UDC 681.3.06:003.26
L 80

中华人民共和国国家标准

GB/T 15278—94

信息处理　数据加密　物理层互操作性要求

Information processing—Data encipherment—Physical layer interoperability requirements

1994-12-07发布　　1995-08-01实施

国家技术监督局　发布

中华人民共和国国家标准

信息处理　数据加密　物理层互操作性要求

GB/T 15278—94

Information processing—Data encipherment—Physical layer interoperability requirements

本标准等效采用国际标准 ISO 9160—1988《信息处理——数据加密——物理层互操作性要求》。

本标准规定了在传送自动数据处理(ADP)信息的远程通信系统中，开放系统互连(OSI)参考模型的物理层采用加密的互操作性和安全性的有关要求。

本标准便于要求密码保护的数据通信设备和系统中使用的数据加密设备互操作的实现。

物理层加密的目的是对抗包括业务分析在内的所有形式的被动攻击。只有在同步操作中才能提供彻底对抗业务分析的保护，这是因为在同步操作中所有比特均可加密，而在异步操作中起始和停止比特不可加密。本标准不提供对物理连接建立的保护。

1　主题内容与适用范围

本标准适用于在数据通信物理层中加密 ADP 信息的系统。

无论数据加密设备(DEE)是作为物理上独立的设备实现，还是作为数据终端设备(DTE)或作为数据电路终接设备(DCE)的一部分实现，本标准均可同等适用。当加密部分集成到 DTE 或 DCE 中时，本标准适用于 DTE 或 DCE 设计中实现本标准要求的那些部分。本标准的互操作性要求是为下述物理接口定义规定的：GB 3454、GB 11592、GB 11593、GB 11599 和 GB 11600。

GB 9387 中描述了物理层。在物理层加密中，所有的 SDU(服务数据单元)通常都被加密。本标准所描述的互操作性要求对全双工方式和半双工方式中的同步操作和异步操作均适用。

本标准的正文规定了适用于使用各种加密算法的要求。附录 B(参考件)举例说明使用一个 64 bit 分组密码算法的附加要求。

本标准规定了同步操作的两种可选方式：延迟选项和立即选项。这两种方式互不兼容。

本标准还规定了对异步操作中断(BREAK)的两种可选动作：A 类和 B 类。这两种动作互不兼容。

2　引用标准

GB 5271.9　数据处理　词汇　09 部分　数据通信

GB 9387　信息处理系统　开放系统互连　基本参考模型

GB/T 15277　信息处理　64 bit 分组密码算法的工作方式

GB 3454　CCITT 建议 V.24　数据终端设备(DTE)和数据电路终接设备(DCE)之间的接口电路定义表

GB 11592　CCITT 建议 X.20　公用数据网上起/止传输业务使用的数据终端设备(DTE)和数据电路终接设备(DCE)间的接口

GB 11593　CCITT 建议 X.21　公用数据网上同步工作的数据终端设备(DTE)和数据电路终接设备(DCE)间的接口

国家技术监督局 1994-12-07 批准　　1995-08-01 实施