SLOVENSKI STANDARD
SIST-TP TR 102 129 V1.1.1:2004

01-april-2004

Harmonizacija telekomunikacij in internetnega protokola prek omrežij (TIPHON) - Študija definicije zahtev - Medsebojno delovanje TIPHON in IPCableCom - Arhitektura, protokol, kakovost storitve (QoS) in varnost

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements Definition Study; Interworking of TIPHON and IPCableCom; Architecture, Protocol, QoS and Security

Ta slovenski standard je istoveten z: **TR 102 129 Version 1.1.1**

ICS:

33.020	Telekomunikacije na splošno	Telecommunications in general

SIST-TP TR 102 129 V1.1.1:2004 **en**

ETSI TR 102 129 V1.1.1 (2003-01)

Technical Report

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements Definition Study; Interworking of TIPHON and IPCablecom; Architecture, Protocol, QoS and Security

Reference
DTR/TIPHON-02010

Keywords
architecture, IP, IPCable, protocol, QoS,
telephony, VoIP

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

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 Report (TR) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

1 Scope

The objective of ETSI Project TIPHON is the specification of interoperability mechanisms and related parameters to enable multimedia communications (particularly voice) to take place, to a defined quality of service, between Switched Circuit Networks (SCN) and Internet Protocol (IP) based networks and their associated terminal equipment.

The present document presents an overview of the architecture, protocols, QoS and security concepts for the interworking between TIPHON and IPCablecom systems. It introduces a possible framework for convergence between TIPHON and IPCablecom.

Annexes A and B give a general overview of IPCablecom and TIPHON.

Annex C addresses architectural issues for interworking between TIPHON and IPCablecom systems.

Annex D provides information on the protocol aspects relating to TIPHON and IPCablecom system interworking.

Annex E examines TIPHON and IPCablecom QoS Policies, architectures and the control of network resources

Annex F reviews TIPHON and IPCablecom security policies and describes the results of a threat analysis.

2 References

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

[1] ITU-T Recommendation J.160: "Architectural framework for the delivery of time-critical services over cable television networks using cable modems".

[2] ETSI TS 101 882 (V1.1.1): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Protocol Framework Definition; General (meta-protocol)".

[3] ETSI TR 101 963: "Access and Terminals (AT); Report on the Requirements of European Cable Industry for Implementation of IPCablecom Technologies; Identification of high level requirements and establishment of priorities".

[4] ITU-T Recommendation J.112: "Transmission systems for interactive cable television services".

[5] ETSI ES 201 488: "Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification".

[6] ETSI ES 200 800: "Digital Video Broadcasting (DVB); DVB interaction channel for Cable TV distribution systems (CATV)".

[7] ITU-T Recommendation Q.767: "Application of the ISDN user part of CCITT signalling system No. 7 for international ISDN interconnections".

[8] ETSI EN 300 347: "V interfaces at the digital Local Exchange (LE); V5.2 interface for the support of Access Network (AN)".

[9] ETSI EN 300 659-1: "Access and Terminals (AT); Analogue access to the Public Switched Telephone Network (PSTN); Subscriber line protocol over the local loop for display (and related) services; Part 1: On-hook data transmission".

[10] ETSI ES 200 778-1: "Access and Terminals (AT); Analogue access to the Public Switched Telephone Network (PSTN); Protocol over the local loop for display and related services; Terminal Equipment requirements; Part 1: On-hook data transmission".

[11] ETSI ETR 206: "Public Switched Telephone Network (PSTN); Multifrequency signalling system to be used for push-button telephones [CEPT Recommendation T/CS 46-02 E (1985)]".

[12] ETSI EN 300 659-2: "Access and Terminals (AT); Analogue access to the Public Switched Telephone Network (PSTN); Subscriber line protocol over the local loop for display (and related) services; Part 2: Off-hook data transmission".

[13] ETSI ES 200 778-2: "Access and Terminals (AT); Analogue access to the Public Switched Telephone Network (PSTN); Protocol over the local loop for display and related services; Terminal Equipment requirements; Part 2: Off-hook data transmission".

[14] ETSI ETS 300 128: "Integrated Services Digital Network (ISDN); Malicious Call Identification (MCID) supplementary service; Service description".

[15] ETSI TS 101 909-19 (sub-parts 1 and 2): "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 19: IPCablecom Audio Server Protocol Specification".

[16] IETF RFC 2719: "Framework Architecture for Signalling Transport".

[17] IETF RFC 2960: "Stream Control Transmission Protocol".

[18] ITU-T Recommendation J.165: "IPCablecom signalling transport protocol".

[19] ETSI TS 101 909-12: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 12: Internet Signalling Transport Protocol (ISTP)".

[20] ETSI TR 102 088: "Public Switched Telephone Network (PSTN); Subscriber line protocol for Advice of Charge (AoC) display services".

[21] ETSI TS 101 909-2 (2001): "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 2: Architectural framework for the delivery of time critical services over cable Television networks using cable modems".

[22] IETF RFC 1899: "Request for Comments Summary RFC Numbers 1800-1899".

[23] ETSI TS 101 312: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Network architecture and reference configurations; Scenario 1".

[24] ETSI TS 101 909-4: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 4: Network Call Signalling Protocol".

[25] IETF RFC 2705 (1999): "Media Gateway Control Protocol (MGCP) Version 1.0".

[26] IETF RFC 2234 (1997): "Augmented BNF for Syntax Specifications: ABNF".

[27] ETSI TS 101 909-5: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 5: Dynamic Quality of Service for the Provision of Real Time Services over Cable Television Networks using Cable Modems".

[28] IETF RFC 2205 (1997): "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification" (Updated by RFC 2750).

[29] IETF RFC 2748 (2000): "The COPS (Common Open Policy Service) Protocol".

[30] IETF RFC 2210 (1997): "The Use of RSVP with IETF Integrated Services".

[31] ETSI TS 101 329-3 (V1.1.1): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); End-to-End Quality of Service in TIPHON Systems; Part 3: Signalling and Control of end-to-end Quality of Service".

[32] ETSI TS 101 909-17: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 17: Inter-domain Quality of Service".

[33] IETF RFC 2543: "SIP: Session Initiation Protocol".

[34] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[35] ETSI TS 101 909-11: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 11: Security".

[36] ETSI TS 101 323: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Interoperable security profiles".

[37] ETSI TR 101 771: " Telecommunications and Internet protocol Harmonization Over Networks (TIPHON) Release 4; Service Independent requirements definition; Threat Analysis".

[38] ITU-T Recommendation J.170: "IPCablecom security specification".

[39] ETSI ETR 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".

[40] ITU-T Recommendation J.162: "Network call signalling protocol for the delivery of time critical services over cable television networks using cable modems".

[41] ITU-T Recommendation H.235: "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals".

[42] ITU-T Recommendation J.166: "IPCablecom management information base (MIB) framework".

[43] IETF RFC 2104: "HMAC: Keyed-Hashing for Message Authentication".

[44] IETF RFC 1890: "Using the Flow Label Field in IPv6".

[45] ITU-T Recommendation H.248: "Gateway control protocol".

[46] ETSI EN 300 356 (all parts): "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface".

[47] ETSI TS 101 909-13: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 13: Trunking Gateway Control Protocol".

[48] IEEE 802.2001: "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture".

[49] ETSI TS 101 878: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Capability Definition; Service Capabilities for a simple call".

[50] ETSI TS 101 909-9: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 9: Network Call Signalling (NCS) MIB Requirements".

[51] ITU-T Recommendation X.800: "Security architecture for Open Systems Interconnection for CCITT applications".

[52] ITU-T Recommendation X.811: "Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework".

3 Definitions and abbreviations

3.1 Definitions

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

authentication header: IPSec security protocol that provides message integrity for complete IP packets, including the IP header

Application-Specific Data: application-specific field in the IPSec header that along with the destination IP address provides a unique number for each SA

Baseline Privacy Interface Plus (BPI+): security portion of the ITU-T Recommendation J.112 standard that runs on the MAC layer

Certification Authority (CA): trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates

Call Agent (CA): part of the CMS that maintains the communication state, and controls the line side of the communication

Call Management Server (CMS): controls the audio connections

NOTE: Also called a Call Agent in MGCP/SGCP terminology. This is one example of an Application Server.

DiffServ Code Point (DSCP): field in every IP packet that identifies the DiffServ per hop behaviour

NOTE: In IP version 4, the Type Of Service (TOS) byte is redefined to be the DSCP. In IP version 6, the traffic class octet is used as the DSCP.

Hashed Message Authentication Code (HMAC): message authentication algorithm, based on either SHA-1 or MD5 hash and defined in IETF RFC 2104

Internet Key Exchange (IKE): key management mechanism used to negotiate and derive keys for SAs in IPSec

IKE-: IKE with pre-shared keys for authentication

IKE+: notation defined to refer to the use of IKE, which requires digital certificates for authentication

Message Authentication Code (MAC): fixed-length data item that is sent together with a message to ensure integrity, also known as a MIC

Operational Support System (OSS): back-office software used for configuration, performance, fault, accounting, and security management

Public Key Infrastructure (PKI): process for issuing public key certificates, which includes standards, certification authorities, communication between authorities and protocols for managing certification processes

quintet: UMTS authentication vector

Record Keeping Server (RKS): device which collects and correlates the various event messages

Signalling Gateway (SG): signalling agent that receives/sends SCN native signalling at the edge of the IP network

NOTE: In particular the SS7 SG function translates variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.

Session Initiation Protocol (SIP): application-layer control (signalling) protocol for creating, modifying, and terminating sessions with one or more participants

Signalling System number 7 (SS7): architecture and set of protocols for performing out-of-band call signalling with a telephone network

triplet: GSM authentication vector

Transaction Capabilities Application Protocol (TCAP): protocol within the SS7 stack that is used for performing remote database transactions with a Signalling Control Point

Ticket Granting Server (TGS): sub-system of the KDC used to grant Kerberos tickets

3.2 Abbreviations

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

AN	Access Node
ANC	ANnouncement Controller
ANP	ANnouncement Player
ANS	ANnouncement Server
AOC	Advice Of Charge
API	Application Programming Interface

ATM	Asynchronous Transfer Mode
BICC	Bearer Independent Call Control
BNF	Backus-Noun Form
BPI+	Baseline Privacy Interface Plus
BRI	Basic Rate ISDN
C7	Signalling System Number 7
CA	Call Agent
CA	Certification Authority
CC	Call Control
CDR	Call Detail Record
CLIR	COnnected Line Identity Restriction
CM	Cable Modem
CMS	Call Management Server
CMSS	Call Management Server Signalling (CMS to CMS) signalling
CMTS	Cable Modem Termination System
COLP	COnnected Line identity Presentation
COPS	Common Open Policy Service
CS	Circuit Switched
CUG	Closed User Group
DCS	Distributed Call Signalling
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DNS	Domain Name System/Server/Service
DOCSIS	Data Over Cable Service Interface Specification
DSCP	DiffServ Code Point
E-MTA	Embedded MTA
ER	Edge Router
FG	Functional Grouping
GC	Gate Controller
HFC	Hybrid Fibre/Coaxial [cable]
HLR	Home Location Register
HMAC	Hashed Message Authentication Code
HTTP	HyperText Transfer Protocol
ID	IDentifier
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IN	Intelligent Network
IN	Intelligent Network
IntServ	Integrated Services
IP	Internet Protocol
ISTP	Internet Signalling Transport Protocol
ISUP	Integrated Services digital network User Part
ITSP	IP-Telephony Service Provider
KDC	Key Distribution Centre
LNP	Local Number Portability
MAC	Media Access Control
MAC	Message Authentication Code
MD5	Message Digest 5
MF	Multi-Frequency
MG	Media Gateway
MGC	Media Gateway Controller
MGC	Media Gateway Controller
MGCI	Media Gateway Controller Interface
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MMH	Multilinear Modular Hash
MP	Media Player
MPC	Media Player Controller
MPLS	MultiProtocol Label Switching
MSC	Message Sequence Chart

MSC	Message Sequence Charts
MSC	Mobile Services switching Centre
MTA	Multimedia Terminal Adapter
NCS	Network Call Signalling
NTS	Number Translation Services
OSS	Operational Support System
PKI	Public Key Infrastructure
PKINIT	Public Key Cryptography Initial Authentication
PS	Packet Switched
PSTN	Public Switched Telephone Network
PSTN	Public Switched Telephony Network
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
QoS	Quality of Service
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RAS	Request Admission Status
RFC	Request For Comments
RKS	Record Keeping Server
RSVP	Resource reSerVation Protocol
RTCP	Real-Time Control Protocol
RTP	Real-Time Transfer Protocol
SA	Source Address
SAP	Service Access Point
SCN	Switched Circuit Networks
SCP	Service Control Point
SCTP	Stream Control Transmission Protocol
SDL	Specification and Description Language
SDP	Session Description Protocol
SG	Signalling Gateway
SHA-1	Secure Hash Algorithm 1
SIP	Session Initiation Protocol
SIP	Session Initiation Protocol
SIP+	Session Initiation Protocol Plus
S-MTA	Standalone MTA
SNMP	Simple Network Management Protocol
SOCLIR	System Override of Calling Line Identity Restriction
SS7	Signalling System 7
SS7	Signalling System number 7
T	Triplet, GSM authentication vector
TCAP	Transaction Capabilities Application Protocol
TCP	Transmission Control Protocol
TCP	Transport Control Protocol
TD	Timeout for Disconnect
TFTP	Trivial File Transfer Protocol
TGCP	Trunking Gateway Control Protocol
TGS	Ticket Granting Server
TIPHON	Telecommunication and Internet Protocol Harmonization Over Networks
TLV	Type-Length-Value
TMSI	Temporary Mobile Subscriber Identity
TOS	Type of Service
TR	Technical Report
UDP	User Datagram Protocol
USIM	User Services Identity Module
VoIP	Voice over IP

4 Overview

The study was initially conducted to identify what was needed to be done for convergence between IPCablecom and TIPHON. However, it was recognized that this task was extremely ambitious, hence the present document describes an analysis of interworking between IPCablecom and TIPHON.

Three interworking scenarios have been defined, interworking through:

- Switched Circuit Network interfaces.
- Media Gateway Control interfaces.
- Session Initiation Protocol interfaces.

The main issues are addressed in the remainder of clause 4 of the present document.

Of interest are the limitations on end-end QoS and security introduced by interworking between TIPHON and IPCablecom systems.

The three interworking scenarios are summarized in the following clauses.

4.1 Interworking through SCN Interfaces

Both TIPHON and IPCablecom support an SCN interface for basic call. The signalling is done through ISUP whilst the media transfer is either PSTN or IP in the case of TIPHON and only PSTN for IPCablecom at this point in time. It is likely that IPCablecom will evolve to ISDN.

This interworking assumes that TIPHON completes the protocol mapping to ISUP. When the protocol mapping to ISUP is completed, then the TIPHON Release 3 basic call will be supported.

That interworking could be assured either through an actual network which would act as a transit network or without an intermediate network in a piggy back fashion (like a null modem). In the later case, one network plays the role of the PSTN and the other plays its normal role.

The advantage of this interworking through SCN Interfaces approach is that it could be readily available.

The drawbacks of this interworking through SCN Interfaces approach are the weaknesses in terms of loss of capabilities in the areas of security and QoS. ISUP does not offer QoS parameter negotiation and does not support security mechanisms for signalling.

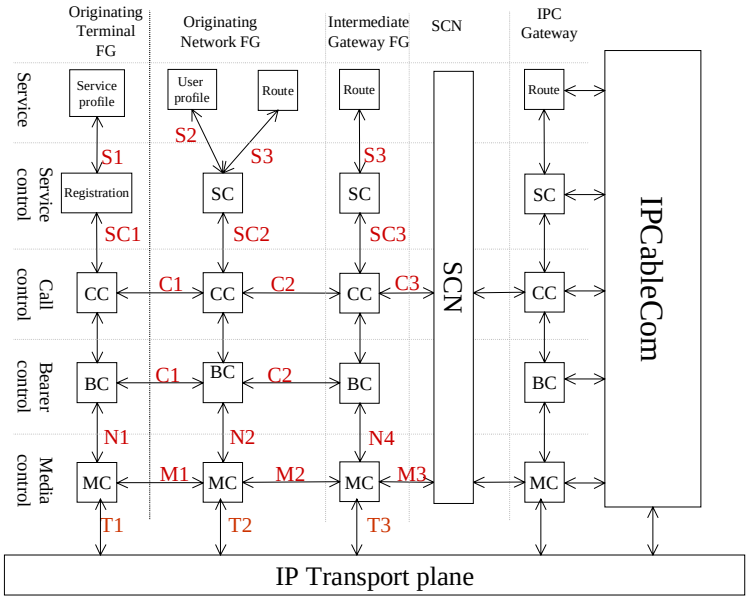

Figure 1: IPCablecom interworking with TIPHON through SCN