ICS 35.100.30
L 78

中华人民共和国国家标准

GB/T 17963—2000
idt ISO/IEC 11577:1995

信息技术　开放系统互连
网络层安全协议

Information technology—Open Systems Interconnection
—Network layer security protocol

2000-01-03 发布　　2000-08-01 实施

国家质量技术监督局　发布

目　　次

前　言

本标准等同采用国际标准 ISO/IEC 11577:1995《信息技术　开放系统互连　网络层安全协议》。

为适应信息处理的需要，本标准依据 OSI 参考模型的层次结构和 GB/T 15274 定义的网络层组织规定了网络层安全协议。本标准无论在技术内容上还是在编排格式上均与国际标准保持一致。

本标准的附录 A、附录 B、附录 C、附录 D 都是标准的附录；附录 E、附录 F、附录 G、附录 H 都是提示的附录。

本标准由中华人民共和国信息产业部提出。

本标准由中国电子技术标准化研究所归口。

本标准起草单位：西安交通大学、中国电子技术标准化研究所。

本标准主要起草人：邓良松、冯惠、邓秦、丁峰。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)是世界性的标准化专门机构。国家成员体(他们都是 ISO 或 IEC 的成员国)通过国际组织建立的各个技术委员会参与制定针对特定技术范围的国际标准,ISO 和 IEC 的各技术委员会在共同感兴趣的领域内进行合作。与 ISO 和 IEC 有联系的其他官方和非官方国际组织也可参与国际标准的制定工作。

对于信息技术领域,ISO 和 IEC 建立了一个联合技术委员会,即 ISO/IEC JTC1。由联合技术委员会提出的国际标准草案需分发给国家成员体进行表决。发布一个国际标准,至少需要 75%的参与表决的国家成员体投票赞成。

国际标准 ISO/IEC 11577 是由 ISO/IEC JTC1"信息技术"联合技术委员会、SC6"系统间远程通信和信息交换"分技术委员会与 ITU-T 合作制定的,该文本也以 ITU-T 建议 X.273 发布。

注:由于本国际标准最终版本编辑日期的缘故,在本国际标准引用的 ISO/IEC 7498-1、ISO/IEC 9646-1、ISO/IEC 9646-2、ISO/IEC 10731、ISO/IEC 10745 和 ISO/IEC TR 13594 的出版日期不同于相同的 ITU 建议 X.273 中引用的这些标准的出版日期。

附录 A 到附录 D 是本国际标准的组成部分。附录 E 到附录 H 仅提供参考信息。

引　　言

本标准定义的协议提供安全服务以支持较低层实体间的通信实例。本协议由 GB/T 9387.1～9387.2 中定义的层次结构和 GB/T 15274 中定义的网络层组织相对其他标准来定位，并按照 ISO/IEC TR 13597(低层安全模型)来扩展。它提供连接方式和无连接方式网络服务的安全服务支持，尤其，本协议位于网络层，在其上边界处和下边界处有功能接口和定义清晰的服务接口。

为了评价特定实现的一致性，需要有对给定 OSI 协议已实现的能力和选项的声明，这种声明称为协议实现一致性声明(PICS)。

中华人民共和国国家标准

信息技术　开放系统互连　网络层安全协议

GB/T 17963—2000
idt ISO/IEC 11577:1995

Information technology—Open Systems Interconnection—Network layer security protocol

1　范围

本标准规定的协议将由端系统和中间系统使用，以在网络层提供安全服务，而网络层由GB/T 15126和GB/T 15274定义。本标准中定义的协议称为网络层安全协议(NLSP)。

本标准规定：

a) 支持GB/T 9387.2中定义的下列安全服务：

1) 对等实体鉴别；

2) 数据原发鉴别；

3) 访问控制；

4) 连接保密性；

5) 无连接保密性；

6) 通信流量保密性；

7) 无恢复的连接完整性(包括数据单元完整性，其中连接上的各个SDU具有完整性保护)；

8) 无连接完整性。

b) 声称与本标准一致的实现的功能要求。

本协议的规程根据下列定义：

1) 可用于本协议实例的加密技术的要求；

2) 用于通信实例安全联系中携带信息的要求。

尽管一些安全机制提供的保护程度取决于一些特定加密技术，而本协议的正确操作并不取决于某种特定的加密或解密算法的选择。这是通信系统的本地事情。

此外，特定的安全策略的选择和实现都不在本标准的范围之内。特定的安全策略的选择以及因此将达到的保护程度，留作使用安全通信的单个实例的系统之间的本地事情。本标准不要求涉及同一开发系统的多个安全通信的实例必须采用相同的协议。

附录D按照ISO/IEC 9646-2中给出的相关指导为网络层协议提供了PICS形式表。

2　引用标准

下列标准包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 9387.1—1998　信息技术　开放系统互连　基本参考模型　第1部分：基本模型(idt ISO/IEC 7498-1:1994)

GB/T 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分：安全体系结构

国家质量技术监督局2000-01-03批准　　2000-08-01实施