GM

CRYPTOGRAPHIC INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

Reference No.: 44626-2014

GM/T 0025-2014

SSL VPN gateway product specification

SSL VPN 网关产品规范

Issued on: February 13, 2014 **Implemented on: February 13, 2014**

Issued by: State Cryptography Administration

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. The issuing authority shall not be held responsible for identifying any or all such patent rights.

This Standard was proposed by and shall be under the jurisdiction of Cryptography Industry Standardization Technical Committee.

Main drafting organizations of this Standard: Shanghai Geer Software Co., Ltd., Wuxi Jiangnan Information Security Engineering Technology Center, Shandong Dean Computer Technology Co., Ltd., Chengdu Guardian Information Industry Co., Ltd., Shanghai Digital Certificate Certification Center Co., Ltd., Xingtang Communication Technology Co., Ltd., Beijing Digital Certified Co., Ltd.

Main drafters of this Standard: Tan Wuzheng, Kong Fanyu, Li Yuanzheng, Liu Cheng, Li Shusheng, Wang Nina, Han Lin.

SSL VPN gateway product specification

1 Scope

This Standard specifies the functional requirements, hardware requirements, software requirements, safety requirements and inspection requirements of SSL VPN gateway products.

This Standard is applicable to guide the development, inspection, use and management of SSL VPN gateway products.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 9813-2000, *Generic specification for microcomputers*

GB/T 15153.1-1998, *Telecontrol equipment and systems -- Part 2: Operating conditions Section 1 Power supply and electromagnetic compatibility*

GB/T 17964, *Information technology - Security Techniques - Modes of operation for a block cipher*

GM/T 0005, *Randomness testing specification*

GM/T 0014, *Digital Certificate Authentication System Password Protocol Specification*

GM/T 0015, *Digital certificate format specification based on SM2 kiln code algorithm*

GM/T 0024, *SSL VPN technical specification*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

The following terms and definitions apply to this document.

3.1.1 cryptographic algorithm

calculation rules of cryptography processing

3.1.2 cryptographic hash algorithm

It is also known as hash algorithm, cryptographic hash algorithm or hash algorithm; this algorithm maps an arbitrary long bit string to a fixed long bit string and satisfies the following three characteristics:

(1) it is computationally difficult to find an input that can be mapped to the output for a given output;

(2) finding another input that can be mapped to the same output for a given input is computationally difficult;

(3) it is computationally difficult to find that different inputs mapped to the same output.

3.1.3 asymmetric cryptographic algorithm / public key cryptographic algorithm

cryptographic algorithm for different keys used by encryption and decryption; one of the keys (public key) can be public, another key (private key) must be kept secret, and the calculation for the private key by the public key is not feasible.

3.1.4 symmetric cryptographic algorithm

cryptographic algorithm of same keys used by encryption and decryption.

3.1.5 block cipher algorithm

a class of symmetric cipher algorithm for dividing the input data into fixed-length packets for encryption and decryption

3.1.6 cipher block chaining operation mode; CBC

a working mode of block cipher algorithm of which the characteristics is that the current cipher text grouping is obtained by the current plaintext grouping is grouped with the previous cipher text via XOR operation and encryption

3.1.7 initialization vector / initialization value; IV

initial data used for data transformation and introduced to increase security or synchronize cryptographic devices during cryptography conversion

3.1.8 digital certificate

It is also known as public key certificate; a data structure containing public key owner information, public key, issuer information, expiration date, and extended information signed by certificate authority; it can be divided into personal certificate, institutional certificate and equipment certificate according to category OR signature certificate and encryption certificate according to use

3.1.9 secure sockets layer protocol; SSL

a transport layer security protocol used to build a safe passage between client and server

3.1.10 virtual private network; VPN

a technology of using cryptographic technique to build a safe passage in the communication network

3.1.11 SM2 algorithm

an elliptic curve public key cryptography algorithm with a key length of 256 bits

3.2 Abbreviations

The following abbreviations apply to this document.

CBC: Cipher Block Chaining

IV: Initialization Vector

SSL: Secure Sockets Layer

VPN: Virtual Private Network

4 Cryptographic algorithm and key type

4.1 Algorithm requirements

SSL VPN uses asymmetric cryptographic algorithm, symmetric cryptographic algorithm, cryptographic hash algorithm, random number generation algorithm approved by state code management department. Algorithm and use are as follows:

- asymmetric cryptographic algorithm is used for authentication, digital signatures and digital envelopes, etc.;
- symmetric cryptographic algorithm uses block cipher algorithm used for encryption protection of key exchange data and encryption protection of

5 SSL VPN gateway products requirements

5.1 Product functional requirements

5.1.1 Random number generation

SSL VPN gateway products shall have random number generation. The random number should be generated by multiple hardware noise sources.

5.1.2 Work mode

SSL VPN gateway products work mode is divided into client-server mode and gateway-gateway mode. The client-server mode is a prerequisite mode while the gateway-gateway mode is optional.

5.1.3 Key exchange

SSL VPN gateway products shall have key exchange function to generate a work key by negotiation.

Key exchange shall be carried out according to the requirements of GM/T 0024.

5.1.4 Secure packet transmission

SSL VPN gateway products shall have secure packet transmission function to endure secure transmission of data.

Secure packet transmission shall be in accordance with requirements of GM/T 0024.

5.1.5 Identification

SSL VPN gateway products shall have the function of entity authentication. The identification method uses digital certificate. Digital certificate format shall meet requirements of GM/T 0015. The identification of the server is a prerequisite function, and the identification of the client is optional. It shall support digital certificate (RSA or SM2) or supervision mechanism based on identification algorithm. Any identification method shall ensure the completeness and effectiveness of identification.

5.1.6 Access control

SSL VPN gateway products shall have fine-grain access control function, based on effective control of user or user group on resources. At least the network access should be controlled to IP addresses, ports and protocols. The access to the web resource should be controlled at least to the URL and

5.2 Product performance parameters

5.2.1 Maximum number of concurrent users

It refers to the maximum number of simultaneously online users. This indicator reflects the maximum number of users who can deliver the product at the same time.

5.2.2 Maximum number of concurrent connections

It refers to the maximum number of simultaneously online SSL connections. This indicator reflects the maximum number of SSL connections of which a product can handle at the same time.

5.2.3 Number of new connections per second

The maximum number of SSL connections that can be created per second. This indicator reflects the ability of the product to access new SSL connections per second.

5.2.4 Throughput rate

In the case of packet loss rate of 0, the bidirectional data maximum flow reached by server products on internal network port

5.3 Security requirements

5.3.1 Key security

5.3.1.1 Server end key

The server end signing key pair is generated by the SSL VPN gateway product itself. Its public key should be exported. A signature certificate is issued by an external certification authority.

The server encryption key pair is generated by an external key authority and is issued by an external authentication authority. See GM/T 0014 for private key protection method of encryption key pair.

The private keys of the signing certificate, the encryption certificate, and the encryption key pair should be imported into the SSL VPN gateway products.

In SSL VPN gateway products, the private key of the server key should have security protection.

The server key should be updated according to the set security policy.

The server key can be backed up safely and can be recovered when needed.

5.3.3 Management security

5.3.3.1 Minimal management

The administrators include the system administrator, the security administrator, and the audit administrator. These three types of administrators decentralize the system. The system administrator is responsible for the management and maintenance of the software environment as well as the system backup and operating system recovery.

The system auditor is responsible for the security audit of the logs in the system.

The security administrator is responsible for management operations such as service configuration, application management, and authorization management.

5.3.3.2 Administrator login security

Administrators use digital certificate authentication and manage SSL VPN gateways through encrypted channels. The administrator can only log in to the SSL VPN gateway through the authorized terminal to carry on the corresponding configuration operation.

5.4 Management requirements

5.4.1 Log management

The SSL VPN gateway products should provide logging, viewing, and export functions. The SSL VPN gateway product client does not require log management.

The log content includes:

- administrator operations, including user management, login authentication, system configuration, key management, etc.;
- user access behaviors, including user, time, access to resources, results, etc.;
- abnormal events, including authentication failure, illegal access and records of other unusual events.

The log format includes the date and time the event occurred, the subject identity, and the event content.

5.4.2 Administrator management

SSL VPN server products shall set up administrator, for system configuration,

software function module correctness are optional. When inspection fails, it shall alarm and stop working.

5.4.4 Hardware requirements

5.4.4.1 External interface

SSL VPN gateway products should have working network port and management interface. The management interface shall include the local maintenance interface and the remote management interface, and may communicate with the same port or serial port. Work network port should have at least two, respectively, for the internal network interface and external network interface.

5.4.4.2 Encryption parts

SSL VPN gateway products should use the encryption chip or encryption card approved by the state cryptography management department as the main encryption components.

5.4.4.3 Random number generator

The random number generator uses the physical noise source approved by the state cryptography management authority. It shall provide multiple random sources, at least two strong physical noise source chip to realize.

SSL VPN gateway products should provide random number acquisition interface. The random number generator can detect random number detection in four different application phases by sample inspection, exit-factory inspection, power-on inspection and use inspection:

a) sampling detection:

Random number detection is based on GM/T 0005.

b) exit-factory inspection:

- inspection quantity: a random number of 50 x 10^6 bits are collected and divided into 50 groups, 10^6 bits each;
- inspection items: in accordance with GM/T 0005;
- inspection qualification standard: if there is an item does not pass the detection standard, the alarm detection shall fail.

Allowing random number acquisition and detection repeated once. It the re-inspection still fails, it shall determine the random number generator of the product is invalid.

- Allowing random number acquisition and detection repeated once. It the re-inspection still fails, it shall determine the random number generator of the product is invalid.

5.4.4.4 Environmental adaptability

The working environment of the SSL VPN gateway product should comply with the requirements of "climate and environment adaptability" according to actual needs in GB/T 9813-2000.

5.4.4.5 Electromagnetic compatibility

SSL VPN gateway products shall meet certain conditions of electromagnetic compatibility level. See GB/T 15153.1-1998 for requirements for electromagnetic compatibility.

5.4.4.6 Reliability

The average trouble-free working hours for SSL VPN gateway products should be no less than 10000 h.

5.5 Process protection

Set the necessary protection measures to protect the product in the transport and installation process of security, not embedded malicious information.

5.6 Parameter configurable capability requirements

The SSL VPN gateway product can support the configuration of the equipment parameters, including the MTU (maximum transmission unit), MAC address, speed (adaptive or fixed rate) of the network interface, duplex / half duplex, whether to open flow control, etc.

6 SSL VPN gateway product inspection

6.1 Product function inspection

6.1.1 Work mode

In the client-server mode, the client should be able to access the protected internal network server. In gateway-gateway mode, a gateway-protected client should have access to another gateway-protected intranet server. The inspection results shall meet requirements of 5.1.1.

6.1.2 Random number function

Extract sample according to requirements of GM/T 0005. Carry out the inspection according to relevant requirements of this specification. The

from the intranet server. And set the page delay on the intranet server, so as to ensure that every session is maintained and data is passed during the entire load increase process. Then, increase the client and repeat this process. Take the average number of concurrent sessions of the load stabilization period as the test result.

6.2.2 Maximum number of concurrent connections

The maximum number of concurrent connections is the maximum number of connections that can interact with the server at the same time. Simulate multiple client behavior on the detection platform. Connect with the server and maintain it. And then continue to increase the client, and repeat this process until it can not establish and maintain the link so far. The number of SSL connections that have been accessed shall be the test results.

6.2.3 Number of new connections per second

Simulate multiple client behavior on the detection platform. Concurrency establish an SSL session with the server. Repeat this process for a period of time. Take the average of the number of SSL sessions per second as test results.

6.2.4 Throughput rate

Simulate multiple client behavior on the detection platform. Establish an SSL session with the server. In this session, download 1MB of data from the intranet server. Repeat the above steps until each user successfully downloads 20 MB of data. And then upload 1MB of data to the intranet server. Repeat the above steps until each user successfully uploads 20 MB of data. Take the average rate of the data sent and received by the intranet server as the test results.

6.3 Security inspection

6.3.1 Key security

6.3.1.1 Server key

The test results shall comply with the requirements of 5.3.1.1.

6.3.1.2 Work key

The test results shall comply with the requirements of 5.3.1.2.

6.3.2 Configure data security

The test results shall comply with the requirements of 5.3.2.

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

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