

ICS 33.040.40
CCS M 33



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 21643-2008

IP Authentication Header

IP认证头(AH)

(English Translation)

Issued on: April 10, 2008

Implemented on: November 1, 2008

Issued by: Standardization Administration of China

Table of Contents

Preface	
1 Scope	
2 Normative references	
3 Abbreviations	
Overview 4	
5 AH protocol header format	
6 AH protocol processing	
6.1 Positioning	
6.2 Authentication Algorithm	
6.3 Out packet processing	
6.4 Into the packet processing	
Conformance Requirements 6	

Foreword

This standard is one (IPSec) IP Security protocol standard series, the series of standards is expected to name and structure as follows.

--- National standard "IP Security Protocol Architecture" (IETF RFC2401.1998, MOD) 1)

--- GB/T 21643-2008 "IP Authentication Header (AH)" (IETF RFC2402.1998, MOD)

--- National standard "IP Encapsulating Security Payload (ESP)" (IETF RFC2406.1998, MOD) 1)

--- YD/T 1466-2006 "IP Security Protocol (IPSec) technical requirements"

--- YD/T 1467-2006 "IP Security Protocol (IPSec) Test Method"

--- YD/T 1468-2006 "IP Security Protocol (IPSec) through Network Address Translation (NAT) technical requirements"

--- Industry standards (YD) "Internet Key Exchange (IKEv2) - Part 1. Technical requirements" 1)

--- Industry standards (YD) "Internet Key Exchange (IKEv2) Part 2. Test methods" 1) this revised standard adopts IETF RFC2402.1998 "IP Authentication Header (AH)", with the main difference compared are.

--- Remove the RFC2402 in Chapter 4, Chapter 6, Section 7 and Appendix A of the

content.

--- The RFC2402 in Chapter 1, Section 2, Clause 3 and Chapter 5 of the present standard, Chapter 4, Chapter 5, Chapter 6 and Chapter 7.

--- According to GB/T 1 series standards, increasing the standard of the first chapters, Chapter 2 and Chapter 3.

The standard proposed by the People's Republic of China Ministry of Information Industry.

The standard by the China Communications Standards Association.

This standard was drafted. Ministry of Information Industry Telecommunications Research Institute.

Drafters of this standard. Yuan Qi, Baohong.

1) to be released.

IP Authentication Header (AH)

1 Scope

This standard specifies the technical requirements for the AH protocol, including the AH protocol header format, AH protocol processing, consistency requirements.

This standard applies to support AH protocol data devices.

2 Normative references

The following documents contain provisions which, through reference in this standard and become the standard terms. For dated references, subsequent Amendments (not including errata content) or revisions do not apply to this standard, however, encourage the parties to the agreement are based on research Whether the latest versions of these documents. For undated reference documents, the latest versions apply to this standard.

IETF RFC2401.1998 IP Security Protocol Architecture IETF RFC2406.1998 IP Encapsulating Security Payload (ESP) IETF RFC1883.1995 IPv6 protocol IETF RFC2403.1998 ESP and AH use of HMAC algorithm MD5-96 IETF RFC2404.1998 ESP and AH use of HMAC SHA-1-96 algorithm

3 Abbreviations

The following abbreviations apply to this standard.

AH AuthenticationHeader Authentication Header Data Encryption Standard DES
DataEncryptionStandard Encapsulating Security Payload ESP
EncapsulatingSecurityPayload HMAC HASH MAC hash MAC IANA

InternetAssignedNumbersAuthority Internet Assigned Numbers Authority ICMP
InternetControlMessageProtocol Internet Control Message Protocol Integrity Check Value
ICV IntegrityCheckValue IPsec IP Security IP Security IP InternetProtocol Internet Protocol
Message Digest 5 MD5 MessageDigest5 SA SecurityAssociation SA SHA-1
SecureHashAlgorithm-1 Secure Hash Algorithm -1 SPI SecurityParameterIndex security
parameter index Transmission Control Protocol TCP TransmissionControlProtocol Type of
Service TOS TypeofService User Datagram Protocol UDP UserDatagramProtocol

4 Overview

AH provides connectionless IP packet integrity, data origin authentication and anti-replay protection. Anti-replay protection is optional and determined by the recipient Set whether to use. When creating a security association, it requires the sender to increment the serial number for anti-replay protection only if the receiver checks the sequence no, the service is valid.

AH provides authentication possible for the IP header and upper layer protocols. Some IP header fields may change in transit, when the IP packet arrives at the receiver