工作组，负责与 X.509 有关的规范管理。PKIX 工作组从 1995 年 10 月 26 日开始启动，到 2013 年 10 月 31 日关闭。在近 20 年间，发布的 RFC 规范主要包括：

RFC 2459：Internet X.509 Public Key Infrastructure Certificate and CRL Profile，1999-01，被 RFC 3280 替代。

RFC 2510：Internet X.509 Public Key Infrastructure Certificate Management Protocols，1999-03，被 RFC 4210 替代。

RFC 2511：Internet X.509 Certificate Request Message Format，1999-03，被 RFC 4211 替代。

RFC 2527：Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework，1999-03，被 RFC 3647 替代。

RFC 2528：Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates，1999-03。

RFC 2559：Internet X.509 Public Key Infrastructure Operational Protocols—LDAPv2，1999-04，被 RFC 3494 替代。

RFC 2560：X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP，1999-06，被 RFC 6960 替代，由 RFC 6277 更新。

RFC 2585：Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP，1999-05。

RFC 2587：Internet X.509 Public Key Infrastructure LDAPv2 Schema，1999-06，被 RFC 4523 替代。

RFC 2797：Certificate Management Messages over CMS，2000-04，被 RFC 5272 替代。

RFC 2875：Diffie-Hellman Proof-of-Possession Algorithms，2000-07，被 RFC 6955 替代。

RFC 3029：Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols，2001-02。

RFC 3039：Internet X.509 Public Key Infrastructure Qualified Certificates Profile，2001-01，被 RFC 3739 替代。

RFC 3161：Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)，2001-08，被 RFC 5816 更新。

RFC 3279：Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile，2002-05，被 RFC 4055、RFC 4491、RFC 5480、RFC 5758 更新。

RFC 3280：Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile，2002-05，被 RFC 5280 替代，由 RFC 4325、RFC 4630 更新。

RFC 3281：An Internet Attribute Certificate Profile for Authorization，2002-05，被 RFC 5755 替代。

RFC 3379：Delegated Path Validation and Delegated Path Discovery Protocol Requirements，2002-09。

RFC 3628：Policy Requirements for Time-Stamping Authorities (TSAs)，2003-11。

RFC 3647：Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework，2003-11。

RFC 3709：Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates，2004-02，被 RFC 6170 更新。

RFC 3739：Internet X.509 Public Key Infrastructure: Qualified Certificates Profile，2004-03。

RFC 3770：Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)，2004-05，被 RFC 4334 替代。

RFC 3779：X.509 Extensions for IP Addresses and AS Identifiers，2004-06。

RFC 3820：Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile，2004-06。

RFC 4043：Internet X.509 Public Key Infrastructure Permanent Identifier，2005-05。

RFC 4055：Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile，2005-06，被 RFC 5756 更新。

RFC 4059：Internet X.509 Public Key Infrastructure Warranty Certificate Extension，2005-05。

RFC 4158：Internet X.509 Public Key Infrastructure: Certification Path Building，2005-09。

RFC 4210：Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)，2005-09，被 RFC 6712 更新。

RFC 4211：Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)，2005-09。

RFC 4212：Alternative Certificate Formats for the Public-Key Infrastructure Using X.509 (PKIX) Certificate Management Protocols. October 2005。

RFC 4262：X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities. December 2005。

RFC 4325：Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension，2005-12，被 RFC 5280 替代。

RFC 4334：Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)，2006-02。

RFC 4386：Internet X.509 Public Key Infrastructure Repository Locator Service，2006-02。

RFC 4387：Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP，2006-02。

RFC 4476：Attribute Certificate (AC) Policies Extension，2006-05。

RFC 4491：Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile，2006-05。

RFC 4510：Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map. June 2006。

RFC 4511：Lightweight Directory Access Protocol (LDAP): The Protocol. June 2006。

RFC 4512：Lightweight Directory Access Protocol (LDAP): Directory Information Models，June 2006。

RFC 4513：Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms，June 2006。

RFC 4514：Lightweight Directory Access Protocol (LDAP): String Representation of

Distinguished Names，June 2006。

RFC 4515：Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters，June 2006。

RFC 4522：Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option，June 2006。

RFC 4523：Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates，June 2006。

RFC 4630：Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile，2006-08，被 RFC 5280 替代。

RFC 4683：Internet X.509 Public Key Infrastructure Subject Identification Method (SIM)，2006-10。

RFC 4985：Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name，2007-08。

RFC 5019：The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments，2007-09。

RFC 5055：Server-Based Certificate Validation Protocol (SCVP)，2007-12。

RFC 5272：Certificate Management over CMS (CMC)，2008-06，被 RFC 6402 更新。

RFC 5273：Certificate Management over CMS (CMC): Transport Protocols，2008-06，被 RFC 6402 更新。

RFC 5274：Certificate Management Messages over CMS (CMC): Compliance Requirements，2008-06，被 RFC 6402 更新。

RFC 5280：Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile，2008-05，被 RFC 6818 更新。

RFC 5480：Elliptic Curve Cryptography Subject Public Key Information，2009-03。

RFC 5636：Traceable Anonymous Certificate，2009-08。

RFC 5697：Other Certificates Extension，2009-11。

RFC 5755：An Internet Attribute Certificate Profile for Authorization，2010-01。

RFC 5756：Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters，2010-01。

RFC 5758：Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA，2010-01。

RFC 5816：ESSCertIDv2 Update for RFC 3161，2010-04。

RFC 5877：The application/pkix-attr-cert Media Type for Attribute Certificates，2010-05。

RFC 5912：New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)，2010-06，被 RFC 6960 更新。

RFC 5913：Clearance Attribute and Authority Clearance Constraints Certificate Extension，2010-06。

RFC 6025：ASN.1 Translation，2010-10。

RFC 6170：Internet X.509 Public Key Infrastructure -- Certificate Image，2011-05。

RFC 6277：Online Certificate Status Protocol Algorithm Agility，2011-06，被 RFC 6960 替代。

RFC 6402：Certificate Management over CMS (CMC) Updates，2011-11。

RFC 6664：S/MIME Capabilities for Public Key Definitions，2012-07。

RFC 6712：Internet X.509 Public Key Infrastructure—HTTP Transfer for the Certificate Management Protocol (CMP)，2012-09。

RFC 6818：Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile，2013-01。

RFC 6844：DNS Certification Authority Authorization (CAA) Resource Record，2013-01。

RFC 6960：X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP，2013-06。

RFC 7030：Enrollment over Secure Transport，2013-10。

4．其他标准规范

ITU-T X.208 Specification of Abstract Syntax Notation One (ASN.1)。

ITU-T X.690 Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules(CER) and Distinguished Encoding Rules (DER)。

Specification for Integrated Cirsuit(s) Cards Interface Devices (CCID)。

Interoperability Specification for ICCs and Personal Computer System (PC/SC)。

Microsoft Cryptographic Service Provider。

Java Cryptography Architecture (JCA)。

Java Cryptography Extention (JCE)。

2.7 PKI/信任模型

如同现实生活中的二代身份证一样，在网络世界中，通过验证对方数字证书的合法性就可确认对方身份，从而帮助互不认识或互不相信的交易双方建立信任关系。显然，PKI 体系中已经蕴含“信任”的概念。

什么是“信任”呢？在 ITU X.509 规范中，“信任”定义为“当实体 A 认为实体 B 的行为与 A 所预期的完全一致时，则称实体 A 信任实体 B”。PKI 体系中，用户因为信任 CA 中心，所以信任该 CA 中心签发的数字证书，本质上是实现了一种“信任传递”关系。需要说明的是，用户信任 CA 中心是指，用户相信该 CA 中心的所有数字证书管理行为均符合政策法规、运营规范和信息安全等要求，不会出现伪造数字证书、数字证书中信息不正确、数字证书对应的私钥不安全、数字证书作废后不及时发布等行为；用户信任数字证书，是指用户相信该数字证书持有人的身份是真实有效的，并不等于用户信任该数字证书的持有人。

从信任 CA 中心到信任其签发的用户数字证书，这种信任传递关系的前提是，该用户数字证书必须通过以下四个方面的合法性验证：

（1）验证该数字证书是否伪造。使用 CA 证书中公钥即可脱机验证。

（2）验证该数字证书中信息是否正确。由 CA 中心在签发数字证书时已保证。

（3）验证该数字证书是否与持证人一致。可要求持证人使用私钥对特定数据进行加密或

签名，然后使用数字证书中的公钥来解密该数据或验签，从而可验证持证人是否持有与数字证书中公钥对应的私钥。

（4）验证该数字证书是否在黑名单上。通过 CRL 或 OCSP 方式可实现。

为方便理解信任传递关系，PKI 引入“信任模型”，用于描述和分析同一 CA 管理域内部或不同 CA 管理域之间信任关系的建立和传递过程。PKI 信任模型中，CA 中心是信任的产生来源或信任起点，称作信任锚，而 X.509 数字证书是信任的表达和传递工具。从信任锚到数字证书，可以构建一条信任关系传递的路径，称作认证路径、证书路径或信任链。信任链越长，信任传递过程中验证次数越多，复杂度越高。图 2-4 显示了 Web 浏览器中的证书路径。

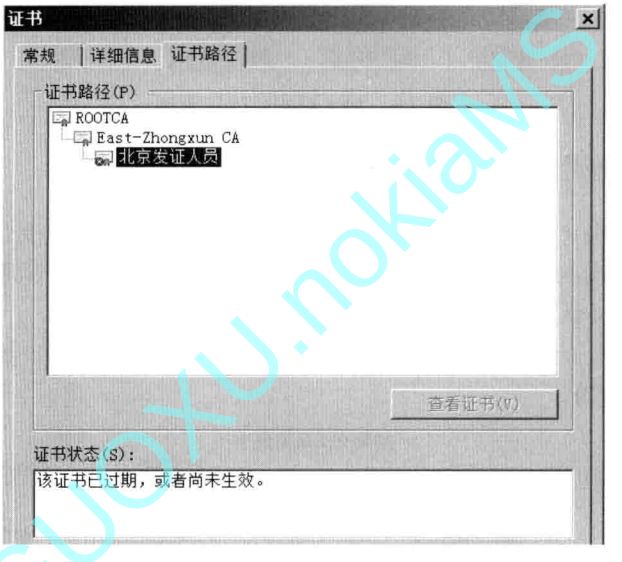

图 2-4　Web 浏览器中证书路径显示

PKI 信任模型可分为以下几类。

2.7.1　根 CA 信任模型

根 CA 信任模型，也称作严格层次信任模型。该信任模型下，CA 中心可以分为多级，用户证书由 CA 中心签发，各级 CA 中心之间呈现严格的层次关系，最上级 CA 中心只有一个，称作根 CA，其他 CA 称作子 CA。根 CA 的数字证书由自己签发，属于自签名证书，子 CA 的数字证书由上级 CA 签发。信任锚可以是根 CA，也可以是子 CA。

如图 2-5 所示，根 CA 签发子 CA1 证书和子 CA2 证书，子 CA2 签发子 CA3 证书和子 CA4 证书，子 CA1 签发用户 A 证书，子 CA3 签发用户 B 证书和用户 C 证书，子 CA4 签发用户 D 证书。

用户 X 的信任锚为根 CA，因此它可信任子 CA1，从而信任用户 A 证书。于是，从用户 X 的角度，用户 A 证书的信任链为：根 CA→子 CA1→用户 A 证书。

用户 Y 的信任锚为子 CA2，因此它可信任子 CA4，从而信任用户 D 证书。于是，从用户 Y 的角度，用户 D 证书的信任链为：子 CA2→子 CA4→用户 D 证书。