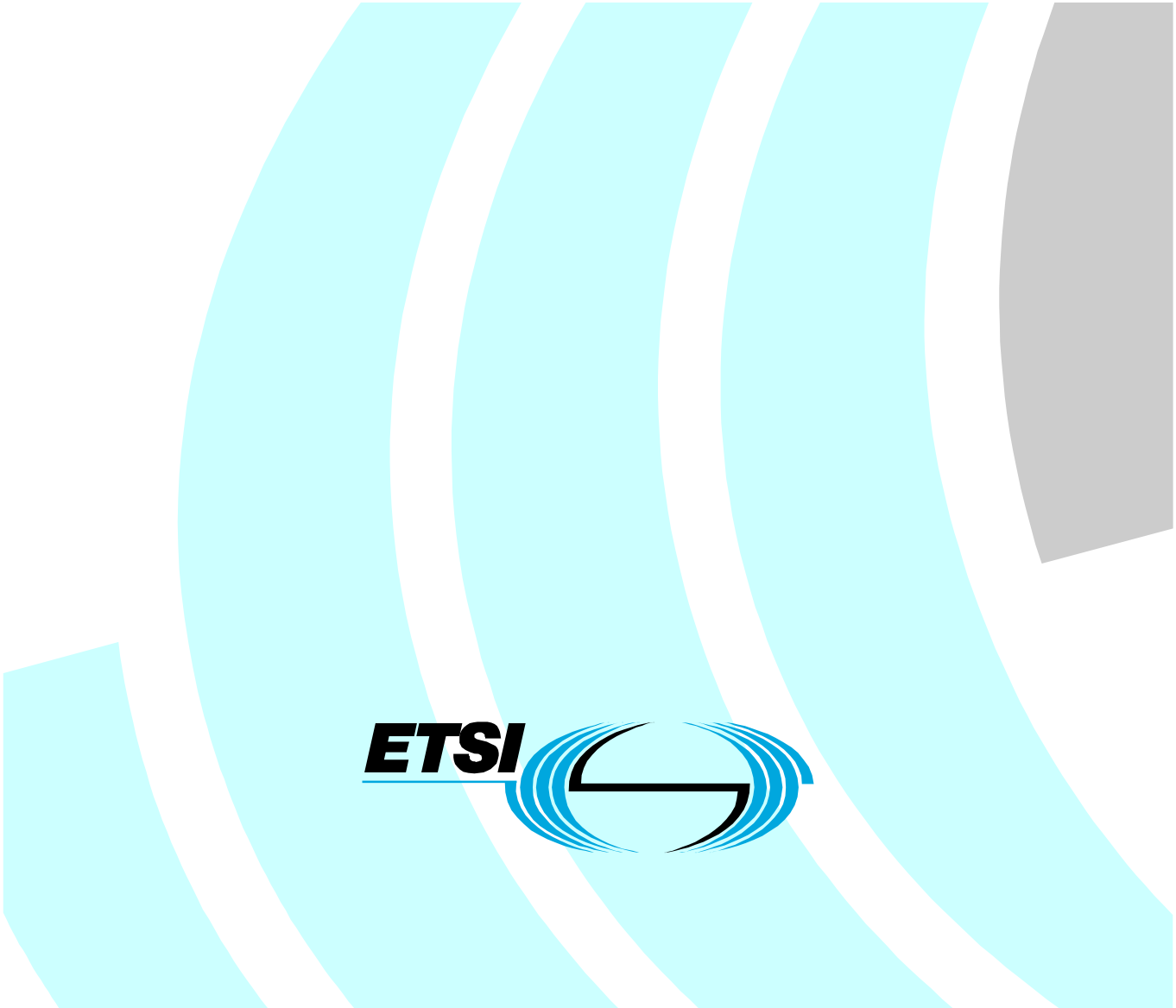
# ETSI TR 101 053-1 V1.1.2 (2006-01)

*Technical Report*

**Security Algorithms Group of Experts (SAGE);
Rules for the management of the TETRA standard encryption algorithms;
Part 1: TEA1**



Reference
RTR/SAGE-00023-1

Keywords
algorithm, security, TETRA

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - 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

# 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 ETSI 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://webapp.etsi.org/IPR/home.asp).

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 ETSI 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).

The present document is part 1 of a multi-part deliverable covering the rules for the management of the TETRA standard encryption algorithms, as identified below:

**Part 1: "TEA1";**

Part 2: "TEA2";

Part 3: "TEA3";

Part 4: "TEA4".

# 1 Scope

The purpose of the present document is to specify the rules for the management of the TETRA standard encryption algorithm TEA1. This algorithm is intended for air interface encryption in TETRA products.

The specification for TEA1 consists of the following three parts:

Part 1: Algorithm specification;

Part 2: Design conformance test data;

Part 3: Algorithm input/output test data.

The procedures described in the present document apply to Parts 1 and 2 of the specifications. Parts 1 and 2 are confidential for each of the algorithms.

Part 3 of each of the specifications is not confidential and can be obtained directly from the TEA4 Custodian (see clause 5.3). There are no restrictions on the distribution of this part of the specifications.

The management structure is defined in clause 4. This structure is defined in terms of the principals involved in the management of the TEA1 (ETSI, ETSI PROJECT TETRA, TEA1 Custodian and approved recipients) together with the relationships and interactions between them.

The procedures for delivering the TEA1 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 TEA1 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 TEA1 Custodian. Furthermore in this clause the temporary role of the Interim Custodian is described.

# 2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[2] ETSI ETS 300 393-7: "Terrestrial Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 7: Security".

[3] ETSI EN 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

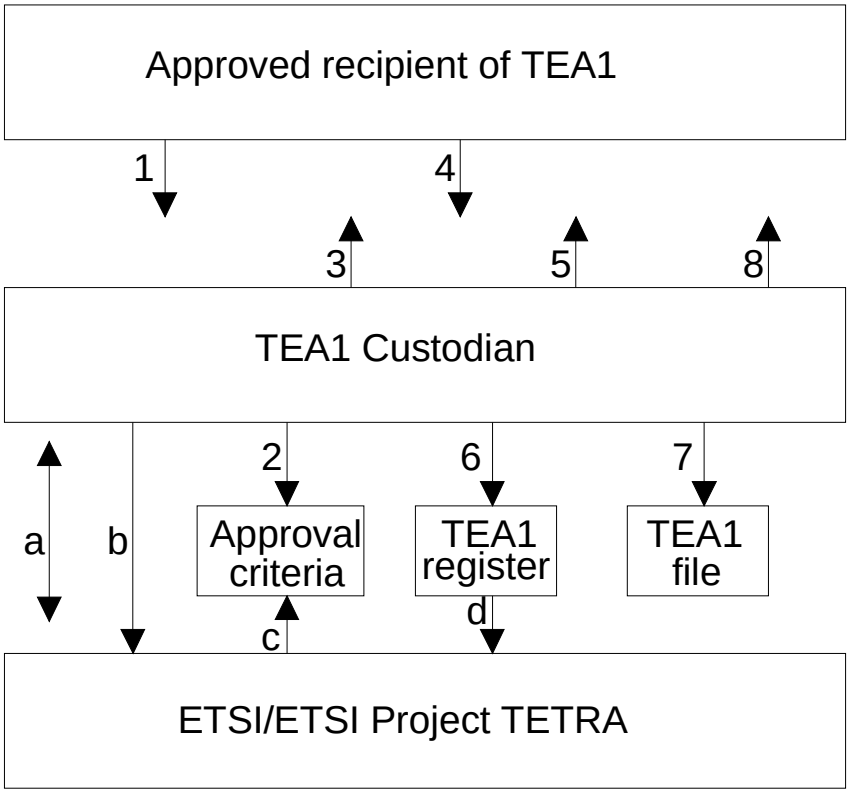
# 3 Abbreviations

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

| | |
|---|---|
| CRUU | Confidential and Restricted Usage Undertaking |
| TEA1 | TETRA Encryption Algorithm No. 1 |
| TETRA | TErrestrial Trunked RAdio |

# 4 TEA1 management structure

The management structure is depicted in figure 1.




Key:
a = Agreement between TEA1 Custodian and ETSI
b = Status reports and recommendations
c = Setting of approval criteria
d = Restricted details of the TEA1 register
1 = Request for TEA1
2 = Check of request against approval criteria
3 and 4 = Exchange of Confidentiality and Restricted Usage Undertaking
5 = Dispatch of TEA1 specification
6 = Update the TEA1 register
7 = Document filing
8 = Technical advice

**Figure 1: TEA1 management structure**

Figure 1 shows the three principals involved in the management of the TEA1 and the relationships and interactions between them.

ETSI is the owner of TEA1. The ETSI Secretariat together with ETSI Project TETRA sets the approval criteria for receipt of the algorithm (see clause 6).

The TEA1 Custodian is the interface between ETSI and the approved recipients of TEA1.

The Custodian shall be the ETSI Secretariat unless it is decided by ETSI Secretariat and/or ETSI Project TETRA to (temporarily) delegate this task to a third party on the basis of an agreement between the latter and the ETSI Secretariat. The TEA1 Custodian's duties are detailed in clause 7. They include distributing TEA1 to approved recipients, as detailed in clause 5, providing limited technical advice to approved recipients and providing algorithm status reports to ETSI Project TETRA.

# 5 Distribution procedures

## 5.1 Distribution by TEA1 Custodian

The following procedures for distributing TEA1 to approved recipients are defined with reference to figure 1.

1) The TEA1 Custodian receives a written request for N copies of the TEA1 specification (see note 1).

2) The TEA1 Custodian indicates whether the requesting organization meets the approval criteria (see clause 6). In case of non-compliance of the organization with the approval criteria, the Custodian shall justify its decision.

3) If the request is approved, the TEA1 Custodian dispatches 2 copies of the corresponding 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 TETRA standard encryption algorithm TEA1).

4) Both copies of the Confidentiality and Restricted Usage Undertaking (CRUU) shall be signed by the approved recipient (see notes 5 and 7) and returned to the TEA1 Custodian, together with the payment of charges if any.

5) The TEA1 Custodian sends up to N (see note 3) numbered copies of the TEA1 specification to the approved recipient, together with one countersigned copy of the returned Confidentiality and Restricted Usage Undertaking (CRUU) and a covering letter (see notes 4 and 6).

6) The TEA1 Custodian updates the TEA1 Register by recording the name and address of the recipient, the numbers of the copies of the TEA1 specification delivered and the date of delivery. If the original request is not approved, the TEA1 Custodian records the name and address of the requesting organization and the reason for rejecting the request in the TEA1 Register (see also note 8).

7) The TEA1 Custodian countersigns and files the second returned copy of the Confidentiality and Restricted Usage Undertaking (CRUU) in the TEA1 File together with a copy of the covering letter sent to the approved recipient.

8) The TEA1 Custodian may provide very limited technical advice with respect to answering questions concerning the TEA1 specification.

NOTE 1: Requests for the TEA1 specification may be made directly to the TEA1 Custodian or through ETSI, where appropriate.

NOTE 2: The Confidentiality and Restricted Usage Undertaking (CRUU) specifies the number of copies requested.

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

NOTE 4: The TEA1 Custodian sends 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 (CRUU) signed by the second organization. refer to the transfer details given in clause 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 Customs Services.

NOTE 7: The approved recipient is represented by its authorized officers.

NOTE 8: If a TEA1 specification is returned to the TEA1 Custodian (for example the recipient may decide not to make use of the information), then the TEA1 Custodian destroys the specification and enters a note to this effect in the TEA1 Register.

## 5.2 Transfers by a licencee

An organization which has already been approved and has obtained TEA1 specifications may transfer one or more of these specifications, subject to national legislation, to a second organization which requires the specification.

In this case, the first organization has to ensure that the second organization meets the approval criteria. The first organization has to get the second organization to sign two copies of the Confidentiality and Restricted Usage Undertaking (CRUU). The first organization then sends these to the TEA1 Custodian, together with the numbers of the specifications which are to be transferred.

The TEA1 Custodian then enters the transfer details in the TEA1 Register, countersigns the Confidentiality and Restricted Usage Undertakings (CRUU), 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 TEA1 File.

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

## 5.3 Distribution of TEA1 specification Part 3 by the TEA1 Custodian

The following procedures for distributing the TEA1 specification Part 3 are defined:

1) The TEA1 Custodian receives a written request for one single copy of the TEA1 specification Part 3.

2) The TEA1 Custodian sends one copy of the requested Part 3 of the TEA1 specification Part 3 to the applicant.

# 6 Approval criteria and restrictions

The approval criteria are set by the ETSI Secretariat together with ETSI Project TETRA and maintained by the TEA1 Custodian. The TEA1 Custodian may recommend changes to these criteria.

In order for an organization to be considered an approved recipient of one of the TEA1 it has to satisfy at least one of the following criteria :

C1 The organization is designer of or competent to manufacture TETRA portable or TETRA fixed systems, where the algorithm requested is included in the systems.

C2 The organization is designer of or competent to manufacture components for TETRA portable or TETRA fixed systems, where at least one of the components includes the algorithm requested.

C3 The organization is designer of or competent to manufacture a TETRA system simulator for approval testing of TETRA portable or fixed systems, where the simulator includes the algorithm requested.

C4 The organization intends to use the algorithm requested in order to become an operator of a TETRA system.

The TEA1 Custodian will decide whether an organization requesting the TEA1 specification may be considered to be an approved recipient. Any doubtful cases will be referred back to ETSI Secretariat or ETSI Project TETRA.

# 7 The TEA1 Custodian

## 7.1 Responsibilities

The TEA1 Custodian is expected to perform the following tasks:

T1 To approve requests for the TEA1 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 Customs Services of its country if any.

T3 To distribute the TEA1 specifications as detailed in clause 5 (see note 1).

T4 To maintain the TEA1 Register as described in clause 5.

T5 To hold in custody the contents of the TEA1 File as specified in clause 5.

T6 To provide recipients of the TEA1 with limited technical support, i.e. answer written queries arising from the specification or test data (see note 2).

T7 To advise ETSI/ETSI Project TETRA of any problems arising with the approval criteria.

T8 In the light of written queries from recipients of the TEA1 specifications, to make recommendations to ETSI/ETSI Project TETRA for improvements/corrections to the specification and, subject to ETSI/ETSI Project TETRA approval, make and distribute the changes (see note 3).

T9 To provide ETSI/ETSI Project TETRA with information from the TEA1 Register when requested to do so.

T10 To monitor published advances in crypto-analysis and advise the ETSI Project TETRA of any advances which have a significant impact upon the continued suitability of the TEA1 for the TETRA application.

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 TEA1 Custodian will only endeavour to answer questions relating to the TEA1 specifications. He is not expected to provide technical support for development programmes.

NOTE 3: Numbered copies of any changes to the TEA1 specifications will be automatically distributed to all recipients of the specification and a record of the distribution entered in the TEA1 Register.

## 7.2 Appointment

The TEA1 Custodian is:

ETSI Secretariat

The contact person is:

Gina Ebenezersson

ETSI

F-06921 Sophia Antipolis Cedex

France

The TEA1 Custodian will ask a fee from the recipient to cover the cost of distribution of Part 1 and 2 of the specifications. This fee is set to EURO 1 000 per application per algorithm requested (i.e. TEA1).

The TEA1 Custodian may ask for an optional fee from the recipient to cover the cost of distribution of Part 3.

All requests for either the TEA3 specification Part 1 and 2 or the TEA3 specification Part 3 should be addressed to the indicated contact person or to ETSI.

# Annex A:
# Items delivered to approved recipient of TEA1

ITEM-1: Up to N numbered paper copies to the TEA1 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 TEA1 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 clause 5.2), only ITEM-2 and the cover letter are delivered. Moreover, the cover letter details the numbers of the transferred specifications.

# Annex B:
# Confidentiality and Restricted Usage Undertaking for TEA1

## CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the TEA1 algorithm for the protection of the information exchanged over the radio channels of the Terrestrial Trunked Radio (TETRA) System.

Between

(COMPANY NAME).....

(COMPANY ADDRESS).....

.....

.....

hereinafter called: the LICENCEE;

and

(COMPANY NAME).....

(COMPANY ADDRESS).....

.....

.....

hereinafter called: the CUSTODIAN.

Whereas

The LICENCEE 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 TETRA portable or TETRA fixed systems where TETRA Standard Encryption Algorithm 1(hereinafter referred to as TEA1) is included in the systems.
- He is designer of or competent to manufacture components for TETRA portable or TETRA fixed systems where at least one of the components include the TEA1.
- He is designer of or competent to manufacture TETRA system simulator for approval testing of TETRA portable or fixed systems where the simulator includes the TEA1.
- He will provide the services as an operator of a TETRA system using the TEA1.

The CUSTODIAN undertakes to give to the LICENCEE:

- Registered copies of the detailed specification of the confidentiality algorithm TEA1 Part 1 and Part 2 for protection of the information exchanged over the radio channels of a Trans European Trunked Radio system.

The LICENCEE undertakes:

1) To keep strictly confidential all information contained in the detailed specification of the TEA1 and all related communications written or verbal which have been associated with that information after the signature of the present undertaking (the "INFORMATION").
2) Not to make copies of the TEA1 specifications (all copies of these specifications must be produced, numbered and registered by the TEA1 Custodian).

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

4) 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 TEA1 specification exclusively for the provision of TETRA components, systems or services, thus refraining from making any other use of the TEA1 or information in the TEA1 specification.

6) Not to register, or attempt to register, any IPR (patents or the like rights) relating to the TEA1 and containing all or part of the INFORMATION.

7) To design his equipment in a manner that protects the TEA1 from disclosure and ensures that it cannot be used for any purpose other than to provide the TETRA air interface security services for which it is intended.

   These services are specified in the following standards:

   ETSI EN 300 392-7 [1]: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7:Security".

   ETSI ETS 300 393-7 [2]: "Terrestrial Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 7: Security".

   ETSI EN 300 396-6 [3]: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".".

   The TEA1 may not be used to provide the end-to-end security services described in these standards.

8) Not to subcontract any part of the design and build of his equipment, or the provision of his TETRA services, which requires a knowledge of the TEA1, 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 TEA1 in any document that is circulated outside the premises of the LICENCEE.

The above restriction does not apply to information which:

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

- is received by the LICENCEE 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 LICENCEE 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 LICENCEE 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 LICENCEE breaches the obligations of confidentiality imposed on him pursuant to bullets 1 to 9 above and ETSI demonstrates that it has suffered loss as a direct result of such breach, the LICENCEE agrees to indemnify ETSI for such reasonable losses which are a direct result of such breach. The LICENCEE may not be held liable for any indirect or consequential or incidental losses (including loss of profits) suffered by any third party claiming against ETSI.

All disputes which derive from the present undertaking or its interpretation will be settled by the Court of Justice located in Grasse (Alpes Maritimes) and with the application of French Law regarding questions of interpretation.

The obligations of confidentiality herein will not apply vis-à-vis other LICENCEES. Evidence of being a LICENCEE will 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 will 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 CUSTODIAN, the other for the LICENCEE.

| For the CUSTODIAN | For the LICENCEE |
|---|---|
| ..... | ..... |
| (Name, Title (typed)) | (Name, Title (typed)) |
| ..... | ..... |
| (Name, Title (typed)) | (Name, Title (typed)) |
| ..... | ..... |
| (Date) | (Date) |

# History

| Document history | | |
|---|---|---|
| V1.1.1 | June 1997 | Publication |
| V1.1.2 | January 2006 | Publication |
| | | |
| | | |
| | | |