(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101183932 B
(45)授权公告日 2011.02.16

(21)申请号 200710077463.8

(22)申请日 2007.12.03

(73)专利权人 宇龙计算机通信科技(深圳)有限公司

地址 518057 广东省深圳市南山区高新技术产业园北区梦溪道2号酷派信息港1号楼

(72)发明人 张贤玮

(74)专利代理机构 深圳中一专利商标事务所 44237

代理人 陈健

(51)Int.Cl.

H04L 9/08(2006.01)

H04L 29/06(2006.01)

(56)对比文件

CN 1444386 A,2003.09.24, 说明书第3－6页,说明书附图1－8.

CN 1437376 A,2003.08.20, 说明书第2－5页,说明书附图1－4.

US 2007/0150723 A1,2007.06.28, 全文.

CN 1399490 A,2003.02.26, 全文.

审查员 方亮

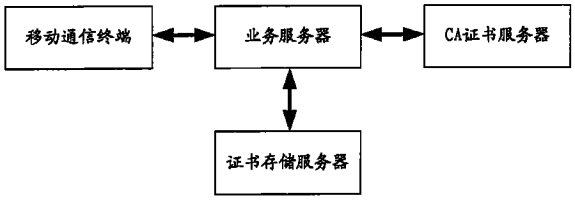
权利要求书 2 页 说明书 5 页 附图 2 页

(54)发明名称

一种无线应用服务的安全认证系统及其注册和登录方法

(57)摘要

本发明公开一种无线应用服务的安全认证系统及其注册和登录方法,该系统包括依次通过无线网络或有线网络相互连接的移动通信终端、业务服务器和CA证书服务器、以及连接到业务服务器的证书存储服务器;注册方法包括移动通信终端生成一对公钥和私钥,向业务服务器发出注册请求,业务服务器返回注册结果,CA证书服务器生成用户数字证书通过证书存储服务器存储;登录方法包括移动通信终端向业务服务器发送登录请求;业务服务器进行验证,返回验证结果。本发明通过移动通信终端生成公钥和私钥,并通过本地安全密码来保护公钥和私钥,由于本地安全密码不在网络上传输,所以大大降低了公钥和私钥被获取的风险,从而提高了无线网络中应用服务的使用安全性。



CN 101183932 B

1. 一种无线应用服务的安全认证系统，其特征在于：包括依次通过无线网络或有线网络相互连接的移动通信终端、业务服务器和 CA 证书服务器、以及连接到业务服务器的证书存储服务器；

所述移动通信终端用于生成并存储公钥和私钥，向业务服务器发送包含注册信息的注册请求和登录请求，所述注册信息包括移动通信终端唯一标识和所述公钥；

所述业务服务器用于获取移动通信终端发送的注册信息转发到 CA 证书服务器，并返回注册结果，存储所述注册信息；以及获取移动通信终端发送的登录请求，向移动通信终端发送验证信息，获取移动通信终端返回结果信息后，根据结果信息进行验证，并返回验证结果；

所述 CA 证书服务器用于根据业务服务器发送的注册信息生成唯一对应的用户数字证书，返回给业务服务器；

所述证书存储服务器用于存储业务服务器获取的 CA 证书服务器根据注册信息生成的用户数字证书；

所述验证信息为业务服务器临时生成的一个随机数，所述结果信息包括移动通信终端利用所述存储于移动通信终端中的私钥对所述随机数进行加密生成的签名值和注册资料信息中的用户名；所述业务服务器根据所述用户名调用对应的用户数字证书，通过用户数字证书中的公钥按照约定的解密算法对所述签名值进行解密，并与所述业务服务器临时生成的随机数进行对比来实现验证。

2. 如权利要求 1 所述的无线应用服务的安全认证系统，其特征在于：所述存储于移动通信终端中的公钥和私钥通过设置本地安全密码来保护，并在发出登录请求时通过输入本地安全密码来读取公钥和私钥。

3. 如权利要求 1 所述的无线应用服务的安全认证系统，其特征在于：所述注册资料信息还包括用户名和 / 或用户资料。

4. 如权利要求 1 至 3 中任一项所述的无线应用服务的安全认证系统，其特征在于：所述公钥和私钥存储于移动通信终端的隐藏保护分区中。

5. 一种无线应用服务的安全认证系统的注册方法，其特征在于：包括以下步骤：

移动通信终端生成一对公钥和私钥并存储上述公钥和私钥；

将包括移动通信终端唯一标识和所述公钥的注册信息打包发送到业务服务器；

业务服务器将所述注册信息发送到 CA 证书服务器，请求一份用户数字证书；

CA 证书服务器根据业务服务器发送的注册信息生成唯一对应的用户数字证书，返回给业务服务器；

业务服务器存储注册信息，并将上述获取的用户数字证书存储到证书存储服务器中，向移动通信终端返回注册成功结果。

6. 如权利要求 5 所述的无线应用服务的安全认证系统的注册方法，其特征在于：所述注册资料信息还包括用户名和 / 或用户资料。

7. 如权利要求 5 或 6 中任一项所述的无线应用服务的安全认证系统的注册方法，其特征在于：所述公钥和私钥存储于移动通信终端的隐藏保护分区中。

8. 一种无线应用服务的安全认证系统的登录方法，其特征在于：包括以下步骤：

移动通信终端向业务服务器发送登录请求；

业务服务器向移动通信终端发送验证信息；

移动通信终端根据获取验证信息返回结果信息；

业务服务器根据结果信息进行验证，并返回验证结果；

所述验证信息为业务服务器临时生成的一个随机数，所述结果信息包括移动通信终端利用所述存储于移动通信终端中的私钥对所述随机数进行加密生成的签名值和注册资料信息中的用户名；所述业务服务器根据所述用户名调用对应的用户数字证书，通过用户数字证书中的公钥按照约定的解密算法对所述签名值进行解密，并与所述业务服务器临时生成的随机数进行对比来实现验证。

9. 如权利要求 8 所述的无线应用服务的安全认证系统的登录方法，其特征在于：所述存储于移动通信终端中的公钥和私钥通过设置本地安全密码来保护，并在发出登录请求时通过输入本地安全密码来读取公钥和私钥。

一种无线应用服务的安全认证系统及其注册和登录方法

技术领域

[0001] 本发明涉及信息安全认证技术领域，尤其是涉及一种移动通信终端安全证书认证系统及其注册和登录方法。

背景技术

[0002] 中国专利《一种无线电子商务领域中进行交易的方法》，其公开日为2002年4月17日，公开号为CN1345514，该专利主要技术特点是：

[0003] 1. 系统需要包括一个具有根公共密钥证书的无线网络运营商认证机构和至少一个具有独立于根公共密钥证书的数字证书的属性机构，属性机构可以由一个无线客户设备经过一个无线网络来访问；

[0004] 2. 该方法需要数字证书从属性机构传送到无线设备；无线客户设备需要预装载根公共密钥证书。

[0005] 3. 无线客户设备需要使用无线客户设备中预装载的数字证书和跟公共密钥证书对属性机构进行验证。

[0006] 缺陷在于：

[0007] 1. 现有的无线网络领域的安全证书方案主要是针对电子商务领域，而没有面向所有的无线应用领域。

[0008] 2. 现有的方案需要一个具有根公共密钥证书的无线网络运营商认证机构和至少一个具有独立于根公共密钥证书的数字证书的属性机构。而实际情况中对于一般的无线应用服务来说，获取具有根公共密钥证书的无线网络运营商认证机构的服务支持，服务成本偏高；而且安全级别较高，不利于一般的安全性的服务的推广。

[0009] 3. 现有的方案需要将数字证书从属性机构传输到无线设备，而在无线网络中传输10K-十几K的数字证书文件，对服务的效率和用户感受方面都有影响。

[0010] 4. 现有的方案需要客户设备采用双证书对属性机构进行验证，而对于有些应用来说，服务器属性是安全的，不需要验证，而安全认证的重点是针对客户设备的访问。

[0011] 发明内容

[0012] 本发明所要解决的技术问题是提供一种无线应用服务的安全证书认证系统，其提高了无线网络中应用服务的使用安全性。

[0013] 为解决本发明的技术问题，本发明公开一种无线应用服务的安全认证系统，包括依次通过无线网络或有线网络相互连接的移动通信终端、业务服务器和CA证书服务器、以及连接到业务服务器的证书存储服务器；

[0014] 所述移动通信终端用于生成并存储公钥和私钥，向业务服务器发送包含注册信息的注册请求和登录请求，所述注册信息包括移动通信终端唯一标识和所述公钥；

[0015] 所述业务服务器用于获取移动通信终端发送的注册信息转发到CA证书服务器，并返回注册结果，存储所述注册信息；以及获取移动通信终端发送的登录请求，向移动通信终端发送验证信息，获取移动通信终端返回结果信息后，根据结果信息进行验证，并返回验

证结果；

[0016] 所述 CA 证书服务器用于根据业务服务器发送的注册信息生成唯一对应的用户数字证书，返回给业务服务器；

[0017] 所述证书存储服务器用于存储业务服务器获取的 CA 证书服务器根据注册信息生成的用户数字证书；

[0018] 所述验证信息为业务服务器临时生成的一个随机数，所述结果信息包括移动通信终端利用所述存储于移动通信终端中的私钥对所述随机数进行加密生成的签名值和注册资料信息中的用户名；所述业务服务器通过根据所述用户名调 用对应的用户数字证书，通过用户数字证书中的公钥按照约定的解密算法对所述签名值进行解密，并与所述业务服务器临时生成的随机数进行对比来实现验证。

[0019] 其中，所述存储于移动通信终端中的公钥和私钥通过设置本地安全密码来保护，并在发出登录请求时通过输入本地安全密码来读取公钥和私钥。

[0020] 其中，所述注册资料信息还包括用户名和 / 或用户资料。

[0021] 其中，所述公钥和私钥存储于移动通信终端的特定隐藏保护分区中。

[0022] 本发明所要解决的另一技术问题是提供一种无线应用服务的安全认证系统的注册方法，其提高了无线网络中应用服务的使用安全性。

[0023] 一种无线应用服务的安全认证系统的注册方法，包括以下步骤：

[0024] 移动通信终端生成一对公钥和私钥并存储上述公钥和私钥；

[0025] 将包括移动通信终端唯一标识和所述公钥的注册信息打包发送到业务服务器；

[0026] 业务服务器将所述注册信息发送到 CA 证书服务器，请求一份用户数字证书；

[0027] CA 证书服务器根据业务服务器发送的注册信息生成唯一对应的用户数字证书，返回给业务服务器；

[0028] 业务服务器存储注册信息，并将上述获取的用户数字证书存储到证书存储服务器中，向移动通信终端返回注册成功结果。

[0029] 其中，所述注册资料信息包括用户名和 / 或用户资料。

[0030] 其中，所述公钥和私钥存储于移动通信终端的特定隐藏保护分区中。

[0031] 本发明所要解决的又一技术问题是提供一种无线应用服务的安全认证系统的登录方法，其提高了无线网络中应用服务的使用安全性。

[0032] 一种无线应用服务的安全认证系统的登录方法，包括以下步骤：

[0033] 移动通信终端向业务服务器发送登录请求；

[0034] 业务服务器向移动通信终端发送验证信息；

[0035] 移动通信终端根据获取验证信息返回结果信息；

[0036] 业务服务器根据结果信息进行验证，并返回验证结果；

[0037] 所述验证信息为业务服务器临时生成的一个随机数，所述结果信息包括移动通信终端利用所述存储于移动通信终端中的私钥对所述随机数进行加密生成的签名值和注册资料信息中的用户名；所述业务服务器通过根据所述用户名调用对应的用户数字证书，通过用户数字证书中的公钥按照约定的解密算法对所述签名值进行解密，并与所述业务服务器临时生成的随机数进行对比来实现验证。

[0038] 其中，所述存储于移动通信终端中的公钥和私钥通过设置本地安全密码来保护，

并在发出登录请求时通过输入本地安全密码来读取公钥和私钥。

[0039] 与现有技术相比，本发明具有如下有益效果：本发明通过移动通信终端生成公钥和私钥，并通过本地安全密码来保护公钥和私钥，由于本地安全密码不在网络上传输，所以大大降低了公钥和私钥被获取的风险，从而提高了无线网络中应用服务的使用安全性；另外，本发明采用业务服务器发送临时随机数、移动通信终端用私钥加密做数字签名的登录方式，有效解决了通常证书认证在无线网络中传输影响效率的问题，而且业务服务器通过对数字签名随机数的验证来识别客户端设备的身份，加强了无线网络中应用服务的访问安全性。

[0040] 附图说明

[0041] 图 1 是本发明实施例的移动通信终端安全证书认证系统结构图；

[0042] 图 2 是本发明实施例的无线应用服务的安全认证系统的注册方法流程图；

[0043] 图 3 是本发明第一实施例的无线应用服务的安全认证系统的登录方法流程图；

[0044] 图 4 是本发明第二实施例的无线应用服务的安全认证系统的登录方法流程图。

具体实施方式

[0045] 下面结合附图和实施例，对本发明作进一步详细说明。

[0046] 如图 1 所示，本发明实施例的移动通信终端安全证书认证系统，包括依次通过无线网络或有线网络相互连接的移动通信终端、业务服务器和 CA(Certification Authority，认证中心）证书服务器、以及连接到业务服务器的证书存储服务器；

[0047] 其中移动通信终端主要用于生成并存储公钥和私钥，向业务服务器发送包含注册信息的注册请求和登录请求，以及在注册成功后通过设置本地安全密码来保护所述公钥和私钥，并在发出登录请求时通过本地安全密码读取公钥和私钥。由于本地安全密码设置于移动通信终端本地，不在网络上传输，大大降低了公钥和私钥被获取的风险。

[0048] 为进一步加强公钥和私钥的安全性，在本实施例中，将公钥和私钥存储在移动通信终端的特定隐藏保护分区中而不被其他程序直接读取。

[0049] 在本实施例中，移动通信终端主要是指手机、PDA 等。

[0050] 业务服务器主要用于获取移动通信终端发送的注册信息转发到 CA 证书服务器，并返回注册结果，存储所述注册信息；以及根据移动通信终端发送的登录请求，向移动通信终端发送验证信息，获取移动通信终端返回结果信息后，根据结果信息进行验证，并返回验证结果；其中，注册信息包括注册资料信息、移动通信终端唯一标识和所述公钥；注册资料信息主要包括用户 名和 / 或用户资料。

[0051] CA 证书服务器用于根据业务服务器发送的注册信息生成唯一对应的用户数字证书，返回给业务服务器；CA 证书服务器可以是任何一个获得证书发放资质的 CA 认证机构，也可以是 INTERNET 有线领域的，而不需要是无线网络运营商的认证机构。

[0052] 证书存储服务器是用来存储业务服务器获取的 CA 证书服务器根据注册信息生成的用户数字证书；

[0053] 如图 2 所示，本发明实施例的无线应用服务的安全认证系统的注册方法，包括以下步骤：

[0054] a1、移动通信终端生成一对公钥和私钥；

[0055] a2、存储上述公钥和私钥；

[0056] a3、用户通过移动通信终端输入注册资料信息；

[0057] a4、移动通信终端将包括注册资料信息、移动通信终端唯一标识和所述公钥的注册信息打包发送到业务服务器；

[0058] a5、业务服务器将注册信息发送到 CA 证书服务器，请求一份用户数字证书；

[0059] a6、CA 证书服务器根据业务服务器发送的注册信息生成唯一对应的用户数字证书，返回给业务服务器；

[0060] a7、业务服务器存储注册信息，并将上述用户数字证书存储到证书存储服务器中，向移动通信终端返回注册成功结果；

[0061] a8、移动通信终端设置本地安全密码来保护所述公钥和私钥；

[0062] 如图 3 所示，本发明第一实施例的无线应用服务的安全认证系统的登录方法，包括以下步骤：

[0063] b1、移动通信终端输入注册资料信息和本地安全密码，读取公钥和私钥，携带注册资料信息向业务服务器发送登录请求；

[0064] b2、业务服务器向移动通信终端发送验证信息；

[0065] b3、移动通信终端根据获取验证信息返回结果信息；

[0066] b4、业务服务器根据结果信息进行验证，并返回验证结果。

[0067] 在步骤 a6 中 CA 证书服务器主要是通过根密钥对注册信息进行数字签名来生成唯一对应的用户数字证书。

[0068] 本实施例通过移动通信终端生成公钥和私钥，并通过本地安全密码来保护公钥和私钥，由于本地安全密码只存储于移动通信终端不在网络上传输，所以大大降低了公钥和私钥被获取的风险，从而提高了无线网络中应用服务的使用安全性；

[0069] 如图 4 所示，本发明第二实施例的无线应用服务的安全认证系统的登录方法包括以下步骤：

[0070] c1、用户通过移动通信终端输入用户名和本地安全密码，读取公钥和私钥，携带用户名，向业务服务器发送登录请求；

[0071] c2、业务服务器临时产生一随机数，向移动通信终端发送；

[0072] c3、移动通信终端利用私钥对所述随机数进行加密生成的签名值，并将用户名和签到名值发送到业务服务器；

[0073] c4、业务服务器根据用户名调用对应的用户数字证书，将用户数字证书中的公钥按照约定的解密算法对所述签名值进行解密，并与所述随机数进行对比；

[0074] c5、判断上述对签到名值解密后的数据是否与随机数一致，若一致，则：

[0075] c6、验证通过，丢弃随机数；

[0076] 若不一致，则：

[0077] c7、验证失败，丢弃随机数，返回验证失败结果。

[0078] 上述业务服务器向移动通信终端发送的验证信息为业务服务器临时生成的一个随机数。由于随机数是临时性的，且只使用一次，防止了其他非法用 户的复制访问。

[0079] 移动通信终端利用私钥对随机数进行加密生成签名值，加上用户名作为结果信息一起返回给业务服务器。业务服务器通过根据用户名调用证书存储器中对应的用户数字证

书，将用户数字证书中的公钥按照约定的解密算法对所述签名值进行解密，并与随机数进行对比，若一致，则验证通过，丢弃随机数，用户登录系统；若不一致，则验证失败，丢弃随机数，返回验证失败结果。在现有技术条件下，传输的签名值在一定期限内不会被破解，保证了用户身份登录的安全性，又由于在本实施例中，用户验证过程只需要客户端传输用户名和随机数的签名值，大大减少了数据传输量，节约了无线网络流量。

[0080] 本实施例采用业务服务器发送临时随机数、移动通信终端用私钥加密做数字签名的登录方式，有效解决了通常证书认证在无线网络中传输影响效率的问题，而且业务服务器通过对数字签名随机数的验证来识别客户端设备的身份，加强了无线网络中应用服务的访问安全性。

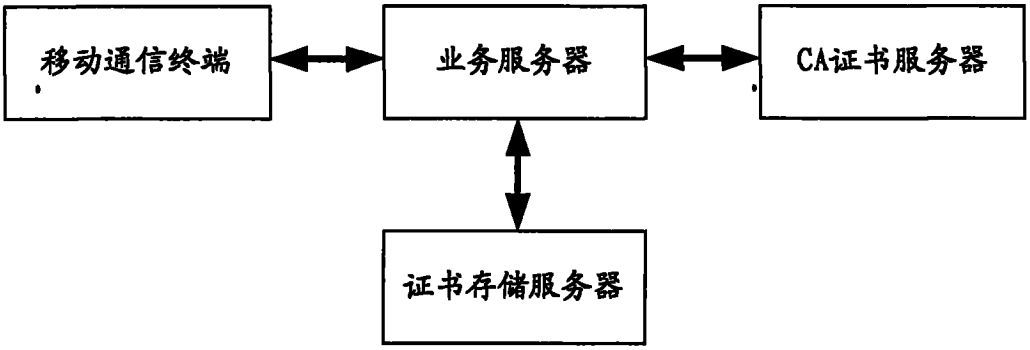

移动通信终端
业务服务器
CA证书服务器
证书存储服务器

图 1

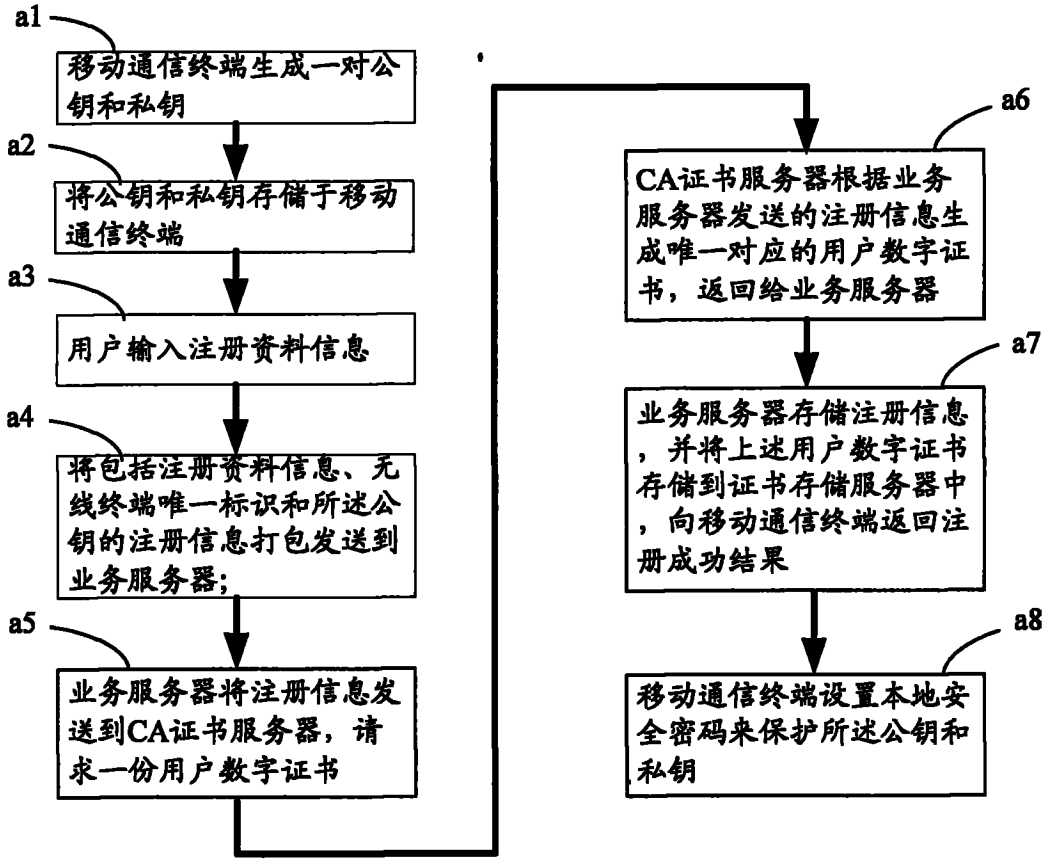

a1
移动通信终端生成一对公钥和私钥
a2
将公钥和私钥存储于移动通信终端
a3
用户输入注册资料信息
a4
将包括注册资料信息、无线终端唯一标识和所述公钥的注册信息打包发送到业务服务器;
a5
业务服务器将注册信息发送到CA证书服务器，请求一份用户数字证书
a6
CA证书服务器根据业务服务器发送的注册信息生成唯一对应的用户数字证书，返回给业务服务器
a7
业务服务器存储注册信息，并将上述用户数字证书存储到证书存储服务器中，向移动通信终端返回注册成功结果
a8
移动通信终端设置本地安全密码来保护所述公钥和私钥

图 2

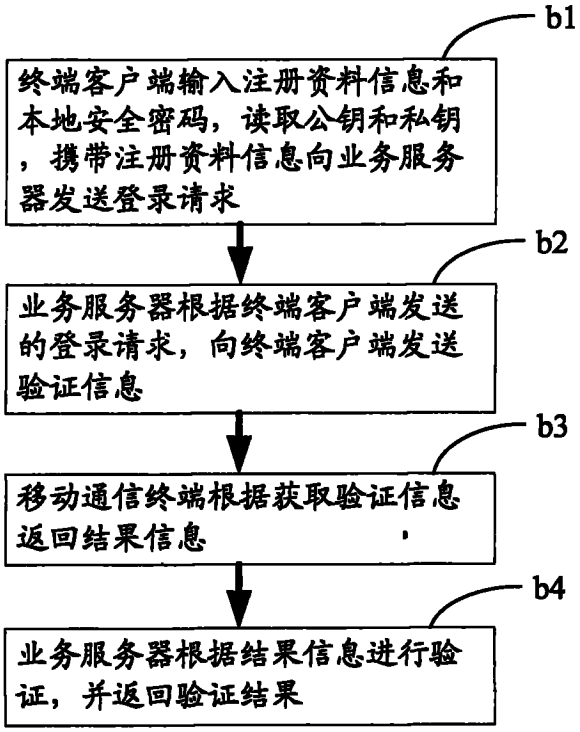

b1
终端客户端输入注册资料信息和本地安全密码，读取公钥和私钥，携带注册资料信息向业务服务器发送登录请求
b2
业务服务器根据终端客户端发送的登录请求，向终端客户端发送验证信息
b3
移动通信终端根据获取验证信息返回结果信息
b4
业务服务器根据结果信息进行验证，并返回验证结果

图 3

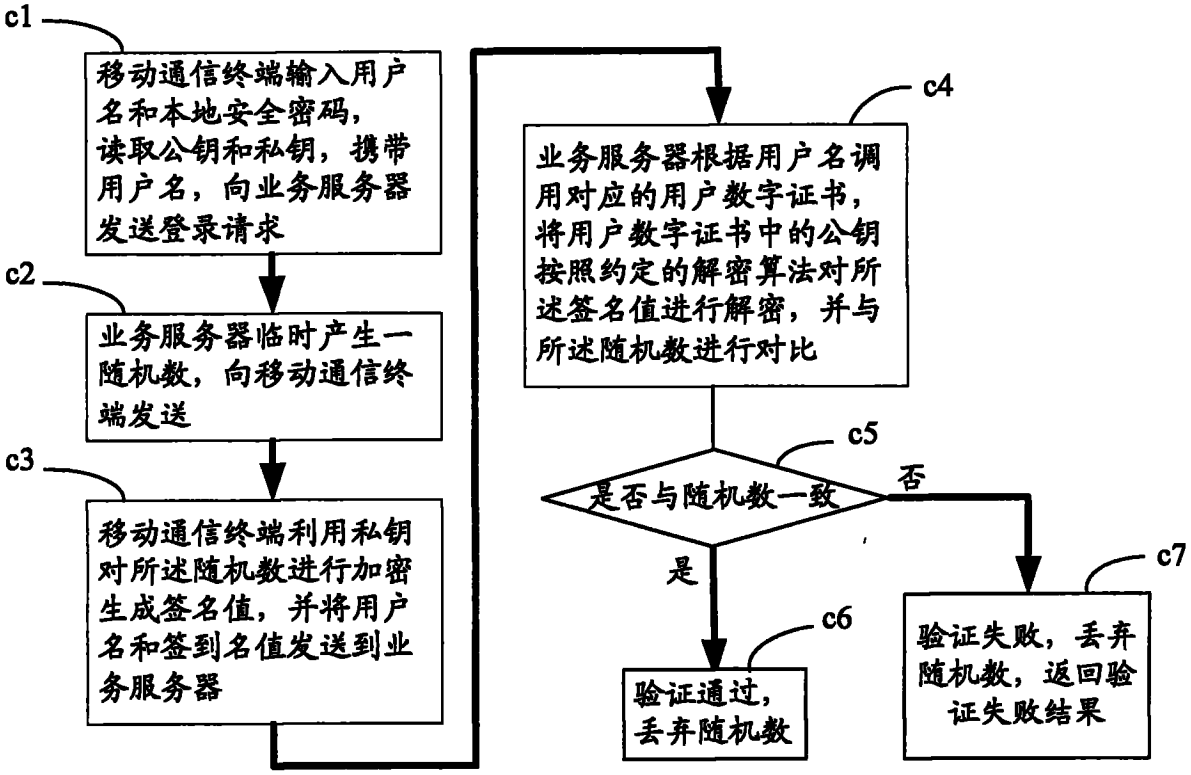

c1
移动通信终端输入用户名和本地安全密码，读取公钥和私钥，携带用户名，向业务服务器发送登录请求
c2
业务服务器临时产生一随机数，向移动通信终端发送
c3
移动通信终端利用私钥对所述随机数进行加密生成签名值，并将用户名和签到名值发送到业务服务器
c4
业务服务器根据用户名调用对应的用户数字证书，将用户数字证书中的公钥按照约定的解密算法对所述签名值进行解密，并与所述随机数进行对比
c5
是否与随机数一致
否
是
c6
验证通过，丢弃随机数
c7
验证失败，丢弃随机数，返回验证失败结果

图 4