专栏：信息安全

公钥密码基础设施在电信运营商的应用

王聪丽[1,2]，王锦华[1,2]，薛伟佳[1,2]

（中国电信股份有限公司研究院，上海 201315；
2. 移动互联网系统与应用安全国家工程实验室，上海 201315）

摘　要：随着密码法的实施，我国将信息系统密码应用提升到了法律层面，要求加强公钥基础设施在网络实体互通互信方面的应用。提出了一种采用严格层次结构建设统一电信公钥基础设施的方案，即建立一个全国电信运营商根 CA 作为信任锚，而各大电信运营商成为独立的子 CA，形成“全国电信运营商根 CA－电信运营商子 CA”的证书信任链，提供 PKI 安全服务。该方案不仅可以实现电信运营商 CA 之间的互通互认，也有利于统一电信公钥基础设施成为全球范围信任的电子认证服务提供商，进而在国际证书标准制定上有更大的影响力和话语权。

关键词：公钥基础设施；数字证书；电信运营商；互联互通

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000−0801.2020292

Application of public key infrastructure in telecom operators

WANG Congli[1,2], WANG Jinhua[1,2], XUE Weijia[1,2]

1. Research Institute of China Telecom Co., Ltd., Shanghai 201315, China
2. Mobile Internet System and Application Security National Engineering Laboratory, Shanghai 201315, China

Abstract: With the implementation of cryptography law, the application of cryptography in information system in China has been promoted to the legal level, which requires the application of public key infrastructure in the mutual trust of network entities to be strengthened. A scheme of constructing unified telecom public key infrastructure with strict hierarchical structure was proposed, that is, establishing a national telecom root CA as a trust anchor, and each major telecom operator becomes an independent sub-ca, forming a certificate trust chain of “national telecom root CA- telecom operator sub-ca” and providing PKI security services. This scheme can not only realize the mutual recognition between telecom operators, but also help unify the telecom public key infrastructure to become a globally trusted electronic authentication service provider, so as to have more influence and say in the formulation of international certification standards.

Key words: public key infrastructure, digital certificate, telecom operator, connectivity

收稿日期：2020−09−01；修回日期：2020−11−13

1　引言

公钥基础设施（public key infrastructure，PKI）基于公钥密码学，通过权威证书认证中心（Certificate Authority，CA）签发的数字证书实现互联网身份真实性、数据保密性和完整性、操作的不可否认性。在互联网应用中，PKI 为网络空间安全提供重要保障作用。随着密码法、网络安全等级保护 2.0 制度、关键信息基础设施安全保护条例等多项与网络空间安全相关法律法规的落地，昭示着国家对信息系统密码应用和密码技术自主可控的重视，加强公钥基础设施在网络实体互通互信方面的应用，统一网络互信服务数据加密传输服务标准，推动不同运营商电子认证服务的互通互认，是电信运营商努力的方向。

公钥密码基础设施主要包括 CA 和密钥管理中心两部分。密钥全生命周期管理，包括密钥的生成、存储、导入和导出、分发、使用、备份和恢复、归档、销毁等在国家密码行业标准《信息系统密码应用基本要求》[1-2]中有详细的规定。本文将主要针对 CA 的应用和建设方案进行探讨。

基于商用密码安全、自主、可控打造国产 CA 品牌，提高 CA 认证的权威性、互联互通性、可靠性，研究国密算法数字证书，推动国密算法与国际标准体系的接轨，提升中国电子认证服务国际影响力和话语权是当务之急。目前中国 CA 机构在国际组织和标准制定中的参与度不够，CA 市场存在同质竞争、技术层面上没有统一标准、难以互联互通等现象。本文认为，基于一个权威电信行业根 CA，建立“全国电信运营商根 CA－电信运营商子 CA”的证书信任链由多个运营商构成的多子 CA 结构，可以为电信用户提供最专业便捷的服务，避免各方在协调和服务的过程中相互牵扯和不相容。此外，目前全球信任的根证书多为国外 CA 证书，近年来 CA 安全事件[3-7]频发也给我们敲响了警钟，应该集中电信行业的力量，争取使统一电信公钥基础设施成为全球范围信任的电子认证服务提供商，从而摆脱对国外 CA 的依赖。

2　CA 认证中心现状

CA 认证中心是公钥基础设施的重要组成部分，根据国内 CA 建设背景和提供的服务来看，大致可以分为两类：建设性 CA 和运营性 CA。建设性 CA 主要帮助企业完成内部 CA 平台的搭建，如时代亿信。运营性 CA 需要获得工业和信息化部（工信部）颁发的电子认证服务许可证，签发的数字证书具有法律效力，国内大约有 34 家运营性 CA[8]。运营性 CA 可以分为 3 类：第一类是行业性 CA（如中国金融认证中心（China Financial Certification Authority，CFCA）），第二类是地方性 CA（如上海 CA），第三类是商业性 CA（如天威诚信）。

国际知名的 CA 认证机构有 Let’s Encrypt、Sectigo（Comodo）、Digicert（Symantec）等，这些 CA 机构于 2020 年 2 月 23 日一天签发的证书数量见表 1[9]。

表 1　CA 认证机构证书签发量

CA 机构	签发证书量	比例
Let’s Encrypt	2 845 088	69%
Sectigo(Comodo)	851 522	21%
Digicert(Symantec)	244 084	6%
其他	153 746	4%

由国际性电子认证机构、浏览器厂商、操作系统厂商联合成立的 CA/B（CA/Browser Forum）论坛[10]致力于电子认证标准的制定，其成员作为标准制定的参与者拥有更多的话语权。目前 CA/B 论坛拥有来自全球的 53 个 CA 成员、8 个浏览器厂商成员，包括微软、谷歌、苹果、Mozilla 等知名浏览器厂商以及 Digicert、GlobalSign、Let’s Encrypt 等知名 CA 机构。此外，我国的天威诚信、中国金融认证中心、上海 CA 也是 CA/B 论坛的成

员，这对于推动国产密码算法成为国际安全技术标准、促进我国 CA 提供全球电子认证服务具有重大意义。

3 电信运营商业务需求

电信行业业务庞大而复杂，需要提升安全服务意识，加强公钥基础设施在身份认证、数据加密、完整性保护和非否认性等方面的应用，构建完善的电信运营商安全体系。

电信运营商对公钥基础设施的需求主要集中在以下 4 个方面。

（1）业务系统

无纸化营业厅的电子印章、数字签名以及各种终端设备的安全接入都需要公钥基础设施保证其数据的真实性、完整性、有效性；企业内部办公系统要确保有相应权限才能够访问和操作；业务网站要进行 HTTPS 升级；电子邮件、语音通信等数据传输需进行加密；自有 App 需要进行代码签名，防止盗版、仿冒、篡改等风险；手机支付软件（例如中国电信翼支付）需要验证支付服务器及域名的真实性，从而保证交易安全。以上业务系统的安全性都可以通过公钥基础设施实现。

（2）物联网安全

物联网给电信运营商带来巨大机遇，在拓展业务的同时，也要重视物联网安全问题，公钥基础设施是解决物联网安全保障和身份认证问题的一种解决方案。中国电信物联网开放平台提供物联网设备安全接入能力，目前支持基于 SIM 卡安全能力的 SimID 认证、基于身份标识的国密算法 SM9 认证，后续将基于公钥基础设施，增加利用证书保障物联网设备安全接入与安全通信的认证方式，拓展物联网开放平台的终端接入安全认证能力。在视频监控中，国家标准《公共安全视频监控联网信息安全技术要求》[11]提出，前端设备和用户终端必须具有基于数字证书的设备身份认证功能，并且要求在系统中访问加密视频信息的用户是经过基于数字证书认证的用户。公钥基础设施发挥着关键作用，提供数据传输存储以及验证身份所需的信任。

（3）区块链节点身份认证

中国电信、中国移动、中国联通均在区块链领域有不同程度的涉足，探索区块链在电信行业的应用场景，例如国内运营商间利用码号优势建立数字身份、国内运营商与国际运营商间的国际漫游结算、运营商与银行共享征信、运营商间共享计算和带宽、共享基站等[12-14]。这些区块链在电信运营商的应用场景中均需要不互信的多方参与、协作，所以身份认证问题是区块链应用不可避免的挑战。就联盟链而言，电子认证是必选项，联盟链节点通常需要电子认证确定节点的真实身份，这就是“CA”节点的主要用途，也是电子认证在联盟链中的价值所在。联盟链中的 CA 节点负责对网络中的成员身份进行管理；采用数字证书机制实现对成员身份的鉴别与权限控制。

（4）5G 新场景

公钥密码基础设施在 5G 新的应用场景中也将为身份认证、互联互通提供有力支撑。安全网关和 5G 基站 gNB（next generation node-B）之间以及有直接链路的 gNB 和 4G 基站 eNB（evolved node-B）之间采用 PKI 证书进行双向认证保证组网传输安全；5G 核心网的 NF（network function，网络功能）之间、NF 与 NRF（NF repository function，网络存储功能）之间、NRF 之间均应使用基于证书的 TLS（transport layer security）建立安全会话并进行双向认证。在车联网中，美国的 V2X 通信以 IEEE1609.2 为基准，定义了 V2X（vehicle to everything）通信中应用和管理信息的安全服务、安全交互信息格式，提出了 LTCA 和 PCA 等新的机制，均基于公钥密码基础设施改良，为车联网提供安全保障[15]。

4　公钥基础设施建设方案

4.1　PKI/CA 系统建设模式

常见 PKI/CA 系统建设模式有以下 5 种。

（1）完全自行建设的模式

完全自行建设的模式是指企业购买单独的安全产品和系统，建设一个独立的证书认证系统，包括 PKI/CA 系统软件、防火墙、入侵检测、病毒防治等安全产品以及机房、门禁、消防、供电、容灾备份等物理安全措施。对于完全自行建设的数字证书认证系统，企业需要考虑系统的设计、建设、检测、运行以及后期运营管理和维护升级等。

完全自行建设的模式又分为建立企业级 CA 和建立运营性 CA，这两种方式各有利弊。企业级 CA 结构简单、投资较少、便于集中管理、无须取得电子认证服务许可，但是不会被公开信任；运营性 CA 签发的证书具有法律效力，但是需要满足《电子认证服务管理办法》[16]中的所有要求，建设和维护等各方面都需投入很高的成本。

（2）基于服务的托管自建模式

基于服务的托管自建模式是指将 CA 服务器远程托管建设在第三方认证中心，将注册机构（registration authority，RA）和远程管理软件建设在企业本地。采用这种方式，企业直接使用第三方认证中心提供的 PKI/CA 服务，无须考虑运营资质和复杂的 CA 建设问题，通过本地 RA 和 CA 管理软件，企业可以自定义数字证书模板，并对数字证书的全生命周期进行管理。但是这种方式下，要防止第三方认证中心恶意签发虚假证书从而造成企业财产和名誉的损失，且费用是长期问题。

（3）采用国内的商业性 CA 模式

采用国内的商业性 CA 模式是指企业或最终用户直接向国内商业 CA 购买数字证书，企业只需要在业务系统中对证书有效性进行验证即可。这种模式中，商业性 CA 是按证书数量收费的，且证书过期之后，需要重新购买，如果用户量大且长期使用的话，费用会很高。此外，申请数字证书时，商业性 CA 的身份审核、相应速度较慢，证书模板相对固定。

（4）针对不同业务使用不同的 CA 模块

如果不打算建立一个完整的数字证书认证系统，那么可以在必要的业务系统中建立模块化 CA 系统，这种方式简单易用、可按需定制、开发成本低。但是，采用私有协议，难以和其他系统互联互通，如果多个业务系统都需要 CA 模块，用户需要使用多个数字证书，用户体验不好。

（5）采用全球信任的根证书模式

国际 CA 认证机构 DigiCert、GlocalSign、Sectigo（Comodo）等均通过了 Web Trust 国际安全审计认证，支持所有主流操作系统、浏览器、服务器、移动端。采用全球信任的根证书模式是指全球信任顶级根证书签发一个中间 CA 证书给企业，该中间 CA 证书由企业自己管理，使企业不仅可以灵活签发数字证书，而且签发的数字证书被浏览器等信任。但是目前全球信任的根证书多为境外 CA，而境外电子认证服务提供者签发数字证书的法律效力还未明确。

4.2　电信运营商 PKI/CA 系统建设方案

由工信部牵头，中国移动、中国电信、中国联通等电信运营商共同建立权威、公正的电信行业统一公钥基础设施，有助于电信运营商之间实现互联互通。统一电信 PKI 系统结构如图 1 所示，建议采用严格层次方案建设统一电信 PKI 系统，也就是说建立一个全国电信运营商根 CA 作为信任锚，而各大电信运营商成为独立的子 CA，形成“全国电信运营商根 CA－电信运营商子 CA”的证书信任链，提供 PKI 安全服务。

在具体的实施过程中，涉及全国电信运营商根 CA、电信运营商子 CA、省公司子 CA 的系统建设，建议借鉴完全自行建设的模式、基于服务的托管自建模式以及采用全球信任的根证书模式三者结合的方式建设统一电信公钥基础设施。本

文对统一电信公钥基础设施的系统组成及建设模式进行介绍。

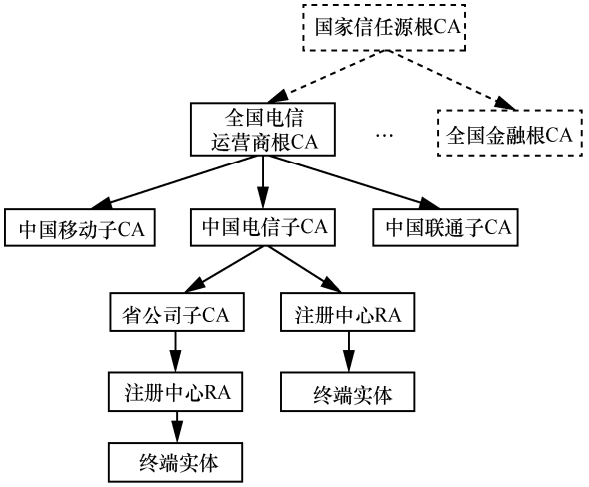


图 1　统一电信 PKI 系统结构

（1）全国电信运营商根 CA

全国电信运营商根 CA 持有自签名 CA 证书，由它签发电信运营商子 CA 证书，它是整个信任体系的信任起点，各大电信运营商 CA 的相互信任源自它，将来同时它也作为与其他 CA 交叉认证的起点，例如金融行业统一公钥基础设施 CFCA。如有需要，全国电信运营商根 CA 也可以成为国家信任源根 CA 的下级子 CA，从而与所有国家信任源根 CA 签发的子 CA 互联互通，实现“一证在手，走遍全国”。

全国电信运营商根 CA 的建设模式，借鉴完全自行建设的模式（运营级 CA）和采用全球信任的根证书模式。只有获得电子认证服务许可成为运营级 CA 才可以具有法律效力，进而在全国范围内提供电子认证服务；通过国际权威的 Webtrust 认证，进而有资格预埋在微软、Mozilla、谷歌、苹果等操作系统、浏览器、设备，从而提供全球范围的数字证书、不受制于国外 CA，实现安全、自主、可控。

（2）电信运营商子 CA、省公司子 CA、注册中心 RA

电信运营商管理各自的子 CA，彼此的物理结构是独立的体系，电信运营商可以根据实际情况选择适合自己的 CA 结构。业务成熟的省市可以采用自行建设的模式建立省级 CA 以及注册中心 RA，业务开展不成熟的省市可以采用托管的模式，即本地暂不建设维护省级 CA，而是通过 Web 的方式，访问电信运营商子 CA 中心为各省建立的托管 CA 和 RA。

此外，三大运营商在中国 PKI 发展的早期建立了一些 CA 中心，例如 CTCA（China Telecom Certificate Authority）、CMCA（China Mobile Certificate Authority）、CUCA（China Unicom Certificate Authority），这些 CA 有的目前处于暂停状态，有的只能为企业内部提供服务，导致电信运营商对外业务系统中只能选择购买地方性 CA、商业 CA 的数字证书。为了防止资源浪费，也为了防止对现有用户造成影响，建议在保留已有 CA 中心的基础上，按照上述统一电信 PKI 系统结构建立新的 CA 中心体系，并逐步完成已有 CA 和新 CA 的对接。

5　结束语

公钥基础设施是网络环境中提供身份鉴别、数据保密性、完整性、不可否认性等安全服务的重要支撑，密码法出台之后，信息系统密码应用和合规性检查成为法律要求，推动了国产算法数字证书的研发和 PKI 系统国密化改造。PKI/CA 系统的安全性、互联互通、可靠性对于当前的电子认证服务自主安全可控以及国际化接轨融合至关重要。

电信运营商内部业务系统、物联网安全以及区块链等新兴技术均需要公钥密码基础设施提供服务，本文建议由工信部牵头，联合三大电信运营商共同建立权威、公正的电信行业统一公钥密码基础设施，形成“全国电信运营商根 CA－电信运营商子 CA”的证书信任链，提供 PKI 安全服务。这样不仅可以实现互联互通，也可以遵循统一鉴证标准，用中国电信行业的力量争取参与国际证

书标准的制定，推动国产密码算法国际化进程以及全球电子认证服务的进程。

参考文献：

[1] 全国信息安全标准化技术委员会. 证书认证系统密码相关安全技术规范: GB/T 25056-2018[S]. 2018.
National Information Security Standardization Technical Committee. Specifications of cryptograph and related security technology for certificate authentication system: GB/T 25056-2018[S]. 2018.

[2] 国家密码管理局.信息系统密码应用基本要求: GM/T 0054-2018 [S]. 2019.
State Cryptography Administration. General requirements for information system cryptography application: GM/T 0054-2018[S]. 2019.

[3] Google Security Blog. Sustaining digital certificate security[EB]. 2015-10-28.

[4] RYAN S. Intent to deprecate and remove: trust in existing symantec-issued certificates [EB]. 2017-03-24.

[5] DARIN F. Intent to deprecate and remove: Trust in existing symantec-issued certificates [EB]. 2017-03-24.

[6] IVAN R. Monitoring of symantec certificates[EB]. 2017-08-15.

[7] Wikipedia. Flame (malware)[EB]. 2018-11-21.

[8] 中华人民共和国工业和信息化部. 获得电子认证服务行政许可的认证机构名单[EB]. 2014-04-09.
Ministry of Industry and Information Technology of the People's Republic of China. List of certificate authorities that have obtained administrative license for electronic certification services [EB]. 2014-04-09.

[9] Cloudflare. Merkle town explore the certificate transparency ecosystem [EB]. 2020-02-23.

[10] CA/Browser forum[EB]. 2020-02-23.

[11] 中华人民共和国公安部. 公共安全视频监控联网信息安全技术要求: GB 35114-2017[S]. 2017-11-01.
The Ministry of Public Security of the People's Republic of China. Technical requirements for information security of video surveillance network system for public security: GB 35114-2017[S]. 2017-11-01.

[12] 薛淼, 刘千仞, 符刚, 等. 区块链在电信运营商应用场景的探讨[J]. 邮电设计技术，2019(4): 76-80
XUE M, LIU Q R, FU G, et al. Discussion on the application scenarios of blockchain in telecom operator[J]. Designing Techniques of Posts and Telecommunications, 2019(4): 76-80.

[13] 庞松涛. 基于公钥密码体制的网络认证技术[J]. 电信科学, 2016, 32(2): 170-174.
PANG S T . Network authentication technology based on public key system[J]. Telecommunications Science, 2016, 32(2): 170-174.

[14] 刘冰洋, 杨飞, 任首首, 等. 去中心化互联网基础设施[J]. 电信科学, 2019, 35(8): 74-87.
LIU B Y, YANG F, REN S S, et al. Decentralized internet infrastructure[J]. Telecommunications Science, 2019, 35(8): 74-87.

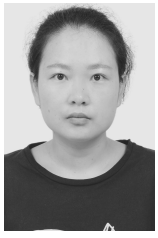
[15] 全国信息安全标准化技术委员会. 汽车电子网络安全标准化白皮书[R]. 2018.
National Information Security Standardization Technical Committee. White paper on automotive electronic network safety standardization[R]. 2018.

[16] 中华人民共和国工业和信息化部. 电子认证服务管理办法[R]. 2009.
Ministry of Industry and Information Technology of the People's Republic of China. Measures for the administration of electronic authentication services[R]. 2009.

[作者简介]

王聪丽（1994— ），女，中国电信股份有限公司研究院工程师，移动互联网系统与应用安全国家工程实验室工程师，主要研究方向为密码应用安全、公钥基础设施等。

王锦华（1982— ），男，中国电信股份有限公司研究院工程师，移动互联网系统与应用安全国家工程实验室工程师，主要研究方向为云计算、大数据安全、终端安全、密码应用等。



薛伟佳（1990— ），女，博士，中国电信股份有限公司研究院工程师，移动互联网系统与应用安全国家工程实验室工程师，主要研究方向为密码学、物联网安全、数据安全等。