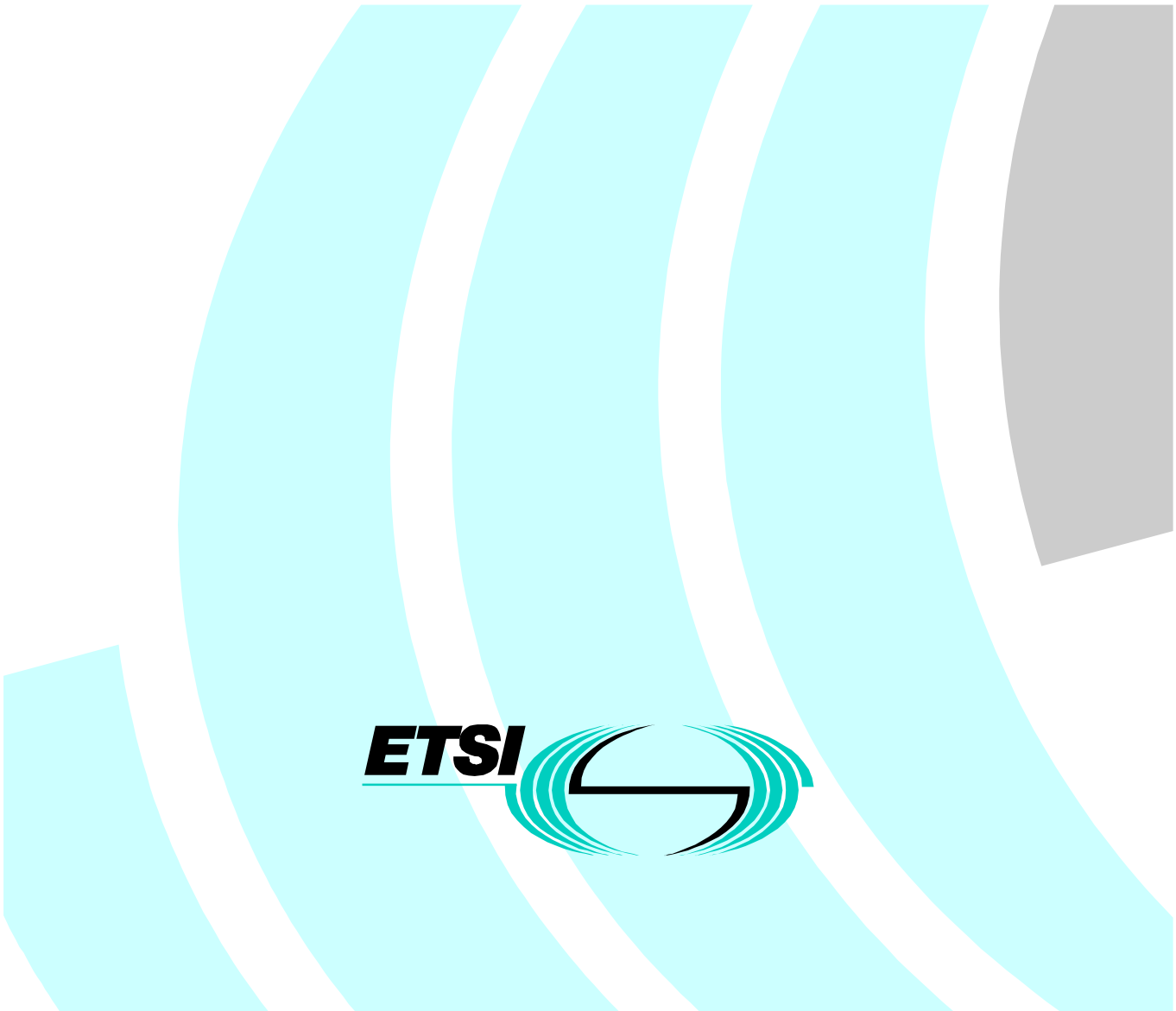
TR 101 690 V1.1.1 (1999-08)

Technical Specification

Security Algorithms Group of Experts (SAGE); Rules for the management of the GSM CTS standard Authentication and Key Generation Algorithms (CORDIAL)



Reference
DTR/SAGE-00016 (fnc00ics.PDF)

Keywords
security, algorithm, GSM, CTS

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 **free of charge** 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 GSM Cordless Integrity Algorithms (CORDIAL). These algorithms are intended for providing authentication, key generation and integrity services in GSM Cordless Telephony products.

The actual specification for CORDIAL is confidential and will not be published. It consists of the following three documents:

Document 1: Algorithm specification;

Document 2: Design conformance test data;

Document 3: Algorithm input/output test data.

The procedures described in the present document apply to Document 1 and Document 2 of the specifications. The Documents 1 and 2 are confidential and their distribution will be controlled as described in the present document.

Document 3 of the specification is not confidential and can be obtained directly from the CORDIAL Custodian (see subclause 5.3). There are no restrictions on the distribution of this Document 3 of the specification.

The management structure is defined in clause 4. This structure is defined in terms of the principals involved in the management of the CORDIAL specification (ETSI, ETSI SMG/SMG10, CORDIAL Custodian and approved recipients) together with the relationships and interactions between them.

The procedures for delivering the CORDIAL specification 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 CORDIAL specification 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 CORDIAL Custodian.

2 References

Void

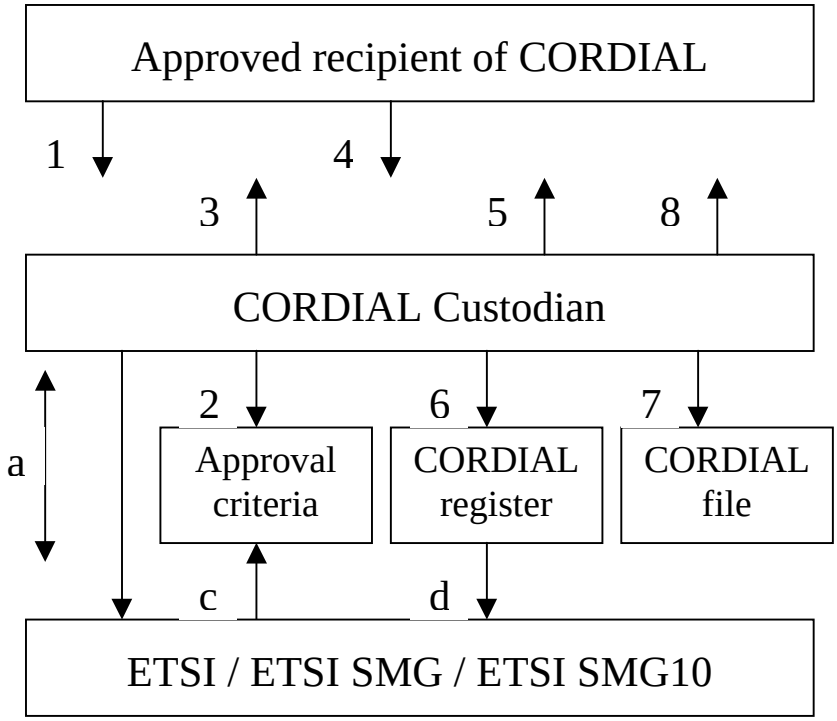
3 Abbreviations

For the purposes of the present document, the following abbreviation applies:

CTS Cordless Telephony System (GSM)

4 CORDIAL management structure

The management structure is depicted in figure 1.



Key:

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

Figure 1: CORDIAL management structure

The figure shows the three principals involved in the management of CORDIAL and the relationships and interactions between them.

ETSI is the owner of CORDIAL. The ETSI Secretariat together with ETSI sets the approval criteria for receipt of the algorithm (see clause 5).

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

The Custodian shall be the ETSI Secretariat unless it is decided by ETSI Secretariat and/or ETSI SMG/SMG10 to (temporary) delegate this task to a third party on the basis of an agreement between the latter and the ETSI Secretariat. The CORDIAL Custodian's duties are detailed in clause 5. They include distributing the CORDIAL specification to approved recipients, as detailed in clause 5, providing limited technical advice to approved recipients and providing algorithm status reports to ETSI SMG/SMG10.

5 Distribution Procedures

The procedures described in subclause 5.1 and subclause 5.2 refer to distribution of Document 1 and Document 2 of the CORDIAL specification.

The distribution of Document 3 of the CORDIAL specification is described in subclause 5.3.

5.1 Distribution of CORDIAL specification Documents 1 and 2 by CORDIAL Custodian

The following procedures for distributing the CORDIAL specification to approved recipients are defined with reference to figure 1.

1) The CORDIAL Custodian receives a written request for N (max. 10) copies of the CORDIAL specification (see note 1).

2) The CORDIAL 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 CORDIAL 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 the present document (Rules for the Management of the of the GSM CTS Standard Authentication and Key Generation Algorithms CORDIAL).

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 CORDIAL Custodian, together with the payment of charges if any.

5) The CORDIAL Custodian sends up to N numbered copies (see note 3) of the CORDIAL specification Document 1 and Document 2 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 CORDIAL Custodian updates the CORDIAL Register by recording the name and address of the recipient, the numbers of the copies of the CORDIAL specification delivered and the date of delivery. If the original request is not approved, the CORDIAL Custodian records the name and address of the requesting organization and the reason for rejecting the request in the CORDIAL Register (see also note 8).

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

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

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

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

NOTE 3: The confidentiality and Restricted Usage Undertaking specifies the number of the copies delivered (max 10).

NOTE 4: The CORDIAL Custodian sends all items listed in appendix 1. 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 Customs Services.

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

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

5.2 Transfers of CORDIAL specification Documents 1 and 2 by a LICENCEE

An organization which has already been approved and has obtained CORDIAL 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. The first organization then sends these to the CORDIAL Custodian, together with the numbers of the specifications which are to be transferred.

The CORDIAL Custodian then enters the transfer details in the CORDIAL 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 CORDIAL File.

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

5.3 Distribution of CORDIAL specification Document 3 by the CORDIAL Custodian

The following procedures for distributing the CORDIAL specification Document 3 are defined:

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

2) The CORDIAL Custodian sends one copy of the requested Document 3 of the CORDIAL specification Document 3 to the applicant.

6 Approval criteria and restrictions

The approval criteria are set by the ETSI Secretariat together with ETSI SMG/SMG10 and maintained by the CORDIAL Custodian. The CORDIAL Custodian may recommend changes to these criteria.

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

C1 The organization is designer of or competent to manufacture GSM Cordless Telephony System mobile or GSM Cordless Telephony System fixed systems where Cordless Integrity Algorithms for the providing authentication, key generation and integrity for the GSM Cordless Telecommunication System (CTS) System (hereinafter referred to as CORDIAL) are included in the systems.

C2 The organization is designer of or competent to manufacture components for GSM Cordless Telephony System mobile or GSM Cordless Telephony System fixed systems where at least one of the components include CORDIAL.

C3 The organization is designer of or competent to manufacture a GSM Cordless Telephony System simulator for approval testing of GSM Cordless Telephony System mobile or fixed systems where the simulator includes CORDIAL.

C4 The organization provides services as an Operator for a GSM Cordless Telephony System using CORDIAL.

The CORDIAL Custodian will decide whether an organization requesting the CORDIAL specification may be considered to be an approved recipient. Any doubtful cases will be referred back to ETSI Secretariat or ETSI SMG/SMG10.

7 The CORDIAL Custodian

7.1 Responsibilities

The CORDIAL Custodian is expected to perform the following tasks:

T1	To approve requests for CORDIAL 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 CORDIAL specification as detailed in clause 5 (see note 1).
T4	To maintain the CORDIAL Register as described in clause 5.
T5	To hold in custody the contents of the CORDIAL File as specified in clause 5.
T6	To provide recipients of the CORDIAL specification 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/ETSI SMG10 of any problems arising with the approval criteria.
T8	In the light of written queries from recipients of the CORDIAL specification, to make recommendations to ETSI/ETSI SMG/SMG10 for improvements/corrections to the specification and, subject to ETSI/ETSI SMG/SMG10 approval, make and distribute the changes (see note 3).
T9	To provide ETSI/ETSI SMG/ETSI SMG10 with information from the CORDIAL Register when requested to do so.
T10	To monitor published advances in crypto-analysis and advise ETSI/ETSI SMG/ETSI SMG10 of any advances which have a significant impact upon the continued suitability of CORDIAL for the GSM CTS application.

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

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

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

7.2 Appointment

The CORDIAL Custodian is:

ETSI Secretariat

The contact person is:

Mr Pierre de Courcel email: decourcel@etsi.fr

ETSI

F-06921 Sophia Antipolis Cedex

France

7.3 Fee

Both the CORDIAL Custodian as well as the Interim Custodian (if appointed) will ask a fee from the recipient to cover the cost of distribution of Document 1 and Document 2 of the specification. This fee is set to ECU 1000 per application.

Both the CORDIAL Custodian as well as the Interim Custodian (if appointed) may ask an optional fee from the recipient to cover the cost of distribution of Document 3 of the specification.

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

Annex A (informative): Items delivered to approved recipient of the CORDIAL specification

ITEM-1: Up to N (max. 10) numbered paper copies of the CORDIAL specification Document 1 and Document 2 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 CORDIAL Custodian listing the delivered items (ITEM-1 and ITEM-2 above) and the numbers of the specifications delivered (see note 1).

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 for CORDIAL

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the Cordless Integrity Algorithms (CORDIAL) for providing authentication, key generation and integrity for the GSM Cordless Telecommunication System (CTS) System.

Between

(COMPANY NAME).....

(COMPANY ADDRESS).....

.....

.....

hereinafter called: the LICENSEE;

and

(COMPANY NAME).....

(COMPANY ADDRESS).....

.....

.....

hereinafter called: the CUSTODIAN.

Whereas

The LICENSEE 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 Cordless Telephony System mobile or GSM Cordless Telephony System fixed systems where Cordless Integrity Algorithms for the providing authentication, key generation and integrity for the GSM Cordless Telecommunication System (CTS) System (hereinafter referred to as CORDIAL) are included in the systems.
- He is designer of or competent to manufacture components for GSM Cordless Telephony System mobile or GSM Cordless Telephony System fixed systems where at least one of the components include CORDIAL.
- He is designer of or competent to manufacture a GSM Cordless Telephony System simulator for approval testing of GSM Cordless Telephony System mobile or fixed systems where the simulator includes CORDIAL.
- He will provide the services as an Operator for a GSM Cordless Telephony System using CORDIAL.

The CUSTODIAN undertakes to give to the LICENSEE:

- …. registered copies of Document 1 and Document 2 of the CORDIAL specification for providing authentication, key generation and integrity for the GSM Cordless Telecommunication System (CTS).

The LICENSEE undertakes:

1) To keep strictly confidential all information contained in the detailed specification of CORDIAL 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 CORDIAL specifications (all copies of these specifications must be produced, numbered and registered by the CORDIAL 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 CORDIAL specification exclusively for the provision of GSM CTS components, systems or services, thus refraining from making any other use of CORDIAL or information in the CORDIAL specification.

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

7) To design his equipment in a manner that protects CORDIAL from disclosure and ensures that it cannot be used for any purpose other than to provide the GSM CTS Authentication and Key Generation services for which it is intended.

   The use of CORDIAL is specified in the following standard:

   GSM 03.20 [1] annex E: Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephony System (CTS), Phase 1); Security related network functions; Stage 2.

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

The above restriction does not apply to information which:

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

- is received by the LICENSEE 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 LICENSEE 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 LICENSEE 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 LICENSEE 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 LICENSEE agrees to indemnify ETSI for such reasonable losses which are a direct result of such breach. The LICENSEE 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 LICENSEES. Evidence of being a LICENSEE 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 LICENSEE.

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

History

Document history		
V1.1.1	August 1999	Publication

ISBN 2-7437-3136-2
Dépôt légal : Août 1999