附件：

信息安全等级保护
商用密码技术实施要求

国家密码管理局

2009 年

目　录

引　言

密码技术作为信息安全的基础性核心技术，是信息保护和网络信任体系建设的基础，是实行信息安全等级保护不可或缺的关键技术，充分利用密码技术能够有效地保障信息安全等级保护制度的落实，科学合理地采用密码技术及其产品，是落实信息安全等级保护最为有效、经济和便捷的手段。

国家标准《GB/T 22239－2008 信息安全技术 信息系统安全等级保护基本要求》（以下简称“《基本要求》”）规定了对不同安全保护等级信息系统的基本安全要求，对于涉及到身份的真实性、行为的抗抵赖、内容的机密性和完整性的要求项，密码技术都可以直接或间接地为满足这些要求提供支持，因此如何科学合理地应用密码技术对信息系统进行安全保护就成为实施等级保护的关键工作内容，直接影响着信息安全等级保护的全面推进。为此，我们以《商用密码管理条例》和《信息安全等级保护商用密码管理办法》为指导，结合《基本要求》中的相关安全要求项，在《信息安全等级保护商用密码技术要求》的基础上，编制了《信息安全等级保护商用密码技术实施要求》，用以规范使用商用密码实施等级保护的相关技术工作，并为商用密码产品的研发和系统的集成提供依据。

本要求明确了一、二、三、四级信息系统使用商用密码技术来实施等级保护的基本要求和应用要求。在基本要求中根据密码技术的特点，从技术实施上对商用密码应用系统的功能、密钥管理、密码配用、密码实现和密码保护等方面提出了相关要求和规定。在应用要求中，从应用密码技术来实现相应等级的物理安全、网络安全、主机安全、应用安全和数据安全提出了要求。为方便使用，我们将各级信息系统的商用密码需求和相关技术实施要求按照不同安全等级集中进行编排。

第一章　第一级信息系统商用密码技术实施要求

1.1　商用密码技术基本要求

1.1.1　功能要求

1.1.1.1　真实性

第一级信息系统使用商用密码进行真实性保护时，应提供以下功能：

1）　提供基于实体的身份标识和鉴别服务；

2）　为访问网络设备提供身份鉴别服务；

3）　为登录操作系统和数据库提供身份鉴别服务；

4）　为访问应用系统提供身份鉴别服务；

5）　向访问控制系统提供身份真实性的凭证。

1.1.1.2　完整性

第一级信息系统使用商用密码进行完整性保护时，应提供以下功能：

1）　应提供数据完整性校验服务；

2）　为通信过程和数据传输提供完整性校验服务；

3）　为访问控制系统提供访问控制信息的完整性校验服务。

1.1.2　密钥管理要求

密钥管理至少应包括密钥的生成、存储和使用等过程，并满足：

1）　密钥生成：密钥应具有一定的随机性；

2）　密钥存储：采取必要的安全防护措施，防止密钥被轻易非授权获取；

3）　密钥使用：采取必要的安全防护措施，防止密钥被非法使用。

1.1.3　密码配用策略要求

采用国家密码管理部门批准使用的算法。

1.1.4　密码实现机制要求

不做强制性要求。

1.1.5　密码安全防护要求

不做强制性要求。

1.2　商用密码技术应用要求

1.2.1　物理安全

第一级物理安全基本技术要求的实现不需使用密码技术。

1.2.2　网络安全

实现第一级网络安全基本技术要求在访问控制和身份鉴别方面可以使用密码技术。

在访问控制机制中，可以使用密码技术的完整性服务来保证访问控制列表的完整性。

在身份鉴别机制中，可以使用密码技术的真实性服务来实现鉴别信息的防假冒，可以使用密码技术的机密性服务来实现鉴别信息的防泄露。

1.2.3　主机安全

实现第一级主机安全基本技术要求在身份鉴别和访问控制方面可以使用密码技术。

在身份鉴别机制中，可以使用密码技术的真实性服务来实现鉴别信息的防假冒。

在访问控制机制中，可以使用密码技术的完整性服务来保证访问控制信息的完整性。

1.2.4　应用安全

实现第一级应用安全基本技术要求在身份鉴别、访问控制和通信安全方面可以使用密码技术。

在身份鉴别机制中，可以使用密码技术的真实性服务来实现鉴别信息的防假冒，保证应用系统用户身份的真实性。

在访问控制机制中，可以使用密码技术的完整性服务来保证系统功能和用户数据访问控制信息的完整性。

在通信安全方面，可以使用密码技术的完整性服务来实现对通信过程中数据完整性。

1.2.5　数据安全及备份恢复

第一级数据安全及备份恢复基本技术要求在数据传输安全方面，可以使用密码技术的完整性服务来实现对重要用户数据在传输过程中完整性检测。

第二章　第二级信息系统商用密码技术实施要求

2.1　商用密码技术基本要求

2.1.1　功能要求

2.1.1.1　真实性

第二级信息系统使用商用密码进行真实性保护时，应提供以下功能：

1）　提供基于单个实体的身份鉴别功能；

2）　能唯一标识并有效区分实体，包括用户、设备、系统等；

3）　为建立网络会话提供身份鉴别服务；

4） 为访问网络设备提供身份鉴别服务；

5） 保证身份鉴别信息的唯一性；

6） 向访问控制系统提供身份真实性的凭证。

2.1.1.2 机密性

第二级信息系统使用商用密码进行机密性保护时，应提供以下功能：

1） 提供数据机密性服务；

2） 为初始化会话过程中提供加密保护；

3） 对通信过程中的重要字段提供加密保护；

4） 对存储的鉴别信息提供加密保护。

2.1.1.3 完整性

第二级信息系统使用商用密码进行完整性保护时，应提供以下功能：

1） 对鉴别信息和重要业务数据在传输过程中提供完整性校验服务；

2） 对系统资源的访问控制信息提供完整性校验服务；

3） 对文件/数据库表等客体的访问控制信息提供完整性校验服务；

4） 对审计记录提供完整性校验服务。

2.1.2 密钥管理要求

密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、更换等过程，并满足：

1） 密钥生成：应使用随机数发生器产生密钥；

2） 密钥存储：密钥应加密存储，并采取必要的安全防护措施，防止密钥被非法获取。

3） 密钥分发：密钥分发应采取有效的安全措施，防止在分发过程中泄露。

4） 密钥导入与导出：密钥的导入与导出应采取有效的安全措施，保证密钥的导入与导出安全，以及密钥的正确。

5） 密钥使用：密钥必须明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换；应按照密钥更换周期要求更换密钥，密钥更换允许系统中断运行。

6） 密钥备份与恢复：应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复。

2.1.3 密码配用策略要求

2.1.3.1 密码算法配用策略

采用国家密码管理部门批准使用的算法。

2.1.3.2　密码协议使用策略

采用经国家密码管理部门安全性评审的密码协议实现密码功能。

2.1.3.3　密码设备使用策略

使用密码设备时应符合以下要求：

1)　应选用国家密码管理部门批准的密码设备；

2)　信源加密、完整性校验、身份鉴别应选用智能密码钥匙、智能 IC 卡、可信密码模块 TCM、密码卡、密码机等密码设备；

3)　信道加密应选用链路密码机、网络密码机、VPN 密码机等密码设备。

2.1.4　密码实现机制

应采用专用固件或硬件方式实现。

2.1.5　密码安全防护要求

密码安全防护应符合以下要求：

1)　专用固件或硬件应具有有效的物理安全保护措施；

2)　专用固件或硬件应满足相应运行环境的可靠性要求。

2.2　商用密码技术应用要求

2.2.1　物理安全

实现第二级物理安全基本技术要求不需使用密码技术。

2.2.2　网络安全

实现第二级网络安全基本技术要求在访问控制和身份鉴别方面推荐使用密码技术。

在访问控制方面，推荐使用密码技术的完整性服务来保证网络边界访问控制信息、系统资源访问控制信息的完整性。

在身份标识与鉴别方面，推荐使用密码技术的真实性服务来实现鉴别信息的防重用和防冒用，保证网络设备用户身份的真实性；推荐使用密码技术的机密性服务来保证网络设备远程管理时，鉴别信息传输过程中的机密性。

2.2.3　主机安全

实现第二级主机安全基本技术要求在身份鉴别、访问控制和审计记录方面推荐使用密码技术。

在身份鉴别方面，推荐使用密码技术的真实性服务来实现鉴别信息的防冒用和防重用，保证操作系统和数据库系统用户身份的真实性；推荐使用密码技术的机密性服务来

实现鉴别信息远程传输过程中的机密性。

在访问控制方面，推荐使用密码技术的完整性服务来保证系统资源访问控制信息的完整性。

在审计记录方面，推荐使用密码技术的完整性服务来对审计记录进行完整性保护。

2.2.4　应用安全

实现第二级应用安全基本技术要求在身份鉴别、访问控制、审计记录和通信安全方面推荐使用密码技术。

在身份鉴别方面，推荐使用密码技术的真实性服务来实现鉴别信息的防重用和防冒用，保证应用系统用户身份的真实性和通信双方身份的真实性。

在访问控制方面，推荐使用密码技术的完整性服务来保证文件、数据库表等客体访问控制信息的完整性。

在审计记录方面，推荐使用密码技术的完整性服务来保证审计记录的完整性，防止对审计记录的非法修改。

在通信安全方面，推荐使用密码技术的完整性服务来保证通信过程中数据的完整性；推荐使用密码技术的机密性服务来对通信过程中敏感数据加密，保证通信过程中敏感信息的机密性。

2.2.5　数据安全及备份恢复

实现第二级数据安全及备份恢复基本技术要求在数据传输安全和数据存储安全方面可以使用密码技术。

在数据传输安全方面，推荐使用密码技术的完整性服务来实现对鉴别信息和重要业务数据在传输过程中完整性检测。

在数据存储安全方面，推荐使用密码技术的机密性服务来实现鉴别信息的存储机密性。

第三章　第三级信息系统商用密码技术实施要求

3.1　商用密码技术基本要求

3.1.1　功能要求

3.1.1.1　真实性

第三级信息系统使用商用密码进行真实性保护时，应提供以下功能：

1）　提供重要区域进入人员身份真实性鉴别服务；

2） 提供安全访问路径中通信主体身份的真实性鉴别服务；

3） 提供访问网络设备用户身份的真实性鉴别服务；

4） 提供登录操作系统和数据库系统用户的身份真实性的鉴别服务；

5） 提供应用系统用户身份真实性鉴别服务；

6） 提供通信双方身份真实性鉴别服务；

7） 能够提供组合鉴别方式；

8） 在建立网络会话时提供身份鉴别服务；

9） 保证身份鉴别信息的唯一性；

10） 向访问控制系统提供身份真实性的凭证。

3.1.1.2 机密性

第三级信息系统使用商用密码进行机密性保护时，应提供以下功能：

1） 提供通信过程中整个报文或会话过程的机密性保护服务；

2） 提供存储过程中系统管理数据、鉴别信息和重要业务数据的机密性保护服务；

3） 提供传输过程中系统管理数据、鉴别信息和重要业务数据的机密性保护服务。

3.1.1.3 完整性

第三级信息系统使用商用密码进行完整性保护时，应提供以下功能：

1） 提供电子门禁系统记录的完整性服务；

2） 提供安全访问路径中路由信息的完整性服务；

3） 提供网络边界和系统资源访问控制信息的完整性服务；

4） 提供审计记录的完整性服务；

5） 提供系统资源访问控制信息的完整性服务；

6） 提供重要信息资源敏感标记的完整性服务；

7） 提供重要程序的完整性服务；

8） 提供文件、数据库表等客体访问控制信息的完整性服务；

9） 提供重要信息资源敏感标记的完整性服务；

10） 提供通信过程中所有数据的完整性服务；

11） 提供存储过程中系统管理数据、鉴别信息和重要业务数据的完整性服务。

3.1.1.4 抗抵赖性

第三级信息系统使用商用密码进行抗抵赖保护时，应提供以下功能：

1） 提供进入重要区域人员行为的抗抵赖服务；

2） 支持原发抗抵赖服务；

3） 支持接收抗抵赖服务。

3.1.2 密钥管理要求

密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档和销毁等环节进行管理和策略制定的全过程，并满足：

1） 密钥生成：应使用国家密码管理部门批准的硬件物理噪声源产生随机数；密钥必须在密码设备内部产生，不得以明文方式出现在密码设备之外；应具备检查和剔除弱密钥的能力。

2） 密钥存储：密钥应加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥应存储在专用硬件中。

3） 密钥分发：密钥分发应采取身份鉴别、数据完整性、数据机密性等安全措施，应能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

4） 密钥导入与导出：密钥的导入与导出应采取有效的安全措施，保证密钥的导入与导出安全，以及密钥的正确。

5） 密钥使用：密钥必须明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换；应按照密钥更换周期要求更换密钥，密钥更换允许系统中断运行；密钥泄露时，必须停止使用，并启动相应的应急处理和响应措施。

6） 密钥备份与恢复：应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

7） 密钥归档：应采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档应进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥应进行数据备份，并采用有效的安全保护措施。

8） 密钥销毁：应具有在紧急情况下销毁密钥的措施。

3.1.3 密码配用策略要求

3.1.3.1 密码算法配用策略

采用国家密码管理部门批准使用的算法。

3.1.3.2 密码协议使用策略

采用经国家密码管理部门安全性评审的密码协议实现密码功能。

3.1.3.3　密码设备使用策略

使用密码设备时应符合以下要求：

1）　应选用国家密码管理部门批准的密码设备；

2）　信源加密、完整性校验、身份鉴别、抗抵赖应选用可信密码模块 TCM、智能密码钥匙、智能 IC 卡、密码卡、密码机等密码设备；

3）　信道加密应选用链路密码机、网络密码机、VPN 密码机等密码设备；

4）　需要配用独立的密钥管理系统或使用数字证书认证系统提供的密钥管理服务。

3.1.4　密码实现机制

必须采用专用固件或硬件方式实现。

3.1.5　密码安全防护要求

密码安全防护应符合以下要求：

1）　专用固件或硬件以及密码设备应具有有效的物理安全保护措施；

2）　专用固件或硬件以及密码设备应满足相应运行环境的可靠性要求；

3）　应建立有效的密码设备安全管理制度。

3.2　商用密码技术应用要求

3.2.1　物理安全

第三级物理安全基本技术要求在电子门禁系统方面推荐使用密码技术。

在电子门禁系统中，推荐使用密码技术的真实性服务来保护身份鉴别信息，保证重要区域进入人员身份的真实性；推荐使用密码技术的完整性服务来保证电子门禁系统进出记录的完整性。

3.2.2　网络安全

第三级网络安全基本技术要求在安全访问路径、访问控制和身份鉴别方面应当使用密码技术。

在建立安全访问路径过程中，应当使用密码技术的真实性服务来保证通信主体身份鉴别信息的可靠，实现安全访问路径中通信主体身份的真实性；应当使用密码技术的完整性服务来保证安全访问路径中路由控制信息的完整性。

在访问控制机制中，应当使用密码技术的完整性服务来保证网络边界和系统资源访问控制信息的完整性。

在审计记录方面，应当使用密码技术的完整性服务来对审计记录进行完整性保护。

在身份标识与鉴别方面，应当使用密码技术来实现组合鉴别，使用密码技术的机密性和真实性服务来实现防窃听、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备用户身份的真实性。

3.2.3　主机安全

第三级主机安全基本技术要求在身份鉴别、访问控制、审计记录和程序安全方面应当使用密码技术。

在身份标识与鉴别方面，应当使用密码技术来实现组合鉴别，使用密码技术的真实性服务来实现鉴别信息的防假冒和防重用，保证操作系统和数据库系统用户身份的真实性，并在远程管理时使用密码技术的机密性服务来实现鉴别信息的防窃听。

在访问控制方面，应当使用密码技术的完整性服务来保证系统资源访问控制信息的完整性，并使用密码技术的完整性服务来保证重要信息资源敏感标记的完整性。

在审计记录方面，应当使用密码技术的完整性服务来对审计记录进行完整性保护。

在程序安全方面，推荐使用密码技术的完整性服务来实现对重要程序的完整性检测。

3.2.4　应用安全

第三级应用安全基本技术要求在身份鉴别、访问控制、审计记录和通信安全方面应当使用密码技术。

在身份鉴别方面，应当使用密码技术来实现组合鉴别，使用密码技术的机密性和真实性服务来实现防窃听、防假冒和防重用，保证应用系统用户身份的真实性。

在访问控制方面，应当使用密码技术的完整性服务来保证文件、数据库表访问控制信息和重要信息资源敏感标记的完整性。

在审计记录方面，应使用密码技术的完整性服务来实现对审计记录完整性的保护。

在通信安全方面，应当使用密码技术的完整性服务来保证通信过程中数据完整性；应当使用密码技术的真实性服务来实现通信双方会话初始化验证；应当使用密码技术的机密性服务来实现对通信过程中整个报文或会话过程加密保护；应当使用密码技术的抗抵赖服务来提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

3.2.5　数据安全及备份恢复

第三级数据安全及备份恢复基本技术要求在数据传输安全和数据存储安全方面应当使用密码技术。

在数据传输安全方面，应当使用密码技术的完整性服务来实现对系统管理数据、鉴别

信息和重要业务数据在传输过程中完整性的检测。应当使用密码技术的机密性服务来实现系统管理数据、鉴别信息和重要业务数据的传输机密性。

在数据存储安全方面，应当使用密码技术的完整性服务来实现对系统管理数据、鉴别信息和重要业务数据在存储过程中完整性的检测。应当使用密码技术的机密性服务来实现系统管理数据、鉴别信息和重要业务数据的存储机密性。

第四章　第四级信息系统商用密码技术实施要求

4.1　商用密码技术基本要求

4.1.1　功能要求

4.1.1.1　真实性

第四级信息系统使用商用密码进行真实性保护时，应提供以下功能：

1）　应提供基于单个实体(用户、主机)的身份鉴别功能；

2）　能唯一标识并有效区分实体，包括用户、设备、系统等；

3）　能够提供两种或两种以上的身份鉴别方式；

4）　身份鉴别信息具备不易被冒用的防范能力；

5）　身份鉴别信息具备不可伪造性；

6）　保证身份鉴别信息的唯一性；

7）　提供进入重要区域人员身份真实性鉴别服务；

8）　在建立网络会话时提供身份鉴别服务；

9）　提供安全访问路径中通信主体身份的真实性鉴别服务；

10）　提供通信双方身份真实性鉴别服务；

11）　支持在网络设备身份鉴别时提供身份鉴别服务；

12）　提供主机平台基于可信密码模块 TCM 的身份真实性鉴别服务；

13）　提供登录操作系统和数据库系统用户的身份真实性的鉴别服务；

14）　提供应用系统用户身份真实性鉴别服务；

15）　应向访问控制系统提供身份真实性的凭证。

4.1.1.2　机密性

第四级信息系统使用商用密码进行机密性保护时，应提供以下功能：

1）　能提供数据机密性服务；

2）　提供通信过程中整个报文或会话过程的机密性保护服务；

3） 提供存储过程中系统管理数据、鉴别信息和重要业务数据的机密性保护服务；

4） 提供传输过程中系统管理数据、鉴别信息和重要业务数据的机密性保护服务。

4.1.1.3 完整性

第四级信息系统使用商用密码进行完整性保护时，应提供以下功能：

1） 能够提供对数据的完整性保护；

2） 支持对重要信息资源敏感标记提供完整性服务；

3） 提供电子门禁系统记录的完整性服务；

4） 支持对通信过程数据提供完整性服务；

5） 提供安全访问路径中数据的完整性服务；

6） 提供网络边界和系统资源访问控制信息的完整性服务；

7） 提供系统资源访问控制信息的完整性服务；

8） 支持对系统管理数据、鉴别信息和业务数据在传输过程中提供完整性服务，并能够检测完整性错误，提供必要的恢复手段；

9） 支持对系统管理数据、鉴别信息和业务数据在存储过程中提供完整性服务，并能够检测完整性错误，提供必要的恢复手段；

10） 提供主机平台基于可信密码模块 TCM 的完整性服务；

11） 提供重要程序的完整性服务；

12） 提供文件、数据库表等客体访问控制信息的完整性服务；

13） 提供审计记录的完整性服务。

4.1.1.4 抗抵赖

第四级信息系统使用商用密码进行抗抵赖保护时，应提供以下功能：

1） 提供进入重要区域人员行为的抗抵赖服务；

2） 支持原发抗抵赖服务；

3） 支持接收抗抵赖服务。

4.1.2 密钥管理要求

密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档和销毁等环节进行管理和策略制定的全过程，并满足：

1） 密钥生成：应使用国家密码管理部门批准的硬件物理噪声源产生随机数；密钥必须在密码设备内部产生，不得以明文方式出现在密码设备之外；应具备检查和剔除弱密钥的能力；生成密钥审计信息，密钥审计信息包括：种类、长度、拥有者信息、使用起始时间、

使用终止时间。

2） 密钥存储：密钥应加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥应存储在专用硬件中；应具有密钥可能泄露时的应急处理和响应措施。

3） 密钥分发：密钥分发应采取身份鉴别、数据完整性、数据机密性等安全措施，应能够抗截获、假冒、篡改、重放等攻击，保证密钥的安全性。应具有密钥可能泄露时的应急处理和响应措施。

4） 密钥导入与导出：密钥的导入与导出应采取有效的安全措施，保证密钥的导入与导出安全，以及密钥的正确；密钥的导入与导出应采用密钥分量的方式或者专用设备的方式；密钥的导入与导出应保证系统密码服务功能不间断。

5） 密钥使用：密钥必须明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换；应按照密钥更换周期要求更换密钥，密钥更换允许系统中断运行；密钥泄露时，必须停止使用，并启动相应的应急处理和响应措施。

6） 密钥备份与恢复：应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

7） 密钥归档：应采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档应进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥应进行数据备份，并采用有效的安全保护措施。

8） 密钥销毁：应具有在紧急情况下销毁密钥的措施。

4.1.3 密码配用策略要求

4.1.3.1 密码算法配用策略

采用国家密码管理部门批准使用的算法。

4.1.3.2 密码协议使用策略

采用经国家密码管理部门安全性评审的密码协议实现密码功能。

4.1.3.3 密码设备使用策略

使用密码设备时应符合以下要求：

1） 应选用国家密码管理部门批准的密码设备；

2） 信源加密、完整性校验、身份鉴别、抗抵赖应选用可信密码模块 TCM、智能密码

钥匙、智能 IC 卡、密码卡、密码机等密码设备；

3） 信道加密应选用链路密码机、网络密码机、VPN 密码机等密码设备；

4） 需要配用独立的密钥管理系统或使用数字证书认证系统提供的密钥管理服务。

4.1.4 密码实现机制

必须采用专用硬件或固件方式实现。

4.1.5 密码安全防护要求

密码安全防护应符合以下要求：

1） 专用硬件或固件以及密码设备应具有严格的物理安全保护措施；

2） 专用硬件或固件以及密码设备应满足相应运行环境的可靠性要求；

3） 应建立严格的密码设备安全管理制度。

4.2 商用密码技术应用要求

4.2.1 物理安全

第四级物理安全基本技术要求在电子门禁系统方面应当使用密码技术。

在电子门禁系统中，应当使用密码技术的真实性服务来实现对进入重要区域人员的身份鉴别，并使用密码技术的完整性服务来保证电子门禁系统进出记录的完整性。

4.2.2 网络安全

第四级网络安全基本技术要求在安全访问路径、访问控制和身份鉴别方面应当使用密码技术。

在建立安全访问路径过程中，应当使用密码技术的真实性服务来保证通信主体身份鉴别信息的可靠，实现安全访问路径中通信主体身份的真实性应当使用密码技术的完整性服务来保证安全访问路径中路由控制信息的完整性。

在访问控制方面，应当使用密码技术的完整性服务来保证网络边界访问控制信息和数据敏感标记的完整性。

在审计记录方面，应当使用密码技术的完整性服务来对审计记录进行完整性保护。

在身份标识与鉴别方面，应当采用密码技术实现组合鉴别，使用密码技术的机密性和真实性服务来实现传输过程中鉴别信息防窃听、防假冒和防重用，保证网络设备用户身份的真实性。

4.2.3 主机安全

第四级主机安全基本技术要求在身份鉴别、访问控制、安全信息传输路径、审计记录和程序安全方面可以使用密码技术。

在身份鉴别方面，应当采用密码技术来实现组合鉴别，使用密码技术的真实性服务来实现鉴别信息的防假冒和防重用，并在远程管理时使用密码技术的机密性服务来实现鉴别信息的防窃听。

在访问控制方面，应当使用密码技术的完整性服务来保证细粒度访问控制信息的完整性和所有主体和客体敏感标记的完整性。

在审计记录方面，应当使用密码技术的完整性服务来实现对审计记录和重要程序的完整性检测。

4.2.4　应用安全

第四级应用安全基本技术要求在身份鉴别、访问控制、审计记录和通信安全方面应当使用密码技术。

在身份鉴别方面，应当采用密码技术来实现组合鉴别，使用密码技术的真实性和机密性服务来实现鉴别信息的防重用、防冒用、防泄露，保证应用系统用户身份的真实性

在访问控制方面，应使用密码技术的完整性服务来保证主体对客体访问控制信息和敏感标记的完整性。

在建立安全的信息传输路径过程中，应当使用密码技术的真实性服务来实现通信主体身份鉴别，并综合使用密码技术的机密性和完整性服务来建立安全通道。

在审计记录方面，应使用密码技术的完整性服务来对审计记录进行完整性保护。

在通信安全方面，应当使用密码技术的完整性服务来保证通信过程中数据完整性；应当使用密码技术的真实性服务来实现通信双方会话初始化验证；应当使用密码技术的机密性服务来实现对通信过程中整个报文或会话过程加密保护；应当使用密码技术的抗抵赖服务来提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

4.2.5　数据安全及备份恢复

第四级数据安全及备份恢复基本技术要求在数据传输安全、数据存储安全和安全通信协议方面应当使用密码技术。

在数据传输安全方面，应使用密码技术的完整性服务来实现对系统管理数据、鉴别信息和重要业务数据在传输过程中完整性的检测；应使用密码技术的机密性服务来实现系统管理数据、鉴别信息和重要业务数据的传输机密性。

在数据存储安全方面，应使用密码技术的完整性服务来实现对系统管理数据、鉴别信息和重要业务数据在存储过程中完整性的检测；应使用密码技术的机密性服务来实现系

统管理数据、鉴别信息和重要业务数据的存储机密性。

在安全通信协议方面，应综合使用密码技术的真实性、完整性和机密性服务来建立安全通信协议。