GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 38626-2020

Information security technology - Guide to password protection for intelligent connected device

信息安全技术

智能联网设备口令保护指南

Issued on: April 28, 2020 **Implemented on: November 01, 2020**

Issued by: State Administration for Market Regulation;
Standardization Administration of PRC.

Table of Contents

Information security technology - Guide to password protection for intelligent connected device

1 Scope

This standard provides security technical guidelines for the generation, management, use of accounts and passwords for intelligent connected devices.

This standard applies to the guidance of intelligent connected device manufacturers to secure design and implementation of password protection functions; it also applies to the supervision and inspection of the secure use of passwords for intelligent connected device.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GB/T 25069-2010 Information security technology - Glossary

3 Terms and definitions

The terms and definitions as defined in GB/T 25069-2010 as well as the following terms and definitions apply to this document. For ease of use, some terms and definitions in GB/T 25069-2010 are listed repeatedly below.

3.1

Intelligent connected device

A device with the ability to access the network for communication, data perception, data storage, data processing and human-computer interaction.

Note: Mainly refers to the end devices in the Internet of Things, including web cameras, smart home appliances, network set-top boxes, smart projectors, home routers, etc., excluding computers, mobile phones and other general computing devices.

encryption function, which can be used to calculate password authentication data.

[GB/T 25069-2010, definition 2.2.2.186]

4 Abbreviations

The following abbreviations apply to this document.

API: Application Programming Interface

ID: Identity

IP: Internet Protocol

5 Overview

Due to the different access modes of intelligent connected devices, the implementation of password authentication can be divided into two types:

- Equipment authentication: the password authentication process is carried out in the intelligent networked equipment.

- Non-device local authentication: the process of password authentication is not carried out in intelligent networked equipment, including but not limited to user terminal authentication through cloud platform. See Appendix A for details.

Non-device local authentication is essentially the platform that performs password authentication instead of intelligent connected devices. Therefore, the security technical requirements for account and passwords in this standard are applicable in both cases.

The password is used as the authentication credential to be associated with the account as the user's identity. Account security is a very important part of the password authentication protection. This standard proposes protection rules and requirements from two aspects of account security and password security; meanwhile provides guidance on the secured use and management of account passwords for users.

In this standard, once involving the use of cryptographic technology to solve the requirements of confidentiality, integrity, authenticity, non-repudiation, it shall follow the national and industry standards related to cryptography.

7 Password security

7.1 Password generation

Matters of concern include:

a) The automatically generated password is random, and the length is not less than 6 characters.

b) The basic policy content that the password set by the user complies with is as follows:

1) The password length is not less than 8 characters;

2) The maximum allowed length of the password is not less than 64 characters;

3) The password contains at least two types of characters among numbers, lowercase letters, uppercase letters, special characters.

c) For intelligent connected devices that use the activation mechanism in exit-factory configuration, when the user accesses the device for the first time, it needs to activate the device by setting a password for the device. Inactive devices refuse to operate other than activation.

Note: "Activation" means that the user sets a password that meets the password complexity requirements when the device is used for the first time.

d) For the intelligent networked devices that use the initial password in the exit-factory configuration, the initial password is randomly generated for each device; the user is reminded to modify the password every time they log in, until the initial password is modified.

7.2 Password usage

Matters of concern include:

a) Password transmission adopts secure transmission channel or encrypted transmission;

b) By default, the password in the input box is hidden-displayed;

c) The function that prohibits the password from being copied from the input box;

d) The user cannot view his password after successfully logging in;

e) The password authentication process has the function of preventing brute force cracking. If the wrong login attempts exceed the set number of times, the operating account is locked, or the IP is operated for a period of time.

7.3 Password management

Matters of concern include:

a) All passwords can be modified; hard-coded passwords cannot be used;

b) Before the user changes the password, provide the function of verifying the old password and reconfirming the new password;

c) Encryption is required when storing passwords;

d) The stored password has an anti-cracking mechanism, including but not limited to salt;

e) Restrict access to and modification of password files, including but not limited to using the access control function of the operating system;

f) Cannot read the password plaintext through the user interface or API;

g) Provide the function of restoring the device to the exit-factory state through physical buttons or other security methods when the account or password is forgotten;

h) The password complexity strategy is configurable, allowing administrators to configure enhanced password complexity strategies according to application scenarios;

i) Have the ability to display the security strength of the password.

7.4 Log

All users' operations on passwords are recorded in logs. The contents of the logs include user ID, IP address, operation time, operation content, operation result and other information.

8 User security

Matters of concern include:

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

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