ATIS STANDARD

ATIS-0100024.2009(*S*2019)

User-Network Interface (UNI) Media Plane Security Standard For Evolving VoIP/Multimedia Networks

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-0100024.2009(S2019), *User-Network Interface (UNI) Media Plane Security Standard for Evolving VoIP/Multimedia Networks*

Is an American National Standard developed by the ATIS **Network Performance, Reliability, and Quality of Service Committee (PRQC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0100024.2009(S2019)

American National Standard for Telecommunications

USER-NETWORK INTERFACE (UNI) MEDIA PLANE SECURITY STANDARD FOR EVOLVING VOIP/MULTIMEDIA NETWORKS

Alliance for Telecommunications Industry Solutions

Approved May 5, 2009

(Republished April 2022 with an administrative edit)

American National Standards Institute, Inc.

Abstract

This Standard provides a set of security guidelines and requirements for Media (User) Plane Security in Next Generation Networks.

Foreword

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Network Performance, Reliability, and Quality of Service Committee (PRQC) develops and recommends standards, requirements, and technical reports related to the performance, reliability, and associated security aspects of communications networks, as well as the processing of voice, audio, data, image, and video signals, and their multimedia integration. PRQC also develops and recommends positions on, and foster consistency with, standards and related subjects under consideration in other North American and international standards bodies.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PRQC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, PRQC, which was responsible for its development, had the following roster:

M. Neibert, PRQC Chair (Telcordia)

P. Tarapore, PRQC Vice-Chair (AT&T)

C. Underkoffler, ATIS Chief Editor

A. Webster, Technical Editor (US Department of Commerce)

J. Colombo, Technical Editor (Verizon)

TABLE OF CONTENTS

TABLE OF FIGURES

American National Standard for Telecommunications –

User-Network Interface (UNI) Media Place Security Standard for Evolving VoIP/Multimedia Networks

INTRODUCTION/EXECUTIVE SUMMARY

Many security threats exist to the media plane of telecommunications networks. In addition, new security threats to the media plane are being introduced as the network evolves. The purpose of this standard is to provide user to network interface (UNI) media plane (user plane) security requirements for packet based evolving telecommunications networks

1 SCOPE, PURPOSE AND APPLICATION

The scope of this standard is to define the user to network interface media plane security requirements. The standard addresses security requirements for voice over packet and multimedia media plane security, including media plane traffic as set up under the Session Initiation Protocol (SIP). [RFC 3261].

This standard addresses VoP/Multimedia media plane security requirements of evolving telecommunications networks. Evolving telecommunications networks often combine legacy telecommunication facilities with new technologies such as Wireless (air interface), Asynchronous Transfer Mode (ATM), and Internet Protocol (IP) transport mechanisms. The security requirements given in this standard apply to service provider networks and may also be applicable to individual company single location and corporate enterprise multi-location networks.

This standard takes the following into consideration:

- Network operators may not always have complete control with respect to which terminal the user uses to connect to the network, and thereby its capabilities with respect to security may not be known.

- The user may use a separate access provider network.

- There may be differences in security depending on the access technology used to connect the user to the network.

This standard concerns the user to network interface (UNI) of evolving networks. For this standard, the UNI is defined as the interface between a VoP/multimedia end user device or terminal (e.g. SIP UA) and the network that provides service to the device or terminal. This standard identifies the various security mechanisms that could be used on this interface. For each of these various mechanisms the specific requirements are defined.

This standard is not intended to imply that each terminal type must support all security mechanisms. Given that a terminal supported a particular security mechanism then it is expected that for that option the terminal would support the appropriate requirements identified.

In this standard, “shall” indicates a mandatory requirement and “should” indicates an optional requirement.

Management and Signaling Plane security issues are outside the scope of this standard.

The purpose of this standard is to specify baseline security requirements for media plane functions of evolving telecommunications networks that use SIP protocols to set up media plane sessions. The intent of this standard is to provide media plane security requirements which may be used by carriers and vendors to allow secure interoperability of multi-vendor end-user devices and networks. This standard provides a minimal set of security requirements as well as general security guidance.

2 Normative References

[RFC 3261] [1]	SIP: Session Initiation Protocol, Internet Engineering Task Force, June 2002.
[RFC 4301] [1]	Security Architecture for the Internet Protocol, Internet Engineering Task Force, December 2005.
[RFC 3706] [1]	A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, Engineering Task Force, February 2004. ftp://ftp.rfc-editor.org/in-notes/rfc3706.txt
[RFC 3711] [1]	The Secure Real-time Transport Protocol (SRTP). Internet Engineering Task Force, March 2004.
[RFC 760] [1]	User Datagram Protocol. Internet Engineering Task Force, August 1980
[RFC 4303] [1]	ESP Encapsulating Security Payload (ESP). Internet Engineering Task Force, December 2005. http://www.ietf.org/rfc/rfc4303.txt
[RFC 4305] [1]	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) Internet Engineering Task Force, December 2005.
[RFC 4306] [1]	The Internet Key Exchange (IKEv2) Protocol, Internet Engineering Task Force, December 2005.
[RFC 4307] [1]	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2) December 2005
[RFC 4347] [1]	Datagram Transport Layer Security,. Internet Engineering Task Force, April 2006. http://www.ietf.org/rfc/rfc4347.txt
[IEEE 802.11i][2]	IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, July 2004
[WPA][3]	Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. Wi-Fi Alliance. 2003.

[1] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org

[2] This document is available from the Institute of Electrical and Electronics Engineers (IEEE). < http://shop.ieee.org/store/ >

[3] This document is available from http://www.wi-fi.org/

[WPA2] [3]	WPA2 (Wi-Fi Protected Access 2) Wi-Fi Alliance. 2004.
[ATIS-0100014][4]	Information and Communications Security for NGN Converged Services IP Networks and Infrastructure
[ITU-T X.805][5]	ITU-T SG17 Recommendation X.805, Security Architecture for Systems Providing End-to-End Communications (10/03).
[ATIS-1000007][4]	Generic Signaling and Control Plane Security Requirements for Evolving Networks: ATIS-1000007.2006(R2011)
[ATIS-1000025[4]].	US Standard for Signaling Security – UNI Access and Signaling Standard: ATIS-1000025.2008
[ISO/IEC 15408-1][6]	ISO/IEC 15408-1:2005(E), Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, Second edition, International Standards Organization/ International Electrotechnical Commission, 2005-10-01
[ISO/IEC 15408-2[6]	ISO/IEC 15408-2:2005(E), Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements, Second edition, International Standards Organization/ International Electrotechnical Commission, 2005-10-01
[ISO/IEC 15408-3] [6]	ISO/IEC 15408-3:2005(E), Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements, Second edition, International Standards Organization/ International Electrotechnical Commission, 2005-10-01

[4] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

[5] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[6] This document is available from the International Organization for Standardization. < http://www.iso.ch/iso/en/prods-services/ISOstore/store.html >

[FIPS-140-1][7]	FIPS PUB 140-1, FIPS PUB 140-1, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, 1994 Janruary, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology
[FIPS-140-2][7]	FIPS PUB 140-2, FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, 2001 May 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology
[FIPS-180-1] [7]	FIPS PUB 180-1, FIPS PUB 180-1, SECURE HASH STANDARD, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, 1995 April 17, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology
[FIPS-198-1] [7]	FIPS PUB 198-1, FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC), FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, 2008 July,, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology
[FIPS-186-2] [7]	FIPS PUB 186-2, FIPS PUB 186-2, DIGITAL SIGNATURE STANDARD (DSS), FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, 2000 January 27, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology
[FIPS-197] [7]	FIPS PUB 197, FIPS PUB 197, ADVANCED ENCRYPTION STANDARD (AES), FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, November 26, 2001, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

3 DEFINITIONS

This document uses definitions as defined in “Technical Report – Information and Communications Security for Evolving Networks”, Reference [ATIS 0100014]. In addition, the following definitions are used in this document:

Media Plane: End user information content of a packet based communications, for example voice, video or multimedia. The media plane may also be called the end-user plane, and represents actual end-user data flows.

[7] This document is available from the National Institute of Standards and Technology (NIST) at < http://csrc.nist.gov/publications/fips/ >.

4 ABBREVIATIONS

This standard uses the following abbreviations:

ACL: Access Control List

NAT: Network Address Translation

RAS: Registration, Admission, Status

CRV: Call Reference Value

UA: User Agent

5 REFERENCE NETWORK MODEL AND ARCHITECTURE

This standard uses the framework and architecture proposed in ITU-T Recommendation X.805. Reference [ITU-T X.805]. ITU-T Recommendation X.805 is discussed in detail in Reference [ATIS-1000007].

The Security Architectural Model presented in ITU-T Recommendation X.805 consists of three architectural components:

1. Security Planes (End User Plane, Media Plane, and Management Plane).
2. Security Layers (Applications Security, Network Services Security and Infrastructure Security).
3. Security Dimensions (Access Control, Authentication, Non-repudiation, Data Confidentiality, Communications, Data Integrity, Availability, Privacy).

This standard is related to the ITU-T Recommendation X.805 model in the following manner:

1. Security Planes Addressed: Media Plane Only
2. Security Layers Addressed: Applications Security only (SIP).
3. Security Dimensions Addressed: All

Figure 1 illustrates SIP media and signaling plane interfaces:

- I1 – is the media plane interface between a SIP User Agent (UA) and the IP Network. (UNI)
- I2 – is the signaling plane interface between a SIP UA and a SIP Signaling Element. (Signaling plane UNI)
- I3 – is the signaling plane interface between two SIP Signaling Elements

This standard addresses interface I1 only.
Note: The SIP Signaling Element may be a SIP Registrar, SIP Proxy or Back to Back UA (B2BUA).

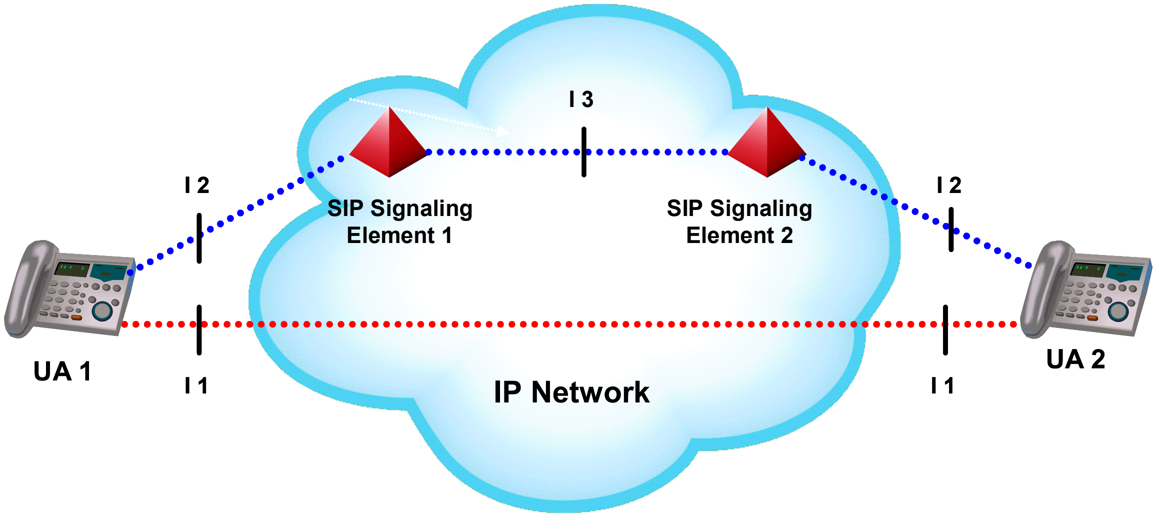

Figure 1 - SIP Reference Model

6 SIP User Plane Security

Session Initiation Protocol (SIP) is a control protocol used to support multimedia services over packet networks including services such as telephony, conferencing and instant messaging. The SIP protocol initiates media plane call/session setup, authentication and other call features within an IP domain. The SIP protocol is specified in IETF RFC-3261 and the SIP family of RFCs.

6.1 Access Control Security Dimension

<REQ-SEC-UNI-00500>

Some means on the network side of the UNI shall be used to restrict/grant access to media plane information from specific UAs on the customer side of the UNI.

<End of REQ-SEC-UNI-00500>

Note: Access Control Lists (ACL) are one possible mechanism that may be used to provide SIP media plane Access Control, however when using DHCP to obtain IP addresses, ACLs should not be used due to changing IP addresses.

<REQ-SEC-UNI-00600>

Means to detect and log unauthorized media plane access attempts to the network at the UNI shall be supported.

<End of REQ-SEC-UNI-00600>

Note: A system configurable threshold may be set for the number of unauthorized access attempts beyond which a system alarm will be generated, logged, and reported to a management system.

6.2 Authentication Security Dimension

This section will address the authentication requirements for user plan security for the UNI.

Authentication of User Agents and terminal equipment on the user side of the UNI is performed via the signaling and control plane. Requirements for the authentication security dimension for the signaling and control plane are specified in Reference [ATIS-1000025]..

6.3 Non-repudiation Security Dimension

Non-repudiation here is defined as a service that provides proof of the integrity and origin of data, both in an un-forgeable relationship, which can be verified by any third party at any time; or, in authentication, an authentication that with high assurance can be asserted to be genuine, and that can not subsequently be refuted. Non-repudiation is a signaling/control or management plane issue and does not apply to the media plane.

6.4 Audit Logging Security Dimension

The creation of an audit log is critical for the incident post-mortem and resulting investigation. This section will address the unique audit logging requirements of the user plane in the UNI. Audit logging was not originally included as a security dimension in X.805 however this concept is included here for completeness. Reference [ITU-T X.805].

<REQ-SEC-UNI-01300>
Any unauthorized media plane traffic arriving at the UNI shall be logged locally or remotely..
<End of REQ-SEC-UNI-01300>

Note:

This objective will be considered to be met if the occurrences of “unauthorized packets” are logged. The content of the “unauthorized packet” may be captured, however if it is, the system may be subject to DoS attacks and mechanisms to mitigate such events should be provided.

<REQ-SEC-UNI-01310>
Occurrences of unauthorized media plane traffic arriving at the UNI shall be tabulated.
<End of REQ-SEC-UNI-01310>

<REQ-SEC-UNI-01320>
Whenever the tabulation of unauthorized media plane traffic arriving at the UNI is updated, the tabulation shall be compared to a system configurable threshold.
<End of REQ-SEC-UNI-01320>

<REQ-SEC-UNI-01330>
When the tabulation of unauthorized media plane traffic arriving at the UNI exceeds the threshold, an alarm shall be generated and sent to a management system.
<End of REQ-SEC-UNI-01330>

<REQ-SEC-UNI-01335>
When the tabulation of unauthorized media plane traffic exceeds the threshold, the generated alarm shall be logged locally or remotely.
<End of REQ-SEC-UNI-01335>

<CR-SEC-UNI-01937>

The IPsec ESP transform should support Null integrity [RFC 4303].

<End of CR-SEC-UNI-01937>

<REQ-SEC-UNI-01340>
The threshold for unauthorized media plane traffic arriving at the UNI shall be configurable only by authorized entities either locally or remotely.
<End of REQ-SEC-UNI-01340>

Note: Media plane traffic arriving at the UNI that is not associated with an authorized UA (as per section 6.1) is to be considered as unauthorized media plane traffic.

6.5 Data Confidentiality Security Dimension

Data confidentiality of media plane traffic on an end-to-end basis between communicating UAs can be accomplished via the application of the following encryption mechanisms:

- Secure Real Time Protocol (SRTP) [RFC 3711],
- IP Security (IPsec) [RFC 4301], or
- Datagram Transport Layer Security (DTLS) protocol [RFC 4347].

However service/access providers should be sensitive to other obligations (e.g., lawful intercept) that may conflict with end-to-end data confidentiality of medial plane traffic.

<CR-SEC-UNI-01600>
End-to-end data confidentiality for media plane traffic traversing the UNI may be provided by the use of SRTP to protect media traffic such as phone conversations, video, and multimedia from unauthorized access or observation.
<End of CR-SEC-UNI-01600>

<CR-SEC-UNI-01610>
End-to-end data confidentiality for media plane traffic traversing the UNI may be provided by the use of IPsec ESP-3DES [RFC 4303] or IPsec ESP-AES [RFC 4303] to protect media traffic such as phone conversations, video, and multimedia from unauthorized access or observation.
<End of CR-SEC-UNI-01610>

<CR-SEC-UNI-01620>
End-to-end data confidentiality for media plane traffic traversing the UNI may be provided by the use of DTLS to protect media traffic such as phone conversations, video, and multimedia from unauthorized access or observation.
<End of CR-SEC-UNI-01620>

Different access technologies used to connect the end user device to the network may have different inherent security capabilities. For example, a DSL line from a service provider connecting a single residential SIP user to the service provider's domain may have a similar level of security for the user to network connection as a traditional phone connection. However a service provider connecting a SIP user via a wireless access technology without air interface security enabled may be less secure than a traditional phone connection. As such, it is recommended that all end user terminals connecting to networks via wireless access technology employ some form of confidentiality mechanism

<CR-SEC-UNI-01630>

Wireless access data confidentiality for media plane traffic arriving at the UNI should be provided by the use of 802.11i [IEEE 802.11i] to protect media traffic such as phone conversations, video, and multimedia from unauthorized access or observation.

<End of CR-SEC-UNI-01630>

<CR-SEC-UNI-01640>

Wireless access data confidentiality for media plane traffic arriving at the UNI may be provided by the use of WPA [WPA] or WPA2 [WPA2] to protect media traffic such as phone conversations, video, and multimedia from unauthorized access or observation. It should be noted that WPA TKIP is considered weak and thus this mode no longer is no longer recommended and its use should be deprecated. Instead, it is recommended that WPA2 be used with the AES encryption mode.

<End of CR-SEC-UNI-01640>

6.6 Communication Security Dimension

No additional requirements to address the Communication Security dimension have been identified beyond those specified in the Authentication Security (Section 6.2) and Data Integrity (Section 6.6) dimensions in this standard.

6.7 Data Integrity Security Dimension

Data integrity of media plane traffic to protect it from transmission errors or errors from malicious actions can be accomplished via the application of the following mechanisms:

- User Datagram Protocol (UDP) [RFC 768] (error protection only)
- SRTP
- IPsec
- DTLS

However service/access providers should be sensitive to other obligations (e.g., lawful intercept) that may conflict with SRTP, IPsec or DTLS provided data integrity of media plane traffic. Additionally, UDP checksum does not protect against unauthorized malicious and intentional data modification where an attacker adapts the checksum according to the made data manipulation.

<CR-SEC-UNI-01700>

Data integrity protection against media plane traffic transmission errors across the UNI may be provided by the use of the UDP checksum.

<End of CR-SEC-UNI-01700>

<CR-SEC-UNI-01710>

Data integrity against malicious actions for media plane traffic traversing the UNI may be provided by the use of SRTP to protect media traffic such as phone conversations, video, and multimedia from undetected modification.

<End of CR-SEC-UNI-01710>

<CR-SEC-UNI-01720>

Data integrity against malicious actions for media plane traffic traversing the UNI may be provided by the use of IPsec ESP-3DES [RFC 4303] or IPsec ESP-AES [RFC 4303] to protect media traffic such as phone conversations, video, and multimedia from undetected modification.

<End of CR-SEC-UNI-01720>

<CR-SEC-UNI-01730>

Data integrity against malicious actions for media plane traffic traversing the UNI may be provided by the use of IPsec ESP-nul [RFC 4303] to protect media traffic such as phone conversations, video, and multimedia from undetected modification.

<End of CR-SEC-UNI-01730>

<CR-SEC-UNI-01740>

Data integrity against malicious actions media plane traffic traversing the UNI may be provided by the use of DTLS to protect media traffic such as phone conversations, video, and multimedia from undetected modification.

<End of CR-SEC-UNI-01740>

6.8 Availability Security Dimension

As a best practice, network entities communicating across the UNI should implement mechanisms to detect and mitigate IP media plane DoS attacks. Both application layer flooding attacks, network layer flooding attacks, and malformed packet attacks should be mitigated by the DoS protection mechanisms.

Attacks directly against the SIP media plane are not necessarily required to break or disable the service entirely. Where SIP relies upon ancillary services, such as DNS, RSVP, SNMP, and others, attacks against these underlying infrastructure services should also be mitigated by security and DoS protection mechanisms.

6.9 Privacy Security Dimension

Privacy is the right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. {Reference [ITU X.800]}. Privacy, as it relates to the media plane, involves the right of individuals to control or influence the media plane information sent or received such as VoIP and/or Multimedia user information. Users have no mechanisms to influence the disclosure or collection of media plane information once it has left the UA. The best protection mechanism a user may employ is to ensure that media plane information is protected by a confidentiality security mechanism as per <CR-SEC-UNI-01600> so that only desired end UA may receive this information. This will help ensure that any media plane information collected remains confidential to all but the desired end UA, however it is still possible for the end UA (or any other party that obtains the session encryption key) to collect or disclose the media plane information. Please note that ITU X.800 goes on to qualify privacy in the following manner; “Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security”. {Reference [ITU X.800]}.

7 LAWFUL INTERCEPT

Data confidentiality or data integrity of media plane traffic are provided by any of the following encryption mechanisms:

- SRTP,
- IPsec ESP-3DES,
- IPsec ESP-AES, or
- DTLS,

Use of encryption algorithms may interfere with other service/access provider obligations (e.g., lawful intercept).

8 CRYPTOGRAPHY WHEN DATA CONFIDENTIALITY OR DATA INTEGRITY OF MEDIA PLANE TRAFFIC ARE PROVIDED BY ANY OF THE FOLLOWING MECHANISMS:

- SRTP,
- IPsec ESP-3DES,
- IPsec ESP-AES,
- IPsec ESP-nul, or
- DTLS,

There are a number of important configuration attributes that need be considered. The following sub-clauses address these considerations for each of the above mechanisms.

8.1 SRTP Configuration

8.1.1 SRTP Algorithms

At the time of writing of this document, SRTP implementation should minimally support the following cryptographic parameters as per [RFC 3711]:

If SRTP is selected as the option by which security is to be invoked then the following requirements are to be met:

<REQ-SEC-UNI-01800>

The SRTP Encryption Algorithm shall be AES_CM

<End of REQ-SEC-UNI-01800>

<REQ-SEC-UNI-01805>

The SRTP Authentication Algorithm shall be HMAC_SHA1

<End of REQ-SEC-UNI-01805>

<REQ-SEC-UNI-01810>

The SRTP Key derivation function shall be AES_CM

<End of REQ-SEC-UNI-01810>

<REQ-SEC-UNI-01815>

The SRTP Master key length shall be at least 128 bits

<End of REQ-SEC-UNI-01815>

> NOTE: The term Master can be interpreted to have unfortunate connotations in current usage. This terminology has been used in the approved IETF References and is being retained solely to assist the reader in understanding the principles and when referring to the referenced text.

<REQ-SEC-UNI-01820>

The SRTP Master salt key length shall be at least 112 bit s

<End of REQ-SEC-UNI-01820>

<REQ-SEC-UNI-01825>

The SRTP Session encryption key length shall be at least 128 bit s

<End of REQ-SEC-UNI-01825>

<REQ-SEC-UNI-01830>

The SRTP Session authentication key length shall be at least 160 bits

<End of REQ-SEC-UNI-01830>

<REQ-SEC-UNI-01835>

The SRTP Session salt key length shall be at least 112 bits

<End of REQ-SEC-UNI-01835>

<REQ-SEC-UNI-01840>

The SRTP packet maximum lifetime shall be 2^48 packets

<End of REQ-SEC-UNI-01840>

<REQ-SEC-UNI-01845>

The SRTP SRTCP packet maximum lifetime shall be 2^31 packets

<End of REQ-SEC-UNI-01845>

<REQ-SEC-UNI-01850>

The SRTP authentication tag length shall be at least 80 bits

<End of REQ-SEC-UNI-01850>

<REQ-SEC-UNI-01855>

The SRTP SRTCP authentication tag length shall be at least 80 bits

<End of REQ-SEC-UNI-0185>

8.1.2 SRTP Key Management

Key exchange for SRTP is currently conducted over the signaling and control plane (for example via the "Session Description Protocol") and as such it is beyond the scope of this document. There is work being conducted at the IETF which may result in key exchange performed over the media plane, however at the time of writing of this document no standardized methods are available. Key exchange mechanisms over the media plane may have implications for Lawful Intercept. See Reference [RFC 4568] for more information on the Session Description Protocol.

8.2 IPsec Configuration

If IPsec is selected as the option by which security is to be invoked then the following requirements are to be met:

At the time of writing of this document, IPsec implementations should minimally support the following capabilities and cryptographic parameters:

<REQ-SEC-UNI-01900>

IPsec implementations shall conform to Crypto Suites for IPsec [RFC 4308, RFC 4869]

<End of REQ-SEC-UNI-01900>

<CR-SEC-UNI-01902>

IPsec usage of HMAC-SHA1-96 should be used rather than HMAC-MD5-96

<End of CR-SEC-UNI-01902>

<CR-SEC-UNI-01904>

Use of pre-shared keys with IKE should not be used.

<End of CR-SEC-UNI-01904>

<CR-SEC-UNI-01906>

IPsec implementations should use secure random number generators if available.

<End of CR-SEC-UNI-01906>

<REQ-SEC-UNI-01908>

IPsec implementations shall use strong pseudo-random number generator software conforming with the IETF informational RFC – Randomness Requirements for Security [RFC 4086].

<End of REQ-SEC-UNI-01908>

8.2.1 IPsec Modes

<CR-SEC-UNI-01910>

IPsec Tunnel mode should be used when IPsec has to traverse NAT functional entities.

<End of CR-SEC-UNI-01910>

<CR-SEC-UNI-01912>

IPsec Transport mode should be used when NAT is not encountered.

<End of CR-SEC-UNI-01912>

8.2.2 IPsec Transforms

<CR-SEC-UNI-01920>

The IPsec ESP-nul transform should be used when confidentiality is not required

<End of CR-SEC-UNI-01920>

<CR-SEC-UNI-01922>

The IPsec AH transform should not be used.

<End of CR-SEC-UNI-01922>

<CR-SEC-UNI-01924>

The IPsec ESP transform should support 3DES CBC-mode [RFC 2451] with 3 independent 56 bit keys.

<End of CR-SEC-UNI-01924>

<CR-SEC-UNI-01926>

The IPsec ESP transform should support AES CBC [RFC 3602] with 128 bit keys.

<End of CR-SEC-UNI-01926>

<CR-SEC-UNI-01928>

The IPsec ESP transform should support AES CBC [RFC 3602] with 196 bit keys.

<End of CR-SEC-UNI-01928>

<CR-SEC-UNI-01930>

The IPsec ESP transform should support AES CBC [RFC 3602] with 256 bit keys.

<End of CR-SEC-UNI-01930>

<CR-SEC-UNI-01932>

The IPsec ESP transform should support AES-counter mode [RFC 3686].

<End of CR-SEC-UNI-01932>

<CR-SEC-UNI-01934>

The IPsec ESP transform should support AES CCM [RFC 4309] (with 128 bit key).

<End of CR-SEC-UNI-01934>

<CR-SEC-UNI-01936>

The IPsec ESP transform should support Null encryption [RFC 2410].

<End of CR-SEC-UNI-01936>

<CR-SEC-UNI-01938>

3DES CBC-mode and AES CBC should only be used with some additional data-origin authentication mechanism as per [RFC 4305].

<End of CR-SEC-UNI-01938>

<CR-SEC-UNI-01940>

The IPsec ESP transform should support HMAC-SHA1-96 [RFC 2404] with 160 bit key.

<End of CR-SEC-UNI-01940>

<CR-SEC-UNI-01942>

The IPsec ESP transform should support HMAC-SHA with key lengths of 256, 384 and 512 bit keys [RFC 4868].

<End of CR-SEC-UNI-01942>

<CR-SEC-UNI-01944>

The IPsec ESP transform should support HMAC-MD5-96 with 128 bit key [RFC 2403].

<End of CR-SEC-UNI-01944>

<CR-SEC-UNI-01946>

The IPsec ESP transform should support AES-XCBC with 128 bit key [RFC 3566].

<End of CR-SEC-UNI-01946>

<CR-SEC-UNI-01948>

The IPsec ESP transform should support AES CMAC [RFC 4494].

<End of CR-SEC-UNI-01948>

8.2.3 IPsec Key Management

If IPsec is selected as the option by which security is to be invoked then the following requirements are to be met:

<REQ-SEC-UNI-01950>

The Internet Key Exchange (IKE) protocol shall be used to provide peer-entity authentication.

<End of REQ-SEC-UNI-01950>

> *<CR-SEC-UNI-01951>*
>
> *Implementations that use IKEv2 [RFC 4306] should as a minimum support the cryptographic algorithms of [RFC 4307].*
>
> *<End of CR-SEC-UNI-01951>*

<REQ-SEC-UNI-01952>

The Internet Key Exchange (IKE) protocol shall be used to provide an automatic mechanism for symmetric shared key generation, distribution and re-keying.

<End of REQ-SEC-UNI-01952>

<REQ-SEC-UNI-01954>

IKEv1 [RFCs, 2407, 2408, 2409, and 4109] shall be supported.

<End of REQ-SEC-UNI-01954>

<REQ-SEC-UNI-01956>

IKEv1 main mode operation shall be supported.

<End of REQ-SEC-UNI-01956>

<CR-SEC-UNI-01958>

IKEv1 aggressive mode operation should be supported.

<End of CR-SEC-UNI-01958>

<REQ-SEC-UNI-01960>

IKE shall support 3DES [3DES] (with three independent 56 bit keys) encryption algorithm.

<End of REQ-SEC-UNI-01960>

<REQ-SEC-UNI-01962>
IKE shall support AES [FIPS-197] (with 128 bit key) encryption algorithm.
<End of REQ-SEC-UNI-01962>

<CR-SEC-UNI-01964>
IKE should support AES [FIPS-197] (with 196 bit key) encryption algorithm.
<End of CR-SEC-UNI-01964>

<CR-SEC-UNI-01966>
IKE should support AES [FIPS-197] (with 256 bit key) encryption algorithm.
<End of CR-SEC-UNI-01966>

<CR-SEC-UNI-01968>
IKE should support AES XCBC Pseudo random function [RFC 4434] with 128 bit key encryption algorithm.
<End of CR-SEC-UNI-01968>

<REQ-SEC-UNI-01970>
IKE shall support MD5 [RFC 1321] (with 128 bit message digest).
<End of REQ-SEC-UNI-01970>

<CR-SEC-UNI-01972>
IKE should support SHA-1 [FIPS 180-2] (with 160 bit message digest).
<End of CR-SEC-UNI-01972>

<CR-SEC-UNI-01974>
IKE should support authentication of device identities as part of the key exchange protocol using Pre-shared keys (out-of-band' symmetric shared key).
<End of CR-SEC-UNI-01974>

<REQ-SEC-UNI-01976>
IKE shall support authentication of device identities as part of the key exchange protocol using Digital signatures (RSA) with a 1024 bit or greater key.
<End of REQ-SEC-UNI-01976>

<CR-SEC-UNI-01978>
Use of pre-shared keys with IKE should not be used.
<End of CR-SEC-UNI-01978>

<REQ-SEC-UNI-01980>

Use of Digital Signatures with IKE shall be used for peer-entity authentication and simplified electronic key distribution.

<End of REQ-SEC-UNI-01980>

<CR-SEC-UNI-01982>

The IKE implementation should support X.509v3 digital certificates, including extensions.

<End of CR-SEC-UNI-01982>

<CR-SEC-UNI-01984>

The IKE implementation should support On-line Certificate Status Protocol (RFC 2560).

<End of CR-SEC-UNI-01984>

<CR-SEC-UNI-01986>

The IKE implementation should support LDAP retrieval of digital certificates.

<End of CR-SEC-UNI-01986>

<CR-SEC-UNI-01988>

The IKE implementation should support LDAP retrieval of certificate revocation lists (CRLs).

<End of CR-SEC-UNI-01988>

<CR-SEC-UNI-01990>

The IKE implementation should support CA Trust Hierarchy traversal.

<End of CR-SEC-UNI-01990>

<CR-SEC-UNI-01992>

All IKE implementations should support the Diffie-Hellman Group 1 (768 bit prime MODP group).

<End of CR-SEC-UNI-01992>

<CR-SEC-UNI-01994>

All IKE implementations should support the Diffie-Hellman Group 2 (1024 bit prime MODP group).

<End of CR-SEC-UNI-01994>

<CR-SEC-UNI-01996>

All IKE implementations should support the Diffie-Hellman Group 3 (Elliptic curve group over GF[2^155]).

<End of CR-SEC-UNI-01996>

<CR-SEC-UNI-01998>

All IKE implementations should support the Diffie-Hellman Group 4 (Elliptic curve group over GF[2^185]).

<End of CR-SEC-UNI-01998>

<CR-SEC-UNI-01999>

IPsec implementations should include support for detecting a dead Internet Key Exchange (IKE) peers, called Dead Peer Detection (DPD), based upon IPSec traffic patterns to minimize the number of IKE messages that are needed to determine when to perform IKE peer failover, and to reclaim lost resources [RFC 3706].

<End of CR-SEC-UNI-01999>

8.3 DTLS Configuration

If DTLS is selected as the option by which security is to be invoked then the following requirements are to be met:

At the time of writing of this document, DTLS implementations should minimally support the following capabilities and cryptographic parameters:

<CR-SEC-UNI-02000>

DTLSv1 should be supported.

<End of CR-SEC-UNI-02000>

<REQ-SEC-UNI-02005>

DTLSv1 shall rely on the HMAC-SHA-1 (with 160 bit key) cryptographic algorithm to provide data origin authentication and data integrity services.

<End of REQ-SEC-UNI-02005>

<REQ-SEC-UNI-02010>

DTLSv1 shall provide support for Rivest Shamir Adleman (RSA) asymmetric encryption for key exchange.

<End of REQ-SEC-UNI-02010>

<REQ-SEC-UNI-02015>

DTLSv1 shall provide support for Diffie Hellman (DH) for key exchange.

<End of REQ-SEC-UNI-02015>

<CR-SEC-UNI-02020>

DTLSv1 implementations should use secure random number generators if available.

<End of CR-SEC-UNI-02020>

<CR-SEC-UNI-02025>

DTLSv1 implementations should use strong pseudo-random number generator software conforming with the IETF informational RFC – Randomness Requirements for Security [RFC 4086].

<End of CR-SEC-UNI-02025>

8.2.1 DTLS Authentication

<REQ-SEC-UNI-02030>

DTLSv1 shall not be used with “no authentication” where neither party authenticates it's identity to the other party.

<End of REQ-SEC-UNI-02030>

<CR-SEC-UNI-02035>

DTLSv1 should be used with “uni-directional authentication”, where only the server is authenticated to the client only, only when client authentication occurs following DTLS session establishment.

<End of CR-SEC-UNI-02035>

<CR-SEC-UNI-02040>

DTLSv1 should be used with “bi-directional authentication”, where both client and server authenticate to each other, when client authentication does not occur following DTLS session establishment.

<End of CR-SEC-UNI-02040>

8.2.2 DTLS Algorithms

<CR-SEC-UNI-02045>

DTLSv1 shall support the 3DES CBC-mode (with 3 independent 56 bit keys) cryptographic algorithm to provide encryption services.

<End of CR-SEC-UNI-02045>

<REQ-SEC-UNI-02050>

DTLSv1 shall support the AES CBC (with 128 bit key) cryptographic algorithm to provide encryption services.

<End of REQ-SEC-UNI-02050>

<CR-SEC-UNI-02055>

DTLSv1 should not support the Null encryption option.

<End of CR-SEC-UNI-02055>

<REQ-SEC-UNI-02060>

DTLSv1 shall support the TLS_RSA_WITH_NULL_SHA cipher suite.

<End of REQ-SEC-UNI-02060>

<REQ-SEC-UNI-02065>

DTLSv1 shall support the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite.

<End of REQ-SEC-UNI-02065>

<REQ-SEC-UNI-02070>

DTLSv1 shall support the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite.

<End of REQ-SEC-UNI-02070>

<REQ-SEC-UNI-02075>

DTLSv1 shall support the TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA cipher suite.

<End of REQ-SEC-UNI-02075>

<REQ-SEC-UNI-02080>

DTLSv1 shall support the TLS_DH_RSA_WITH_AES_128_CBC_SHA cipher suite.

<End of REQ-SEC-UNI-02080>

8.4 Cryptographic Module Certification

Certification of cryptographic functionality implemented in either hardware or software can be certified as complying with different standards. US Federal Government non-classified but confidential applications must be certified according to Federal Information Processing Standards (FIPS) produced by the Department of Commerce National Institute of Science and Technology (NIST). Commercial applications do not require any form of certification unless used in, or part of products and services purchased by or offered to Federal Government entities. The requirements for certification in each case are covered in the following two sub-clauses.

8.4.1

The following requirements specifically apply to those government activities that fall under FIPS mandates.

<REQ-SEC-UNI-03000>

Software cryptographic modules shall be certified as compliant to [FIPS-140-2] Level 1..

<End of REQ-SEC-UNI-03000>

<REQ-SEC-UNI-03005>

Hardware cryptographic modules shall be certified to a minimum of [FIPS-140-2] Level 2.

<End of REQ-SEC-UNI-03005>

<REQ-SEC-UNI-03010>

All implementations of the Secure Hash Algorithm (SHA-1) shall conform to, and be compliant with [FIPS-180-1].

<End of REQ-SEC-UNI-03010>

<REQ-SEC-UNI-03015>

The use of Keyed-Hash Message Authentication Codes (HMAC) shall conform to, and be compliant with [FIPS-198-1].

<End of REQ-SEC-UNI-03015>

<REQ-SEC-UNI-03020>

All implementations of the DIGITAL SIGNATURE STANDARD (DSS) shall conform to, and be compliant with [FIPS-186-2].

<End of REQ-SEC-UNI-03020>

<REQ-SEC-UNI-03025>

All implementations of the ADVANCED ENCRYPTION STANDARD (AES) shall conform to, and be compliant with [FIPS-197].

<End of REQ-SEC-UNI-03025>

8.4.2

The following requirements apply to those commercial products and services that do not fall under FIPS mandates.

<CR-SEC-UNI-03050>

Software cryptographic modules should be certified as compliant to [FIPS-140-2] Level 1.

<End of CR-SEC-UNI-03050>

<CR-SEC-UNI-03055>

Hardware cryptographic modules should be certified to a minimum of [FIPS-140-2] Level 2.

<End of CR-SEC-UNI-03055>

<CR-SEC-UNI-03060>

All implementations of the Secure Hash Algorithm (SHA-1) should conform to, and be compliant with [FIPS-180-1].

<End of CR-SEC-UNI-03060>

<CR-SEC-UNI-03065>

The use of Keyed-Hash Message Authentication Codes (HMAC) should conform to, and be compliant with [FIPS-198-1].

<End of CR-SEC-UNI-03065>

<CR-SEC-UNI-03070>

All implementations of the DIGITAL SIGNATURE STANDARD (DSS) should conform to, and be compliant with [FIPS-186-2].

<End of CR-SEC-UNI-03070>

<CR-SEC-UNI-03075>

All implementations of the ADVANCED ENCRYPTION STANDARD (AES) should conform to, and be compliant with [FIPS-197].

<End of CR-SEC-UNI-03075>

There any many cryptographic algorithms available within commercial products and services that do not have corresponding certification standards.

9 Quality of Experience/Quality of Service Related Aspects

The selection of security mechanisms and features must consider the QoE and QoS targets of the system. Issues related to the length of time to establish security associations; to encryption of the packet payload that prevents deep packet inspect to provide necessary priority service; to cryptographic overhead, that reduces the effective through put of the system. Recommendations on the selection of appropriate mechanisms to ensure that QoE and QoS targets are achievable are outside the scope of this document.

10 Advantages and Disadvantages of Various Media Security Protocols

The section will make recommendations as to appropriate security protocols to provide security mechanisms and services to secure the media plane of the UNI.

10.1 SRTP

The Secure Real-time Transport Protocol (SRTP) has been developed and promoted by the IETF as a method of securing real time transport protocol media plane traffic. SRTP is a profile of the Real-time Transport Protocol (RTP), and is used to provide confidentiality, message (data origin) authentication, and replay protection to the RTP traffic. For more information see Reference [RFC 3711].

10.1.1 SRTP Advantages

The Secure Real-time Transport Protocol (SRTP) has the following advantages:

- SRTP provides low packet expansion overhead. Typical packet expansion is 80 bits (only a 32-bit authentication tag, plus optional padding and master key identifier).
- With SRTP, all authentication and encryption keys are derived from a single master key. This key derivation reduces the need for multiple exchanges for key establishment,
- SRTP preserves RTP header compression which allows the IP/UDP/RTP headers to be efficiently compressed from typically 40 bytes to 2 bytes. Reference [RFC 3095], [RFC 4815].

10.1.1 SRTP Disadvantages

The Secure Real-time Transport Protocol (SRTP) has the following disadvantages:

- With SRTP, security is only provided for the RTP payload application layer information, and no security is provided for layer 3 and layer 4 information.

10.2 IPsec

The IPsec suite of protocols have been developed as a standard method of securing any type of traffic, including media plane traffic, that relies on IP at the internetworking protocol. IPsec can provide peer-entity authentication, message confidentiality, message (data-origin) authentication, and replay protection to RTP traffic.

10.2.1 IPsec Advantages

IPsec has the following advantages:

- IPsec provides the strongest security for IP traffic and protects all layers from layer 3 (transport layer) and above.
- IPsec can protect any traffic whether TCP or UDP based and any application layer protocol.
- IPsec may already be deployed in some network topologies.

10.2.2 IPsec Disadvantages

IPsec has the following disadvantages:

- IPsec has large packet expansion overhead (>20 bytes) which is large compared with the typically small RTP packet size of approximately 40 bytes.

- It is not possible to perform network address translation and network and port address translation with some modes of IPsec.

10.3 DTLS

The DTLS protocol has been developed as a standard method of securing any type of traffic, including media plane traffic that relies on the UDP transport protocol. DTLS can provide peer-entity authentication, message confidentiality, message (data-origin) authentication, and replay protection to RTP traffic. For more information see Reference [RFC 4347].

10.3.1 DTLS Advantages

DTLS has the following advantages:

- DTLS is based on the widely deployed TLS protocol, thus some preexisting TLS infrastructure and implementations may be adapted to DTLS.
- DTLS handshake (based on TLS) may be used as a method of exchanging keying material for SRTP.

10.3.1 DTLS Disadvantages

DTLS has the following disadvantages:

- DTLS has large packet expansion overhead (>17 bytes) which is large compared with the typically small RTP packet size of approximately 40 bytes.

APPENDIX A – INFORMATIVE REFERENCES

(Informative)

[ATIS-0300276.2008][8]	ATIS-0300276.2008, American National Standard for Telecommunications Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane.
[RFC 4568][9]	Session Description Protocol (SDP) Security Descriptions for Media Streams, Internet Engineering Task Force. July 2006. http://www.ietf.org/rfc/rfc4568.txt?number=4568
[RFC 4960] [9]	Stream Control Transmission Protocol, Internet Engineering Task Force, Sept 2007. http://www.ietf.org/rfc/rfc4960.txt?number=4960
[RFC 4302] [9]	IP Authentication Header, Internet Engineering Task Force, December 2005. http://www.ietf.org/rfc/rfc4302.txt?number=4302
[ITU X.800[10]]	ITU-T Recommendation X.800, Security Architecture for Open Systems Interconnection for CCITT Applications. 1991.
[ISO 15408][11]	The Common Criteria for Information Technology Security Evaluation, International Organization for Standardization – ISO. http://www.iso.org/iso/home.htm

[8] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

[9] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[10] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[11] This document is available from the International Organization for Standardization. < http://www.iso.ch/iso/en/prods-services/ISOstore/store.html >

APPENDIX B - COMMON CRITERIA SECURITY CONSIDERATIONS

(informative)

While the subject of product security evaluation and certification is outside the scope of this document, there is merit in highlighting that some work is ongoing in this area. In particular [ISO/IEC 15408-1] [ISO/IEC 15408-2] [ISO/IEC 15408-3] are a suite of ISO/IEC documents that deal with the subject of Information technology — Security techniques — Evaluation criteria for IT security. Sometimes this suite of documents is referred to as the Common Criteria for IT Security.

ATIS Technical Report, ATIS-0100014 provides background information related to this topical area in section 4.7.3.2. The intention of this work is make available a Common Criteria process which, when followed, would provide assurance that the process of specification, implementation and evaluation of a network element has been conducted in a rigorous and standard manner.

The Common Criteria process allows for seven Evaluation Assurance Levels (EAL) which correspond to the numerical rating describing the depth and rigor of an evaluation. These EAL's are:

EAL1: Functionally Tested

EAL2: Structurally Tested

EAL3: Methodically Tested and Checked

EAL4: Methodically Designed, Tested and Reviewed

EAL5: Semi formally Designed and Tested

EAL6: Semi formally Verified Design and Tested

EAL7: Formally Verified Design and Tested

Interested parties may apply the common criteria process to assist in achieving the proper depth and rigor of an evaluation consistent with their business needs, an EAL level from 1 – 4 may be most appropriate.