



中华人民共和国国家标准

GB/T 29841.3—2013

卫星定位个人位置信息服务系统 第3部分：信息安全规范

Satellite positioning personal position information service system (PPISS)—
Part 3: Information security specification

2013-11-12 发布

2014-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号和缩略语	2
4.1 符号	2
4.2 缩略语	3
5 信息安全系统参考模型	3
5.1 基本组成	3
5.2 业务功能	4
5.3 参考接口	4
6 信息安全系统运行机制	5
6.1 密码体制	5
6.2 密钥管理机制	8
6.3 设备认证机制	9
6.4 数据加密机制	12
6.5 加密机制启动	12
7 信息安全系统接口规程	13
7.1 概述	13
7.2 接口点	13
7.3 信息帧类型	15
7.4 信息帧处理规程	16
8 信息安全系统报文定义	19
8.1 概述	19
8.2 本地报文定义	19
8.3 端端报文定义	21

前 言

GB/T 29841《卫星定位个人位置信息服务系统》目前分为以下 4 个部分：

- 第 1 部分：功能描述；
- 第 2 部分：终端与服务中心信息交换协议；
- 第 3 部分：信息安全规范；
- 第 4 部分：终端通用规范。

本部分为 GB/T 29841 的第 3 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由中华人民共和国工业和信息化部提出。

本部分由中国电子技术标准化研究院归口。

本部分起草单位：南京联慧通信技术有限公司、厦门雅迅网络股份有限公司、中国电子技术标准化研究院、熊猫电子集团有限公司。

本部分主要起草人：牟中平、韦昌荣、赵安、赵志旺、陈倩、唐洁。

卫星定位个人位置信息服务系统

第3部分：信息安全规范

1 范围

GB/T 29841 的本部分规定了卫星定位个人位置信息服务系统(以下简称系统)中信息安全系统的参考模型、运行机制、接口规程及报文定义。

本部分适用于采用卫星定位、公众移动通信网络、具有信息服务中心和信息安全要求的系统,可作为系统信息安全功能设计的依据。采用非卫星定位技术、专用移动通信网络、具有信息服务中心和信息安全要求的系统亦可参照执行。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 29841.1—2013 卫星定位个人位置信息服务系统 第1部分:功能描述

GB/T 29841.2—2013 卫星定位个人位置信息服务系统 第2部分:终端与服务中心信息交换协议

GB/T 29841.4—2013 卫星定位个人位置信息服务系统 第4部分:终端通用规范

3 术语和定义

GB/T 29841.1—2013、GB/T 29841.2—2013 和 GB/T 29841.4—2013 中界定的以及下列术语和定义适用于本文件。

3.1

信息安全 infomation security

卫星定位个人位置信息服务系统中面向个人终端和信息服务中心所实现的设备认证、传输数据保密、密钥管理等功能的总称。

3.2

信息安全规程 infomation security protocol

卫星定位个人位置信息服务系统中实现设备认证、传输数据保密、密钥管理等功能的方法、流程及规则。

3.3

信息安全系统 infomation security system

卫星定位个人位置信息服务系统中实现信息安全规程的硬件和软件的实体。

3.4

终端安全保密实体 security and crypto entity of personal terminal

个人位置终端(PT)中依据信息安全机制实现加密、解密、密钥管理、中心认证及访问控制等功能的软件和硬件。