3GPP TSG SA WG3 Security — S3#22 **S3-020095**

25 - 28 February 2002

Bristol, UK

Source: Ericsson

Title: New and updated SIP drafts

Document for: Informative

1 Scope and objectives

Ericsson, Nokia and Nortel Networks have been involved in submitting altogether five new drafts and an updated one to IETF:

- Three core security requirements have been separated from "3GPP requirements on SIP [3gpp-requirements] and submitted as separate requirements by Ericsson per request of IETF chairs and ADs. The separate small requirement drafts should go forward smoother. The submissions are individual, and ~~the~~ draft-garcia-sipping-3gpp-reqs-02.txt is still the official 3GPP requirement draft. Corresponding solution drafts are needed for each requirement draft.

  Contents of the drafts:

  - Draft "3GPP Requirements for SIP Authentication" introduces the need for AKA algorithm in SIP, and discusses also recent extensible vs. specific authentication issues [SIP-AKA]. Solution draft "HTTP Digest Authentication Using AKA" is already submitted, see more status information in [S3-0200XX, Digest-AKA].

  - Draft "Requirements for SIP Security Mechanism Agreement" [SIP-AGR] introduces security mode setup needs. See more status information related to the corresponding solution draft below.

  - Draft "Requirements for Delegation of Message Protection for SIP" [SIP-DEL] introduces message protection delegation and key transport needs in IETF manner, i.e. using application layer security. A solution draft is needed, but hasn't been produced yet. Alternatively, this can be done outside the IETF domain, for example using an XML body for transporting keys.

  First indications from IETF chairs are that we still need to go to the IETF meeting to accept the drafts above (contrary to what they said before).

- Enhanced HTTP Digest status is discussed in [S3-020067].

- The need for "security mode set-up" in SIP has been discussed in IETF. Discussions in a SIPPING ad-hoc meeting in IETF-53 concluded that the issue is relevant for SIP, however, there is no agreement whether the existing SIP headers (e.g. Supported/Require) or new headers should be used. Furthermore, enhanced HTTP Digest has now some support for bidding down protection. Ericsson thinks that enhanced HTTP Digest is sufficient as a backup solution for security mode set-up, though not sufficient e.g. for upgrading from Digest to S/MIME or TLS.

  The existing solution draft, "Security Mechanism Agreement for SIP Connections", will be updated and submitted to the IETF by March 1. The draft is not available at the time this contribution is submitted to S3#22, however, an early version may be available from Ericsson delegations in the meeting. The main modifications will be:

- Full-path protection will probably be removed (we don't want to partly duplicate functionality in sips: URI)
- Client and server roles are reversed to allow servers be stateless
- better explanations about why new headers are needed and Supported / Require will not be suitable.

2 References

[Digest-AKA] Niemi et al, "HTTP Digest Authentication Using AKA", IETF, Work in progress, February 2002, draft-niemi-sipping-digest-aka-00.

[3gpp-requirements] Garcia et al, "3GPP requirements on SIP", IETF, Work in progress, November 2001, draft-garcia-sipping-3gpp-reqs-02.txt.

[S3-020067] Nortel Networks, "SIP Message Integrity Protection Work in the IETF", 3GPP, S2#22, 25-28 February 2002, Bristol, UK

[S3-0200XX] Nokia, Status report on HTTP Digest authentication using AKA, 3GPP, S2#22, 25-28 February 2002, Bristol, UK

[SIP-AKA] Arkko et al, "3GPP Requirements for SIP Authentication", IETF, Work in progress, February 2002, draft-uusitalo-sipping-authentication-00.txt

[SIP-AGR] Arkko et al., "Requirements for SIP Security Mechanism Agreement", IETF, Work in progress, February 2002, draft-uusitalo-sipping-algorithm-agreement-00.txt

[SIP-DEL] Arkko et al., "Requirements for Delegation of Message Protection for SIP", IETF, Work in progress, February 2002, draft-uusitalo-sipping-delegation-00.txt

Network Working Group   J. Arkko
INTERNET-DRAFT   V. Torvinen
draft-uusitalo-sipping-algorithm-agreement-00.txt   I. Uusitalo
Expires: August 2002   Ericsson
                                                           February 2002

Requirements for SIP Security Mechanism Agreement

Status of this Memo

1. Abstract

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution and multimedia conferences. SIP has a number of security mechanisms used for hop-by-hop or end-to-end protection. In this document we discuss requirements concerning SIP security mechanism agreement.

2. Conventions used in this document

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 [RFC 2119].

3. Table of contents

4. Introduction and Motivation

SIP has a number of security mechanisms for hop-by-hop and end-to-end protection. Some of the security mechanisms are built-in to the SIP protocol, such as variants of HTTP authentication and secure attachments such as S/MIME. SIP can also use underlying security protocols such as IPSec/IKE [7] and TLS [6]. Some of the built-in security protocols have alternative algorithms and parameters. A way to negotiate the used mechanisms, and parameters used within them, is needed. Without a secure negotiation method SIP is vulnerable to certain attacks. For example, HTTP authentication is known to be vulnerable to so called Bidding-Down attacks. There a Man-In-The-Middle attacker modifies messages in such a way that communicating parties believe the other side only supports weaker algorithms than they actually do. In small workstation networks these issues might not be very relevant, but the deployment of hundreds of millions of small devices with little or no possibilities for coordinated security policies, let alone software upgrades makes these issues much worse. You either deny connections from large amounts of older equipment or risk losing the benefit of new algorithms through attacks that are trivial to attackers.

The need for a security mechanism agreement is also supported by the fact that deployment of a large number of SIP-based consumer devices such as 3GPP terminals requires all network devices to be able to accommodate both current and future mechanisms. There is no possibility for instantaneous change since new solutions are coming gradually as new standards and product releases occur. It isn't even possible to upgrade some of the devices without getting completely new hardware.

The conclusions above are supported by the requirements from 3GPP [2] and discussed in more detail in [5].

This document is an effort to define requirements for secure algorithm agreement used with SIP protocol. Most of the requirements

are discussed also in "3GPP Requirements on SIP" [2], but we consider them to be beneficial also to infrastructures other than 3GPP. Therefore they've been separated into this new draft that's easier to deal with.

The requirements of this document address attacks discussed in chapter 22.1.3 and mechanisms discussed in chapter 22.2 of SIP-draft [1].

5. Definitions

MITM: Man-In-The-Middle

6. Requirements

Some of the built-in SIP security functions like HTTP Digest have alternative algorithms and other parameters. Different algorithms are suitable for different situations. Also, security holes might be found from old algorithms and new algorithms will evolve. Without a secure method to choose between algorithms and their parameters SIP is vulnerable to certain attacks, for example the MITM attack described above and in [5].

>> Req 1: It MUST be possible for a SIP node to select message protection algorithms and parameters within security mechanisms.

Also new security mechanisms will evolve and existing ones, like HTTP Digest or TLS, might be used in parallel depending on the situation. In order to achieve interoperability and backward compatibility, it would be beneficial if a SIP node could choose the security mechanism used.

>> Req 2: A SIP node MUST be able to select a SIP security mechanism among supported alternatives.

The negotiation methods must not be vulnerable to so called Bidding-Down attacks. In such an attack a MITM attacker modifies messages in such a way that parties believe the other side supports weaker security methods than they actually do.

>> Req 3: The negotiation mechanism MUST protect against attackers who do not have access to authentication credentials. In particular, it must not be possible for man-in-the-middle attackers to influence the negotiation result such that services with lower or no security are negotiated.

7. Discussion

Bidding-down protection is needed between different security schemes. It will not be sufficient to do bidding-down protection just for e.g. Digest. In SIP [8], only Digest is required, and most 3GPP terminals will also apply Digest. Hence a very large number of devices supporting only Digest will be deployed, and these devices

will probably be used for long in the future. Now, assume that in the future other mechanisms, for example S/MIME or TLS, are used in parallel with Digest. The new devices capable of these additional security mechanisms could offer to run e.g. TLS, but without protection against bidding-down attacks an attacker could make parties believe that the device on the other end does not support

TLS. Therefore TLS would not be used even if both devices supported it.

Algorithms can be agreed upon with basic SIP features, such as OPTIONS request and Require, Supported headers. They are capable of informing parties about various capabilities including security mechanisms. However, using these features in a straightforward manner does not guarantee the security of an agreement. In their basic form these methods are vulnerable to for example bidding-down attacks. At least some kind of integrity protection for the methods is needed.

Draft "Security Mechanism Agreement for SIP connections" [5] proposes a secure solution for algorithm agreement. There the security features are represented as regular option tags in SIP. The client announces a list of supported option tags in its first message, and the server returns its selection in the second message. The agreement is secured by simply repeating the client's original list of option tags in the client's first protected request (protected with a lower layer protocol). The solution in [5] supports both end-to-end and hop-by-hop agreement in a controllable fashion and without a large increase in roundtrips.

8. Acknowledgments

We would like to thank Allison Mankin, Dean Willis, Rohan Mahy, Bernard Aboba, Miguel Garcia, as well as numerous people at 3GPP SA3 and Ericsson for interesting discussions in this problem space.

9. References

1. Rosenberg, J., et al., "SIP: Session Initiation Protocol", draft-ietf-sip-rfc2543bis-07.txt, February 2002, work in progress.

2. Garcia, M., et al., "3GPP requirements on SIP", draft-garcia-sipping-3gpp-regs-02.txt, November 2001, work in progress.

3. 3GPP TS 23.228: "IP Multimedia (IM) Subsystem (Stage 2) - Release 5". Version 5.3.0 is available at ftp://ftp.3gpp.org/Specs/2001-12/Rel-5/23_series/23228-530.zip

4. 3GPP TS 24.228: "Signaling flows for the IP Multimedia call control based on SIP and SDP". Version 1.9.0 is available at ftp://ftp.3gpp.org/tsg_cn/WG1_mm-cc-sm/TSGN1_22/Docs/N1-

20280_24228-190.zip

5. Arkko, J., et al., "Security Mechanism Agreement for SIP Connections", draft-arkko-sip-sec-agree-00.txt, November 2001, work in progress.

6. Dierks, T., Allen, C., "The TLS Protocol, Version 1.0", RCF 2246, January 1999.

7. Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

8. Rosenberg, J., et al., "SIP:Session Initiation Protocol", draft-ietf-sip-rfc2543bis-05.txt, October 2001, work in progress.

10. Authors' Addresses

Jari Arkko
Oy LM Ericsson Ab
02420 Jorvas
Finland

Phone: +358 40 5079256
EMail: jari.arkko@ericsson.com

Vesa Torvinen
Oy LM Ericsson Ab
Joukahaisenkatu 1
20520 Turku
Finland

Phone: +358 40 7230822
EMail: vesa.torvinen@ericsson.fi

Ilkka Uusitalo
Oy LM Ericsson Ab
Tutkijantie 2C
90570 Oulu
Finland

Phone: +358 40 7245404
EMail: ilkka.uusitalo@ericsson.fi

Full Copyright Statement

Network Working Group J. Arkko
INTERNET-DRAFT V. Torvinen
draft-uusitalo-sipping-algorithm-agreement-00.txt I. Uusitalo
Expires: August 2002 Ericsson
February 2002

Requirements for SIP Security Mechanism Agreement

Status of this Memo

This document is an Internet Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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/1id-abstracts.html

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

1. Abstract

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution and multimedia conferences. SIP has a number of security mechanisms used for hop-by-hop or end-to-end protection. In this document we discuss requirements concerning SIP security mechanism agreement.

2. Conventions used in this document

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 [RFC 2119].

3. Table of contents

4. Introduction and Motivation

SIP has a number of security mechanisms for hop-by-hop and end-to-end protection. Some of the security mechanisms are built-in to the SIP protocol, such as variants of HTTP authentication and secure attachments such as S/MIME. SIP can also use underlying security protocols such as IPSec/IKE [7] and TLS [6]. Some of the built-in security protocols have alternative algorithms and parameters. A way to negotiate the used mechanisms, and parameters used within them, is needed. Without a secure negotiation method SIP is vulnerable to certain attacks. For example, HTTP authentication is known to be vulnerable to so called Bidding-Down attacks. There a Man-In-The-Middle attacker modifies messages in such a way that communicating parties believe the other side only supports weaker algorithms than they actually do. In small workstation networks these issues might not be very relevant, but the deployment of hundreds of millions of small devices with little or no possibilities for coordinated security policies, let alone software upgrades makes these issues much worse. You either deny connections from large amounts of older equipment or risk losing the benefit of new algorithms through attacks that are trivial to attackers.

The need for a security mechanism agreement is also supported by the fact that deployment of a large number of SIP-based consumer devices such as 3GPP terminals requires all network devices to be able to accommodate both current and future mechanisms. There is no possibility for instantaneous change since new solutions are coming gradually as new standards and product releases occur. It isn’t even possible to upgrade some of the devices without getting completely new hardware.

The conclusions above are supported by the requirements from 3GPP [2] and discussed in more detail in [5].
This document is an effort to define requirements for secure algorithm agreement used with SIP protocol. The requirements are discussed also in "3GPP Requirements on SIP" [2], but we consider

them to be beneficial also to infrastructures other than 3GPP. Therefore they’ve been separated into this new draft that’s easier to deal with.

The requirements of this document address attacks discussed in chapter 22.1.3 and mechanisms discussed in chapter 22.2 of SIP-draft [1].

5. Definitions

MITM: Man-In-The-Middle

6. Requirements

Some of the built-in SIP security functions like HTTP Digest have alternative algorithms and other parameters. Different algorithms are suitable for different situations. Also, security holes might be found from old algorithms and new algorithms will evolve. Without a secure method to choose between algorithms and their parameters SIP is vulnerable to certain attacks, for example the MITM attack described above and in [5].

>> Req 1: It MUST be possible for a SIP node to select message protection algorithms and parameters within security mechanisms.

Also new security mechanisms will evolve and existing ones, like HTTP Digest or TLS, might be used in parallel depending on the situation. In order to achieve interoperability and backward compatibility, it would be beneficial if a SIP node could choose the security mechanism used.

>> Req 2: A SIP node MAY be able to select a SIP security mechanism among supported alternatives.

The negotiation methods must not be vulnerable to so called Bidding-Down attacks. In such an attack a MITM attacker modifies messages in such a way that parties believe the other side supports weaker security methods than they actually do.

>> Req 3: The negotiation mechanism MUST protect against attackers who do not have access to authentication credentials. In particular, it must not be possible for man-in-the-middle attackers to influence the negotiation result such that services with lower or no security are negotiated.

7. Discussion

Algorithms can be agreed upon with basic SIP features, such as OPTIONS request and Require, Supported headers. They are capable of informing parties about various capabilities including security mechanisms. However, using these features in a straightforward manner does not guarantee the security of the agreement. In their basic form these methods are vulnerable to for example bidding-down attacks. At least some kind of integrity protection for the methods is needed. The method of using Require and Support headers in agreement might imply that the method must be supported in all SIP nodes along the path.

Draft "Security Mechanism Agreement for SIP connections" [5] proposes a secure solution for algorithm agreement. There the security features are represented as regular option tags in SIP. The client announces a list of supported option tags in its first message, and the server returns its selection in the second message. The agreement is secured by simply repeating the client’s original list of option tags in the client’s first protected request (protected with a lower layer protocol). The solution in [5] supports both end-to-end and hop-by-hop agreement in a controllable fashion and without a large increase in roundtrips. This solution requires the SIP servers to store state from previous messages. This is not a problem since where this method is applied security associations have been created, so those SIP servers need to be statefull anyway.

Bidding-down protection is needed between different schemes. It will not be sufficient to do bidding-down protection just for Digest. This is because in SIP [8], only Digest is a MUST. Also in 3GPP, Digest will be applied by most terminals. This implies that a large number, potentially hundreds of millions, of devices support only Digest. Now, assume that some day more than Digest, for example S/MIME or TLS, is wanted. But the large amount of Digest-only devices will probably be in the network for long in the future. The new devices capable of additional security mechanisms could offer to run e.g. TLS, but without protection against bidding-down attacks an attacker could make parties believe that there is old equipment on the other end and TLS is not supported. Therefore TLS would not be used even if both parties support it.

8. Acknowledgments

We would like to thank Allison Mankin, Dean Willis, Rohan Mahy, Bernard Aboba, Miguel Garcia, as well as numerous people at 3GPP SA3 and Ericsson for interesting discussions in this problem space.

9. References

1. Rosenberg, J., et al., "SIP: Session Initiation Protocol", draft-ietf-sip-rfc2543bis-07.txt, February 2002, work in progress.

2. Garcia, M., et al., "3GPP requirements on SIP", draft-garcia-sipping-3gpp-regs-02.txt, November 2001, work in progress.

3. 3GPP TS 23.228: "IP Multimedia (IM) Subsystem (Stage 2) -

Release 5". Version 5.3.0 is available at ftp://ftp.3gpp.org/Specs/2001-12/Rel-5/23_series/23228-530.zip

4. 3GPP TS 24.228: "Signaling flows for the IP Multimedia call control based on SIP and SDP". Version 1.9.0 is available at ftp://ftp.3gpp.org/tsg_cn/WG1_mm-cc-sm/TSGN1_22/Docs/N1-20280_24228-190.zip

5. Arkko, J., et al., "Security Mechanism Agreement for SIP Connections", draft-arkko-sip-sec-agree-00.txt, November 2001, work in progress.

6. Dierks, T., Allen, C., "The TLS Protocol, Version 1.0", RCF 2246, January 1999.

7. Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

8. Rosenberg, J., et al., "SIP:Session Initiation Protocol", draft-ietf-sip-rfc2543bis-05.txt, October 2001, work in progress.

10. Authors' Addresses

Jari Arkko
Oy LM Ericsson Ab
02420 Jorvas
Finland

Phone: +358 40 5079256
EMail: jari.arkko@ericsson.com

Vesa Torvinen
Oy LM Ericsson Ab
Joukahaisenkatu 1
20520 Turku
Finland

Phone: +358 40 7230822
EMail: vesa.torvinen@ericsson.fi

Ilkka Uusitalo
Oy LM Ericsson Ab
Tutkijantie 2C
90570 Oulu
Finland

Phone: +358 40 7245404
EMail: ilkka.uusitalo@ericsson.fi

Full Copyright Statement

Network Working Group J. Arkko
INTERNET-DRAFT V. Torvinen
draft-uusitalo-sipping-delegation-00.txt I. Uusitalo
Expires: August 2002 Ericsson
February 2002

Requirements for Delegation of Message Protection for SIP

Status of this Memo

1. Abstract

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution and multimedia conferences. SIP has a number of security mechanisms used for hop-by-hop or end-to-end message protection. The SIP node handling authentication and initial message protection may decide, for efficiency reasons, to delegate subsequent message protection to another SIP node. In this document we discuss requirements concerning the delegation of message protection for SIP.

2. Conventions used in this document

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 RFC 2119.

3. Table of contents

4. Introduction and Motivation

A SIP node that shares a security context with a user may decide to delegate, according to a policy, further message protection after the initial authentication to another SIP node. This might be necessary due to e.g. re-allocation of clients for capacity reasons, or in order to avoid additional authentication in a multi-hop situation (e.g. via TLS and PKI for the first hop).

An essential part of delegating message protection is the transportation of keys used for message protection. Since the security of a system relies on the secrecy of the keys, care has to be taken to ensure that the keys are transported in a secure manner. For example, it is not recommended to specify a key transport mechanism that relies on underlying security because the application using the keys might not be aware of the security. It is also not recommended to make bundled key transport features into authentication mechanisms without confidentiality protection.

It may also be possible to use Kerberos [5] in SIP in the future. Even though Kerberos tickets are safe as such, the same delegation and key transport features as proposed in this document may be needed. This document assumes that keying material and tickets require the same mechanisms from SIP.

This document is an effort to define requirements applicable for delegation of message protection with SIP protocol. Most of these requirements are listed also in "3GPP Requirements on SIP" [2], but we consider them to be beneficial also to infrastructures other than 3GPP. Therefore they've been separated into this new draft that's easier to deal with.

5. Requirements

A SIP node may decide, according to a policy, to delegate further message protection after the initial authentication to another SIP node. For example, the SIP node delegating further message protection might be a registrar.

>> Req 1. A SIP node MUST be able to send keying material (or tickets) to another SIP node.

Performing authentication on all SIP signaling messages would likely create bottlenecks in the authentication infrastructure. Therefore, a distributed implementation of security functions responsible for authentication may be required in some SIP implementations (e.g. 3GPP).

>> Req 2: It SHOULD be possible to perform an initial authentication based on long-term authentication credentials, followed by subsequent protected signaling that uses short-term authentication credentials.

Secret keys and tickets are of importance to a security of a system and compromising them would be harmful.

>> Req 3. The key transport mechanism MUST protect transferred keys (or tickets) in a secure manner.

SIP can be transported over different underlying protocols, some of which offer security while some don’t. The application using the keys is not necessarily aware of lower layer security deployment. Therefore it is not recommended to specify a key transport mechanism that relies on the security of the underlying layers.

>> Req 4. The key transport mechanism MUST not depend on the security of any underlying layers.

6. Discussion

Currently, SIP does not have secure way to transport keying material or tickets between the SIP nodes. SIP does not include a mechanism for delegation of security tasks either. SIP body (e.g. SDP) can be used to carry keying material to protect subsequent multimedia sessions. It has also been proposed that SIP could be used to carry keys to protect SIP [2]. Similar requirements may be found if other similar security credentials, such as tickets or tokens, are utilized in SIP in the future. For example, the transport of Kerberos tickets [5] between SIP nodes may be required. Even though tickets may be secured by some other means, the same transport and delegation features as proposed in this document may be needed.

The key transport should be specified as an individual function, with its specific headers or bodies used for transporting the keys in SIP.

The reliance to lower-layer security schemes in the transport of the keys is also problematic. Due to the importance of the session keys for the security of the system, the applications should be aware of where they are receiving keys. While some SIP implementations may be able to trust on the underlying network security, a standardized key transport mechanism is likely to find other users as well, and needs to prepare for different network cases. For example, a separate gateway solution is unlikely to provide application layer information about the source of the keys - it can at most guarantee that the keys came from one of the sources trusted by the gateway. In a multi-hop situation, even information provided from an underlying security mechanism may not be very helpful. Therefore, the recommendation is that an application layer mechanism is used to protect key transport. One such mechanism is S/MIME, though also other possibilities such as XML Digital Signatures exist.

Delegation of security tasks should be somehow integrated as a part of key transport. In practice, there should be some way to communicate the purpose for which the transported keys are used.

HTTP authentication framework [6] includes functionality similar to the delegation requirement. HTTP server may be responsible for authenticating data that is situated in another server. This basic delegation mechanism is achieved by using the "opaque" parameter together with sequential 401 unauthorized and 301/302 redirection error messages. The servers do not exchange key material, however the delegating server is able to send delegation-related data to the delegated server in the "opaque" parameter.

7. Acknowledgments

We would like to thank Allison Mankin, Dean Willis, Rohan Mahy, Bernard Aboba, Miguel Garcia, as well as numerous people at 3GPP SA3 and Ericsson for interesting discussions in this problem space.

8. References

1. Rosenberg, J., et al., "SIP:Session Initiation Protocol", draft-ietf-sip-rfc2543bis-05.txt, October 2001, work in progress.

2. Garcia, M., et al., "3GPP requirements on SIP", draft-garcia-sipping-3gpp-regs-02.txt, November 2001, work in progress.

3. 3GPP TS 23.228: "IP Multimedia (IM) Subsystem (Stage 2) - Release 5". Version 5.3.0 is available at ftp://ftp.3gpp.org/Specs/2001-12/Rel-5/23_series/23228-530.zip

4. 3GPP TS 24.228: "Signaling flows for the IP Multimedia call control based on SIP and SDP". Version 1.9.0 is available at ftp://ftp.3gpp.org/Specs/Latest-drafts/24288-190.zip

5. Kohl, J., Neuman, C., " The Kerberos Network Authentication Service (V5)", RCF 1510, September 1993.

6. Franks, J., et al., "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

9. Authors' Addresses

Jari Arkko
Oy LM Ericsson Ab
02420 Jorvas
Finland

Phone: +358 40 5079256
EMail: jari.arkko@ericsson.com

Vesa Torvinen
Oy LM Ericsson Ab
Joukahaisenkatu 1
20520 Turku
Finland

Phone: +358 40 7230822
EMail: vesa.torvinen@ericsson.fi

Ilkka Uusitalo
Oy LM Ericsson Ab
Tutkijantie 2C
90570 Oulu
Finland

Phone: +358 40 7245404
EMail: ilkka.uusitalo@ericsson.fi

Full Copyright Statement