Chinastandards.org

ICS 35.02
CCS L70

YD

INDUSTRY STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

YD/T 4691-2024

Privacy computing federated learning product security requirements and testing methods

隐私计算 联邦学习产品安全要求和测试方法

(English Translation)

Issued on: March 29, 2024 **Implemented on: July 1, 2024**

Issued by: Ministry of Industry and Information Technology

Preview: page 1 of 3 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/yd-t-4691-2024

Table of Contents

[Preview only]
1 Scope
2 Normative references
3 Abbreviations
3.1 Terms and definitions
4 General
4.1 Test environment
4.2 UE Information
4.3 Test Implementation
5 Requirements

1 Foreword

YD/T 4691-2024 was issued by Ministry of Industry and Information Technology on 29 March 2024 and has been in force since 1 July 2024.

The YD/T prefix marks a recommended standard. It is not law in itself: it becomes binding when a contract names it, when a regulation or a mandatory standard refers to it, or when a producer declares conformity with it.

The document runs to 15 pages in English translation.

2 Scope Preview

This standard specifies the security requirements and corresponding test methods for privacy computing products based on federated learning, including general algorithm protocol security, secure intersection algorithm protocol security, feature engineering algorithm protocol security, joint modeling algorithm protocol security, joint prediction algorithm protocol security, cryptographic security, communication security, authorization and authentication, system security, stability, storage security, logs and evidence storage. This standard applies to the research and development, testing, evaluation and acceptance of privacy computing products based on federated learning.

YD/T 4691-2024 falls under ICS 35.02, in the field of information technology.

This catalogue holds 725 other YD/T standards in that field.

In this catalogue, YD/T standards carry edition years from 1982 to 2026.

Preview: page 2 of 3 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/yd-t-4691-2024

3 About this standard

Sector: Telecommunication Industry Standard (Recommended)

Issued by: Ministry of Industry and Information Technology

English translation: about 15 pages (approximate)

4 Related standards

Standards on related subjects:

YD/T 3746-2020 - Specification of internet of vehicle information service - User personal information protection

GB/T 28826.2-2020 - Information technology-Common biometric exchange formats framework-Part 2:Procedures for the operation of the biometric registration authority

GB/T 31071-2014 - General science and technology infrastructure-Principles and methods for conformance testing

YD/T 4692-2024 - Privacy computing federated learning product performance requirements and testing methods

YD/T 4690-2024 - Privacy computing Multi-party secure computing product security requirements and testing methods

YD/T 4683-2024 - Cloud Service Customer Information Security Management Guide

5 Classification and status

International classification (ICS): 35.02

Chinese Standard Classification (CCS): L 70

Prefix YD/T: recommended standard.

Preview: page 3 of 3 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/yd-t-4691-2024