ETSI
TECHNICAL COMMITTEE
REFERENCE TECHNICAL REPORT

TCR-TR 032

November 1995

Source: ETSI TC-SAGE

Reference: DTR/SAGE-00006

ICS: 33.020

Key words: Management rules, cryptographic algorithm

Security Algorithms Group of Experts (SAGE); Rules for the management of the TESA-7 algorithm

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

New presentation - see History box

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Blank page

Foreword

This Technical Committee Reference TCR-TR (TCR-TR) has been produced by the Security Algorithm Group of Experts (SAGE) of the European Telecommunications Standards Institute (ETSI). It was given the classification of TCR-TR by the 20th TC Chairmans' Co-ordination (TCC) meeting and postal approval (CL 1227) by the Technical Assembly (TA).

A TCR-TR is a deliverable for use inside ETSI which records output results of ETSI Technical Committee (TC) or Sub-Technical Committee (STC) studies which are not appropriate for European Telecommunication Standard (ETS), Interim European Telecommunication Standard (I-ETS) or ETSI Technical Report (ETR) status. They can be used for guidelines, status reports, co-ordination documents, etc. They are to be used to manage studies inside ETSI and shall be mandatorially applied amongst the concerned TCs. They shall also be utilised by the TC with overall responsibility for a study area for co-ordination documents (e.g. models, reference diagrams, principles, structures of standard, framework and guideline documents) which constitute the agreed basis for several, if not all, TCs and STCs to pursue detailed standards.

Blank page

1 Scope

Within European Telecommunications Standards Institute (ETSI) Sub-Technical Committee (STC)/Terminal Equipment 9 (TE9) standards have been produced for a European multi-application IC card and security modules (EN 726 series). These standards contain security functions which are specified in EN 726-2 [1] and EN 726-7 [2].

A cryptographic algorithm, called the TESA-7 algorithm, which is needed as part of the security functionality, was developed and specified by TC-SAGE. The management and distribution of TESA-7 will be according to a clearly defined set of rules.

The purpose of this TCR-TR is to specify the rules for the management of the TESA-7 cryptographic algorithm.

2 References

This TCR-TR incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this TCR-TR only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] EN 726-2 (1995): "Identification card systems; Requirements for IC cards and terminals for telecommunication use; Part 2: Security framework".

[2] EN 726-7 (1995): "Telecommunications integgrated circuit(s); Cards and terminals; Part 7: Security module".

3 Abbreviations

For the purposes of this TCR-TR, the following abbreviations apply:

SAGE	Security Algorithms Group of Experts
TE	Terminal Equipment

4 Outline

The contents of this TCR-TR is as follows.

The management structure is defined in clause 5. This structure is defined in terms of the principals involved in the management of the TESA-7 (ETSI, ETSI TC-TE, TESA-7 Custodian and Approved Recipients) together with the relationships and interactions between them.

The procedures for delivering the TESA-7 to Approved Recipients are defined in clause 6. This clause is supplemented by annex A which specifies the items which are to be delivered.

Clause 7 is concerned with the criteria for approving an organisation for receipt of the TESA-7 and with the responsibilities of an Approved Recipient. This clause is supplemented by annex B and annex C which contains a Confidentiality and Restricted Usage Undertaking to be signed by each Approved Recipient.

Clause 8 is concerned with the appointment and responsibilities of the TESA-7 Custodian.

5 TESA-7 Management Structure

The management structure is depicted in figure 1. The figure shows the three principals involved in the management of the TESA-7 and the relationships and interactions between them.

ETSI is the owner of the TESA-7 and together with TC-TE sets the approval criteria for receipt of the algorithm (see clause 7).

The TESA-7 Custodian is the interface between ETSI and the Approved Recipients of the TESA-7.

The activities of the TESA-7 Custodian are supported by an agreement between ETSI and the Custodian.

The TESA-7 Custodian's duties are detailed in clause 8. They include distributing the TESA-7 specification to Approved Recipients, as detailed in clause 6, providing limited technical advice to Approved Recipients and providing algorithm status reports to TC-TE.

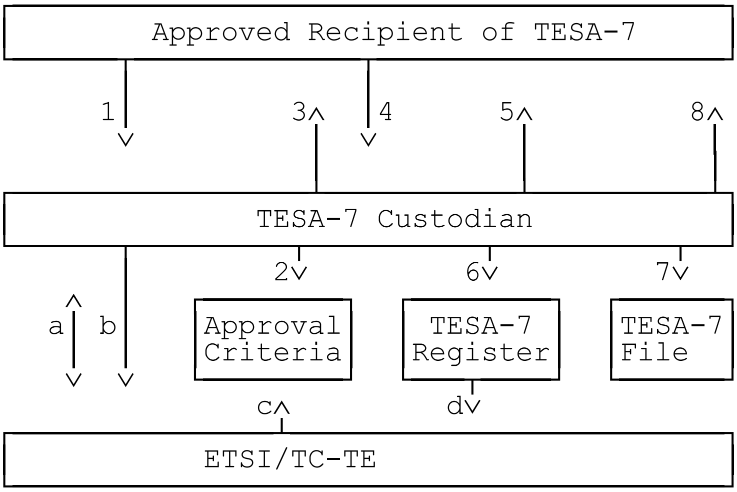

Figure 1: TESA-7 management structure

Key to figure:

a = agreement between TESA-7 Custodian and ETSI;
b = status reports and recommendations;
c = setting of approval criteria;
d = restricted details of the TESA-7 register;

1 = request for TESA-7;
2 = check of request against approval criteria;
3/4 = exchange of Confidentiality and Restricted Usage Undertaking;
5 = dispatch of TESA-7 Specification;
6 = update the TESA-7 register;
7 = document filing;
8 = technical advice.

6 Distribution procedures

The TESA-7 specifications consist of four separate parts:

Part 1 - TESA-7 IC Card Functions;
Part 2 - TESA-7 Security Module Functions;
Part 3 - TESA-7 IC Card Test Data;
Part 4 - TESA-7 Security Module Test Data.

There will be two specification sets for the TESA-7 algorithm. Each of these sets contains two documents. One set consists of Parts 1 and 3; this is for the use in the multi-application IC card. The other set consists of Parts 2 and 4; this is for use in the related security modules.

For each of these two sets there is a separate Confidentiality and Restricted Usage Undertaking.

The following procedures for distributing the TESA-7 to Approved Recipients are defined with reference to figure 1.

1) The TESA-7 Custodian receives a written request for N copies of the TESA-7 Specification (see note 1), where N should not be bigger than six. The request should indicate if the algorithm is meant for use in the multi-application IC card or in a related security module.

2) The TESA-7 Custodian confirms (or otherwise) whether the requesting organisation meets the approval criteria (see clause 7).

3) If the request is approved, the TESA-7 Custodian dispatches 2 copies of the appropriate Confidentiality and Restricted Usage Undertaking (as given in annex 2) for signature by the Approved Recipient (see notes 2 and 6) together with a copy of this TCR-TR (Rules for the Management of the TESA-7 Algorithm).

4) Both copies of the Confidentiality and Restricted Usage Undertaking must be signed by the approved recipient (see notes 5 and 7) and returned to the TESA-7 Custodian.

5) The TESA-7 Custodian sends up to N (note 3) numbered copies of the TESA-7 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 TESA-7 Custodian updates the TESA-7 Register by recording the name and address of the recipient, the numbers of the copies of the TESA-7 Specification delivered and the date of delivery. If the original request is not approved, the TESA-7 Custodian records the name and address of the requesting organisation and the reason for rejecting the request in the TESA-7 Register.

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

NOTE 1: Requests for the TESA-7 Specification should be made directly to the TESA-7 Custodian.

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 and the usage (multi-application IC card or security module).

NOTE 4: The TESA-7 Custodian sends all items listed in annex A. Requests for part of the package of items are rejected.

NOTE 5: Under normal circumstances the Custodian is expected to respond within 25 working days. This does not include delays in the process of applying for an export licence.

NOTE 6: The approved recipient is the legal representative of the receiving organisation.

NOTE 7: If a TESA-7 Specification is returned to the TESA-7 Custodian (for example the recipient may decide not to make use of the information), then the TESA-7 Custodian destroys the specification and enter a note to this effect in the TESA-7 Register.

NOTE 8: The TESA-7 Custodian may impose a reasonable charge to cover administrative costs involved in issuing the TESA-7 specification documents.

7 Approval criteria

The approval criteria are set by the ETSI together with ETSI TC/TE and are maintained by the TESA-7 Custodian. The TESA-7 Custodian may recommend changes to these criteria.

In order for an organisation to be considered an Approved Recipient of the TESA-7 for use in an IC card it shall satisfy at least one of the following criteria:

C1 The organisation is designer of or competent to manufacture systems according to EN 726, where the TESA-7 is included in the systems.

C2 The organisation is designer of or competent to manufacture components for systems according to EN 726, where at least one of the components includes the TESA-7.

C3 The organisation is designer of or competent to manufacture a system simulator for a system according to EN 726, where the simulator includes the TESA-7.

C4 The organisation will provide the services as an operator of a system according to EN 726 using the TESA-7.

In order for an organisation to be considered an Approved Recipient of the TESA-7 for use in a security module it shall satisfy at least one of the following criteria:

D1 The organisation is designer of or competent to manufacture systems incorporating a security module according to EN 726, where the TESA-7 is included in the systems.

D2 The organisation is designer of or competent to manufacture components for systems incorporating a security module according to EN 726, where at least one of the components includes the TESA-7.

D3 The organisation is designer of or competent to manufacture a system simulator incorporating a security module for a system according to EN 726, where the simulator includes the TESA-7.

D4 The organisation will provide the services as an operator of a system incorporating a security module according to EN 726 using the TESA-7.

The TESA-7 Custodian will decide whether an organisation requesting the TESA-7 Specification may be considered to be an Approved Recipient. Any doubtful cases will be referred back to ETSI/ TC-TE, after taking the advice of the ETSI Deputy Director.

8 The TESA-7 Custodian

8.1 Responsibilities

The TESA-7 Custodian is expected to perform the following tasks:

T1 To approve requests for the TESA-7 by reference to the Approval Criteria given in clause 7.

T2 To exchange the Confidentiality and Restricted Usage Undertaking with Approved Recipients as described in clause 6.

T3 To distribute the TESA-7 Specification as detailed in clause 6 (see note 1).

T4 To maintain the TESA-7 Register as described in clause 6.

T5 To hold in custody the contents of the TESA-7 File as specified in clause 6.

T6 To provide recipients of the TESA-7 with limited technical support, i.e, answer written queries arising from the specification or test data (see note 2).

T7 To liaise with the ETSI Deputy Director over any problems of a legal nature concerning the issue of the Specifications or the Confidentiality and Restricted Usage Undertakings.

T8 To advise ETSI/TC-TE of any problems arising with the approval criteria.

T9 In the light of written queries from recipients of the TESA-7 Specification, to make recommendations to ETSI/TC-TE for improvements/corrections to the specification and, subject to ETSI/TC-TE approval, make and distribute the changes (see note 3).

T10 To provide ETSI/TC-TE with information from the TESA-7 Register when requested to do so.

T11 To monitor published advances in cryptanalysis and advise the ETSI TC-TE of any advances which have a significant impact upon the continued suitability of the TESA-7 for the use in the context of EN 726.

NOTE 1: Registered mail will be used. (The specification documents will be sent in a double envelope, the inner envelope carrying the return address of the custodian.)

If recipients require a different delivery service then they will be expected to pay the full costs.

NOTE 2: The TESA-7 Custodian will only endeavour to answer questions relating to the TESA-7 Specification. He is not expected to provide technical support for development programmes.

NOTE 3: Numbered copies of any changes to the TESA-7 Specification are automatically distributed to all recipients of the specification and a record of the distribution entered in the TESA-7 Register.

The TESA-7 Custodian is

Mr H. Gilbert
CNET
PAA/TSA/SRC
38-40 Rue General Leclerc
F-92131 Issy-les-Moulineaux
France
Fax number: +33 1 45 29 65 19

Annex A: Items delivered to Approved Recipient of TESA-7

ITEM-1: up to N numbered copies to the TESA-7 Specification, either for use in the multi-application IC card or for use in the related security modules (as indicated in the request), 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 TESA-7 Custodian listing the delivered items (ITEM-1 and ITEM-2 above) and the numbers of the specifications delivered.

Annex B: Confidentially and restricted usage undertaking

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the TESA-7 cryptographic algorithm for use in the European multi-application IC card as specified by ETSI STC TE9 (EN 726 series).

Between

(COMPANY NAME) ....

(COMPANY ADDRESS)...

....

....

hereinafter called: the BENEFICIARY;

and

(COMPANY NAME) ....

(COMPANY ADDRESS)...

....

....

hereinafter called: the PROVIDER.

Whereas

The BENEFICIARY has alleged that he fulfils at least one of the following criteria:

- he is designer of or competent to manufacture systems according to EN 726, where the TESA-7 is included in the systems;

- he is designer of or competent to manufacture components for systems according to EN 726, where at least one of the components includes the TESA-7;

- he is designer of or competent to manufacture a system simulator for a system according to EN 726, where the simulator includes the TESA-7;

- he will provide the services as an operator of a system according to EN 726 using the TESA-7.

The PROVIDER undertakes to give to the BENEFICIARY:

- registered copies of the detailed specification of the TESA-7 cryptographic algorithm for use in the European multi-application IC card as specified by ETSI STC TE9 (EN 726 series).

The BENEFICIARY undertakes:

1) to keep strictly confidential all information contained in the detailed specification of the TESA-7 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 TESA-7 specifications (all copies of these specifications shall be produced, numbered and registered by the TESA-7 Custodian);

3) not to disclose the INFORMATION to any third party without prior and explicit authorization in writing by the PROVIDER;

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 PROVIDER, all or part of the INFORMATION;

5) to use the INFORMATION in the TESA-7 specification exclusively to enable the provision of components, systems or services according to EN 726 and to the annex to this undertaking (Modes of use of TESA-7 for the multi-application IC card), thus refraining from making any other use of the TESA-7 or information in the TESA-7 specification;

6) not to register, or attempt to register, any IPR (patents or the like rights) relating to the TESA-7 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 TESA-7 from disclosure and ensures that it cannot be used for any purpose other than to provide the services for which it is intended. (These services are defined in the EN 726 series of standards);

8) not to subcontract any part of the design and build of his equipment, or the provision of his services, which requires a knowledge of the TESA-7, to any organisation which has not signed the Confidentiality and Restricted Usage Undertaking;

9) not to communicate a description or analysis of any aspects which may disclose the operation of the TESA-7 in any document that is circulated outside the premises of the BENEFICIARY, except to the PROVIDER.

The above restrictions 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 PROVIDER.

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 clauses 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 Arbitration of the International Chamber of Commerce situated in Paris, 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 constitutes the entire agreement between the parties. All amendments to this undertaking shall be agreed in writing and signed by a duly authorised representative of each of the parties.

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

For the PROVIDER	For the BENEFICIARY
....	....
TESA-7 Custodian	....
	(Name, Title (typed))
....	....
(Date)	(Date)

ANNEX TO TESA-7 CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING FOR THE MULTI-APPLICATION IC CARD

Modes of use of TESA-7 for the multi-application IC card

The TESA-7 specification for use on the multi-application IC card contains the following modes.

- key establishment function;
- authentication function;
- message authentication mode.

The usage of these modes is specified as follows.

Key Establishment Function

The algorithm, when used in the key establishment function, has been designed to load keys for the following purposes:

- keys used in SAGE-supplied algorithms in appropriate modes of operation;

- keys used in any authentication (including message authentication) algorithm.

The implementation should not permit down loaded keys to be read from the card.

Authentication Function

The algorithm, when used as authentication function, has been designed to be a common resource suitable for use by any application.

Message Authentication Mode

The algorithm, when used in the message authentication mode, has been designed to be a common resource which may be used by any application.

Annex C: Confidentially and restricted usage undertaking

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the TESA-7 cryptographic algorithm for use in security modules for the European multi-application IC card as specified by ETSI STC TE9 (EN 726 series).

Between

(COMPANY NAME) ....

(COMPANY ADDRESS)..

....

....

hereinafter called: the BENEFICIARY;

and

(COMPANY NAME) ....

(COMPANY ADDRESS)..

....

....

hereinafter called: the PROVIDER.

Whereas

The BENEFICIARY has alleged that he fulfils at least one of the following criteria:

- he is designer of or competent to manufacture systems incorporating a security module according to EN 726, where the TESA-7 is included in the systems;

- he is designer of or competent to manufacture components for systems incorporating a security module according to EN 726, where at least one of the components includes the TESA-7;

- he is designer of or competent to manufacture a system simulator incorporating a security module for a system according to EN 726, where the simulator includes the TESA-7;

- he will provide the services as an operator of a system incorporating a security module according to EN 726 using the TESA-7.

The PROVIDER undertakes to give to the BENEFICIARY:

- registered copies of the detailed specification of the TESA-7 cryptographic algorithm for use in a security module for the European multi-application IC card as specified by ETSI STC TE9 (EN 726 series).

The BENEFICIARY undertakes:

1) to keep strictly confidential all information contained in the detailed specification of the TESA-7 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 TESA-7 specifications (all copies of these specifications shall be produced, numbered and registered by the TESA-7 Custodian);

3) not to disclose the INFORMATION to any third party without prior and explicit authorization in writing by the PROVIDER;

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 PROVIDER, all or part of the INFORMATION;

5) to use the INFORMATION in the TESA-7 specification exclusively to enable the provision of components, systems or services according to EN 726 and to the annex to this undertaking (Modes of use of TESA-7 for the security module), thus refraining from making any other use of the TESA-7 or information in the TESA-7 specification;

6) not to register, or attempt to register, any IPR (patents or the like rights) relating to the TESA-7 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 TESA-7 from disclosure and ensures that it cannot be used for any purpose other than to provide the services for which it is intended. (These services are defined in the EN 726 series of standards.)

8) not to subcontract any part of the design and build of his equipment, or the provision of his services, which requires a knowledge of the TESA-7, to any organisation which has not signed the Confidentiality and Restricted Usage Undertaking;

9) not to communicate a description or analysis of any aspects which may disclose the operation of the TESA-7 in any document that is circulated outside the premises of the BENEFICIARY, except to the PROVIDER.

The above restrictions 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 PROVIDER.

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 clauses 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 Arbitration of the International Chamber of Commerce situated in Paris, 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 constitutes the entire agreement between the parties. All amendments to this undertaking shall be agreed in writing and signed by a duly authorised representative of each of the parties.

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

For the PROVIDER	For the BENEFICIARY
....	....
TESA-7 Custodian	....
	(Name, Title (typed))
....	....
(Date)	(Date)

ANNEX TO TESA-7 CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING FOR THE SECURITY MODULE

Modes of use of TESA-7 for the security module

The TESA-7 specification for use in the security module contains the following modes:

- authentication function;
- message authentication mode;
- inverse key establishment function;
- key diversification function.

The usage of these modes is specified as follows.

Authentication Function

The algorithm, when used as authentication function, has been designed to be a common resource suitable for use by any application.

Message Authentication Mode

The algorithm, when used in the message authentication mode, has been designed to be a common resource which may be used by any application.

Inverse Key Establishment Function

The algorithm, when used in the inverse key establishment function, has been designed to load keys for the following purposes:

- keys used in SAGE-supplied algorithms in appropriate modes of operation;
- keys used in any authentication (including message authentication) algorithm.

Key Diversification Function

The algorithm, when used as the key diversification function, has been designed to for use by a security module. It enables the security module to derive from diversification data contained in a command and a key file of a certain number of master keys, a new file containing a same number of diversified keys.

History

Document history		
December 1994	Draft	For endorsement by TCC 19
June 1995	Final draft	Endorsed by TCC 20, for approval by TA
November 1995	First Edition	
March 1996	Converted into Adobe Acrobat Portable Document Format (PDF)	