ICS 35.240.01
CCS L67

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 37036.8-2022

Information technology - Biometrics used with mobile devices - Part 8: Presentation attack detection

信息技术 移动设备生物特征识别 第8部分：呈现攻击检测

Issued on: December 30, 2022 **Implemented on: July 1, 2023**

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

Table of Contents

Foreword

This document was issued on 30 December 2022 by the State Administration for Market Regulation; Standardization Administration of the PRC and takes effect on 1 July 2023.

It is a GB/T standard: recommended rather than compulsory, but it is the text a Chinese reviewer applies when assessing a submission.

It is classified under ICS 35.240.01, Chinese classification L67.

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for Standardization Work Part 1.Structure and Drafting Rules for Standardization Documents"

drafting.

This document is part 8 of GB/T 37036 "Biometric Identification of Information Technology Mobile Devices". GB/T 37036 has been published

the following sections.

--- Part 1.General requirements;

--- Part 2.Fingerprint;

--- Part 3.Human face;

--- Part 4.Iris;

--- Part 6.Finger veins;

--- Part 7.Multimodal;

--- Part 8.Presentation attack detection.

Please note that some contents of this document may refer to patents. The issuing agency of this document assumes no responsibility for identifying patents.

This document is proposed and managed by the National Information Technology Standardization Technical Committee (SAC/TC28).

This document was drafted by. Alipay (China) Network Technology Co., Ltd., East China Branch of China Electronics Standardization Institute, Human Resources

Source and Information Center of the Ministry of Social Security, Xiamen Yicheng Information Technology Co., Ltd., Newland Digital Technology Co., Ltd., Beijing Megvii

Technology Co., Ltd., Ant Technology Group Co., Ltd., China Electronics Standardization Research Institute, Zhejiang Standardization Research Institute, Beijing Zhongke

Hongba Technology Co., Ltd., Beijing Shuguang Yitong Technology Co., Ltd., Beijing Deyi Yintong Technology Co., Ltd., Beijing Eyes Intelligent Technology Co., Ltd.

Co., Ltd., Lenovo Zhongtian Technology Co., Ltd., Shanghai SenseTime Intelligent Technology Co., Ltd., Xiaomi Technology Co., Ltd., Huawei Terminal Co., Ltd.

Company, Guangdong Jiulian Technology Co., Ltd., Beijing Zunguan Technology Co., Ltd., Xi'an Kaihong Electronic Technology Co., Ltd., Beijing University of Posts and Telecommunications

Science, Beijing Qihoo Technology Co., Ltd., Jianxin Financial Technology Co., Ltd., Wuhan Hongshi Technology Co., Ltd., Zhejiang University, Huizhou University,

Beijing Wanlihong Technology Co., Ltd., Tianfu (Dongguan) Standard Technology Co., Ltd., Shenzhen Mingtu Innovation Technology Co., Ltd., State Grid Blockchain

Technology (Beijing) Co., Ltd., Ziguang Tongxin Microelectronics Co., Ltd., and Guangdong Zhongke Zhenheng Information Technology Co., Ltd.

The main drafters of this document. Lin Guanchen, Zhong Chen, Wang Wenfeng, Li Liang,

Song Jiwei, Peng Jin, Chen Jidong, Ding Jingting, Lang Junqi, Guo Mingyu,

Chen Tao, Wang Zhifei, Shi Hongyan, Chen Jianlong, Mei Jingqing, Gao Jian, Liu Qianying, Jiang Jianping, Lu Xiaosi, Li Xingguang, Yang Chunlin, Zhang Yahao, Zheng Fang,

Li Yang, Jiang Hui, Zhu Yajun, Wang Sishan, He Qiang, Gong Qiong, Huang Guiling, Xu Jianmin, He Zhaofeng, Zhang Yi, Liu Lijuan, Gao Junxiong, Zhang Bingsheng, Wei Xiaohui,

Luo Sixin, Zhang Xiaoliang, Yang Zhanjin, Wang Cheng, Li Qingshun, Wang Dong, Lai Huatian, Yang Jingfeng.

Introduction

GB/T 37036 "Information Technology Mobile Device Biometric Identification" is proposed to be composed of 9 parts.

--- Part 1.General requirements. The purpose is to establish the technical framework, common process and ticket requirements for biometric identification of mobile devices.

--- Part 2.Fingerprints. The purpose is to establish the processes and requirements for fingerprint biometric identification of mobile devices.

--- Part 3.Human face. The purpose is to establish the process and requirements for face biometrics on mobile devices.

--- Part 4.Iris. The purpose is to establish the processes and requirements for iris biometrics on mobile devices.

--- Part 5.Voiceprint. The purpose is to establish the procedures and requirements for voiceprint biometric identification of mobile devices.

--- Part 6.Finger veins. The purpose is to establish the process and requirements for finger vein biometrics on mobile devices.

--- Part 7.Multimodal. The purpose is to establish the processes and requirements for multimodal biometric identification on mobile devices.

--- Part 8.Presentation attack detection. The purpose is to specify mobile device presentation attack detection requirements.

--- Part 9.Test methods. The purpose is to describe functional and performance testing methods for different types of biometric identification in mobile devices.

With the gradual maturity of mobile device biometric identification technology and industrial development, for mobile device fingerprint, face, iris, voiceprint, fingerprint

Concerns about presenting attacks in modalities such as veins and multimodality also increase, and the importance of presenting attack detection is further highlighted, and the demand for standardization is becoming more and more

It is becoming more and more intense that it is necessary to formulate relevant standards to ensure the healthy, benign and orderly development of the mobile device biometric identification industry. This document gives

Mobile devices present attack detection technical requirements.

Information technology mobile device biometrics

Part 8.Rendering attack detection

1 Scope

GB/T 37036.8-2022 is the part of the mobile device biometrics series that deals with presentation attack detection - the case where a sensor is shown an artefact instead of the live person it is meant to recognise. After the terms and the abbreviations, it lays out the detection process as a general framework and a technical architecture, then the technical requirements on the detecting system: the local mode, in which the decision is reached on the handset itself; the remote mode, in which the captured data is judged elsewhere; the hybrid of the two; and the functions the system has to provide. The last clause governs testing and reporting - the general requirements, the types of attacker assumed, the types of assessment, what part of the mechanism is the object of evaluation, and the dependence of all of it on the business process the device serves. That dependence is the point: unlocking a screen and authorising a payment carry very different consequences from the same false accept, so a detection claim quoted without the process it was measured in tells a buyer very little. Of use to handset and sensor makers, biometric software suppliers, and the laboratories that evaluate them.

This document defines the biometric identification presentation attack detection process of mobile devices, and puts forward the technical requirements for presentation attack system detection.

The testing and reporting requirements for the evaluation of mobile device presentation attack detection are given.

This document is applicable to activities such as the design, application, and evaluation of biometric presence attack detection on mobile devices.

2 Normative references

This document has no normative references.

3 Terms and Definitions

The following terms and definitions apply to this document.

3.1