ERICSSON

S3z010128

3GPP SIP Security Requirements for IETF

Jari Arkko

Ericsson

Nice, France

13th-14th September 2001

Background

1. 3GPP has been developing new SIP solutions
2. IETF SIPPING WG requests for requirements before solutions can be discussed
   - Centralised requirements gathering from multiple organisations in order to co-ordinate development and control complexity
3. Only one version of SIP protocol is needed in order to guarantee interoperability and flexible development
4. Follow the principles as defined in RFC 3113

How to proceed?

Two organizations must be able to work on the same thing

Let IETF in to the process sooner

Convince the IETF on the need for standard solutions even for our problems

How to proceed?

"Take requirements written in 3GPP specifications, de-3GPP-fied, IETF-ied, and write them down."

ERICSSON

Work in progress: 3GPP requirements on SIP

- CN1 has initiated an internet draft trying to capture the 3GPP SIP requirements
- IETF prefers all requirements in just one document
  - draft shall also include security requirements
  - (may include pointers to possible solutions if there is agreement that such solutions exists)
- Authors from CN1 including several organizations (Ericsson, Vodafone, Nokia, Siemens, Alcatel, AWS and Motorola)
- New co-authors are welcome!

ERICSSON

SIP Security

- Ericsson has defined preliminary security requirements to the document in order to accelerate the process
- Preliminary work is based on documents
  - 23.228 IP Multimedia (IM) Subsystem - Stage 2
  - 33.203 Access Security for IP-Based Services
  - 33.210 Network Domain Security
  - I-D: SIP security requirements from 3G wireless networks (draft-kroeselberg-sip-3g-security-req-00.txt)
- SA3 comments and contributions required!

IETF-ied Presentation

- Security Model
- Access Domain Security
  - Authentication
  - Scalability and Efficiency
    - Bandwidth and Roundtrips
    - Computation
    - Delegation of Security Tasks
  - Secure negotiation of mechanisms
  - Message protection
- Network Domain Security

Security Model

- MUST provide independent security from the underlying network
- MUST be possible to access the IMS services securely from other accesses
- Each operator acts as its own domain of trust, and shares a long-term security association with its subscribers
- Roaming agreements between operators
- A hop-by-hop model MUST be used to protect actual SIP signaling
- MUST allow separate access domain and network domain solutions

Access Domain Security (1/4)

- Authentication methods
  - MUST use strong, mutual authentication method
  - MUST provide legacy authentication methods
  - MUST support secure storage of long-term authentication keys

Access Domain Security (2/4)

- Scalability and Efficiency
  - bandwidth and roundtrips
    - SHOULD NOT unnecessarily increase the bandwidth needs
    - MUST minimize the number of necessary extra roundtrips
  - computation
    - MUST be possible to provide security without PKI
  - delegation of security tasks
    - MUST be possible to perform an initial authentication, followed by subsequent protected signaling that uses only session keys

Access Domain Security (3/4)

- Secure negotiation of mechanisms
  - MUST be possible to choose among several security services, and select parameters they might need
  - MUST be possible to protect the service and parameter negotiation against attackers

Access Domain Security (4/4)

- Message protection
  - MUST be able to communicate using integrity and replay protection
  - MUST be based on initial authentication
  - MUST be possible using symmetric cryptographic keys
  - MUST be possible to handle also error conditions in a satisfactory manner

Network Domain Security

- MUST provide
  - authentication
  - key agreement
  - integrity
  - replay protection
  - confidentiality
- security associations MUST be independent of the number of network elements

Time plan

- Preferred deadline for SA3 comments and contributions on security requirements during next week
- Submission to SIPPING WG beginning of October
- New security solutions will be developed in IETF SIP Security team and SA3
  - Contribution on both forums needed from the participating companies
- Goal: new SIP security solutions available around April 2002 (two IETF meetings)

Conclusion

- We need access security for Release 5
- We do not want to end-up with two SIP protocols
- N1 has taken the first rapid move to solve the problem
- SA3 contribution required
- In order to continue this path, SA3 support required

Network Working Group
Request for Comments: 3113
Category: Informational

K. Rosenbrock
3GPP PCG Chair
R. Sanmugam
Ericsson
S. Bradner
Harvard University
J. Klensin
AT&T

June 2001

3GPP-IETF Standardization Collaboration

Status of this Memo

Copyright Notice

Abstract

This document describes the standardization collaboration between 3GPP and IETF.

1. Conventions used in this document

This document uses significant terminology that is specialized to IETF, 3GPP, or their areas of work. See Appendix A for definitions of acronyms. The organizational definitions can be found in their respective web-sites.

2. Introduction

This document contains a set of principles and guidelines that serves as the basis for establishing the collaboration between 3GPP and IETF, with the objective of securing timely development of technical specification that facilitate maximum interoperability with existing (fixed and mobile) Internet systems, devices, and protocols.

Each organization will operate according to their own rules and procedures including rules governing IPR policy, specification elaboration, approval and maintenance.

3. Reasons For Collaboration

3.1 3GPP use of IETF Internet Standards

In the further development of 3GPP specifications, the benefit of adopting Internet specifications has been identified.

The preferred 3GPP approach is to use the Internet standards unchanged, if feasible. In any case, 3GPP has no intention to duplicate work performed in IETF.

However, while this document recognizes the importance of 3GPP interoperability with the existing Internet and hence the use of IETF standards, 3GPP recognizes that additions or modifications might be needed in order to make the IETF internet specification fulfill the needs of 3GPP. In such cases, 3GPP will take its concerns directly to the appropriate IETF working groups for resolution, or to an appropriate Area Director if no appropriate working group can be found.

3.2 IETF access to 3GPP Wireless expertise

The technical work in 3GPP is organized in Technical Specification Groups TSGs each with their area of responsibilities. TSG-RAN and TSG-GERAN are responsible for the Radio Access networks based on UTRAN and GERAN and thus the experts in the areas of the characteristics of the physical transport. TSG CN is responsible for the Mobility Management and other core network protocol and functionalities. TSG-T is responsible for Terminal aspects and applications. TSG-SA is responsible for the service and system aspects including the overall architecture, security and O&M aspects. Contacts for the TSGs can be found on the 3GPP web-site http://www.3gpp.org/.

4. Document Sharing

Both 3GPP and IETF encourage the sharing of draft documents that are of mutual interest.

3GPP documents are available on its official web-site (http://www.3gpp.org/) and is open to anyone. IETF documents, including preliminary working documents ("Internet Drafts") are available on its web-site (http://www.ietf.org/) and various shadow sites.

IETF representatives can obtain information about the 3GPP document and web-site structures by contacting the relevant 3GPP contact points indicated at the 3GPP web-site http://www.3gpp.org/.

3GPP representatives can obtain information about the IETF document and web-site structures by contacting the relevant IETF contact points (the Area Directors indicated at the IETF web-site http://www.ietf.org/).

5. Communication

Whenever possible, informal communication at working level is encouraged.

The vast majority of the technical discussions and decision making in both IETF and 3GPP is done over mailing lists. Both 3GPP and IETF web sites contain information concerning the associated mailing lists.

It is recommended that interested individuals subscribe to and participate in these lists.

When deemed necessary, formal communication between 3GPP and IETF is also permitted. Relevant IETF Area Directors and 3GPP technical leadership are encouraged and authorized to facilitate such communications when needed.

6. Rapporteurs/coordinators

6.1 IETF coordination support in 3GPP

An IETF rapporteur function is established in 3GPP TSG-SA.

The individual(s) appointed to undertake the responsibility of this function should be the initial contact point in 3GPP for matters pertaining to the 3GPP-IETF cooperation. Of course, the chairman of TSG-SA can always be contacted.

The 3GPP-IETF rapporteur function, therefore, is expected to work with the concerned working groups and TSGs and support the interaction between 3GPP and IETF.

6.2 3GPP Liaison in IETF

The preferred way for organizations to work with IETF is through the working groups. However, IETF has a limited number of liaison relationships with other organizations when conditions warrant the appointment of a specific person.

The appointment, by the IAB, of a specific person to function as a "3GPP liaison" is proposed.

The role of the 3GPP Liaison is to act as an initial contact point in IETF for administrative aspects of this collaboration that cannot easily be handled in other ways (e.g., at a technical level by interactions with IETF Working Groups or Area Directors). It is agreed that the role does not carry the expectation of attendance at 3GPP meetings or participation in 3GPP administrative processes and anticipated that all liaison efforts assigned to this individual will be carried out by electronic mail. It is understood that the liaison will not have the ability to make exceptions to, or special provisions for, IETF policies and procedures.

9. Participation

In order to assist the information flow between the organizations, the IETF can on per case basis appoint a rapporteur to participate and represent IETF at 3GPP technical meetings.

IETF meetings are open to any interested individuals.

3GPP partners (OPs, MRPs) or individual members can participate in any of the IETF meetings, in accordance with the existing IETF procedures.

8. Security Considerations

This type of non-protocol document does not directly affect the security of the Internet.

9. Authors' Addresses

Questions about this memo can be directed to:

Karl Heinz Rosenbrock
ETSI
06921 Sophia Antipolis
CEDEX
France

Phone: +33 492 94 4212
EMail: rosenbrock@etsi.fr

Raj Sanmugam
Director, Systems and Technology
Ericsson Canada Inc.
8400 Decarie Blvd
TMR, Quebec
H4P 2N2

Phone: +1 514 345 7862
Email: Raj.Sanmugam@ericsson.ca

Scott Bradner
Harvard University
Cambridge, MA 02138
USA

Phone: +1 617 495 3864
EMail: sob@harvard.edu

John C. Klensin
AT&T Labs
99 Bedford St
Boston, MA 02111
USA

Phone: +1 617 513 7285
EMail: Klensin+iab@jck.com

Note: Changes to the contents of this memo requires the approval from 3GPP PCG: EMail: 3GPPContact@etsi.fr

Appendix A: Acronyms

Glossary Of Acronyms:

3GPP	Third Generation Partnership Project
BCP	Best Current Practice
IAB	Internet Architecture Board
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IPR	Intellectual Property rights
MRP	Market Representation Partner
OP	Organizational Partner
O&M	Operation and Maintenance
PCG	Project coordination Group
RFC	Request for Comments
TSG	Technical Specification Group
TSG-SA	TSG Services and systems aspects
TSG-CN	TSG Core Network
TSG-RAN	TSG Radio Access Network
TSG-GERAN	TSG GSM Radio Access Network
TSG-T	TSG Terminals
UTRAN	Universal Terrestrial Radio Access Network
WWW	World Wide Web

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.