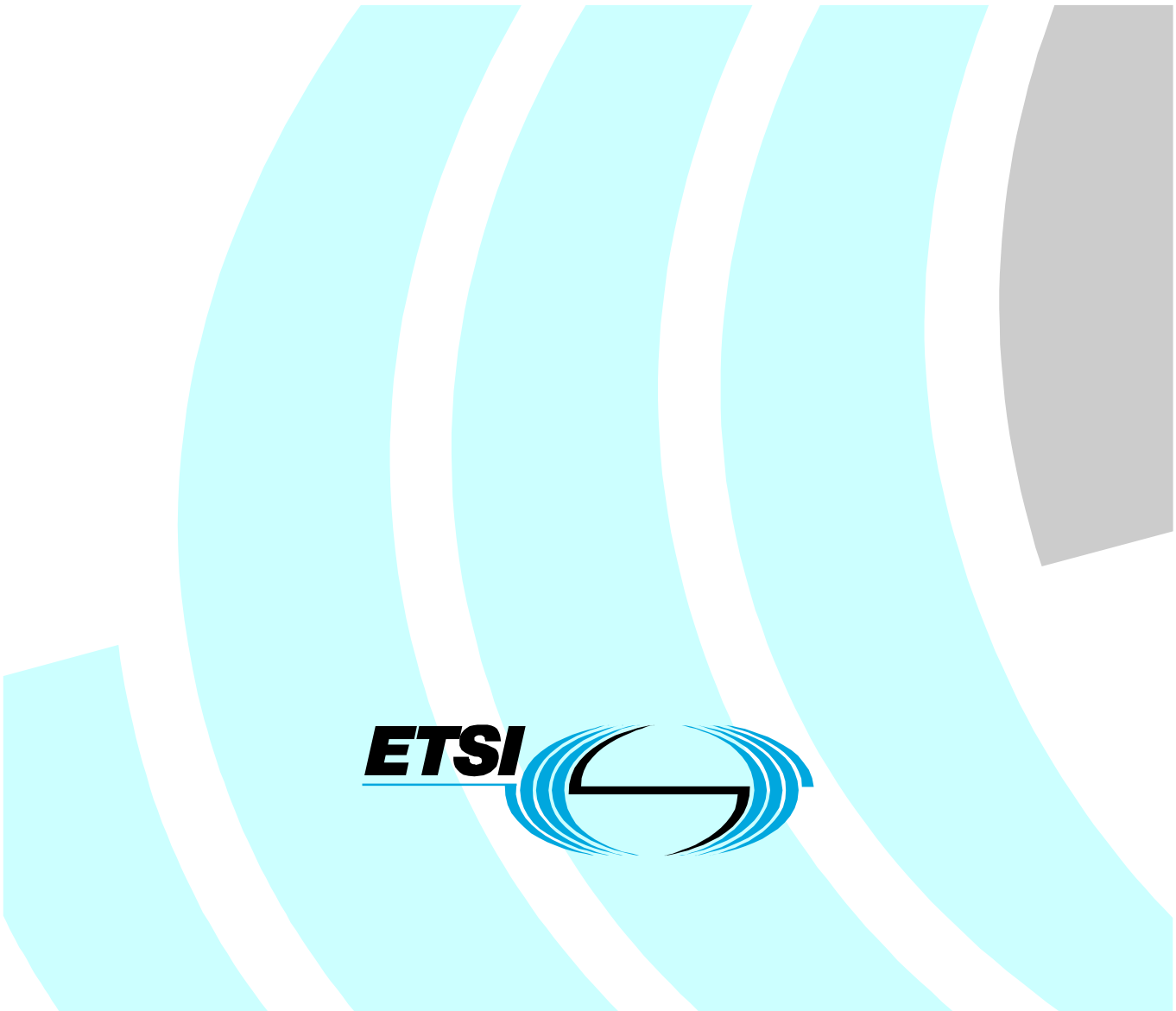
ETSI TS 102 144 V1.1.1 (2003-05)

Technical Specification

Services and Protocols for Advanced Networks (SPAN); MTP/SCCP/SSCOP and SIGTRAN (Transport of SS7 over IP); Stream Control Transmission Protocol (SCTP)

[Endorsement of RFC 2960 and RFC 3309, modified]



Reference
DTS/SPAN-130265

Keywords
MTP, SCCP, SCTP, SIGTRAN, SS7,

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).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Services and Protocols for Advanced Networks (SPAN).

Endorsement notice

The Elements of the Internet Engineering Task Force Request For Comments RFC 2960 [1] and RFC 3309 [2] apply with the following modifications.

Introduction

The present document records the changes to the Internet Engineering Task Force (IETF) RFC 2960 [1] and RFC 3309 [2]. These RFCs specify the Stream Control Transmission Protocol, which is the common transport protocol used by all SIGTRAN adaptation layers.

1 Scope

The present document specifies the requirements for the Stream Control Transmission Protocol (SCTP) when used in conjunction with the SIGTRAN adaptation layers for the transport of Signalling Systems No.7 (SS7) messages over the Internet Protocol (IP). The document endorses and constrains where relevant the SCTP defined in RFC 2960 [1] and RFC 3309 [2].

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 and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] IETF RFC 2960 (2000): "Stream Control Transmission Protocol", R. Stewart., Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, V. Paxson.

[2] IETF RFC 3309 (2002): "Stream Control Transmission Protocol (SCTP) Checksum Change", J. Stone, R. Stewart, D. Otis.

[3] IETF RFC 3436 (2002): "Transport Layer Security over Stream Control Transmission Protocol", A. Jungmaier, E. Rescorla, M. Tüxen.

[4] ETSI TS 102 141: "Services and Protocols for Advanced Networks (SPAN); MTP/SCCP/SSCOP and SIGTRAN; M2UA [Endorsement of RFC 3331 (2002), modified]".

[5] ETSI TS 102 142: "Services and Protocols for Advanced Networks (SPAN); MTP/SCCP/SSCOP and SIGTRAN; M3UA [Endorsement of RFC 3332 (2002), modified]".

[6] ETSI TS 102 143: "Services and Protocols for Advanced Networks (SPAN); MTP/SCCP/SSCOP and SIGTRAN; SUA [Endorsement of SIGTRAN-SUA-14 (Dec. 2002), modified]".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

example 1: text used to clarify abstract rules by applying them literally

3.2 Abbreviations

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

ECN	Explicit Congestion Notification
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6

MTU	Maximum Transmission Unit
RFC	Request Ffor Comment
SCTP	Stream Control Transmission Protocol

4 SCTP protocol considerations

4.1 SCTP checksum

The CRC32C algorithm given in RFC 3309 [2] shall be used instead of the Adler32 algorithm given in RFC 2960 [1].

4.2 SCTP streams

A minimum of two incoming and two outgoing streams shall be supported.

4.3 Path MTU discovery

Path MTU discovery is not required. This value shall be configurable.

4.4 Multihoming

An SCTP end-point shall support two or more paths towards its peer. If association initialization to an IP destination address is unsuccessful, and alternative destination IP addresses are known, the sending node shall reattempt initialization by the sending the INIT chunk to the alternative IP address.

4.5 SCTP chunk size

IP-packets containing SCTP packets shall not be larger than the Path MTU.

An SCTP end-point shall use INIT and INIT-ACK chunks such that the resulting IP-packet is not larger than the Path MTU. This limits the number of paths used by SCTP associations. DATA chunks shall not exceed a size that would result in IP-packets larger than the path MTU. The size of HEARTBEAT chunks shall be equivalent to the size of DATA chunks.

4.6 Addressing methods

An SCTP end-point shall support IPv4 address parameters, may support IPv6 address parameters and shall not support the hostname address parameter. The sender of an INIT-chunk shall include the Supported Address parameter indicating the support of IPv4 and optionally IPv6. Support for Hostname addresses shall not be indicated. If a hostname address parameter is included in an INIT or INIT-ACK chunk, the receiver shall reply with an ABORT chunk using the error cause Unresolvable Address.

Singlehomed SCTP end-points shall not include an address parameter in INIT and INIT-ACK chunks.

4.7 Path supervision

SCTP end-points shall support the heartbeat mechanism and the sending of HEARTBEAT chunks on idle paths shall be enabled by default.

4.8 User data size

An SCTP end-point shall support the sending and reception of user data with the maximum size defined by the upper layer. An SCTP end-point is not required to support the handling of larger user data sizes. If transport layer security is used the user data size which has to be supported is 18 437, see RFC 3436 [3] for more information.

4.9 User data fragmentation

If the supported user data size (see clause 4.8) would result in DATA chunks larger than allowed by clause 4.5, the sending SCTP end-point shall support fragmentation of user data. However, if this is not the case the support of user data fragmentation on the sending side is not required. This is the case for TS 102 141 [4] and TS 102 142 [5] when not used in combination with RFC 3436 [3]. The reception of fragmented user data shall be supported.

4.10 Unordered delivery of DATA chunks

Support for unordered delivery at the sending SCTP-end-point is not required. The receiving SCTP end-point shall support the reception of DATA chunks marked for unordered delivery. Please note, that TS 102 141 [4], TS 102 142 [5] and TS 102 143 [6] do not make use of unordered delivery and RFC 3436 [3] does not support it.

4.11 Bundling of DATA chunks

An SCTP end-point shall allow disabling of that DATA-chunk bundling which introduces additional delay. This does not affect bundling which introduces no additional delays.

4.12 Explicit Congestion Notification (ECN)

The support of ECN is not required.

5 SCTP parameter considerations

Table 1 gives a list of relevant SCTP parameters which shall be configurable. The parameters shall be tuneable within the given interval and with the given granularity. The choice of the parameter values applicable for signalling transport is out of scope of the present document. The default values are given for information only.

Table 1: SCTP parameter values

Parameter	Minimum value	Maximum value	Default in RFC 2960 [1]	Granularity
RTO.Min	10 ms	5 s	1 s	10 ms
RTO.Max	1 s	120 s	60 s	10 ms
RTO.Initial	RTO.Min	RTO.Max	3 s	10 ms
RTO.Alpha	1/8	1/8	1/8	
RTO.Beta	1/4	1/4	1/4	
Valid.Cookie.Life	5 s	120 s	60 s	1 s
HB.Interval	1 s	300 s	30 s	1 s
SACK period	0 ms	500 ms	200 ms	10 ms
SACK frequency	1	5	2	1
MTU size	508 bytes	65 535 bytes	1 500 bytes	1 byte

The *SACK period* defines the maximum delay for generating an acknowledgement after receipt of a packet containing a DATA chunk. The *SACK frequency* defines how often a SACK is generated for every *n* packets received containing one or more DATA chunks within the *SACK period.*

History

Document history		
V1.1.1	May 2003	Publication