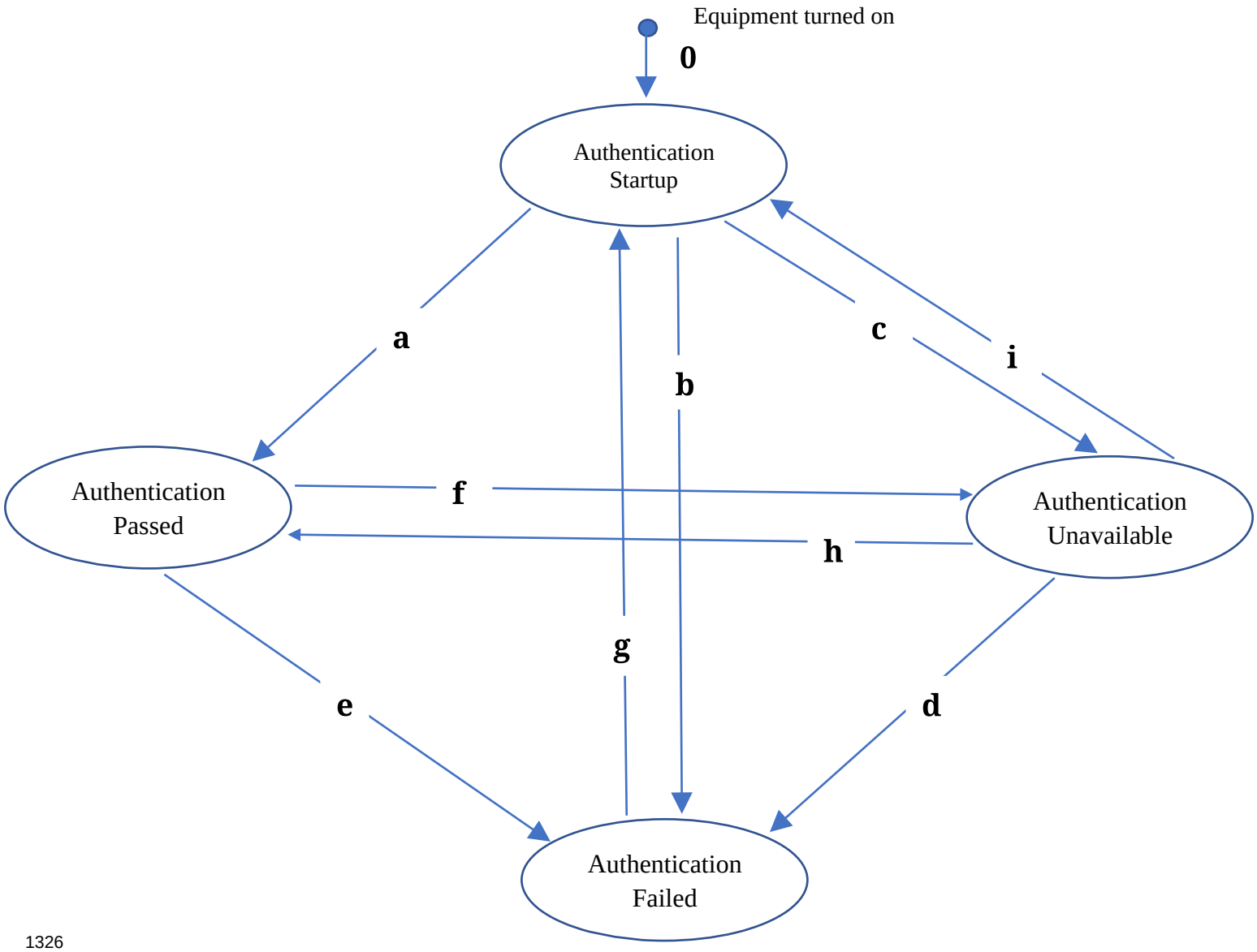
a	**Receiver has acquired and confirmed data for a minimum number of satellites on at least one frequency.**	**b**	**Receiver has sufficient satellite observations to generate a PVT solution with RAIM or ARAIM integrity.**
c	Receiver can no longer generate a PVT solution with RAIM or ARAIM integrity and SBAS integrity is not available. This could occur due to a detection and failed exclusion, interference, inability to track signals (e.g. scintillation), or receiver inherent spoofing detection invalidating some or all satellites.	**d**	Receiver has validated the TESLA Confirmed Hash Point and has validated the broadcast hash point received in the MT-20 or MT-50 to the TESLA Confirmed Hash Point. Receiver authenticates all of the required information to generate an SBAS solution.
e	Transition to another SBAS signal that meets all of condition **d** when a) SBAS solution from the SBAS signal in use is no longer valid (unable to authenticate data from signal, receipt of an MT-0, signal is no longer trackable), or b) there is a better PVT solution from another SBAS signal.	**f**	Transition to RAIM/ARAIM per condition **b** when a) Tracking an SBAS system that supports authentication and unable to authentication SBAS data (either failure to authenticate or loss of signal that should be present), or b) there is a better PVT solution using RAIM/ARAIM than the authenticated SBAS solution and SBAS is not required for the operation (includes exiting the SBAS coverage area).

g	Transition from an SBAS with authentication to an SBAS that does not support authentication when: a) the SBAS system is required (i.e. approach), or b) protection levels with the authenticated SBAS are no longer sufficient to support the operation and the unauthenticated SBAS will support the operation (e.g. edge of coverage) *Note: When there is a failure to authenticate, it is required to transition to RAIM/ARAIM rather than an unauthenticated SBAS signal.*	**h**	Transition to an SBAS system that supports authentication that meets all of condition **d** and is able to support the intended operation anytime a specific SBAS is not required for the operation. *Note: This reflects a preference to use a signal that provides authentication, provided it can support the operation and there is not a requirement to use a specific signal. However, there is not a requirement to do so.*
i	Transition from RAIM/ARAIM to an SBAS that does not support authentication when: a) the SBAS system is required (i.e. approach), or b) Receiver can no longer generate a PVT solution with RAIM or ARAIM integrity and SBAS integrity is available. *Note: There is a preference to use authenticated SBAS or RAIM/ARAIM before using unauthenticated SBAS.*	**j**	There is a better PVT solution using RAIM/ARAIM than the SBAS solution and SBAS is not required for the operation.
k	Transition to another SBAS signal when a) SBAS solution from the SBAS signal in use is no longer valid (receipt of MT-0, or the signal is no longer trackable), or b) there is a better PVT solution from another SBAS signal.	m	Loss of valid position while using an unauthenticated SBAS and transitions **h** or **j** are not available.
n	Expected when position solution returns after an m transition	0	Equipment turn-on, initial acquisition

1322

1323

1324 ATTACHMENT B: RECEIVER STATES AND TRANSITIONS - 1325 SINGLE CHANNEL MODEL



1326
1327 **States and Possible Transitions**
1328

1329
1330 **State Descriptions**

State	*Description*	*PVT Outputs*	*Authentication Status Output Value*
Startup	Tracking satellites, have not yet tried to authenticate (do not have all of the data describing the currently employed keys)	According to PVT output requirements for GPS RAIM or ARAIM	None
Authentication Unavailable	Insufficient valid authentication information is available to execute the authentication protocols	• Use a different SBAS channel or; • Provide PVT output from RAIM/ARAIM • Provide a valid PVT output with indication that it is unauthenticated according to legacy PVT output requirements	None
Authentication Passed	All authentication information is available and valid and the authentication has passed	Provide a valid PVT using authenticated SABS date according to legacy PVT output requirements	True
Authentication Failed	All authentication information is available and valid and the authentication has had a recent failure	• Use a different channel that has authentication, or; • No computed data —or — output but flagged consistent with legacy requirements when MI is detected, integrity alert with indication that it is due to failed authentication (latter would be preferred for reporting purposes)	False

1331
1332 **Notes on States and Possible Transitions**

1. In all states, the receiver continuously tries to execute the authentication protocols when the receiver has indication that the channel supports authentication (has received keys or MT-20/50 messages).
2. State description covers SBAS use only and does not extend to other uses of GNSS
    a. Does not include the incorporation of non-authentication based spoofing detection schemes
3. Authentication is initially evaluated on a per SBAS GEO basis. It is employed on a message by message basis where each individual message is accepted or discarded based upon whether or not it passes authentication.
4. Individual messages may pass authentication or may not be able to be authenticated. These do not by themselves cause a change in the receiver state as different messages have different levels of criticality in supporting quality and availability of the PVT solution.

Notional State Transition Conditions

Notes:

(2) Conditions bulleted with "+" are OR conditions. If any of the "+" conditions are met, a state transition occurs.

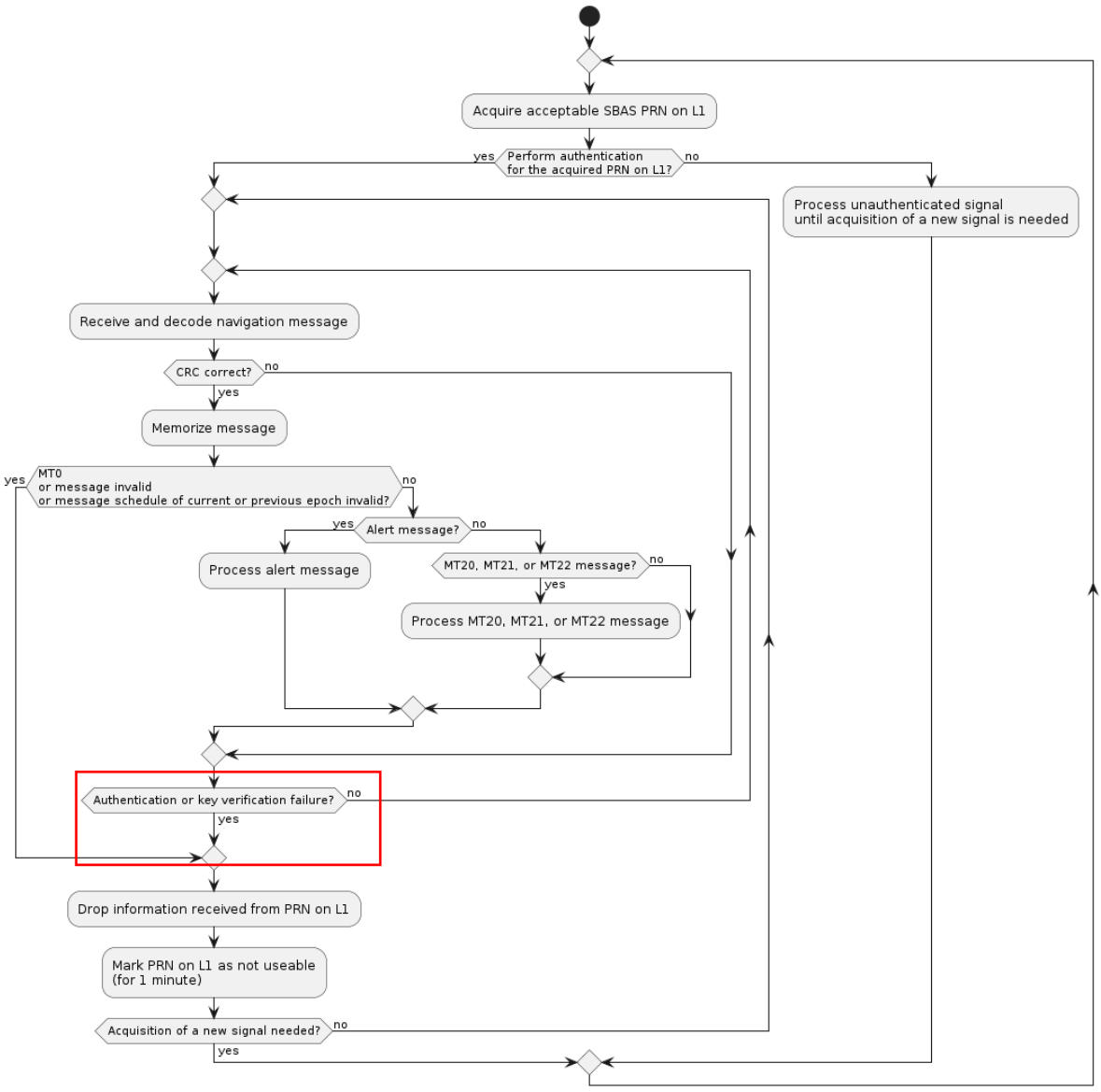
(3) This table only addresses the assessment of a single SBAS channel. On authentication fail for this channel, the equipment could look for another channel with authentication that passes the authentication protocol. However, when there is spoofing of an SBAS channel, there is also likely spoofing of core satellite constellation signals.

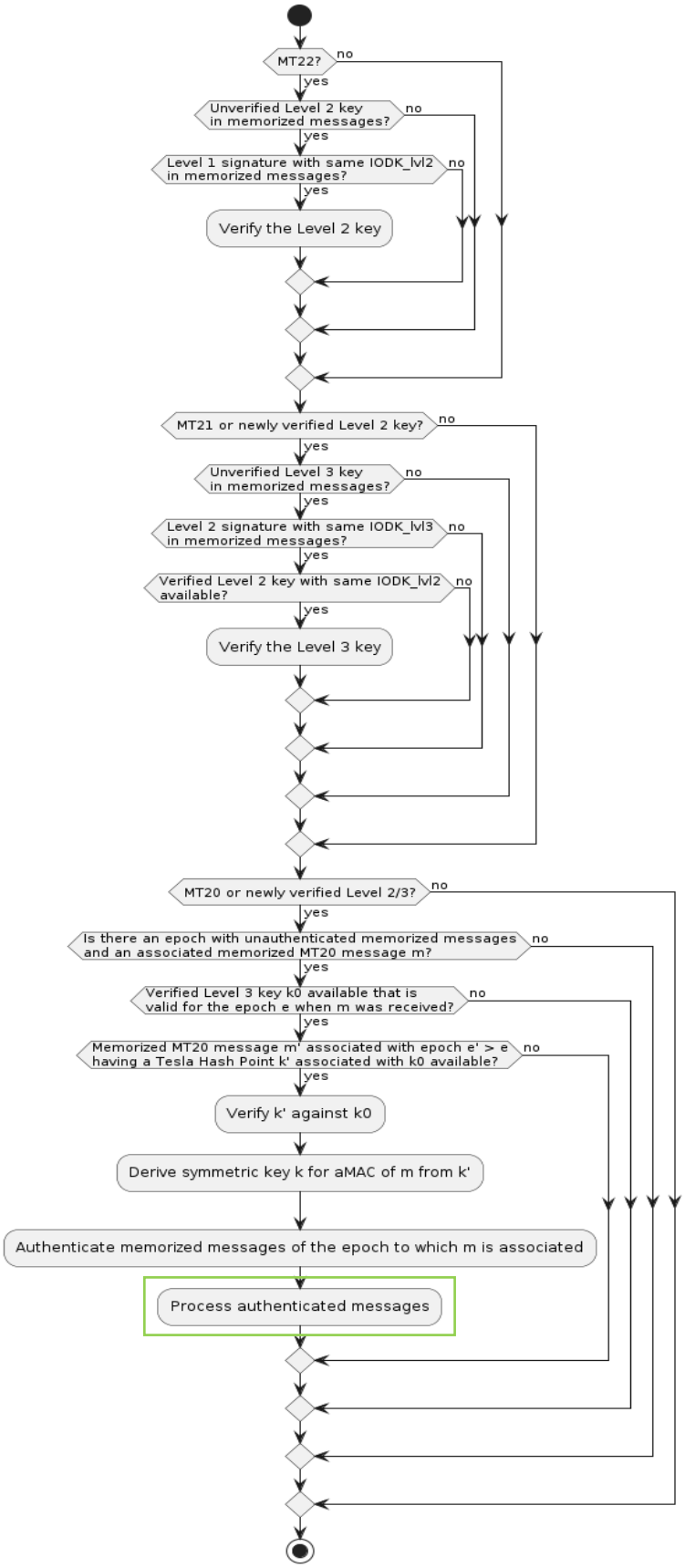
a	Receiver obtains all of the required information to use the current set of keys (verified the TELSA hash point) and has collected and authenticated sufficient SBAS messages, from at least one SBAS satellite, to form an SBAS PVT solution using authentication SBAS data.	**f**	Fly outside coverage of SBAS with authentication (better service from unauthenticated SBAS), or; + Aircraft has flown outside of area covered by the SBAS satellite providing authentication (or better service with unauthenticated SBAS) + Unauthenticated SBAS required for the operation
b	TELSA Hash Point is verified and +aMAC comparison fails when received in MT-20 (with valid CRC) +multiple MT-50 aMAC comparisons fail and unable to provide PVT output Or TESLA Hash Point does not hash to a confirmed TELSA Hash Point	**g**	+ If on the same signal/satellite/provider, one hour or 200 NM has transpired from entering the state *(previously this was 15 minutes) (Note: This is to support an in-flight reset possibility.)* + If another authenticated signal/satellite/provider is available
c	+ Receiver obtains all of the required	**h**	Same as a

	information to use the current set of keys and has not collected and authenticated sufficient SBAS messages to form an SBAS PVT solution + Unable to validate a TESLA Confirmed Hash Point or unable to validate Level 1 or Level 2 asymmetric keys (keys are unavailable) R + SBAS satellite doesn't provide authentication service		
d	Same as b	**i**	Current keys expire and the next set not yet obtained
e	Same as b	**0**	Tracking SBAS satellite (Revisit this in regard to covering the case of SV transition. for example after failure or leaving coverage region)

ATTACHMENT C: Example of receiver processing logic of an SBAS L1 signal with authentication

The following figures shows the processing logic of an SBAS L1 signal with authentication. The first figure provides the overall steps to be followed to authenticate SBAS data, the second figure provides more details on the "process MT20, MT21, MT22" step inserted in the first figure, detailing how the various key material is to be used.


Acquire acceptable SBAS PRN on L1
Perform authentication for the acquired PRN on L1?
yes
no
Process unauthenticated signal until acquisition of a new signal is needed
Receive and decode navigation message
CRC correct?
no
yes
Memorize message
MT0 or message invalid or message schedule of current or previous epoch invalid?
yes
no
Alert message?
yes
no
Process alert message
MT20, MT21, or MT22 message?
no
yes
Process MT20, MT21, or MT22 message
Authentication or key verification failure?
no
yes
Drop information received from PRN on L1
Mark PRN on L1 as not useable (for 1 minute)
Acquisition of a new signal needed?
no
yes


MT22?
no
yes
Unverified Level 2 key in memorized messages?
no
yes
Level 1 signature with same IODK_lvl2 in memorized messages?
no
yes
Verify the Level 2 key
MT21 or newly verified Level 2 key?
no
yes
Unverified Level 3 key in memorized messages?
no
yes
Level 2 signature with same IODK_lvl3 in memorized messages?
no
yes
Verified Level 2 key with same IODK_lvl2 available?
no
yes
Verify the Level 3 key
MT20 or newly verified Level 2/3?
no
yes
Is there an epoch with unauthenticated memorized messages and an associated memorized MT20 message m?
no
yes
Verified Level 3 key k0 available that is valid for the epoch e when m was received?
no
yes
Memorized MT20 message m' associated with epoch e' > e having a Tesla Hash Point k' associated with k0 available?
no
yes
Verify k' against k0
Derive symmetric key k for aMAC of m from k'
Authenticate memorized messages of the epoch to which m is associated
Process authenticated messages

Those diagrams cover initial receiver states discussed in previous versions of the SBAS authentication ConOps. For example, “authentication passed” corresponds to the green box in the figure above while the “authentication failed” corresponds to the red box.