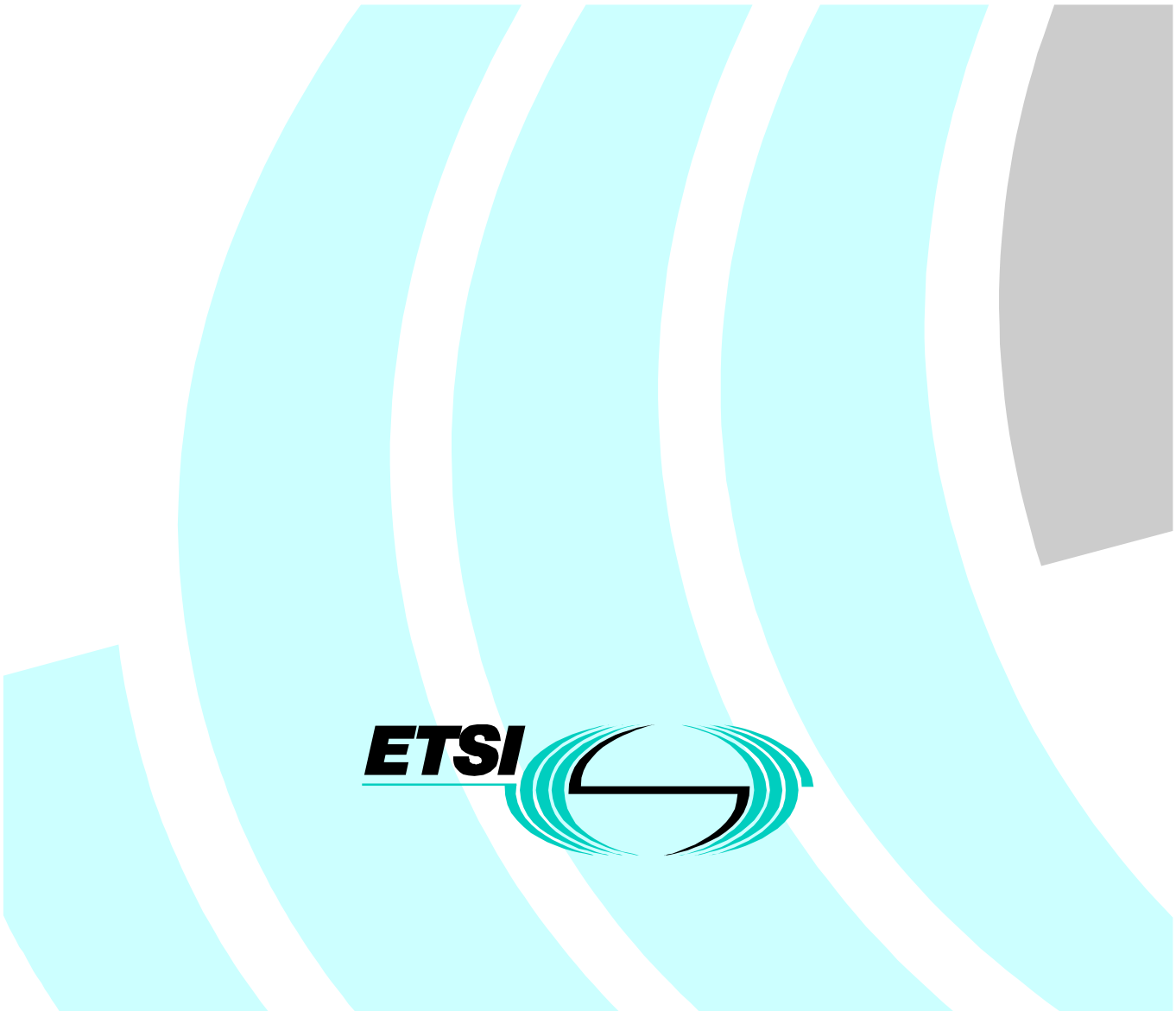
ETSI TR 101 740 V1.1.1 (1999-08)

Technical Report

Security algorithms Group of Experts (SAGE); Rules of the management of the standard GSM GPRS Encryption Algorithm 2 (GEA2)



Reference
DTR/SAGE-00019-1 (g4000ics.PDF)

Keywords
algorithm, GSM, security

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by Advisory Committee Security Algorithms Group of Experts (SAGE).

1 Scope

The purpose of the present document is to specify the rules for the management of the Standard GSM GPRS Encryption Algorithm 2 (GEA2).

The management structure is defined in clause 4. This structure is defined in terms of the principals involved in the management of the GEA2 (ETSI, ETSI SMG, GEA2 Custodian and Approved Recipients) together with the relationships and interactions between them.

The procedures for delivering the GEA2 to Approved Recipients are defined in clause 5. This clause is supplemented by Annex A which specifies the items which are to be delivered.

Clause 6 is concerned with the criteria for approving an organization for receipt of the GEA2 and with the responsibilities of an Approved Recipient. This clause is supplemented by Annex B which contains a Confidentiality and Restricted Usage Undertaking to be signed by each Approved Recipient.

Clause 7 is concerned with the appointment and responsibilities of the GEA2 Custodian.

The specification of the GEA2 consists of the following three documents:

1) Specification of the GPRS Encryption Algorithm 2 (GEA2)
   Document 1: Algorithm Specification.

2) Specification of the GPRS Encryption Algorithm 2 (GEA2)
   Document 2: Design Conformance Test Data.

3) Specification of the GPRS Encryption Algorithm 2 (GEA2)
   Document 3: Algorithm Input/Output Test Data.

The rules for management as described in the present document apply for Document 1 and Document 2 only. Document 3 will be a publicly available document and its distribution will not be subject to any rules.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

GSM 02.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 1 (GSM 02.60 version 6.2.1 Release 1997)".

GSM 03.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description;Stage 2 (GSM 03.60 version 7.0.0 Release 1998)".

GSM 03.64: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Overall description of the GPRS radio interface; Stage 2 (GSM 03.64 version 7.0.0 Release 1998)".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

GEA2	GSM GPRS Algorithm 2
GPRS	General Packet Radio Service
GSM	Group Special Mobile
SAGE	Security algorithms Group of Experts

4 GEA2 Management Structure

The management structure is depicted in Figure 1. The figure shows the three principals involved in the management of the GEA2 and the relationships and interactions between them.

ETSI is the owner of the GEA2 algorithm. The ETSI Secretariat together with ETSI SMG sets the approval criteria for receipt of the algorithm (see clause 6).

The GEA2 Custodian is the interface between ETSI and the Approved Recipients of the GEA2.

The custodian shall be the ETSI Secretariat unless it is decided by ETSI Secretariat and/or ETSI SMG to delegate this task to a third party on the basis of an agreement signed between the latter and the ETSI Secretariat.

The GEA2 Custodian's duties are detailed in clause 7. They include distributing the GEA2 to Approved Recipients, as detailed in clause 5, providing limited technical advice to Approved Recipients and providing algorithm status reports to ETSI SMG.

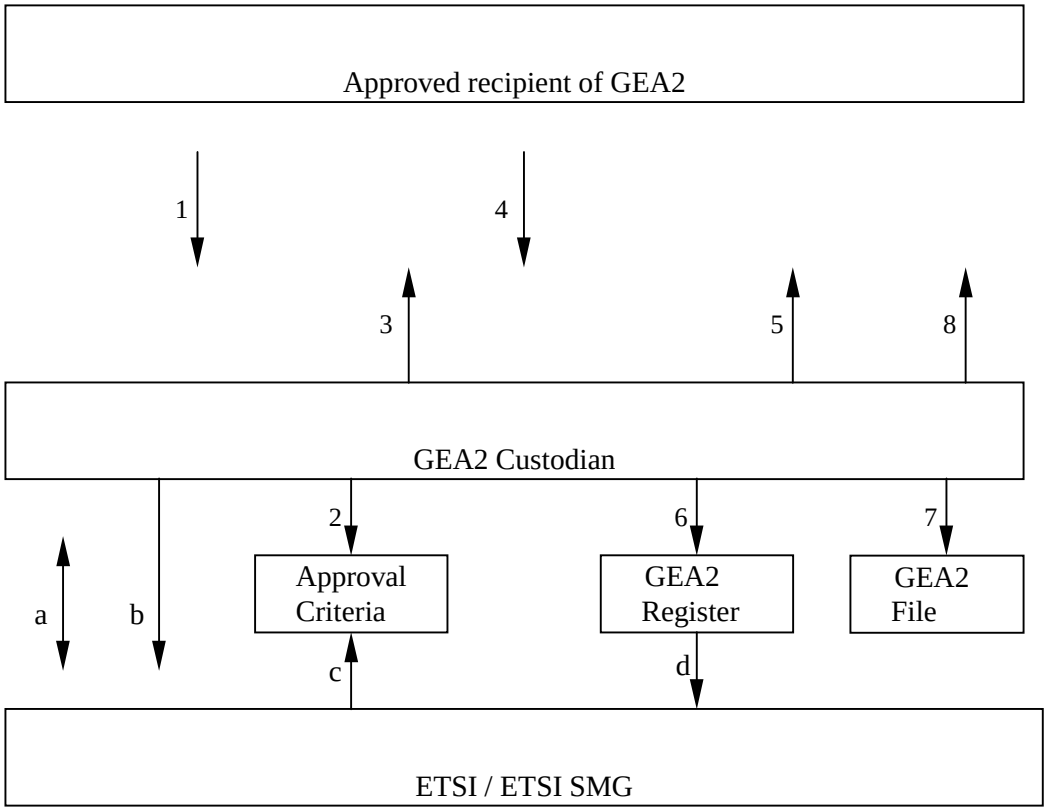


Figure 1: GEA2 Management Structure

Key to Figure:

a	=	Agreement between GEA2 Custodian and ETSI;
b	=	Status reports and recommendations;
c	=	Setting of approval criteria;
d	=	Restricted details of the GEA2 register.
1	=	Request for GEA2;
2	=	Check of request against approval criteria;
3/4	=	Exchange of Confidentiality and Restricted Usage Undertaking;
5	=	Dispatch of GEA2 Specification;
6	=	Update the GEA2 register;
7	=	Document filing;
8	=	Technical advice.

5 Distribution Procedures

5.1 Distribution by GEA2 Custodian

The following procedures for distributing the GEA2 to Approved Recipients are defined with reference to Figure 1.

1) The GEA2 Custodian receives a written request for N copies of the GEA2 Specification (see note 1), where N should not be bigger than six.

2) The GEA2 Custodian checks whether the requesting organization meets the approval criteria (see clause 6).

3) If the request is approved, the GEA2 Custodian dispatches 2 copies of the Confidentiality and Restricted Usage Undertaking (as given in Annex B) for signature by the Approved Recipient (see notes 2 and 6) together with a copy of this document (Rules for the Management of the Standard GSM GPRS Encryption Algorithm 2).

4) Both copies of the Confidentiality and Restricted Usage Undertaking shall be signed by the approved recipient (see notes 5 and 7) and returned to the GEA2 Custodian, together with the payment of charges if any.

5) The GEA2 Custodian sends up to N (note 3) numbered copies of the GEA2 Specification to the Approved Recipient, together with one countersigned copy of the returned Confidentiality and Restricted Usage Undertaking and a covering letter (see notes 4 and 6).

6) The GEA2 Custodian updates the GEA2 Register by recording the name and address of the recipient, the numbers of the copies of the GEA2 Specification delivered and the date of delivery. If the original request is not approved, the GEA2 Custodian records the name and address of the requesting organization and the reason for rejecting the request in the GEA2 Register (see also note 8).

7) The GEA2 Custodian countersigns and files the second returned copy of the Confidentiality and Restricted Usage Undertaking in the GEA2 File together with a copy of the covering letter sent to the Approved Recipient.

NOTE 1: Requests for the GEA2 Specification may be made directly to the GEA2 Custodian or through ETSI, where appropriate.

NOTE 2: The confidentiality and Restricted Usage Undertaking specifies the number of copies requested.

NOTE 3: The covering letter specifies the numbers of the copies delivered.

NOTE 4: The GEA2 Custodian shall send all items listed in Annex A. Requests for part of the package of items are rejected.

NOTE 5: An organization may request the specification on behalf of a second organization to which it is subcontracting work which requires the specification. In this case, the first organization is responsible for returning a Confidentiality and Restricted Usage Undertaking signed by the second organization. Refer to the Transfer details given in subclause 5.2.

NOTE 6: Under normal circumstances the Custodian is expected to respond within 25 working days, excluding the delay of the procedures with the National Authorities.

NOTE 7: The approved recipient shall be a legal representative of the receiving organization.

NOTE 8: If a GEA2 Specification is returned to the GEA2 Custodian (for example the recipient may decide not to make use of the information), then the GEA2 Custodian shall destroy the specification and enter a note to this effect in the GEA2 Register.

5.2 Transfers by a Beneficiary

An organization which has already been approved and has obtained GEA2 specification may transfer one or more of these specifications to a second organization which requires the specification.

In this case, the first organization shall ensure that the second organization meets the approval criteria. The first organization shall get the second organization to sign two copies of the Confidentiality and Restricted Usage Undertaking. The first organization then sends these to the GEA2 Custodian, together with the numbers of the specifications which are to be transferred.

The GEA2 Custodian then enters the transfer details in the GEA2 Register, countersigns the Confidentiality and Restricted Usage Undertakings, returns one of these together with a covering letter to the first organization , and files the other and a copy of the letter in the GEA2 File.

The first organization is responsible for passing (a copy of) the countersigned Confidentiality and Restricted Usage Undertaking to the second organization.

6 Approval Criteria

The approval criteria are set by the ETSI Secretariat together with ETSI SMG and maintained by the GEA2 Custodian. The GEA2 Custodian may recommend changes to these criteria.

In order for an organization to be considered an Approved Recipient of the GEA2 it shall satisfy at least one of the following criteria:

C1	The organization is designer of or competent to manufacture GSM GPRS systems, where the GEA2 is included in the systems.
C2	The organization is designer of or competent to manufacture components for GSM GPRS systems, where at least one of the components includes the GEA2.
C3	The organization is designer of or competent to manufacture a GSM GPRS system simulator for approval testing of GSM GPRS systems, where the simulator includes the GEA2.
C4	The organization is an operator of a GSM GPRS system which includes the GEA2.

The GEA2 Custodian will decide whether an organization requesting the GEA2 Specification may be considered to be an Approved Recipient. Any doubtful cases will be referred back to ETSI Secretariat or ETSI SMG.

7 The GEA2 Custodian

7.1 Responsibilities

The GEA2 Custodian is expected to perform the following tasks:

T1	To approve requests for the GEA2 by reference to the Approval Criteria given in clause 6.
T2	To exchange the Confidentiality and Restricted Usage Undertaking with Approved Recipients as described in clause 5.
T2bis	To obtain the Administrative authorization and export licences required by the National Authorities of its country if any.
T3	To distribute the GEA2 Specification as detailed in clause 5 (see note 1).
T4	To maintain the GEA2 Register as described in clause 5.
T5	To hold in custody the contents of the GEA2 File as specified in clause 5.
T6	To provide recipients of the GEA2 with limited technical support, i.e, answer written queries arising from the specification or test data (see note 2).
T7	To advise ETSI/ETSI SMG of any problems arising with the approval criteria.

T8 In the light of written queries from recipients of the GEA2 Specification, to make recommendations to ETSI/ETSI SMG for improvements/corrections to the specification and, subject to ETSI/ETSI SMG approval, make and distribute the changes (see note 3).

T9 To provide ETSI/ETSI SMG with information from the GEA2 Register when requested to do so.

NOTE 1: Registered postage will be used. If recipients require a different delivery service then they can be expected to pay the full costs.

NOTE 2: The GEA2 Custodian will only endeavour to answer questions relating to the GEA2 Specification. He is not expected to provide technical support for development programmes.

NOTE 3: Numbered copies of any changes to the GEA2 Specification shall be automatically distributed to all recipients of the specification and a record of the distribution entered in the GEA2 Register.

7.2 Appointment

The GEA2 Custodian is:

ETSI Secretariat

The contact person is:

Mr Pierre De Courcel Fax +33 4 93 65 47 16

ETSI Email pierredecourcel@etsi.fr

F-06921 Sophia Antipolis Cedex

France

The GEA2 Custodian will ask a fee from the recipient to cover the cost of distribution of the specification document 1 and specification document 2. This fee is set to EURO 1000,-per request.

The GEA2 Custodian may ask an optional fee from the recipient to cover the cost of distribution of the specification document 3.

All requests for either the GEA2 specification document 1 and specification document should be addressed to the indicated contact person or to ETSI.

Annex A (informative): Items delivered to Approved Recipient of GEA2

ITEM-1: Up to N numbered copies to the GEA2 Specification where N is the number of copies requested.

ITEM-2: A countersigned Confidentiality and Restricted Usage Undertaking.

ITEM-3: A cover letter from and signed by the GEA2 Custodian listing the delivered items (ITEM-1 and ITEM-2 above) and the numbers of the specifications delivered (see note).

NOTE: In the case of a transfer (see subclause 5.2), only ITEM-2 and the cover letter are delivered. Moreover, the cover letter details the numbers of the transferred specifications.

Annex B (informative): Confidentiality and Restricted Usage Undertaking

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the GPRS Encryption Algorithm 2 for the protection of the information exchanged over the radio channels of a GSM General Packet Radio Service (GPRS) System.

Between

(COMPANY NAME) .....

(COMPANY ADDRESS) .....

.....

.....

.....

hereinafter called: the BENEFICIARY;

and

(COMPANY NAME) .....

(COMPANY ADDRESS) .....

.....

.....

.....

hereinafter called: the CUSTODIAN.

Whereas:

The BENEFICIARY has alleged supported by additional information provided, that he fulfils at least one of the following criteria:

* He is designer of or competent to manufacture GSM GPRS where GSM GPRS Standard Encryption Algorithm 2 (hereinafter referred to as GEA2) is included in the systems.

* He is designer of or competent to manufacture components for GSM GPRS systems where at least one of the components include the GEA2.

* He is designer of or competent to manufacture GSM GPRS system simulator for approval testing of GSM GPRS systems where the simulator includes the GEA2.

The CUSTODIAN undertakes to give to the BENEFICIARY:

- registered copies of the detailed specification of the confidentiality algorithm GEA2 for protection of the information exchanged over the radio channels of a GSM GPRS system.

The BENEFICIARY undertakes:

1) To keep strictly confidential all information contained in the detailed specification of the GEA2 and all related communications written or verbal which have been associated with that information before and after the signature of the present undertaking (the "INFORMATION").

2) Not to make copies of the GEA2 specifications (all copies of these specifications shall be produced, numbered and registered by the GEA2 Custodian).

3) Not to disclose the INFORMATION to any third party without prior and explicit authorization in writing by the CUSTODIAN.

4) To the best of his ability to take measures to avoid that his personnel disclose to third parties, without prior and explicit authorization in writing by the CUSTODIAN, all or part of the INFORMATION.

5) To use the INFORMATION in the GEA2 specification exclusively for the provision of GSM GPRS components, systems or services, thus refraining from making any other use of the GEA2 or information in the GEA2 specification.

6) Not to register, or attempt to register, any IPR (patents or the like rights) relating to the GEA2 and containing all or part of the INFORMATION.

7) To design his equipment, to the best of his ability, in a manner that protects the GEA2 from disclosure and ensures that it cannot be used for any purpose other than to provide the GSM GPRS services for which it is intended.

   These services are specified in the documents: ETSI GSM 02.60 (GPRS Service Description: Stage 1), ETSI GSM 03.60 (GPRS Service Description: Stage 2), and ETSI GSM 3.64 (Overall description of the GPRS Radio Interface: Stage 2).

8) Not to subcontract any part of the design and build of his equipment, or the provision of his GSM GPRS services, which requires a knowledge of the GEA2, to any organization which has not signed the Confidentiality and Restricted Usage Undertaking.

9) Not to publish a description or analysis of any aspects which may disclose the operation of the GEA2 in any document that is circulated outside the premises of the BENEFICIARY.

The above restriction shall not apply to information which:

- is or subsequently becomes (other than by breach by the BENEFICIARY of its obligations under this agreement) public knowledge; or

- is received by the BENEFICIARY without restriction on disclosure or use from a third party and without breach by a third party of any obligations of confidentiality to the CUSTODIAN.

If, after five years from the effective date hereof, the BENEFICIARY has not used the INFORMATION, or if he is no more active in the business mentioned above, he shall return the written INFORMATION which he has received. The BENEFICIARY is not authorized to keep copies or photocopies; it is forbidden for him to make any further use of the INFORMATION.

In the event that the BENEFICIARY breaches the obligations of confidentiality imposed on him pursuant to items 1 to 9 above and ETSI demonstrates that it has suffered loss as a direct result of such breach, the BENEFICIARY agrees to indemnify ETSI for such reasonable losses which are a direct result of such breach provided that such indemnity shall

not extend to any losses incurred by ETSI as a result of any third party claiming against ETSI for any consequential or incidental losses (including loss of profits) suffered by that third party.

All disputes which derive from the present undertaking or its interpretation shall be settled by the Court of Justice situated in Grasse (Alpes Maritimes), in accordance with the procedures of this Court of Arbitration and with the application of French Law regarding questions of interpretation.

The obligations of confidentiality herein shall not apply vis-à-vis other BENEFICIARIES. Evidence of being a BENEFICIARY shall be given by providing a certified copy of this undertaking duly undersigned.

This undertaking supersedes all prior confidentiality and restricted scope undertakings between the parties and constitutes the entire agreement between the parties. All amendments to this undertaking shall be agreed in writing and signed by a duly authorized representative of each of the parties.

Made in two originals, one of which is for the PROVIDER, the other for the BENEFICIARY.

For the CUSTODIAN	For the BENEFICIARY
.....	.....
.....	.....
(Name, Title (typed))	(Name, Title (typed))
.....	.....
(Date)	(Date)

History

Document history		
V1.1.1	August 1999	Publication

ISBN 2-7437-3464-7
Dépôt légal : Août 1999