

**Integrity of Aeronautical
Information - Data
Exchange**

CHAIN

*Controlled and Harmonised
Aeronautical Information Network*

CHAIN/0029

Edition	:	1.0
Edition Date	:	29th August 2007
Status	:	Released Issue
Class	:	General Public

DOCUMENT IDENTIFICATION SHEET

DOCUMENT DESCRIPTION

Document Title
Integrity of Aeronautical Information - Data Exchange

EWP DELIVERABLE REFERENCE NUMBER

ACTIVITY REFERENCE INDEX

CHAIN/0029

EDITION :

1.0

EDITION DATE :

29th August 2007

Abstract

This document exists as one of a set of documents which provide guidance for organisations wishing to improve and enhance the integrity of their information.

It contains all the requirements which apply explicitly to the exchange of aeronautical information from one point within the data processing chain to another. Requirements for general data management and processing, as well as quality management are included within an over-arching document "Principles – Data and Quality Management".

Although provided as guidance only, it is written in a style to allow States to use as regulatory material.

Keywords

CONTACT PERSON : Manfred Unterreiner

TEL :

UNIT :

DOCUMENT STATUS AND TYPE

STATUS	CATEGORY	CLASSIFICATION
Working Draft <input type="checkbox"/>	Executive Task <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>
Draft <input type="checkbox"/>	Specialist Task <input type="checkbox"/>	EATM <input type="checkbox"/>
Proposed Issue <input type="checkbox"/>	Lower Layer Task <input type="checkbox"/>	Restricted <input type="checkbox"/>
Released Issue <input checked="" type="checkbox"/>		

INTERNAL REFERENCE NAME : EUROCONTROL Electronic Filing System

DOCUMENT APPROVAL

The following table identifies all management authorities that have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE
Author/Editor	Roy Langridge / Kathryn Miles Mileridge Limited	29 th August 2007
Activity Manager	Manfred Unterreiner EUROCONTROL	29 th August 2007
Quality Assurance	Nicholas Ashley EUROCONTROL	29 th August 2007

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION	DATE	REASON FOR CHANGE	SECTIONS PAGES AFFECTED
0.1	19 th October 2005	First Release.	All
0.2	20 th October 2005	Updated following review.	All
0.3	18 th November 2005	Updated following EUROCONTROL review.	All
0.4	18 th November 2005	Updated following review.	All
0.5	29 th January 2006	Updated following Stakeholder review.	All
0.6	26 th February 2006	Updated following further stakeholder comments.	All
0.7	19 th April 2006	Updated following further Stakeholder comments.	All
0.8	20 th September 2006	Updated with modified reference index	All
1.0	29 th August 2007	Updated for public release.	All

TABLE OF CONTENTS

1.	INTRODUCTION	1
1.1	General.....	1
1.2	Relationship with other Documents	1
1.3	Application of Guidance Material	1
1.4	Scope of this Document	1
1.5	Structure of this Document.....	1
1.6	Requirements References.....	2
2.	PRINCIPLES OF EXCHANGE	3
2.1	General.....	3
3.	DATA CONFORMANCE AND VALIDATION	5
3.1	General.....	5
3.2	Input Data.....	5
3.3	Output Data.....	5
3.4	Data Transmission	6
3.4.1	General.....	6
3.4.2	Use of the Public Internet	6
3.4.3	Loss of Integrity	7
3.4.4	Malicious Intervention.....	7
3.4.5	Misinformation	8
4.	EXCHANGE FORMATS	9
4.1	General.....	9
4.2	AIXM	9
4.2.1	General.....	9
4.2.2	Application	9
4.3	AMXS.....	9
4.3.1	General.....	9
4.3.2	Application	10
5.	KEY MANAGEMENT	11
APPENDIX A	CYCLIC REDUNDANCY CHECKS	12
A.1	General Introductions.....	12
A.2	Recommendation	12
A.3	Alternatives.....	12
	Figure 1: Secure Transmission	4

This page is intentionally left blank.

1. INTRODUCTION

1.1 General

A set of guidance material documents has been produced by EUROCONTROL to support the implementation of processes and systems throughout the Aeronautical Information data chain.

This document 'Data Exchange' describes a number of measures that should be undertaken in the exchanging of data between actors, in order to maintain data integrity.

1.2 Relationship with other Documents

This document exists as one of a set of documents aimed at providing guidance to organisations wishing to improve and enhance the integrity of their information.

A full description of the set of documents, their status and applicability may be found in the over-arching document "Integrity of Aeronautical Information Principles – Data and Quality Management".

1.3 Application of Guidance Material

This guidance material *shall* apply to all organisations within the European Civil Aviation Conference (ECAC) area involved in the management of Aeronautical Information data.

[CHAIN-0029-0010]

All organisations *shall* determine the extent to which this document applies to their own responsibilities and functions.

[CHAIN-0029-0020]

Data and quality management *shall* be deemed to be necessary throughout the data process chain from origination to publication, by the relevant National Administration responsible for Aeronautical Information Services (AIS).

[CHAIN-0029-0030]

1.4 Scope of this Document

The requirements contained in this document apply to all Aeronautical Information data which is exchanged between actors. The requirements relate to the exchange of surveyed, calculated and derived aeronautical data throughout the data process chain from surveyor, through to the AIS and publication and to the next intended user.

1.5 Structure of this Document

Section 2 specifies data exchange requirements and the recommended practices and methods to meet them, which apply to all organisations involved in the management of aeronautical data.

Section 3 explains and clarifies the meaning of the requirements of Key Management, as well as recommended practices and methods to meet those requirements.

1.6 Requirements References

Each statement of guidance, be it recorded using 'shall', 'should', or 'may', has been uniquely identified with a reference number which is enclosed in square brackets [].

These reference numbers will be used to allow requirements to be traced from the compendium of standards, through guidance and to assessment of actual performance by a State, through its auditing process.

2. PRINCIPLES OF EXCHANGE

2.1 General

Much information transmission today is performed using electronic mail which, in turn, makes use of the public Internet as a means of distribution. Whilst the Internet provides a convenient, cheap and fast means of distribution, it is open to unwanted and unauthorised interference with the information transmitted over it.

Other means of transmission may be more secure in terms of unwarranted access but may be open to loss or corruption of data.

It is, therefore, recommended that the following steps be taken to protect data from these risks during transmission:

1. Protection through CRC Wrapping (see Appendix A);
2. Encryption;
3. Digital signing.

Figure 1, opposite, shows a secure transmission. The process applied is as follows:

- A** The data as seen at the sender's location.
- B** The data has a CRCV calculated and appended.
- C** The message has a digital signature added. Although shown here as initials for clarity, digital signatures are a complex algorithm involving private and public keys.
- D** The data is encrypted so that the content and structure are no longer visible.
- E** The data is transmitted electronically from the sender to the receiver.
- F** At the receiver's location, the message is received as transmitted.
- G** The data is decrypted making both the data and structure visible again.
- H** The signature is checked to confirm that the sender was known and approved to send this information.
- I** The CRCV is checked and as, in the example shown, it is correct, the information is made available to the receiver.

Through such a process and application of suitable encryption, digital signatures and CRC algorithms, it may be guaranteed that the data received matches that sent with a sufficiently high degree of confidence to achieve the necessary integrity requirements.

Should any step have failed, at the receiver's end the data will be rejected and the sender requested to resend the information.

The subsequent chapters reflect the key requirements necessary for such a secure transmission to be achieved.

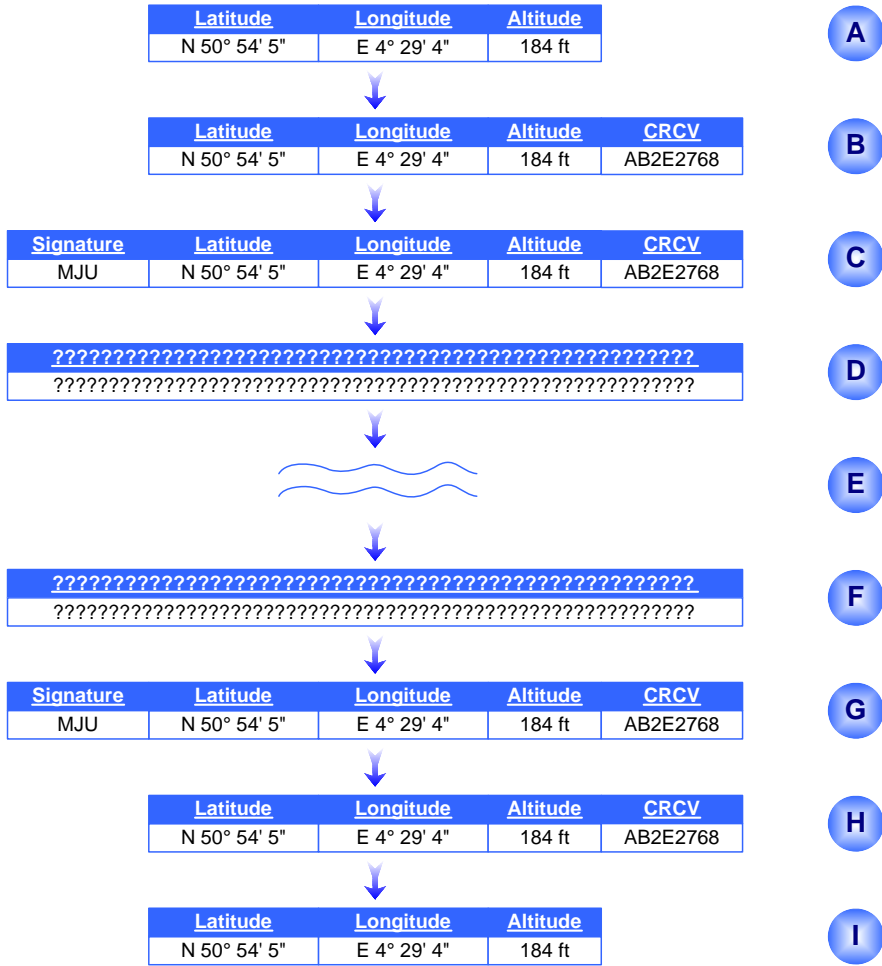


Figure 1: Secure Transmission

3. DATA CONFORMANCE AND VALIDATION

3.1 General

Having established the required integrity and design requirements for the data (see CHAIN/0028), it is necessary to develop suitably qualified data processing tools¹ and criteria at each phase of the process to deal with the various issues of conformance, validation and verification. For example, at the *RECEIVE* phase, a qualified tool shall be used to unpack the CRC for each of the data items received to confirm conformance with requirements and to ensure that the *INPUT* data is correct.

For the purposes of this discussion, *INPUT* Data is assumed to be either:

- a. Data received from another source, or
- b. Data created or generated by the organisation/entity.

OUTPUT data is the data set or sub-set being passed on to the next user in the Aeronautical Information data chain. This requirement is to ensure that the integrity of the data at *OUTPUT* is at least as good as the data at *INPUT*.

3.2 Input Data

For data received from another source, the reception criteria *shall* include the following:

- a. Confirmation of the data integrity requirement through the unpacking and validation of the CRC;

[CHAIN-0029-1010]

- b. Validation of key attributes of the data element such as:

- ◇ Position (in three axes, if appropriate);
- ◇ Resolution of values (co-ordinate data, frequency, range, etc.);
- ◇ Syntax;
- ◇ Date of implementation.

[CHAIN-0029-1020]

- c. Verification of key attributes such as:

- ◇ Position within stated country/area of stated ownership/control;
- ◇ Relative position with associated data elements (including terrain, etc.);
- ◇ Relativity with associated records (e.g., an ILS antenna cannot exist without a runway);
- ◇ Where an attribute of an existing record is changed, a logical test of which attributes have changed.

[CHAIN-0029-1030]

3.3 Output Data

In determining the output data, a number of requirements must be considered. Firstly, ICAO states that consideration must be given to the needs of the user. EUROCAE expands this, requiring that output data should include compatibility with the target system requirements.

¹ CHAIN/0028 discusses the requirements for tool qualification.

Nonetheless, it is essential that the issue of interoperability be considered and that, as far as possible, standard digital products, such as the AIXM, are used.

The needs for CRC encapsulation of the data elements and for the output data to have full internal integrity must also be considered.

3.4 Data Transmission

3.4.1 General

Whenever data is transmitted from one user to the next, processes *shall* be established to protect the data during the transfer.

[CHAIN-0029-1040]

For each phase of the process, the specific criteria for the next phase *shall* be included, together with the basic set of criteria, as shown in Section 3.2 above.

[CHAIN-0029-1050]

3.4.2 Use of the Public Internet

The public internet (The Internet) is now widely used for the exchange of aeronautical information and its use is now acknowledged by ICAO, with specific guidance being provided by way of Document 9855 (“Guidelines on the Use of the Public Internet for Aeronautical Applications”).

ICAO has addressed the use of The Internet in terms of:

1. State responsibilities;
 - a. Technical considerations;
 - b. Risk assessment;
 - c. Security.
2. Risk mitigation;
3. Information exchange:
 - a. Meteorological information;
 - b. Aeronautical Information Services;
 - c. Flight plans.

Whilst this document is primarily aimed at the provision of information between a service provider and its users, much of the material presented is equally applicable throughout the data processing chain.

States AIS, who make use of The Internet, *should* apply the guidelines provided within ICAO Doc 9855 for the provision of aeronautical information to the next intended user.

[CHAIN-0029-1060]

States *shall* undertake an assessment of the applicability of the ICAO guidelines (Doc 9855) for transfer of aeronautical information between actors within the data processing chain, prior to publication.

[CHAIN-0029-1070]

States *shall* document the assessed applicability of the ICAO guidelines (Doc 9855) for transfer of aeronautical information between actors within the data processing chain prior, to publication.

[CHAIN-0029-1080]

States *shall* act in accordance with the assessed applicability of the ICAO guidelines (Doc 9855) for transfer of aeronautical information between actors within the data processing chain, prior to publication.

[CHAIN-0029-1090]

3.4.3 Loss of Integrity

Most communications paths in use today typically provide a secure means of transmitting data, however, it is often not possible for the user to be able to guarantee this, as the checks are performed at a system level.

The application of Cyclic Redundancy Checks (CRC) provides a means by which either a user application or, through the use of suitable tools, the user him or herself may confirm the receipt or extraction of data without a loss of integrity².

The loss of integrity of data during transmission from one user to the next *shall* be protected through the use of CRC.

[CHAIN-0029-1100]

All data packets *shall* be individually protected, with a CRC Value included as part of the transmission.

[CHAIN-0029-1110]

Upon receipt, the CRC value *shall* be confirmed.

[CHAIN-0029-1120]

3.4.4 Malicious Intervention

Whilst the information published within the AIP is considered to be publicly available, there are good reasons why it is deemed advisable that the data should be encrypted during transfers within the data chain, prior to publication.

Firstly, metadata is often transmitted from point-to-point prior to publication and this information may not ordinarily be publicly available. Furthermore, some of this information may be considered commercially sensitive.

Secondly, if information is 'visible' during transfer from one point to another it may be maliciously intervened with – deliberately changed. Given that the CRC algorithm is publicly known, without encryption there would be nothing to stop somebody from intercepting data, changing it and recalculating the CRC value. Once received, the information would appear normal.

In order to protect against malicious intervention during transmission, all data *shall* be encrypted prior to forwarding and decrypted upon receipt.

[CHAIN-0029-1130]

It *shall* be the responsibility of the State to determine the means by which this encryption and decryption is achieved.

[CHAIN-0029-1140]

² Whilst a CRC does not provide a guarantee that the data has 100% integrity, the various algorithms will provide a known level of guarantee. For example, a 32-bit CRC guarantees that the integrity of information exceeds the 1×10^{-8} error rate required for critical data. For this reason, within this guidance, the use of a CRC is considered to meet the required integrity levels and hence, ensure that integrity is not lost.

3.4.5 Misinformation

With traditional means of providing information, typically paper in the form of letters, signatures were used to confirm the identity of the sender and their rights to provide the information contained.

The move to electronic transfer introduced new challenges in providing a means of authenticating the sender of information, for example, an email may be made to look like somebody sent it when they did not.

One solution to this problem is the use of electronic signatures. These provide a means of signing information to guarantee that it has been sent by the person who claims to have done so and, secondly, a means of proving that the information was sent by somebody in the event of dispute (non-repudiation).

To prevent an impostor who has assumed the identity of a legitimate body from transmitting data to a user, digital signing *shall* be used for all data transmission.

[CHAIN-0029-1150]

Such signing *shall* be used both to protect against fraudulent messages and as a means of providing non-repudiation.

[CHAIN-0029-1160]

4. EXCHANGE FORMATS

4.1 General

To allow the most efficient and flexible approach to the exchange of aeronautical information, the use of digital formats is recommended. Furthermore, true interoperability of systems within and across States may only be achieved through the adoption of common formats.

4.2 AIXM

4.2.1 General

The Aeronautical Information Exchange Model (AIXM) has been established to allow for the digital exchange of aeronautical information in a computer literate form. Whilst it is primarily intended for the exchange of complete features (e.g. a Navaid), it may be used to exchange incomplete features (e.g. the location of a Navaid only), however, in this latter case, without the same levels of validation being achieved.

The AIXM has been developed using the eXtensible Mark-up Language (XML) which permits a computer to fully understand the content of a message and hence be able to perform automatic processing of it.

The AIXM update message is used to provide aeronautical information related to a feature and includes aspects such as temporality. The newer releases of AIXM are extensible, allowing additional metadata to be included in a transfer.

4.2.2 Application

Wherever aeronautical AIP data is exchanged digitally between two points within the data chain, the AIXM update message *should* be used.

[CHAIN-0029-2010]

Software tools and applications in place which are used to create, transmit and receive the AIXM update message, *shall* validate the data values present in the message.

[CHAIN-0029-2020]

When a complete AIXM entity has been created, full validation against the AIXM schema *shall* be performed.

[CHAIN-0029-2030]

The extensibility features of the AIXM *shall* be used to provide the associated metadata within the same AIXM update message.

[CHAIN-0029-2040]

4.3 AMXS

4.3.1 General

The Airport Mapping Exchange Schema (AMXS) has been established in a similar vein to the AIXM but aimed specifically at the exchange of information involved in the display of airport maps. The technology used is Geography Mark-up Language (GML) which is a subset of XML.

4.3.2 Application

Wherever airport mapping data is exchanged digitally between two points within the data chain, the AMXS *shall* be used.

[CHAIN-0029-2050]

Software tools and applications in place which are used to create, transmit and receive AMXS messages, *shall* validate the data values present in the message.

[CHAIN-0029-2060]

When a complete AMXS entity has been created, full validation against the AMXS schema *shall* be performed.

[CHAIN-0029-2070]

The extensibility features of the AMXS *shall* be used to provide the associated metadata within the same AMXS update message.

[CHAIN-0029-2080]

5. KEY MANAGEMENT

The introduction of encryption and digital signatures brings about the necessity for the management of the corresponding keys – an essential component in their operation.

It is, therefore, proposed that the key management within a State be performed by a designated body, such as the regulator. Whether, in turn, the actual day-to-day management is contracted to one of the commercial key management companies would then be an internal decision of the State.

Each State *should* consider nominating a single body, the Certification Authority, responsible for the management of the keys used for encryption and digital signatures within that State.

[CHAIN-0029-3010]

The Certification Authority *should* only issue keys to those organisations considered competent to perform their allocated duties.

[CHAIN-0029-3020]

States *should* consider allocating keys to individuals within a role or function as this allows for easier management of keys, as a result of staff turnover.

[CHAIN-0029-3030]

APPENDIX A CYCLIC REDUNDANCY CHECKS

A.1 General Introductions

This guidance has been provided on the basis that use is made of Cyclic Redundancy Check values to prove, to a mathematically proven degree of certainty, that data has not been amended or corrupted from that for which the original CRC Value (CRCV) was calculated.

The use of CRC is widespread and is the most common form of check used to ensure that the information contained within a dataset has not been changed. It forms the basis of the methodology employed within internet communications to ensure that the information received has not been corrupted. Many international organisations have adopted the use of CRC within their standards, such as the International Organisation for Standardisation (ISO), the Institute of Electrical and Electronics Engineers (IEEE) and, most importantly in our domain, ICAO.

CRC also forms an inherent part of many other technologies used for data security and CRCs are utilised within most digital signature and encryption technologies in use today.

A.2 Recommendation

The use of CRC technology for all storage and exchange of data has been recommended for a number of reasons:

- a. It is the ICAO mandated technology;
- b. It is the most widely used and accepted technology;
- c. Interoperability is aided if all actors and systems involved make use of the same technology;
- d. Through the use of supporting tools (which are widely available) its use is relatively simple.

A.3 Alternatives

Whilst the use of alternatives would be discouraged, should a State wish to implement alternative methods which may also demonstrate the assurance of integrity, both in storage and distribution, then this may be permitted. Such a decision should not be taken lightly, however, as interoperability may be lost (and hence, result in a loss of integrity) and a non-compliance with ICAO SARPs and the Single European Sky Common Requirements result.

End of Document