International Civil Aviation Organization

MIDANPIRG/22 & RASG-MID/12 Meetings

(Doha, Qatar, 4 – 8 May 2025)

Agenda Item 5.3: ANS (AIM, PBN, AGA-AOP, ATM-SAR, CNS and MET)

STRENGTHENING AIM DATA INTEGRITY

(Presented by United Arab Emirates / General Civil Aviation Authority)

SUMMARY

This paper presents the UAE commitment in ensuring AIM data integrity by transitioning from MD5 hashing to the latest and stronger hashing technology SHA-512 for AIM data integrity. It also explains why the transition to SHA-512 was essential to ensure stronger cryptographic security.

Action by the meeting is at paragraph 3

REFERENCE

- ICAO ANNEX 15
- ICAO PANS-AIM DOC 10066

1. INTRODUCTION

1.1 The United Arab Emirates / General Civil Aviation Authority (UAE GCAA) would like to share its experience in enhancing data integrity in critical document management. Guided by ICAO recommendations in Annex 15 and DOC 10066, UAE prioritized strengthening cryptographic measures to ensure that aeronautical data remains intact and unaltered since its origin.

1.2 The initial step was using MD5 hashing algorithm which was replaced with the more robust SHA-512. The latter offers superior collision resistance and aligns with modern standards. This paper highlights UAE approach, challenges encountered, and solutions implemented during the upgrade process, reflecting commitment to maintaining high data integrity and authenticity standards.

2. DISCUSSION

2.1 Cryptographic hash functions ensure data integrity by generating unique hash values for data. MD5 (Message Digest Algorithm 5) produces a 128-bit hash, which is inadequate for modern security. It is now easy to generate collisions, where different data results in the same hash, compromising data integrity. SHA-512 (Secure Hash Algorithm 512), generates a 512-bit hash, making it much harder to find collisions. This larger hash size improves security, ensuring data remains intact and unaltered, making it a better choice for modern cryptography.

2.2 UAE transition from MD5 to SHA-512 is driven by the need for stronger cryptographic security. The transition from MD5 to SHA-512, was not without challenges. One of the key hurdles was the need to update existing applications that were built around MD5 hashing.

2.3 The application code was updated to generate SHA-512 hashes, replacing the previous MD5 algorithm. Extensive testing was conducted to ensure the accuracy of the SHA-512 hash generation process and its integration across all relevant components.

2.4 The SHA-512 hash for the AIP.zip file is included with each AIP update notification email, along with clear instructions for users on how to generate and verify the hash on their end.

2.5 Additionally, all AIP related files are hashed using SHA-512, and the updated hash values are included in an Excel file, along with a Windows shell command that users can run for generating SHA-512 hashes for comparison. Updated instructions and guidance materials are also provided within the package.

2.6 Running the new command generates SHA-512 hash values, and any change of information will result in a different value not matching the code provided, confirming that there is a change or corruption in data. Customers are advised to report, if the SHA-512 hash value generated by the customer does not match the SHA-512 hash value provided by UAE GCAA AIM.

2.7 Previously, hash functions were shared only during publication updates, preventing new subscribers from verifying data integrity. Now, hash lists are also made directly accessible from the AIP, which is always available on the website.

2.8 Transitioning to SHA-512 ensures compliance with modern cryptographic standards, significantly enhancing the data integrity of published aeronautical information. This change offers UAE AIP users a higher degree of confidence and assurance in the reliability of the information.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note UAE’s experience and the information contained in this paper; and

b) encourage states to consider introducing such data integrity measures.

- END -