ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29241—2012

信息安全技术　公钥基础设施
PKI 互操作性评估准则

Information security technology—Public key infrastructure—PKI interoperability evaluation criteria

2012-12-31 发布　　2013-06-01 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

本标准按照 GB/T 1.1—2009 规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国科学院数据与通信保护研究教育中心、赞嘉电子科技(北京)有限公司。

本标准主要起草人:荆继武、马存庆、林璟锵、查达仁、吴晶晶、张帆、王平建。

引　言

PKI 系统作为普适性的安全基础设施，同时为各种不同的应用提供安全服务。通过 PKI 提供的安全服务信息，PKI 应用可以获得真实性、保密性、完整性、非否认等安全服务。

由于 PKI 系统的设计建设和运行维护所依据的标准和规范具有较大的灵活性和可选自由度，应用从 PKI 系统获得的服务数据也就具有一定的不确定性。证书私有扩展大量使用和证书策略意义不明确、撤销状态信息不全面等问题，都会影响安全服务的使用，甚至导致应用无法获得安全服务。上述问题，对于跨域的 PKI 事务尤为突出。由于跨域的 PKI 应用和 PKI 系统通常由不同的厂商或设计开发人员实现，双方对于各种服务数据的理解和使用不一致更加明显，导致二者之间难以互操作，难以获取安全服务。

当 PKI 系统进行互联互通时，就必须考虑 PKI 系统为跨域 PKI 应用提供安全服务信息的水平，也就是 PKI 系统与 PKI 应用之间的互操作问题。为更多的跨域应用提供全面的安全服务信息，是 PKI 系统进行互操作能力优化和改进的目标。如果 PKI 系统仅限于为特定的少数 PKI 应用提供服务，那么该 PKI 系统则难以在互联互通中发挥效用。作为一种安全基础设施，PKI 系统应该面向各种应用，采取有效的办法提高互操作能力，为网络通信做好全面的安全基础。另一方面，用户会希望自己的 PKI 应用能够与更多的 PKI 系统互操作，有能力从不同的电子认证服务机构获得安全服务。

本标准考虑了 PKI 安全服务相关的各种信息及其性能。PKI 系统提供安全服务的方式是生成各种证书的相关信息，包括：证书、证书撤销状态信息、证书策略和认证业务声明等。PKI 应用就是利用上述信息获得安全服务。安全服务信息的格式是否正确设置、内容是否明确表达、功能体现是否完善、操作过程是否按标准化执行、信息来源是否可靠等问题，都会影响安全服务的提供。

本标准分别从 PKI 系统和 PKI 应用 2 个方面，提出了分等级的互操作性评估准则。高等级的 PKI 系统，能够为更多的 PKI 应用提供更全面可靠的安全服务。高等级的 PKI 应用，能够从更多的 PKI 系统中获取更全面的安全服务。

本标准通过分等级的互操作评估，为 PKI 系统和 PKI 应用都指出了改进的方向，将促进建设和开发具有全面互操作能力的 PKI 系统和应用，从而为 PKI 系统的全面互联互通，为最终形成统一的认证体系，奠定坚实的基础。

信息安全技术　公钥基础设施
PKI 互操作性评估准则

1　范围

本标准规定了 PKI 系统和 PKI 应用的五个互操作能力等级，完成了分等级的 PKI 互操作性评估准则，为 PKI 系统和 PKI 应用提供了互操作能力等级评估的依据。

本标准适用于需要进行跨域互操作的 PKI 系统和 PKI 应用，可用于 PKI 系统和 PKI 应用的设计、开发、制造、采购、测试、评估、使用等过程。

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 16264.8—2005　信息技术　开放系统互连　目录　第 8 部分：公钥和属性证书框架

GB/T 19713—2005　信息技术　安全技术　公钥基础设施　在线证书状态协议

GB/T 20518—2006　信息安全技术　公钥基础设施　数字证书格式

GM/T 0003—2012　SM2 椭圆曲线公钥密码算法

GM/T 0004—2012　SM3 密码杂凑算法

RFC 3647　因特网 X.509 公钥基础设施：证书策略和认证业务框架(Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework)

RFC 3709　因特网 X.509 公钥基础设施：X.509 证书中的徽标(Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates)

RFC 3779　用于 IP 地址和 AS 标识符的 X.509 证书扩展(X.509 Extensions for IP Addresses and AS Identifiers)

RFC 4059　因特网 X.509 公钥基础设施：担保信息证书扩展(Internet X.509 Public Key Infrastructure: Warranty Certificate Extension)

RFC 4334　支持点对点协议(PPP)和无线局域网(WLAN)鉴别的证书扩展和属性[Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)]

RFC 4387　因特网 X.509 公钥基础设施操作协议：通过 HTTP 访问证书存储(Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP)

RFC 4523　用于 X.509 证书的轻量级目录访问协议(LDAP)模式定义(Lightweight Directory Access Protocol(LDAP) Schema Definitions for X.509 Certificates)

RFC 5280　因特网 X.509 公钥基础设施：证书和证书撤销列表(CRL)概要(Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile)

3　术语和定义

GB/T 16264.8—2005 界定的以及下列术语和定义适用于本文件。

3.1

PKI 系统　PKI system

提供证书的颁发以及相关服务的软硬件设备和人员的总称。

3.2

PKI 应用　PKI application

使用数字证书以及相关信息、获得安全服务的软硬件系统。

3.3

PKI 应用管理者　administrator of PKI application

配置、控制、操作和使用 PKI 应用的人员。

3.4

PKI 互操作性能　PKI interoperability

两个以上(含)PKI 系统或 PKI 应用正确地交互和使用证书以及相关安全信息的性能。

3.5

完全互操作 PKI 系统　fully interoperable PKI system

概念性的 PKI 系统,能够与所有 PKI 应用实现完全的互操作。

3.6

完全互操作 PKI 应用　fully interoperable PKI application

概念性的 PKI 应用,能够与所有 PKI 系统实现完全的互操作。

3.7

PKI 互操作能力等级　PKI interoperability level

特定 PKI 系统与完全 PKI 应用的 PKI 互操作性能的量化结果,或者是特定 PKI 应用与完全 PKI 系统的 PKI 互操作性能的量化结果。

4　缩略语

下列缩略语适用于本文件。

BER　基本编码规则 (Basic Encoding Rules)
CA　证书认证机构 (Certificate Authority)
CP　证书策略 (Certificate Policy)
CPS　认证业务声明 (Certification Practice Statement)
CRL　证书撤销列表 (Certificate Revocation List)
DER　可辨别编码规则 (Distinguished Encoding Rules)
DN　可辨别名称 (Distinguished Name)
F-APP　完全互操作 PKI 应用 (Fully interoperable PKI Application)
F-SYS　完全互操作 PKI 系统 (Fully interoperable PKI System)
HTTP　超文本传输协议 (Hyper Text Transfer Protocol)
IOL　互操作能力等级 (Interoperability Level)
IOL1　互操作能力第一级 (Interoperability Level 1)
IOL2　互操作能力第二级 (Interoperability Level 2)
IOL3　互操作能力第三级 (Interoperability Level 3)
IOL4　互操作能力第四级 (Interoperability Level 4)
IOL5　互操作能力第五级 (Interoperability Level 5)
LDAP　轻量级目录访问协议 (Lightweight Directory Access Protocol)

OCSP　在线证书状态协议（Online Certificate Status Protocol）
OID　对象标识符（Object Identifier）
RDN　相对可辨别名称（Relative Distinguished Name）
TOE　评估对象（Target of Evaluation）
URI　统一资源标识符（Universal Resource Identifier）

5　评估模型

5.1　PKI 互操作性能

PKI 互操作性能是指两个以上（含）PKI 系统或 PKI 应用正确地交互和使用证书以及相关安全信息的性能（在不引起混淆的情况下，本标准将 PKI 互操作性能简称为互操作性）。互操作性同时取决于参加事务过程的 PKI 系统和 PKI 应用：PKI 系统提供的信息不足，或者 PKI 应用所能理解接受的信息不足，都可能导致事务失败、无法获取安全服务。

互操作性具有相对性，与参加事务过程的对象相关。相同的 PKI 系统，与不同的 PKI 应用进行事务时，其互操作性可能完全不一样。同样，相同的 PKI 应用，与不同的 PKI 系统进行事务时，其互操作性也可能完全不一样。

改进 PKI 系统和 PKI 应用，使二者对 PKI 安全服务相关信息的理解趋于一致，能够提高互操作性。但是，由于互操作性的相对性，针对某一些特定事务的改进，可能反而会导致其他事务的互操作性降低。例如，对某 PKI 应用 app-1 进行改进，使其与某 PKI 系统 sys-1 具有更好的互操作性，会同时导致 app-1 与另一个 PKI 系统 sys-2 的互操作性大大降低。所以，盲目的改进反而有可能导致互操作性的整体下降。

本标准通过分等级的互操作评估，同时为 PKI 系统和 PKI 应用指出了改进 PKI 互操作能力等级的方向（在不引起混淆的情况下，本标准将 PKI 互操作能力等级简称为互操作能力），促进建设和开发具有全面互操作能力的 PKI 系统和 PKI 应用。

5.2　评估对象

本标准的评估对象可以是 PKI 系统或者 PKI 应用。

本标准分别针对 PKI 系统和 PKI 应用给出了不同等级互操作能力的要求。本标准中的 PKI 系统和 PKI 应用是按照评估对象在事务中所起作用来区分：PKI 系统在事务中提供数字证书的颁发以及相关服务；PKI 应用在事务中使用数字证书以及相关信息、获得安全服务。

本标准所指的 PKI 系统和 PKI 应用不一定与现实概念中的 PKI 系统和 PKI 应用完全对应。例如，当某个 CA 系统向其他的 PKI 系统请求信息以获得安全服务时，则该 CA 系统在本标准中被视为 PKI 应用。当该 CA 系统提供数字证书服务时，则被视为 PKI 系统。

5.3　互操作能力评估

互操作能力是 PKI 系统或者 PKI 应用自身的性能，体现了评估对象的自身属性。与互操作性不同，互操作能力具有确定性，与事务的对象无关。对于特定的 PKI 系统或者 PKI 应用，即使在不同的事务中，它的互操作能力也是确定不变的。虽然互操作能力与特定的事务无关，但是互操作能力只有在事务中才能表现出来。从概念而言，互操作能力是 TOE 与所有 PKI 系统或者所有 PKI 应用进行事务的互操作性的综合度量。也就是说，需要与所有 PKI 应用或者所有 PKI 系统进行事务，才可以准确地量化 PKI 系统的安全服务对所有 PKI 应用的可用程度，或者 PKI 应用对所有 PKI 系统所提供的安全服务的理解接受能力。

与所有 PKI 系统或者所有 PKI 应用进行事务，才能够准确地量化 TOE 的互操作能力。但是使用

这种方法来评估互操作能力是不切合现实的。所以，本标准引入了完全互操作能力实体（完全互操作PKI系统和完全互操作PKI应用）的概念，通过评估TOE与完全互操作能力实体进行事务时影响互操作性的各种因素（即确定了与完全互操作能力实体的互操作性），从而确定TOE的互操作能力等级IOL。

互操作性和互操作能力具有如下特性：不同IOL的PKI系统与PKI应用进行事务时，其互操作性取决于IOL低的一方。当TOE与完全互操作能力实体进行事务时，事务的互操作性就只取决于TOE的互操作能力，所以通过与完全互操作能力实体进行事务，能够得到TOE的互操作能力。即有如下[其中，I(　)表示事务的互操作性能，IOL(　)表示评估对象的互操作能力等级，app表示被评估的PKI应用，sys表示被评估的PKI系统]：

$$I(F-SYS,app)=IOL(app)$$

或者

$$I(sys,F-APP)=IOL(sys)$$

IOL是TOE与完全互操作能力实体进行事务时的互操作性能的量化，体现了全部事务中被理解和使用的安全信息的程度，也体现了被评估的PKI系统或者PKI应用的互操作能力。

本标准定义了五个互操作能力等级，高等级的PKI系统或者PKI应用具有更全面的互操作能力。本标准给出了各级IOL的互操作能力要求，也相当于指出了提高互操作能力的改进方向。需要注意：TOE互操作能力的提高改进并不意味着能够提高与该TOE的所有事务的互操作性，而是说明该TOE可与更多的PKI系统或PKI应用更好地进行事务。

5.4　互操作能力等级划分原则

5.4.1　划分依据

PKI系统与PKI应用在事务中交换和使用的信息主要包括：

- 证书信息。证书是PKI系统提供安全服务的最基本手段，也是PKI应用获得安全服务的最基本途径。证书信息是安全服务所需的基本信息。各种安全服务（真实性、保密性、完整性、非否认等）都是通过证书实现的。
- 证书撤销状态信息。证书撤销状态信息是证书信息的补充，用于验证证书信息在特定的时刻是否有效。PKI应用在使用证书上的信息之前，需要检查其撤销状态，确定该证书是否有效。常见的证书撤销状态信息是CRL和OCSP。
- 其他多种辅助信息。辅助信息包括供PKI系统和PKI应用使用的CP/CPS、第三方审查认证结果、设计文档等等。CP/CPS作为证书信息的补充，用来表明证书上信息的可靠程度和适用范围等安全程度信息。PKI应用在使用安全服务之前，需要在PKI应用管理者的直接或者间接指导下，确定证书信息的安全程度是否适用、是否满足应用需求。

依据各IOL的互操作能力要求的显著特点，本标准将五个IOL等级分别称为格式正确级、内容明确级、功能完善级、执行标准化级和安全审计级。

需要注意：IOL名称并不完全表示该等级的互操作能力要求的全部内容，只是给出了该级别的评估对象的重要特点，表示了互操作能力等级的主要要求。例如，IOL1格式正确级表示本IOL的主要要求是格式正确，但是IOL1同时也对互操作能力的其他方面提出了要求。

5.4.2　PKI系统

PKI系统提供PKI应用使用的安全信息，其互操作能力表现为提供安全信息的全面程度。

PKI系统的五个互操作能力等级逐一递进，前者是后者的基础，后者是前者的增强。高等级的PKI系统能够为更大范围的PKI应用提供更多的可用安全服务信息：

- IOL1 的 PKI 系统能提供格式正确的信息；
- IOL2 的 PKI 系统能提供内容明确的信息，并满足 IOL1 的要求；
- IOL3 的 PKI 系统能执行完善的功能和提供对应的信息，并满足 IOL2 的要求；
- IOL4 的 PKI 系统能提供标准化执行而产生的信息，并满足 IOL3 的要求；
- IOL5 的 PKI 系统能提供产生过程可审计的信息，并满足 IOL4 的要求。

a） IOL1 格式正确级

本级 PKI 系统的重要特征是能够颁发格式正确的证书和 CRL。

格式正确是 PKI 应用接受安全服务信息的基础。如果格式不正确，PKI 应用就无法获取信息，相当于 PKI 系统提供的安全服务是不可用的。格式正确级主要考虑证书和 CRL 的基本格式、PKI 系统的基本功能，确保达到本等级的 PKI 实体拥有基本的互操作能力，能够正确生成证书和 CRL，以及正确地使用私有扩展项。

b） IOL2 内容明确级

本级 PKI 系统的重要特征是能够颁发内容明确的证书和 CRL，通过对证书扩展项和 CRL 扩展项的使用，提供明确的信息；具有 CPS，明确地描述证书服务过程；能够支持增量 CRL 或者 OCSP，支持 LDAP 或者 HTTP 发布证书和 CRL。

安全服务依赖于从 PKI 系统获取的信息，充分明确的信息使更多的 PKI 应用能够接受安全服务。内容明确级要求 PKI 系统必须能够产生重要的证书和 CRL 扩展项，支持增量 CRL 或者 OCSP，而且对格式正确级中提出的各项评估指标有了进一步限制，明确了安全服务信息的内容。

c） IOL3 功能完善级

本级 PKI 系统的重要特征是具备证书服务的完善功能，能够同时支持增量 CRL 和 OCSP，同时支持 LDAP 和 HTTP 发布证书和 CRL，正确地设定证书扩展项、CRL 扩展项及 OCSP 扩展项的取值；具有 CP，提供包含重要基本内容章节的 CP/CPS，并具备执行 CP/CPS 的各种操作的能力。

功能完善级在内容明确级的基础上增加了对 CP 和 PKI 系统操作的评估，协助 PKI 应用管理者判断 PKI 系统的安全服务能否适用于特定的 PKI 应用。证书扩展项和 CRL 扩展项为 PKI 应用提供辅助信息，使得 PKI 应用更加准确地使用 PKI 系统提供的服务。功能完善的 PKI 系统应该能够支持所有的扩展项，并可正确有效地设定各种扩展项的取值，从而实现更加完善的功能。

d） IOL4 执行标准化级

本级 PKI 系统的重要特征是证书服务过程按照标准化流程执行，提供标准格式的完整 CP/CPS，并按照标准流程执行该 CP/CPS 的各种操作。

执行标准化级在功能完善级的基础上加强了对 PKI 系统操作流程的要求，使得安全服务信息更加标准化。按照标准化流程执行的 PKI 系统能更顺利地为不同的 PKI 应用提供服务，标准格式的完整 CP/CPS 更容易获得 PKI 应用管理者的认可。

e） IOL5 安全审计级

本级 PKI 系统的重要特征是可审计的证书服务管理过程，在标准化服务的基础上，进一步提供额外的可供第三方检查的审计证明，并且在 CP/CPS 中有相应的安全程度声明。

安全审计级在执行标准化级的基础上加强了对 PKI 系统可审计项目的评估，对各评估项做了严格的限定，从而使互操作能力达到最强。通过可供第三方检查的审计证明，PKI 系统将会提供更安全可靠的证书服务，能够同时满足不同应用的安全需求（包括高安全程度需求和低安全程度需求），适用于最大范围的 PKI 应用。

5.4.3 PKI 应用

PKI 应用直接或者间接地接受 PKI 系统提供的安全信息，其互操作能力表现为接受和理解安全信息的程度。

PKI 应用的五个互操作能力等级逐一递进，前者是后者的基础，后者是前者的增强。高等级的 PKI 应用支持更大范围的 PKI 系统，接受更多的可用安全服务信息：

- IOL1 的 PKI 应用能接受格式正确的信息；
- IOL2 的 PKI 应用能明确地获取和解释安全服务信息，并满足 IOL1 的要求；
- IOL3 的 PKI 应用能完善地执行安全服务信息所对应的功能，并满足 IOL2 的要求；
- IOL4 的 PKI 应用按照标准化流程执行功能，并满足 IOL3 的要求；
- IOL5 的 PKI 应用以可审计的方式执行功能，并满足 IOL4 的要求。

a） IOL1 格式正确级

本级 PKI 应用能够正确理解基本格式的证书和 CRL。

支持证书和 CRL 基本格式是 PKI 应用获取安全服务的基础。对证书和 CRL 的基本格式正确解析之后，PKI 应用才能够正确地使用证书。格式正确级主要考虑对证书和 CRL 的基本格式支持，确保达到本等级的 PKI 实体能够使用证书和 CRL，能够使用基本的安全服务信息。

b） IOL2 内容明确级

本级 PKI 应用能正确理解证书和 CRL 中的各项内容，支持重要的证书扩展项和 CRL 扩展项，能够使用增量 CRL 或者 OCSP，使用 LDAP 或者 HTTP 获取证书和 CRL。

获得更充分明确的信息（包括各种重要扩展），PKI 应用将能够更全面地接受安全服务。内容明确级要求 PKI 应用必须能够支持重要扩展项，从而明确地理解安全服务信息。

c） IOL3 功能完善级

本级 PKI 应用功能完善，能够完善地支持解析证书和 CRL，包括各种证书扩展项和 CRL 扩展项，支持增量 CRL 和 OCSP 功能，使用 LDAP 和 HTTP 获取证书和 CRL。

功能完善级在内容明确级的基础上增加了对扩展项使用的评估，功能完善的 PKI 应用应该能够支持所有的扩展项，能够处理各种扩展项的不同取值，从而实现更加完善的功能。

d） IOL4 执行标准化级

本级 PKI 应用应按照标准化的流程执行证书查询、下载与验证等操作。

按照标准化流程执行的 PKI 应用能更顺利地从不同的 PKI 系统获得服务，标准化的执行流程会更容易获得 PKI 应用管理者的认可。执行标准化级在功能完善级的基础上加强了对 PKI 应用操作流程的要求，使得获取和使用安全服务信息更加标准化、更为准确。

e） IOL5 安全审计级

本级 PKI 应用可以提供应用程序的完全审计记录以及额外的可供第三方检查的保障。

通过提供可供第三方检查的保障和完全审计记录，PKI 应用的安全可靠性得到保证，适用于最大范围的 PKI 系统。安全审计级在执行标准化级的基础上加强了对 PKI 应用可审计项目的评估，对各评估项做了最严格的限定。

第 6 章中将规定 PKI 系统和 PKI 应用各个互操作能力等级的具体要求，并在附录 A 和附录 B 中以表格的形式列出。

6 评估内容

6.1 第一级：格式正确级

6.1.1 PKI 系统

6.1.1.1 编解码方式

对编解码方式的要求如下：

a） 编码方式

应使用 BER 编码。

b) 解码方式

应支持 DER 解码。

6.1.1.2 证书格式

证书基本项的格式和编码应符合 GB/T 20518—2006 的要求。对证书格式的要求如下：

a) 版本 version

取值应为 v1(0)、v2(1)或 v3(2)。

b) 序列号 serialNumber

1) 取值应为自然数；

2) 对于相同 CA 颁发的证书，每个证书序列号应只出现一次；

3) 长度应不大于 20 字节。

c) 签名算法 signature

1) 应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2(见 GM/T 0003—2012 和 GM/T 0004—2012)，(MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS，GOST R 34.11-94 with (GOST R 34.10-94，GOST R 34.10-2001)；

2) 本项取值应与 signatureAlgorithm 项取值一致。

d) 颁发者 issuer

1) 应为非空的 X.501 DN；

2) RDN 应使用下列属性：country，organization，organizational unit，distinguished name qualifier，state or province name，common name，serial number，locality，title，surname，given name，initials，pseudonym，generation qualifier，domain component，或 email address；

3) 每个 RDN 应只有一个属性值。

e) 有效期 validity

1) 应对 2049 年以前的时间按照 UTCTime 编码，2050 年(含)以后的时间按照 GeneralizedTime 编码；

2) notAfter 子项表示的时间应比 notBefore 子项表示的时间晚；

3) 使用 GeneralizedTime 格式时，不应编码为 99991231235959Z。

f) 主体 subject

1) RDN 应使用下列属性：country，organization，organizational unit，distinguished name qualifier，state or province name，common name，serial number，locality，title，surname，given name，initials，pseudonym，generation qualifier，domain component，或 email address；

2) 每个 RDN 应只有一个属性值；

3) 本项的 DN 为空时，subjectAltName 扩展项应包含主体名称信息，且标记为关键扩展。

g) 主体公钥信息 subjectPublicKeyInfo

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM2，RSA，RSASSA-PSS，RSAES-OAEP，DSA，DH，KEA，ECDSA，ECDH，ECMQV，GOST R 34.10-94，GOST R 34.10-2001。

h) 颁发者唯一标识符 issuerUniqueID
当版本为 v1(0)时,不应使用本项。

i) 主体唯一标识符 subjectUniqueID
当版本为 v1(0)时,不应使用本项。

6.1.1.3 证书扩展

私有扩展应标记为非关键扩展。

6.1.1.4 CRL 格式

CRL 基本项的格式和编码应符合 RFC 5280 的要求。对 CRL 格式的要求如下:

a) 版本 version
不应使用本项或取值为 v2(1)。

b) 签名算法 signature
1) 应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种:SM3 with SM2,(MD2,MD4,MD5,SHA-1,SHA-224,SHA-256,SHA-384,SHA-512) with RSA,(SHA-1,SHA-224,SHA-256) with DSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512) with ECDSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512) with RSASSA-PSS,GOST R 34.11-94 with (GOST R 34.10-94,GOST R 34.10-2001);
2) 本项取值应与 signatureAlgorithm 项取值一致。

c) 颁发者 issuer
1) 应为非空的 X.501 DN;
2) RDN 应使用下列属性:country,organization,organizational unit,distinguished name qualifier,state or province name,common name,serial number,locality,title,surname,given name,initials,pseudonym,generation qualifier,domain component,或 email address;
3) 每个 RDN 应只有一个属性值。

d) 本次更新 thisUpdate
应对 2049 年以前的时间按照 UTCTime 编码,2050 年(含)以后的时间按照 GeneralizedTime 编码。

e) 下次更新 nextUpdate
1) 应对 2049 年以前的时间按照 UTCTime 编码,2050 年(含)以后的时间按照 GeneralizedTime 编码;
2) 本项表示的时间应比 thisUpdate 项表示的时间晚。

f) 被撤销的证书 revokedCertificates
没有被撤销证书时,不应使用本项。

6.1.1.5 系统功能要求

对系统功能的要求如下:

a) 颁发证书
系统应具备此功能。

b) 颁发证书撤销状态信息
系统应颁发完全 CRL。

6.1.2 PKI 应用

6.1.2.1 编解码方式

对编解码方式的要求如下：

a) 编码方式

应使用 BER 编码。

b) 解码方式

应支持 DER 解码。

6.1.2.2 证书格式

应按照 GB/T 20518—2006 解析证书基本项。对证书格式的要求如下：

a) 版本 version

应支持取值为 v1(0)、v2(1)或 v3(2)。

b) 序列号 serialNumber

支持长度应至少为 8 字节。

c) 签名算法 signature

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(SHA-1，SHA-256) with RSA。

d) 颁发者 issuer

RDN 应支持下列属性：country，organization，organizational unit，common name。

e) 有效期 validity

应支持 2049 年以前的时间按照 UTCTime 解码，2050 年（含）以后的时间按照 GeneralizedTime 解码。

f) 主体 subject

RDN 应支持下列属性：country，organization，organizational unit，common name。

g) 主体公钥信息 subjectPublicKeyInfo

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM2，RSA。

6.1.2.3 CRL 格式

应按照 RFC 5280 标准解析 CRL 基本项。对 CRL 格式的要求如下：

a) 版本 version

应支持本项不出现或取值为 v2(1)。

b) 签名算法 signature

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(SHA-1，SHA-256)with RSA。

c) 颁发者 issuer

RDN 应支持下列属性：country，organization，organizational unit，common name。

d) 本次更新 thisUpdate

应支持 2049 年以前的时间按照 UTCTime 解码，2050 年（含）以后的时间按照 GeneralizedTime 解码。

e) 下次更新 nextUpdate

应支持 2049 年以前的时间按照 UTCTime 解码，2050 年（含）以后的时间按照 GeneralizedTime 解码。

f) 被撤销的证书 revokedCertificates

应支持本项。

6.1.2.4 应用功能要求

对应用功能的要求如下：

a) 证书解码

应支持证书基本域。

b) CRL 解码

应支持 CRL 基本域。

6.2 第二级：内容明确级

6.2.1 PKI 系统

6.2.1.1 编解码方式

应使用 DER 编码。

6.2.1.2 证书格式

对证书格式的要求如下：

a) 版本 version

取值应为 v3(2)。

b) 签名算法 signature

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS。

c) 颁发者 issuer

RDN 不应使用属性 distinguished name qualifier。

d) 主体 subject

1) 应为非空的 X.501 DN；

2) RDN 不应使用属性 distinguished name qualifier。

e) 主体公钥信息 subjectPublicKeyInfo

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM2，RSA，RSASSA-PSS，RSAES-OAEP，DSA，DH，KEA，ECDSA，ECDH，ECMQV。

f) 颁发者唯一标识符 issuerUniqueID

不应使用本项。

g) 主体唯一标识符 subjectUniqueID

不应使用本项。

6.2.1.3 证书扩展

下列证书扩展项的格式和编码，除 i)、j)、k)、l)、m)项应符合相应的 RFC 标准，其他都应符合 GB/T 20518—2006的要求。对证书扩展的要求如下：

a） 颁发机构密钥标识符 authorityKeyIdentifier
应在自签名证书以外的所有证书中使用。
b） 主体密钥标识符 subjectKeyIdentifier
应在所有 CA 证书中使用。
c） 密钥用法 keyUsage
1） 应在用于验证证书或者 CRL 中数字签名的证书中使用；
2） 应至少有一位值不为零。
d） 证书策略 certificatePolicies
1） 每个证书策略 OID 应只出现一次；
2） 应只在 CA 证书中使用 AnyPolicy OID。
e） 策略映射 policyMappings
应只在 CA 证书中使用。
f） 基本限制 basicConstraints
应在所有 CA 证书中使用。
g） 证书撤销列表分发点 cRLDistributionPoints
1） 应在自签名证书以外的所有证书中使用；
2） distributionPoint 子项取值应包含 LDAP 或者 HTTP 形式的 URI。
h） 私有密钥使用期 privateKeyUsagePeriod
应标记为非关键扩展。
i） 徽标 logotypes
应标记为非关键扩展，其格式和编码应符合 RFC 3709 的要求。
j） IP 地址表示 iPAddressDelegation
应标记为非关键扩展，其格式和编码应符合 RFC 3779 的要求。
k） AS 标识符表示 autonomousSystemIdentifierDelegation
应标记为非关键扩展，其格式和编码应符合 RFC 3779 的要求。
l） 担保 warranty
应标记为非关键扩展，其格式和编码应符合 RFC 4059 的要求。
m） WLAN 服务集合标识符 wLANSSID
应标记为非关键扩展，其格式和编码应符合 RFC 4334 的要求。
n） 个人身份标识码 identityCode
应标记为非关键扩展。
o） 个人社会保险号 insuranceNumber
应标记为非关键扩展。
p） 企业工商注册号 iCRegistrationNumber
应标记为非关键扩展。
q） 企业组织机构代码 organizationCode
应标记为非关键扩展。
r） 企业税号 taxationNumber
应标记为非关键扩展。

6.2.1.4 CRL 格式

对 CRL 格式的要求如下：
a） 版本 version

取值应为 v2(1)。

b) 签名算法 signature

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2,(MD5,SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with RSA,(SHA-1,SHA-224,SHA-256)with DSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with ECDSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with RSASSA-PSS。

c) 颁发者 issuer

RDN 不应使用属性 distinguished name qualifier。

d) 下次更新 nextUpdate

应在所有 CRL 中使用。

6.2.1.5 CRL 扩展

CRL 扩展项的格式和编码应符合 RFC 5280 要求。对 CRL 扩展的要求如下：

a) 颁发机构密钥标识符 authorityKeyIdentifier

应在所有 CRL 中使用。

b) 证书撤销列表编号 cRLNumber

长度应不大于 20 字节。

c) 增量证书撤销列表指示 deltaCRLIndicator

应在所有增量 CRL 中使用。

6.2.1.6 CRL Entry 扩展

CRL Entry 扩展项的格式和编码应符合 RFC 5280 要求。

6.2.1.7 OCSP 请求格式

应按照 GB/T 19713—2005 的要求解析 OCSP 请求。对 OCSP 请求格式的要求如下：

a) 版本 version

应支持取值为 v1(0)。

b) 请求者名称 requestorName

应至少支持 rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID 中的一种名称。

c) 签名算法 signatureAlgorithm

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2,(SHA-1,SHA-256)with RSA,(SHA-1,SHA-256)with RSASSA-PSS。

d) 请求列表 requestList

支持请求单个证书，包含单个 Request。

e) 请求的证书 reqCert

hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3,SHA-1,SHA-256。

6.2.1.8 OCSP 响应格式

应按照 GB/T 19713—2005 的要求生成 OCSP 响应。对 OCSP 响应格式的要求如下：

a) 响应状态 responseStatus

取值应为 successful,malformedRequest,internalError,tryLater,sigRequired,unauthorized

之一。

b) 响应字节 responseBytes

应使用本项。

c) 响应类型 responseType

取值应为 id-pkix-ocsp-basic。

d) 签名算法 signatureAlgorithm

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS。

e) 响应者标识符 responderID

1) byName 子项取值应为响应者 DN；

2) byKey 子项取值应为对响应者公钥使用 SHA-1 算法进行哈希运算后得出的值。

f) 生成时间 producedAt

应使用 GeneralizedTime 格式编码。

g) 响应 responses

支持响应单个证书，包含单个 SingleResponse。

h) 证书标识符 certID

hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512。

i) 证书状态 certStatus

取值应为 good、revoked、unknown 之一。

j) 本次更新 thisUpdate

应使用 GeneralizedTime 格式编码。

k) 下次更新 nextUpdate

应使用 GeneralizedTime 格式编码。

6.2.1.9 OCSP 扩展

应按照 GB/T 19713—2005 的要求生成 OCSP 响应消息中的扩展项，并标记为非关键扩展。

6.2.1.10 CP/CPS

应具备符合 RFC 3647 要求的 CPS。

6.2.1.11 系统功能要求

对系统功能的要求如下：

a) 颁发交叉证书

系统应具备此功能。

b) 颁发证书撤销状态信息

系统应颁发增量 CRL 或提供 OCSP 服务。

c) 证书发布

系统应通过 HTTP 或者 LDAP 发布除终端实体证书之外的所有证书。

d) 证书撤销状态信息发布

系统应通过 HTTP 或者 LDAP 发布所有 CRL。

6.2.2 PKI 应用

6.2.2.1 编解码方式

应使用 DER 编码。

6.2.2.2 证书格式

对证书格式的要求如下：

a) 序列号 serialNumber
支持长度应至少为 16 字节。

b) 签名算法 signature
应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(SHA-1，SHA-256)with RSA，(SHA-1，SHA-256)with RSASSA-PSS。

c) 有效期 validity
应支持任意格式的时间解码。

d) 主体 subject
本项为空时，支持从 subjectAltName 扩展项中获取主体名称信息。

e) 主体公钥信息 subjectPublicKeyInfo
应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM2，RSA，RSASSA-PSS，RSAES-OAEP。

f) 颁发者唯一标识符 issuerUniqueID
应支持本项。

g) 主体唯一标识符 subjectUniqueID
应支持本项。

6.2.2.3 证书扩展

应按照 GB/T 20518—2006 解析证书扩展项。对证书扩展的要求如下：

a) 颁发机构密钥标识符 authorityKeyIdentifier
应支持本扩展项。

b) 主体密钥标识符 subjectKeyIdentifier
应支持本扩展项。

c) 密钥用法 keyUsage
应支持本扩展项。

d) 证书策略 certificatePolicies
应支持本扩展项。

e) 主体替换名称 subjectAltName
1) 应支持本扩展项；
2) 应能够识别以下类型的名称：rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID。

f) 颁发者替换名称 issuerAltName
1) 应支持本扩展项；
2) 应能够识别以下类型的名称：rfc822Name、dNSName、x400Address、directoryName、ediP-

artyName、uniformResourceIdentifier、iPAddress、registeredID。

g) 基本限制 basicConstraints

应支持本扩展项。

h) 证书撤销列表分发点 cRLDistributionPoints

1) 应支持本扩展项；

2) distributionPoint 子项支持使用 LDAP 或 HTTP 形式的 URI。

6.2.2.4 CRL 格式

对 CRL 格式的要求如下：

a) 签名算法 signature

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(SHA-1，SHA-256)with RSA，(SHA-1，SHA-256)with RSASSA-PSS。

b) 本次更新 thisUpdate

应支持任意格式的时间解码。

c) 下次更新 nextUpdate

应支持任意格式的时间解码。

6.2.2.5 CRL 扩展

应按照 RFC 5280 标准解析 CRL 扩展项。对 CRL 扩展的要求如下：

a) 颁发机构密钥标识符 authorityKeyIdentifier

应支持本扩展项。

b) 颁发者替换名称 issuerAltName

1) 应支持本扩展项；

2) 应能够识别 rfc822Name 、dNSName 、x400Address、directoryName 、ediPartyName 、uniformResourceIdentifier 、iPAddress 、registeredID 类型的名称。

c) 证书撤销列表编号 cRLNumber

1) 应支持本扩展项；

2) 支持长度应至少为 20 字节。

d) 增量证书撤销列表指示 deltaCRLIndicator

应支持本扩展项。

6.2.2.6 CRL Entry 扩展

应按照 RFC 5280 标准解析 CRL Entry 扩展项。对 CRL Entry 扩展的要求如下：

a) 原因码 reasonCode

应支持本扩展项。

b) 失效时间 invalidityDate

应支持本扩展项。

c) 证书颁发者 certificateIssuer

应支持本扩展项。

6.2.2.7 OCSP 请求格式

应按照 GB/T 19713—2005 的要求生成 OCSP 请求。对 OCSP 请求格式的要求如下：

a) 版本 version

取值应为 v1(0)。

b) 请求者名称 requestorName

应使用 otherName、rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID 中的一种名称。

c) 签名算法 signatureAlgorithm

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS，GOST R 34.11-94 with (GOST R 34.10-94，GOST R 34.10-2001)。

d) 请求列表 requestList

应能够请求单个证书，包含单个 Request。

e) 请求的证书 reqCert

hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512。

6.2.2.8 OCSP 响应格式

应按照 GB/T 19713—2005 的要求解析 OCSP 响应。对 OCSP 响应格式的要求如下：

a) 响应状态 responseStatus

应支持取值为 successful，malformedRequest，internalError，tryLater，sigRequired，unauthorized。

b) 响应类型 responseType

支持取值为 id-pkix-ocsp-basic。

c) 签名算法 signatureAlgorithm

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(SHA-1，SHA-256) with RSA。

d) 响应者标识符 responderID

支持使用 byName 或 byKey。

e) 生成时间 producedAt

应能够正常解码。

f) 响应 responses

取值为单个 SingleResponse 时，应能够正常解码。

g) 证书标识符 certID

hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，SHA-1，SHA-256。

h) 证书状态 certStatus

应支持取值为 good，revoked，unknown。

i) 本次更新 thisUpdate

应能够正常解码。

j) 下次更新 nextUpdate

应能够正常解码。

6.2.2.9 OCSP 扩展

应按照 GB/T 19713—2005 的要求生成 OCSP 请求消息中的扩展项，并标记为非关键扩展。

OCSP 响应消息中证书撤销列表入口扩展域 cRLEntryExtension 扩展项应满足 6.2.2.6 中的要求。

6.2.2.10 应用功能要求

对应用功能的要求如下：

a) 证书解码
应支持证书扩展。

b) CRL 解码
应支持 CRL 扩展和 CRL Entry 扩展。

c) OCSP
应支持 OCSP 基本域。

6.3 第三级：功能完善级

6.3.1 PKI 系统

6.3.1.1 编解码方式

应支持 BER 解码。

6.3.1.2 证书格式

对证书格式的要求如下：

a) 序列号 serialNumber
长度应不大于 16 字节。

b) 签名算法 signature
应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS。

c) 颁发者 issuer
RDN 应使用下列属性：country，organization，organizational unit，state or province name，locality，或 common name。

d) 主体 subject
RDN 应使用下列属性：country，organization，organizational unit，state or province name，locality，或 common name。

e) 主体公钥信息 subjectPublicKeyInfo
应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM2，RSA，RSASSA-PSS，RSAES-OAEP，DSA。

6.3.1.3 证书扩展

对证书扩展的要求如下：

a) 颁发机构密钥标识符 authorityKeyIdentifier
1) 应标记为非关键扩展；
2) 应使用 keyIdentifier 子项；
3) keyIdentifier 子项取值应使用 GB/T 20518—2006 的 5.2.3.2.1 中的方法 a)或 b)生成。

b) 主体密钥标识符 subjectKeyIdentifier

1) 应标记为非关键扩展；

2) 应使用 GB/T 20518—2006 的 5.2.3.2.1 中的方法 a)或 b)生成。

c) 密钥用法 keyUsage

应在所有证书中使用。

d) 证书策略 certificatePolicies

应在所有证书中使用。

e) 策略映射 policyMappings

1) 应在不同 CP 体系的交叉证书中使用；

2) issuerDomainPolicy 子项取值应为交叉证书颁发者证书的 certificatePolicies 扩展项中出现过的 CP OID。

f) 主体替换名称 subjectAltName

1) 应标记为非关键扩展；

2) 应使用 otherName、rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID 中的名称。

g) 颁发者替换名称 issuerAltName

1) 应标记为非关键扩展；

2) 应使用 otherName、rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID 中的名称。

h) 主体目录属性 subjectDirectoryAttributes

应标记为非关键扩展。

i) 基本限制 basicConstraint

1) 如果 cA 子项取值为 FALSE，keyUsage 扩展项的 keyCertSign 子项取值不应为 1；

2) pathLenConstraint 子项应只在 cA 子项取值为 TRUE 且 keyUsage 扩展项的 keyCertSign 子项取值为 1 时使用；

3) pathLenConstraint 子项出现时，取值应大于或等于 0。

j) 名称限制 nameConstraints

1) 应只在 CA 证书中使用；

2) 应使用 directoryName、rfc822Name、uniformResourceIdentifier、dNSName、iPAddress 中的名称；

3) minimum 子项取值应为 0，不应使用 maximum 子项。

k) 策略限制 policyConstraints

应只在 CA 证书中使用。

l) 扩展密钥用途 extKeyUsage

1) 应标记为非关键扩展；

2) 应只在终端实体证书中使用。

m) 证书撤销列表分发点 cRLDistributionPoints

1) 应标记为非关键扩展；

2) reasons 子项应与 distributionPoint 子项或者 cRLIssuer 子项一起使用；

3) 如果证书颁发者与 CRL 颁发者不同，cRLIssuer 子项应出现，且取值包含 CRL 颁发者 DN；

4) 如果证书颁发者与 CRL 颁发者相同，distributionPoint 子项应出现且 cRLIssuer 子项不应出现。

n) 限制所有策略 inhibitAnyPolicy

应只在 CA 证书中使用。

o) 最新证书撤销列表 freshestCRL

1) 应标记为非关键扩展；

2) 应在终端实体证书中使用；

3) distributionPoint 子项取值应包含 LDAP 或者 HTTP 形式的 URI。

p) 机构信息访问 authorityInfoAccess

1) 应标记为非关键扩展；

2) 应在所有终端实体证书中使用，accessMethod 子项取值应包含 id-ad-ocsp。

q) 主体信息访问 subjectInfoAccess

1) 应标记为非关键扩展；

2) 当 accessMethod 子项取值为 id-ad-caRepository 时，accessLocation 子项取值应为 HTTP 或者 LDAP 形式的 URI。

6.3.1.4 CRL 格式

对 CRL 格式的要求如下：

a) 签名算法 signature

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS。

b) 颁发者 issuer

RDN 应使用下列属性：country，organization，organizational unit，state or province name，locality，或 common name。

6.3.1.5 CRL 扩展

对 CRL 扩展的要求如下：

a) 颁发机构密钥标识符 authorityKeyIdentifier

1) 应标记为非关键扩展；

2) 应使用 keyIdentifier 子项；

3) keyIdentifier 子项取值应使用 GB/T 20518—2006 的 5.2.3.2.1 中的方法 a)或 b)生成。

b) 颁发者替换名称 issuerAltName

1) 应标记为非关键扩展；

2) 应使用 otherName、rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID 中的名称。

c) 证书撤销列表编号 cRLNumber

1) 应标记为非关键扩展；

2) 应在所有 CRL 中使用；

3) 取值应为递增序号；

4) 提供相同信息的完全 CRL 和增量 CRL 中，本扩展项取值应相同；

5) 长度应不大于 16 字节。

d) 增量证书撤销列表指示 deltaCRLIndicator

1) 两个完全 CRL 之间的信息差异，应与前一次 CRL 颁发之后的所有增量 CRL 信息之和

相同；

2） 同一个颁发者颁发的基本 CRL 和增量 CRL 应使用同一个私钥签名。

e） 颁发分布点 issuingDistributionPoints

1） 如果 distributionPoint 子项出现，内容应非空；

2） 如果 distributionPoint 子项未出现，则 CRL 应包含所有撤销证书；

3） 如果 onlySomeReasons 子项出现，CRL 中所有 Entry 应有 unspecified 以外的撤销理由；

4） 如果 onlyContainsUserCerts 子项、onlyContainsCACerts 子项、indirectCRL 子项、onlyContainsAttributeCerts 子项都取值为 FALSE，则 distributionPoint 子项或 onlySomeReasons 子项应出现；

5） 基本 CRL 和增量 CRL 使用的本扩展取值应相同。

f） 最新证书撤销列表 freshestCRL

1） 应标记为非关键扩展；

2） 不应使用 reasons 子项和 cRLIssuer 子项；

3） 不应在增量 CRL 中使用。

g） 机构信息访问 authorityInfoAccess

应标记为非关键扩展。

6.3.1.6 CRL Entry 扩展

对 CRL Entry 扩展的要求如下：

a） 原因码 reasonCode

1） 应标记为非关键扩展；

2） 本扩展项取值不应为 0；

3） 本扩展项取值为 removeFromCRL 时，CRL 应为增量 CRL。

b） 停用证书指示码 holdInstructionCode

应标记为非关键扩展。

c） 失效时间 invalidityDate

1） 应标记为非关键扩展；

2） 应在所有 Entry 中出现。

d） 证书颁发者 certificateIssuer

如果 CRL 颁发者与证书颁发者不同，本扩展项应出现。

6.3.1.7 OCSP 请求格式

对 OCSP 请求格式的要求如下：

a） 签名算法 signatureAlgorithm

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，（MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSA，（SHA-1，SHA-224，SHA-256）with DSA，（SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSASSA-PSS。

b） 请求列表 requestList

支持请求多个证书，包含多个 Request。

c） 请求的证书 reqCert

hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，SHA-1，SHA-256，MD5。

6.3.1.8 OCSP 响应格式

对 OCSP 响应格式的要求如下：

a) 签名算法 signatureAlgorithm

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512)with RSASSA-PSS。

b) 签名 signature

OCSP 服务器证书 extKeyUsage 扩展项应包含 id-kp-OCSPSigning OID。

c) 响应 responses

支持响应多个证书，包含多个 SingleResponse。

d) 证书标识符 certID

hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512。

6.3.1.9 OCSP 扩展

对 OCSP 扩展的要求如下：

a) 现时 nonce

如果 OCSP 请求中使用本扩展项，OCSP 响应应在 responseExtensions 项中使用本扩展项，且取值相同。

b) 证书撤销列表参考 cRLReferences

使用本扩展项时，crlUrl 子项、crlNum 子项和 crlTime 子项应至少有一项被使用。

c) 可接受的响应类型 acceptableResponseTypes

1) 应支持本扩展项；

2) 应支持使用 id-pkix-ocsp-basic OID。

d) 存档截止 archiveCutoff

应使用 GeneralizedTime 格式编码。

e) 服务定位器 serviceLocator

应支持本扩展项。

f) 证书撤销列表入口扩展域 cRLEntryExtension

应满足 6.3.1.6 中的要求。

6.3.1.10 CP/CPS

应具备符合 RFC 3647 要求的 CP。对 CP/CPS 的要求如下：

a) CP/CPS 整体要求

1) 应说明如下章节：概括性描述，信息发布与资料库职责，身份标识与鉴别，证书生命周期操作要求，认证机构设施、管理和运作控制，认证机构技术安全控制，证书、证书撤销列表和在线证书状态协议，认证机构合规性审计和相关评估，其他商业和法律条款；

2) 应能够通过公开途径获得。

b) 概括性描述

应说明如下章节：概述、文档名称与标识、参与方和证书应用。

c) 信息发布与资料库职责

应说明如下章节：资料库的标识和责任方、信息的发布、信息发布的时间和频率、资料库的访问控制。

d) 身份标识与鉴别

应说明如下章节：命名、初始申请证书的身份鉴别、密钥更新请求的身份鉴别、证书撤销请求的身份鉴别。

e) 证书生命周期操作要求

应说明如下章节：证书申请、证书申请的处理、证书颁发、证书接受、密钥对和证书的使用、证书更新、证书密钥更换、证书变更、证书撤销和挂起、证书状态服务。

f) 认证机构设施、管理和运作控制

应说明如下章节：物理安全控制、流程控制、人员控制。

g) 认证机构技术安全控制

应说明如下章节：密钥对的生成和安装、私钥保护和密码模块的工程控制、密钥激活数据、计算机安全控制、生命周期安全控制、网络安全控制。

h) 证书、证书撤销列表和在线证书状态协议

应说明如下章节：证书、证书撤销列表、在线证书状态协议。

6.3.1.11 系统功能要求

对系统功能的要求如下：

a) 颁发证书撤销状态信息

系统应颁发增量 CRL 和提供 OCSP 服务。

b) CP/CPS 发布

系统应通过 HTTP 或者 LDAP 发布 CP/CPS。

c) 证书发布

系统应通过 HTTP 和 LDAP 发布所有证书。通过 LDAP 发布证书的方式应符合 RFC 4523 的要求。

d) CRL 发布

系统应通过 HTTP 和 LDAP 发布所有 CRL。通过 LDAP 发布 CRL 的方式应符合 RFC 4523 的要求。

6.3.1.12 系统操作要求

对系统操作的要求如下：

a) CP/CPS 管理

1) 应指定 CA 所支持的证书策略 OID；

2) CA 应对其订户和依赖方公开证书策略和认证业务声明。

b) 个人隐私保护

CA 所收集的订户信息在未经订户许可的情况下不应被泄露(法律规定的情况除外)。

c) 身份标识与鉴别

1) 证书中不应包含未经验证的信息；

2) 每个终端实体在证书中应拥有可区别的唯一 DN；

3) 应能够通过如下几个类别的用户证件对订户进行身份验证：身份证、护照、驾驶证。

d) 密钥更新请求的身份鉴别和证书撤销请求的身份鉴别

身份鉴别应达到初始申请证书的身份鉴别强度。

e) 证书申请

1） 订户应提供自身身份信息的证明；

2） 订户应提供所有需要出现在证书中的信息的证明。

f） 证书更新和证书密钥更换

应由拥有已颁发证书的订户提出请求。

g） 证书变更、撤销和挂起

1） 如果证书中任何信息发生改变，应将此证书撤销；

2） CA 应支持订户的撤销请求。

h） 物理安全控制

1） 仅有授权用户可以进入 CA 设备所在的安全区域，进出时间和人员信息应记录日志；

2） CA 设备所在区域应具备空调设备等以保证系统正常运转；

3） CA 设备应满足防水、防火等要求；

4） CA 设备应保证其存储介质不会因温度、湿度和电磁等因素而失效；

5） CA 系统应具备离线备份功能。

i） 流程控制

应在至少两人同时在场的情况下进行 CA 密钥的产生、激活以及备份操作。

6.3.2 PKI 应用

6.3.2.1 编解码方式

应支持 BER 解码。

6.3.2.2 证书格式

对证书格式的要求如下：

a） 版本 version

应支持取值为 v1(0)、v2(1)和 v3(2)。

b） 序列号 serialNumber

支持长度应至少为 20 字节。

c） 签名算法 signature

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS。

d） 颁发者 issuer

RDN 应支持下列属性：country，organization，organizational unit，state or province name，locality，common name。

e） 主体 subject

RDN 应支持下列属性：country，organization，organizational unit，state or province name，locality，common name。

f） 主体公钥信息 subjectPublicKeyInfo

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM2，RSA，RSASSA-PSS，RSAES-OAEP，DSA。

6.3.2.3 证书扩展

对证书扩展的要求如下：

a) 策略映射 policyMappings
应支持本扩展项。
b) 主体目录属性 subjectDirectoryAttributes
应支持本扩展项。
c) 名称限制 nameConstraints
应支持本扩展项。
d) 策略限制 policyConstraints
应支持本扩展项。
e) 扩展密钥用途 extKeyUsage
应支持本扩展项。
f) 限制所有策略 inhibitAnyPolicy
应支持本扩展项。
g) 最新证书撤销列表 freshestCRL
1) 应支持本扩展项；
2) distributionPoint 子项支持使用 LDAP 或 HTTP 形式的 URI。
h) 机构信息访问 authorityInfoAccess
1) 应支持本扩展项；
2) accessMethod 子项应支持使用 id-ad-ocsp。
i) 主体信息访问 subjectInfoAccess
应支持本扩展项。
j) 私有密钥使用期 privateKeyUsagePeriod
应支持本扩展项。

6.3.2.4 CRL 格式

对 CRL 格式的要求如下：

a) 版本 version
应支持本项不出现和取值为 v2(1)。
b) 签名算法 signature
应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS。
c) 颁发者 issuer
RDN 应支持下列属性：country，organization，organizational unit，state or province name，locality，common name。

6.3.2.5 CRL 扩展

对 CRL 扩展的要求如下：

a) 颁发分布点 issuingDistributionPoints
应支持本扩展项。
b) 最新证书撤销列表 freshestCRL
应支持本扩展项。
c) 机构信息访问 authorityInfoAccess

应支持本扩展项。

6.3.2.6 CRL Entry 扩展

应支持停用证书指示码 holdInstructionCode 扩展项。

6.3.2.7 OCSP 请求格式

对 OCSP 请求格式的要求如下：

a) 签名算法 signatureAlgorithm
应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512)with RSA，(SHA-1，SHA-224，SHA-256)with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512)with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512)with RSASSA-PSS。

b) 请求列表 requestList
应能够请求多个证书，包含多个 Request。

c) 请求的证书 reqCert
hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512。

6.3.2.8 OCSP 响应格式

对 OCSP 响应格式的要求如下：

a) 签名算法 signatureAlgorithm
应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(SHA-1，SHA-256)with RSA，(SHA-1，SHA-256)with RSASSA-PSS。

b) 响应 responses
取值为多个 SingleResponse 时，应能够正常解码。

c) 证书标识符 certID
hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，MD5，SHA-1，SHA-256。

6.3.2.9 OCSP 扩展

对 OCSP 扩展的要求如下：

a) 现时 nonce
应支持本扩展项。

b) 证书撤销列表参考 cRLReferences
应支持本扩展项。

c) 可接受的响应类型 acceptableResponseTypes
应包含取值为 id-pkix-ocsp-basic 的 OID。

d) 存档截止 archiveCutoff
应支持本扩展项。

e) 服务定位器 serviceLocator
1) issuer 子项取值应与被请求证书的 issuer 项取值相同；
2) locator 子项取值应与被请求证书的 authorityInfoAccess 扩展项的取值相同。

f) 证书撤销列表入口扩展域 cRLEntryExtension

应满足 6.3.2.6 中的要求。

6.3.2.10 应用功能要求

对应用功能的要求如下：

a) OCSP

应支持 OCSP 扩展。

b) 操作流程

应提供操作流程。

c) 审计

应具备审计功能。

d) 源代码

应提供完整的源代码供第三方检查。

6.4 第四级：执行标准化级

6.4.1 PKI 系统

6.4.1.1 证书格式

对证书格式的要求如下：

a) 序列号 serialNumber

长度应不大于 8 字节。

b) 签名算法 signature

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(SHA-1，SHA-256)with RSA，(SHA-1，SHA-256)with RSASSA-PSS。

c) 颁发者 issuer

1) RDN 应使用下列属性：country，organization，organizational unit，或 common name；

2) RDN 序列中属性的顺序应该为：country，organization，organizational unit，common name；

3) organizational unit 属性的出现次数应当为 3 次(含)以下。

d) 主体 subject

1) RDN 应使用下列属性：country，organization，organizational unit，或 common name；

2) RDN 序列中属性的顺序应该为：country，organization，organizational unit，common name；

3) organizational unit 属性的出现次数应当为 3 次(含)以下。

e) 主体公钥信息 subjectPublicKeyInfo

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM2，RSA，RSASSA-PSS，RSAES-OAEP。

6.4.1.2 证书扩展

对证书扩展的要求如下：

a) 颁发机构密钥标识符 authorityKeyIdentifier

1) keyIdentifier 子项取值应使用 GB/T 20518—2006 的 5.2.3.2.1 中的方法 a)生成；

2) keyIdentifier 子项取值应与颁发本证书的 CA 证书中的 subjectKeyIdentifier 扩展项的 keyIdentifier 子项取值一致。

b) 主体密钥标识符 subjectKeyIdentifier

应使用 GB/T 20518—2006 的 5.2.3.2.1 中的方法 a)生成。

c) 证书策略 certificatePolicies

不应在任何证书中使用 AnyPolicy OID。

d) 主体替换名称 subjectAltName

不应使用 otherName。

e) 颁发者替换名称 issuerAltName

不应使用 otherName。

f) 扩展密钥用途 extKeyUsage

不应使用 anyExtendedKeyUsage OID。

g) 证书撤销列表分发点 cRLDistributionPoints

1) 应有包含所有撤销原因的 CRL 的 distributionPoint 子项；

2) cRLIssuer 子项中应仅包含 CRL 颁发者的 DN，并且其编码应与 CRL 颁发者的 DN 编码完全一致。

h) 限制所有策略 inhibitAnyPolicy

skipCerts 子项取值应为 0。

i) 机构信息访问 authorityInfoAccess

当 accessMethod 子项取值为 id-ad-caIssuers 时，accessLocation 子项取值应为 HTTP 或者 LDAP 形式的 URI。

j) 主体信息访问 subjectInfoAccess

当 accessMethod 子项取值为 id-ad-timeStamping 时，accessLocation 子项取值类型应为 uniformResourceIdentifier、rfc822Name、dNSName、iPAddress 之一。

k) 私有密钥使用期 privateKeyUsagePeriod

1) notBefore 子项和 notAfter 子项应使用 GeneralizedTime 格式编码；

2) notBefore 子项或 notAfter 子项应出现。

l) 徽标 logotypes

不应使用 otherLogos 子项。

m) IP 地址表示 iPAddressDelegation

max 子项使用的 IP 地址，应至少要有一位为 1。

6.4.1.3 CRL 格式

对 CRL 格式的要求如下：

a) 签名算法 signature

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(SHA-1，SHA-256)with RSA，(SHA-1，SHA-256)with RSASSA-PSS。

b) 颁发者 issuer

1) RDN 应使用下列属性：country，organization，organizational unit，或 common name；

2) RDN 序列中属性的顺序应该为：country，organization，organizational unit，common name；

3) organizational unit 属性的出现次数应当为 3 次(含)以下。

6.4.1.4 CRL 扩展

对 CRL 扩展的要求如下：

a) 颁发机构密钥标识符 authorityKeyIdentifier

keyIdentifier 子项取值应使用 GB/T 20518—2006 的 5.2.3.2.1 中的方法 a)生成。

b) 颁发者替换名称 issuerAltName

不应使用 otherName。

c) 证书撤销列表编号 cRLNumber

长度应不大于 8 字节。

d) 颁发分布点 issuingDistributionPoints

1) 如果 revokedCertificates 项只包含 CRL 颁发者颁发的证书，indirectCRL 子项取值应为 FALSE；

2) 如果 revokedCertificates 项只包含终端实体证书，onlyContainsUserCerts 子项取值应为 TRUE；

3) 如果 revokedCertificates 项只包含 CA 证书，onlyContainsCACerts 子项取值应为 TRUE。

e) 机构信息访问 authorityInfoAccess

当 accessMethod 子项取值为 id-ad-caIssuers 时，accessLocation 子项取值应为 HTTP 或者 LDAP 形式的 URI。

6.4.1.5 OCSP 请求格式

对 OCSP 请求格式的要求如下：

a) 签名算法 signatureAlgorithm

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS。

b) 请求的证书 reqCert

hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512。

6.4.1.6 OCSP 响应格式

对 OCSP 响应格式的要求如下：

a) 签名算法 signatureAlgorithm

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(SHA-1，SHA-256) with RSA，(SHA-1，SHA-256) with RSASSA-PSS。

b) 证书标识符 certID

hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，MD5，SHA-1，SHA-256。

6.4.1.7 CP/CPS

应具备英语版本的 CP/CPS。对 CP/CPS 的要求如下：

a) CP/CPS 整体要求

支持的 CP OID 应在 CP/CPS 中描述。

b) 概括性描述

应说明如下章节：策略管理、定义和缩写。

c) 证书生命周期操作要求

应说明如下章节：认证服务订购终止、密钥托管和恢复。

d) 认证机构设施、管理和运作控制

应说明如下章节：审计日志处理流程、记录归档、认证机构密钥更替、事故和灾难恢复、认证机构服务终止。

e) 认证机构技术安全控制

应说明如下章节：密钥对管理的其他方面、时间标记。

f) 认证机构合规性审计和相关评估

应说明如下章节：评估所涵盖的主题和评估的方法列表、评估的频率、评估者的身份和资质、评估者与被评估实体之间的关系、对评估中出现的不足所采取的措施、评估结果的传达。

g) 其他商业和法律条款

应说明如下章节：费用、财务责任、业务信息保密、个人隐私保护、知识产权、陈述和担保、免责申明、有限责任、赔偿、有效期限和终止、对参与者的个别通告与沟通、修订、争议处理、管辖法律、与适用法律的符合性、杂项条款、其他条款。

6.4.1.8 系统功能要求

对系统功能的要求如下：

a) 证书发布

通过 HTTP 发布证书的方式应符合 RFC 4387 的要求。

b) CRL 发布

通过 HTTP 发布 CRL 的方式应符合 RFC 4387 的要求。

6.4.1.9 系统操作要求

对系统操作的要求如下：

a) CP/CPS 管理

证书策略 OID 的生命周期不应小于 4 年。

b) 密钥更新请求的身份鉴别和证书撤销请求的身份鉴别

初始身份鉴别之后，应至少每 9 年重新对订户进行一次初始身份鉴别。

c) 证书申请

1) 颁发证书之前，全部证书内容(包括扩展项)应经过审核；

2) 证书应在申请完成后 30 天内颁发。

d) 证书变更、撤销和挂起

CA 应在 24 h 之内将订户的撤销请求处理完毕。

e) 流程控制

1) 审计员不应该在系统中拥有除了审计之外的其他权限；

2) RA 操作员只能在 RA 系统中拥有权限。

f) 人员控制

系统中的所有人员应没有犯罪记录。

g) 审计日志处理流程

除审计程序之外，审计日志数据不应被任何人员或者程序查看或修改。

h) 密钥对的生成和安装

在初始分发自签名证书的时候，CA 应提供其证书的防篡改机制。

i) 密钥激活数据

1) CA 私钥激活应使用多因素认证(例如口令结合生物特征，或口令结合智能卡)；

2) 如果密码模块中使用了 PIN 码或口令，应至少每 3 个月修改一次。

j） 私钥保护和密码模块的工程控制

1） 在密钥对的生命周期结束时，CA 私钥的所有部分应该被完全销毁；

2） 如果密码设备需要永久性地从系统中移除，应清除其中的所有密钥信息。

k） 事故和灾难恢复

1） 当 CA 私钥泄露或怀疑泄露时，CA 应该立即主动通知其已经颁发了交叉证书的所有 CA；

2） 当 CA 私钥泄露或怀疑泄露时，CA 应立即使用公开的文档说明该问题。

6.4.2 PKI 应用

6.4.2.1 证书格式

对证书格式的要求如下：

a） 签名算法 signature

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，（MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSA，（SHA-1，SHA-224，SHA-256）with DSA，（SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with ECDSA，（SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSASSA-PSS。

b） 颁发者 issuer

RDN 应支持下列属性：country，organization，organizational unit，distinguished name qualifier，state or province name，common name，serial number，locality，title，surname，given name，initials，pseudonym，generation qualifier，domain component，email address。

c） 主体 subject

RDN 应支持下列属性：country，organization，organizational unit，distinguished name qualifier，state or province name，common name，serial number，locality，title，surname，given name，initials，pseudonym，generation qualifier，domain component，email address。

d） 主体公钥信息 subjectPublicKeyInfo

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM2，RSA，RSASSA-PSS，RSAES-OAEP，DSA，DH，KEA，ECDSA，ECDH，ECMQV。

6.4.2.2 证书扩展

对证书扩展的要求如下：

a） 徽标 logotypes

应支持本扩展项。

b） IP 地址表示 iPAddressDelegation

应支持本扩展项。

c） AS 标识符表示 autonomousSystemIdentifierDelegation

应支持本扩展项。

d） 担保 warranty

应支持本扩展项。

e） WLAN 服务集合标识符 wLANSSID

应支持本扩展项。

f） 个人身份标识码 identityCode

应支持本扩展项。

g） 个人社会保险号 insuranceNumber

应支持本扩展项。

h) 企业工商注册号 iCRegistrationNumber
应支持本扩展项。

i) 企业组织机构代码 organizationCode
应支持本扩展项。

j) 企业税号 taxationNumber
应支持本扩展项。

6.4.2.3 CRL 格式

对 CRL 格式的要求如下：

a) 签名算法 signature
应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS。

b) 颁发者 issuer
RDN 应支持下列属性：country，organization，organizational unit，distinguished name qualifier，state or province name，common name，serial number，locality，title，surname，given name，initials，pseudonym，generation qualifier，domain component，email address。

6.4.2.4 OCSP 请求格式

对 OCSP 请求格式的要求如下：

a) 请求者名称 requestorName
不应使用 otherName。

b) 签名算法 signatureAlgorithm
应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS。

c) 请求的证书 reqCert
hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，MD5，SHA-1，SHA-256。

6.4.2.5 OCSP 响应格式

对 OCSP 响应格式的要求如下：

a) 签名算法 signatureAlgorithm
应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS。

b) 证书标识符 certID
hashAlgorithm 子项支持应国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512。

6.4.2.6 应用功能要求

应具备完整的源代码开发日志。

6.5 第五级:安全审计级

6.5.1 PKI 系统

6.5.1.1 证书格式

对证书格式的要求如下:

a) 序列号 serialNumber

长度应不小于 4 字节。

b) 签名算法 signature

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种:SM3 with SM2,(SHA-1,SHA-256)with RSA。

c) 主体公钥信息 subjectPublicKeyInfo

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种:SM2,RSA。

6.5.1.2 CRL 格式

签名算法 signature 应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种:SM3 with SM2,(SHA-1,SHA-256)with RSA。

6.5.1.3 OCSP 请求格式

对 OCSP 请求格式的要求如下:

a) 签名算法 signatureAlgorithm

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法:SM3 with SM2,(MD2,MD4,MD5,SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with RSA,(SHA-1,SHA-224,SHA-256)with DSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with ECDSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with RSASSA-PSS,GOST R 34.11-94 with (GOST R 34.10-94,GOST R 34.10-2001)。

b) 请求的证书 reqCert

hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法:SM3,MD2,MD4,MD5,SHA-1,SHA-224,SHA-256,SHA-384,SHA-512。

6.5.1.4 OCSP 响应格式

对 OCSP 响应格式的要求如下:

a) 签名算法 signatureAlgorithm

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种:SM3 with SM2,(SHA-1,SHA-256)with RSA。

b) 证书标识符 certID

hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种:SM3,SHA-1,SHA-256。

6.5.1.5 CP/CPS

应具备多种语言版本的 CP/CPS。

6.5.1.6 系统操作要求

对系统操作的要求如下：

a) CP/CPS 管理

1) 证书策略 OID 的生命周期不应小于 10 年；
2) 认证业务声明的生命周期不应高于 1 年；
3) 应具有指定的管理小组，用以评估和核准 CA 的证书策略和认证业务声明。

b) 信息发布与资料库职责

1) 资料库应提供 7×24 h 的服务，每年机器损坏的时间累计应不超过 0.5%，无故障运行时间不低于 20 000 h；
2) 并发处理连接数应不低于 1 000 个；
3) 资料库中的信息应在生成后 30 s 内进行更新。

c) 密钥更新请求的身份鉴别和证书撤销请求的身份鉴别

初始身份鉴别之后，应至少每 3 年重新对订户进行一次初始身份鉴别。

d) 证书更新和证书密钥更换

用于签名和加密的终端用户证书应至少每 3 年进行一次密钥更换。

e) 证书变更、撤销和挂起

1) 根 CA 发布的 CRL 有效期不应超过 35 天；
2) 如果子 CA 有撤销请求，根 CA 应在 18 h 之内处理完毕；
3) 颁发终端实体证书的 CA 颁发的 CRL 有效期不应超过 7 天。

f) 物理安全控制

应至少每 24 h 检查一遍 CA 设备，确保没有破坏物理安全的行为发生。

g) 审计日志处理流程

审计日志数据每年应至少检查 6 次，每次检查应至少覆盖审计日志数据的 25%。

h) 认证机构设施、管理和运作控制

1) CA 的记录数据应至少保存 10 年；
2) CA 应至少每 6 个月检查一次备份数据的完整性；
3) 根 CA 的证书有效期不应超过 26 年。

6.5.2 PKI 应用

6.5.2.1 证书格式

对证书格式的要求如下：

a) 签名算法 signature

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS，GOST R 34.11-94 with (GOST R 34.10-94，GOST R 34.10-2001)。

b) 主体公钥信息 subjectPublicKeyInfo

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM2，RSA，RSASSA-PSS，RSAES-OAEP，DSA，DH，KEA，ECDSA，ECDH，ECMQV，GOST R 34.10-94，GOST R 34.10-2001。

6.5.2.2 CRL 格式

签名算法 signature 应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS，GOST R 34.11-94 with (GOST R 34.10-94，GOST R 34.10-2001)。

6.5.2.3 OCSP 请求格式

对 OCSP 请求格式的要求如下：

a) 签名算法 signatureAlgorithm

应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(SHA-1，SHA-256) with RSA，(SHA-1，SHA-256) with RSASSA-PSS。

b) 请求的证书 reqCert

hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，SHA-1，SHA-256。

6.5.2.4 OCSP 响应格式

对 OCSP 响应格式的要求如下：

a) 签名算法 signatureAlgorithm

应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS。

b) 证书标识符 certID

hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512。

6.5.2.5 应用功能要求

对应用功能的要求如下：

a) 操作流程

所有操作应按照操作流程进行。

b) 审计

应至少每 7 天进行一次审计。

c) 额外保障

应提供第三方额外保障。

d) 源代码

应通过第三方的源代码安全审查。

附　录　A
（规范性附录）
PKI 系统评估内容列表

A.1　编解码方式

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
编码方式	应使用 BER 编码	应使用 DER 编码			
解码方式	应支持 DER 解码		应支持 BER 解码		

A.2　证书格式

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
version	取值应为 v1(0)、v2(1)或 v3(2)	取值应为 v3(2)			
serialNumber	1. 取值应为自然数； 2. 对于相同 CA 颁发的证书，每个证书序列号应只出现一次； 3. 长度应不大于 20 字节		长度应不大于 16 字节	长度应不大于 8 字节	长度应不小于 4 字节

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
signature	1. 应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，（MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSA，（SHA-1，SHA-224，SHA-256）with DSA，（SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with ECDSA，（SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSASSA-PSS，GOST R 34.11-94 with（GOST R 34.10-94，GOST R 34.10—2001）； 2. 本项取值应与 signatureAlgorithm 项取值一致	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，（MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSA，（SHA-1，SHA-224，SHA-256）with DSA，（SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with ECDSA，（SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSASSA-PSS	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，（MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSA，（SHA-1，SHA-224，SHA-256）with DSA，（SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSASSA-PSS	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，（SHA-1，SHA-256）with RSA，（SHA-1，SHA-256）with RSASSA-PSS	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，（SHA-1，SHA-256）with RSA
issuer	1. 应为非空的 X.501 DN； 2. RDN 应使用下列属性：country，organization，organizational unit，distinguished name qualifier，state or province name，common name，serial number，locality，title，surname，given name，initials，pseudonym，generation qualifier，domain component，或 email address； 3. 每个 RDN 应只有一个属性值	RDN 不应使用属性 distinguished name qualifier	RDN 应使用下列属性：country，organization，organizational unit，state or province name，locality，或 common name	1. RDN 应使用下列属性：country，organization，organizational unit，或 common name； 2. RDN 序列中属性的顺序应该为：country，organization，organizational unit，common name； 3. organizational unit 属性的出现次数应当为 3 次（含）以下	

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
validity	1. 应对 2049 年以前的时间按照 UTCTime 编码，2050 年（含）以后的时间按照 GeneralizedTime 编码； 2. notAfter 子项表示的时间应比 notBefore 子项表示的时间晚； 3. 使用 GeneralizedTime 格式时，不应编码为 99991231235959Z				
subject	1. RDN 应使用下列属性：country，organization，organizational unit，distinguished name qualifier，state or province name，common name，serial number，locality，title，surname，given name，initials，pseudonym，generation qualifier，domain component，或 email address； 2. 每个 RDN 应只有一个属性值； 3. 本项的 DN 为空时，subjectAltName 扩展项应包含主体名称信息，且标记为关键扩展	1. 应为非空的 X.501 DN； 2. RDN 不应使用属性 distinguished name qualifier	RDN 应使用下列属性：country，organization，organizational unit，state or province name，locality，或 common name	1. RDN 应使用下列属性：country，organization，organizational unit，或 common name； 2. RDN 序列中属性的顺序应该为：country，organization，organizational unit，common name； 3. organizational unit 属性的出现次数应当为 3 次（含）以下	
subjectPublicKeyInfo	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM2，RSA，RSASSA-PSS，RSAES-OAEP，DSA，DH，KEA，ECDSA，ECDH，ECMQV，GOST R 34.10—94，GOST R 34.10—2001	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM2，RSA，RSASSA-PSS，RSAES-OAEP，DSA，DH，KEA，ECDSA，ECDH，ECMQV	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM2，RSA，RSASSA-PSS，RSAES-OAEP，DSA	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM2，RSA，RSASSA-PSS，RSAES-OAEP	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM2，RSA

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
issuerUniqueID	当版本为 v1（0）时，不应使用本项	不应使用本项			
subjectUniqueID	当版本为 v1（0）时，不应使用本项	不应使用本项			

A.3 证书扩展

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
authorityKeyIdentifier		应在自签名证书以外的所有证书中使用	1. 应标记为非关键扩展； 2. 应使用 keyIdentifier 子项； 3. keyIdentifier 子项取值应使用 GB/T 20518—2006 的 5.2.3.2.1 中的方法 a)或 b)生成	1. keyIdentifier 子项取值应使用 GB/T 20518—2006 的 5.2.3.2.1 中的方法 a)生成； 2. keyIdentifier 子项取值应与颁发本证书的 CA 证书中 subjectKeyIdentifier 扩展项的 keyIdentifier 子项取值一致	
subjectKeyIdentifier		应在所有 CA 证书中使用	1. 应标记为非关键扩展； 2. 应使用 GB/T 20518—2006 的 5.2.3.2.1 中的方法 a)或 b)生成	应使用 GB/T 20518—2006 的 5.2.3.2.1 中的方法 a)生成	
keyUsage		1. 应在用于验证证书或者 CRL 中数字签名的证书中使用； 2. 应至少有一位值不为零	应在所有证书中使用		
certificatePolicies		1. 每个证书策略 OID 应只出现一次； 2. 应只在 CA 证书中使用 AnyPolicy OID	应在所有证书中使用	不应在任何证书中使用 AnyPolicy OID	

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
policyMappings		应只在 CA 证书中使用	1. 应在不同 CP 体系的交叉证书中使用； 2. issuerDomainPolicy 子项取值应为交叉证书颁发者证书的 certificatePolicies 扩展项中出现过的 CP OID		
subjectAltName			1. 应标记为非关键扩展； 2. 应使用 otherName、rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID 中的名称	不应使用 otherName	
issuerAltName			1. 应标记为非关键扩展； 2. 应使用 otherName、rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID 中的名称	不应使用 otherName	
subjectDirectoryAttributes			应标记为非关键扩展		
basicConstraints		应在所有 CA 证书中使用	1. 如果 cA 子项取值为 FALSE，keyUsage 扩展项的 keyCertSign 子项取值不应为 1； 2. pathLenConstraint 子项应只在 cA 子项取值为 TRUE 且 keyUsage 扩展项的 keyCertSign 子项取值为 1 时使用； 3. pathLenConstraint 子项出现时，取值应大于或等于 0		

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
nameConstraints			1. 应只在 CA 证书中使用； 2. 应使用 directoryName、rfc822Name、uniformResourceIdentifier、dNSName、iPAddress 中的名称； 3. minimum 子项取值应为 0，不应使用 maximum 子项		
policyConstraints			应只在 CA 证书中使用		
extKeyUsage			1. 应标记为非关键扩展； 2. 应只在终端实体证书中使用	不应使用 anyExtendedKeyUsage OID	
cRLDistributionPoints		1. 应在自签名证书以外的所有证书中使用； 2. distributionPoint 子项取值应包含 LDAP 或者 HTTP 形式的 URI	1. 应标记为非关键扩展； 2. reasons 子项应与 distributionPoint 子项或者 cRLIssuer 子项一起使用； 3. 如果证书颁发者与 CRL 颁发者不同，cRLIssuer 子项应出现，且取值包含 CRL 颁发者 DN； 4. 如果证书颁发者与 CRL 颁发者相同，distributionPoint 子项应出现且 cRLIssuer 子项不应出现	1. 应有包含所有撤销原因的 CRL 的 distributionPoint 子项； 2. cRLIssuer 子项中应仅包含 CRL 颁发者的 DN，并且其编码应与 CRL 颁发者的 DN 编码完全一致	
inhibitAnyPolicy			应只在 CA 证书中使用	skipCerts 子项取值应为 0	
freshestCRL			1. 应标记为非关键扩展； 2. 应在终端实体证书中使用； 3. distributionPoint 子项取值应包含 LDAP 或者 HTTP 形式的 URI		

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
authorityInfoAccess			1. 应标记为非关键扩展； 2. 应在所有终端实体证书中使用，accessMethod 子项取值应包含 id-ad-ocsp	当 accessMethod 子项取值为 id-ad-caIssuers 时，accessLocation 子项取值应为 HTTP 或者 LDAP 形式的 URI。	
subjectInfoAccess			1. 应标记为非关键扩展； 2. 当 accessMethod 子项取值为 id-ad-caRepository 时，accessLocation 子项取值应为 HTTP 或者 LDAP 形式的 URI	当 accessMethod 子项取值为 id-ad-timeStamping 时，accessLocation 子项取值类型应为 uniformResourceIdentifier、rfc822Name、dNSName、iPAddress 之一	
privateKeyUsagePeriod		应标记为非关键扩展		1. notBefore 子项和 notAfter 子项应使用 GeneralizedTime 格式编码； 2. notBefore 子项或 notAfter 子项应出现	
logotypes		应标记为非关键扩展，其格式和编码应符合 RFC 3709 的要求		不应使用 otherLogos 子项	
iPAddressDelegation		应标记为非关键扩展，其格式和编码应符合 RFC 3779 的要求		max 子项使用的 IP 地址，应至少要有一位为 1	
autonomous SystemIdentifierDelegation		应标记为非关键扩展，其格式和编码应符合 RFC 3779 的要求			
warranty		应标记为非关键扩展，其格式和编码应符合 RFC 4059 的要求			
wLANSSID		应标记为非关键扩展，其格式和编码应符合 RFC 4334 的要求			
identityCode		应标记为非关键扩展			
insuranceNumber		应标记为非关键扩展			
iCRegistrationNumber		应标记为非关键扩展			

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
organizationCode		应标记为非关键扩展			
taxationNumber		应标记为非关键扩展			
私有扩展	应标记为非关键扩展				

A.4 CRL 格式

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
version	不应使用本项或取值为 v2(1)	取值应为 v2(1)			
signature	1. 应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS，GOST R 34.11-94 with (GOST R 34.10-94，GOST R 34.10—2001)； 2. 本项取值应与 signatureAlgorithm 项取值一致	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(SHA-1，SHA-256) with RSA，(SHA-1，SHA-256) with RSASSA-PSS	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，(SHA-1，SHA-256) with RSA

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
issuer	1. 应为非空的 X.501 DN； 2. RDN 应使用下列属性：country，organization，organizational unit，distinguished name qualifier，state or province name，common name，serial number，locality，title，surname，given name，initials，pseudonym，generation qualifier，domain component，或 email address； 3. 每个 RDN 应只有一个属性值	RDN 不应使用属性 distinguished name qualifier	RDN 应使用下列属性：country，organization，organizational unit，state or province name，locality，或 common name	1. RDN 应使用下列属性：country，organization，organizational unit，或 common name； 2. RDN 序列中属性的顺序应该为：country，organization，organizational unit，common name； 3. organizational unit 属性的出现次数应当为 3 次（含）以下	
thisUpdate	应对 2049 年以前的时间按照 UTCTime 编码，2050 年（含）以后的时间按照 GeneralizedTime 编码				
nextUpdate	1. 应对 2049 年以前的时间按照 UTCTime 编码，2050 年（含）以后的时间按照 GeneralizedTime 编码； 2. 本项表示的时间应比 thisUpdate 项表示的时间晚	应在所有 CRL 中使用			
revokedCertificates	没有被撤销证书时，不应使用本项				

A.5 CRL 扩展

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
authorityKeyIdentifier		应在所有 CRL 中使用	1. 应标记为非关键扩展； 2. 应使用 keyIdentifier 子项； 3. keyIdentifier 子项取值应使用 GB/T 20518—2006 的 5.2.3.2.1 中的方法 a)或 b)生成	keyIdentifier 子项取值应使用 GB/T 20518—2006 的 5.2.3.2.1 中的方法 a)生成	
issuerAltName			1. 应标记为非关键扩展； 2. 应使用 otherName、rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID 中的名称	不应使用 otherName	
cRLNumber		长度应不大于 20 字节	1. 应标记为非关键扩展； 2. 应在所有 CRL 中使用； 3. 取值应为递增序号； 4. 提供相同信息的完全 CRL 和增量 CRL 中，本扩展项取值应相同； 5. 长度应不大于 16 字节	长度应不大于 8 字节	
deltaCRLIndicator		应在所有增量 CRL 中使用	1. 两个完全 CRL 之间的信息差异，应与前一次 CRL 颁发之后的所有增量 CRL 信息之和相同； 2. 同一个颁发者颁发的基本 CRL 和增量 CRL 应使用同一个私钥签名		

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
issuingDistributionPoints			1. 如果 distributionPoint 子项出现，内容应非空； 2. 如果 distributionPoint 子项未出现，则 CRL 应包含所有撤销证书； 3. 如果 onlySomeReasons 子项出现，CRL 中所有 Entry 应有 unspecified 以外的撤销理由； 4. 如果 onlyContainsUserCerts 子项、onlyContainsCACerts 子项、indirectCRL 子项、onlyContainsAttributeCerts 子项都取值为 FALSE，则 distributionPoint 子项或 onlySomeReasons 子项应出现； 5. 基本 CRL 和增量 CRL 使用的本扩展取值应相同	1. 如果 revokedCertificates 项只包含 CRL 颁发者颁发的证书，indirectCRL 子项取值应为 FALSE； 2. 如果 revokedCertificates 项只包含终端实体证书，onlyContainsUserCerts 子项取值应为 TRUE； 3. 如果 revokedCertificates 项只包含 CA 证书，onlyContainsCACerts 子项取值应为 TRUE	
freshestCRL			1. 应标记为非关键扩展； 2. 不应使用 reasons 子项和 cRLIssuer 子项； 3. 不应在增量 CRL 中使用		
authorityInfoAccess			应标记为非关键扩展	当 accessMethod 子项取值为 id-ad-caIssuers 时，accessLocation 子项取值应为 HTTP 或者 LDAP 形式的 URI	

A.6 CRL Entry 扩展

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
reasonCode			1. 应标记为非关键扩展； 2. 本扩展项取值不应为 0； 3. 本扩展项取值为 removeFromCRL 时，CRL 应为增量 CRL		
holdInstructionCode			应标记为非关键扩展		
invalidityDate			1. 应标记为非关键扩展； 2. 应在所有 Entry 中出现		
certificateIssuer			如果 CRL 颁发者与证书颁发者不同，本扩展项应出现		

A.7 OCSP 请求格式

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
version		应支持取值为 v1(0)			
requestorName		应至少支持 rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID 中的一种名称			

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
signatureAlgorithm		应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，（SHA-1，SHA-256）with RSA，（SHA-1，SHA-256）with RSASSA-PSS	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256）with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSASSA-PSS	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256）with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256）with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS，GOST R 34.11-94 with (GOST R 34.10-94，GOST R 34.10—2001)。
requestList		支持请求单个证书，包含单个 Request	支持请求多个证书，包含多个 Request		
reqCert		hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，SHA-1，SHA-256	hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，SHA-1，SHA-256，MD5	hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512	hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512

A.8 OCSP 响应格式

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
responseStatus		取值应为 successful，malformedRequest，internalError，tryLater，sigRequired，unauthorized 之一			
responseBytes		应使用本项			
responseType		取值应为 id-pkix-ocsp-basic			
signatureAlgorithm		应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，（MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSA，（SHA-1，SHA-224，SHA-256）with DSA，（SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with ECDSA，（SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSASSA-PSS	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，（MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSA，（SHA-1，SHA-224，SHA-256）with DSA，（SHA-1，SHA-224，SHA-256，SHA-384，SHA-512）with RSASSA-PSS	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，（SHA-1，SHA-256）with RSA，（SHA-1，SHA-256）with RSASSA-PSS	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3 with SM2，（SHA-1，SHA-256）with RSA
signature			OCSP 服务器证书 extKeyUsage 扩展项应包含 id-kp-OCSPSigning OID		
responderID		1. byName 子项取值应为响应者 DN； 2. byKey 子项取值应为对响应者公钥使用 SHA-1 算法进行哈希运算后得出的值			

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
producedAt		应使用 GeneralizedTime 格式编码			
responses		支持响应单个证书，包含单个 SingleResponse	支持响应多个证书，包含多个 SingleResponse		
certID		hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512	hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512	hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，MD5，SHA-1，SHA-256	hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，SHA-1，SHA-256
certStatus		取值应为 good，revoked，unknown 之一			
thisUpdate		应使用 GeneralizedTime 格式编码			
nextUpdate		应使用 GeneralizedTime 格式编码			

A.9 OCSP 扩展

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
nonce		应标记为非关键扩展	如果 OCSP 请求中使用本扩展项，OCSP 响应应在 responseExtensions 项中使用本扩展项，且取值相同		
cRLReferences		应标记为非关键扩展	使用本扩展项时，crlUrl 子项、crlNum 子项和 crlTime 子项应至少有一项被使用		

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
acceptableResponseTypes			1. 应支持本扩展项； 2. 应支持使用 id-pkix-ocsp-basic OID		
archiveCutoff		应标记为非关键扩展	应使用 GeneralizedTime 格式编码		
serviceLocator			应支持本扩展项		
cRLEntryExtension			应满足 A.6 中功能完善级的要求		

A.10 CP/CPS

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
CP/CPS		应具备符合 RFC 3647 要求的 CPS	应具备符合 RFC 3647 要求的 CP	应具备英语版本的 CP/CPS	应具备多种语言版本的 CP/CPS
CP/CPS 整体要求			1. 应说明如下章节：概括性描述，信息发布与资料库职责，身份标识与鉴别，证书生命周期操作要求，认证机构设施、管理和运作控制，认证机构技术安全控制，证书、证书撤销列表和在线证书状态协议，认证机构合规性审计和相关评估，其他商业和法律条款； 2. 应能够通过公开途径获得	支持的 CP OID 应在 CP/CPS 中描述	
概括性描述			应说明如下章节：概述、文档名称与标识、参与方和证书应用	应说明如下章节：策略管理、定义和缩写	
信息发布与资料库职责			应说明如下章节：资料库的标识和责任方、信息的发布、信息发布的时间和频率、资料库的访问控制		

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
身份标识与鉴别			应说明如下章节：命名、初始申请证书的身份鉴别、密钥更新请求的身份鉴别、证书撤销请求的身份鉴别		
证书生命周期操作要求			应说明如下章节：证书申请、证书申请的处理、证书颁发、证书接受、密钥对和证书的使用、证书更新、证书密钥更换、证书变更、证书撤销和挂起、证书状态服务	应说明如下章节：认证服务订购终止、密钥托管和恢复	
认证机构设施、管理和运作控制			应说明如下章节：物理安全控制、流程控制、人员控制	应说明如下章节：审计日志处理流程、记录归档、认证机构密钥更替、事故和灾难恢复、认证机构服务终止	
认证机构技术安全控制			应说明如下章节：密钥对的生成和安装、私钥保护和密码模块的工程控制、密钥激活数据、计算机安全控制、生命周期安全控制、网络安全控制	应说明如下章节：密钥对管理的其他方面、时间标记	
证书、证书撤销列表和在线证书状态协议			应说明如下章节：证书、证书撤销列表、在线证书状态协议		
认证机构合规性审计和相关评估				应说明如下章节：评估所涵盖的主题和评估的方法列表、评估的频率、评估者的身份和资质、评估者与被评估实体之间的关系、对评估中出现的不足所采取的措施、评估结果的传达	

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
其他商业和法律条款				应说明如下章节：费用、财务责任、业务信息保密、个人隐私保护、知识产权、陈述和担保、免责申明、有限责任、赔偿、有效期限和终止、对参与者的个别通告与沟通、修订、争议处理、管辖法律、与适用法律的符合性、杂项条款、其他条款	

A.11 系统功能要求

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
颁发证书	应具备此功能				
颁发交叉证书		应具备此功能			
颁发证书撤销状态信息	应颁发完全 CRL	应颁发增量 CRL 或提供 OCSP 服务	应颁发增量 CRL 和提供 OCSP 服务		
CP/CPS 发布			应通过 HTTP 或者 LDAP 发布 CP/CPS		
证书发布		应通过 HTTP 或者 LDAP 发布除终端实体证书之外的所有证书	应通过 HTTP 和 LDAP 发布所有证书。通过 LDAP 发布证书的方式应符合 RFC 4523 的要求	通过 HTTP 发布证书的方式应符合 RFC 4387 的要求	
CRL 发布		应通过 HTTP 或者 LDAP 发布所有 CRL	应通过 HTTP 和 LDAP 发布所有 CRL。通过 LDAP 发布 CRL 的方式应符合 RFC 4523 的要求	通过 HTTP 发布 CRL 的方式应符合 RFC 4387 的要求	

A.12 系统操作要求

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
CP/CPS 管理			1. 应指定 CA 支持的证书策略 OID； 2. CA 应对其订户和依赖方公开证书策略和认证业务声明	证书策略 OID 的生命周期不应小于 4 年	1. 证书策略 OID 的生命周期不应小于 10 年； 2. 认证业务声明的生命周期不应高于 1 年； 3. 应具有指定的管理小组，用以评估和核准 CA 的证书策略和认证业务声明
信息发布与资料库职责					1. 资料库应提供 7×24 h 的服务，每年机器损坏的时间累计应不超过 0.5%，无故障运行时间不低于 20 000 h； 2. 并发处理连接数应不低于 1 000 个； 3. 资料库中的信息应在生成后 30 s内进行更新。
个人隐私保护			CA 所收集的订户信息在未经订户许可的情况下不应被泄露(法律规定的情况除外)		
身份标识与鉴别			1. 证书中不应包含未经验证的信息； 2. 每个终端实体在证书中应拥有可区别的唯一 DN； 3. 应能够通过如下几个类别的用户证件对订户进行身份验证：身份证、护照、驾驶证		

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
密钥更新请求的身份鉴别和证书撤销请求的身份鉴别			身份鉴别应达到初始申请证书的身份鉴别强度	初始身份鉴别之后，应至少每 9 年重新对订户进行一次初始身份鉴别	初始身份鉴别之后，应至少每 3 年重新对订户进行一次初始身份鉴别
证书申请			1. 订户应提供自身身份信息的证明； 2. 订户应提供所有需要出现在证书中的信息的证明	1. 颁发证书之前，全部证书内容（包括扩展项）应经过审核； 2. 证书应在申请完成后 30 天内颁发	
证书更新和证书密钥更换			应由拥有已颁发证书的订户提出请求		用于签名和加密的终端用户证书应至少每 3 年进行一次密钥更换
证书变更、撤销和挂起			1. 如果证书中任何信息发生改变，应将此证书撤销； 2. CA 应支持订户的撤销请求	CA 应在 24 h 之内将订户的撤销请求处理完毕	1. 根 CA 发布的 CRL 有效期不应超过 35 天； 2. 如果子 CA 有撤销请求，根 CA 应在 18 h 之内处理完毕； 3. 颁发终端实体证书的 CA 颁发的 CRL 有效期不应超过 7 天
物理安全控制			1. 仅有授权用户可以进入 CA 设备所在的安全区域，进出时间和人员信息应记录日志； 2. CA 设备所在区域应具备空调设备等以保证系统正常运转； 3. CA 设备应满足防水、防火等要求； 4. CA 设备应保证其存储介质不会因温度、湿度和电磁等因素而失效； 5. CA 系统应具备离线备份功能		应至少每 24 h 检查一遍 CA 设备，确保没有破坏物理安全的行为发生
流程控制			应在至少两人同时在场的情况下进行 CA 密钥的产生、激活以及备份操作	1. 审计员不应在系统中拥有除了审计之外的其他权限； 2. RA 操作员应只能在 RA 系统中拥有权限	

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
人员控制				系统中的所有人员应没有犯罪记录	
审计日志处理流程				除审计程序之外，审计日志数据不应被任何人员或者程序查看或修改	审计日志数据每年应至少检查6次，每次检查应至少覆盖审计日志数据的25%
认证机构设施、管理和运作控制					1. CA的记录数据应至少保存10年； 2. CA应至少每6个月检查一次备份数据的完整性； 3. 根CA的证书有效期不应超过26年
密钥对的生成和安装				在初始分发自签名证书的时候，CA应提供其证书的防篡改机制	
密钥激活数据				1. CA私钥激活应使用多因素认证（例如口令结合生物特征，或口令结合智能卡）； 2. 如果密码模块中使用了PIN码或口令，该PIN码或口令，应至少每3个月修改一次	
私钥保护和密码模块的工程控制				1. 在密钥对的生命周期结束时，CA私钥的所有部分应该被完全销毁； 2. 如果密码设备需要永久性地从系统中移除，应清除其中的所有密钥信息	

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
事故和灾难恢复				1. 当 CA 私钥泄露或怀疑泄露时，CA 应该立即主动通知其已经颁发了交叉证书的所有 CA； 2. 当 CA 私钥泄露或怀疑泄露时，CA 应立即使用公开的文档说明该问题	

附 录 B
（规范性附录）
PKI 应用评估内容列表

B.1 编解码方式

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
编码方式	应使用 BER 编码	应使用 DER 编码			
解码方式	应支持 DER 解码		应支持 BER 解码		

B.2 证书格式

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
version	应支持取值为 v1(0)、v2(1)或 v3(2)		应支持取值为 v1(0)、v2(1)和 v3(2)		
serialNumber	支持长度应至少为 8 字节	支持长度应至少为 16 字节	支持长度应至少为 20 字节		
signature	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(SHA-1，SHA-256)with RSA	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(SHA-1，SHA-256) with RSA，(SHA-1，SHA-256) with RSASSA-PSS	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512)with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512)with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSASSA-PSS	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with RSA，(SHA-1，SHA-224，SHA-256) with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512) with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512)with RSASSA-PSS，GOST R 34.11-94 with (GOST R 34.10-94，GOST R 34.10—2001)

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
issuer	RDN 应支持下列属性：country，organization，organizational unit，common name		RDN 应支持下列属性：country，organization，organizational unit，state or province name，locality，common name	RDN 应支持下列属性：country，organization，organizational unit，distinguished name qualifier，state or province name，common name，serial number，locality，title，surname，given name，initials，pseudonym，generation qualifier，domain component，email address	
validity	应支持 2049 年以前的时间按照 UTCTime 解码，2050 年（含）以后的时间按照 GeneralizedTime 解码	应支持任意格式的时间解码			
subject	RDN 应支持下列属性：country，organization，organizational unit，common name	本项为空时，支持从 subjectAltName 扩展项中获取主体名称信息	RDN 应支持下列属性：country，organization，organizational unit，state or province name，locality，common name	RDN 应支持下列属性：country，organization，organizational unit，distinguished name qualifier，state or province name，common name，serial number，locality，title，surname，given name，initials，pseudonym，generation qualifier，domain component，email address	

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
subjectPublicKeyInfo	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM2，RSA	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM2，RSA，RSASSA-PSS，RSAES-OAEP	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM2，RSA，RSASSA-PSS，RSAES-OAEP，DSA	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM2，RSA，RSASSA-PSS，RSAES-OAEP，DSA，DH，KEA，ECDSA，ECDH，ECMQV	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM2，RSA，RSASSA-PSS，RSAES-OAEP，DSA，DH，KEA，ECDSA，ECDH，ECMQV，GOST R 34.10-94，GOST R 34.10—2001
issuerUniqueID		应支持本项			
subjectUniqueID		应支持本项			

B.3 证书扩展

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
authorityKeyIdentifier		应支持本扩展项			
subjectKeyIdentifier		应支持本扩展项			
keyUsage		应支持本扩展项			
certificatePolicies		应支持本扩展项			
policyMappings			应支持本扩展项		
subjectAltName		1. 应支持本扩展项； 2. 应能够识别以下类型的名称：rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID			

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
issuerAltName		1. 应支持本扩展项； 2. 应能够识别以下类型的名称：rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID			
subjectDirectoryAttributes			应支持本扩展项		
basicConstraints		应支持本扩展项			
nameConstraints			应支持本扩展项		
policyConstraints			应支持本扩展项		
extKeyUsage			应支持本扩展项		
cRLDistributionPoints		1. 应支持本扩展项； 2. distributionPoint 子项支持使用 LDAP 或 HTTP 形式的 URI			
inhibitAnyPolicy			应支持本扩展项		
freshestCRL			1. 应支持本扩展项； 2. distributionPoint 子项支持使用 LDAP 或 HTTP 形式的 URI		

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
authorityInfoAccess			1. 应支持本扩展项； 2. accessMethod 子项应支持使用 id-ad-ocsp		
subjectInfoAccess			应支持本扩展项		
privateKeyUsagePeriod			应支持本扩展项		
logotypes				应支持本扩展项	
iPAddressDelegation				应支持本扩展项	
autonomousSystemIdentifierDelegation				应支持本扩展项	
warranty				应支持本扩展项	
wLANSSID				应支持本扩展项	
identityCode				应支持本扩展项	
insuranceNumber				应支持本扩展项	
iCRegistrationNumber				应支持本扩展项	
organizationCode				应支持本扩展项	
taxationNumber				应支持本扩展项	

B.4 CRL 格式

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
version	应支持本项不出现或取值为 v2(1)		应支持本项不出现和取值为 v2(1)		
signature	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法:SM3 with SM2,(SHA-1,SHA-256)with RSA	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法:SM3 with SM2,(SHA-1,SHA-256)with RSA,(SHA-1,SHA-256)with RSASSA-PSS	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法:SM3 with SM2,(MD5,SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with RSA,(SHA-1,SHA-224,SHA-256)with DSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with RSASSA-PSS	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法:SM3 with SM2,(MD5,SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with RSA,(SHA-1,SHA-224,SHA-256)with DSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with ECDSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with RSASSA-PSS	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法:SM3 with SM2,(MD2,MD4,MD5,SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with RSA,(SHA-1,SHA-224,SHA-256)with DSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with ECDSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with RSASSA-PSS,GOST R 34.11-94 with (GOST R 34.10-94,GOST R 34.10—2001)
issuer	RDN 应支持下列属性:country,organization,organizational unit,common name		RDN 应支持下列属性:country,organization,organizational unit,state or province name,locality,common name	RDN 应支持下列属性:country,organization,organizational unit,distinguished name qualifier,state or province name,common name,serial number,locality,title,surname,given name,initials,pseudonym,generation qualifier,domain component,email address	

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
thisUpdate	应支持 2049 年以前的时间按照 UTCTime 解码，2050 年（含）以后的时间按照 GeneralizedTime 解码	应支持任意格式的时间解码			
nextUpdate	应支持 2049 年以前的时间按照 UTCTime 解码，2050 年（含）以后的时间按照 GeneralizedTime 解码	应支持任意格式的时间解码			
revokedCertificates	应支持本项				

B.5 CRL 扩展

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
authorityKeyIdentifier		应支持本扩展项			
issuerAltName		1. 应支持本扩展项； 2. 应能够识别 rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID 类型的名称			
cRLNumber		1. 应支持本扩展项； 2. 支持长度应至少为 20 字节			
deltaCRLIndicator		应支持本扩展项			
issuingDistributionPoints			应支持本扩展项		
freshestCRL			应支持本扩展项		
authorityInfoAccess			应支持本扩展项		

B.6 CRL Entry 扩展

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
reasonCode		应支持本扩展项			
holdInstructionCode			应支持本扩展项		
invalidityDate		应支持本扩展项			
certificateIssuer		应支持本扩展项			

B.7 OCSP 请求格式

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
version		取值应为 v1(0)			
requestorName		应使用 otherName、rfc822Name、dNSName、x400Address、directoryName、ediPartyName、uniformResourceIdentifier、iPAddress、registeredID 中的一种名称		不应使用 otherName	
signatureAlgorithm		应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种:SM3 with SM2,(MD2,MD4,MD5,SHA-1,SHA-224,SHA-256,SHA-384,SHA-512) with RSA,(SHA-1,SHA-224,SHA-256) with DSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with ECDSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512) with RSASSA-PSS,GOST R 34.11-94 with (GOST R 34.10-94,GOST R 34.10—2001)	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种:SM3 with SM2,(MD5,SHA-1,SHA-224,SHA-256,SHA-384,SHA-512) with RSA,(SHA-1,SHA-224,SHA-256) with DSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512) with ECDSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512)with RSASSA-PSS	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种:SM3 with SM2,(MD5,SHA-1,SHA-224,SHA-256,SHA-384,SHA-512) with RSA,(SHA-1,SHA-224,SHA-256) with DSA,(SHA-1,SHA-224,SHA-256,SHA-384,SHA-512) with RSASSA-PSS	应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种:SM3 with SM2,(SHA-1,SHA-256) with RSA,(SHA-1,SHA-256)with RSASSA-PSS

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
requestList		应能够请求单个证书，包含单个 Request	应能够请求多个证书，包含多个 Request		
reqCert		hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512	hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512	hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，MD5，SHA-1，SHA-256	hashAlgorithm 子项应使用国家密码管理局批准的算法。经国家密码管理局许可后可使用下列算法中的一种：SM3，SHA-1，SHA-256

B.8 OCSP 响应格式

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
responseStatus		应支持取值为 successful，malformedRequest，internalError，tryLater，sigRequired，unauthorized			
responseType		支持取值为 id-pkix-ocsp-basic			

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
signatureAlgorithm		应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(SHA-1，SHA-256)with RSA	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(SHA-1，SHA-256)with RSA，(SHA-1，SHA-256)with RSASSA-PSS	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512)with RSA，(SHA-1，SHA-224，SHA-256)with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512)with RSASSA-PSS	应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3 with SM2，(MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512)with RSA，(SHA-1，SHA-224，SHA-256)with DSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512)with ECDSA，(SHA-1，SHA-224，SHA-256，SHA-384，SHA-512)with RSASSA-PSS
responderID		支持使用 byName 或 byKey			
producedAt		应能够正常解码			
responses		取值为单个 SingleResponse 时，应能够正常解码	取值为多个 SingleResponse 时，应能够正常解码		
certID		hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，SHA-1，SHA-256	hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，MD5，SHA-1，SHA-256	hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512	hashAlgorithm 子项应支持国家密码管理局批准的算法。应支持下列算法中经国家密码管理局许可的算法：SM3，MD2，MD4，MD5，SHA-1，SHA-224，SHA-256，SHA-384，SHA-512
certStatus		应支持取值为 good、revoked、unknown			
thisUpdate		应能够正常解码			
nextUpdate		应能够正常解码			

B.9 OCSP 扩展

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
nonce		应标记为非关键扩展	应支持本扩展项		
cRLReferences			应支持本扩展项		
acceptableResponseTypes		应标记为非关键扩展	应包含取值为 id-pkix-ocsp-basic 的 OID		
archiveCutoff			应支持本扩展项		
serviceLocator		应标记为非关键扩展	1. issuer 子项取值应与被请求证书的 issuer 项取值相同； 2. locator 子项取值应与被请求证书的 authorityInfoAccess 扩展项的取值相同		
cRLEntryExtension		应满足 B.6 中内容明确级的要求	应满足 B.6 中功能完善级的要求		

B.10 应用功能要求

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
证书解码	应支持证书基本域	应支持证书扩展			
CRL 解码	应支持 CRL 基本域	应支持 CRL 扩展和 CRL Entry 扩展			
OCSP		应支持 OCSP 基本域	应支持 OCSP 扩展		

表（续）

	格式正确级	内容明确级	功能完善级	执行标准化级	安全审计级
操作流程			应提供操作流程		所有操作应按照操作流程进行
审计			应具备审计功能		应至少每 7 天进行一次审计
额外保障					应提供第三方额外保障
源代码			应提供完整的源代码供第三方检查	应具备完整的源代码开发日志	应通过第三方的源代码安全审查。

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 公钥基础设施
PKI 互操作性评估准则
GB/T 29241—2012
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100013)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:010-68522006
2013 年 5 月第一版
*
书号:155066·1-46990

GB/T 29241-2012