GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GM/T 0022-2023

Replacing GM/T 0022-2014

IPSec VPN Technical Specification

IPSec VPN 技术规范

Issued on: December 4, 2023 **Implemented on: June 1, 2024**

Issued by: State Cryptography Administration

Table of Contents

IPSec VPN Technical Specification

1 Scope

This document specifies the technical protocols and product functions of IPSec VPN, including the key exchange protocol and security message protocol, as well as product functional requirements and security management requirements.

This document applies to the development, testing, use and management of IPSec VPN products.

2 Normative References

The contents of the following documents constitute indispensable clauses of this document through the normative references in the text. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 20518-2018 Information Security Technology - Public Key Infrastructure - Digital Certificate Format

GB/T 32905-2016 Information Security Techniques - SM3 Cryptographic Hash Algorithm

GB/T 32907-2016 Information Security Technology - SM4 Block Cipher Algorithm

GB/T 35276-2017 Information Security Technology - SM2 Cryptographic Algorithm Usage Specification

GB/T 36624-2018 Information Technology - Security Techniques - Authenticated Encryption

GM/T 0005-2021 Randomness Test Specification

GM/T 0016 Smart Token Cryptography Application Interface Specification

GM/T 0062-2018 Random Number Test Requirements for Cryptographic Modules

GM/T 0092-2020 Specification of Certificate Request Syntax Based on SM2 Cryptographic Algorithm

GM/Z 4001 Cryptology Terminology

RFC 2408 Internet Security Association and Key Management Protocol

RFC 3947 Negotiation of NAT-traversal in the IKE

RFC 3948 UDP Encapsulation of IPSec ESP Packets

RFC 4304 Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for ISAKMP

3 Terms and Definitions

The terms and definitions defined in GM/Z 4001 and the following are applicable to this document.

3.1 security association

An agreement that is established through negotiation between two communicating entities.

NOTE 1: it describes how the entities utilize security services for secure communication.

NOTE 2: security association includes all information required to execute various network security services, such as IP layer services (such as header authentication and payload encapsulation), transport layer and application layer services, or self-protection of negotiated communications.

3.2 payload

The data format of messages exchanged between ISAKMP communicating parties.

NOTE: the payload is the basic unit of ISAKMP message construction.

3.3 authentication header

An IPSec protocol that is used to provide the functions of data integrity, data origin authentication and anti-replay attack for IP data packets, but it does not provide the function of data confidentiality.

3.4 encapsulating security payload

An IPSec protocol that is used to provide the functions of confidentiality, data integrity, data origin authentication and anti-replay attack for IP data packets.

3.5 data origin authentication

A mechanism that confirms that received data is the source claimed.

3.6 authenticated encryption mechanism

The cryptographic technology that is used to protect data confidentiality and provide data integrity and data origin authentication.

NOTE: it includes both encryption and decryption.

[source: GB/T 36624-2018, 3.2, modified]

3.7 virtual private network

Use cryptographic technology to establish a secure channel within a communication network.

3.8 IPSec implementation

Software and hardware products that specifically implement the IPSec VPN protocol.

NOTE: IPSec implementation includes hardware products in a hardware-software-integrated form, as well as IPsec VPN products implemented purely by software (for example, IPsec VPN products in a virtual machine or container form).

4 Symbols and Abbreviations

4.1 Symbols

The following symbols apply to this document.

HDR: an ISAKMP header.

HDR*: indicates that the payload following the ISAKMP header is encrypted.

SA: security association payload with one or multiple proposal payloads.

IDi: initiator’s identification payload.

IDr: responder’s identification payload.

HASHi: initiator’s hash payload.

HASHr: responder’s hash payload.

HASH_<n>: intermediate hash data used in the negotiation interaction between two parties.

SIGi: initiator’s signature payload.

SIGr: responder’s signature payload.

CERT_sig_r: signature certificate payload.

CERT_enc_r: encryption certificate payload.

Ni: initiator’s nonce payload.

Nr: responder’s nonce payload.

<p>_b: the body of payload[1)] <p>.

[1)] Including the payload without the ISAKMP generic header.

VPN: Virtual Private Network

5 Cryptographic Algorithms and Key Categories

5.1 Cryptographic Algorithms

The asymmetric cryptographic algorithm, symmetric cryptographic algorithm, cryptographic hash algorithm and random number generation algorithm used in IPSec VPN shall comply with the relevant requirements of national and industry cryptographic standards. The various algorithms and their usage requirements are as follows:

a) The asymmetric cryptographic algorithm shall support the SM2 elliptic curve cryptography algorithm for entity authentication, digital signature and digital envelope.

b) The symmetric cryptographic algorithm shall support the SM4 block cipher algorithm for encryption and protection of key exchange data and message data. The algorithm shall operate in either CBC or GCM mode. The use of the SM4 algorithm shall comply with GB/T 32907-2016. The use of the GCM mode shall comply with mechanism 5 of GB/T 36624-2018.

c) The cryptographic hash algorithm shall support the SM3 cryptographic hash algorithm for integrity check. The use of the SM3 algorithm shall comply with GB/T 32905-2016.

d) Random numbers generated by the random number generation algorithm shall comply with the requirements of GM/T 0005-2021 and the provisions of GM/T 0062-2018 for Class E products.

5.2 Key Categories

IPSec VPN uses the following key categories.

a) Device key: public and private key pairs used by asymmetric algorithm, including signature key pairs and encryption key pairs, used for entity authentication, digital signature and digital envelope.

NOTE: the devices include both hardware-implemented products (for example, hardware-software-integrated products) and purely software-implemented products (for example, virtual machine form products).

b) Work key: the key obtained in the first phase of key exchange, used to protect the session key exchange process.

c) Session key: the key obtained in the second phase of key exchange, used for the encryption and integrity check of data message.

6 Protocols

6.1 Key Exchange Protocol

6.1.1 Definitions of related functions

Asymmetric_Encrypt (msg, pub_key): use the asymmetric algorithm Asymmetric, with pub_key as the key to encrypt the input message msg_b, and its output is the concatenation of the generic payload header and ciphertext of msg. For example, SM2_Encrypt (Ski, pub_key) indicates the use of SM2 algorithm to encrypt Ski_b by using the public key pub_key, and its output is the concatenation of the generic payload header and ciphertext of Ski.

Asymmetric_Sign (msg, priv_key): use the asymmetric algorithm Asymmetric, with priv_key as the key to digitally sign msg.

Symmetric_Encrypt (msg, key): use the symmetric encryption algorithm Symmetric, with key as the key to encrypt the input message msg_b, and its output is the concatenation of the generic payload header and ciphertext of msg. For example, SM4_Encrypt (Ni, key) indicates the use of SM4 algorithm to encrypt Ni_b by using key as the key, and its output is the concatenation of the generic payload header and ciphertext of Ni.

HASH (msg): use the cryptographic hash algorithm to perform a data digest operation on msg. The hash function calculates a fixed-length value. If the SM3 cryptographic hash algorithm is used to calculate the data digest of msg, then, a 256-bit hash value is calculated.

PRF (key, msg): use the key “key” to perform a data digest operation on the message msg. The calculation result is a fixed-length value. The PRF is calculated as follows:

PRF (key, msg) = HMAC (key, msg), in which, HMAC is implemented based on SM3.

6.1.2 Exchange phase and mode

6.1.2.1 Exchange phase

The key exchange protocol defines the process and message format for negotiating, establishing, altering and deleting security associations. Protocol messages shall be transmitted using UDP protocol port 500 or 4500.

The key exchange protocol consists of two phases: Phase 1 and Phase 2.

In the Phase 1 exchange, the communicating parties establish an ISAKMP security association. This security association is the shared policy and key used by the negotiating parties to protect their communications. This security association is used to protect the IPSec security association negotiation process. A single ISAKMP security association can be used to establish multiple IPSec security associations.

In the Phase 2 exchange, the communicating parties use the ISAKMP security association of

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------