Message Authentication Candidates for the SBAS Dual Frequency Multi-Constellation Standard

Ignacio Fernandez-Hernandez[†], Todd Walter, Mikael Mabilleau[††], Luciano Tosato**, Andrea Dalla Chiara**, Daniele Pozza**, Oscar Pozzobon**, Alessandra Calabrese[§], Jason Anderson*, Eric Châtre[†]*

[†]European Commission, *Stanford University, [††]EUSPA, **QASCOM, [§]GMV

ABSTRACT

The first version of the SBAS Dual Frequency Multi-Constellation (DFMC) standard has been recently finalized. It is foreseen that its extension includes message authentication, to protect avionics from SBAS data spoofing attacks. This paper focuses on the main candidate scheme at the moment, based on the TESLA protocol in the L5-I channel. This paper analyzes which data needs to be used before authentication in order to maintain time to alert. It describes two options, named Authenticate-then-Use and Use-then-Authenticate, and analyzes its prospective performance for EGNOS and WAAS.

INTRODUCTION

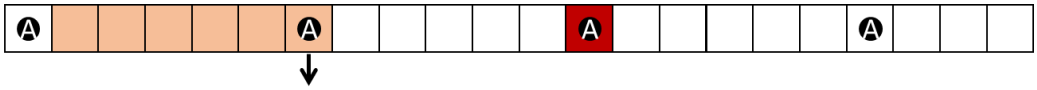
SBAS data spoofing can become a single point of failure, as spoofed SBAS data can lead a receiver to a coherently false position. Over the last years, SBAS providers and researchers have developed message authentication solutions [1] [2] [3] [4] for the DFMC (Dual Frequency Multi Constellation) standard, currently under finalization [5]. Several message authentication schemes have been studied including several options, such as delayed disclosure protocols (e.g. TESLA, Timed-Efficient Stream Loss-Tolerant Authentication) vs. digital signatures, or the existing I channel vs. a new component in quadrature (Q channel) [6]. Another open design aspect is the use of information only before it is authenticated, in order to maintain the SBAS TTA (Time To Alert) requirement [7].

Our main challenge is to authenticate SBAS data with a good-enough level of security, while maintaining accuracy, integrity, continuity and availability performance for precision approach operations [8], and do this for the different SBAS and satellite configurations, including single- and multi-constellation.

This paper focuses on a scheme based on TESLA and short MACs in the L5-I component. After the description of the scheme, we analyze authenticate vs. use approaches in relation to the SBAS DFMC message type information. We focus on two approaches, referred to as Authenticate-then-Use (AtU) and Use-then-Authenticate (UtA), and test their performance impact for both WAAS and EGNOS for different validity intervals. We finalize with the conclusions and next steps.

SBAS AUTHENTICATION MAIN SCHEME DESCRIPTION

The scheme under analysis is based on the TESLA protocol implemented in the L5-I channel, as shown in Figure 1. There is one authentication message every 6 seconds (represented with an 'A'), that carries authentication tags computed with an HMAC (Hash-based Message Authentication Code), one for each of the preceding pages in the SBAS stream, and a key that is part of a TESLA one-way keychain and authenticates the MACs of the previous block [9]. This scheme is further defined and justified in in [1] and its latest specification can be found in [10].



Preamble	MT	HMAC1	HMAC2	HMAC3	HMAC4	HMAC5	Hash Point	Spare	CRC
4	6	16	16	16	16	16	128	8	24

Figure 1 - SBAS message authentication candidate scheme under analysis. Each block represents a page. The authentication messages are transmitted every 6 seconds ('A'). The key (Hash Point) of the message in red authenticates the tags (HMACs) of the five messages of the preceding block (light orange).

USE VS. AUTHENTICATE RECEIVER LOGIC

In principle, the security obtained from applying cryptography for data origin authentication is based on the premise that the data is used only *after* it is authenticated. However, SBAS restrictions make it impossible to fulfil the 6-second TTA requirement if authentication adds latency in the use of the data, on top of the SBAS latency for the satellite monitoring. If an alert is only processed after it is authenticated and this introduces an additional latency, then the 6-second TTA cannot be respected, unless authentication were transmitted in the Q channel in parallel, which is out of scope of this work. Another parameter impacted is the message timeout, or validity interval (VI). If a latency is added, validity intervals may be surpassed and the data timed out. Finally, applying the SBAS data later than at their reception time may lead to higher navigation errors and protection levels (PLs).

Table 1 proposes an authentication receiver logic per SBAS DFMC message type. MT31, MT39-40, MT42 and MT47 are not a priori the most sensitive, due to their high validity interval and the type of information: satellite mask, GEO ephemeris and almanac, timing and service provider parameters. On the other extreme there is MT35 (with MT34 and MT36, if transmitted), with the integrity and alert information in the DFREI table. Satellite alerts (DFREI = DON'T USE) need to be processed instantaneously, even if they are not authenticated, in order to guarantee the TTA fulfilment. MT32 provides also per-satellite DFREIs and satellite corrections and the variance-covariance matrix used in the position and protection level (PL) computation, and the authenticate vs. use logic needs to ensure coherency with MT35. This is also the case for MT37 but this MT is expected to be very stable and therefore can be authenticated before use.

MT	*Main Content*	*Update & Validity Intervals (Precision Approach)*	*Data Authentication Policy*
31	Satellite mask	UI = 120s (max) VI = 600s	Authenticate before use.
32	Corrections (1 sat) • Satellite corrections (delta x,y,z,b,x',y',z',b') • Satellite error covariance matrix • DF Range Error Indicator (DFREI) • Degradation multiplier	UI: Flexible (MT37); Typical UI: 30-60 sec VI: Flexible (MT37)	Authenticate before use. Affordable impact in performance. Ensure MT32-35-37 consistency: may replicate MT35 DFREI auth policy.
35 (34, 36)	Integrity • DFREI (many sats) • DFRE change indicator (DFRECI) (MT34)	UI: 6 sec (max) VI: 12 sec	Shall process Alarms (DFREI = 15; DON'T USE) before authentication. Several options for DFREI ≠ 15.
37	Degradation parameters and DFREI Scale Table • OBAD (old-but-active data) parameters, incl. VI. • Other degradation/time parameters • DFREI Scaling factor	UI = 120s (max) VI = 600s	Authenticate before use. Affordable impact in performance. Ensure MT32-35-37 consistency.
39-40	GEO ephemeris	UI = 120s (max) VI: Flexible (MT37)	Authenticate before use.
42	Timing	UI = 240s (max) VI: variable (hours)	Authenticate before use.
47	Provider ID, GEO almanac	UI = 240s (max) VI = 600s	Authenticate before use.

Table 1 - SBAS DFMC message types and data authentication policy

Therefore, the authenticate vs. use tradeoff mainly relates to MT35 with possible impact in MT32. All the other messages can be authenticated before use. Some authenticate vs. use options are:

- Alerts-only: use when authenticated except DFREI = DON'T USE.
- Use the maximum of the most recent unauthenticated and authenticated DFREIs [7]. This approach is called "Authenticate-then-Use" (AtU) hereinafter.
- Use all DFREIs immediately, irrespective of their previous value, and authenticate them later. This approach is called "Use-then-Authenticate" (UtA) hereinafter.

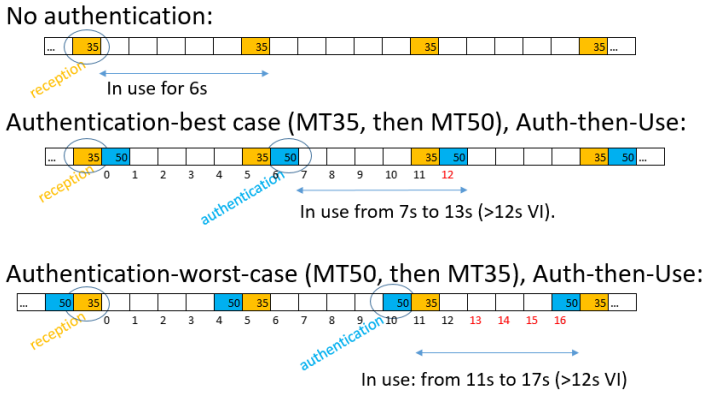
We will now analyze the impact of AtU and UtA impact in MT35 timeout. Figure 2 shows examples of message sequences for SBAS DFMC, where MT50 is the message carrying the authentication. The top chart shows an example of the EGNOS sequence, which has a flexible scheduler. In this example, MT35 is transmitted just after MT50, showing the worst case for MT35 timeout. The bottom chart shows an example of the WAAS scheduler, which is rigid, and where MT35 is transmitted just before MT50. In this case, MT35's authentication tag will be received one second later, minimizing latency (best case).

t_m = 1 MT 35	t_m = 2 MT 32, SV 87	t_m = 3 MT 32, SV 88	t_m = 4 MT 32 SV 89	t_m = 5 MT 32 SV 90	t_m = 6 MT 50
t_m = 7 MT 35	t_m = 8 MT 32, SV 91	t_m = 9 MT 32, SV 92	t_m = 10 MT 32, SV 93	t_m = 11 MT 32 SV 94	t_m = 12 MT 50
t_m = 13 MT 35	t_m = 14 MT 32, SV 95	t_m = 15 MT 32, SV 96	t_m = 16 MT 32, SV 97	t_m = 17 MT 32 SV 98	t_m = 18 MT 50
t_m = 19 MT 35	t_m = 20 MT 31	t_m = 21 MT 37	t_m = 22 MT 47	t_m = 23 MT 47	t_m = 24 MT 50
t_m = 25 MT 35	t_m = 26 MT 39	t_m = 27 MT 40	t_m = 28 MT 32 SV 1	t_m = 29 MT 32 SV 2	t_m = 30 MT 50

t_m = 1 MT 32 SV 01	t_m = 2 MT 32 SV 11	t_m = 3 MT 32 SV 20	t_m = 4 MT 31 (or 37)	t_m = 5 MT 35	t_m = 6 MT 50
t_m = 7 MT 32 SV 02	t_m = 8 MT 32 SV 12	t_m = 9 MT 32 SV 21	t_m = 10 MT 32 SV 29	t_m = 11 MT 35	t_m = 12 MT 50
t_m = 13 MT 32 SV 03	t_m = 14 MT 32 SV 13	t_m = 15 MT 32 SV 22	t_m = 16 MT 32 SV 30	t_m = 17 MT 35	t_m = 18 MT 50
t_m = 19 MT 32 SV 04	t_m = 20 MT 32 SV 14	t_m = 21 MT 32 SV 23	t_m = 22 MT 32 SV 31	t_m = 23 MT 35	t_m = 24 MT 50
t_m = 25 MT 32 SV 05	t_m = 26 MT 32 SV 15	t_m = 27 MT 32 SV 24	t_m = 28 MT 32 SV 32	t_m = 29 MT 35	t_m = 30 MT 50

Figure 2 – example of SBAS message schedulers for EGNOS (top) and WAAS (bottom). The EGNOS scheduler is flexible and the example represents the worst case. The SBAS scheduler is rigid and optimized for reducing latency (best case).

The authentication latency and its impact in the validity interval is shown in Figure 3. Note that this impact is applicable to the AtU case only, as the UtA allows full use of MT35 DFREIs before authentication, as abovementioned. For the 'no authentication' case, the 12-second VI is consumed if there is a message loss, as shown in the Figure. Therefore, the VI must be extended up to 19 seconds in the best case, and 23 seconds in the worst case. Based on this analysis, we set up our test configurations for the tests described in the next section.



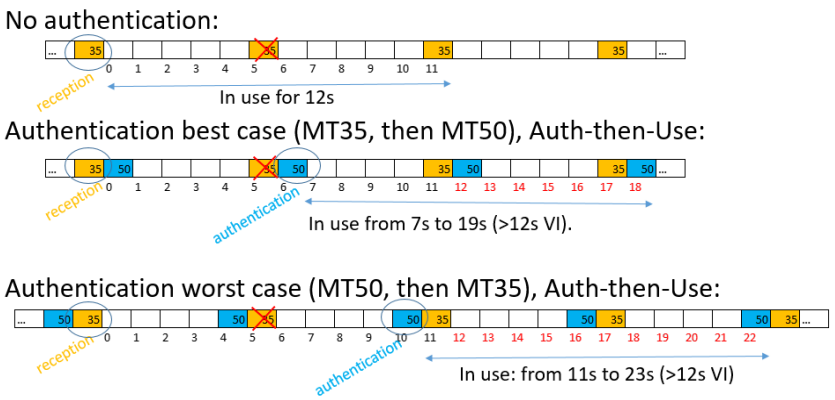


Figure 3 – Impact of authentication latency of MT35 in validity interval (VI) for AtU with no message loss (top) and with message loss (bottom). Each chart shows the case of no authentication, best case and worst case.

TEST RESULTS

Table 2 presents the configuration of the EU (EGNOS) and US (WAAS) tests. The results were generated with the PROSBAS and MAAST tools respectively.

EGNOS Results

Figure 4 shows in the top charts the availability results in Europe. The top left chart shows the availability with a timeout of 23 seconds, AtU. As expected, the timeout extension allows the timely use of MT35 and availability is fulfilled in the service area and beyond. The top right chart shows that if the timeout is not extended and maintained at 12 seconds, the availability is highly degraded, as DFREIs are systematically timed out, as shown in Figure 3, and therefore the satellites removed from the solution. The remaining availability between 50-75% is attributed to the fact that the flexible scheduler does not implement the worst-case sequence all the time and sometimes MT35 is closer to MT50, and that some DFREIs are updated also from MT32. Figure 4 bottom charts present the continuity results in Europe, which follow a similar trend. With a 23-s timeout, continuity can be guaranteed, but if reduced to 12 s, continuity is systematically disrupted. Note that the presented continuity results are shown for WER = 0, while continuity can be severely affected by authentication in case of page reception errors, as shown in [4]. However, by authenticating each message separately with a different MAC in the current solution, the effect in continuity is attenuated [1]. The evaluation of the continuity impact of the current scheme in Europe with different values of WER is left for further work.

Figure 5 and Figure 6 present the HPL and VPL results respectively. In Figure 5, the top left chart shows the ‘no authentication’ case, used as the benchmark. The top right chart presents the UtA case, showing a very small impact in the PL values. The color scale shows a small increase in the PL values compared to the benchmark. The bottom left chart presents the AtU case a with 23-s timeout. In this case the HPLs are again slightly higher, by one to a few decimeters. This is due to the conservative approach of using the highest DFREI with respect to UtA. Finally, in the bottom right chart, the AtU with 12-s timeout shows that HPLs cannot be calculated due to the message timeouts. Figure 6 shows the same trend for VPLs as Figure 5 for HPLs. Both figures show that HPL/VPLs can fulfil the precision approach requirements with respect to the AL (Alert Limits) (we take HAL=40m and VAL=35m as a reference) in the UtA case and in the AtU case if the timeouts are extended.

Parameter	***EU Configuration***	***US Configuration***
SBAS config	*L5 DFMC*	*L5 DFMC*
Augmented constellation	GPS+GAL	GPS+GAL
Integrity data update rate	6s	6s
Integrity data timeout (Validity Interval)	12s / 23s	12s / 23s
Integrity data authentication delay	11s	7s
Channel conditions (Word Error Rate)	WER = 0	WER=[0,10^{-1}]
Receiver logic	AtU, UtA	AtU, UtA

Table 2 – SBAS message authentication configuration parameters

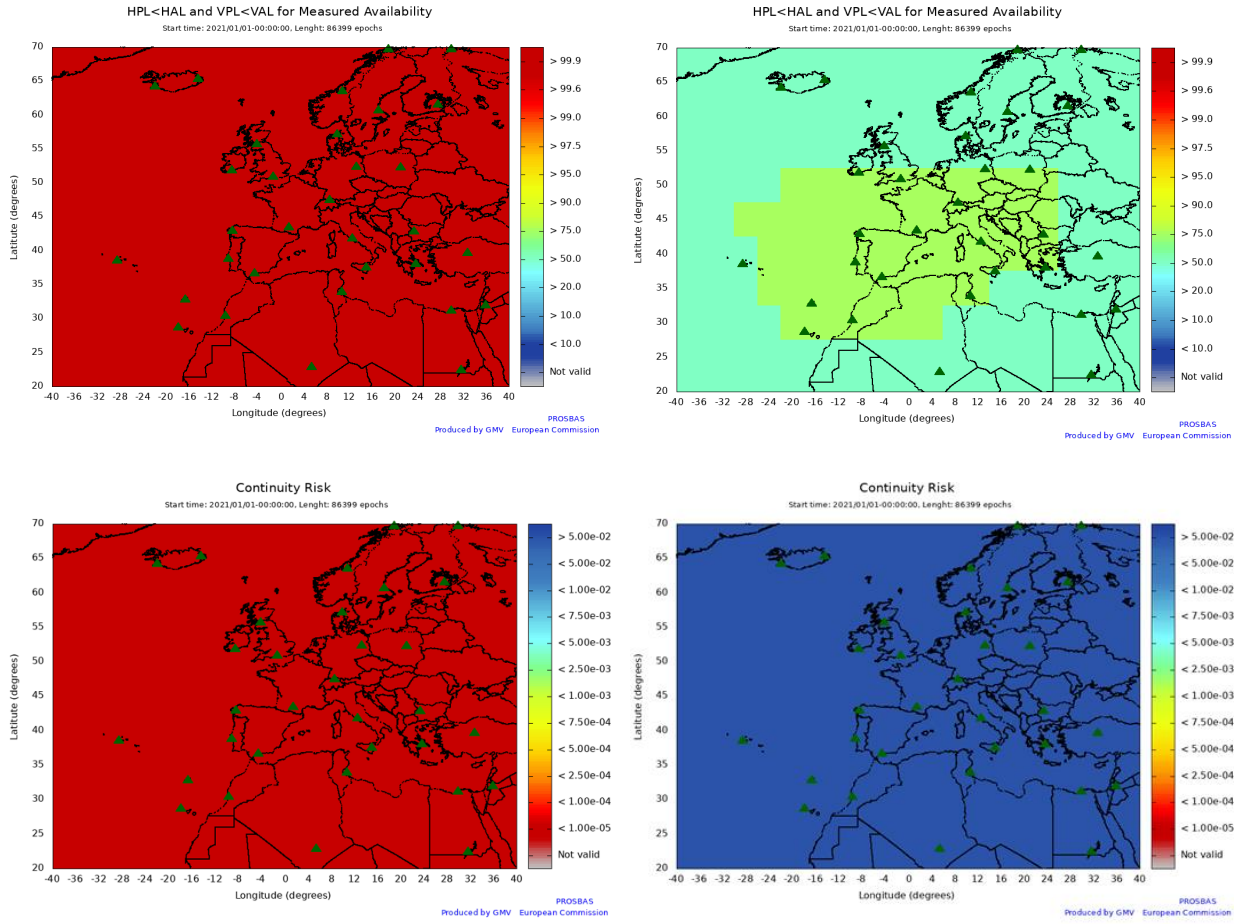


Figure 4 – Europe availability and continuity results, AtU. Top left: Availability, 23-s timeout. Top right: Availability, 12-s timeout. Bottom left: Continuity, 23-s timeout. Bottom right: Continuity, 12-s timeout.

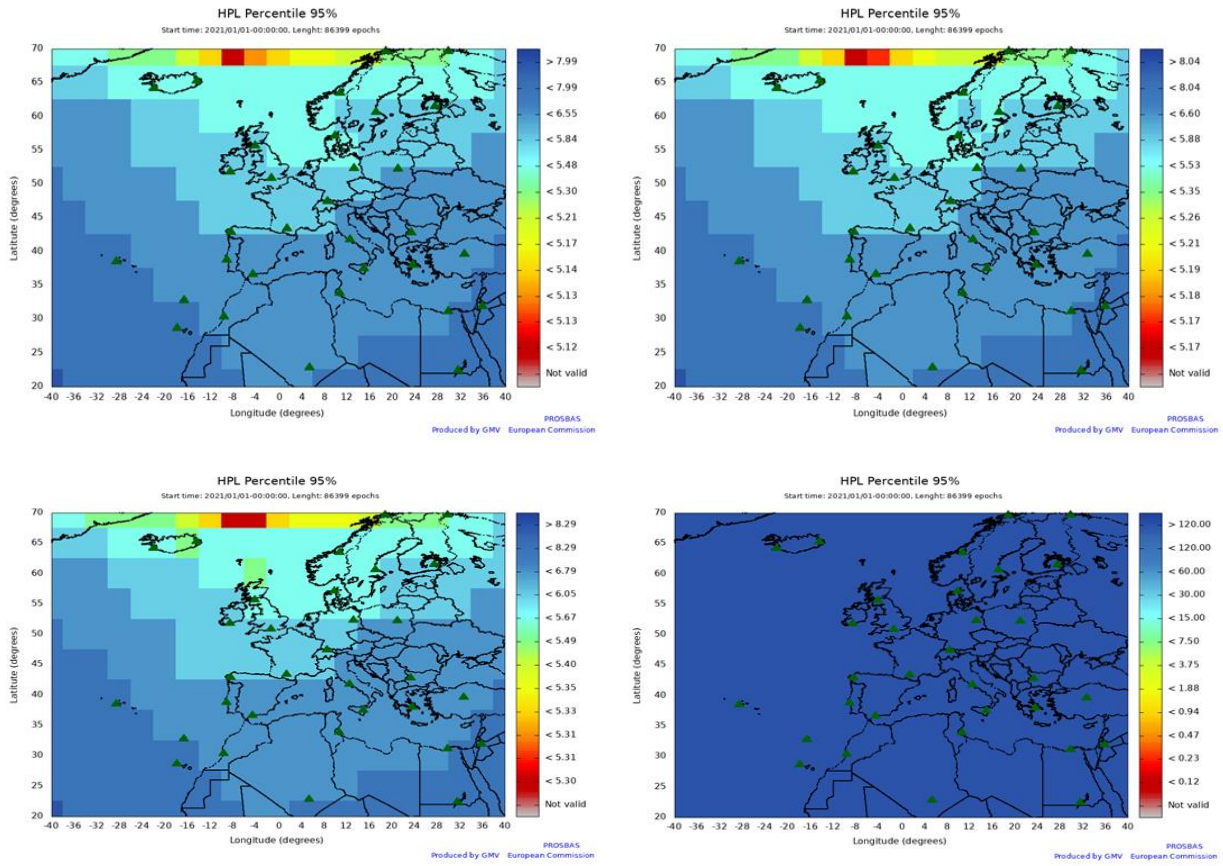
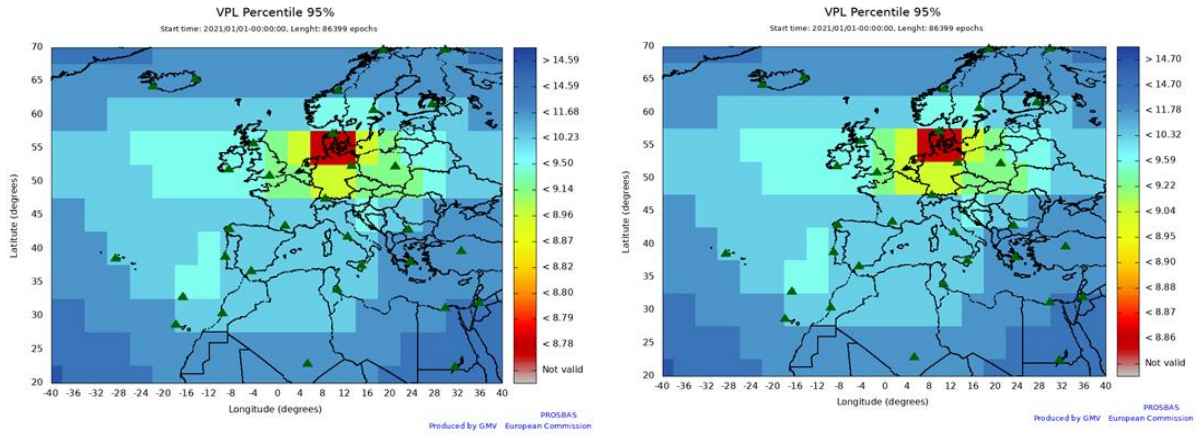


Figure 5 – Europe Horizontal Protection Level (HPL) results. Top left: No authentication. Top right: UtA, 23-s timeout. Bottom left: AtU, 23-s timeout. Bottom right: AtU, 12-s timeout.



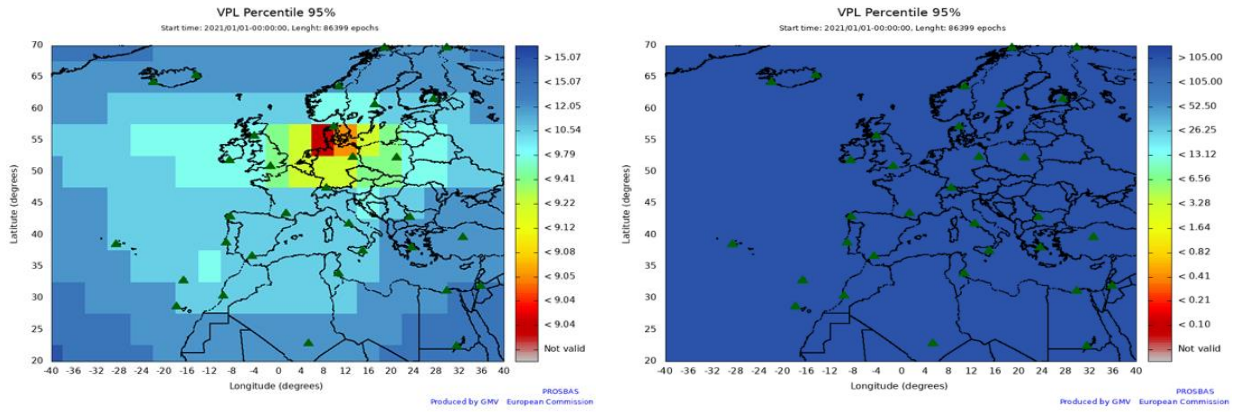


Figure 6 – Europe Vertical Protection Level (VPL) results. Top left: No authentication. Top right: UtA, 23-s timeout. Bottom left: AtU, 23-s timeout. Bottom right: AtU, 12-s timeout.

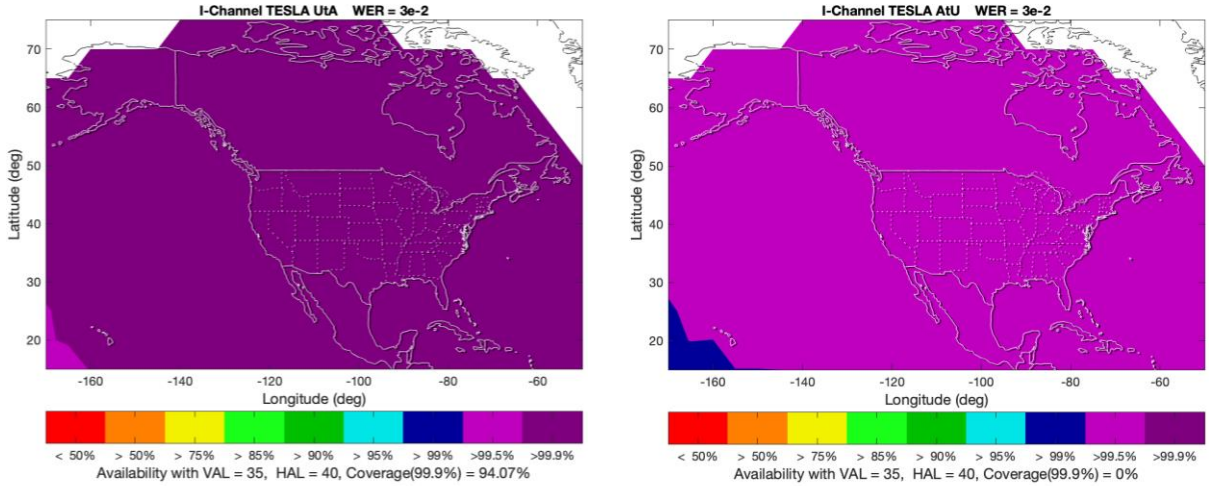


Figure 7 – US availability results. Left: UtA. Right: AtU, 23-s timeout.

Figure 7 presents the availability results for the US area. The left chart shows no availability degradation in the UtA case, even with a high WER of 10^{-2}. The right chart shows the AtU case, where there is a degradation but availability is still high (99.5%), especially for such a high WER. Figure 8 shows the increase in VPL (95%) for different WER values and three cases: no authentication (benchmark), AtU and UtA. For both AtU and UtA, the VPL increase is low, always below a decimeter. The more conservative approach of AtU vs UtA shows a slight degradation, as shown for the EGNOS case previously. This degradation remains constant up to high WER values, and only for WER > 10^{-2} PLs increase above the decimeter. These results are provided in more detail and complemented with further tests in [10].

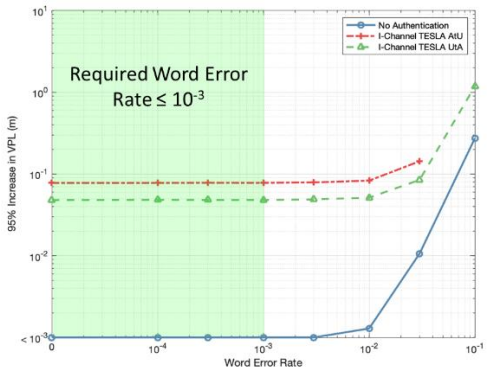


Figure 8 – 95% increase in VPL (m) vs. WER for AtU, UtA and no authentication.

CONCLUSION AND NEXT STEPS

This paper has presented the first US-EU consolidated results on DFMC SBAS message authentication. The focus of this work is on one scheme, based on TESLA in the L5-I channel and providing five short MACs, one per preceding message.

While most messages are used only after the authentication, DFREIs require use before authentication, at least to maintain the TTA. Two receiver logic candidates have been analyzed: AtU, which uses the highest DFREI of the previous ones; and UtA, which uses the latest DFREI even if not yet authenticated.

AtU and UtA are analyzed taking into account the prospective implementations in EGNOS and WAAS. In case of EGNOS, the message scheduler is assumed to be flexible, while in case of WAAS it is assumed to be fixed. In the latter case, MT35's DFREIs are transmitted just after MT50's authentication data, which is considered as the best case. However, MT35 validity interval, or timeout, should be extended in all AtU cases from 12 seconds to 19 or 23 seconds, for the best-case or worst-case scheduler, respectively.

We analyse SBAS availability, continuity and HPL/VPL for UtA and AtU with and without timeout extension. As expected, AtU without MT35 timeout extension degrades severely the performance with the flexible scheduler. UtA shows slightly better performance than AtU, although it requires more data to be used before authenticated. Both candidates seem compliant with SBAS precision approach operation performance.

Further work will include consolidating the authentication scheme and cryptographic parameters of the solution, extending the EU analyses with non-zero WERs, and continuing the work within the technical and standardization groups in US and EU and ICAO. This work should contribute to an updated SBAS DFMC standard including message authentication in the following years.

DISCLAIMER

This work is performed under the Resilience Subgroup of EU-US Working Group C of the EU-US Agreement on GPS-Galileo Cooperation. The content of this article does not necessarily reflect the official position the authors' organizations. Responsibility for the information and views set out in this article lies entirely with the authors.

REFERENCES

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

[2] 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), pp. 3208-3221*, Portland, Oregon, 2016.

[3] 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. 11-25*, September 2020.

[4] I. Fernandez-Hernandez, 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, the Journal of the Institute of Navigation,* vol. 65, no. 4, pp. 517-32, 2018.

[5] International Civil Aviation Organization, "DFMC SBAS SARPS - Baseline draft for validation," 2018. [Online]. Available: https://www.icao.int/airnavigation/Pages/DFMC-SBAS.aspx. [Accessed Sept 2021].

[6] I. Fernández-Hernández, T. Walter, A. M. Neish, J. Anderson, M. Mabilleau, G. Vecchione and E. Châtre, "SBAS Message Authentication: A review of Protocols, Figures of Merit and Standardization Plans," in *Proceedings of the 2021 International Technical Meeting of The Institute of Navigation, , January 2021, pp. 111-124.*, 2021.

[7] A. Neish, T. Walter and J. D. Powell, "SBAS Data Authentication: A Concept of Operations," in *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019), pp. 1812-1823.*, Miami, FL, 2019.

[8] International Civil Aviation Organisation, "International Standards and Recommended Practices - Annex 10 - Aeronautical Telecommunications - Vol 1 - Radio Navigation Aids - Sixth Edition - No. 90," ICAO publications, 2016.

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

[10] T. Walter, J. Anderson and S. Lo, "SBAS Message Schemes to Support Inline Message Authentication," in *Proceedings of the 2021 International Technical Meeting of The Institute of Navigation (ION GNSS+ 2021)*, St. Louis, MO, 2021.