International Civil Aviation Organization

MIDANPIRG/20 and RASG-MID/10 Meetings

(Muscat, Oman, 14-17 May 2023)

Agenda Item 6.2: AIM

PUBLISHED AERONAUTICAL INFORMATION DATA INTEGRITY

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

SUMMARY

The integrity of published aeronautical information data plays a critical role in international aviation safety, quality, and efficiency.

This paper outlines UAE GCAA implementation in order to fulfill the need of data integrity monitoring and assurance. It also highlights its importance with respect to the rapid expansion of digital technology.

REFERENCES

– Annex 15 "Aeronautical Information Services"

– DOC 10066 "PANS-AIM"

1. INTRODUCTION

1.1 The United Arab Emirates / General Civil Aviation Authority (UAE GCAA) would like to share its experience in the implementation of the cryptographic technology hash function for data integrity monitoring and assurance.

1.2 According to ICAO, Data integrity is defined as: "A degree of assurance that an aeronautical data and its value has not been lost or altered since the origination or authorized amendment". UAE is continuously seeking ways for improvements in order to assure its data integrity level; that no data will be either altered or lost. The hash function is introduced based on the standards of Annex 15 and DOC 10066 for data integrity.

2. DISCUSSION

2.1 The rapid growth and widespread use of digital technology increases the possibility of data manipulation and data breaches. It is vital to ensure that published aeronautical information is protected from such cases.

2.2 With reference to *DOC 10066 PANS – Aeronautical Information Management* and *Annex 15 – Aeronautical Information Services*, the implementation of cryptographic technologies should be utilized to ensure the integrity of data is maintained at all stages of the data chain - from its inception to distribution to the next intended user. The cryptographic technologies could be in the form of for e.g. hash functions, message authentication codes, asymmetric and symmetric encryption, and digital certificates.

2.3 To ensure Data integrity assurance UAE researched, identified, and introduced that MD5 (message-digest 5 cryptographic hash algorithm) the hash function, can be used to authenticate files, detection of errors and data manipulation.

2.4 The MD5 hashing algorithm uses a complex mathematical formula to create a hash. It converts data into blocks of specific sizes and manipulates that data a number of times. While this is happening, the algorithm adds a unique value into the calculation and converts the result into a small signature or hash.

2.5 Hash functions (MD5 checksum) for the AIP.zip file is provided along with each AIP update notification email, with clear instruction how to generate the hash at the users' end to verify.

2.6 Hash functions (MD5 checksum) for each file within the AIP Package is provided in an excel file along with Windows shell command for generating the codes for comparison, of each file in the package. Instructions and guidance material are provided within the package.

2.7 When the command is run, the algorithm generates specific values and any change of information will result in a different value not matching the code provided, conforming that there is a change or corruption in data. Customers are advised to report, if the MD5 checksum code generated by the customer does not match the MD5 checksum code provided by UAE GCAA AIM.

2.8 The hash function satisfies the requirement of data integrity for published aeronautical information, furthermore; provides UAE AIP users a high degree of assurance.

3. ACTION BY THE MEETING

3.1 The meeting is invited to take note of UAE experience and consider such procedures in implementation planning.

- END -