

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3201

(10/2007)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN –
Signalling and control requirements and protocols to
support attachment in NGN environments

EAP-based security signalling protocol architecture for network attachment

ITU-T Recommendation Q.3201



International
Telecommunication
Union

Documents
Document Sharing Hub

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3999
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	Q.3600–Q.3649
NGN applications	Q.3700–Q.3849
Testing for NGN networks	Q.3900–Q.3999

For further details, please refer to the list of ITU-T Recommendations.

11/11/2007 10:11:11 AM

ITU-T Recommendation Q.3201

EAP-based security signalling protocol architecture for network attachment

Summary

ITU-T Recommendation Q.3201 describes the security signalling requirements and protocol architecture for supporting access security aspects of network attachment procedure in a next generation network (NGN). Basic threats and security requirements for the attachment of NGN access networks are analysed, and a model of an extensible authentication protocol (EAP)-based security signalling protocol architecture accommodating heterogeneous multi-links in the next generation network access environment is presented. Based on it, three feasible scenarios for authentication signalling in NGN network attachment control functions are developed.

Source

ITU-T Recommendation Q.3201 was approved on 29 October 2007 by ITU-T Study Group 11 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2008

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

	Page
1 Scope	1
1.1 Relationship	1
2 References.....	1
3 Abbreviations.....	2
4 Threats on access networks	3
5 Conventions	4
6 Security requirements for access networks.....	4
7 Signalling protocol architecture for authentication	5
7.1 Basic authentication model.....	7
7.2 EAP-based authentication architecture in access networks.....	8
7.3 EAP authentication model	9
7.4 Integrated authentication model in NGN	9
7.5 Authentication scenarios based on network architecture	10
Bibliography.....	14

Document Sharing Hub

ITU-T Recommendation Q.3201

EAP-based security signalling protocol architecture for network attachment

1 Scope

This Recommendation provides the basic security framework protocol architecture to support network attachment in NGN environments. This Recommendation also provides some threats and security requirements related to the signalling and control for network attachment.

The goal of this Recommendation is to identify security requirements for access networks and to define an EAP-based security protocol architecture for network access attachment. The main focus of this Recommendation is on an EAP-based security signalling protocol architecture for authentication and authorization in the network attachment system of NGN.

This Recommendation incorporates the overall context of related standards, on the issue of network security protocol, from IETF, IEEE and ITU-T.

1.1 Relationship

Work for this Recommendation is based upon the context of [ITU-T Y.2701] and [ITU-T Y.2012]; this Recommendation complies with the security requirements and guidelines specified in [ITU-T Y.2701], and considers the compatibility with the functional architecture in [ITU-T Y.2012].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- | | |
|-----------------|--|
| [ITU-T Y.2012] | ITU-T Recommendation Y.2012 (2006), <i>Functional requirements and architecture of the NGN release 1</i> . |
| [ITU-T Y.2701] | ITU-T Recommendation Y.2701 (2007), <i>Security requirements for NGN release 1</i> . |
| [IETF RFC 2865] | IETF RFC 2865 (2000), <i>Remote Authentication Dial In User Service (RADIUS)</i> .
< http://www.ietf.org/rfc/rfc2865.txt > |
| [IETF RFC 2989] | IETF RFC 2989 (2000), <i>Criteria for Evaluating AAA Protocols for Network Access</i> .
< http://www.ietf.org/rfc/rfc2989.txt > |
| [IETF RFC 3127] | IETF RFC 3127 (2001), <i>Authentication, Authorization, and Accounting: Protocol Evaluation</i> .
< http://www.ietf.org/rfc/rfc3127.txt > |
| [IETF RFC 3588] | IETF RFC 3588 (2003), <i>Diameter Base Protocol</i> .
< http://www.ietf.org/rfc/rfc3588.txt > |