GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GM/T 0026-2023

Replacing GM/T 0026-2014

Security authentication gateway product specification

安全认证网关产品规范

Issued on: December 04, 2023 **Implemented on: June 01, 2024**

Issued by: State Cryptography Administration

Table of Contents

Security authentication gateway product specification

1 Scope

This document specifies the cryptographic algorithms and key types, product requirements, product testing and qualification determination for security authentication gateways.

This document is used for the development, testing, use and management of security authentication gateway products.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the version corresponding to that date is applicable to this document; for undated references, the latest version (including all amendments) is applicable to this document.

GB/T 9813.3, General specification for computer - Part 3: Server

GB/T 15153.1, Telecontrol equipment and systems - Part 2: Operating conditions - Section 1: Power supply and electromagnetic compatibility

GB/T 15843.3, Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques

GB/T 17964, Information security technology - Modes of operation for a block cipher

GB/T 25069, Information security techniques - Terminology

GB/T 36624-2018, Information technology - Security techniques - Authenticated encryption

GM/T 0005, Randomness test specification

GM/T 0022, IPSec VPN technical specification

GM/T 0023, IPSec VPN gateway product specification

GM/T 0024, SSL VPN specification

GM/T 0025, SSL VPN gateway product specification

GM/T 0028, Security requirements for cryptographic modules

GM/T 0050, Cryptography Device Management - Specification of Device Management Technology

GM/T 0062, Random number test requirements for cryptographic modules

GM/T 0068, Open third party resource authorization protocol framework

GM/T 0069, Open identity authentication framework

GM/Z 4001, Cryptology terminology

3 Terms and definitions

For the purposes of this document, the terms and definitions given in GB/T 25069 and GM/Z 4001 apply.

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

AH: Authentication Header

CBC: Cipher Block Chaining

ESP: Encapsulate Security Payload

GCM: Galois Counter Mode

IPSec: Internet Protocol Security

NAT: Network Address Translation

SSL: Secure Sockets Layer

TLCP: Transport Layer Cryptography Protocol

VPN: Virtual Private Network

5 Deployment modes

A security authentication gateway is a product that uses digital certificates to provide user management, identity authentication, single sign-on, transmission encryption, access control, and information auditing services for application systems. The security authentication gateway uses digital certificate technology for identification. The deployment modes of security authentication gateways are divided into two types: series and parallel.

a) Series: From a network topology perspective, users must go through a gateway to access protected applications.

b) Parallel: From a network topology perspective, users can access protected applications without going through a gateway. The application or firewall can perform some logical judgment to identify users who access the application without going through the gateway (for example, by source IP), thereby achieving a logical series effect.

The security authentication gateway shall at least support the serial deployment mode. At the same time, taking into account the needs of actual conditions, the security authentication gateway shall be able to support parallel deployment in addition to the serial deployment mode, but it shall provide the application with technical means to identify whether the user accesses the application through the gateway.

6 Cryptographic algorithms and key types

6.1 Algorithm requirements

The asymmetric cryptographic algorithms, symmetric cryptographic algorithms, cryptographic hash algorithms, and random number generation algorithms used by the security authentication gateway shall comply with the relevant requirements of national cryptographic standards and industry standards. The algorithms and usage methods are as follows.

a) Asymmetric cryptographic algorithms are used for authentication, digital signatures, and digital envelopes.

b) The symmetric encryption algorithm uses a block cipher algorithm for encryption protection of key exchange data and message data. The algorithm works in GCM mode or CBC mode. GCM shall comply with GB/T 36624, and CBC shall comply with GB/T 17964.

c) Cryptographic hashing algorithms are used for symmetric key generation, integrity verification and digital signatures.

d) The random number generation algorithm is used to generate random numbers that meet the testing requirements of GM/T 0005.

6.2 Key types

For security authentication gateways that comply with the IPSec protocol, the key type shall comply with GM/T 0022; for security authentication gateways that comply with the TLCP protocol, the key type shall comply with GM/T 0024.

7 Security authentication gateway product requirements

7.1 Product functional requirements

7.1.1 User management

The security authentication gateway shall be able to manage access users:

a) The gateway shall be able to add, delete, modify and query relevant users who need to access the system;

b) The gateway shall be able to synchronize certificate user information from other identity management systems (such as CA, RA);

c) The gateway shall be able to group users into roles to a certain extent, or manage them according to organizational structures.

7.1.2 Identity authentication

The security authentication gateway shall provide a digital certificate-based method to authenticate the end user's identity, and the identity authentication protocol shall comply with GB/T 15843.3. When the security authentication gateway uses proxy mode:

For security authentication gateways that comply with the IPSec protocol, the end user's certificate and signature shall be authenticated during the IKE negotiation phase, and a Certificate Revocation List (CRL) shall be checked.

For security authentication gateways that comply with the TLCP protocol, the end user's certificate and signature shall be authenticated during each TLCP handshake, and a Certificate Revocation List (CRL) shall be checked.

When the security authentication gateway uses the call mode, the gateway shall authenticate the end user's certificate and signature when it is called, and check the Certificate Revocation List (CRL).

Under the conditions supported by external environment (OCSP verification, or real-time certificate status verification based on other interfaces provided by the CA), the gateway should support real-time certificate status verification.

7.1.3 Application management

Security authentication gateway products shall be able to manage applications that need to be protected and be able to add, delete, modify and query application information. Application information shall include the application address, which can be divided into three categories:

a) Network segment: Identified by network address + mask, for example, 192.168.1.0/24;

b) TCP/UDP applications: Identified by protocol (TCP/UDP) and port number, for example, tcp://192.168.3.6:25/ or udp://192.168.1.9:53/;

c) WEB application: Identified by protocol (HTTP/HTTPS), domain name, port number and WEB path, such as http://www.site.com:8080/myapp or https://www.securesite.com/mysecure.

7.1.4 Access control

Based on user management and application management information, the gateway defines the permissions for applications that users can access.

a) Control access to an application based on individual users or user group (role) definitions.

b) The access rights are configured in whitelist or blacklist mode.

c) If a mixed blacklist and whitelist approach is used (e.g., a user can access the application as role A, but is prohibited from accessing the application as role B), a method for sorting permission priorities shall be provided.

7.1.5 Single sign-on

When a user accesses multiple applications protected by the same gateway, there shall only be one identity authentication process. The identification process should comply with GM/T 0068 and GM/T 0069.

7.1.6 Information audit

Security authentication gateway products shall have information auditing functions that can record user access to the system in detail. The recorded information should include but is not limited to: time, user IP, user certificate information, event type, access resources, upload traffic, download traffic, access results, error reasons, success and failure indicators.

7.1.7 Random number generation

The security authentication gateway shall have an independent random number generation function.

7.1.8 Operation mode

The operation mode of security authentication gateway products that comply with the IPSec protocol shall comply with GM/T 0022. The operation mode of security

authentication gateway products that comply with the TLCP protocol shall comply with GM/T 0024.

7.1.9 Key exchange

Security authentication gateway products shall have key exchange functions to generate working keys and session keys through negotiation.

a) Key exchange using the IPSEC protocol shall comply with GM/T 0022, and using the TLCP protocol shall comply with GM/T 0024.

b) The working key and session key generated by key exchange shall be reset to zero each time the security authentication gateway is started.

7.1.10 Transmission of secure messages

Security authentication gateway products shall have secure message transmission functions to ensure the secure transmission of data.

7.1.11 Key update

Security authentication gateway products shall have the function of updating keys based on two conditions: time period and message flow. Among them, key updating based on time period conditions is a required function, and key updating based on message flow conditions is an optional function.

For security authentication gateways that comply with the IPSec protocol, the maximum update period for the working key shall not exceed 24 hours, and the maximum update period for the session key shall not exceed 1 hour.

For security authentication gateways that comply with the TLCP protocol, the maximum update period for the working key in client-server mode shall not exceed 8 hours; and the maximum update period for the working key in gateway-gateway mode shall not exceed 1 hour.

7.1.12 NAT traversal

For security authentication gateway products that comply with the IPSec protocol, NAT traversal is a necessary test. For the specific test process, see the functional requirements for NAT traversal in GM/T 0023.

7.1.13 Anti-replay attack

The security authentication gateway shall have the function of resisting replay attacks during the secure message transmission stage.

7.1.14 Packet filtering

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

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