

AMENDMENT LIST NUMBER 9 TO THE
TECHNICAL SPECIFICATION
FOR IGC-APPROVED GNSS FLIGHT RECORDERS

EFFECTIVE 1 JULY 2006

ISSUED BY FAI
ON BEHALF OF THE INTERNATIONAL GLIDING COMMISSION

Glossary, Add:

ECC - Elliptic Curve Cryptography. A patented second-generation Public/private Key-based Cryptographic (PKC) system. It has a smaller private key length compared to systems such as RSA and DSA for the equivalent level of electronic security. For IGC flight recorder purposes, ECC with a 160 bit private key is accepted as equivalent to RSA with a 512 bit key. See: http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm . See also in this Glossary under DSA, PKC and RSA. (AL9)

1.3.4.2 Pressure Altitude Calibration. To read: "... a calibration table and the IGC file for the calibration from which the figures in the table were obtained must be ... ".

2.1.1 IGC Responsibility. New sub-para: 2.1.1.1 IGC disclaimer. Where modules and sub-systems are used by a manufacturer in a particular design of recorder and do not originate from that manufacturer, it is the responsibility of the recorder manufacturer to ensure that any Intellectual Property Rights (IPR) pertaining to the module or sub-system concerned are properly covered. This includes the fulfilment of patent and equivalent requirements. Such modules or sub-systems may consist of hardware, firmware, software, or a mixture. FAI and IGC have no responsibility for such rights and agreements as part of the IGC-approval process and proceed on the basis that the recorder manufacturer has obtained them for the international use of the recorder concerned. (AL9)

2.7.1.1 New para 2.7.1.1 as follows: Recorder functions not to be interfered with. Where the flight recorder is part of a larger system with other functions as well as the recording of flight data, the flight recorder functions and their security devices must be kept separate (in design terms) from other, wider functions of the design. This also applies to a recorder design that includes modules inside it that have functions other than the recording of flight data to the IGC criteria. The manufacturer must be able to show that the design is such that there can be no un-scheduled interference with the recording functions, the security of their output and download of data. (AL9)

2.7.2.2.2 Antenna. Delete last two sentences about the need for an interface cable so that the 4mm SMC connector can be used with an antenna connector with the 9mm BNC bayonet. Reason, customer choice rather than a Specification matter.

2.8.3.1 Message Digest. Title, add "and Public/Private Keys".

New 2.8.3.1.1, re-number existing 2.8.3.8.1 as 2.8.3.8.2.

2.8.3.1.1 Public and Private Keys. It must be ensured that the minimum number of persons have knowledge of any security keys and details of any encryption used in IGC-approved recorders. Such knowledge must be confined to persons at the manufacturer's facility and not, for instance, passed on to agents or others in such a way that they could build a list of such keys. (AL9)

2.8.3.1.1.1 Public Keys. The purpose of the public key is to check that the IGC file was digitally signed with the unique private key that is held in each recorder. As used in IGC-approved recorders, the public key is not intended to be available "in clear" to everyone, but should be regarded as a confidential part of the IGC security system in the same way as the private key. The batch of public keys that a manufacturer intends to use with a production run of IGC-approved recorders must be encrypted and embedded in the DLL file supplied by the manufacturer and that is posted on the IGC GNSS web pages for use with the IGC Shell program (or for older recorders, in the VALI-XXX program file). A DLL is expected to contain at least 500, and preferably 1000 encrypted public keys, to allow for a production run of this number of recorders, each with their own unique key pair. It is not acceptable to have public keys embedded in the recorder and/or the IGC output file, even if encrypted. (AL9)

2.8.3.1.1.2 Private Keys. Before initial sale, a private key of the appropriate length must be placed in the flight recorder by the manufacturer in such a way that it will be erased if the recorder is opened or otherwise tampered with. After sale, if a security re-set becomes necessary, it may be replaced only by the manufacturer or by an agent authorised by the manufacturer to re-set the security of the recorder having obtained replacement key data from the manufacturer in a secure way. (AL9)

Existing 2.8.3.1.1 (re-numbered as 2.8.3.1.2) RSA, DSA and data transfer times.

Change title to "Public/Private Key Cryptography (PKC) systems and data transfer times."

After "The DSA system (see Glossary) is a permissible alternative to RSA and may give shorter times for data transfer from the GNSS FR to a PC." add "The ECC system (see Glossary) is also a permissible alternative and enables a shorter private key length to be used compared to RSA and DSA for a similar level of electronic security."

2.10.1 Calibration. First sentence, after "output", add "as recorded in the IGC file". Also, under sub-para (c) change "Chapter 3" to "Chapter 2".

Appendix 1 - IGC Data File Format

1.1.1.1 Third sentence from the end, add "external" before power".

Para 2.4, Units, time, line 1 to read "UTC obtained from the same GNSS data package from which the recorded lat/long and GPS altitude are also obtained, or, if GPS is not locked on, from the Real-Time Clock in the recorder"

Para 2.5.6 Manufacturer Codes. Add: Aircotec - ACT - I

Para 3.3.1 Header Record. Add a row to the table: FR Type line - As required - F - Includes detailed model data including sub-types. For instance, not only the Model XXX 1 but 1a,1b, etc. (AL9)

Para 3.6.1 Declaration. Second sentence to start: "Optionally, the recorder may be configured ..."

Para 4.1 B RECORD - FIX. In last column of table: For Time UTC, add: "When a valid GNSS fix is received, the UTC time in a B-record line must be obtained directly from the same GNSS data package that was the source of the Lat/long and GPS altitude that is recorded in the same B-record line. Other sources for the time in a B-record line (such as the Real-Time Clock in the recorder) must only be used

to provide time-continuity where GNSS fixes are not available (AL9)". In the table, for Latitude, Longitude and GNSS altitude, add in the last column "obtained directly from the same GPS data package that was the source of the UTC time that is recorded in the same B-record line (AL9)".

Para 4.2 E RECORD - EVENTS. To start: "The E-record is used to record specific events on the IGC file that occur at irregular intervals. Such events include a pilot-initiated event (PEV code) or, for recorders fitted with proximity sensing devices, a proximity event using one of the appropriate Three-Letter Codes followed by the appropriate data as defined under the appropriate TLC in para 7. The E Record is placed before the individual fix (B) Record for the same time ... "

Appendix 3 - Windows-based short programs

1.1 General. Delete reference to Windows 98, updates no longer supported by Microsoft and needs drivers for many programs including for the IGC Shell with manufacturers DLLs

2.1 Change "Windows 95/98/ME, NT/2000, and subsequent releases" to "Windows XP Home and Professional and subsequent releases of the XP system".
