GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GB/T 43779-2024

Cybersecurity Technology - Technical Specification for Caller Identity Authentication Using Crypto Tokens

网络安全技术 基于密码令牌的主叫用户可信身份鉴别技术规范

Issued on: April 25, 2024 **Implemented on: November 1, 2024**

Issued by: State Administration for Market Regulation;

Standardization Administration of the People's Republic of China.

Table of Contents

Cybersecurity Technology - Technical Specification for Caller Identity Authentication Using Crypto Tokens

1 Scope

This document specifies the technical requirements for transmitting, verifying and displaying the trusted identity of the caller based on crypto tokens in communications, and describes the corresponding test and evaluation methods.

This document is applicable to the design, production and test of systems that guide the transmission, verification and display of the trusted identity of the caller.

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 15843.2 Information Technology - Security Techniques - Entity Authentication - Part 2: Mechanisms Using Symmetric Encipherment Algorithm

GB/T 15843.3 Information Technology - Security Techniques - Entity Authentication - Part 3: Mechanisms Using Digital Signature Techniques

GB/T 16262.1 Information Technology - Abstract Syntax Notation One (ASN.1) - Part 1: Specification of Basic Notation

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

GB/T 32905 Information Security Technology - SM3 Cryptographic Hash Algorithm

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

GB/T 32918.2 Information Security Technology - Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves - Part 2: Digital Signature Algorithm

3 Terms and Definitions

The following terms and definitions are applicable to this document.

3.1 caller

A system that provides trusted identity management and certification / verification services.

3.11 trusted identity ticket

A digital certificate issued by a trusted identity services system that contains the trusted identity information and public key of the communicator.

3.12 trusted user

The caller or the called party who has applied for and obtained a trusted identity ticket.

NOTE: the communicator who can verify and display the trusted identity of the caller but does not necessarily possess the trusted identity tickets is referred to as a user in this document.

3.13 trusted identity

An identity that is certified by a third party and that matches the user's behavior.

4 Symbols and Abbreviations

4.1 Symbols

The following symbols apply to this document.

ID*i*: the identity ID issued by the operating system to the i^{th} trusted user for the authentication using the service. The ID is a randomly generated 128-bit data to protect the user's personal information.

K*i*: the symmetric key corresponding to the ID*i* of the i^{th} trusted user securely transmitted by the carrier.

RK: a root key for managing users of the carrier that manages trusted users.

4.2 Abbreviations

The following abbreviations apply to this document.

CA: Certificate Authority

CHAKEN: Caller Identity Authentication Using Crypto Tokens

DER: Distinguished Encoding Rules

SIP: Session Initiation Protocol

service for the crypto token sent by the caller;

⑤---if the called terminal does not cache the trusted identity ticket of the caller, query the identity ticket acquisition system through the calling number. After verification, the trusted identity of the caller is displayed on the user interface. Then, the user or the rules defined by the user decide whether to connect or reject the call.

Figure 2 -- Basic Process of Trusted Identity Authentication

When using the SIP protocol to make a call, the SIP protocol call message may carry the query address and query index of the caller identity token, or directly carry the identity token, or carry the token and identity ticket.

6 Security Requirements

6.1 Issuance of Trusted Identity Ticket

6.1.1 Identity ticket issuer authorization authority

The issuance of tickets of the identity ticket issuer authorization authority satisfies the following aspects:

a) The identity ticket issuer authorization authority shall formulate its own electronic certification business statement, including its own responsibilities and obligations in the issuance and use of identity tickets, the process of issuing identity tickets for the subordinate identity ticket issuer, and the definition of security policies related to the tickets;

b) The identity ticket issuer authorization authority shall issue a self-signed ticket for itself in accordance with the format requirements in GB/T 20518, and the self-signed ticket shall be available for users to download in at least two modes;

c) The identity ticket issuer authorization authority should set the value of pathLenConstraint in the Basic constraints extensions in the self-signed identity ticket to 1;

d) The ticket issuance system used shall be run offline and shall not have any wireless or wired connection with any network;

e) The identity ticket issued to the identity ticket issuer shall be encoded using the DER encoding method in accordance with the format requirements in GB/T 20518. The content of the issued ticket shall satisfy the requirements of the trusted identity ticket data content in 6.3;

f) The identity ticket issued to the identity ticket issuer shall have the Basic constraints extensions. The meaning of the extensions shall be set in accordance with GB/T 20518. It is advisable to set pathLenConstraint = 0 to prevent nesting among the

identity ticket issuers.

6.1.2 Identity ticket issuer

The issuance of tickets of the identity ticket issuer satisfies the following aspects:

a) The identity ticket issuer shall formulate its own ticket issuance business statement for the ticket security policy and make it public. The business statement shall describe the risk response and compensation strategy prepared for legal and economic issues caused by errors in the tickets it issues, or fraudulent behaviors caused by its tickets.

b) The identity ticket issuer can provide online services through the Internet and can also provide offline services.

c) The trusted identity ticket issued by the identity ticket issuer to the user shall be encoded using the DER encoding method in accordance with the format requirements in GB/T 20518. The content and format of the issued tickets shall satisfy the requirements of 6.3 and Appendix A.

d) The identity ticket issuer can only issue identity tickets to trusted users and must not issue identity tickets to other identity ticker issuers.

e) The identity ticket issuer should support the issuance service model of cloud tenants, that is, subscribers; subscribers may utilize their administrative accounts in the identity ticket issuer to type-in and review their employees, and the identity ticket issuer may automatically issue employee identity tickets containing the subscriber's name to users who have been reviewed by the subscriber administrator in accordance with its own security requirements.

f) The business statement shall make it clear that whether the ticket is issued directly by the identity ticket issuer or through the review of the subscriber administrator, the identity ticket issuer shall bear the same legal responsibilities in accordance with its published business statement.

6.1.3 Calling and called terminals

The certificate application and acquisition of the calling and called terminals satisfy the following aspects:

a) The terminals shall be equipped with a cryptographic module certified by the national cryptographic authority, which can generate the authentication key pair used in the algorithm in GB/T 32918.2 and complete the application, download and destruction of identity tickets;

b) The calling and called terminals shall be able to download and store the self-signed identity tickets of the authorization authority in a secure mode;

c) The terminals shall be able to apply for and accept no less than 5 identity tickets.

identity to remind the user that the cached identity tickets are used this time. If necessary, the user can be reminded to query the tickets for update or the user can set the time for automatic ticket update.

e) After verification is completed, the called terminal shall display at least the following information on the home page of calling. For specific display methods, see Appendix D:

1) The country name (c) and organization name (o) of the identity ticket issuer, and mark it as the identity issuer;

2) The policy of the caller identity ticket. If there is no policy in the identity ticket, it shall be displayed as a normal user;

3) Basic information of the trusted identity ticket, including the country name (c), organization name (o), organization unit name (ou), user or role name (cn);

4) Video, graphic or audio information contained in the ticket. At least one of them shall be taken out in order for demonstration;

5) The product name and certification certificate No. of the cryptographic module that supports cryptographic operations.

f) The called terminal shall provide a ticket viewing function, through which, the called user can view all the information of the caller identity ticket.

6.2.3 Token message service

The token message service satisfies the following aspects:

a) The token message service operating organization can set the service usage rights. The operating organization shall set its own operation root key RK in accordance with the algorithm requirements specified in GB/T 32907 and assign a random and different user ID*i* (128 bit) to the trusted caller of its service. By using the current operation root key RK and the algorithm specified in GB/T 32907, encrypt the trusted user's ID*i* and obtain the user's service key K*i*. The operating organization shall securely send the user's ID*i* and K*i* to the user terminal. The operating organization can use the user's public key in the identity ticket to encrypt the above information and send it to the trusted user.

b) The token message service can utilize the privilege credential (Credential) to verify the caller's privilege to use the token message service. Encrypt ID*i* in Credential with the operation root key RK to obtain K*i* and use K*i* to decrypt the last 128 bits of Credential. If {the integer representation of the number of seconds from (GeneralizedTime) to 2020-01-01 00:00:00 (32-bit length, using big-endian byte order) || "Mess" || 64-bit random number} is obtained, the privilege check is passed.

c) The token message service should improve its capability to resist denial of service attacks through the following means:

1) Utilize load balancing to ensure that the message service is not subject to general denial of service attacks;

2) Monitor the data traffic from the same source address and do not accept calls from the same address that exceed the normal traffic, including abnormal calls from trusted users;

3) For suspicious addresses, utilize identity tickets for further identity authentication.

d) The token message service shall at least support the connectionless UDP protocol when accepting token messages and query requests. It shall at least support using UDP protocol to send messages in the format of "PUT" || Identity_token to upload crypto tokens; at least support using UDP protocol to send messages in the format of "GET" || token_index1 || "OR" || token_index2 for query.

e) The token message service shall monitor query requests to prevent abnormal token queries.

6.2.4 Identity ticket acquisition system

The identity ticket acquisition system satisfies the following aspects.

a) The identity ticket acquisition system shall provide technical means to prevent malicious queries on user's identity tickets and avoid user information leakage to irrelevant entities.

b) The identity ticket acquisition system shall be able to require the called user to provide the privilege credential in the crypto token of the caller for the current call in accordance with its own security policy. Only the called party who provides the correct privilege credential can query the caller's identity ticket.

c) The identity ticket acquisition system shall be able to require the called to provide the caller's number, the serialNumber (ticket serial No.) in the caller's token, the signatureValue (signature value) in the caller's token, the credential in the caller's token, or the TBSIdentityToken (token signed content) in the caller's token in accordance with its own security policy. The identity ticket acquisition system verifies the correctness of the token signed content. After confirming that the above-mentioned information is correct, the corresponding caller's trusted identity ticket can be sent to the called.

d) The identity ticket acquisition system shall be configured to verify the inquirer as a query-first-then-verify strategy in accordance with its own security capabilities.

2) The identity ticket verification is valid;

3) The application review and issuance process of the trusted identity ticket can be completed, and the data format of the issued trusted identity ticket shall comply with the requirements of 6.3 and Appendix A.

c) Result judgment:

If all the above-mentioned expected results are met, it is compliant, and in other cases, it is non-compliant.

7.2 Calling Terminal

The function test method, expected results and result judgment of the calling terminal are as follows.

a) Test method:

1) Review the documents submitted by the terminal manufacturer to check whether the cryptographic module used has been certified by the national cryptographic authority and has cryptographic functions, such as SM4 encryption and decryption, SM3 hash operation, SM2 signature / verification, key management and identity ticket storage, etc.;

2) Use the terminal to apply for and download the identity ticket at least once to check whether the identity ticket information can be accurately displayed;

3) Use the terminal to apply for 5 different identity tickets;

4) Use the terminal to make at least one phone call to check whether it has the function of selecting a trusted identity ticket for calling;

5) Use the terminal to make at least one phone call to review the identity token generated by it and check whether the identity token data structure and encoding format comply with the provisions of 6.4 and whether the cryptographic operation result is accurate.

b) Expected results:

1) The cryptographic module used by the terminal complies with the relevant standards and has the cryptographic function required for the communication process;

2) It can accurately display the contents of the identity ticket;

3) It can apply for 5 or more identity tickets and correctly store them;

4) It has the ability to choose or not to use a trusted identity to make a phone call;

5) The token generated by the terminal complies with the identity token data and format requirements specified in 6.4, the digital signature value in the identity token can be verified using the public key in the identity ticket, the token index value is accurately calculated, and the encryption result in the credential is accurately calculated.

c) Result judgment:

If all the above-mentioned expected results are met, it is compliant, and in other cases, it is non-compliant.

7.3 Called Terminal

The function test method, expected results and result judgment of the called terminal are as follows.

a) Test method:

1) Review the documents submitted by the terminal manufacturer to check whether the cryptographic module used has been certified by the national cryptographic authority and has cryptographic functions, such as SM4 encryption and decryption, SM3 hash operation, and SM2 signature verification, etc.;

2) Use the terminal to answer at least one call to check whether it can complete the calculation of the identity token index value, the download of the identity token and identity ticket, the digital signature verification and other cryptographic functions, and can display the caller's trusted identity ticket information in accordance with the requirements of 6.2.2;

3) Use multiple identity tickets required by Appendix A to make calls and test whether the called terminal can correctly display the ticket content and audio and video files in accordance with the requirements of 6.2.2.

b) Expected results:

1) The cryptographic module used by the terminal complies with the relevant standards and has the cryptographic function required by the called terminal during the communication process in the text;

2) It can complete the necessary cryptographic operation capabilities in the communication process and can accurately display the caller's trusted identity tickets;

3) It can display the audio and video information in the tickets in accordance with the requirements of 6.2.2.

c) Result judgment:

2) Access the identity ticket acquisition system to detect whether the query of the caller's identity ticket by the called satisfies the requirements of the trusted identity ticket query authorization process in this document;

3) Detect the identity ticket query performance, including system throughput, response time, etc.;

4) Detect whether the identity ticket acquisition system has appropriate risk response measures for key data protection;

5) Use multiple addresses to launch denial of service attacks on the identity ticket acquisition service to detect the capability of the trusted identity ticket acquisition system to resist denial of service attacks.

b) Expected results:

1) The process of trusted identity ticket query has an authorization verification mechanism;

2) The process and results of the called querying the caller's identity ticket meet the requirements of identity ticket acquisition service in 6.2.4;

3) Detect the performance of the identity ticket acquisition service and record the test results of indicators, such as system throughput and response time, etc. The average response time is not less than 200 ms;

4) There are relevant risk response measures for the protection of key data in the identity ticket acquisition system;

5) Record the test results of the identity ticket acquisition system to prevent and resist denial of service attacks. It shall be able to withstand denial of service attacks launched by no more than 20 physical servers with the same performance.

c) Result judgment:

If all the above-mentioned expected results are met, it is compliant, and in other cases, it is non-compliant.

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

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