(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2010 年 7 月 1 日 (01.07.2010)

PCT

(10) 国际公布号
WO 2010/072086 A1

(51) 国际专利分类号:
H04L 9/14 (2006.01) *H04L 12/66* (2006.01)

(21) 国际申请号: PCT/CN2009/073959

(22) 国际申请日: 2009 年 9 月 16 日 (16.09.2009)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200810246871.6 2008 年 12 月 26 日 (26.12.2008) CN

(71) 申请人 (对除美国外的所有指定国): **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人; 及
(75) 发明人/申请人 (仅对美国): **嵇盛育 (JI, Shengyu)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: **北京康信知识产权代理有限责任公司 (KANGXIN PARTNERS, P.C.)**; 中国北京市海淀区知春路甲 48 号盈都大厦 A 座 16 层, Beijing 100098 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title**: KEY CERTIFICATE GENERATION METHOD AND SYSTEM USED FOR HOME GATEWAY

(54) **发明名称** : 用于家庭网关的密钥证书生成方法和系统

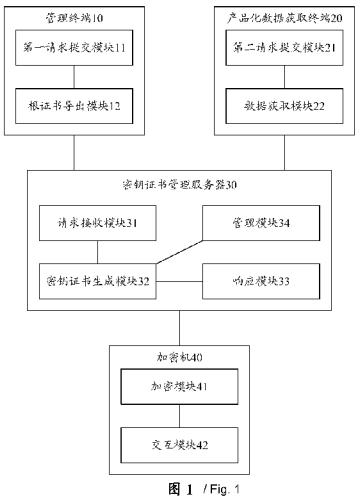

图 1 / Fig. 1

10 MANAGEMENT TERMINAL
11 THE FIRST REQUEST SUBMISSION MODULE
12 ROOT CERTIFICATE EXPORTING MODULE
20 COMMERCIALIZATION DATA OBTAINING TERMINAL
21 THE SECOND REQUEST SUBMISSION MODULE
22 DATA OBTAINING MODULE
30 KEY CERTIFICATE MANAGEMENT SERVER
31 REQUEST RECEIVING MODULE
32 KEY CERTIFICATE GENERATION MODULE
33 RESPONSE MODULE
34 MANAGEMENT MODULE
40 ENCRYPTION MACHINE
41 ENCRYPTION MODULE
42 INTERACTION MODULE

(57) **Abstract**: A key certificate generation system used for home gateway is provided by the invention. In the above described system, a key certificate management server (30) interacts with an encryption machine (40), based on the requests submitted by a management terminal (10) and a commercialization data obtaining terminal (20), executes the operations of generating a root key and a root certificate, exporting the root certificate, generating a version signed key, signing version data, generating the key and certificate of the home gateway, and so on; the generated root certificate is exported to the management terminal (10), the signed version data is returned to the commercialization data obtaining terminal (20), the generated key and certificate of the home gateway are returned to the commercialization data obtaining terminal (20), the public key corresponding to the version signed private key is exported and returned to the commercialization data obtaining terminal (20). According to the invention, the security of the communication can be ensured, the confidentiality and integrity of the information transmission can be guaranteed, and the validity of the identity can be guaranteed.

[见续页]

WO 2010/072086 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(57) 摘要:

本发明公开了一种用于家庭网关的密钥证书生成系统。在上述系统中，密钥证书管理服务器（30）与加密机（40）进行交互，根据管理终端（10）和产品化数据获取终端（20）提交的请求，执行生成根密钥和根证书、根证书导出、生成版本签名的密钥、版本数据签名、生成家庭网关的密钥和证书等操作；将生成的根证书导出给管理终端（10），将签名后的版本数据返回给产品化数据获取终端（20），将生成的家庭网关的密钥和证书返回给产品化数据获取终端（20），将版本签名私钥对应的公钥导出返回给产品化数据获取终端（20）。根据本发明，可以确保通信的安全性和保证信息传输的保密性和完整性以及保证身份的真实性。

用于家庭网关的密钥证书生成方法和系统

技术领域

本发明涉及网络安全技术领域，尤其涉及一种用于家庭网关的密钥证书生成方法和系统。

背景技术

随着互联网的飞速发展，各种网络业务迅速展开，网络业务除了传统的互联网浏览业务外，还包括网络电视（IPTV，Internet Protocol Television）、IP 电话等其他业务。目前，用户上网需要借助调制解调器、宽带路由器和家庭网关（Home Gateway）等多种设备。而在实际应用中，由于网络业务的不断扩张，用户所需的设备配置工作也越来越多，对设备的运营商来说，则需要通过运营商服务器对家庭网关进行配置和软件升级，以达到增加新业务的目的。但是，由于现有技术还无法提供一种运营商服务器和家庭网关之间的安全认证机制，从而造成运营商服务器和家庭网关之间进行通信时存在安全隐患，例如：家庭网关被恶意控制以及非法的家庭网关接入等等。

发明内容

有鉴于此，本发明的主要目的在于提供一种用于家庭网关的密钥证书生成方法和系统，以保证家庭网关与运营商服务器之间的通信安全。

为达到上述目的，本发明的技术方案是这样实现的：

根据本发明的一个方面，首先提供了一种用于家庭网关的密钥证书生成系统。

根据本发明的用于家庭网关的密钥证书生成系统，包括：管理终端、产品化数据获取终端、密钥证书管理服务器和加密机。其中，

管理终端，用于提交生成根密钥和根证书的请求，提交生成版本签名的密钥请求，提交根证书导出请求，并获取导出的根证书；

产品化数据获取终端，用于提交版本数据和版本签名请求，并获取签名后的版本数据；提交家庭网关的个性数据，提交生成家庭网关密钥和证书的

请求，以及导出签名私钥对应公钥数据的请求；获取家庭网关的密钥和证书，以及版本签名私钥对应的公钥数据；

密钥证书管理服务器，用于接收来自管理终端和产品化数据获取终端的请求并响应，根据上述请求通知加密机执行生成密钥和签名操作，根据上述请求执行生成证书操作；

加密机，用于生成密钥和签名，对密钥进行保存，并将上述根密钥和版本签名密钥对应的标识，以及上述签名返回给密钥证书管理服务器；将家庭网关的密钥直接返回给密钥证书管理服务器。

上述管理终端进一步包括：

第一请求提交模块，用于向密钥证书管理服务器提交生成根密钥和根证书的请求，提交生成版本签名的密钥请求，提交根证书导出请求；

根证书导出模块，用于获取密钥证书管理服务器导出的根证书。

产品化数据获取终端进一步包括：

第二请求提交模块，用于向密钥证书管理服务器提交家庭网关的个性数据，提交生成家庭网关密钥和证书的请求，以及导出版本签名私钥对应的公钥数据的请求，提交版本数据和版本签名请求；

数据获取模块，用于获取家庭网关的密钥和证书，获取签名后的版本数据，以及版本签名私钥对应的公钥。

密钥证书管理服务器进一步包括：

请求接收模块，用于接收来自管理终端和产品化数据获取终端的请求；

密钥证书生成模块，用于根据上述请求与加密机进行交互，得到生成的根密钥和版本密钥的标识、家庭网关的公私钥数据，根据公钥标识得到根公钥和版本签名私钥对应的公钥数据，得到签名后的数据；根据上述请求生成证书；

响应模块，用于对上述请求进行响应，向管理终端提供生成的根证书，向上述产品化数据获取终端提供生成的家庭网关的密钥和证书，版本签名私钥对应的公钥以及签名后的版本数据；

管理模块，用于对生成的密钥所对应的标识、以及上述证书、运营商配置信息、用户权限、操作日志进行管理。

上述加密机进一步包括:

加密模块，用于执行生成密钥和签名的操作，并对密钥进行保存;

交互模块，用于与密钥证书管理服务器进行交互，并将根密钥和版本签名密钥对应的标识，以及上述签名返回给密钥证书管理服务器；将该家庭网关的密钥直接返回给密钥证书管理服务器。

根据本发明的另一个方面，还提供了一种用于家庭网关的密钥证书生成方法。

根据本发明的用于家庭网关的密钥证书生成方法，包括:

密钥证书管理服务器根据管理终端提交的生成根密钥和根证书的请求，与加密机进行交互，生成根密钥和根证书，并将根证书导出给管理终端;

密钥证书管理服务器根据管理终端提交的生成版本签名的密钥请求，与加密机进行交互，生成用于版本签名的密钥;

密钥证书管理服务器根据上述产品化数据获取终端提交的版本数据和版本签名请求，与加密机进行交互，生成签名后的版本数据;

密钥证书管理服务器根据上述产品化数据获取终端提交的家庭网关的个性数据，提交的生成家庭网关密钥和证书的请求，和导出版本签名私钥对应的公钥的请求，与加密机进行交互，生成家庭网关的密钥和证书，导出版本签名的私钥对应的公钥数据，并返回给产品化数据获取终端。

上述生成根密钥和根证书的请求中携带运营商标识;生成版本签名密钥的请求，版本签名请求，以及生成家庭网关密钥和证书的请求中携带运营商标识和地区标识。

该方法进一步包括:加密机生成根密钥和用于版本签名的密钥时，仅将上述密钥对应的标识返回给密钥证书管理服务器。

该方法进一步包括:密钥证书管理服务器对生成的密钥所对应的标识，以及上述证书、运营商配置信息、用户权限、操作日志进行管理。

根据本发明的另一个方面，还提供了一种用于家庭网关的密钥证书生成系统。

根据本发明的用于家庭网关的密钥证书生成系统，包括：管理终端、产品化数据获取终端、密钥证书管理服务器和加密机，其中，

管理终端用于提交生成根密钥和根证书的请求，以及根证书导出请求，并获取导出的根证书；产品化数据获取终端用于提交家庭网关的个性数据，以及生成家庭网关密钥和证书的请求，并获取家庭网关的密钥和证书；密钥证书管理服务器用于接收来自上述管理终端和产品化数据获取终端的请求并响应，根据上述请求通知加密机执行生成密钥和证书操作；加密机用于生成密钥和签名，对生成的密钥进行保存，并将生成的根密钥对应的标识返回给上述密钥证书服务器，将上述家庭网关的密钥直接返回给上述密钥证书管理服务器。

根据本发明的再一个方面，还提供了一种家庭网关的密钥证书生成方法。

根据本发明的家庭网关密钥生成方法，包括：1）密钥证书管理服务器根据管理终端提交的生成根密钥和根证书的请求，与加密机进行交互，生成根密钥和根证书，并将根证书导出给管理终端；2）密钥证书管理服务器根据上述产品化数据获取终端提交的家庭网关的个性数据，以及提交的生成家庭网关的密钥和证书的请求，与加密机进行交互，生成家庭网关的密钥和证书，并将生成的家庭网关的密钥和证书返回给上述产品化数据终端。

本发明所提供的用于家庭网关的密钥证书生成方法和系统，其生成密钥和证书的过程，完全屏蔽直接与外界交互，保证了生成密钥和证书的绝对安全；能够批量生成家庭网关的密钥和证书，提交的个性数据通过表格形式直接导入，只需要选择运营商和地区，无需任何配置，使得操作简单，也大大降低了生成密钥和证书，以及对其进行管理的难度；运营商服务器与家庭网关之间采用基于密钥和证书的认证机制进行通信，从而确保通信的安全性；将传输的数据进行加密，保证了信息传输的保密性和完整性；对要传输的数据进行签名，保证了身份的真实性。

本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优

点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

附图用来提供对本发明的进一步理解，并且构成说明书的一部分，与本发明的实施例一起用于解释本发明，并不构成对本发明的限制。在附图中：

图 1 为本发明一种用于家庭网关的密钥证书生成系统的组成结构示意图；

图 2 为本发明一种用于家庭网关的密钥证书生成方法的流程图。

具体实施方式

功能概述

在本发明实施例中，通过一种新型的用于家庭网关的密钥证书生成方法和系统，在其生成密钥和证书的过程中，密钥证书管理服务器密钥证书管理服务器与加密机进行交互，根据管理终端和产品化数据获取终端提交的请求，执行生成根密钥和根证书、根证书导出、生成版本签名的密钥、版本数据签名、生成家庭网关的密钥和证书等操作；将生成的根证书导出给管理终端，将签名后的版本数据返回给产品化数据获取终端，将生成的家庭网关的密钥和证书返回给产品化数据获取终端，将版本签名私钥对应的公钥导出返回给产品化获取终端。这样就避免了运营商服务器和家庭网关之间进行通信时所存在的安全隐患问题的发生。

为了更好地理解本发明，下面结合附图和具体实施例对关于基于区域策略的位置广告业务分众的具体实施方式和实施例加以详细说明。应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明。

在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

根据本发明实施例，首先提供了一种用于家庭网关的密钥证书生成系统。

根据本发明实施例提供的一种用于家庭网关的密钥证书生成系统，如图

1 所示，该系统由管理终端 10、产品化数据获取终端 20、密钥证书管理服务器 30 和加密机 40 组成。

管理终端 10，用于向密钥证书管理服务器 30 提交生成根密钥和根证书的请求，请求密钥证书管理服务器 30 生成根密钥和根证书，该请求携带运营商标识。密钥证书管理服务器 30 根据请求中的运营商标识从自身的数据库中读出根密钥的位数、类型和格式等参数信息，以及根证书的序列号、有效期、名字项信息和扩展项信息等，由密钥证书管理服务器 30 与加密机进行交互，生成根密钥和根证书。在生成根密钥和根证书之后，管理终端 10 可以向密钥证书管理服务器 30 提交根证书导出请求，请求密钥证书管理服务器 30 导出所生成的根证书。管理终端 10 还用于向密钥证书管理服务器 30 提交生成版本签名的密钥请求，请求密钥证书管理服务器 30 生成用于版本签名的密钥。

产品化数据获取终端 20，用于在需要进行版本数据的签名时，向密钥证书管理服务器 30 提交版本数据和版本签名请求，并在签名完毕后，从密钥证书管理服务器 30 获取签名后的版本数据；还用于在需要生成家庭网关的密钥和证书时，向密钥证书管理服务器 30 提交家庭网关的个性数据，提交生成家庭网关密钥和证书的请求，以及导出版本签名私钥对应的公钥的请求，并从密钥证书管理服务器 30 获取家庭网关的密钥和证书，以及版本签名私钥对应的公钥。提交的请求中包括运营商标识和地区标识，密钥证书管理服务器根据运营商标识和地区标识从自身的数据库中读出家庭网关的个性数据，包括家庭网关密钥的位数、类型和格式等参数，产品证书的名字项和扩展项等信息，以及需要导出的版本签名私钥对应的公钥标识。

密钥证书管理服务器 30，用于接收来自管理终端 10 和产品化数据获取终端 20 的各种请求并响应，根据各种请求与加密机 40 进行交互，以执行各项操作，具体包括：

密钥证书管理服务器 30 在接收到来自管理终端 10 的生成根密钥的请求时，根据请求读取数据库中的根密钥的位数、类型和格式等参数信息，生成新的请求信息并通知加密机 40，由加密机 40 根据新的请求信息中携带的根密钥的位数、类型和格式等信息，执行生成根密钥的操作，生成的根密钥包括根的公钥和私钥；并在操作完成后保存生成的根密钥，将生成的根密钥所对应的标识返回给密钥证书管理服务器 30，由密钥证书管理服务器 30 将标识存储在自身的数据库中并进行管理；需要指出的是，出于安全性的考虑，

加密机 40 向密钥证书管理服务器 30 返回根密钥对应的标识，而不是直接向密钥证书管理服务器 30 返回生成的根密钥；

密钥证书管理服务器 30 在接收到来自管理终端 10 的生成根证书的请求时，根据请求从数据库中读出根的公私钥标识，根证书的序列号、有效期、名字项信息和扩展项信息等，执行生成根证书的操作；生成根证书的操作需要从加密机 40 中获取根的公私钥数据，并通知加密机 40 利用根私钥对根证书进行签名；生成的根证书存储在密钥证书管理服务器 30 自身的数据库中，密钥证书管理服务器 30 可以对数据库中存储的根证书进行管理；

密钥证书管理服务器 30 在接收到来自管理终端 10 的根证书导出请求时，将数据库中的根证书导出给管理终端 10；

密钥证书管理服务器 30 在接收到来自管理终端 10 的生成版本签名的密钥请求时，根据请求读取数据库生成新的请求信息并通知加密机 40，由加密机 40 根据新的请求中携带的密钥的位数、类型和格式等信息，执行生成版本签名的密钥操作，并在操作完成后保存生成的密钥，将生成的密钥所对应的标识返回给密钥证书管理服务器 30，密钥证书管理服务器 30 将标识存储在自身的数据库中并进行管理，生成的版本签名的密钥包括公钥和私钥；

密钥证书管理服务器 30 在接收到来自产品化数据获取终端 20 的版本数据和版本签名请求时，从数据库中读取版本签名私钥的标识并通知加密机 40，由加密机 40 用版本签名私钥对版本数据执行签名操作，并在操作完成后，将签名后的版本数据返回给密钥证书管理服务器 30，密钥证书管理服务器 30 将签名后的版本数据返回给产品化数据获取终端 20；

密钥证书管理服务器 30 在接收到来自产品化数据获取终端 20 的生成家庭网关密钥和证书的请求，以及家庭网关的个性数据时，根据请求读取数据库生成新的请求信息并通知加密机 40，由加密机 40 根据新的请求中携带的位数、类型和格式等信息执行家庭网关的密钥生成操作；密钥证书管理服务器 30 根据新的请求中携带的名字项信息和扩展项信息、根证书、根私钥标识，证书有效期等，执行家庭网关的证书生成操作；密钥证书管理服务器 30 将生成的家庭网关的密钥和证书返回给产品化数据获取终端 20。

加密机 40，用于执行生成密钥和数据的签名操作，其中，签名操作包括生成证书时的签名和对版本数据的签名；还用于对生成的根密钥和版本签

名密钥进行保存，并将根密钥和版本签名密钥对应的标识，以及签名后的版本数据返回给密钥证书管理服务器 **30**；还用于将生成的家庭网关的密钥和证书返回给密钥证书管理服务器 **30**。

其中，管理终端 **10** 进一步包括：相互连接的第一请求提交模块 **11** 和根证书导出模块 **12**。第一请求提交模块 **11**，用于向密钥证书管理服务器 **30** 提交生成根密钥和根证书的请求，提交生成版本签名的密钥请求，提交根证书导出请求。根证书导出模块 **12**，用于获取密钥证书管理服务器 **30** 导出的根证书。

产品化数据获取终端 **20** 进一步包括：相互连接的第二请求提交模块 **21** 和数据获取模块 **22**。第二请求提交模块 **21**，用于向密钥证书管理服务器 **30** 提交家庭网关的个性数据，以及生成家庭网关密钥和证书的请求，提交版本数据和版本签名请求。数据获取模块 **22**，用于获取家庭网关的密钥和证书，获取签名后的版本数据。

密钥证书管理服务器 **30** 进一步包括：请求接收模块 **31**、密钥证书生成模块 **32**、响应模块 **33** 和管理模块 **34**。请求接收模块 **31**，用于接收来自管理终端 **10** 和产品化数据获取终端 **20** 的各种请求。密钥证书生成模块 **32**，连接请求接收模块 **31**，用于根据请求与加密机 **40** 进行交互，得到密钥标识和签名后的数据；还用于根据请求生成证书。响应模块 **33**，连接密钥证书生成模块 **32**，用于对请求进行响应，向管理终端 **10** 提供生成的根证书，向产品化数据获取终端 **20** 提供生成的家庭网关的密钥和证书，以及签名后的版本数据、版本签名私钥对应的公钥数据。管理模块 **34**，连接密钥证书生成模块 **32**，用于对生成的密钥所对应的标识、以及所述证书、运营商配置信息、用户权限、操作日志进行管理。

加密机 **40** 进一步包括：相互连接的加密模块 **41** 和交互模块 **42**。加密模块 **41**，用于执行生成密钥和签名的操作，并对生成的密钥进行保存。交互模块 **42**，用于与密钥证书管理服务器 **30** 进行交互，并将根密钥和版本签名密钥对应的标识，以及签名返回给密钥证书管理服务器 **30**；将家庭网关的密钥直接返回给密钥证书管理服务器 **30**。

根据本发明实施例，还提供了一种用于家庭网关的密钥证书生成方法。

根据本发明实施例的用于家庭网关的密钥证书生成方法，如图 2 所示，

该方法包括以下步骤（步骤 201 - 步骤 204）:

步骤 201，密钥证书管理服务器根据管理终端提交的生成根密钥和根证书的请求，与加密机进行交互，生成根密钥和根证书，并将根证书导出给管理终端。

需要指出的是，由于实际应用中对于不同的运营商而言，其根密钥和根证书是不同的，即根密钥和根证书是按照不同的运营商对应生成的；因此，作为本发明的一种较佳实施例，密钥证书管理服务器可以将各个运营商定制的配置数据导入数据库中，这些配置数据包括：根密钥的位数、类型和格式，以及根证书的名字项信息和扩展项信息等。从而，管理终端在提交生成根密钥和根证书的请求时，只需要选择运营商标识；相应的，密钥证书管理服务器根据请求中的运营商标识，从自身的数据库中读取与该运营商标识相对应的配置数据，从而根据配置数据执行根密钥和根证书的生成操作。

出于安全性的考虑，加密机执行加密操作并生成根密钥后，仅仅将根密钥对应的标识返回给密钥证书管理服务器，而不是将根密钥直接返回给密钥证书管理服务器；密钥证书管理服务器的数据库对根密钥对应的标识，以及证书进行存储，且密钥证书管理服务器可以对数据库中的标识和证书进行管理。此外，根证书是用于签发其他证书的基础，如果没有根证书，则不能实现其他证书的生成和签发。

根证书生成以后，管理终端可以向密钥证书管理服务器提交根证书导出请求，请求中携带运营商标识；密钥证书管理服务器根据请求中的运营商标识查找对应的根证书，并将根证书导出给管理终端，并由管理终端将根证书提供给运营商。

步骤 202，密钥证书管理服务器根据管理终端提交的生成版本签名的密钥请求，与加密机进行交互，生成用于版本签名的密钥。

需要指出的是，由于实际应用中运营商在每一个地区所使用的版本签名的密钥都是不同的，因此需要根据不同地区的需要产生不同的密钥。作为本发明的一种较佳实施例，管理终端在提交生成版本签名的密钥请求时，只需要选择运营商标识和地区标识；相应的，密钥证书管理服务器根据请求中的运营商标识和地区标识，从自身的数据库中读取相应的配置数据，从而与加密机进行交互，以实现密钥的生成操作。

出于安全性的考虑，加密机执行加密操作并生成用于版本签名的密钥后，仅仅将密钥对应的标识返回给密钥证书管理服务器，而不是将该密钥直接返回给密钥证书管理服务器；密钥证书管理服务器的数据库对该密钥对应的标识进行存储，且密钥证书管理服务器可以对数据库中的标识进行管理。

步骤 203，密钥证书管理服务器根据产品化数据获取终端提交的版本数据和版本签名请求，与加密机进行交互，生成签名后的版本数据。

实际应用中，每次发布新的版本数据时，都需要对版本数据进行签名。产品化数据获取终端可以选择运营商标识和地区标识，向密钥证书管理服务器提交版本数据和版本签名请求；密钥证书管理服务器根据请求读取数据库中版本签名私钥标识并通知加密机执行版本数据的签名操作，操作完成后，加密机将签名后的版本数据返回给密钥证书管理服务器，由密钥证书管理服务器再将签名后的版本数据返回给产品化数据获取终端。

需要指出的是，在版本数据的签名操作中，产品化数据获取终端在提交版本签名请求后，可以登出操作页面；通过操作页面查看版本数据的签名状态，如果状态显示签名完毕，则从操作页面上点击下载，即可以从密钥证书管理服务器上获取签名后的版本数据。

步骤 204，密钥证书管理服务器根据产品化数据获取终端提交的家庭网关的个性数据，提交的生成家庭网关密钥和证书的请求，以及导出版本签名私钥对应的公钥的请求，与加密机进行交互，生成家庭网关的密钥和证书，导出版本签名私钥对应的公钥，并返回给产品化数据获取终端。

本发明支持家庭网关密钥和证书的批量生成，产品化数据获取终端可以将提交的个性数据以表格的形式进行排列存储，提交的个性数据中包括家庭网关的序列号等。产品化数据获取终端选择营运商标识和地区标识，并提交含有个性数据的表格后，可以登出操作页面；密钥证书管理服务器从数据库中读取根密钥标识、根证书、版本签名私钥对应的公钥标识、产品密钥的类型和格式等信息以及证书的名字项和扩展项信息。并与加密机进行交互，实现生成家庭网关的密钥和证书操作，导出版本签名私钥对应的公钥，并将生成的密钥和证书，以及版本签名私钥对应的公钥数据填入表格的对应项中；产品化数据获取终端通过操作页面查看生成密钥和证书的操作状态，如果状态显示生成完毕，则从操作页面上点击下载，即可以从密钥证书管理服务器上获取含有家庭网关密钥和证书，以及版本签名私钥对应的公钥数据的表格。

产品化数据终端在获取含有家庭网关密钥和证书的表格以及签名后的版本数据之后，将表格和签名后的版本数据提供给家庭网关的生产线，进而在生产线上将签名后的版本数据，以及各个家庭网关的密钥和证书烧入各个对应的家庭网关中。

需要说明的是，在实际应用中，如果不需要能版本进行验证，则不需要生成用于版本签名的密钥、版本数据、版本签名私钥和公钥，因此，根据本发明实施例，还提供了另一种用于家庭网关的密钥证书生成系统及方法。

根据本发明实施例的另一种用于家庭网关的密钥证书生成系统包括：管理终端，用于提交生成根密钥和根证书的请求，以及根证书导出请求，并获取导出的根证书；产品化数据获取终端，用于提交家庭网关的个性数据，以及生成家庭网关密钥和证书的请求，并获取家庭网关的密钥和证书；密钥证书管理服务器，用于接收来自管理终端和产品化数据获取终端的请求并响应，根据请求通知加密机执行生成密钥和证书操作；加密机，用于生成密钥和签名，对生成的密钥进行保存，并将生成的根密钥对应的标识返回给密钥证书管理服务器，将家庭网关的密钥直接返回给密钥证书管理服务器。

根据本发明实施例的另一种用于家庭网关的密钥证书生成方法包括：步骤 1，密钥证书管理服务器根据管理终端提交的生成根密钥和根证书的请求，与加密机进行交互，生成根密钥和根证书，并将根证书导出给管理终端；步骤 2，密钥证书管理服务器根据产品化数据获取终端提交的家庭网关的个性数据，以及提交的生成家庭网关密钥和证书的请求，与加密机进行交互，生成家庭网关的密钥和证书，并将生成的家庭网关的密钥和证书返回给产品化数据获取终端。

综上所述，由于各个家庭网关都被烧入各自对应的密钥和证书，以及版本签名私钥对应的公钥数据，以及签名后的版本数据，因此，运营商的服务器与家庭网关进行通信时，可以根据家庭网关的密钥和证书，利用现有的基于密钥和证书的安全认证机制，实现安全通信，从而避免出现家庭网关被恶意控制以及非法的家庭网关接入等各种安全隐患。

应当理解的是，对本领域普通技术人员来说，可以根据上述方案的说明加以改进或变换，例如利用其他的用户属性进行的分众细化方法，而所有这些改进和变换都本应属于本发明所附权利要求的保护范围。

权 利 要 求 书

1. 一种用于家庭网关的密钥证书生成系统，其特征在于，包括:

管理终端，用于提交生成根密钥和根证书的请求，提交生成版本签名的密钥请求，提交根证书导出请求，并获取导出的根证书;

产品化数据获取终端，用于提交版本数据和版本签名请求，并获取签名后的版本数据；提交家庭网关的个性数据，提交生成家庭网关密钥和证书的请求，以及导出签名私钥对应公钥数据的请求；获取家庭网关的密钥和证书，以及版本签名私钥对应的公钥数据;

密钥证书管理服务器，用于接收来自所述管理终端和产品化数据获取终端的请求并响应，根据所述请求通知加密机执行生成密钥和签名操作，根据所述请求执行生成证书操作;

加密机，用于生成密钥和签名，对密钥进行保存，并将所述根密钥和版本签名密钥对应的标识，以及所述签名返回给所述密钥证书管理服务器；将所述家庭网关的密钥直接返回给所述密钥证书管理服务器。

2. 根据权利要求 1 所述用于家庭网关的密钥证书生成系统，其特征在于，所述管理终端进一步包括:

第一请求提交模块，用于向所述密钥证书管理服务器提交生成根密钥和根证书的请求，提交生成版本签名的密钥请求，提交根证书导出请求;

根证书导出模块，用于获取所述密钥证书管理服务器导出的根证书。

3. 根据权利要求 1 所述用于家庭网关的密钥证书生成系统，其特征在于，所述产品化数据获取终端进一步包括:

第二请求提交模块，用于向所述密钥证书管理服务器提交家庭网

关的个性数据，提交生成家庭网关密钥和证书的请求，以及导出版本签名私钥对应的公钥数据的请求，提交版本数据和版本签名请求；

数据获取模块，用于获取家庭网关的密钥和证书，获取签名后的版本数据，以及版本签名私钥对应的公钥。

4. 根据权利要求 1 所述用于家庭网关的密钥证书生成系统，其特征在于，所述密钥证书管理服务器进一步包括：

请求接收模块，用于接收来自所述管理终端和产品化数据获取终端的请求；

密钥证书生成模块，用于根据所述请求与所述加密机进行交互，得到生成的根密钥和版本密钥的标识、家庭网关的公私钥数据，根据公钥标识得到根公钥和版本签名私钥对应的公钥数据，得到签名后的数据；根据所述请求生成证书；

响应模块，用于对所述请求进行响应，向所述管理终端提供生成的根证书，向所述产品化数据获取终端提供生成的家庭网关的密钥和证书，版本签名私钥对应的公钥以及签名后的版本数据；

管理模块，用于对生成的密钥所对应的标识、以及所述证书、运营商配置信息、用户权限、操作日志进行管理。

5. 根据权利要求 1 所述用于家庭网关的密钥证书生成系统，其特征在于，所述加密机进一步包括：

加密模块，用于执行生成密钥和签名的操作，并对密钥进行保存；

交互模块，用于与所述密钥证书管理服务器进行交互，并将所述根密钥和版本签名密钥对应的标识，以及所述签名返回给所述密钥证书管理服务器；将所述家庭网关的密钥直接返回给所述密钥证书管理服务器。

6. 一种用于家庭网关的密钥证书生成方法，其特征在于，该方法包括：

密钥证书管理服务器根据管理终端提交的生成根密钥和根证书的请求，与加密机进行交互，生成根密钥和根证书，并将根证书导出给所述管理终端；

所述密钥证书管理服务器根据所述管理终端提交的生成版本签名的密钥请求，与加密机进行交互，生成用于版本签名的密钥；

所述密钥证书管理服务器根据所述产品化数据获取终端提交的版本数据和版本签名请求，与加密机进行交互，生成签名后的版本数据；

所述密钥证书管理服务器根据所述产品化数据获取终端提交的家庭网关的个性数据，提交的生成家庭网关密钥和证书的请求，和导出版本签名私钥对应的公钥的请求，与加密机进行交互，生成家庭网关的密钥和证书，导出版本签名的私钥对应的公钥数据，并返回给所述产品化数据获取终端。

7. 根据权利要求 6 所述用于家庭网关的密钥证书生成方法，其特征在于，所述生成根密钥和根证书的请求中携带运营商标识；所述生成版本签名密钥的请求，版本签名请求，以及生成家庭网关密钥和证书的请求中携带运营商标识和地区标识。

8. 根据权利要求 6 所述用于家庭网关的密钥证书生成方法，其特征在于，该方法进一步包括：所述加密机生成根密钥和用于版本签名的密钥时，仅将所述密钥对应的标识返回给所述密钥证书管理服务器。

9. 根据权利要求 6、或 7、或 8 所述用于家庭网关的密钥证书生成方法，其特征在于，该方法进一步包括：所述密钥证书管理服务器对生成的密钥所对应的标识，以及所述证书、运营商配置信息、用户权限、操作日志进行管理。

10. 一种用于家庭网关的密钥证书生成系统，其特征在于，包括：

管理终端，用于提交生成根密钥和根证书的请求，以及根证书导出请求，并获取导出的根证书；

产品化数据获取终端，用于提交家庭网关的个性数据，以及生成家庭网关密钥和证书的请求，并获取家庭网关的密钥和证书；

密钥证书管理服务器，用于接收来自所述管理终端和所述产品化数据获取终端的请求并响应，根据所述请求通知加密机执行生成密钥和证书操作；

加密机，用于生成密钥和签名，对生成的密钥进行保存，并将生成的根密钥对应的标识返回给所述密钥证书管理服务器，将所述家庭网关的密钥直接返回给所述密钥证书管理服务器。

11. 一种用于家庭网关的密钥证书生成方法，其特征在于，所述方法包括：

密钥证书管理服务器根据管理终端提交的生成根密钥和根证书的请求，与加密机进行交互，生成根密钥和根证书，并将根证书导出给所述管理终端；

所述密钥证书管理服务器根据所述产品化数据获取终端提交的家庭网关的个性数据，以及提交的生成家庭网关密钥和证书的请求，与加密机进行交互，生成家庭网关的密钥和证书，并将生成的家庭网关的密钥和证书返回给所述产品化数据获取终端。

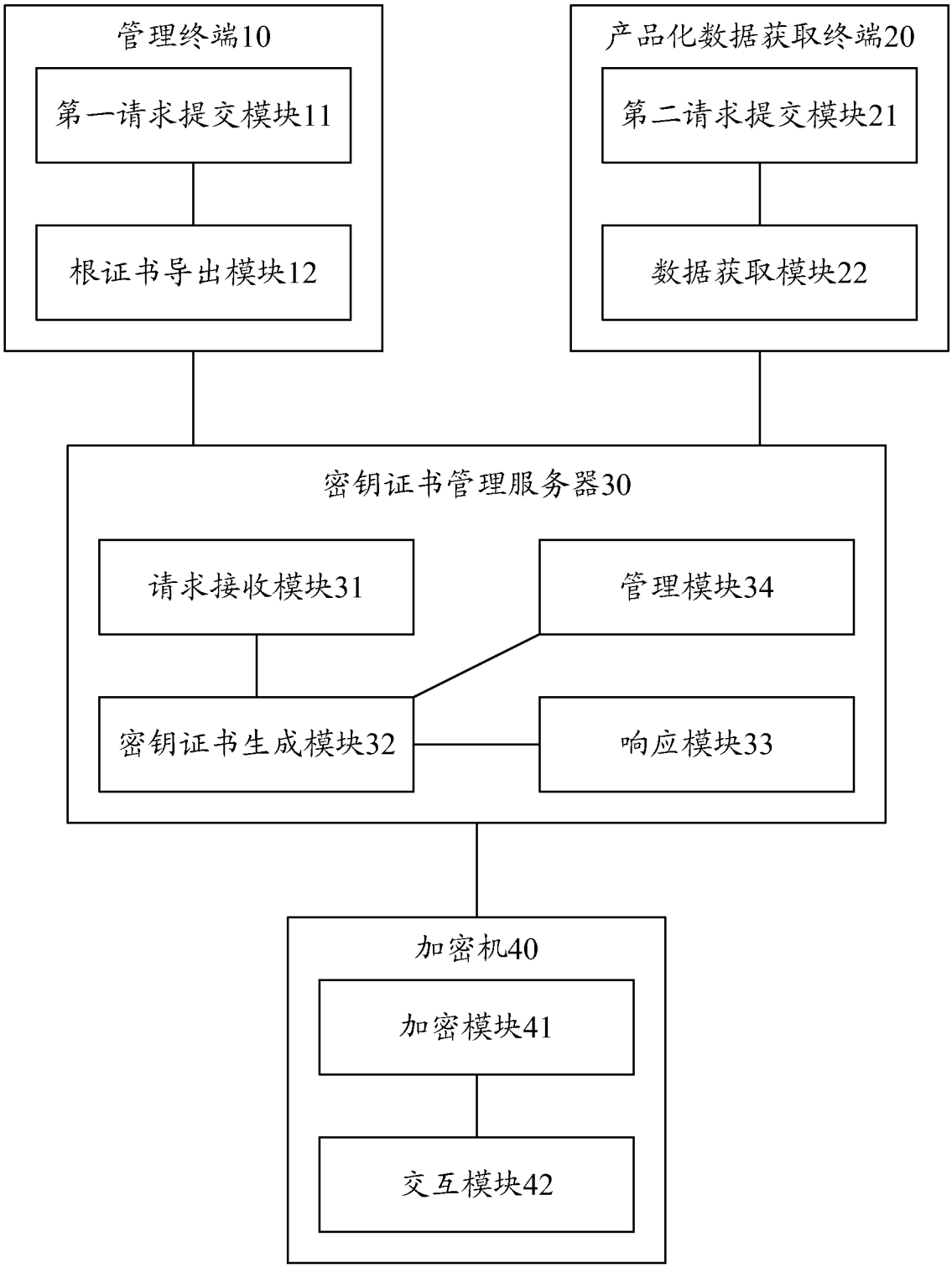
管理终端10
第一请求提交模块11
根证书导出模块12
产品化数据获取终端20
第二请求提交模块21
数据获取模块22
密钥证书管理服务器30
请求接收模块31
管理模块34
密钥证书生成模块32
响应模块33
加密机40
加密模块41
交互模块42

图 1

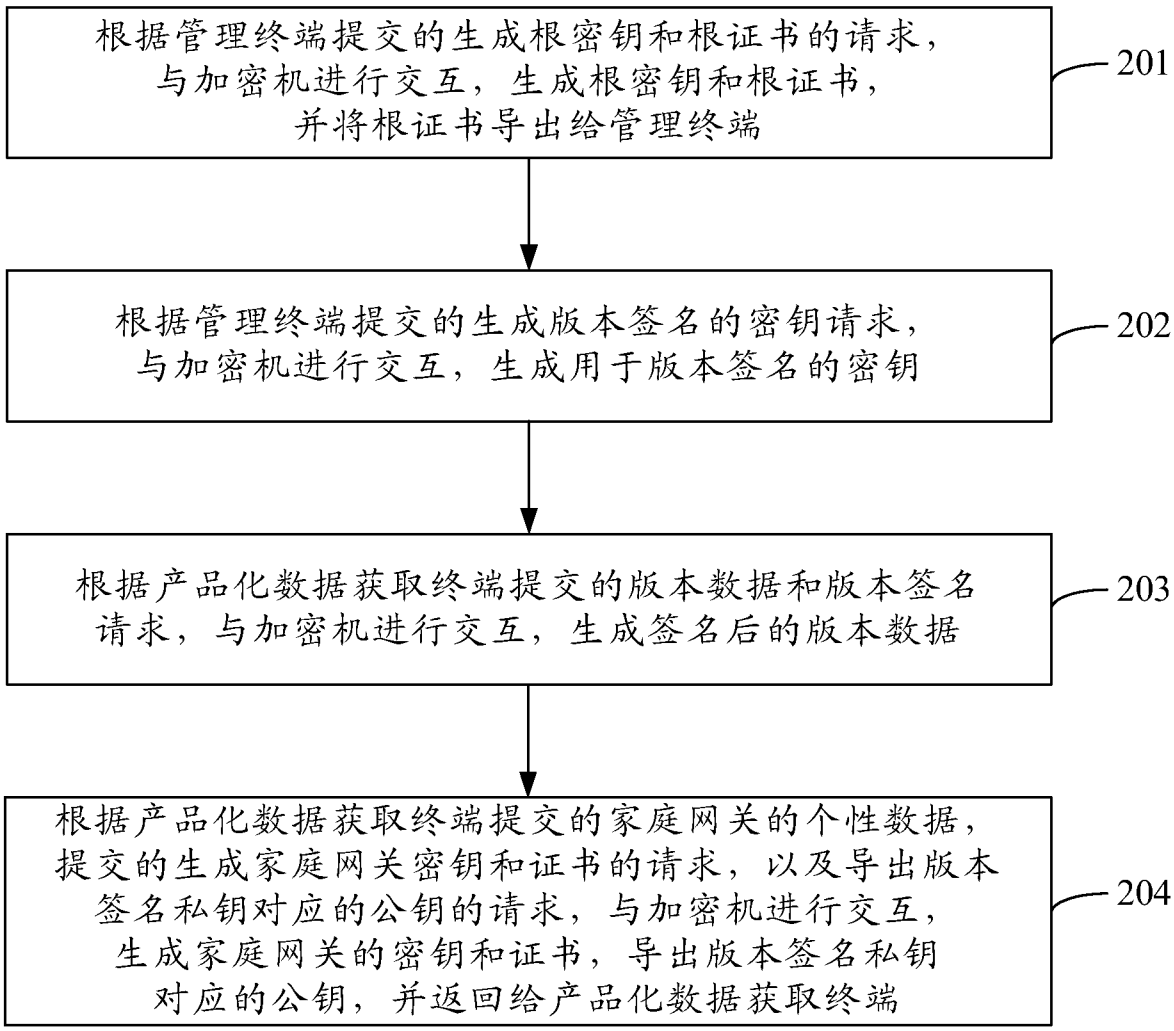
根据管理终端提交的生成根密钥和根证书的请求，
与加密机进行交互，生成根密钥和根证书，
并将根证书导出给管理终端
201
根据管理终端提交的生成版本签名的密钥请求，
与加密机进行交互，生成用于版本签名的密钥
202
根据产品化数据获取终端提交的版本数据和版本签名
请求，与加密机进行交互，生成签名后的版本数据
203
根据产品化数据获取终端提交的家庭网关的个性数据，
提交的生成家庭网关密钥和证书的请求，以及导出版本
签名私钥对应的公钥的请求，与加密机进行交互，
生成家庭网关的密钥和证书，导出版本签名私钥
对应的公钥，并返回给产品化数据获取终端
204

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/073959

A. CLASSIFICATION OF SUBJECT MATTER

See Extra Sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC, IEEE, CSA: HOME RESIDENTIAL HOUS+ FAMILY GATEWAY? ROOT MASTER PRIMARY KEY? CERTIFICATE? SECURITY REQUEST?

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BAEHYO PARK, et al. Research on Issuing a certificate and Generating a private key of a Home-gateway. Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers. December 16-18, 2005, pages 169-172.	10-11
A		1-9
A	CN1788460A (NIPPON TELEGRAPH & TELEPHONE) 14 June 2006(14.06.2006), The whole document	1-11
A	WO2007142566A1 (ERICSSON TELEFON AB L M) 13 Dec. 2007(13.12.2007), The whole document	1-11
A	JP2006013757A (MATSUSHITA ELECTRIC IND CO LTD) 12 Jan. 2006(12.01.2006), The whole document	1-11
A	WO2008002081A1 (ELECTRONICS & TELECOM RES INST) 03 Jan. 2008(03.01.2008), The whole document	1-11

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 Dec. 2009 (15.12.2009)	**24 Dec. 2009 (24.12.2009)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer FU qi Telephone No. (86-10)62411231

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2009/073959

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1788460A	14.06.2006	US2006280127A1	14.12.2006
		EP1755285A1	21.02.2007
		EP1755285A4	12.11.2008
		WO2005122492A1	22.12.2005
WO2007142566A1	13.12.2007	EP2027666A1	25.02.2009
		US2009199001A1	06.08.2009
		CA2653543A1	13.12.2007
JP2006013757A	12.01.2006	None	
WO2008002081A1	03.01.2008	KR20080001574A	03.01.2008
		US2009240941A1	24.09.2009

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/073959

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/14 (2006.01) i
H04L 12/66 (2006.01) n

国际检索报告

国际申请号
PCT/CN2009/073959

A. 主题的分类

参见附加页

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04L, H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNKI, CNPAT：家庭 家居 家用 网关 根 主 密钥 证书 安全 请求

WPI, EPODOC, IEEE, CSA：HOME RESIDENTIAL HOUS+ FAMILY GATEWAY? ROOT MASTER PRIMARY KEY? CERTIFICATE? SECURITY REQUEST?

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
X	BAEHYO PARK, et al. Research on Issuing a certificate and Generating a private key of a Home-gateway. Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers. December 16-18, 2005, pages 169-172.	10-11
A		1-9
A	CN1788460A（日本电信电话株式会社）14.6 月 2006（14.06.2006），全文	1-11
A	WO2007142566A1（ERICSSON TELEFON AB L M）13.12 月 2007（13.12.2007），全文	1-11
A	JP2006013757A（MATSUSHITA ELECTRIC IND CO LTD）12.1 月 2006（12.01.2006），全文	1-11
A	WO2008002081A1（ELECTRONICS & TELECOM RES INST） 03.1 月 2008（03.01.2008），全文	1-11

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
15.12 月 2009 (15.12.2009)	**24.12 月 2009 (24.12.2009)**

ISA/CN 的名称和邮寄地址：
中华人民共和国国家知识产权局
中国北京市海淀区蓟门桥西土城路 6 号 100088
传真号：　(86-10)62019451

受权官员
傅琦
电话号码：(86-10) **62411231**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2009/073959

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1788460A	14.06.2006	US2006280127A1	14.12.2006
		EP1755285A1	21.02.2007
		EP1755285A4	12.11.2008
		WO2005122492A1	22.12.2005
WO2007142566A1	13.12.2007	EP2027666A1	25.02.2009
		US2009199001A1	06.08.2009
		CA2653543A1	13.12.2007
JP2006013757A	12.01.2006	无	
WO2008002081A1	03.01.2008	KR20080001574A	03.01.2008
		US2009240941A1	24.09.2009

国际检索报告

国际申请号
PCT/CN2009/073959

A. 主题的分类

H04L 9/14〔2006.01〕i

H04L 12/66〔2006.01〕n