21. RFC 3779

名称：X.509 Extensions for IP Addresses and AS Identifiers。

发布日期：2004-06。

简述：定义了两个 X.509 v3 证书扩展项。第一项绑定 IP 地址列表或 IP 前缀，第二项绑定自治系统标识列表。其目的是使证书使用者有权限访问这些系统和 IP 地址。

22. RFC 3820

名称：Internet X.509 Public Key Infrastructure（PKI）Proxy Certificate Profile。

发布日期：2004-06。

简述：描述了在互联网使用的代理证书格式。代理证书来源于实体证书，相比实体证书，代理证书在应用系统使用的权限受限。

23. RFC 4055

名称：Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List（CRL）Profile。

发布日期：2005-06。

状态：被 RFC5756 更新。

简述：描述了 RSASSA-PSS（RSA Probabilistic Signature Scheme）、RSAES-OAEP（RSA Encryption Scheme - Optimal Asymmetric Encryption Padding）算法，以及应用于 PKCS#1 的哈希函数算法，包括编码格式、算法标识符、参数格式。

24. RFC 4158

名称：Internet X.509 Public Key Infrastructure: Certification Path Building。

发布日期：2005-09。

简述：对指导开发者构建证书认证路径提供指南和建议。

25. RFC 4210

名称：Internet X.509 Public Key Infrastructure Certificate Management Protocol（CMP）。

发布日期：2005-09。

状态：被 RFC6712 更新。

简述：替代 RFC2510。描述了互联网 X.509 PKI 证书管理协议 CMP，定义了 X.509 v3 证书生成和管理协议消息。CMP 提供了 PKI 组成部分之间的在线交互消息，包括 CA 和客户系统之间的数据交换。

26. RFC 4211

名称：Internet X.509 Public Key Infrastructure Certificate Request Message Format（CRMF）。

发布日期：2005-09。

简述：替代 RFC2511。描述了证书请求消息格式（CRMF）。它被用来向 CA 传递一个产生 X.509 证书请求（可能通过 RA）。请求消息一般包括公钥和有关的注册信息。

27. RFC 4325

名称：Internet X.509 Public Key Infrastructure Authority Information Access Certificate

Revocation List（CRL）Extension。

发布日期：2005-12。

状态：被 RFC5280 替代。

简述：定义了 CRL 扩展项，即机构信息访问扩展项，此扩展项便于发现和获取 CRL 发布者证书。

28. RFC 4387

名称：Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP。

发布日期：2006-02。

简述：描述了使用 HTTP/HTTPS 从 PKI 资源库中获取证书和证书撤销列表的接口。

29. RFC 4476

名称：Attribute Certificate（AC）Policies Extension。

发布日期：2006-05。

简述：定义了属性证书策略扩展项。

30. RFC 4630

名称：Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List（CRL）Profile。

发布日期：2006-08。

状态：被 RFC5280 替代。

简述：更新了对 DirectoryString 类型数据的处理方法。建议使用 UTF8String 和 PrintableString 类型数据。

31. RFC 4985

名称：Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name。

发布日期：2007-08。

简述：在 X.509 的使用者替代名扩展项中，对 otherName 字段定义了新名称格式，以允许证书使用者关联服务名称和 DNS 服务资源记录域名称。

32. RFC 5019

名称：The Lightweight Online Certificate Status Protocol（OCSP）Profile for High-Volume Environments。

发布日期：2007-09。

简述：定义了在线证书状态协议（OCSP）的服务框架，以解决在大规模（高容量）公钥基础设施使用 OCSP 的可扩展性问题，或在需要 PKI 的环境中提供轻量级解决方案，以尽量减少通信带宽和客户端处理。

33. RFC 5055

名称：Server-Based Certificate Validation Protocol（SCVP）。

发布日期：2007-12。

简述：描述了客户端委托服务端进行证书路径构建和证书路径验证，服务端依据验证策略进行证书路径构建和证书路径验证，以简化客户端实现和允许使用预定义的验证策略。

34. RFC 5272

名称：Certificate Management over CMS（CMC）。

发布日期：2008-06。

状态：被 RFC6402 更新。

简述：替代 RFC2797。定义了使用 CMS 进行证书管理的协议，以满足基于 CMS 和 PKCS10 进行证书服务的接口需求，以及满足仅加密密钥证书注册协议请求。

35. RFC 5280

名称：Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List（CRL）Profile。

发布日期：2008-05。

状态：被 RFC6818 更新。

简述：替代 RFC3280、RFC4325、RFC4630。描述了 X.509 v3 证书和 X.509 v2 的证书撤销列表（CRL）在互联网的使用。详细描述了 X.509 v3 证书格式及有关互联网名格式和语义的附加信息，并描述了证书标准扩展和两项与互联网相关的扩展。详细描述了 X.509 v2 证书撤销列表格式、标准扩展及互联网相关的扩展。

36. RFC 5480

名称：Elliptic Curve Cryptography Subject Public Key Information。

发布日期：2009-03。

简述：描述了使用者证书中支持椭圆曲线密码公钥信息的语法和语义。

37. RFC 5636

名称：Traceable Anonymous Certificate。

发布日期：2009-08。

简述：定义了一个实用的体系结构和协议，使证书使用者采用化名方式的 X.509 证书以提供身份保密性，又能保证需要时把此证书映射到真正的用户。

38. RFC 5697

名称：Other Certificates Extension。

发布日期：2009-11。

简述：定义了一个扩展项，使一个实体的一系列证书能够关联起来，在检索应用信息时，可以使用此数据而不需要考虑证书的更新。

39. RFC 5755

名称：An Internet Attribute Certificate Profile for Authorization。

发布日期：2010-01。

简述：替代 RFC3281。描述了基于授权的属性证书。

40. RFC 5758

名称：Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA。

发布日期：2010-01。

简述：更新 RFC3279。描述了当使用 SHA-224、SHA-256、SHA-384 或 SHA-512 作为哈希算法时，DSA 和 ECDSA 签名算法的标识符和 ASN.1 编码规则。适用于签发 X.509 证书和证书撤销列表签名。

41. RFC 5816

名称：ESSCertIDv2 Update for RFC 3161。

发布日期：2010-04。

简述：更新了 RFC3161。允许使用在 RFC5035 定义的 ESSCertIDv2 数据类型引用签名者证书哈希值。

42. RFC 5912

名称：New ASN.1 Modules for the Public Key Infrastructure Using X.509（PKIX）。

发布日期：2010-06。

状态：被 RFC6960 更新。

简述：更新 PKIX 证书格式及关联格式的 ASN.1 编码与 2002 年版本的 ASN.1 标准一致。没有更改生成后的实际数据格式，只是更改了语法。

43. RFC 6025

名称：ASN.1 Translation。

发布日期：2010-10。

简述：提供从一个 ASN.1 版本转换到另一个 ASN.1 版本模块的语法指南，以规范 ASN.1 模块作者和实现者。

44. RFC 6170

名称：Internet X.509 Public Key Infrastructure—Certificate Image。

发布日期：2011-05。

简述：更新 RFC3709。通过定义一个新的 RFC3709 otherLogos 类型，以可视化方式绑定证书图像到公钥证书中。

45. RFC 6277

名称：Online Certificate Status Protocol Algorithm Agility。

发布日期：2011-06。

状态：被 RFC6960 替代。

简述：规定了 OCSP 服务端签名算法选择规则及扩展，以允许客户端通知服务端其支持的特定签名算法。

46. RFC 6402

名称：Certificate Management over CMS（CMC）Updates。

发布日期：2011-11。

简述：更新了 RFC5272、RFC5273 和 RFC5274。包含一组对 CMC 基础语法的更新。新项目有：定义服务端密钥产生策略的新控制，定义使用者信息访问值以标识 CMC 服务端，注册运行 CMC 服务的 TCP/IP 端口号。

47. RFC 6712

名称：Internet X.509 Public Key Infrastructure—HTTP Transfer for the Certificate Management Protocol（CMP）。

发布日期：2012-09。

简述：更新了 RFC4210。描述了如何通过 HTTP 协议承载 CMP（证书管理协议）。

48. RFC 6818

名称：Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List（CRL）Profile。

发布日期：2013-01。

简述：更新 RFC5280。本文档更新了证书策略中 explicitText 字段可接受编码方法，以及转换国际域名标签到 ASCII 的规则。提供了一些对使用自签名证书、信任链和一些安全注意事项的说明。

49. RFC 6960

名称：X.509 Internet Public Key Infrastructure Online Certificate Status Protocol（OCSP）。

发布日期：2013-06。

简述：替代 RFC2560 和 RFC6277，更新 RFC5912。描述了在不需要 CRL（证书撤销列表）的情况下确定当前证书状态的有用协议。

50. RFC 7030

名称：Enrollment over Secure Transport。

发布日期：2013-10。

简述：描述了使用 CMC（Certificate Management over CMS）通过安全传输进行客户端证书注册的框架。

29.4 Microsoft 规范

在 PKI 应用中，使用较多的是 CryptoAPI 或 CNG 接口库。

1. CryptoAPI

Windows CryptoAPI 是微软公司提出的安全加密应用服务框架，它提供了在 Win32 环境下使用认证、编码、加密和签名等安全服务的标准加密接口，用于增强应用程序的安全性与可控性。应用开发者在不了解复杂的加密机制和加密算法的情况下，可以简便、快速