TECHNICAL REPORT

ISO/IEC

TR

16166

First edition
2010-08-01

Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Security of session-based communications

Technologies de l'information — Téléinformatique — Réseaux d'entreprise de prochaine génération (NGCN) — Sécurité des communications sur la base de sessions

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 16166 was prepared by Ecma International (as ECMA TR/100) and was adopted, under a special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

Introduction

This Technical Report is one of a series of Ecma publications that explore IP-based enterprise communication involving Corporate telecommunication Networks (CNs) (also known as enterprise networks) and in particular Next Generation Corporate Networks (NGCN). The series particularly focuses on inter-domain communication, including communication between parts of the same enterprise, between enterprises and between enterprises and carriers. This particular Technical Report discusses issues related to the security of session-based communications and builds upon concepts introduced in ISO/IEC TR 12860.

This Technical Report is based upon the practical experience of Ecma member companies and the results of their active and continuous participation in the work of ISO/IEC JTC1, ITU-T, ETSI, IETF and other international and national standardization bodies. It represents a pragmatic and widely based consensus. In particular, Ecma acknowledges valuable input from experts in ETSI TISPAN.

Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Security of session-based communications

1   Scope

This Technical Report is one of a series of publications that provides an overview of IP-based enterprise communication involving Corporate telecommunication Networks (CNs) (also known as enterprise networks) and in particular Next Generation Corporate Networks (NGCN). The series particularly focuses on session level communication based on the Session Initiation Protocol (SIP) [4], with an emphasis on inter-domain communication. This includes communication between parts of the same enterprise (on dedicated infrastructures and/or hosted), between enterprises and between enterprises and public networks. Particular consideration is given to Next Generation Networks (NGN) as public networks and as providers of hosted enterprise capabilities. Key technical issues are investigated, current standardisation work and gaps in this area are identified, and a number of requirements and recommendations are stated. Among other uses, this series of publications can act as a reference for other standardisation bodies working in this field, including ETSI TISPAN, 3GPP, IETF and ITU-T.

This particular Technical Report discusses security of session-based communications. It uses terminology and concepts developed in ISO/IEC TR 12860 [1]. It identifies a number of requirements impacting NGN standardisation and makes a number of recommendations concerning deployment of enterprise networks. Also a number of standardisation gaps are identified. Both signalling security and media security are considered.

The scope of this Technical Report is limited to communications with a real-time element, including but not limited to voice, video, real-time text, instant messaging and combinations of these (multi-media). The non-real-time streaming of media is not considered. For media, only security of transport (e.g., securing the Real-time Transport Protocol, RTP [6]) is considered, and higher level security measures (e.g., digital rights management) are not considered. Peer-to-peer signalling between SIP user agents (without involving SIP intermediaries) is not considered.

Detailed considerations for lawful interception are outside the scope of this Technical Report, although general considerations for call recording and audit are discussed.

2   References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[1]   ISO/IEC TR 12860, Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — General

[2]   ISO/IEC TR 12861, Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Identification and routing

[3]   ISO/IEC TR 16167, Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Emergency calls

[4]   IETF RFC 3261, SIP: Session Initiation Protocol

[5]   IETF RFC 3325, Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks

[6]   IETF RFC 3550, RTP: A Transport Protocol for Real-Time Applications

[7]   IETF RFC 3711, The Secure Real-time Transport Protocol (SRTP)

[8]   IETF RFC 3830, MIKEY: Multimedia Internet KEYing

[9]   IETF RFC 3893, Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format

[10]   IETF RFC 4119, A Presence-based GEOPRIV Location Object Format

[11]   IETF RFC 4301, Security Architecture for the Internet Protocol

[12]   IETF RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1

[13]   IETF RFC 4347, Datagram Transport Layer Security

[14]   IETF RFC 4474, Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)

[15]   IETF RFC 4567, Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)

[16]   IETF RFC 4568, Session Description Protocol (SDP) Security Descriptions for Media Streams

[17]   IETF RFC 4650, HMAC-Authenticated Diffie-Hellman for Multimedia Internet KEYing (MIKEY)

[18]   IETF RFC 4738, MIKEY-RSA-R: An Additional Mode of Key Distribution in Multimedia Internet KEYing (MIKEY)

[19]   IETF RFC 4916, Connected Identity in the Session Initiation Protocol (SIP)

[20]   IETF RFC 4961, Symmetric RTP / RTP Control Protocol (RTCP)

[21]   IETF RFC 5626, Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)

[22]   IETF RFC 5630, The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)

[23]   IETF RFC 5761, Multiplexing RTP Data and Control Packets on a Single Port

[24]   IETF RFC 5763, Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)

[25]   IETF RFC 5764, Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)

[26]   IETF draft-ietf-sip-connect-reuse-14, Connection Reuse in the Session Initiation Protocol (SIP)

NOTE   At the time of publication of this Technical Report, the IETF had approved this draft as a standards track RFC but had not published the RFC and had not allocated an RFC number. If the draft is no longer available, readers should look for the RFC with the same title.

[27]   IETF draft-ietf-sipcore-location-conveyance-02, Location Conveyance for the Session Initiation Protocol

NOTE   At the time of publication of this Technical Report, the IETF had not completed the approval process for this draft and had not allocated an RFC number. If the draft (or a later version) is no longer available, readers should look for the RFC with the same title.

[28]   IETF draft-zimmermann-avt-zrtp-16, ZRTP: Media Path Key Agreement for Secure RTP

NOTE   At the time of publication of this Technical Report, the IETF had not published this as an informational RFC. If the draft (or a later version) is no longer available, readers should look for the RFC with the same title.

[29]   ITU-T Recommendation E.164, The international public telecommunication numbering plan

[30]   ISO/IEC 9594-8│ITU-T Rec. X.509, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

[31]   3GPP TS 33.203, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services (Release 8)

[32]   3GPP TS 33.210, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Network domain security; IP network layer security (Release 8)

[33]   3GPP TS 33.310, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network domain security; Authentication Framework (AF) (Release 8)

[34]   ETSI TS 187 003, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture

[35]   IEEE 802.1x, IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control (2004)

[36]   IEEE 802.11, IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements - Part 11: Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications (2007)

[37]   OASIS, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 (March 2005)

[38]   ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements