

国家标准《信息安全技术 网络支付服务数据安全指南》

（征求意见稿）编制说明

一、工作简况

1、任务来源

《信息安全技术 网络支付服务数据安全指南》是国家标准化管理委员会下达的信息安全国家标准制定项目。该项目由蚂蚁科技集团股份有限公司牵头，并联合中国电子技术标准化研究院、滴滴、小米、马上金融等10余家单位编制。2020年8月11日，全国信息安全标准化技术委员会发布了标准的立项通知，2020年12月24日，国家标准化管理委员会下达了国家标准计划号20205163-T-469。该标准由全国信息安全标准化技术委员会提出并归口。

2、主要起草单位和工作组成员

本标准自主制定标准，牵头单位为蚂蚁科技集团股份有限公司，参与单位有中国电子技术标准化研究院、中国信息通信研究院、中国网络安全审查技术与认证中心、国家计算机网络应急技术处理协调中心、浙江大学、深圳市腾讯计算机系统有限公司、马上消费金融股份有限公司、北京小桔科技有限公司、北京钱袋宝支付技术有限公司、北京小米移动软件有限公司、中国移动通信集团有限公司、天翼电子商务有限公司、苏宁易购集团股份有限公司、京东数字科技控股有限公司等10余家单位，归口单位为全国信息安全标准化技术委员会（简称信安标委）。

本标准主要起草人：彭晋、金涛、胡影、落红卫、王昕、周晨炜、李海英、李洁、宋铮、马天羿、张秉晟、舒敏、王文磊、张娜、刘源、焦伟、李映婧、李明菊、邱勤、兰安娜、胡铁、曹京、卢启祯、李玲、刘熙君、宋建、蒋尉、黄莹、冷杉、李丛、衣强、程瑜琦、魏立、蒋增增、武杨、杨锋、高砚。

3、主要工作过程

标准制定的主要工作过程如下：

- a) 2020年1月14日，课题研究启动，与信安标委联合牵头成立标准课题研究组；
- b) 2020年2月31日，召开研究项目启动会，研讨确定标准名称为《信息安全技术 网络支付服务平台数据安全指南》；
- c) 2020年3月，根据信安标委国标立项通知，发起国家标准立项申请；

- d) 2020年4月，为保持系列标准名称一致，修改标准名称为《信息安全技术 网络支付服务数据安全指南》，以个人信息保护为主，兼顾数据安全，根据标准名称调整修订标准大纲；组织召开专家研讨会，对标准草案进行修改完善；
- e) 2020年5月至8月，形成标准草案并专家评审；标准编制组分析了网络支付服务的数据收集、存储、使用和共享等方面防护现状，分析其面临的主要风险，形成了标准草案初稿；组织4次专家研讨评审会并参加中央网信办2次专家推进会，根据会议专家意见编制组内部多轮会议、第三方共享专题研讨并封闭编制，对标准草案进行了修改完善；
- f) 2020年9月至10月，草案完善并中央网信办专项汇报；公开征集参编单位，修改完善数据活动图、风险分析，裁剪与上位标准重叠条款，听取标准责任专家修改意见，进行中央网信办标准工作专项汇报暨专家评审会，对草案主要修改内容进行研讨，对标准草案进行修改完善；
- g) 2020年11月初，编制组大群内组织标准文稿讨论，就几项关键问题进行分工完善，补充标准对照表、系统权限等部分内容；
- h) 2020年11月12日，标准在信安标委会议周上进行了汇报与讨论，经过投票同意进入征求意见稿阶段；
- i) 2020年12月，编制组组织线上编制讨论，就标准文稿中的数据分级分类、自动化决策和系统权限部分进行修改和完善；
- j) 2021年1月，编制组分工就标准数据存储、数据委托处理部分进行讨论与修改。

二、标准编制原则和确定主要内容的论据及解决的主要问题

1、标准编制原则

本标准在编制过程中遵循了先进性和合理性原则。

先进性原则体现在与国内安全技术同步。本标准在制定过程中主要参考了《信息安全技术 个人信息安全规范》和《信息安全技术 网络数据处理安全规范》（征求意见稿）等安全要求。

合理性原则体现在与网络支付行业实际情况相结合。网络支付服务运营者具积累了大量的数据，与用户个人信息相关的数据较多，保护任务重。本标准基于网络支付行业的特点制定数据收集、告知同意、数据存储、数据使用和共享等安全管理和技术防护条款，起到实际的指导作用。

2、标准解决的问题及主要内容

本标准提出网络支付服务的数据安全工作指南，以个人信息保护为主，兼顾数据安全，包括网络支付服务类型和典型场景相关特色数据问题，明确网络支付服务运营者开展服务时数据收集、存储、使用、共享、公开披露、删除的数据类型、范围、方式和条件，以及数据安全要求。具体内容包括：网络支付服务数据活动和主要风险分析，网络支付服务数据收集、数据传输存储、数据使用、数据共享和披露的安全管理要求和技术保护措施，以及网络支付服务中收集的个人信息数据应采取的安全措施等内容。

三、主要试验[或验证]情况分析

无。

四、知识产权情况说明

本标准不涉及专利。

五、产业化情况、推广应用论证和预期达到的经济效果

《网络支付服务数据安全指南》后续将在网络支付服务运营企业的落地试点，将有助于网络支付运营者提升自身的数据安全保护能力，有效促进网络支付服务行业的数据安全健康发展，为保障网络支付服务数据安全、公众个人信息安全提供有力支持。目前，国内网络支付服务的相关企业不断增加，标准应用范围自然也不断扩大，标准应用将取得良好的经济效益。

六、采用国际标准和国外先进标准情况

无。

七、与现行相关法律、法规、规章及相关标准的协调性

本标准符合现有法律法规的要求。符合《中华人民共和国网络安全法》提出的对于数据安全保护的相关要求，是在国家标准《信息安全技术 个人信息安全规范》和《信息安全技术 网络数据处理安全规范》（征求意见稿）指导下制定的实施指南类标准。

《中华人民共和国网络安全法》中第四十一条至第四十五条中，明确要求了对个人信息的保护和使用要求，网络支付服务运营者，收集使用大量个人信息，需要落实法律相关安全要求。

GB/T 35273—2020《信息安全技术 个人信息安全规范》提出了个人信息收集、存储、处理、使用等过程中的安全要求。网络支付服务领域是具体要求的执行者，对于如何满足规范的要求，需要具体落地的手段指导。

《信息安全技术 网络数据处理安全规范》（征求意见稿）提出了数据识别、分级分类、风险防控、审计追溯等方面提出数据处理总体要求。网络支付服务领域是具体要求的执行者，对于如何满足规范的要求，需要具体落地的手段指导。

八、重大分歧意见的处理经过和依据

无。

九、标准性质的建议

根据本标准的性质，建议本标准为推荐性标准。

十、贯彻标准的要求和措施建议

本文件适用于网络支付服务运营者规范数据活动，也适用于主管监管部门、第三方评估机构对网络支付服务数据活动进行监督、管理、评估时参考。

十一、替代或废止现行相关标准的建议

无。

十二、其它应予说明的事项

无。

《信息安全技术 网络支付服务数据安全指南》编制工作组

2021年2月1日