ICS 35.030
CCS L 80



# NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

# 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 PRC**

# Table of Contents



## 1 Scope

The document lays down the technical requirements for transmitting, verifying and displaying the trusted identity of the calling user in communication on the basis of a crypto token, and describes the corresponding test and evaluation methods.

It applies to guiding the system design, the production and the testing of the transmission, verification and display of the trusted identity of the calling user.

## 2 Normative references

The documents cited are GB/T 15843.2, entity authentication using symmetric encipherment algorithms; GB/T 15843.3, entity authentication using digital signature techniques; GB/T 16262.1, abstract syntax notation one; GB/T 20518, public key infrastructure, digital certificate format; GB/T 32905, the SM3 cryptographic hash algorithm; GB/T 32907, the SM4 block cipher algorithm; and GB/T 32918.2, the SM2 elliptic curve public key cryptographic algorithm, Part 2, digital signature algorithm.

## 3 Terms and definitions

3.1 caller: originator of a call connection, or the intelligent terminal equipment of the originator of a call connection.

3.2 called: receiver of a call connection, or the intelligent terminal equipment of the receiver of a call connection.

3.3 carrier: network service provider of the caller or of the called party. A note adds that the carrier of the caller and the carrier of the called party may be the same or different.

3.4 crypto token: data message signed by a trusted user using cryptographic technology and submitted to the called user for verification, which serves to represent the identity of the signer. A note adds that the data message is also called the cryptographic identity token or the identity token.

3.5 identity ticket issuer: body that generates and issues trusted identity tickets for users.

3.6 identity ticket issuer authorization authority: authorizing party of the identity ticket issuer, which carries out authorization management by digitally signing the identity ticket issued to the identity ticket issuer.

3.7 identity ticket acquisition service: service that provides the called user with the means of querying the identity ticket of the caller. A note adds that the service is implemented in the form of a cloud service or of other network services and is accessed in the calling or the called network.

3.8 privilege credential: data obtained by a trusted user by computation with symmetric cryptographic technology, which shows that the user holds the right of use. A note adds that the privilege credential is valid only for the current use.

3.9 token message service: service that provides the delivery of token messages for the calls of trusted users. A note adds that the token message service is deployed on the Internet, in the calling network or in the called network.

3.10 trusted identity services system: system that provides trusted identity management and attestation or verification services.

3.11 trusted identity ticket: digital ticket issued by the trusted identity services system that contains the trusted identity information of a communicating party together with its public key.

3.12 trusted user: caller or called party that has applied for and obtained a trusted identity ticket. A note adds that a communicating party that can verify and display the caller trusted identity but does not necessarily hold a trusted identity ticket itself is called a user in the document.

3.13 trusted identity: identity that has been certified by a third party and that can be matched with the behaviour of the user.

## 4 Symbols and abbreviations

4.1 Symbols. ID with the index i is the identity identifier issued by the operating system to the i-th trusted user for authentication when the service is used; it is randomly generated data of 128 bit, so as to protect the personal information of the user. K with the index i is the symmetric key corresponding to that ID, transmitted securely by the carrier to the i-th trusted user. RK is a master key by which the carrier that manages trusted users manages the users.

4.2 Abbreviations. CA is the certificate authority; CHAKEN is caller identity authentication using crypto tokens; DER is the distinguished encoding rules; SIP is the session initiation protocol.

## 5 Overview

5.1 Basic principle. The CHAKEN technique laid down in the document aims to present the trusted identity of the caller securely to the called party. To present the trusted identity, a trusted identity ticket is first issued to the trusted user who has been vetted; that ticket contains the verified caller user information available for display, which may be text, a picture, an audio signal or video information. The called party then verifies the identity of the caller by means of the crypto token and the trusted identity ticket of the caller, so making sure that the caller is the holder of that trusted identity ticket.

5.2 Issuing architecture. In the CHAKEN technique the identity management of trusted users follows a two-layer pattern made up of the identity ticket issuer authorization authority and the identity ticket issuer. The authorization authority is the root of trust of the CHAKEN

system; its self-signed identity ticket is pre-installed in the cryptographic module of the user by a trusted means, or a trusted download route is provided to the user. An identity ticket issuer needs the permission of the authorization authority and shall have obtained a valid identity ticket issued by it before it can issue identity tickets to ordinary users. Figure 1 shows the issuing architecture, with the authorization authority above, the identity ticket issuers below it, the trusted identity subscribers below those and the trusted identities at the bottom.

5.3 Issuing modes. Two modes are used. In the first, the identity ticket issuer vets the user information directly and issues the trusted identity ticket to the user. In the second, a subscriber of the identity ticket issuer, that is an organisational user or a group user, vets its own subordinate staff and the identity ticket issuer then issues the trusted identity ticket to that member of staff. The connecting lines in Figure 1 represent the issuing paths of the trusted identity ticket: for a given subscriber, the trusted vetting of the identity tickets of its staff may be carried out by the subscriber itself, but the organisation information in the identity information of the member of staff can only be the organisation information of the subscriber as vetted by the identity ticket issuer.

5.4 Verification of the trusted user. The CHAKEN technique verifies a trusted user in a pattern of two layers of ticket plus one token: the root ticket of the authorization authority verifies the identity ticket of the identity ticket issuer, the identity ticket of the issuer then verifies the trusted identity ticket of the calling user, and finally the trusted identity ticket of the calling user verifies the crypto token that the calling user has sent.

5.5 Basic flow. Figure 2 shows the basic flow of authenticating the calling user on an existing telephone call. As a precondition, marked 0, the calling terminal obtains, online or offline, the trusted identity ticket issued by the identity ticket issuer before it places the call. At step 1 the caller selects the called number and one of its own identities, of which it may have one or several; if that is a trusted identity, a crypto token is built and sent to the token message service. At step 2 the caller places the call to the called party through the calling network, and the calling network, having received the call, places the call to the called network through a transit network. At step 3 the called network sends the call request of the caller to the called terminal. At step 4 the called terminal, having received the call request, uses the index to query the token message service for the crypto token the caller has sent. At step 5, if the trusted identity ticket of the caller is not cached in the called terminal, the called terminal queries the identity ticket acquisition system by the caller number; once verification is correct, the trusted identity of the caller is displayed on the user interface, and the user, or a rule the user has defined, then decides whether to accept or reject the call.

5.5 Use with SIP. When the call uses the SIP protocol, the SIP call message can carry the query address and the query index of the caller identity token, or can carry the identity token directly, and can also carry both the token and the identity ticket.