SBAS Authentication SARPs

APPENDIX

**PROPOSED AMENDMENT TO
INTERNATIONAL STANDARDS
AND RECOMMENDED PRACTICES**

AERONAUTICAL TELECOMMUNICATIONS

**ANNEX 10
TO THE CONVENTION ON INTERNATIONAL CIVIL AVIATION**

**VOLUME I
(RADIO NAVIGATION AIDS)**

NOTES ON THE PRESENTATION OF THE AMENDMENT

The text of the amendment is arranged to show deleted text with a line through it and new text highlighted with grey shading, as shown below:

~~Text to be deleted is shown with a line through it.~~	text to be deleted
New text to be inserted is highlighted with grey shading.	new text to be inserted
~~Text to be deleted is shown with a line through it~~ followed by the replacement text which is highlighted with grey shading.	new text to replace existing text

CHAPTER 3. SPECIFICATIONS FOR RADIO NAVIGATION AIDS

. . .

3.7 Requirements for the Global Navigation Satellite System (GNSS)

3.7.1 Definitions

. . .

Integrity. A measure of the trust that can be placed in the correctness of the information supplied by the total system. Integrity includes the ability of a system to provide timely and valid warnings to the user (alerts).

. . .

3.7.3.4 Satellite-based augmentation system (SBAS)

Note.— All SBAS have to fulfil the requirements introduced in this section and in Appendix B, 3.5 except when a specific condition is mentioned in the requirement such as the provision of optional functions.

. . .

3.7.3.4.2 *Functions.* SBAS shall perform one or more of the following functions:

a) L1 SBAS ranging: provide an additional L1 ranging signal with an accuracy indicator from an SBAS satellite (3.7.3.4.3 and Appendix B, 3.5.7.2);

b) L1 SBAS GNSS satellite status: determine and transmit the GNSS satellite health status (Appendix B, 3.5.7.3);

c) L1 SBAS basic differential correction: provide GNSS satellite ephemeris and clock corrections (fast and long-term) to be applied to the L1 pseudo-range measurements from satellites (Appendix B, 3.5.7.4);

d) L1 SBAS precise differential correction: determine and transmit the L1 ionospheric corrections and associated integrity data (Appendix B, 3.5.7.5);~~.~~

e) DFMC SBAS ranging: provide additional ionosphere-free ranging capability using L1 and L5 signals from SBAS satellites (Appendix B, 3.5.14.2); ~~and~~

f) DFMC SBAS ionosphere-free differential correction: determine and transmit GNSS satellite health status, satellite ephemeris and clock corrections to be applied to the ionosphere-free pseudo-range measurements from satellites (Appendix B, 3.5.14.3) and associated integrity data; and

g) SBAS Message Authentication: provide authentication codes for SBAS messages (Appendix B, 3.5.7.6.4 or Appendix B, 3.5.14.6).

Note 1.— For single-frequency users, if functions b) and c) are provided, SBAS in combination with core satellite constellation(s) can support departure, en-route, terminal and non-precision approach operations, and if function d) is provided in addition to b) and c) then SBAS can also support precision approach operations including Category I. The level of performance that can be achieved depends upon the infrastructure incorporated into SBAS and the ionospheric conditions in the geographic area of interest.

Note 2.— For dual-frequency users, if function f) is provided, SBAS in combination with core satellite constellation(s) can support departure, en-route, terminal, non-precision approach operations, and precision approach operations including Category I.

Note 3.— In order to provide function e), SBAS needs to broadcast an L1 signal that meets the requirements for ionosphere-free ranging using L1 and L5 pseudo-range measurements.

Note 4.— The ionospheric corrections are only broadcast on L1. Dual-frequency users will use an ionosphere-free pseudo-range measurement and not require ionospheric corrections. Ionosphere-free pseudo-range combination for DFMC SBAS is further defined in Appendix B, 3.5.15.1.

Note 5. – Authentication can be implemented on the L1 SBAS service and/or DFMC SBAS service. Implementation of authentication on both services will provide higher protection of SBAS operations. Authentication keys and certificate may be applicable to both authentication services. See Attachment D, TBC.

. . .

APPENDIX B. TECHNICAL SPECIFICATIONS FOR THE GLOBAL NAVIGATION SATELLITE SYSTEM (GNSS)

. . .

3. GNSS ELEMENTS

. . .

3.5 Satellite-based augmentation system (SBAS)

3.5.1 General

. . .

3.5.3 Data structure on SBAS L1 signal

Note.— Messages broadcast on SBAS L1 signal are independent of those broadcast on SBAS L5 signal. Information broadcast on SBAS L1 signal is used only for the L1 SBAS service using GPS L1 C/A and GLONASS L1OF (FDMA signal).

3.5.3.1 *Format summary*. All messages shall consist of a message type identifier, a preamble, a data field and a cyclic redundancy check as illustrated in Figure B-25.

3.5.3.2 *Preamble.* For L1, the preamble shall consist of the sequence of bits "01010011 10011010 11000110", distributed over three successive blocks. The start of every other 24-bit preamble shall be synchronous with a 6-second GPS subframe epoch.

. . .

Table B-62. L1 broadcast message types

L1 Message type	Contents
0	"Do Not Use" (SBAS test mode) – Content applies to L1 SBAS service only
1	PRN mask
2 to 5	Fast corrections
6	Integrity information
7	Fast correction degradation factor
8	Spare
9	GEO ranging function parameters
10	Degradation parameters
11	Spare
12	SBAS network time/UTC offset parameters
13 to 16	Spare
17	GEO satellite almanacs
18	Ionospheric grid point masks
19 ~~to 23~~	Spare
20	Authentication Code
21	TESLA hash chain
22	SBAS Authentication Certificate

L1 Message type	Contents
23	Spare
24	Mixed fast/long-term satellite error corrections
25	Long-term satellite error corrections
26	Ionospheric delay corrections
27	SBAS service message
28	Clock-ephemeris covariance matrix
29 to 61	Spare
62	Reserved – content applies to L1 SBAS service only
63	Null message – content applies to L1 SBAS service only

Note.— L1 messages (Table B-24) are for use with L1 SBAS service and L5 messages (Table B-98) are for use with DFMC SBAS service. Types 0, 62 and 63 messages are used independently by both L1 SBAS and DFMC SBAS services and their contents only apply to their service.

3.5.4 L1 SBAS data content

. . .

{Editorial Note: All new text follows for 3.5.4.11 and 3.5.4.13}

3.5.4.11 *L1 SBAS Authentication Parameters*: The L1 SBAS authentication parameters shall be as follows.

3.5.4.11.1 *Authentication Code*: For authentication, the messages broadcasted by a L1 SBAS service are organised in authentication frames consisting of 6 consecutive messages.

3.5.4.11.1.1 Each authentication frame in a week is identified by a sequence number *af* being an integer in the interval [0, 100799] and ends with a regular slot for an Authentication Code message (Type 20 message). The regular slot is filled by an Authentication Code message unless there is an alert.

3.5.4.11.2 The authentication frame of a message is determined by

$$af = \left\lceil \frac{t - Authentication\ Message\ Slot}{6} \right\rceil,$$

where

- *af* identifies the authentication frame as described above,
- $\lceil x \rceil$ is the ceiling function mapping x to the least integer greater than or equal to x,
- *t* is the time of the week when the broadcast of the message starts in seconds since beginning of the week with respect to SNT, and
- *Authentication Message Slot:* parameter broadcast in TESLA hash chain message and is defined in 3.5.4.12.

3.5.4.11.3 The parameters of an Authentication Code message in an authentication frame identified by *af* shall be as follows.

Aggregated MAC (aMAC): Aggregated Message Authentication Code (MAC) in a Type 20 Message Slot for the first five L1 messages in the authentication frame.

TESLA Hash Point (HP): TESLA Hash Point associated with the authentication frame *af*' immediately preceding *af* (or, in case of alerts, with the authentication frame before the one preceding *af*).

Block Erasure Codes (BEC1, BEC2): Block erasure codes to recover the MACs of missed messages.

Note.— All parameters in 3.5.4.11.3 are broadcast in a Type 20 message.

3.5.4.12 *TESLA hash chain Parameters*: The TESLA hash chain parameters shall be as follows.

Issue of Data TESLA (IODT): Indicator of a specific TESLA hash chain. This is used to link TESLA Confirmed Hash Point with the associated hash chain signature.

Note 1.— Each IODT will refer to one valid TESLA Hash Chain for an SBAS provider as defined by the Salt and initial hash point.

Note 2.— There is a common IODT parameter set used by both L1 SBAS and DFMC SBAS services. If the same TESLA Hash Chain is used on multiple signals by the SBAS provider (e.g. on both the L1 signal and the L5 signal), then IODT value will be the same. Otherwise IODT value will be different on the signals.

Sequence Flag: Identifies a consistent set of TESLA hash chain messages for a given IODT.

Note.— The sequence flag is used to indicate a change in the broadcast TESLA hash chain parameters in the same TESLA hash chain identified by IODT.

Payload Number: A parameter between 1 and 8 that identifies the contents of the 203-bit message payload in the TESLA hash chain message. See Table B-y2.

Note.— The TESLA hash chain is broadcast in a sequence of 5 to 8 messages.

TESLA Confirmed Hash Point: Identifies a TESLA hash point in the TESLA hash chain identified by IODT. This hash point is digitally signed by the SBAS provider. The digital signature is distributed via payload parameters of TESLA hash chain messages. The hash chain signature can be verified using the provider's certificate distributed via SBAS Authentication Certificate messages.

Note.— The TESLA hash chain is the set of TESLA Hash Points derived from the TESLA initial hash point following the protocol in 3.5.5.7.

Authentication Message Slot: A value from 0 to 5 that indicates when the Authentication Code message is sent per 3.5.7.6.4.2.3. The Authentication code is sent when (t modulo 6) = authentication message slot value.

TESLA confirmed hash point time: Provided as a Week Number and Authentication Frame number, identifies the authentication frame associated with the TESLA Confirmed Hash Point provided in the message.

TESLA hash chain end time: Provided in units of Weeks and Authentication Frames, identifies the end time of the associated TESLA hash chain.

TESLA hash chain applicability: Identifies the applicable signals for this TESLA hash chain.

0 –Applies only to the SBAS signal on which it was received.
1 – Applies to both the L1 and L5 signals from the broadcasting SBAS PRN code.

2 – Applies to all SBAS PRN codes of the same corresponding service (i.e. L1 SBAS or DFMC SBAS service) from the broadcasting SBAS provider.
3 – Applies to all SBAS satellite signals and PRN codes associated to L1 SBAS and DFMC SBAS services from the broadcasting SBAS provider.

MAC Generation Function: Identifies the cryptographic approach used for MAC generation for the associated signal

0 – HMAC with SHA-256
1 – HMAC with SHA3-256
2 – KMAC256
3 to 15 – Reserved

Note.— For SHA (SHA2) family of hash functions, see NIST FIPS 180-4. For SHA3 family of hash functions, see NIST-FIPS 202. HMAC is the Keyed-Hash MAC function as defined by NIST FIPS 198-1. KMAC is the Keccak Message Authentication Code as defined by NIST SP 800-185.

Key derivation Function: Identifies the cryptographic approach used for key generation for the associated signal

0 – HMAC with SHA-256
1 – HMAC with SHA3-256
2 – KMAC256
3 to 15 – Reserved

TESLA Hash Function (H): Identifies the cryptographic hash function used to create the TESLA hash chain on the associated signal.

0 – SHA-256
1 – SHA3-256
2 to 15 – Reserved

Note.— For SHA (SHA2) family of hash functions, see NIST FIPS 180-4 or RFC-5754. For SHA3 family of hash functions, see NIST-FIPS 202.

TESLA hash chain Salt (S): Identifies a cryptographically secure pseudorandom 128-bit number drawn for each TESLA hash chain.

Issue of Data Public Key (IODPK): Identifier of the SBAS authentication certificate. It is used to sign the TESLA hash chain.

Note.— There is a common IODPK parameter set used by both L1 SBAS and DFMC SBAS services. If the same SBAS authentication certificate is used for L1 SBAS and DFMC SBAS services by the SBAS provider, then IODPK value will be the same. Otherwise IODPK value will be different on the different SBAS services.

Issue of Data TESLA (IODT) validity flag: Flag to indicate whether there is a valid TESLA hash chain associated with this IODT.

IODT validity flag time: Provided in units of Weeks and Authentication Frames, identifies the time of the IODT validity flag parameter.

TESLA hash chain signature: Signature of Payload 1 and 2 contents divided into 203-bit segments. The signature is a sequence of two elements *signatureAlgorithm* and *signatureValue* encoded according to CBOR C509:

[signatureAlgorithm: AlgorithmIdentifier, signatureValue: any]

With:

- *signatureAlgorithm* indicates the algorithm used for computing the signature and is of type *AlgorithmIdentifier* as defined by the CBOR C509
- *signatureValue* is of type *any*. Its interpretation depends on the signature algorithm indicated by *signatureAlgorithm*.

Note.— All parameters in 3.5.4.12 are broadcast in a TESLA hash chain message.

3.5.4.13 *SBAS authentication certificate Parameters*: The SBAS authentication certificate is broadcasted as a CBOR C509-encoded X.509 digital certificate divided into up to sixteen 205-bit certificate segments and the associated parameters shall be as follows.

Note 1.— The CBOR C509 encoding is only available as an IETF RFC draft for the moment.

Issue of Data Public Key (IODPK): Indicator of the SBAS authentication certificate.

Certificate segment number: A parameter between 0 and 15 that identifies the sequence of the 205-bit certificated segment in the SBAS authentication certificate message.
Note.— The SBAS authentication certificate is broadcast in a sequence of 7 to 16 messages.

Certificate segment: Content corresponding to the certificate segment number.

Note 2. — All parameters in 3.5.4.13 are broadcast in a SBAS Authentication Certificate message.

{Editorial Note: End new material}

…

3.5.5 Definitions of protocols for L1 SBAS data application

{Editorial Note: All new text follows for 3.5.5.7}

3.5.5.7 Authentication Protocols

3.5.5.7.1 Computation of the TESLA hash chain

Note. – Repetitive application of the hash point calculation (hashes or hash operation) develops the TESLA hash chain.

The TESLA Hash Point associated with the previous authentication frame (HP') shall be computed from the hash point (HP) from the current authentication frame defined by WN and af as follows

$$HP' = \mathrm{Trunc}_{128}\big(\mathrm{H}(HP \| WN \| af \| S)\big),$$

where

- $\mathrm{Trunc}_{128}(X)$ is the function mapping a string X to the string comprised of bits X[0] to X[127] with X[i] being the bit of X with index i,
- $\mathrm{H}(X)$ is the TESLA hash function identified by the TESLA hash chain message,
- $X \| Y$ is the concatenation of bit string X and bit string Y,
- HP is the TESLA Hash Point is associated with the authentication frame defined by WN

and af encoded as a 128-bit unsigned integer,
- WN is the SNT week number encoded as a 16-bit unsigned integer,
- af is encoded as a 24-bit unsigned integer, and
- S is the TESLA hash chain Salt associated with the TESLA Hash Chain, encoded as a 128 − bit unsigned integer.

Note .— All integer values are encoded with the most significant bit first.

When HP' is computed, the associated authentication frame (af') and week number (WN') shall be computed as follow:

$af' = af$ – 1 and WN' = WN, if $af > 0$
af' = 100799 and WN' = WN - 1, if $af = 0$

3.5.5.7.2 Computation of the message keys

Consider a 250-bit SBAS message that is broadcasted at *t* seconds SNT after beginning of week *WN* in the authentication frame *af* by the SBAS SV with PRN code *PRN* on frequency *F*. The cryptographic key k for a particular message on a particular signal and satellite shall be as follows

$$k = \text{HMAC}(HP, Label \| 0x00 \| Context \| L) \; or$$
$$k = \text{KMAC}(HP, Context, L, Label)$$

where
- HMAC is the Keyed-Hash MAC function as defined by NIST FIPS 198-1 using the HMAC hash function identified by the TESLA hash chain message,
- KMAC is the Keccak Message Authentication Code as defined by NIST SP 800-185 and identified by the TESLA hash chain message,
- $X \| Y$ is the concatenation of bit string X and bit string Y,
- *HP* is the TESLA Hash Point associated with *af* in week *WN*,
- *Label*: A string that identifies the purpose for the derived keying material, which is encoded as a bit string: For L1 SBAS, it is the 56-bit "Label" value of 0x4D5432304B6579 (ASCII representation of "MT20Key") and for DFMC SBAS, it is the 56-bit "Label" value of 0x4D5435304B6579 (ASCII representation of "MT50Key"),
- *0x00:* 8-bits 0 spacer,
- *Context:* A bit string being the concatenation of broadcast time t of the message (in SNT seconds of week expressed as a 24-bit unsigned integer), broadcasting PRN encoded as a 16-bit unsigned integer, and the frequency of the signal, written as t||PRN||FL1 for the L1 frequency signal and t||Satellite Slot Number||FL5 for the L5 frequency signal,
- *FL1* equals 1,575,420 indicating the SBAS L1 signal frequency, encoded as a 24-bit unsigned integer,
- *FL5* equals 1,176,450 indicating the SBAS L5 signal frequency, encoded as a 24-bit unsigned integer, and
- *Key Length (L):* The intended key length with keys being 256-bits for KMAC-256, SHA-256 or SHA3-256 and 512-bits for SHA-512 or SHA3-512, encoded as a 16-bit unsigned integer.

Note.— All integer values are encoded with the most significant bit first.

3.5.5.7.3 Computation of the Message Authentication Codes

The aggregated MAC *aMAC* of an Authentication code message is computed over MACs of the broadcasted messages. Consider a 250-bit SBAS message that is broadcasted at *t* seconds SNT after beginning of week

WN in the authentication frame *af* by the SBAS SV with PRN code *PRN* on frequency *F*. The MAC *M* of a message *m is* computed by

$$M = \mathrm{Trunc}_{28}\big(\mathrm{HMAC}(k, m\|000000)\big)\ or$$
$$M = \mathrm{KMAC}(k, m\|000000, 28, \{\})$$

where

- $\mathrm{Trunc}_{28}(X)$ is the function mapping a string X to the string comprised of bits X[0] to X[27] with X[i] being the bit of *X* with index *i*,
- HMAC is the Keyed-Hash MAC function as defined by NIST FIPS 198-1 using the HMAC hash function identified by the Type 21 message,
- KMAC is the Keccak Message Authentication Code as defined by NIST SP 800-185 using the KMAC hash function identified by the Type 21 message,
- *k* is the cryptographic key for the broadcast time, satellite and signal as defined in 3.5.5.7.2,
- $X\|Y$ is the concatenation of bit string X and bit string Y,
- *m* is the message broadcast at time t on the satellite and signal associated with the key k, encoded as a 250-bit string, and
- *000000* is a 0 (zero) encoded as 6-bit string.

3.5.5.7.4 Computation of the aggregated Message Authentication Code (aMAC)

The aggregated MAC *aMAC* broadcasted in a Type 20 message *m* is computed as

$$aMAC = \mathrm{Trunc}_{28}\big(\mathrm{HMAC}(k, M_1\|M_2\|M_3\|M_4\|M_5\|0000)\big)\ or$$
$$aMAC = \mathrm{KMAC}(k, M_1\|M_2\|M_3\|M_4\|M_5\|0000, 28, \{\})$$

where

- $\mathrm{Trunc}_{28}(X)$ is the function mapping a string X to the string comprised of bits X[0] to X[27] with X[i] being the bit of *X* with index *i, where indices increase from left to right (i.e., X[0] is the left-most bit of X, followed by X[1], etc.)*,
- HMAC is the Keyed-Hash MAC function as defined by NIST FIPS 198-1 using the HMAC hash function identified by the Type 21 message,
- KMAC is the Keccak Message Authentication Code as defined by NIST SP 800-185 using the KMAC hash function identified by the Type 21 message,
- *k* is the cryptographic key associated with *m* as defined above,
- $X\|Y$ is the concatenation of string X and string Y, and
- M_i is the MAC of the *i*th message in the authentication frame associated with the regular slot of *m* computed as described above and encoded as a 28-bit unsigned integer.

Note.— All integer values are encoded with the most significant bit first.

3.5.5.7.5 Block Erasure Codes

The block erasure codes BEC1 and BEC2 broadcasted in a Type 20 message are computed as

$$BEC1 = M_1 \oplus M_2 \oplus M_3 \oplus M_4 \oplus M_5 \text{ and}$$

$$BEC2 = b_1 \| b_2 \| b_3 \| b_4 \text{ with}$$

$$b_1 = b \oplus M_1^0 \oplus M_3^3 \oplus M_4^2 \oplus M_5^1,$$

$$b_2 = b \oplus M_1^1 \oplus M_2^0 \oplus M_4^3 \oplus M_5^2,$$

$$b_3 = b \oplus M_1^2 \oplus M_2^1 \oplus M_3^0 \oplus M_5^3,$$

$$b_4 = b \oplus M_1^3 \oplus M_3^2 \oplus M_3^1 \oplus M_4^0,$$

$$b = M_2^3 \oplus M_3^2 \oplus M_4^1 \oplus M_5^0.$$

where

- M_i is the MAC of the *i*th message in the authentication frame associated with the regular slot computed as described above and encoded as a 28-bit unsigned integer,
- M_i^j equals the 7 least significant bits of $M_i/2^{7j}$ encoded as a 7-bit unsigned integer,
- $X \| Y$ is the concatenation of bit string X and bit string Y, and
- $X \oplus Y$ is the string that results from applying the Boolean Exclusive-Or operation to each bit position of bit string X and bit string Y.

Note 1.— All integer values are encoded with the most significant bit first.
Note 2. – See Attachment D TBC for more details.

{Editorial Note: End New Material}

…

3.5.6 L1 SBAS message tables

…

Table B-75. Type 0 "Do Not Use" message broadcast on L1

Data content	Bits used	Range of values	Resolution
Reserved	212	—	—

{Editorial: Message formats for the authentication and key management messages. All new material follows.}

Table B-x1. Type 20 SBAS L1 Authentication Code Message

Section	Name	Length	Scale factor	Effective range min	Effective range max	Unit	Comment
Aggregated Message Authentication Code	aMAC	28	1	0	2^{28}-1	-	Current authentication frame
Block Erasure Code	BEC1	28	1	0	2^{28}-1	-	

	BEC2	28	1	0	2^{28}-1	-	
TESLA Hash Point	HP	128	1	0	2^{128}-1	-	Previous authentication frame

Note 1.— All parameters are defined in 3.5.4.11.

Table B-y1. Type 21 TESLA Hash Chain message (Overall Message Structure)

Section	Name	Length	Scale factor	Effective range		Unit	Comment
				min	max		
Header / Meta Data	Issue of Data, TESLA	5	1	0	31	-	
	Sequence Flag	1	1	0	1	-	
	TESLA Hash Chain Payload Number	3	1	1	8	-	
Payload	TESLA Hash Chain Payload	203	1	0	2^{203}-1	-	See Table B-y2

Note.— All parameters are defined in 3.5.4.12.

Table B-y2. TESLA Hash Chain Payload Structure

Section	Name	Length	Scale factor	Effective range		Unit	Comment
				min	max		
Payload Number 1	TESLA Confirmed Hash Point	128	1	0	2^{128}-1		
	Authentication Message Slot	3	1	0	5	-	Coding range (0 to 7) exceeds effective range.
	TESLA Confirmed Hash Point, Week Number	16	1	0	65535	Week	
	TESLA Confirmed Hash Point, Frame	17	1	0	100799	Frame	Coding range (0 to 131,071) exceeds effective range.
	Hash Chain End Time, Week Number	7	1	0	127	Week	Coding range (0 to 4095) exceeds effective range.
	Hash Chain End Time, Frame	17	1	0	100799	Frame	Coding range (0 to 131,071) exceeds effective range.
	TESLA Hash Chain Applicability	2	1	0	3		
	Key Derivation Function	4	1	0	15	-	
	TESLA Hash Function	4	1	0	15		
	Spare	5	-	-	-	-	
Payload Number 2	Salt	128		0	2^{128}-1	-	
	IODPK	3	1	0	7	-	IODPK of SBAS Authentication Certificate
	For 32 IODT IODT validity flag	1	1	0	1	-	0 - IODT is invalid 1 – IODT is valid

	IODT validity flag time, Week Number	16	1	0	65535		
	IODT validity flag time, Frame	17	1	0	100799		Coding range (0 to 131,071) exceeds effective range.
	MAC Generation Function	4	1	0	15		
	Spare	3	-	-	-	-	-
Payload Number 3	Signature, Segment 1	203		Note 2	Note 2		SBAS Authentication Certificate Signature of Payload 1 & 2
Payload Number 4	Signature, Segment 2	203		Note 2	Note 2		SBAS Authentication Certificate Signature of Payload 1 & 2
Payload Number 5	Signature, Segment 3	203		Note 2	Note 2		SBAS Authentication Certificate Signature of Payload 1 & 2
Payload Number 6	Signature, Segment 4	203		Note 2	Note 2		SBAS Authentication Certificate Signature of Payload 1 & 2
Payload Number 7	Signature, Segment 5	203		Note 2	Note 2		SBAS Authentication Certificate Signature of Payload 1 & 2
Payload Number 8	Signature, Segment 6	203		Note 2	Note 2		SBAS Authentication Certificate Signature of Payload 1 & 2

Note 1.— All parameters are defined in 3.5.4.12.
Note 2.— For Ed25519 as defined in the ICAO Doc 10169 , the signature type and signature are TBD bits from Payloads 3, 4, and 5. A maximum signature of 1218-bits can be supported. Unused bits in a payload are "0". Unused payloads are not sent.

Table B-z1. Type 22 SBAS Authentication Certificate message

Section	Name	Length	Scale factor	Effective range		Unit	Comment
				min	max		
Header / Meta Data	Issue of Data, Public Key	3	1	0	7	-	
	Certificate Segment Number	4	1	0	15	-	
Certificate	Certificate Segment	205	1	0	2^{205}-1	-	

Note.— All parameters are defined in 3.5.4.13.

{Editorial Note: End new Material}

…

Table B-90. Type 63 null message

Data content	Bits used	Range of values	Resolution
Reserved	212	—	—

…

3.5.7 L1 SBAS non-aircraft elements

…

3.5.7.3.1 *Performance of satellite status functions*. Given any valid combination of active data, the probability of a horizontal error exceeding the HPLSBAS (as defined in 3.5.5.6) for longer than 8 consecutive seconds shall be less than 10^{-7} in any hour, assuming a user with zero latency.

Note 1.— Active data is defined to be data that have not timed out per 3.5.8.1.2. This requirement includes core satellite constellation(s) and SBAS failures.

Note 2. —The time-out for authenticated UDREI is longer as per 3.5.8.5.3.

…

Table B-92. Data broadcast intervals and supported functions

Data type	Maximum broadcast interval	Ranging	GNSS satellite status	Basic differential correction	Precise differential correction	L1 SBAS authentication	Associated message types
Clock-Ephemeris covariance matrix	120 s						28
SBAS in test mode	6 s						0
PRN mask	120 s		R	R	R		1
UDREI	6 s		R*	R	R		2 to 6, 24
Fast corrections	$I_{fc}/2$ (see *Note 4*)		R*	R	R		2 to 5, 24
Long-term corrections	120 s		R*	R	R		24, 25
GEO ranging function data	120 s	R	R	R	R		9
Fast correction degradation	120 s		R*	R	R		7
Degradation parameters	120 s				R		10
Ionospheric grid mask	300 s				R		18
Ionospheric corrections, GIVEI	300 s				R		26
Timing data	300 s	R (see *Note 3*)	R (see *Note 3*)	R (see *Note 3*)	R (see *Note 3*)		12
Almanac data	300 s	R	R	R	R		17
Service level	300 s						27
Authentication codes	6 s					R	20
TESLA hash chain	300 s					R	21
SBAS Authentication Certificate	600 s					R	22

Notes.—

1. *"R" indicates that the data must be broadcast to support the function.*
2. *"R*" indicates special coding as described in 3.5.7.3.3.*
3. *Type 12 messages are only required if data are provided for GLONASS satellites.*
4. *I_{fc} refers to the PA/APV time-out interval for fast corrections, as defined in Table B-95.*

…

3.5.7.4.1 *Performance of basic differential correction function*. Given any valid combination of active data, the probability of a horizontal error exceeding the HPLSBAS (as defined in 3.5.5.6) for longer than 8 consecutive seconds shall be less than 10^{-7} in any hour, assuming a user with zero latency.

Note 1.— Active data is defined to be data that has not timed out per 3.5.8.1.2. This requirement includes core satellite constellation(s) and SBAS failures.

Note 2. —The time-out for authenticated UDREI is longer as per 3.5.8.5.3.

…

3.5.7.5.1 *Performance of precise differential correction function*. Given any valid combination of active data, the probability of an out-of-tolerance condition for longer than the relevant time-to-alert shall be less than 2×10^{-7} during any approach, assuming a user with zero latency. The time-to-alert shall be 5.2 seconds for an SBAS that supports precision approach operations, and 8 seconds for an SBAS that supports APV or NPA operations. An out-of-tolerance condition shall be defined as a horizontal error exceeding the HPL_{SBAS} or a vertical error exceeding the VPL_{SBAS} (as defined in 3.5.5.6). When an out-of-tolerance condition is detected, the resulting alert message (broadcast in a Type 2 to 5 and 6, 24, 26 or 27 messages) shall be repeated three times after the initial notification of the alert condition for a total of four times in 4 seconds.

Note 1.— Active data is defined to be data that has not timed out per 3.5.8.1.2. This requirement includes core satellite constellation(s) and SBAS failures.

Note 2.— Subsequent messages can be transmitted at the normal update rate.

Note 3. —The time-out for authenticated UDREI is longer as per 3.5.8.5.3.

…

3.5.7.6 *OPTIONAL FUNCTIONS*

3.5.7.6.1 *Timing data*. If UTC time parameters are broadcast, they shall be as defined in 3.5.4.8 (Type 12 message).

3.5.7.6.2 *Service indication*. If service indication data are broadcast, they shall be as defined in 3.5.4.9 (Type 27 message) and Type 28 messages shall not be broadcast. The IODS in all Type 27 messages shall increment when there is a change in any Type 27 message data.

3.5.7.6.3 *Clock-ephemeris covariance matrix*. If clock-ephemeris covariance matrix data are broadcast, they shall be broadcast for all monitored satellites as defined in 3.5.4.10 (Type 28 message) and Type 27 messages shall not be broadcast.

3.5.7.6.4 *SBAS authentication.* The SBAS shall comply with the following requirements when the SBAS provides the authentication function on its L1 SBAS service:

3.5.7.6.4.1 *Key management requirements*

3.5.7.6.4.1.1 The SBAS shall securely request, renew, rekey and revoke digital certificates as per its Certificate Authority (CA) policy, processes and procedures.

3.5.7.6.4.1.1.1 The SBAS shall protect the private keys associated to digital certificates, and TESLA hash chains stored to support its authentication service(s) against unauthorised access.

3.5.7.6.4.1.2 The SBAS shall sign the TESLA hash chain with the private key associated with a valid SBAS Authentication Certificate provided by its Certificate Authority.

3.5.7.6.4.1.3 *Self-signed root certificate and entity signing CA certificate requirements*

3.5.7.6.4.1.3.1 The SBAS shall use digital certificates compliant with the certificate profile "Self-signed Root Certificate" as defined in ICAO Doc 10169 for the self-signed root certificate public keys with the following specifications for the Subject Public Key Information:

- ECC (id-ecPublicKey {1 2 840 10045 2 1}) with parameters
  - secp256r1/P-256 {1 2 840 10045 3 1 7} or
  - secp521r1/P-521 {1 3 132 0 35} or
  - secp384r1/P-384 {1 3 132 0 34} or
- Ed448 (id-Ed448 {1 3 101 113}).

Note. – The above further restricts the ICAO Doc 10169 approved methods.

3.5.7.6.4.1.3.2 The SBAS shall use digital certificates compliant with the certificate profile "<ENTITY> Signing CA" as defined in ICAO Doc 10169 for the issuer certificate with the following specifications for Subject Public Key Information:

- ECC (id-ecPublicKey {1 2 840 10045 2 1}) with parameters secp384r1/P-384 {1 3 132 0 34} or
- Ed448 (id-Ed448 {1 3 101 113}) or
- Ed25519 (id-Ed25519 {1 3 101 112})

3.5.7.6.4.1.3.3 The SBAS shall use digital certificates compliant with the certificate profile "<ENTITY> Signing CA" as defined in ICAO Doc 10169 for any public key between the Self-signed root certificate and the entity signing CA certificate with the following specifications for Subject Public Key Information:

- ECC (id-ecPublicKey {1 2 840 10045 2 1}) with parameters
  - secp256r1/P-256 {1 2 840 10045 3 1 7} or
  - secp521r1/P-521 {1 3 132 0 35}, or
  - secp384r1/P-384 {1 3 132 0 34}, or
- Ed25519 (id-Ed25519 {1 3 101 112}), or
- Ed448 (id-Ed448 {1 3 101 113}).

Note. – The above further restricts ICAO Doc 10169 approved methods.

3.5.7.6.4.1.3.4 The SBAS shall include in its entity signing CA certificate digital certificate a Subject Alternative Name with an otherName with OID {iso(1) identified-organization(3) icao(27) security(16) PKI(1) Common Security Requirements(1) gnss(1) sbas(4) spid(1)} and the SBAS Provider Identifier for each SBAS Provider for which it signs SBAS authentication certificate.

3.5.7.6.4.1.3.5 The SBAS shall ensure that the self-signed root certificate and entity signing CA certificate (and any intermediate certificate) are made available prior to the SBAS using the certificates to sign the SBAS authentication data.

Note 1. – In case of deactivation of SBAS authentication function, a certain amount of time needs to be assumed for such deactivation at receiver level as it will be handled by receiver maintenance actions.

Note 2. – Self-signed root certificate and entity signing CA certificate need to be published and distributed each time new certificates are created from authentication service activation until authentication service decommission.

Note 3. – See Attachment D TBC need guidance material on the time to be considered in case of activation/deactivation/revocation.

3.5.7.6.4.1.4 SBAS authentication certificate requirements

3.5.7.6.4.1.4.1 The SBAS shall use digital certificates compliant with the certificate profile "SBAS Authentication Certificates" as defined in ICAO Doc 10169 for the SBAS authentication certificate.

Note 1. – See Attachment D section TBC.

Note 2. – SBAS only supports id-Ed25519 for the algorithmIdentifier.

3.5.7.6.4.1.4.2 The SBAS shall assign the SBAS authentication certificate to an IODPK value not already assigned to a valid certificate.

3.5.7.6.4.1.4.3 The SBAS shall broadcast the SBAS Authentication Certificate at least once before using it to sign the TESLA hash chain.

Note. – See attachment D TBC for further details.

3.5.7.6.4.1.4.4 The SBAS shall broadcast TESLA hash chain and SBAS authentication certificate as defined in 3.5.4.12 and 3.5.4.13.

3.5.7.6.4.1.5 TESLA hash chain requirements

3.5.7.6.4.1.5.1 When the SBAS updates parameters in the TESLA Hash Chain for a given IODT, the SBAS shall toggle the sequence flag parameter.

3.5.7.6.4.1.5.2 The SBAS shall update the IODT validity flag time at least daily.
Note. – SBAS may update the TESLA Confirmed Hash Point while updating the IODT validity flag time in the same update to reduce the number of computations to authenticate the hash point at the user level.

3.5.7.6.4.1.5.3 The SBAS shall use new pseudorandom numbers for the Salt and for the hash chain initial hash point from cryptographically secure pseudorandom number generators when creating a new TESLA hash chain.

Note. – A cryptographically secure pseudorandom number generator requires to be (re)seeded by random inputs.

3.5.7.6.4.1.5.4 SBAS shall not use the first broadcast TESLA Confirmed Hash Point from a TESLA hash chain for key derivation.

3.5.7.6.4.1.5.5 The SBAS shall only broadcast a hash point used for key derivation as the TESLA Confirmed Hash Point after broadcast in the SBAS Authentication code message.

3.5.7.6.4.1.5.6 The SBAS shall generate a hash chain not longer than 60 weeks (6 048 000 hashes).

3.5.7.6.4.1.5.7 The SBAS shall generate the TESLA hash chain per 3.5.5.7 in a secure manner starting with a Salt and initial hash point that represents the TESLA Hash Point for the Week Number and Authentication Frame associated with the TESLA hash chain end time.

3.5.7.6.4.1.5.8 The SBAS shall start broadcasting the TESLA Confirmed Hash Point for a new TESLA Hash Chain (IODT) to achieve broadcast of 5 copies of the new TESLA hash chain within 60 minutes prior to transitioning to the new TESLA hash chain.

3.5.7.6.4.1.5.8.1 The SBAS shall broadcast two TESLA Confirmed Hash Points when transitioning to a new TESLA hash chain, one for each TESLA hash chain (IODT).

.

3.5.7.6.4.1.5.9 Except for the TESLA Confirmed Hash Point, the SBAS shall keep secret TESLA hash points prior to being revealed in an authentication code message.

3.5.7.6.4.1.5.10 The SBAS shall compute the signature value of the signature transmitted via Payload Number 3 and the following payloads of a TESLA hash chain message over the TESLA hash chain messages with Payload Number 1 and Payload Number 2 having the same *IODT* and *sequence flag* as follows

$$signatureValue = S(sk, Context \,||\, SPID \,||\, pn_1 || pn_2),$$

where

- S() is the digital signature algorithm indicated by the *algorithmIdentifier* in the same signature,
- *sk* is the private key associated with the SBAS authentication certificate indicated by IODPK in the TESLA hash chain Payload Number 2,
- *Context* is the 72-bits string 0x4C6576656C334B65790A (ASCII representation of "Level3Key"),
- *SPID* is the SBAS Provider Identifier encoded as 8-bit unsigned integer,
- pn_1 is the TESLA hash chain message data field (212 bits) of Payload Number 1, and
- pn_2 is the TESLA hash chain message data field (212 bits) of Payload Number 2.

Note 1.— The SBAS Provider Identifier is the SPID broadcast in Type 17 message for L1 SBAS and Type 39 or 47 messages for DFMC SBAS.

Note 2.— All integer values are encoded with the most significant bit first.

3.5.7.6.4.1.6 IODT requirements

3.5.7.6.4.1.6.1 The SBAS shall indicate whether a TESLA hash chain is valid through use of its associated IODT validity flag.

3.5.7.6.4.1.6.2 The SBAS shall assign at most one valid TESLA hash chain for each IODT value.

3.5.7.6.4.1.6.3 SBAS shall broadcast TESLA hash chain for each signal to which the TESLA hash chain is applied, consistent with the TESLA hash chain applicability.

3.5.7.6.4.2 *Authentication service provision requirements*

3.5.7.6.4.2.1 *Authentication signal*. When providing SBAS authentication on L1 signals, SBAS shall support authentication on all operational SBAS L1 PRNs.

3.5.7.6.4.2.2 *Authentication data*. If an SBAS provides an authentication function, it shall broadcast authentication code data as defined in 3.5.4.11.

3.5.7.6.4.2.3 SBAS shall broadcast the SBAS authentication code data in the identified Authentication Message Slot defined in 3.5.4.12 except if condition in 3.5.7.6.4.2.4 applies.

3.5.7.6.4.2.4 If the SBAS has to broadcast a different message than a Type 20 message as part of an alert sequence in the Authentication Message Slot, the SBAS shall broadcast a Type 20 message as the first message after the alert sequence (see 3.5.7.5.1).

Note.— During an alert sequence, it may be necessary to broadcast a message with UDREI data (Type 2,3,4,5,6 or 24) or GIVEI data (Type 26) in place of the Type 20 message. See Attachment D, Section TBD for demonstration of messages during an alert sequence.

3.5.7.6.4.2.5 The SBAS shall generate keys (k) and MACs (M) per 3.5.5.7 for all SBAS messages except for the SBAS message broadcast in the Authentication message slot as identified in the Type 21 message.

3.5.7.6.4.2.6 The SBAS shall generate the key (k) and aMAC associated with the broadcast time of the Type 20 message as per 3.5.5.7.

Note.— During an alert sequence, the Type 20 message may be delayed and broadcast in the subsequent authentication frame. See 3.5.7.6.4.2.4 and Attachment D, Section TBD for alert processing.

3.5.7.6.4.2.7 The SBAS shall broadcast fast corrections at a rate consistent with Table B-AA as a function of the fast correction degradation factor indicator parameter (ai_i) broadcast in the Type 7 message.

Table B-AA: Fast Degradation Factors with SBAS Authentication

ai_i	**Range of fast correction allowed broadcast [s]**	**a_i [mm/s2]**
0	42 to 48	0.0
1	42 to 48	0.05
2	36 to 42	0.09
3	36	0.12
4	36	0.15
5	30	0.20
6	24	0.30

Note 1. – If the SBAS wants to support an authentication function for the L1 SBAS service, the SBAS correction and bounding mechanisms need to be compatible with at least one ai_i value between 0 and 6.

Note 2. – The timeout associated to fast correction degradation factor indicator (ai_i) indicated in Table B-95 still applies.

Note 3. – See Attachment D TBD

3.5.7.7 *MONITORING*

…

3.5.7.8 *Robustness to core satellite constellation(s) failures*. Upon occurrence of a core satellite constellation(s) satellite anomaly, SBAS shall continue to operate normally using the available healthy satellite signals that can be tracked.

3.5.8 L1 SBAS Aircraft elements

…

3.5.8.1.2 *Conditions for use of data*. The receiver shall use data from an SBAS message only if the CRC of this message has been verified. Reception of a Type 0 message from an SBAS satellite shall result in deselection of that satellite for at least one minute and all data from that satellite shall be discarded, except that there is no requirement to discard data from Type 12, ~~and~~ Type 17, Type 20, Type 21, and Type 22 messages. For GPS satellites, the receiver shall apply long-term corrections only if the IOD matches both the IODE and 8 least significant bits of the IODC. For GLONASS satellites, the receiver shall apply long-term corrections only if the time of reception (t_r) of the GLONASS ephemeris is inside the following IOD validity interval, as defined in 3.5.4.4.1:

$t_{LT} - L - V \leq t_r \leq t_{LT} - L$

Note 1.— For SBAS satellites, there is no mechanism that links GEO ranging function data (Type 9 message) and long-term corrections.

Note 2.— This requirement does not imply that the receiver has to stop tracking the SBAS satellite.

…

3.5.8.1.2.8 The receiver shall not use a broadcast data parameter after it has timed out as defined in Table B-94.

Note.— See additional requirements in 3.5.8.5 for receiver processing SBAS authentication data.

…

Table B-94. Data time-out intervals

Data	Associated message types	En-route, terminal, NPA time-out	Precision approach, APV time-out
Clock-ephemeris covariance matrix	28	360	240
SBAS in test mode	0	N/A	N/A
PRN mask	1	600 s	600 s
UDREI	2 to 6, 24	18 s (Note 3)	12 s (Note 3)
Fast corrections	2 to 5, 24	(see Table B-95)	(see Table B-95)
Long-term corrections	24, 25	360 s	240 s
GEO ranging function data	9	360 s	240 s
Fast correction degradation	7	360 s	240 s
Degradation parameters	10	360 s	240 s
Ionospheric grid mask	18	1 200 s	1 200 s
Ionospheric corrections, GIVEI	26	600 s	600 s
Timing data	12	86 400 s	86 400 s
GLONASS time offset	12	600 s	600 s
Almanac data	17	None	None
Service level	27	86 400 s	86 400 s
SBAS L1 Authentication Code	20	N/A	N/A
TESLA Hash Chain and Signature	21	Note 2	Note 2
SBAS authentication certificate	22	Note 2	Note 2

Note 1.— The time-out intervals are defined from the end of the reception of a message.

Data	Associated message types	En-route, terminal, NPA time-out	Precision approach, APV time-out

Note 2 – The key expiration is identified in the associated Type 21 and Type 22 messages.
Note 3 – When the SBAS provides an authentication service, there is an extended timeout of authenticated UDREI per 3.5.8.5.3.

3.5.8.5 *Authentication function*. The aircraft element requirements applicable to an aircraft element designed to process SBAS authentication when supported by SBAS are amended as follows.

Note.— The aircraft element designed to process SBAS authentication and to manage public keys and digital signatures is generally referred to as "receiver" in the rest of section 3.5.8.5.

3.5.8.5.1 When SBAS authentication is supported on L1 SBAS service of a given SBAS service provider, the receiver shall only use SBAS L1 signal with authentication from that SBAS provider.

3.5.8.5.2 The receiver shall use SBAS data only when the data is authenticated except if the data received meet the requirements in 3.5.8.5.2.1 and 3.5.8.5.2.2.

3.5.8.5.2.1 The receiver shall apply unauthenticated UDREI data or unauthenticated GIVEI data on receipt when the received UDREI data or GIVEI data is larger than the data in use.

Note 1.— When using unauthenticated UDREI data, only $\sigma_{i,UDRE}$ is updated. The time of applicability of the fast correction, t_u, is not adjusted. This ensures that there is no decrease in the protection level.

Note 2.— When using unauthenticated GIVE data, only σ_{UIVE} is updated.

3.5.8.5.2.2 The receiver shall process the Type 0, 20, 21, and 22 messages on receipt.

3.5.8.5.2.3 The receiver shall consider the data authenticated when the calculated aMAC following the protocols in 3.5.5.7 matches the aMAC received in a Type 20 message.

3.5.8.5.3 The receiver shall invalidate UDREI data for a given satellite when the time since receipt of unauthenticated UDREI data is larger than the time-out identified in Table B-94, or when the time since receipt of authenticated UDREI data is larger than the time-out identified in Table B-94 plus 11 seconds.

Note 1.— This requirement complements the requirement in 3.5.8.1.2.8 for receiver processing SBAS authentication data.

Note 2.— The extended use of authenticated UDREI data addresses the latency of the authentication data even with the loss of one Type 6 message or one Type 20 message. The delayed release of the TESLA key creates a 7 to 11 second delay in authentication and use of UDREI data. An alert sequence that delays the Type 20 message will have a similar impact on the ability to authenticate the UDREI data.

Note 3. — SBAS providers will increase the fast correction validity time using the degradation factor indicator (ai_i) as indicated in 3.5.7.6.4.2.7.

3.5.8.5.4 The receiver shall verify each TESLA Hash Point prior to use by checking that it hashes (see 3.5.5.7.1) to a previously verified TESLA Hash Point, that it is sent in the correct authentication frame and that it is received prior the hash chain end time.

Note 1.— To verify a TESLA Hash Point, it is necessary to hash the received TESLA Hash Point to a previously verified TESLA Hash Point, which could be the authenticated TESLA Confirmed Hash Point.

Note 2.— The authentication frame can be calculated from SNT (see 3.5.4.11.2) and can be determined by the number of hashes between the TESLA Hash Point and a known, verified TESLA Hash Point.

3.5.8.5.5 The receiver shall validate the TESLA hash chain prior to use.

Note. – Validating the TESLA hash chain is checking the IODT validity flag, the IODT validity flag time and TESLA hash chain end time.

3.5.8.5.6 The receiver shall authenticate the TESLA Confirmed Hash Point prior to use.

Note.— The TESLA hash chain message provides a signature that authenticates the TESLA Confirmed Hash Point and is one means to perform this confirmation.

3.5.8.5.7 The receiver shall maintain time synchronisation within +/- 3.0 seconds of SNT time.

Note 1.— The clock can be synchronized to UTC time provided that the time reference for the receiver can be expressed in SNT time. For L1 SBAS, Chapter 3 section 3.7.3.4.7.1 requires SNT alignment with GPS time.

Note 2.— To validate the TESLA Hash Point, the receiver needs to determine GPS time within 3 seconds. The receiver will need to manage conversion between UTC and GPS time.

3.5.8.5.8 The receiver shall use a trusted time source for the time synchronisation requirement in 3.5.8.5.7.

3.5.8.5.9 The receiver shall validate the SBAS authentication certificate using the out-of-band certificates.

3.5.8.5.10 The receiver shall be capable to receive self-signed root certificates and entity signing CA certificates from sources external to the aircraft (out-of-band distribution). See attachment D TBD.

Note 1. – The integrity and authenticity of the self-signed root certificates and entity signing CA certificates received out-of-band is critical for the operation conducted with SBAS authentication.

Note 2. – The receiver needs the self-signed root certificates and entity signing CA certificates to initiate use of SBAS authentication and to cover certificate renewal.

3.5.8.5.11 The receiver shall deselect the SBAS satellite and discard all data from that satellite when the SBAS Provider Identifier coded in the otherName field of the Entity Signing CA certificate in the certificate chain used to authenticate the satellite's TESLA Hash Chain does not match with the SBAS Provider Identifier received in an authenticated Type 17 message.

3.5.8.5.12 The receiver shall use only certificates within their associated validity periods.

3.5.8.5.13 The receiver shall provide a mean to deselect a specific SBAS provider from being used.

Note.— In case the cryptographic keys used by an SBAS provider are compromised, the SBAS provider may be deselected from being used until the compromised keys are rolled over.

3.5.9 SBAS L5 RF CHARACTERISTICS

…

3.5.10 Data structure on SBAS L5 signal

Note.— Messages broadcast for use under DFMC SBAS service are independent from those broadcast for use under L1 SBAS service. Information broadcast on SBAS L5 signal is used only for DFMC SBAS service solutions using dual-frequency measurements from core constellations.

3.5.10.1 *Format summary.* All messages, except for Type 50 message, shall consist of a preamble, a message type identifier, a data field and a cyclic redundancy check as illustrated in Figure B-28.

3.5.10.1.1 The Type 50 message shall consist of a preamble, a message type identifier and a 240-bit data field with no cyclic redundancy check.

3.5.10.2 *Preamble.* For L5, the preamble shall consist of the sequence of bits "0101 1100 0110 1001 0011 1010", distributed over six successive blocks. The start of every 24-bit preamble shall be synchronous with SNT time of day in seconds Modulo 6 seconds.

3.5.10.3 *Message type identifier.* The L5 message type identifier shall be a 6-bit value identifying the message type as defined in Table B-98. The message type identifier shall be transmitted MSB first.

Table B-98. L5 broadcast message types

L5 message type	Contents
0	"Do Not Use" – Content applies to DFMC SBAS service only
1-30	Spare
31	SBAS satellite mask
32	Satellite clock-ephemeris corrections and covariance matrix
33	Spare
34, 35, 36	Integrity information (DFREI and DFRECI)
37	Degradation parameters and DFREI scale table
38	Spare
39	SBAS satellite clock, ephemeris and covariance matrix – 1
40	SBAS satellite clock, ephemeris and covariance matrix – 2
41	Spare
42	SNT-to-UTC offset
43-46	Spare
47	SBAS satellites almanacs
48-49~~61~~	Spare
50	Authentication Code
51	TESLA hash chain
52	SBAS Authentication Certificate
53-61	Spare
62	Reserved – content applies to DFMC SBAS service only
63	Null message – content applies to DFMC SBAS service only

Note.— L1 messages (Table B-24) are for use with L1 SBAS service and L5 messages (Table B-98) are for use with DFMC SBAS service. Types 0, 62 and 63 messages are used independently by both L1 SBAS and DFMC SBAS services and their contents only apply to their service.

…

3.5.11 DFMC SBAS data content

…

{Editorial Note: All new text follows for 3.5.11.8 and 3.5.11.10}

3.5.11.8 *DFMC SBAS Authentication Parameters*: The DFMC SBAS authentication parameters shall be as follows.

3.5.11.8.1 *Authentication Code*: For authentication, the messages broadcasted by a DFMC SBAS service are organised in authentication frames consisting of 6 consecutive messages.

3.5.11.8.1.1 Each authentication frame in a week is identified by a sequence number *af* being an integer in the interval [0, 100799] and ends with a regular slot for an Authentication Code message (Type 50 message). The regular slot is filled by an Authentication Code message unless there is an alert.

3.5.11.8.2 The authentication frame of a message is determined by

$$af = \left\lceil \frac{t - AuthenticationMessage\ Slot}{6} \right\rceil,$$

where

- *af* identifies the authentication frame as described above,
- $\lceil x \rceil$ is the ceiling function mapping x to the least integer greater than or equal to x,
- *t* is the time of the week when the broadcast of the message starts in seconds since beginning of the week with respect to SNT, and
- *Authentication Message Slot:* parameter broadcast in TESLA hash chain message and is defined in 3.5.11.9.

3.5.11.8.3 The parameters of an Authentication Code message in an authentication frame identified by *af* shall be as follows.

Aggregated MAC ($aMAC_{L5}$): Aggregated Message Authentication Code ($aMAC_{L5}$) in a Type 50 Message Slot for the first five L5 messages in the authentication frame.

TESLA Hash Point (HP_{L5}): TESLA Hash Point associated with the authentication frame *af'* immediately preceding *af* (or, in case of alerts, with the authentication frame before the one preceding *af*).

Block Erasure Codes ($BEC1_{L5}$, $BEC2_{L5}$): Block erasure codes to recover the MACs of missed messages.

Note.— All parameters in 3.5.11.8 are broadcast in a Type 50 message.

3.5.11.9 *TESLA hash chain Parameters*: The TESLA hash chain parameters shall be as defined in 3.5.4.12.

Note.— All parameters in 3.5.4.12*are broadcast in a Type 51 message.*

3.5.11.10 *SBAS authentication certificate Parameters*: The SBAS authentication certificate parameters shall be as defined in 3.5.4.13.

Note.— All parameters in 3.5.4.13 are broadcast in a Type 52 message.

{Editorial: End new material}

3.5.12 Definitions of protocols for DFMC SBAS data applications

Note.— This section provides the definitions of parameters used by SBAS (non-aircraft and aircraft elements) that are needed to compute the navigation solution and associated integrity (protection levels).

…

{Editorial Note: All new text follows for 3.5.12.6 and 3.5.12.7}

3.5.12.6 Authentication Protocols

3.5.12.6.1 Computation of the TELSA hash chain: See 3.5.5.7.1.
Note. – Repetitive application of the hash point calculation (hashes or hash operation) develops the TESLA hash chain.

3.5.12.6.2 Computation of the message keys

Consider a 250-bit SBAS message that is broadcasted at *t* seconds SNT after beginning of week *WN* in the authentication frame *af* by the SBAS SV with PRN code *PRN* on frequency *F*. The cryptographic key k for a particular message on a particular signal and satellite shall be as per section 3.5.5.7.2.

3.5.12.6.3 Computation of the Message Authentication codes

The MAC *M* of a message *m is* computed by

$$M = \mathrm{Trunc}_{36}\big(\mathrm{HMAC}(k, m\|000000)\big)\ or$$
$$M = \mathrm{KMAC}(k, m\|000000, 36, \{\})$$

where

- $\mathrm{Trunc}_{36}(X)$ is the function mapping a string X to the string comprised of bits X[0] to X[35] with X[i] being the bit of *X* with index *i*,
- HMAC is the Keyed-Hash MAC function as defined by NIST FIPS 198-1 using the HMAC hash function identified by the Type 51 message,
- KMAC is the Keccak Message Authentication Code as defined by NIST SP 800-185 using the KMAC hash function identified by the Type 51 message,
- k is the cryptographic key for the broadcast time, satellite and signal as defined in 3.5.5.7.2,
- $X\|Y$ is the concatenation of bit string X and bit string Y,
- *m* is the message broadcast at time t on the satellite and signal associated with the key k, encoded as a 250-bit string, and
- *000000* is a 0 (zero) encoded as 6-bit string.

3.5.12.6.4 Computation of the aggregated Message Authentication Code (aMAC_{L5})

The aggregated MAC $aMAC_{L5}$ broadcasted in a Type 50 message *m* is computed as

$$aMAC_{L5} = \mathrm{Trunc}_{36}\big(\mathrm{HMAC}(k, M_1\|M_2\|M_3\|M_4\|M_5)\big)\ \text{or}$$
$$aMAC_{L5} = \mathrm{KMAC}(k, M_1\|M_2\|M_3\|M_4\|M_5\|0000, 36, \{\})$$

where

- $\text{Trunc}_{36}(X)$ is the function mapping a string X to the string comprised of bits X[0] to X[35] with X[i] being the bit of *X* with index *i, where indices increase from left to right (i.e., X[0] is the left-most bit of X, followed by X[1], etc.)*,
- HMAC is the Keyed-Hash MAC function as defined by NIST FIPS 198-1 using the HMAC hash function identified by the Type 51 message,
- KMAC is the Keccak Message Authentication Code as defined by NIST SP 800-185 using the KMAC hash function identified by the Type 51 message,
- k is the cryptographic key associated with *m* as defined above,
- $X \| Y$ is the concatenation of string X and string Y, and
- M_i is the MAC of the *i*th message in the authentication frame associated with the regular slot of *m* computed as described above and encoded as a 36-bit unsigned integer.

Note.— All integer values are encoded with the most significant bit first.

3.5.12.6.5 Block Erasure Codes

The block erasure codes BEC1_{L5} and BEC2_{L5} broadcasted in a Type 50 message are computed as

$$BEC1_{L5} = M_1 \oplus M_2 \oplus M_3 \oplus M_4 \oplus M_5 \text{ and}$$

$$BEC2_{L5} = b_1 \| b_2 \| b_3 \| b_4 \text{ with}$$

$$b_1 = b \oplus M_1^0 \oplus M_3^3 \oplus M_4^2 \oplus M_5^1,$$

$$b_2 = b \oplus M_1^1 \oplus M_2^0 \oplus M_4^3 \oplus M_5^2,$$

$$b_3 = b \oplus M_1^2 \oplus M_2^1 \oplus M_3^0 \oplus M_5^3,$$

$$b_4 = b \oplus M_1^3 \oplus M_3^2 \oplus M_3^1 \oplus M_4^0,$$

$$b = M_2^3 \oplus M_3^2 \oplus M_4^1 \oplus M_5^0.$$

where

- M_i is the MAC of the *i*th message in the authentication frame associated with the regular slot of *m* computed as described above and encoded as a 36-bit unsigned integer,
- M_i^j equals the 7 least significant bits of $M_i/2^{7j}$ encoded as a 7-bit unsigned integer,
- $X \| Y$ is the concatenation of bit string X and bit string Y, and
- $X \oplus Y$ is the string that results from applying the Boolean Exclusive-Or operation to each bit position of bit string X and bit string Y.

Note 1.— All integer values are encoded with the most significant bit first.

Note 2. – See Attachment D TBC for more details.

{Editorial Note: End new material}

3.5.13 DFMC SBAS message tables

Each SBAS message shall be coded in accordance with the corresponding message format defined in Tables B-106 through B-118. All signed parameters in these tables shall be represented in two's complement, with the sign bit occupying the MSB.

Note 1.— The value of every parameter contained in a DFMC message is computed as follows, considering that $field_{value}$ is the decimal value of the binary number, after two's complement transformation if specified in the description column of the table:

- *if the parameter is coded as two's complement: parameter = $field_{value}$*$scale_{factor;}$*
- *if the parameter is not coded as two's complement: parameter = offset + $field_{value}$*$scale_{factor}$, where the offset being specified in the comment column if different from the effective range minimum.*

Note 2.— Reserved bits in DFMC messages can take any value.

{Editorial Note: All new text follows for message tables}

Table B-xx1. Type 50 SBAS L5 Authentication Code Message

Section	Name	Length	Scale factor	Effective range		Unit	Comment
				min	max		
Aggregated Message Authentication Code	$aMAC_{L5}$	36	1	0	2^{36}-1	-	
Block Erasure terms	$BEC1_{L5}$	36	1	0	2^{36}-1	-	
	$BEC2_{L5}$	36	1	0	2^{36}-1	-	
TESLA Hash Point	HP_{L5}	128	1	0	2^{128}-1	-	
Reserved	Reserved	4	-	-	-	-	DFMC SBAS use only

Note 1.— All parameters are defined in 3.5.11.8.
Note 2. – The Type 50 message does not contain a CRC. See 3.5.10.1.1.

Table B-yy1. Type 51 TESLA Hash Chain message (Overall Message Structure)

Section	Name	Length	Scale factor	Effective range		Unit	Comment
				min	max		
Header / Meta Data	Issue of Data, TESLA	5	1	0	31	-	Identifies the TESLA Chain
	Sequence Flag	1	1	0	1	-	
	TESLA Hash Chain Payload Number	3	1	1	8	-	
Payload	TESLA Hash Chain Payload	203	1	0	2^{203}-1	-	See Table B-y2 in section 3.5.6.
Reserved	Spare	4	-	-	-	-	DFMC SBAS use only

Note.— All parameters are defined in 3.5.4.12.

Table B-zz1. Type 52 SBAS Authentication Certificate message

Section	Name	Length	Scale factor	Effective range		Unit	Comment
				min	max		
Header / Meta Data	Issue of Data, Public Key	3	1	0	7	-	Identifier of the SBAS Authentication Certificate
	Certificate Segment Number	4	1	0	15	-	
Certificate	Certificate Segment	205	1	0	2^{205}-1	-	SBAS Authenticate Certificate divided into separate messages
Reserved	Spare	4	-	-	-	-	DFMC SBAS use only

Note.— All parameters are defined in 3.5.4.13.

{Editorial Note: End new message tables}

Table B-117. Reserved

Table B-118. Type 63 null message broadcast on L5

Section	Name	Length	Scale factor	Effective Range		Unit	Comment
				min	max		
Reserved	Reserved	216	-	-	-	-	

Note.— The null message is used as a filler message if no other message is available for broadcast for the one-second time slot.

Table B-119. L5 message data time-out intervals

Data	Associated message types	Maximum update interval	En-route, terminal, NPA time-out	Precision approach, APV time-out
"Do Not Use"	0	6 s	N/A	N/A
Satellite mask	31	120 s	600 s	600 s
DFREI or DFRECI (Note 4)	32	6 s	18 s	12 s
	34	6 s	18 s	12 s
	35	6 s	18 s	12 s
	36	6 s	18 s	12 s
	40	6 s	18 s	12 s
Satellite clock- ephemeris corrections and co-variance matrix	32	$0.5x(I_{Valid})_{32}$ s per corrected satellite	$1.5x(I_{Valid})_{32}$	$(I_{Valid})_{32}$
SBAS satellite clock, ephemeris and co-variance matrix	39	$0.5x(I_{Valid})_{39/40}$ s	$1.5x(I_{Valid})_{39/40}$	$(I_{Valid})_{39/40}$
	40			
Degradation parameters	37	120 s	600 s	600 s
DFREI scale table	37	120 s	600 s	600 s
Time reference identifier	37	120 s	600 s	600 s
SBAS service provider Identifier	47	120 s	600 s	600 s
SNT-to-UTC offset	42	240 s	Note 3	Note 3
Authentication codes	50	6 s	N/A	N/A
TESLA hash chain	51	300 s	Note 5	Note 5
SBAS Authentication Certificate	52	600 s	Note 5	Note 5

Note 1.— The time-out intervals are defined from the time of arrival at the receiver's antenna port of the last bit of the message.

Data	Associated message types	Maximum update interval	En-route, terminal, NPA time-out	Precision approach, APV time-out

Note 2.— There is no time-out requirement for other parameters of Type 47 message than those listed above.

Note 3.— The SNT-to-UTC offset information in Type 42 message times out as defined in 3.5.11.6 taking into account the parameters WNapp, ToWapp and VP.

Note 4.—When the SBAS provides an authentication service, there is an extended timeout of authenticated DFREI per 3.5.15.6.3

Note 5.— The key expiration is identified in the associated Type 51 and Type 52 messages.

3.5.14 DFMC SBAS non-aircraft elements

Note.— The parameters that are referred to in this section are defined in 3.5.11.

3.5.14.1 *General*

3.5.14.1.1 *Required data and broadcast intervals*. SBAS shall broadcast the data required for the supported functions described in Chapter 3, 3.7.3.4.2 as shown in Table B-120.

Note.— SBAS may broadcast null messages (Type 63 messages) in each time slot for which no other data are broadcast.

3.5.14.1.1.1 All data broadcast by SBAS, whether required or not for a particular function, shall meet the update requirements in Table B-120.

Table B-120. L5 data broadcast intervals and supported functions

Data type	Maximum broadcast interval	DFMC SBAS Ranging	Iono-free differential correction	DFMC SBAS authentication	Associated message types
"Do Not Use"	6 s				0
Clock-ephemeris error corrections and covariance matrix data	$0.5x(I_{Valid})_{32}$ s per corrected satellite		R		32
SBAS satellite mask	120 s	R	R		31
Integrity information (DFREI and optionally DFRECI)	6 s	R	R		32, 34, 35, 36 and 40
SBAS satellite clock-ephemeris corrections and covariance matrix data	$0.5x(I_{Valid})_{39/40}$ s	R			39 and 40
OBAD, DFREI scale table and time reference identifier	120 s	R	R		37
SBAS almanac data, broadcast indicator and SBAS service provider ID parameters	120 s	R	R		47
SNT-to-UTC offset	240 s				42
Authentication codes	6 s			R	50
TESLA hash chain	300 s			R	51
SBAS Authentication Certificate	600 s			R	52

Note 1.— "R" indicates that the data must be broadcast to support the function.

Note 2.— Integrity information includes DFRECI only if Type 34 message is broadcast otherwise it is limited to DFREI.

3.5.14.1.2 *SBAS radio frequency monitoring.* The SBAS shall monitor the SBAS satellite parameters shown in Table B-109 and take the indicated action.

…

3.5.14.3.1.1 For en-route, terminal and non-precision approach, given any valid combination of active data, the probability of a horizontal error exceeding the HPL (as defined in 3.5.12.5) for longer than eight consecutive seconds shall be less than 10^{-7} in any hour, assuming a user with zero latency.

Note. —The time-out for authenticated DFREI is longer as per 3.5.15.6.3.

…

3.5.14.5 *Robustness to core constellation(s) failures.* SBAS shall continue to provide SBAS services after removal of one or several satellites, including a complete core constellation.

Note. — SBAS systems are expected to maintain operation in the presence of failures or anomalies on one or several satellites or failure of a complete core constellation. The level of supported service degrades as more satellites are removed. Removal of a failed or unhealthy satellite does not impact the ability to monitor and correct other satellites.

3.5.14.6 SBAS authentication: The SBAS shall comply with the following requirements when the SBAS provides the authentication function on its DFMC SBAS service:

3.5.14.6.1 *Key management requirements:* The SBAS shall comply with the generic key management requirements under section 3.5.7.6.4.1.

3.5.14.6.1.1 To use the same TESLA hash chain on the DFMC SBAS service as the one used on L1 SBAS service, the SBAS shall use GPS as Time reference identifier and broadcast the Type 50 message in the same authentication message slot as specified for the Type 20 message.

3.5.14.6.2 *Authentication service provision requirements*

3.5.14.6.2.1 *Authentication signal*. When providing SBAS authentication on L5 signals, it shall support authentication on all operational SBAS L5 PRNs.

3.5.14.6.2.2 *Authentication data*. If an SBAS provides an authentication function, it shall broadcast authentication code data as defined in 3.5.11.8.

3.5.14.6.2.3 SBAS shall broadcast the SBAS authentication code data in the identified Authentication Message Slot defined in 3.5.4.12 except if condition in 3.5.14.6.2.4 applies.

3.5.14.6.2.4 If the SBAS has to broadcast a different message than a Type 50 message as part of an alert sequence in the Authentication Message Slot, the SBAS shall broadcast a Type 50 message as the first message after the alert sequence (see 3.5.14.3.1.3 and Attachment D, 6.7.4).

Note.— During an alert sequence, it may be necessary to broadcast a message with DFREI data (Type 32, 39, 34, 35 or 36) in place of the Type 50 message. See Attachment D, Section TBD for demonstration of messages during an alert sequence.

3.5.14.6.2.5 The SBAS shall generate keys (k) and MACs (M) per 3.5.12.6 for all SBAS messages except for the SBAS message broadcast in the Authentication message slot as identified in the Type 51 message.

3.5.14.6.2.6 The SBAS shall generate the key (k) and aMAC associated with the broadcast time of the Type 50 message as per 3.5.5.7.

Note.— During an alert sequence, the Type 50 message may be delayed and broadcast in the subsequent authentication frame. See 3.5.14.6.2.4 and Attachment D, Section TBD for alert processing.

3.5.15 DFMC SBAS aircraft elements

Note 1.— The parameters that are referred to in this are defined in 3.5.11.

Note 2.— Whereas all SBAS receivers process signals from SBAS GEO satellites, processing non-GEO SBAS signals is optional.

3.5.15.1 DFMC SBAS-capable GNSS receiver.

…

3.5.15.1.4 *Conditions of use data on L5*.

3.5.15.1.4.1 The receiver shall use data from an SBAS message only if the CRC of this message has been verified, except for Type 50 message.

Note.— The Type 50 message does not have a CRC so data can be used on receipt of the message.

3.5.15.1.4.2 The receiver shall use the information transmitted in DFMC messages only within the time-out period, defined in Table B-119, starting from the reception of the last bit of the message.

Note.— See additional requirements in 3.5.15.6 for receiver processing SBAS authentication data.

3.5.15.1.4.3 On reception of a Type 0 message, the receiver shall cease using all data received from this signal that have defined time-out intervals in Table B-107, except for the SBAS service provider identifier which can be used only for the SBAS acquisition process and data from Types 50, 51, and 52 messages.

…

3.5.15.6 *Authentication function*: The aircraft element requirements applicable to an aircraft element designed to process SBAS authentication when supported by SBAS are amended as follows.

Note.— The aircraft element designed to process SBAS authentication and to manage public keys and digital signatures is generally referred to as "receiver" in the rest of section 3.5.15.6.

3.5.15.6.1 When SBAS authentication is supported on DFMC SBAS service of a given SBAS service provider, the receiver shall only use SBAS L5 signal with authentication from that SBAS provider.

3.5.15.6.2 The receiver shall use SBAS data only when the data is authenticated except if the data received meet the requirements in 3.5.15.6.2.1 and 3.5.15.6.2.2.

3.5.15.6.2.1 The receiver shall apply unauthenticated DFREI data on receipt when the received DFREI data is larger than the data in use.

Note.— When using unauthenticated DFREI data, only $\sigma_{i,DFC}$ is updated.

3.5.15.6.2.2 The receiver shall process the Type 0, 50, 51, and 52 messages on receipt.

3.5.15.6.2.3 The receiver shall consider the data authenticated when the calculated aMAC following the protocols in 3.5.5.7 matches the aMAC received in a Type 50 message.

3.5.15.6.3 The receiver shall invalidate DFREI data for a given satellite when the time since receipt of unauthenticated DFREI data is larger than the time-out identified in Table B-119, or when the time since receipt of authenticated UDREI data is larger than the time-out identified in Table B-119 plus 11 seconds.

Note 1.— This requirement complements the requirement in 3.5.15.1.4.2 for receiver processing SBAS authentication data.

Note 2.— The extended use of authenticated DFREI data addresses the latency of the authentication data even with the loss of one Type 34/35/36 message or one Type 50 message. The delayed release of the TESLA key creates a 7 to 11 second delay in authentication and use of DFREI data. An alert sequence that delays the Type 50 message will have a similar impact on the ability to authenticate the DFREI data.

Note 3. — SBAS providers can increase $(I_{valid})_{32}$ and $(I_{valid})_{39/40}$ to cover the time to conduct SBAS authentication.

3.5.15.6.4 The receiver shall verify each TESLA Hash Point prior to use by checking that it hashes (see 3.5.5.7.1) to a previously verified TESLA Hash Point, that it is sent in the correct authentication frame and that it is received prior the hash chain end time.

Note 1.— To verify a TESLA Hash Point, it is necessary to hash the received TESLA Hash Point to a previously verified TESLA Hash Point, which could be the authenticated TESLA Confirmed Hash Point.

Note 2.— The authentication frame can be calculated from SNT (see 3.5.11.8.2) and can be determined by the number of hashes between the TESLA Hash Point and a known, verified TESLA Hash Point.

3.5.15.6.5 The receiver shall validate the TESLA hash chain prior to use.

Note. – Validating the TESLA hash chain is checking the IODT validity flag, the IODT validity flag time and TESLA hash chain end time.

3.5.15.6.6 The receiver shall authenticate the TESLA Confirmed Hash Point prior to use.

Note.— The TESLA hash chain message provides a signature that authenticates the TESLA Confirmed Hash Point and is one means to perform this confirmation.

3.5.15.6.7 The receiver shall maintain time synchronisation within +/- 3.0 seconds of SNT time.

Note 1.— The clock can be synchronized to UTC time provided that the time reference for the receiver can be expressed in SNT time.

Note 2.— To validate the TESLA Hash Point, the receiver needs to determine time within 3 seconds. The receiver will need to manage conversion between UTC and SNT time.

3.5.15.6.8 The receiver shall use a trusted time source for the time synchronisation requirement in 3.5.15.6.7.

3.5.15.6.9 The receiver shall validate the SBAS authentication certificate using the out-of-band certificates.

3.5.15.6.10 The receiver shall be capable to receive self-signed root certificates and entity signing CA certificates from sources external to the aircraft (out-of-band distribution). See attachment D TBD.

Note 1. – The integrity and authenticity of the self-signed root certificates and entity signing CA certificates received out-of-band is critical for the operation conducted with SBAS authentication.

Note 2. – The receiver needs the self-signed root certificates and entity signing CA certificates to initiate use of SBAS authentication and to cover certificate renewal.

3.5.15.6.11 The receiver shall deselect the SBAS satellite and discard all data from that satellite when the SBAS Provider Identifier coded in the otherName field of the Entity Signing CA certificate in the certificate chain used to authenticate the satellite's TESLA Hash Chain does not match with the SBAS Provider Identifier received in an authenticated Type 47 message.

3.5.15.6.12 The receiver shall use only certificates within their associated validity periods.

3.5.15.6.13 The receiver shall provide a mean to deselect a specific SBAS provider from being used.

Note.— In case the cryptographic keys used by an SBAS provider are compromised, the SBAS provider may be deselected from being used until the compromised keys are rolled over.

— END —