

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: August 30, 2007

V. Lehtovirta  
Ericsson Research NomadicLab  
February 26, 2007

Infrastructure aspects to media security  
draft-lehtovirta-rtpsec-infra-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on August 30, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

---

Internet-Draft   Infrastructure aspects to media security   February 2007

## Abstract

This document discusses some infrastructure aspects that should be considered in the media security requirements work.

## Table of Contents

<a href="#">1.</a>	Requirements notation . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Introduction . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Termination of media security in a gateway . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Using shared keys to provide media security . . . . .	<a href="#">6</a>
<a href="#">5.</a>	Setting up media security with the help of a third party . . . .	<a href="#">7</a>
<a href="#">6.</a>	Termination of media streams in different devices . . . . .	<a href="#">8</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">9</a>
<a href="#">8.</a>	References . . . . .	<a href="#">10</a>
<a href="#">8.1.</a>	Normative References . . . . .	<a href="#">10</a>
<a href="#">8.2.</a>	Informative References . . . . .	<a href="#">10</a>
	Author's Address . . . . .	<a href="#">11</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">12</a>

---

Internet-Draft   Infrastructure aspects to media security   February 2007

1.   Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

---

Internet-Draft   Infrastructure aspects to media security   February 2007

## [2.](#) Introduction

Requirements related to the ongoing media security work are discussed for example in [[I-D.wing-media-security-requirements](#)].

This document discusses some infrastructure aspects that should be considered in the media security requirements work.

These aspects are:

- o Termination of media security in a gateway
- o Using shared keys to provide media security
- o Setting up media security with the help of a third party
- o Termination of media streams in different devices

---

Internet-Draft   Infrastructure aspects to media security   February 2007

### [3.](#) Termination of media security in a gateway

A typical case of using media security is the one where two entities are having a VoIP conversation over IP capable networks. However, there are cases where the other end of the communication is not connected to an IP capable network. In this kind of setting, there needs to be some kind of gateway at the edge of the IP network which converts the VoIP conversation to format understood by the other network. An example of such gateway is a PSTN gateway sitting at the edge of IP and PSTN networks.

If media security (e.g. SRTP protection) is employed in this kind of gateway-setting, then media security and the related key management needs to be terminated at the gateway. The other network (e.g. PSTN) may have its own measures to protect the communication, but this means that from media security point of view the media security is not employed end-to-end between the communicating entities.

Therefore, media security solutions should cover the cases where media security is not employed end-to-end but is terminated in a gateway.

#### [4.](#) Using shared keys to provide media security

There are environments where the communicating endpoints set up shared keys with the network infrastructure. An example of such environment is the widely deployed GSM system and its 3G successor, the UMTS. It would be beneficial if the shared keys between the endpoints and the network infrastructure in these kind of systems could be re-used to provide shared keys also between the communicating endpoints.

Therefore, it might be justified to consider using shared keys in addition to public keys to provide media security in some environments.

## [5.](#)   Setting up media security with the help of a third party

Setting up a secured connection to an arbitrary peer requires that the communicating entities have in some way agreed on key management credentials, e.g. shared keys or certificates. From scalability point of view it is in practice not feasible to achieve this to an arbitrary peer without the help of some third party providing the credentials.

To enable a scalable solution that allows to set up a secure connection to an arbitrary peer seems to require the help of some third party.



In some cases, different media streams might be terminated in different devices. For example, the video part of a multimedia session could terminate in one device, while the audio part would terminate in another device. It should be possible to set up media security efficiently in such scenarios.

## [7.](#)   Security Considerations

None.

---

Internet-Draft   Infrastructure aspects to media security   February 2007

## [8.](#)   References

### [8.1.](#)   Normative References

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

### [8.2.](#)   Informative References

[I-D.wing-media-security-requirements]  
Wing, D., "Media Security Requirements",  
[draft-wing-media-security-requirements-00](#) (work in progress), October 2006.

Internet-Draft   Infrastructure aspects to media security   February 2007

Author's Address

Vesa Lehtovirta  
Ericsson Research NomadicLab  
JORVAS   FIN-02420  
FINLAND

Phone: +358 9 299 1  
Email: [vesa.lehtovirta@ericsson.com](mailto:vesa.lehtovirta@ericsson.com)

---

Internet-Draft   Infrastructure aspects to media security   February 2007

#### Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

#### Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information

on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

#### Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).