SBAS message authentication: a review of protocols, figures of merit and standardization plans

Ignacio Fernández-Hernández†, Todd Walter*, Andrew M. Neish*, Jason Anderson*, Mikael Mabilleau**, Giovanni Vecchione**, Eric Châtre†

†European Commission, *Stanford University, **RHEA

Abstract

This paper presents an overview of SBAS L5 message authentication protocols proposed in the last years. We analyze 13 protocols from four sources: Stanford University, the EAST and SPARC projects, and a protocol proposed for the Australian SBAS. The protocols use L5Q, L5I, digital signatures and delayed disclosure based on TESLA. We also analyze figures of merit and weight their importance for the SBAS authentication protocol comparison, including protocol-specific figures AER (Authentication Error Rate), TBA (Time Between Authentications) and latency, and SBAS service figures (accuracy, integrity, continuity, availability). A plan for the definition, assessment and standardization of SBAS message authentication to be carried out by U.S.-EU Working Group C, in cooperation with EUROCAE WG62/RTCA-SC-159, is also outlined, with the goal of a potential addition of SBAS message authentication in the next version of the DFMC standard.

Introduction

Over the last several years, message authentication has emerged as a vital countermeasure against the threat of GNSS spoofing. Message authentication is particularly important for SBAS, as it augments other satellites, and therefore counterfeiting the SBAS message can lead to a coherent false position.

At the current time, SBAS authentication is under development for inclusion in future aviation standards. However, while various concepts have been proposed over the last few years, there is no consolidated specification ready to be standardized.

The Resilience Technical Subgroup of the U.S.-EU Working Group C (WGC-RESSG), aimed at increasing resilience of PNT services, has agreed to a workplan with the intent to consolidate, at U.S.-EU level, an SBAS message authentication specification. Our goal is to enable potential adoption of authentication by EGNOS, WAAS and others over the next several years.

This paper reviews the existing literature on SBAS authentication, including the qualitative comparison of the existing technical concepts using some FoM (Figures of Merit). We highlight both the main points of convergence as well as the open points and challenges. In particular, all SBAS message authentication concepts proposed are based on asymmetric protocols, whereby the receivers only have access to public keys. Several alternatives have been studied over the last years and many design decisions remain open. These include:

- The choice between delayed disclosure lightweight protocols, such as TESLA [1], standard digital signatures [2] such as ECDSA and EC-Schnorr, or hybrid solutions.
- The cryptographic functions and related cryptographic security strength, and the inclusion of the quantum threat mitigation as a security objective.
- The carrier frequencies whose data is authenticated. While the focus is L5, if L1 SBAS remains as an acceptable fall back mode, ideally it should be also authenticated.
- The transmission of authentication in the message structure of the SBAS signal in-phase component (I), or in a quadrature component (Q), and at what power level in the latter case, out of possible SBAS L1/L5 signal design and I-Q power split options, as proposed in [3].
- The receiver logic, and in particular what information the SBAS users can use prior to authentication, in order to maintain the basic SBAS time-to-alert capability, while also maintaining integrity in the face of deliberate attacks.

This paper focuses on message authentication protocols in the SBAS L5 signal for DFMC SBAS data authentication. While L1 implementations are not presented here, some of the presented protocols are intended to work on both L1 and L5. The paper is structured as follows: In the next section, we review existing protocols in the literature. Then we discuss figures of merit and preliminarily characterize the different protocols. Later, we present U.S.-EU plans regarding SBAS DFMC authentication standardization. We finalize the paper with some conclusions.

Review of existing protocols

This section reviews existing SBAS message authentication protocol implementations in the literature. Our focus will be on the implementations proposed by Stanford University, GPS Lab, and those proposed by the European Commission projects SPARC (coordinated by the European GNSS Agency GSA) and EAST. We also include a protocol developed for the Australian/New Zealand SBAS. Some of these protocols are currently not advocated by any particular group and are not actually contenders, but they are provided here for completeness. We focus on L5 implementations on either I or Q channels. All implementations are listed and commented in Table 1, at the end of the section. They are also represented in the scheme of Figure 1, which allows a visual comparison of the different solutions. In the Figure, dots represent an authentication page (in all the proposed solutions, authentication messages occupy full pages). Blue pages represent the first SBAS data page set to be authenticated, and their related authentication pages, which are therefore blue cells with a dot. While this process occurs periodically, only one instance is selected to highlight the different protocol implementations. Dark blue pages imply the end of the delay disclosure for TESLA protocols. For example, in solution SPARCA-I-ECDSA, the pages transmitted in seconds 3-6, 8-11, 13-16, where the 1st second is the 1st cell counting from the left, are authenticated with a digital signature transmitted in seconds 17, 22 and 27 (three authentication pages in total). This pattern is repeated, so that the next group of authenticated pages will be in seconds 18-21, 23-26 and 28-31, and so on. Note that the SPARCD-Q-HYBRID solution (12) contains two solutions, digital signature and TESLA, but only the digital signature option is represented.

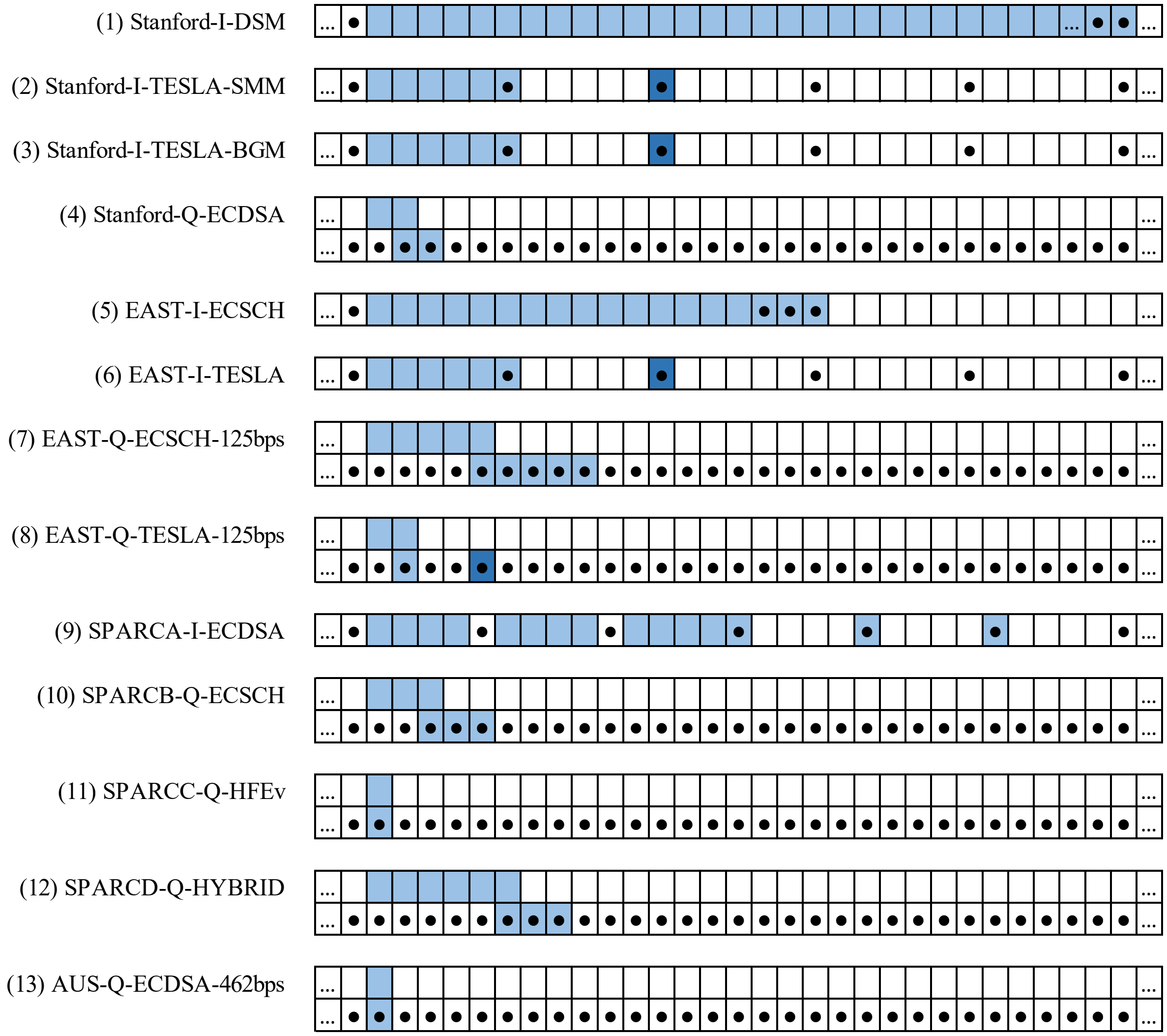

Figure 1 – Representation of SBAS L5 message authentication solutions. Dots represent authentication pages. Blue pages represent the first SBAS data page set to be authenticated and their related authentication pages. Dark blue pages represent the end of the delayed disclosure (TESLA). While authentication takes place periodically, only one instance is highlighted in blue in order to show the different protocol implementations.

SBAS authentication protocols by Stanford

The first reference on SBAS authentication (1) can be found in [4]. Given that the research on SBAS authentication as well as the boundary conditions have evolved over the years, protocol (1) is provided for completeness, but it is currently not recommended for implementation. It proposes a two-page digital signature in the I channel every 60-150s (it cannot be fully represented in Figure 1), which is interleaved with the current SBAS message sequence. In order to maintain continuity, up to four erasure messages can be added, allowing non-reception of up to four pages without affecting the authentication of the whole block. For the rest of this paper, we assume a 60-second 4-recovery page implementation, as this seems the closest to the more modern solutions presented.

A second family of SBAS message authentication solutions is defined in [5] and [6]. It focuses on L5, for incorporation in future DFMC standard versions. Three concrete implementations are proposed: A TESLA implementation in L5-I, with five 15-bit MACs (later implemented with 16-bit MACs, without performance impact), one per 1-second word and a 115-bit key (2); a TESLA implementation in L5-I as well, with one 30-bit MAC for the 5-word data stream (3); and an ECDSA signature in the L5-Q channel (4). The 30-bit MAC implementations lead to continuity losses, as any missing page implies the authentication cannot be performed, dropping 6 unauthenticated messages. The TESLA solution with five 15-bit MACs ((2) Stanford-I-TESLA-SMM) appears to mitigate this effect by authenticating each page separately. Another relevant contribution of [5] is the proposal of different treatment of information, depending on whether its late processing can lead to HMI (Hazardously Misleading Information) or not: Alerts via MT0 or increased DFREIs (Dual Frequency Range Error Indicators) in MTs 32, 34, 35, 36, and/or 40 shall be processed immediately, prior to authentication, while the remaining information can only be processed once authenticated. This approach allows maintaining integrity and a 6-second TTA: as TTA is already consumed by SBAS in the monitoring process, any authentication protocol that adds any latency to integrity information would not fulfil the 6-second TTA. Importantly, this methodology assumes that most data cannot be trusted until it is verified through authentication ("authenticate-then-use" approach, as opposed to "use-then-authenticate"). In this way, it ensures that spoofed data that could lead to HMI would never be used by the receiver.

SBAS authentication protocols by EAST

The EAST project was the first European project specifically on SBAS authentication. The main protocol implementations selected from the project were summarized and analyzed in [7], although other variants were also proposed and studied in [8] and [9]. The L5-I protocols retained in [7] were: (5), an EC-Schnorr digital signature transmitted in three pages at a minimum bandwidth of 1 message out of 6; and (6), an L5-I TESLA implementation with an authentication message every 6 seconds. In the Q channel, several implementations at different bitrates and power levels were proposed. We will consider two cases in this review, both with a ¼ coding rate (125 bps) in the Q-channel: (7), an EC-Schnorr implementation transmitted in 5 seconds, and (8) a TESLA implementation transmitted in 2 seconds, where the MAC is transmitted in the first Q page, and the key in the second Q page. Note that other more optimal implementations are possible if the low-power Q-channel implementation is pursued, and that [7] left this aspect for further work. Further details on SBAS L1/L5 signal design options, including detailed considerations about I-Q power split, can be found in [3] and [10].

SBAS authentication protocols by SPARC

The SPARC project, launched after the EAST project and coordinated by the GSA, continued the work on SBAS authentication definition and testing. Its main results concerning SBAS authentication protocols are publicly available in [11]. Four protocols are proposed in this reference. The first one ("Solution #A", (9)) consists of a 512-bit EC-Schnorr signature in 3 pages of the I channel. In the proposed implementation, one authentication page transmitted every 5 pages, equally spaced. The second one ("Solution #B", (10)) consists of a similar signature (ECDSA) in the Q channel, at an equal power apportionment as the I channel, occupying 3 pages as well. "Solution #C", (11), includes an interesting and bandwidth-efficient proposal of a post-quantum digital signature of only 171 bits based on HFEv, at the expense of a longer 93,500-bit public key, that can be encrypted and pre-stored in the receiver. It is transmitted in the Q channel too. Finally "Solution #D", (12), proposes a hybrid approach including both

TESLA and asymmetric signatures that remains secure if one of the cryptographic schemes is compromised.

Authentication protocols for the Australian/New Zealand SBAS

As part of the Australia/New Zealand SBAS development activities, NMA has been studied in [10]. Two authentication protocols are described in this reference. In the first one, (13), a 320-bit ECDSA signature, of 80 bits of security, is transmitted in the L5-Q channel by removing the FEC encoding layer, obtaining 462 bps, and allowing to sign each simultaneous page in the L5-I. A higher FEC rate of ¾ is also proposed as an option. The second approach relies on a signed one way function (similar to a TESLA chain) but without MACs, and transmitted in the Q channel. The authenticity of the scheme relies on the fact that, if the data integrity in the Q channel is maintained, it must be maintained in the I channel as well: As an adversary cannot modify the signed hashes of the Q component without being noticed (the last one is authenticated), it cannot modify the data in the I channel either. While this approach would provide significant simplifications in the receiver, it is not explained in [10] how a receiver could protect data from an adversary synthesizing and rebroadcasting the signal with a small delay and modified bits in the I channel. Due to the lack of some details in the definition of this second protocol, we only analyze the first protocol in this work.

Table 1 presents a general characterization of the 13 protocols explained above, including the security bits and the MAC size, where needed, some comments about the implementation, and whether the protocol is actively under analysis at the moment or just provided for completeness.

	SL [b]	MAC [b]	Comments	Currently under analysis
(1) Stanford-I-DSM (2014)	106	0	2-page digital signature + 4 recovery pages. Every 60s (up to 150s). No continuity loss expected.	No
(2) Stanford-I-TESLA-SMM	115	15	5 Short MACs (15 bits) signing each page. No continuity loss expected.	Yes
(3) Stanford-I-TESLA-BGM	115	30	Longer MAC (30 bits) authenticating 5 pages.	No
(4) Stanford-Q-ECDSA	112	0	ECDSA signature of 448 bits in 2 pages.	Yes
(5) EAST-I-ECSCH	128	0	512-bit EC-Schnorr signature, assuming that the 3 signature pages are transmitted consecutively every 18 seconds.	No
(6) EAST-I-TESLA	80-128	30	Similar to (3). Key length not fixed but not a driver for the analysis.	No
(7)EAST-Q-ECSCH-125bps	128	0	EC-Schnorr signature every 5s in the Q channel at 125 bps.	No
(8) EAST-Q-TESLA-125bps	80-128	30	One TESLA-MAC every 2s in the Q channel at 125 bps.	No
(9) SPARCA-I-ECDSA	128	0	512-bit signature in 3 pages. ECDSA. The signature is interleaved with data pages (1 auth. Page every 4 data pages)	Yes
(10) SPARCB-Q-ECSCH	128	0	512-bit ECSchnorr signature in 3 pages.	Yes
(11) SPARCC-Q-HFEv	100	0	A priori quantum-resistant. 171-192-bit signatures in 1 message. No continuity loss expected.	Yes
(12) SPARCD-Q-HYBRID	100	0	Only digital signature represented. TESLA hybrid solution not represented.	Yes
(13) AUSTR-Q-MbyM	80	0	One 320-bit ECDSA signature L5Q per page by removing the FEC or raising the coding rate to 3/4. No continuity loss expected.	No

Table 1 – SBAS Data Authentication Protocol high level description including security level (SL) in bits, and MAC size, when a TESLA protocol is implemented. Note that solution (12) only characterizes the signature. The last column specifies if the protocol is currently under analysis as an SBAS authentication candidate, to the knowledge of the authors.

Other issues and protocols

This subsection introduces other issues that, while not the subject of this paper, are relevant for the protocol review. It also presents, for completeness, other satellite navigation authentication protocols, including global and regional systems.

OTAR (Over-The-Air Rekeying) and PKI (Public Key Infrastructure): SBAS authentication based on asymmetric cryptography or delayed-disclosure asymmetry (e.g. TESLA) requires the receiver to store and renew a public key. For the moment, we consider SBAS as a closed system, where the receiver may not be accessed during its lifetime. Therefore SBAS authentication relies on OTAR. However, OTAR is not the focus of this paper. We consider that any protocol can use the spare bits of the message for OTAR, or if needed, additional messages sporadically. Therefore, we consider that the upper key-authenticating-key layers, OTAR messages, and PKI, can be similar for any authentication scheme and are beyond the main scope of this work. We also need to take into account that, according to modern cybersecurity, future crypto systems including SBAS authentication may require firmware key updates, but this is also beyond the scope of this work. Further details can be found in [12].

Post-Quantum cryptography: Some of the proposed solutions above are supposedly robust to post-quantum cryptography attacks, such as SPARC Solution C (11). While quantum robustness is desired, at the moment there is no quantum-robust standard. The standardization process by NIST is ongoing [13] and it is foreseen that it will be concluded in the years to come. We note which solutions of the proposed ones are considered quantum-secure, at the moment, but most of the proposed solutions are considered pre-quantum, or defined for pre-quantum security levels. For example, TESLA solutions are estimated to be quantum-secure (as symmetric cryptography in general), by doubling the key size. Further details on this topic and its application to GNSS and SBAS are available in [14].

Signal authentication: Signal authentication can be a relevant feature of SBAS. In particular, even if SBAS ranging is not used, it can fulfil the TESLA time synchronization to a very high accuracy, in the few-ms level, provided the receiver had a looser synchronization reference already, in the order of e.g. minutes. We consider that, as shown for GPS's CHIMERA in [15] and [16], signal authentication through spreading code watermarking can be designed almost independently from, but based on, data authentication (with some restrictions in case of digital signatures). Further considerations on this are left for further work. See [9] for concrete SBAS signal authentication protocols using spreading code watermarking.

Other protocols: Apart from those in the SBAS domain, other recent GNSS authentication initiatives include Galileo OSNMA [17], based on an adaptation of TESLA and currently under test, GPS's CHIMERA [15] or QZSS authentication [18].

Figures of merit

A broad discussion on SBAS authentication KPIs (Key Performance Indicators) has been taken into account including ICAO Navigation Systems Panel, and this discussion is foreseen to be taken into account as a reference for a formal evaluation of protocols in the months to come. As a complement to this broader and more formal analysis, in this work we define figures of merit them according to two categories: SBAS-related and authentication-specific. The former relates to the standard performance indicators, and the latter relates to specific indicators of the authentication solutions.

SBAS Figures of Merit

As a general framework to analyze GNSS authentication performance, [19] proposes that, since authentication is an additional feature of a navigation system, the priority performance-wise should be to maintaining the original navigation performance, while mitigating the modelled threats. In the case of SBAS, this relates to the main SBAS performance indicators (accuracy, integrity, continuity, availability). Therefore, any impact in accuracy, integrity, continuity and availability due to message authentication should be minimized to the extent possible. In particular, [6] (Appendix A) proposes availability, continuity and TTA as KPIs. References [7] and [11] analyze the full impact of SBAS authentication in all user/service KPIs, including accuracy and integrity (to some extent). HPE, VPE, VPL and HPL (Horizontal/Vertical Error/Protection Level) are calculated over time at a certain representative location in [11], and error/PL maps are presented for the ECAC, for a target of LPV-200 precision approach requirements. Continuity for a 15-second operational period is also analyzed, as in [6], and set to 8 x 10^{-6}. In all the references consulted, continuity is the driving FoM in practice, and it becomes the most difficult to achieve for several protocols, especially those using L5-I. A reference for the computation of accuracy, integrity, continuity, and availability for SBAS can be found in [20].

Authentication-Specific Figures of Merit

Three additional KPIs related to the authentication protocol are proposed in [6] as well as most references: TBA, AER, and latency (measured in [6] as median authentication latency 'MedianAL'). References from EAST/SPARC [11] propose also other metrics, which are currently used in both EU and U.S. analyses, such as ASA (Authentication Service Availability), ATTA (Authentication Time To Alert), or APMD (Authentication Probability of Missed Detection). Some of these parameters can be defined by design, such as TBA, or can be measured taking into account failed authentications. For this work, we focus on AER, TBA and latency. Their main utility is that they are easy to calculate with the provided analytical expressions. The use of these analytical expressions is not intended to replace a more complete SBAS performance analysis. However, the performance of the protocol in terms of AER, TBA and latency may affect SBAS FoMs: high TBA and latencies will degrade accuracy and availability, and prevent 6s-TTA, while a higher AER will impact these and also continuity.

Authentication Error Rate: We define it as the rate at which authentications fail, according to the following analytical expression [7]:

$$\mathrm{AER} = 1 - \ (1 - \mathrm{PER}_m)^{\breve{M}}\ (1 - \mathrm{PER}_a)^{\breve{A}} \qquad (1)$$

Where PER_m and PER_a are the page error rate of the data and authentication pages (e.g. when transmitted in I and Q channels or if they have different coding mechanisms or rates), and $\breve{M}$ and $\breve{A}$ are the number of pages of SBAS data to be authenticated and authentication messages, respectively, *for each authentication*. When both authentication and data are transmitted in the same channel (e.g. the I component), the expression is simplified to

$$\mathrm{AER} = 1 - (1 - \mathrm{PER})^{\breve{M}+\breve{A}} \qquad (2)$$

Where PER is the general page error rate of the channel. Note also that, depending on the channel model, PER can have a different behavior. For example, AWGN (Additive White Gaussian Noise) models usually define a probability, while other more realistic aviation models define a Gauss-Markov chain whereby after a failed page it is likelier that the next page is also corrupted [6]. Note also that the above expressions (1) and (2) are a particularization of the binomial probability distribution, and can be applied only if the protocol has no page recovery. If the protocol has page recovery, as protocol (1), the AER expression for one channel is modelled as a cumulative binomial probability distribution:

$$\mathrm{AER} = 1 - \sum_{i=0}^{K} \binom{\breve{M} + \breve{A}}{i} \mathrm{PER}^{i} (1 - \mathrm{PER})^{\breve{M}+\breve{A}-i} \tag{3}$$

Where K is the number of recovery pages.

In practice, AER can also be computed with the following experimental expression [11]:

$$\mathrm{AER} = \frac{\#failed\ or\ unavailable\ authentication\ verification\ events}{\#all\ authentication\ verification\ events} \tag{4}$$

Note that AER considers not only the failed authentications but also the case when a page is corrupted and therefore not available for the authentication verification.

Time Between Authentications: TBA is defined as the time elapsed between two successive authentications. It can be used as a design parameter (generally a constant value), as it gives information about the TTA for the protocol design, for data that is used prior to authentication, which in turn it's associated to the SBAS integrity requirement. While it may vary in case of failed authentications, this effect should already be captured by AER or the general SBAS performance indicators, without a specific FoM for experimental or 'effective TBA'.

For all the studied cases, we can derive an analytical definition of TBA as follows

$$\mathrm{TBA}_{I} = M + A \ ;\ \mathrm{TBA}_{Q} = A \tag{5}$$

Where M and A are the number of data and authentication pages between authentications, and the subscripts I and Q of TBA represent whether the protocol is implemented in the I or Q channel. Note that for this definition to hold it is required that M and A are constant, the protocol is implemented solely on the I or the Q channel, and that pages are divided between authentication pages (A) and other pages (M), but not in a combination of them. These conditions hold for the 13 protocols analyzed. Note also that, while $\breve{A} = A$ and $\breve{M} = M$ in most cases, this cannot be generalized. In particular, protocol (2) proposes that each MAC authenticates just one out of five pages, so $\breve{M} = 1$ and $M = 5$. Thanks to this feature the protocol maintains continuity.

Authentication Latency: Authentication latency is defined as the time elapsed between a message is decoded by the receiver, and it is authenticated. It can be calculated as a design parameter and as for TBA, any 'effective latency', or impact in latency of failed authentications can be captured by other FoM. We can also derive analytical expressions for the maximum and minimum latencies, as follows

$$AL_{MAX,I} = M + A + D - 1 \ ;\ AL_{MAX,Q} = M + A + D - 2 \tag{6}$$

$$AL_{min,I} = A + D \ ;\ AL_{min,Q} = A + D - 1 \tag{7}$$

Where *D* is the disclosure delay for TESLA protocols. Under the same assumptions as for TBA, and the additional assumption that the data is transmitted with the shortest delay, which is valid for all but one of the analyzed protocols (SPARCA-I-ECDSA, for which the 3-page signature is scattered across 12 pages, possibly to avoid the transmission of more than one authentication page altogether), and anyway is a desired feature of the protocol.

While we suggest that other FoM be used in a formal, more thorough comparison, the analytical expressions in Eq. (5), (6) and (7) prove useful to quickly compare protocols, and they have been used in Table 2 for this purpose.

Other indicators: Other design features that are used to compare solutions are authentication bandwidth consumption (for I and Q components and in total), protocol cryptographic strength (e.g. security bits; shown before in Table 1), TESLA MAC size (do not confound with cryptographic security strength; shown also in Table 1), receiver implementation constraints (e.g. loose time synchronization), and ability to be applied to L1 and L5.

Table 2 presents the comparison of the 13 protocols in relation to these protocol parameters: *M*, the number of data pages per authentication; *A*, the number of authentication pages per authentication; whether the protocol is in the I or the Q channel; *D*, the disclosure delay (if any); latency; TBA; bandwidth in the I and Q channels; total bandwidth for authentication; and AER, all are calculated analytically.

					Latency				Bandwidth				
	M	**A**	**I/Q (I=1; Q=0)**	**D [s]**	**Min Lat [s]**	**Avg Lat [s]**	**Max Lat [s]**	**TBA [s]**	**BW L5-I**	**BW L5-Q**	**BPS-Q**	**Total bps for auth**	**AER**
(1) Stanford-I-DSM (2014)	54	6	1	0	6	32.5	59	60	10%	0%	0	25	3.661E-09
(2) Stanford-I-TESLA-SMM	5	1	1	6	7	9	11	6	17%	0%	0	42	2.997E-03
(3) Stanford-I-TESLA-BGM	5	1	1	6	7	9	11	6	17%	0%	0	42	6.979E-03
(4) Stanford-Q-ECDSA	2	2	0	0	1	1.5	2	2	0%	100%	250	250	3.994E-03
(5) EAST-I-ECSCH	15	3	1	0	3	10	17	18	17%	0%	0	42	1.785E-02
(6) EAST-I-TESLA	5	1	1	6	7	9	11	6	17%	0%	0	42	6.979E-03
(7)EAST-Q-ECSCH-125bps	5	5	0	0	4	6	8	5	0%	50%	125	125	9.955E-03
(8) EAST-Q-TESLA-125bps	2	2	0	2	3	3.5	4	2	0%	50%	125	125	3.994E-03
(9) SPARCA-I-ECDSA	12	3	1	0	3	8.5	14	15	20%	0%	0	50	1.490E-02
(10) SPARCB-Q-ECSCH	3	3	0	0	2	3	4	3	0%	100%	250	250	5.985E-03

(11) SPARCC-Q-HFEv	1	1	0	0	0	0	0	1	0%	100%	250	250	1.999E-03
(12) SPARCD-Q-HYBRID	6	3	0	0	2	4.5	7	6	0%	100%	250	250	8.964E-03
(13) AUSTR-Q-MbyM	1	1	0	0	0	0	0	1	0%	100%	250	250	1.999E-03

Table 2 – SBAS Data Authentication Protocol Classification. BW stands for bandwidth. M: message pages (per authentication). A: authentication pages (per authentication). I/Q: signal component used for authentication (L5-I/L5-Q). D: disclosure delay (for TESLA protocols). Bps-Q: bandwidth in the Q channel. Min-Avg-Max Lat: minimum-average-maximum latency. TBA: Time Between Authentications. BW-L5-I/Q: percentage of bandwidth used in L5-I/L5-Q.

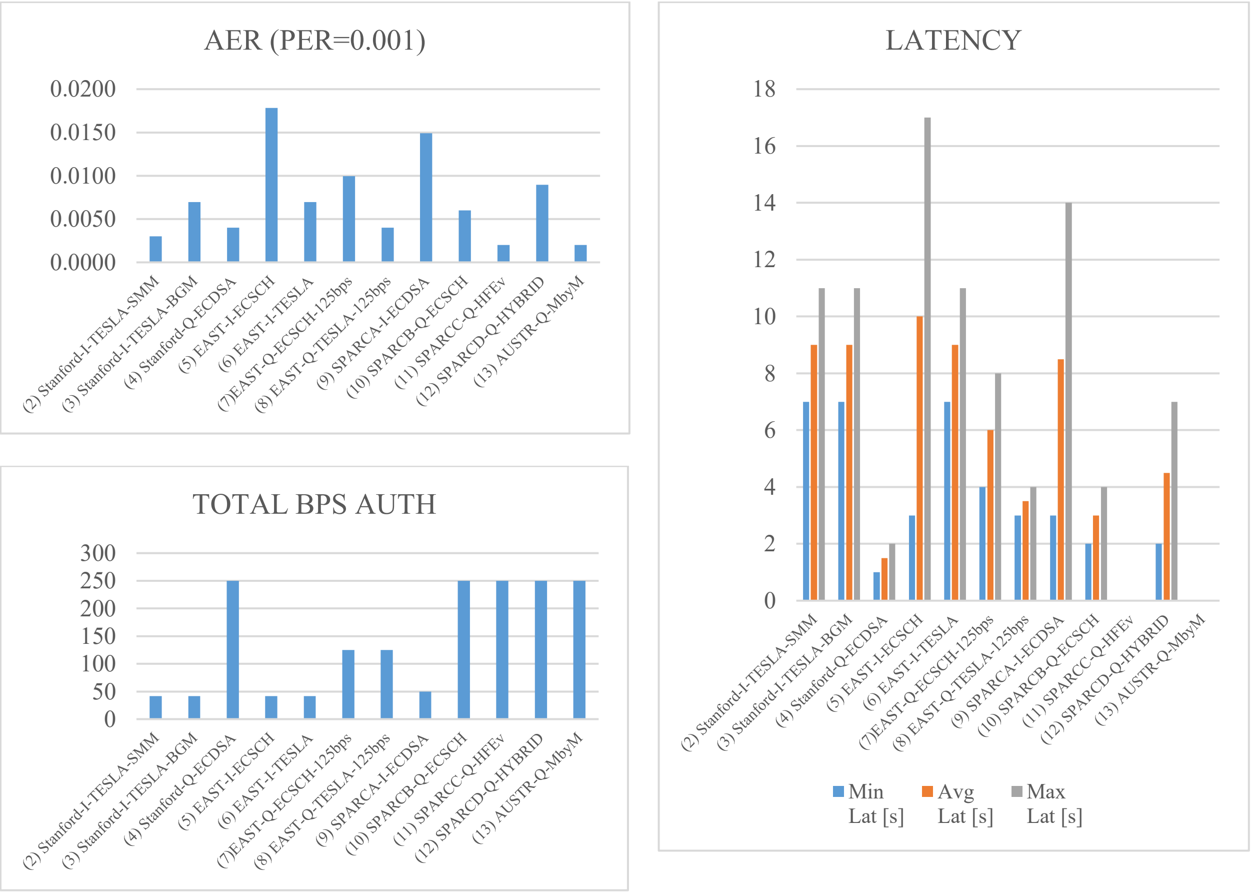

Figure 2 – Evaluation of SBAS authentication protocols vs. Authentication FoM. Top-left: AER for a PER of 0.001. Right: minimum, average and maximum latency. Bottom left: total bandwidth use (bps) for authentication. Protocol (1) excluded from the comparison.

Figure 2 presents graphically some of the authentication FoM, based on Table 2. The top left chart shows the AER based on Eqs. (1) and (2). It is based on a PER of 1/1000, the same for I and Q, and assuming that the power in the Q channel is set accordingly. The right chart shows the minimum, average and maximum latencies. The bottom left chart shows also the total bandwidth used for authentication, which is not presented as a FoM but it is also illustrative of the protocol properties. We can see that Q-channel solutions (4), (7), (8), (10), (11), (12) and (13) use more bandwidth, and in exchange provide a lower latency. Protocol (1) is provided for completion purposes, but it is excluded from the Figure, as it follows a very different approach form the rest and is not currently actively studied. The Figure also shows that similar implementations at page level yield different results. For example protocol (2) has a lower AER compared to protocol (3) thanks to authenticating each page separately, as mentioned before and further explained in [6].

Standardization plans

The DFMC standard has been recently adopted by the ICAO Navigation System Panel (NSP), yet it does not include message authentication. The activities of the U.S.-EU Working Group C, and in particular the Resilience Technical Subgroup (WGC-RESSG), are supporting the introduction of this feature in the DFMC aviation standards, consistently with the ICAO NSP plan to develop SBAS authentication baseline development standard by end 2022. WGC-RESSG's work will consist of a quantitative assessment of SBAS message authentication schemes and configurations and the final selection of a proposal for the next generation standards [21]. The WGC-RESSG SBAS message authentication (SBASMA) roadmap is summarised in Table 3. Note that the dates may vary depending on ICAO NSP schedule and other elements. The workplan items are:

1. **Context and Assumptions**: These include assumptions on SBAS system capabilities, user requirements, and user treatment of authentication information. System implementation constraints and user assumptions should be fixed in this section. As part of the context, this section will take into account existing inputs from other groups, such as ops concepts from ICAO NSP Task Force.

2. **Figures of Merit (FoM):** High-level figures of merit that characterize the solutions. FoM shall include at least performance impact in SBAS due to message authentication (accuracy, integrity, continuity, availability), APMD and authentication latency.

3. **Technical Concepts:** Technical proposals available from the work of the RESSG participants. They shall be characterized at least in terms of receiver requirements, cryptographic functions, SBAS message specification, receiver treatment specification, and any other relevant information for the operation of the concept. Unless otherwise agreed, this includes elements on key management and PKI that are part of the technical concept.

4. **Functional and Performance Analysis**: Analysis of different proposals according to the FoM and any other assumptions. The results will present an overview of the performance of the different solutions as well as potential functional or operational differences (e.g. additional receiver requirements, system requirements, interpretations of the authenticated/non-authenticated information, differences in operational concepts including key management, etc.).

5. Based on the above, an **SBASMA Final Specification** will be prepared and ready to be provided to other groups/panels for consideration of incorporation into the DFMC standards.

The work summarized in this paper represents a first contribution to items 1. to 3. WGC-RESSG inputs will be provided to the joint EUROCAE and RTCA working groups for consideration in the development of the avionics standards. Currently, SBAS authentication is a topic for the next version of the MOPS, scheduled for completion in late 2023.

Items	Step 1 (Spring'21)	Step 2 (Fall'21)	Step 3 (Spring'22)
1. **Context and Assumptions**	Draft	Final	
2. **Figures of Merit**	Draft	Final	
3. **Technical Concepts**	Draft	Final	
4. **Functional and Performance Analysis**		Draft	Final
5. **Final Specification**		Draft	Final

Table 3 – RESSG WGC SBASMA tentative roadmap

Conclusions and Future Work

This paper presents an overview of SBAS message authentication protocols presented in the literature in the last years. Out of the message authentication protocols fully documented in the literature, 13 solutions are discussed and compared, including four from Stanford University, four from the EAST project, four from the SPARC project, and one for the Australian SBAS. While some of these solutions are not anymore considered for SBAS authentication, they are presented and analyzed for completeness. The main differences in the proposed solutions are the use of the L5-Q vs L5-I, and the use of asymmetric cryptographic functions for digital signatures vs. delayed-disclosure (TESLA). Apart from those, the protocols propose different cryptographic functions and security bit levels.

Several figures of merit are presented, based on the literature review. We propose to focus on assessing the impact of SBAS authentication in the main SBAS performance indicators: accuracy, integrity, continuity and availability. Out of those, continuity is most demanding for SBAS authentication, and compliance to TTA may require to use some messages before they are authenticated, except for zero-latency protocols. As authentication-specific metrics, TBA, AER and latency are analyzed in this work. We define analytical expressions for each, under some assumptions, which may not be generalized to every protocol but hold for the protocols under study.

A plan for the definition, comparison, selection and standardization work to be carried out by U.S.-EU WGC Resilience Technical Subgroup (RESSG), in cooperation with EUROCAE WG62/RTCA-SC-159 is presented in the last section, leading to a final specification by spring 2022. By this time, further work will be needed on the SBAS authentication operational concept, including authenticate-then-use vs. use-then-authenticate approaches, and their related spoofing detection capabilities. The need to develop a suitable authentication solution on SBAS L1 will also require further discussion prior to standardization.

References

[1] A. Perrig, R. Canetti, J. D. Tygar and D. Song, "The TESLA Broadcast Authentication Protocol," *CryptoBytes,* 2002.

[2] National Institute of Standards and Technology, "FIPS PUB 197 - Federal Information Processing Standards Publication 197 - Specification for the ADVANCED ENCRYPTION STANDARD (AES)," NIST, 2001.

[3] M. Tran, C. Hegarty, A. Van Dierendonck and T. Morrissey, "SBAS L1/L5 Signal Design Options," in *Proceedings of the 59th Annual Meeting of The Institute of Navigation and CIGTF 22nd Guidance Test Symposium (2003)*, Albuquerque, NM, 2003.

[4] P. Enge and T. Walter, "Digital Message Authentication for SBAS (and APNT)," in *ION GNSS+ 2014*, Tampa, FL, 2014.

[5] A. Neish, T. Walter and J. D. Powell, "SBAS Data Authentication: A Concept of Operations," in *ION GNSS+ 2019*, Miami, FL, 2019.

[6] A. M. Neish, "Establishing Trust Through Authentication in Satellite Based Augmentation Systems; PhD Thesis," Stanford University, 2020.

[7] I. Fernández-Hernández, E. Châtre, A. D. Chiara, G. D. Broi, O. Pozzobon, J. Fidalgo, M. Odriozola, G. Moreno, S. Sturaro, G. Caparra and N. Laurenti, "Impact analysis of SBAS authentication," *Navigation,* vol. 65, no. 4, pp. 517-32, 2018.

[8] A. D. Chiara, G. D. Broi, O. Pozzobon, S. Sturaro, G. Caparra, N. Laurenti, J. Fidalgo, M. Odriozola, J. C. Ramon, I. Fernandez-Hernandez and E. Chatre, "Authentication Concepts for Satellite-Based Augmentation Systems," in *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, Portland, Oregon, 2016.

[9] A. D. Chiara, G. D. Broi, O. Pozzobon, S. Sturaro, G. Caparra, N. Laurenti, J. Fidalgo, M. Odriozola, G. M. Lopez and I. Fernandez-Hernandez, "SBAS Authentication Proposals and Performance Assessment," in *Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017)*, Portland, Oregon, 2017.

[10] K. Cogdell and P. Reddan, "Australia/New Zealand DFMC SBAS and Navigation Message Authentication," Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018), Miami, Florida.

[11] L. Tosato, A. D. Chiara, C. Wullems, G. F. Serrano, A. Calabrese, A. Perrig, M. Mabilleau and G. Vecchione, "Broadcast Data Authentication Concepts for Future SBAS Services," in *Proceedings of*

the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), pp. 1-26., September 2020.

[12] A. Neish, T. Walter and J. D. Powell, "Design and analysis of a public key infrastructure for SBAS data authentication," *NAVIGATION,* vol. 66, no. 4, pp. 831-844, 2020.

[13] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson and D. Smith-Tone, "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process (NISTIR 8309 (DOI)," NIST, July 2020.

[14] A. Neish, T. Walter and P. Enge, "Quantum-Resistant Authentication Algorithms for Satellite-Based Augmentation Systems," *NAVIGATION,* vol. 66, no. 1, 2019.

[15] Anderson, Jon M.; Carroll, Katherine L.; et al., "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals," in *ION GNSS+*, Portland, OR, 2017.

[16] GPS Air Force Research Laboratory, "IS-AGT-100 - Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface," 17 APR 2019.

[17] I. Fernandez-Hernandez, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodriguez and J. D. Calle, "A Navigation Message Authentication Proposal for the Galileo Open Service," *Journal of the Insitute of Navigation,* no. Spring, pp. pp. 85-102, 2016.

[18] R. Hirokawa and S. Fujita, "A Message Authentication Proposal for SatelliteBased Nationwide PPP-RTK Correction Service," in *Proceedings of 32th International Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, Miami, Florida, September 2019.

[19] I. Fernández-Hernández, "GNSS Authentication: Design Parameters and Service Concepts," *Proceedings of the European Navigation Conference,* 2014.

[20] RTCA SC-159, "MOPS WAAS - Minimum Operational Performance Standards for Global Positioning System Wide Area Augmentation System Airborne Equipment- DO229D (with Change 1, Feb 2013)," 2006.

[21] G. Vecchione, I. Fernandez-Hernandez, M. Mabilleau, L. Herlihy, J. Burns, D. Wilkerson and B. Clark, *SBAS Message Authentication Planned Activities,* ICAO NSP - Information Paper, 2020.