ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 42572-2023

Information security technology - Trusted execution environment service specification

信息安全技术 可信执行环境服务规范

Issued on: May 23, 2023 **Implemented on: December 1, 2023**

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

Table of Contents

Foreword

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: 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 Security Standardization Technical Committee (SAC/TC260): This document is drafted by: China UnionPay Co:, Ltd:, University of Chinese Academy of Sciences, Fudan University, Huawei Technologies Co:, Ltd:, Bank of Beijing Lianjinka Technology Co:, Ltd:, Shenzhen Huada Beidou Technology Co:, Ltd:, CICC Financial Certification Center Co:, Ltd:, Beijing Qianchuan Technology Co:, Ltd: Co:, Ltd:, Shanghai Molian Information Technology Co:, Ltd:, Beijing Xiaomi Mobile Software Co:, Ltd:, OPPO Guangdong Mobile Communication Co:, Ltd:, Shenzhen Tencent Computer System Co:, Ltd:, Ant Technology Group Co:, Ltd:, Zhengzhou Xinda Jiean Information Technology Co:, Ltd:, Hengbao Co:, Ltd:, Yuncong Technology Group Co:, Ltd:, Beijing Chuangyuan Tiandi Technology Co:, Ltd:, Datang Gaohong Xin'an (Zhejiang) Xin Information Technology Co:, Ltd:, Shanghai Juhong Optoelectronics Technology Co:, Ltd:, Tongdun Technology Co:, Ltd: The main drafters of this document: Chai Hongfeng, Sun Quan, Chen Chengqian, Wang Yuewu, Wu Jie, Li Xiaowei, Sun Zhongliang, Hu Ying, Zou Fen, Zhang Youju, Zhou Quan, Lei Lingguang, Ye Jiawei, Wang Xin, Chi Haizhang, Wang Sishan, Lu Xin, Meng Qingyang, Xu Gang, Zhou Bo, Zhang Zhongqun, Wang Lei, Li Gen, Jiang Zengzeng, Lin Guanchen, Liu Weihua, Zhao Liming, Li Jun, Xiao Qinghai, Zheng Chi, Li Jiayang, Tan Cheng: Information Security Technology Trusted Execution Environment Service Specification

1 Scope

GB/T 42572-2023 covers the layer that sits between a chip's secure enclave and the applications that rely on it. Most modern phones and payment terminals already ship with a trusted execution environment, a hardware-isolated area that runs alongside the ordinary operating system and is meant to hold what must not leak: keys, fingerprints, PIN entry, the pixels of a confirmation screen. What the hardware gives is isolation. What an application actually consumes is a service built on top of it, and that is where the guarantees are usually lost. This document defines those services and what each of them must prove. It sets out a technical framework, then works through the requirements that apply to every TEE service - key management, service initialisation, secure storage, access control, trusted input and output, application authentication, and the protection of the communication channel - before turning to seven specific services one at a time: human-computer interaction, QR code handling, device security status evaluation, identity authentication, time, location, and cryptographic computation. For each of the two layers it gives the matching test and evaluation method, so a claim of conformance can be checked rather than asserted. It was drafted under SAC/TC260 by China UnionPay together with Huawei, Fudan University and the University of the Chinese Academy of Sciences, which places it squarely in the mobile payment and financial authentication world, and it builds on GB/T 41388-2022, the basic security specification for the environment itself. The audience is anyone designing, building or certifying TEE services: chipset and handset makers, system software vendors, testing laboratories and the banks that depend on the result.

This document establishes a technical framework system for trusted execution environment services, and specifies relevant security technical requirements and testing and evaluation methods: This document is applicable to the design, development, testing, etc: of trusted execution environment services, equipment manufacturers, system software providers, testing agencies and Participants in credible execution environment services such as scientific research institutions can refer to it:

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text: Among them, dated references For documents, only the version corresponding to the date is applicable to this document; for undated reference documents, the latest version (including all amendments) is applicable to this document:

GB/T 17901:1-2020 Information Technology Security Technology Key Management Part 1: Framework

GB/T 25069-2022 Information Security Technical Terminology

GB/T 41388-2022 Information Security Technology Trusted Execution Environment Basic Security Specifications

3 Terms and Definitions

The following terms and definitions defined in GB/T 25069-2022 and GB/T 41388-2022 apply to this document: 3:

1 Based on hardware-level isolation and secure boot mechanism, in order to ensure the confidentiality, integrity, and authenticity of security-sensitive application-related data and codes A software operating environment built with the goal of non-repudiation:

Note: Hardware-level isolation refers to the hardware-based security extension mechanism, through the fixed division or dynamic sharing of computing resources, to ensure that isolated resources are not blocked by the rich execution environment: A security mechanism for environment access: [Source: GB/T 41388-2022, 3:3] 3:2 A software operating environment that provides basic functions and computing resources for applications:

Note: The rich execution environment is an operating environment that exists independently of the trusted execution environment: [Source: GB/T 41388-2022, 3:4] 3:3 A software program that runs in a trusted execution environment and provides basic, general, and public functions for REE:

Note: This document is referred to as "TEE service": 3:4 A software program that runs in a trusted execution environment and provides an information interaction interface: