(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 106549919 B
(45)授权公告日 2021.01.22

(21)申请号 201510604244.5

(22)申请日 2015.09.21

(65)同一申请的已公布的文献号
申请公布号 CN 106549919 A

(43)申请公布日 2017.03.29

(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛西湾路802号木槿街大展览馆31119号邮箱邮编KY1-1205

(72)发明人 孙元博

(74)专利代理机构 北京晋德允升知识产权代理有限公司 11623
代理人 王戈

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 101997824 A,2011.03.30
US 2008215890 A1,2008.09.04

审查员 侯停停

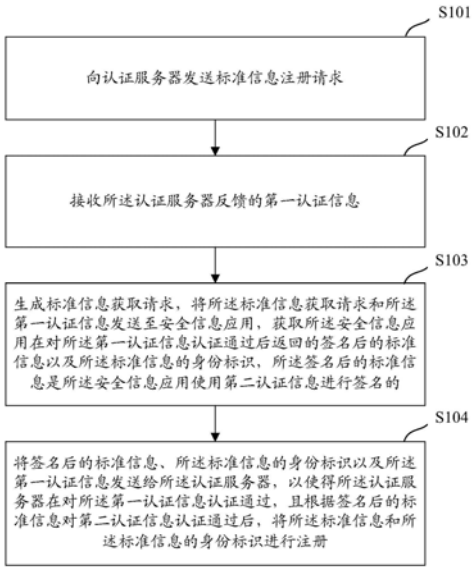
权利要求书7页 说明书16页 附图10页

(54)发明名称

一种信息注册、认证方法及装置

(57)摘要

本申请公开了一种信息注册、认证方法及装置，所述注册方法包括：向认证服务器发送标准信息注册请求，接收认证服务器反馈的第一认证信息，生成标准信息获取请求，将标准信息获取请求和第一认证信息发送至安全信息应用，获取安全信息应用在对所述第一认证信息认证通过后返回的签名后的标准信息以及标准信息的身份标识，其中，所述签名后的标准信息是所述安全信息应用使用第二认证信息进行签名的，将签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息发送给所述认证服务器，以使得所述认证服务器在对所述第一认证信息认证通过，且根据签名后的标准信息对第二认证信息认证通过后，将所述标准信息和所述标准信息的身份标识进行注册。



CN 106549919 B

1.一种信息注册方法,其特征在于,所述方法应用于业务应用,包括:

向认证服务器发送标准信息注册请求;

接收所述认证服务器反馈的第一认证信息,所述第一认证信息用于表明所述认证服务器的身份;

生成标准信息获取请求,将所述标准信息获取请求和所述第一认证信息发送至安全信息应用,由所述安全信息应用对所述第一认证信息进行认证,用以确定所述认证服务器的身份;获取所述安全信息应用在对所述第一认证信息认证通过后返回的签名后的标准信息以及所述标准信息的身份标识,其中,所述签名后的标准信息是所述安全信息应用使用第二认证信息进行签名的,所述标准信息为用户的生物特征信息;

将签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息发送给所述认证服务器,以使得所述认证服务器在对所述第一认证信息认证通过,且根据签名后的标准信息对第二认证信息认证通过后,将所述标准信息和所述标准信息的身份标识进行注册,并将所述标准信息用于对安全信息进行认证。

2.如权利要求1所述的方法,其特征在于,接收所述认证服务器反馈的第一认证信息,具体包括:

接收所述认证服务器发送的、采用该认证服务器自身的第一加密密钥进行签名后的证书,并将签名后的证书作为所述第一认证信息。

3.一种信息注册方法,其特征在于,所述方法应用于安全信息应用,包括:

接收业务应用发送的第一认证信息和标准信息获取请求,所述第一认证信息用于表明认证服务器的身份;

对所述第一认证信息进行认证,并在认证通过后,将使用第二认证信息进行签名后的标准信息,以及所述标准信息的身份标识返回给所述业务应用,使所述业务应用将签名后的标准信息以及所述标准信息的身份标识发送给认证服务器,以使得所述认证服务器在对所述第一认证信息认证通过,且根据签名后的标准信息对第二认证信息认证通过后,将所述标准信息和所述标准信息的身份标识进行注册,并将所述标准信息用于对安全信息进行认证;

其中,所述标准信息为用户的生物特征信息。

4.如权利要求3所述的方法,其特征在于,将使用第二认证信息进行签名后的标准信息,以及所述标准信息的身份标识返回给所述业务应用,具体包括:

接收用户输入的标准信息;

使用第二认证信息对所述标准信息进行签名,并针对所述标准信息,确定所述标准信息的身份标识;

将签名后的标准信息以及所述标准信息的身份标识,返回给所述业务应用。

5.如权利要求4所述的方法,其特征在于,所述标准信息的身份标识,包括所述标准信息的身份密钥信息,该身份密钥信息与所述用户的账户信息相关联。

6.如权利要求3所述的方法,其特征在于,所述第一认证信息中包括认证服务器签名后的证书;

对所述第一认证信息进行认证,具体包括:

使用与所述认证服务器的第一加密密钥相匹配的第一解密密钥对所述签名后的证书

进行解密认证。

7.如权利要求4所述的方法，其特征在于，所述第二认证信息包括预先与认证服务器约定的第二密钥信息；其中，所述第二密钥信息中包括第二加密密钥和第二解密密钥；

使用第二认证信息对所述标准信息进行签名，具体包括：

针对所述标准信息，使用预先与认证服务器约定的第二加密密钥进行签名。

8.一种信息注册方法，其特征在于，所述方法应用于认证服务器，包括：

认证服务器接收业务应用发送的标准信息注册请求；

根据所述标准信息注册请求，生成第一认证信息并反馈给所述业务应用，所述第一认证信息用于表明所述认证服务器的身份；以使所述业务应用生成标准信息获取请求后，将所述标准信息获取请求和所述第一认证信息发送至安全信息应用，由所述安全信息应用对所述第一认证信息进行认证，用以确定所述认证服务器的身份；以及，由所述业务应用获取所述安全信息应用在对所述第一认证信息认证通过后返回的签名后的标准信息以及所述标准信息的身份标识；其中，所述签名后的标准信息是所述安全信息应用使用第二认证信息进行签名的，所述标准信息为用户的生物特征信息；

接收所述业务应用发送的签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息；其中，所述签名后的标准信息是安全信息应用使用第二认证信息进行签名，并发送给所述业务应用的；

对所述第一认证信息进行认证，并根据签名后的标准信息对所述第二认证信息进行认证；

在对所述第一认证信息和所述第二认证信息认证均通过后，将所述标准信息以及所述标准信息的身份标识进行注册，并将所述标准信息用于对安全信息进行认证。

9.如权利要求8所述的方法，其特征在于，根据所述标准信息注册请求，生成第一认证信息并反馈给所述业务应用，具体包括：

根据所述标准信息注册请求，调取该认证服务器自身的证书；

使用自身的第一加密密钥对所述证书进行签名，作为第一认证信息，并反馈给所述业务应用。

10.如权利要求8所述的方法，其特征在于，对所述第一认证信息进行认证，具体包括：

使用第一解密密钥对所述第一认证信息进行解密认证。

11.如权利要求8所述的方法，其特征在于，所述第二认证信息包括预先由所述认证服务器与所述安全信息应用约定的第二密钥信息；其中，所述第二密钥信息包括：第二加密密钥和第二解密密钥；签名后的标准信息是由所述安全信息应用使用第二加密密钥进行签名的；

根据签名后的标准信息对所述第二认证信息进行认证，具体包括：

根据预先约定的第二密钥信息，使用与所述安全信息应用预先约定的第二解密密钥，对签名后的标准信息进行解密，以便对所述第二认证信息进行认证。

12.一种信息认证方法，其特征在于，所述方法应用于业务应用，包括：

向认证服务器发送针对待认证信息的校验请求；

接收所述认证服务器反馈的第一认证信息，所述第一认证信息用于表明所述认证服务器的身份；

生成待认证信息获取请求，将所述待认证信息获取请求和所述第一认证信息发送至安全信息应用，由所述安全信息应用对所述第一认证信息进行认证，用以确定所述认证服务器的身份；获取所述安全信息应用在对所述第一认证信息认证通过后返回的待认证信息以及所述待认证信息的待认证身份标识；其中，所述待认证信息为用户的生物特征信息；

将所述待认证信息、所述待认证身份标识以及所述第一认证信息发送给所述认证服务器，以使得所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给业务应用。

13.一种信息认证方法，其特征在于，所述方法应用于安全信息应用，包括：

接收业务应用发送的、携带有第一认证信息的待认证信息获取请求，所述第一认证信息用于表明认证服务器的身份；

对所述第一认证信息进行认证，并在认证通过后，将待认证信息以及所述待认证信息的待认证身份标识通过所述业务应用发送至认证服务器，以使得所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给所述业务应用；

其中，所述待认证信息为用户的生物特征信息。

14.如权利要求13所述的方法，其特征在于，根据携带有第一认证信息的待认证信息获取请求，将待认证信息以及所述待认证信息的待认证身份标识返回给所述业务应用，具体包括：

对所述待认证信息获取请求中携带的所述第一认证信息进行认证；

在认证通过后，接收用户输入的待认证信息；

识别所述待认证信息所属的标准信息，将与所述标准信息相匹配的身份标识确定为该待认证信息的待认证身份标识；

将所述待认证信息以及所述待认证信息的待认证身份标识返回给所述业务应用。

15.一种信息认证方法，其特征在于，所述方法应用于认证服务器，包括：

认证服务器接收业务应用发送的针对待认证信息的校验请求；

根据所述校验请求，生成第一认证信息并反馈给所述业务应用，所述第一认证信息用于表明所述认证服务器的身份；以使所述业务应用生成待认证信息获取请求后，将所述待认证信息获取请求和所述第一认证信息发送至安全信息应用，由所述安全信息应用对所述第一认证信息进行认证，用以确定所述认证服务器的身份；以及，由所述业务应用获取所述安全信息应用在对所述第一认证信息认证通过后返回的待认证信息以及所述待认证信息的身份标识；其中，所述待认证信息为用户的生物特征信息；

接收所述业务应用发送的待认证信息、所述待认证信息的待认证身份标识以及所述第一认证信息；

分别对所述第一认证信息、所述待认证身份标识以及所述待认证信息进行认证，生成认证结果反馈给所述业务应用。

16.如权利要求15所述的方法，其特征在于，分别对所述第一认证信息、所述身份标识以及所述待认证信息进行认证，具体包括：

针对所述第一认证信息，使用自身的第一解密密钥对所述第一认证信息进行解密，对解密后的证书进行认证；

针对所述待认证身份标识，根据已注册的标准信息的身份标识，判断所述待认证身份标识是否与已注册的标识信息的身份标识相匹配；

针对所述待认证信息，与已注册的标准信息进行比对认证。

17.如权利要求16所述的方法，其特征在于，生成认证结果反馈给所述业务应用，具体包括：

针对所述第一认证信息，若认证通过，则对所述待认证信息及待认证身份标识进行认证；否则，返回认证失败通知；

针对所述身份标识，若认证通过，则对所述待认证信息进行认证；否则，返回认证失败通知；

针对所述待认证信息，若认证成功，则返回成功通知；否则，则返回认证失败通知。

18.一种信息注册装置，其特征在于，所述装置包括：

注册请求模块，用于向认证服务器发送标准信息注册请求；

接收模块，用于接收所述认证服务器反馈的第一认证信息，所述第一认证信息用于表明所述认证服务器的身份；

获取模块，用于生成标准信息获取请求，将所述标准信息获取请求和所述第一认证信息发送至安全信息应用，由所述安全信息应用对所述第一认证信息进行认证，用以确定所述认证服务器的身份；获取所述安全信息应用在对所述第一认证信息认证通过后返回的签名后的标准信息以及所述标准信息的身份标识，其中，所述签名后的标准信息是所述安全信息应用使用第二认证信息进行签名的，所述标准信息为用户的生物特征信息；

发送模块，用于将签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息发送给所述认证服务器，以使得所述认证服务器在对所述第一认证信息认证通过，且根据签名后的标准信息对第二认证信息认证通过后，将所述标准信息和所述标准信息的身份标识进行注册，并将所述标准信息用于对安全信息进行认证。

19.如权利要求18所述的装置，其特征在于，所述接收模块，具体用于接收所述认证服务器发送的、采用该认证服务器自身的第一加密密钥进行签名后的证书，并将签名后的证书作为所述第一认证信息。

20.一种信息注册装置，其特征在于，所述装置包括：

接收模块，用于接收业务应用发送的第一认证信息和标准信息获取请求，所述第一认证信息用于表明认证服务器的身份；

签名模块，用于对所述第一认证信息进行认证，并在认证通过后，将使用第二认证信息进行签名后的标准信息，以及所述标准信息的身份标识返回给所述业务应用，使所述业务应用将签名后的标准信息以及所述标准信息的身份标识发送给认证服务器，以使得所述认证服务器在对所述第一认证信息认证通过，且根据签名后的标准信息对第二认证信息认证通过后，将所述标准信息和所述标准信息的身份标识进行注册，并将所述标准信息用于对安全信息进行认证；

其中，所述标准信息为用户的生物特征信息。

21.如权利要求20所述的装置，其特征在于，所述签名模块，具体用于接收用户输入的标准信息，使用第二认证信息对所述标准信息进行签名，并针对所述标准信息，确定所述标准信息的身份标识，将签名后的标准信息以及所述标准信息的身份标识，返回给所述业务

应用。

22.如权利要求21所述的装置，其特征在于，所述标准信息的身份标识，包括所述标准信息的身份密钥信息，该身份密钥信息与所述用户的账户信息相关联。

23.如权利要求20所述的装置，其特征在于，所述第一认证信息中包括认证服务器签名后的证书；所述签名模块，具体用于使用与所述认证服务器的第一加密密钥相匹配的第一解密密钥对所述签名后的证书进行解密认证。

24.如权利要求21所述的装置，其特征在于，所述第二认证信息包括预先与认证服务器约定的第二密钥信息；其中，所述第二密钥信息中包括第二加密密钥和第二解密密钥；

所述签名模块，具体用于针对所述标准信息，使用预先与认证服务器约定的第二加密密钥进行签名。

25.一种信息注册装置，其特征在于，所述装置包括：

注册请求接收模块，用于接收业务应用发送的标准信息注册请求；

反馈模块，用于根据所述标准信息注册请求，生成第一认证信息并反馈给所述业务应用，所述第一认证信息用于表明认证服务器的身份；以使所述业务应用生成标准信息获取请求后，将所述标准信息获取请求和所述第一认证信息发送至安全信息应用，由所述安全信息应用对所述第一认证信息进行认证，用以确定所述认证服务器的身份；以及，由所述业务应用获取所述安全信息应用在对所述第一认证信息认证通过后返回的签名后的标准信息以及所述标准信息的身份标识；其中，所述签名后的标准信息是所述安全信息应用使用第二认证信息进行签名的，所述标准信息为用户的生物特征信息；

注册信息接收模块，用于接收所述业务应用发送的签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息；其中，所述签名后的标准信息是安全信息应用使用第二认证信息进行签名，并发送给所述业务应用的；

认证模块，用于对所述第一认证信息进行认证，并根据签名后的标准信息对所述第二认证信息进行认证；

注册模块，用于在对所述第一认证信息和所述第二认证信息认证均通过后，将所述标准信息以及所述标准信息的身份标识进行注册，并将所述标准信息用于对安全信息进行认证。

26.如权利要求25所述的装置，其特征在于，所述反馈模块，具体用于根据所述标准信息注册请求，调取认证服务器自身的证书，使用自身的第一加密密钥对所述证书进行签名，作为第一认证信息，并反馈给所述业务应用。

27.如权利要求25所述的装置，其特征在于，所述认证模块，具体用于使用第一解密密钥对所述第一认证信息进行解密认证。

28.如权利要求25所述的装置，其特征在于，所述第二认证信息包括预先由认证服务器与所述安全信息应用约定的第二密钥信息；其中，所述第二密钥信息包括：第二加密密钥和第二解密密钥；签名后的标准信息是由所述安全信息应用使用第二加密密钥进行签名的；

所述认证模块，具体用于根据预先约定的第二密钥信息，使用与所述安全信息应用预先约定的第二解密密钥，对签名后的标准信息进行解密，以便对所述第二认证信息进行认证。

29.一种信息认证装置，其特征在于，所述装置包括：

认证请求模块，用于向认证服务器发送针对待认证信息的校验请求；

接收模块，用于接收所述认证服务器反馈的第一认证信息，所述第一认证信息用于表明所述认证服务器的身份；

获取模块，用于生成待认证信息获取请求，将所述待认证信息获取请求和所述第一认证信息发送至安全信息应用，由所述安全信息应用对所述第一认证信息进行认证，用以确定所述认证服务器的身份；获取所述安全信息应用在对所述第一认证信息认证通过后返回的待认证信息以及所述待认证信息的待认证身份标识；其中，所述待认证信息为用户的生物特征信息；

发送模块，用于将所述待认证信息、所述待认证身份标识以及所述第一认证信息发送给所述认证服务器，以使得所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给业务应用。

30.一种信息认证装置，其特征在于，所述装置包括：

接收模块，用于接收业务应用发送的、携带有第一认证信息的待认证信息获取请求，所述第一认证信息用于表明认证服务器的身份；

签名模块，用于对所述第一认证信息进行认证，并在认证通过后，将待认证信息以及所述待认证信息的待认证身份标识通过所述业务应用发送至认证服务器，以使得所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给所述业务应用；

其中，所述待认证信息为用户的生物特征信息。

31.如权利要求30所述的装置，其特征在于，所述签名模块，具体用于对所述待认证信息获取请求中携带的所述第一认证信息进行认证，在认证通过后，识别所述待认证信息所属的标准信息，将与所述标准信息相匹配的身份标识确定为该待认证信息的待认证身份标识，将所述待认证信息以及所述待认证信息的待认证身份标识返回给所述业务应用。

32.一种信息认证装置，其特征在于，所述装置包括：

认证请求接收模块，用于接收业务应用发送的针对待认证信息的校验请求；

反馈模块，用于根据所述校验请求，生成第一认证信息并反馈给所述业务应用，所述第一认证信息用于表明认证服务器的身份；以使所述业务应用生成待认证信息获取请求后，将所述待认证信息获取请求和所述第一认证信息发送至安全信息应用，由所述安全信息应用对所述第一认证信息进行认证，用以确定所述认证服务器的身份；以及，由所述业务应用获取所述安全信息应用在对所述第一认证信息认证通过后返回的待认证信息以及所述待认证信息的身份标识；其中，所述待认证信息为用户的生物特征信息；

认证信息接收模块，用于接收所述业务应用发送的待认证信息、所述待认证信息的待认证身份标识以及所述第一认证信息；

认证模块，用于分别对所述第一认证信息、所述待认证身份标识以及所述待认证信息进行认证，生成认证结果反馈给所述业务应用。

33.如权利要求32所述的装置，其特征在于，所述认证模块，具体用于针对所述第一认证信息，使用自身的第一解密密钥对所述第一认证信息进行解密，对解密后的证书进行认证；针对所述待认证身份标识，根据已注册的标准信息的身份标识，判断所述待认证身份标识是否与已注册的标识信息的身份标识相匹配；针对所述待认证信息，与已注册的标准

信息进行比对认证。

34.如权利要求33所述的装置，其特征在于，所述认证模块，具体用于针对所述第一认证信息，若认证通过，则对所述待认证信息及待认证身份标识进行认证；否则，返回认证失败通知；针对所述身份标识，若认证通过，则对所述待认证信息进行认证；否则，返回认证失败通知；针对所述待认证信息，若认证成功，则返回成功通知；否则，则返回认证失败通知。

一种信息注册、认证方法及装置

技术领域

[0001] 本申请涉及计算机技术领域，尤其涉及一种信息注册、认证方法及装置。

背景技术

[0002] 随着信息技术的发展，用户可通过终端(如手机、平板电脑等)中安装的服务提供商(如：软件开发商、网站等)的应用程序(以下简称业务应用)，便捷地获取各类业务服务。对于业务应用中所提供的业务服务而言，某些类别的业务服务具有较高的安全级别，比如：支付业务、转账业务等等。安全级别较高的业务服务往往需要用户提供相应的安全信息(如：密码、生物特征信息等)，并针对用户提供的安全信息进行认证后，方可完成业务服务。

[0003] 对于上述需要用户提供安全信息的业务服务而言，通常会在用户第一次使用该业务服务前，获取用户的安全信息作为标准信息(标准信息将作为后续认证过程的认证标准)，以便与后续用户输入的安全信息进行比对。在获取用户的安全信息的过程中，业务应用需要通过终端内的安全信息应用(如：生物信息管理应用，负责采集、存储用户输入的生物特征信息，该生物信息管理应用由终端制造商安装于该终端中)获取用户的安全信息。

[0004] 为了使得业务应用和安全信息应用之间进行调用、信息传输时更加便捷，现有技术中，终端系统(如：Android M系统)将安全信息应用运行在一种称为富可执行环境(Rich Execution Environment，REE)的架构中。REE具备了丰富的调用支持，使得运行在REE中的安全信息应用可更加便捷地被不同的业务应用调用，也可以更加便捷的传输各业务应用所需的信息。

[0005] 但是，REE并不属于安全环境，在安全信息应用与业务应用进行信息传输的过程中，安全信息容易被非法操作者在传输途中截取并进行篡改。尤其对于标准信息而言，由于服务提供商在此之前并未保存过用户提供的标准信息，也就无法识别标准信息的真伪，一旦标准信息在传输过程中被篡改，那么，服务提供商仍会接收被篡改后的标准信息，并作为后续认证过程中的认证标准，显然，这将导致非法操作者以用户的名义获得各类业务服务。

发明内容

[0006] 本申请实施例提供一种信息注册、认证方法及装置，用以解决现有技术中使用安全信息进行注册时安全性较低的问题。

[0007] 本申请实施例提供的一种信息注册方法，包括：

[0008] 向认证服务器发送标准信息注册请求；

[0009] 接收所述认证服务器反馈的第一认证信息；

[0010] 生成标准信息获取请求，将所述标准信息获取请求和所述第一认证信息发送至安全信息应用，获取所述安全信息应用在对所述第一认证信息认证通过后返回的签名后的标准信息以及所述标准信息的身份标识，其中，所述签名后的标准信息是所述安全信息应用使用第二认证信息进行签名的；

[0011] 将签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息发送给所

述认证服务器，以使得所述认证服务器在对所述第一认证信息认证通过，且根据签名后的标准信息对第二认证信息认证通过后，将所述标准信息和所述标准信息的身份标识进行注册。

[0012] 本申请实施例还提供的一种信息注册方法，包括：

[0013] 接收业务应用发送的第一认证信息和标准信息获取请求；

[0014] 对所述第一认证信息进行认证，并在认证通过后，将使用第二认证信息进行签名后的标准信息，以及所述标准信息的身份标识返回给所述业务应用，使所述业务应用将签名后的标准信息以及所述标准信息的身份标识发送给认证服务器，以使得所述认证服务器在对所述第一认证信息认证通过，且根据签名后的标准信息对第二认证信息认证通过后，将所述标准信息和所述标准信息的身份标识进行注册。

[0015] 本申请实施例还提供的一种信息注册方法，包括：

[0016] 认证服务器接收业务应用发送的标准信息注册请求；

[0017] 根据所述标准信息注册请求，生成第一认证信息并反馈给所述业务应用；

[0018] 接收所述业务应用发送的签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息；其中，所述签名后的标准信息是安全信息应用使用第二认证信息进行签名，并发送给所述业务应用的；

[0019] 对所述第一认证信息进行认证，并根据签名后的标准信息对所述第二认证信息进行认证；

[0020] 在对所述第一认证信息和所述第二认证信息认证均通过后，将所述标准信息以及所述标准信息的身份标识进行注册。

[0021] 本申请实施例还提供的一种信息认证方法，包括：

[0022] 向认证服务器发送针对待认证信息的校验请求；

[0023] 接收所述认证服务器反馈的第一认证信息；

[0024] 生成待认证信息获取请求，将所述待认证信息获取请求和所述第一认证信息发送至安全信息应用，获取所述安全信息应用在对所述第一认证信息认证通过后返回的待认证信息以及所述待认证信息的待认证身份标识；

[0025] 将所述待认证信息、所述待认证身份标识以及所述第一认证信息发送给所述认证服务器，以使得所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给所述业务应用。

[0026] 本申请实施例还提供的一种信息认证方法，包括：

[0027] 接收业务应用发送的、携带有第一认证信息的待认证信息获取请求；

[0028] 对所述第一认证信息进行认证，并在认证通过后，将待认证信息以及所述待认证信息的身份标识通过所述业务应用发送至认证服务器，以使得业务应用所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给所述业务应用。

[0029] 本申请实施例还提供的一种信息认证方法，包括：

[0030] 认证服务器接收业务应用发送的针对待认证信息的校验请求；

[0031] 根据所述校验请求，生成第一认证信息并反馈给所述业务应用；

[0032] 接收所述业务应用发送的待认证信息、所述待认证信息的待认证身份标识以及所

述第一认证信息；

[0033] 分别对所述第一认证信息、所述待认证身份标识以及所述待认证信息进行认证，生成认证结果反馈给所述业务应用。

[0034] 本申请实施例还提供的一种信息注册装置，包括：

[0035] 注册请求模块，用于向认证服务器发送标准信息注册请求；

[0036] 接收模块，用于接收所述认证服务器反馈的第一认证信息；

[0037] 获取模块，用于生成标准信息获取请求，将所述标准信息获取请求和所述第一认证信息发送至安全信息应用，获取所述安全信息应用在对所述第一认证信息认证通过后返回的签名后的标准信息以及所述标准信息的身份标识，其中，所述签名后的标准信息是所述安全信息应用使用第二认证信息进行签名的；

[0038] 发送模块，用于将签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息发送给所述认证服务器，以使得所述认证服务器在对所述第一认证信息认证通过，且根据签名后的标准信息对第二认证信息认证通过后，将所述标准信息和所述标准信息的身份标识进行注册。

[0039] 本申请实施例还提供的一种信息注册装置，包括：

[0040] 接收模块，用于接收业务应用发送的第一认证信息和标准信息获取请求；

[0041] 签名模块，用于对所述第一认证信息进行认证，并在认证通过后，将使用第二认证信息进行签名后的标准信息，以及所述标准信息的身份标识返回给所述业务应用，使所述业务应用将签名后的标准信息以及所述标准信息的身份标识发送给认证服务器，以使得所述认证服务器在对所述第一认证信息认证通过，且根据签名后的标准信息对第二认证信息认证通过后，将所述标准信息和所述标准信息的身份标识进行注册。

[0042] 本申请实施例还提供的一种信息注册装置，包括：

[0043] 注册请求接收模块，用于接收业务应用发送的标准信息注册请求；

[0044] 反馈模块，用于根据所述标准信息注册请求，生成第一认证信息并反馈给所述业务应用；

[0045] 注册信息接收模块，用于接收所述业务应用发送的签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息；其中，所述签名后的标准信息是安全信息应用使用第二认证信息进行签名，并发送给所述业务应用的；

[0046] 认证模块，用于对所述第一认证信息进行认证，并根据签名后的标准信息对所述第二认证信息进行认证；

[0047] 注册模块，用于在对所述第一认证信息和所述第二认证信息认证均通过后，将所述标准信息以及所述标准信息的身份标识进行注册。

[0048] 本申请实施例还提供的一种信息认证装置，包括：

[0049] 注册请求模块，用于向认证服务器发送针对待认证信息的校验请求；

[0050] 接收模块，用于接收所述认证服务器反馈的第一认证信息；

[0051] 获取模块，用于生成待认证信息获取请求，将所述待认证信息获取请求和所述第一认证信息发送至安全信息应用，获取所述安全信息应用在对所述第一认证信息认证通过后返回的待认证信息以及所述待认证信息的待认证身份标识；

[0052] 发送模块，用于将所述待认证信息、所述待认证身份标识以及所述第一认证信息

发送给所述认证服务器，以使得所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给所述业务应用。

[0053] 本申请实施例还提供的一种信息认证装置，包括：

[0054] 接收模块，用于接收业务应用发送的、携带有第一认证信息的待认证信息获取请求；

[0055] 签名模块，用于对所述第一认证信息进行认证，并在认证通过后，将待认证信息以及所述待认证信息的身份标识通过所述业务应用发送至认证服务器，以使得业务应用所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给所述业务应用。

[0056] 本申请实施例还提供的一种信息认证装置，包括：

[0057] 认证请求接收模块，用于接收业务应用发送的针对待认证信息的校验请求；

[0058] 反馈模块，用于根据所述校验请求，生成第一认证信息并反馈给所述业务应用；

[0059] 认证信息接收模块，用于接收所述业务应用发送的待认证信息、所述待认证信息的待认证身份标识以及所述第一认证信息；

[0060] 认证模块，用于分别对所述第一认证信息、所述待认证身份标识以及所述待认证信息进行认证，生成认证结果反馈给所述业务应用。

[0061] 本申请实施例提供一种信息注册、认证方法及装置，当用户在使用业务服务需要注册标准信息时，业务应用会向认证服务器发起标准信息注册请求，并接收认证服务器所反馈的第一认证信息，之后，业务应用会生成标准信息获取请求和第一认证信息一并发送给安全信息应用，在安全信息应用针对第一认证信息进行认证通过后，会使用自身的第二认证信息对标准信息进行签名，并确定出该标准信息的身份标识，再将签名后的标准信息及该标准信息的身份标识反馈给业务应用，从而，业务应用会将安全信息应用所反馈的，以及第一认证信息发送给认证服务器，以便认证服务器进行认证后，将标准信息及其身份标识进行注册。从上述方式中可见，第一认证信息作为认证服务器的一种标识，可以使得安全信息应用确定出标准信息注册者的身份；返回认证服务器的第一认证信息，使得认证服务器可以确定出信息在传输途中是否被篡改，而返回认证服务器的签名后的标准信息，使得认证服务器可以确定出标准信息是否由终端内的安全信息应用所提供，这样的方式可以有效保障认证服务器可以准确地识别出在传输途中被篡改后的标准信息，有效提升了在注册标准信息时的安全性。

附图说明

[0062] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0063] 图1至图3为本申请实施例提供的信息注册过程；

[0064] 图4为本申请实施例提供的在实际应用场景下的信息注册过程；

[0065] 图5至图7为本申请实施例提供的信息认证过程；

[0066] 图8为本申请实施例提供的在实际应用场景下的信息认证过程；

[0067] 图9至图11为本申请实施例提供的信息注册装置结构示意图；

[0068] 图12至图14为本申请实施例提供的信息认证装置结构示意图。

具体实施方式

[0069] 为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0070] 如前所述，当服务提供商第一次接收到标准信息时，由于之前并未存储过与该标准信息相关的安全信息，所以，也就无法准确地确定出该标准信息在传输过程中是否被篡改。而如果服务提供商与终端之间事先约定了一系列的认证信息，并使用这些认证信息对标准信息进行认证，也就可以识别出标准信息是否在传输过程中被篡改。正是基于此，本申请中提供了下述的信息注册和认证方法。

[0071] 在本申请实施例中，提供了一种信息注册方法，如图1所示，该方法包括如下步骤：

[0072] S101：向认证服务器发送标准信息注册请求。

[0073] 在实际应用场景下，当用户使用业务应用中提供的安全级别较高的业务服务(如：指纹支付业务)时，通常需要用户提供相应的安全信息(如：指纹信息)，尤其对于用户第一次使用该业务服务的情况下，通常需要用户输入安全信息作为标准信息，用以对用户后续使用该业务服务时输入的安全信息进行对比校验。

[0074] 也就是说，在用户第一使用该业务服务时，需要通过业务应用向相应的认证服务中注册用户提供的标准信息。故在本申请实施例的上述步骤中，由运行在终端内的业务应用向认证服务器发出标准信息注册请求。

[0075] 其中，本申请中所述的终端包括但不限于：手机、平板电脑、智能手表等移动终端，在一些场景中，也可以是计算机终端。所述的认证服务器，可以是服务提供商后台服务系统中用以进行安全认证的服务器，也可以是专门用于进行安全认证的第三方服务器。当然，这里并不构成对本申请的限定。

[0076] S102：接收所述认证服务器反馈的第一认证信息。

[0077] 所述的第一认证信息，是由认证服务器向发出标准信息注册请求的业务应用反馈的标识信息，用以表明认证服务器的身份。在本申请实施例的一种场景中，第一认证信息可包括认证服务自身的证书。

[0078] S103：生成标准信息获取请求，将所述标准信息获取请求和所述第一认证信息发送至安全信息应用，获取所述安全信息应用在对所述第一认证信息认证通过后返回的签名后的标准信息以及所述标准信息的身份标识。

[0079] 其中，所述签名后的标准信息是所述安全信息应用使用第二认证信息进行签名的。

[0080] 当业务应用接收到了认证服务器反馈的第一认证信息后，就会生成标准信息获取请求，以请求终端内的安全信息应用提供注册所需的标准信息。

[0081] 需要说明的是，本申请中的安全信息应用是运行在终端内的本地应用，用于向业务应用提供业务服务所需的安全信息(包括标准信息)。而安全信息属于用户自身的关键信息，为了防止有非法操作者向该安全信息应用请求用户的安全信息，安全信息应用将对标准信息的使用者身份进行认证。基于此，当业务应用将标准信息获取请求发送至安全信息应用时，还会将第一认证信息也发送给安全信息，从而，安全信息应用将对第一认证信息进

行认证，以确定认证服务器的身份。只有在安全信息应用对第一认证信息认证通过后，才会提供标准信息。

[0082] 考虑到在实际应用中，由安全信息应用所提供的标准信息在传输的过程中可能被篡改，所以，在本申请中，安全信息应用在反馈标准信息之前，将对标准信息进行签名操作，用以表明该标准信息是由该终端内的安全信息应用所发送的。同时，也考虑到该标准信息是用户提供的，故可以针对该标准信息，确定该标准信息的身份标识，用以表明该标准信息是由用户提供的。这样一来，安全信息应用向业务应用反馈的标准信息，也就有了两种标识：分别用来表明该标准信息是由终端内的安全信息应用发送的、且该标准信息是由用户提供的。

[0083] 具体而言，本申请中的安全信息应用会使用第二认证信息对该标准信息进行签名，用以表明该标准信息是由该安全信息应用所发送。当然，在本申请中，第二认证信息可以是认证服务器与终端内的安全信息应用(或终端本身)之间预先约定的第二密钥信息，这里并不做具体限定。标准信息的身份标识也由该安全信息应用确定，在本申请中，标准信息的身份标识包括可以表明该标准信息的身份密钥信息，该身份密钥信息通常与用户的账户信息相关联。也就是说，一对身份密钥信息唯一对应一个账户信息，这样也就能够表明该标准信息属于该用户。当然，这里也不做具体限定。

[0084] S104：将签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息发送给所述认证服务器，以使得所述认证服务器在对所述第一认证信息认证通过，且根据签名后的标准信息对第二认证信息认证通过后，将所述标准信息和所述标准信息的身份标识进行注册。

[0085] 当业务应用接收到安全信息应用的反馈后，就会将安全信息应用所反馈的签名后的标准信息、该标准信息的身份标识以及由认证服务器发送的第一认证信息，一并发送给认证服务器进行认证并注册。

[0086] 认证服务器接收到了业务应用发送的上述信息后，就会对所接收到的信息进行认证。如果认证通过，那么也就表明由安全信息应用所发送的标准信息在传输途中并未被篡改，从而，认证服务器也就可以将标准信息及其身份标识进行注册。注册的标准信息以及身份标识也就可以用来对后续用户提供的安全信息进行认证识别。

[0087] 通过上述步骤，当用户在使用业务服务需要注册标准信息时，业务应用会向认证服务器发起标准信息注册请求，并接收认证服务器所反馈的第一认证信息，之后，业务应用会生成标准信息获取请求和第一认证信息一并发送给安全信息应用，在安全信息应用针对第一认证信息进行认证通过后，会使用自身的第二认证信息对标准信息进行签名，并确定出该标准信息的身份标识，再将签名后的标准信息及该标准信息的身份标识反馈给业务应用，从而，业务应用会将安全信息应用所反馈的，以及第一认证信息发送给认证服务器，以便认证服务器进行认证后，将标准信息及其身份标识进行注册。从上述方式中可见，第一认证信息作为认证服务器的一种标识，可以使得安全信息应用确定出标准信息注册者的身份；返回认证服务器的第一认证信息，使得认证服务器可以确定出信息在传输途中是否被篡改，而返回认证服务器的签名后的标准信息，使得认证服务器可以确定出标准信息是否由终端内的安全信息应用所提供，这样的方式可以有效保障认证服务器可以准确地识别出在传输途中被篡改后的标准信息，有效提升了在注册标准信息时的安全性。

[0088] 对于上述的第一认证信息而言，第一认证信息是认证服务器的一种标识，用来标示认证服务器的身份，具体可以将认证服务器自身的证书作为第一认证信息，当然，考虑到传输过程中的安全性，认证服务器可以使用自身的密钥信息对其证书进行签名操作。那么，作为本申请实施例中的一种可选方式，上述步骤S102：接收所述认证服务器反馈的第一认证信息，具体为：接收所述认证服务器发送的、采用该认证服务器自身的第一加密密钥进行签名后的证书，并将签名后的证书作为所述第一认证信息。

[0089] 此外，在实际应用中的某些场景下，认证服务器向业务应用反馈的第一认证信息中，还包含有挑战码。当业务应用向认证服务器发送一次请求后，认证服务器就会生成一个具有唯一性的挑战码，携带在第一认证信息中反馈给业务应用。可以认为，一个挑战码就对应一次业务请求。采用挑战码的方式可以防止重放攻击。

[0090] 以上内容是基于终端内的业务应用的角度所进行的描述。而对于提供标准信息的安全信息应用而言，本申请实施例中还提供了一种信息注册过程，如图2所示，该过程包括如下步骤：

[0091] S201：接收业务应用发送的第一认证信息和标准信息获取请求。

[0092] 本实施例中的第一认证信息和标准信息获取请求如前所述。在此不再赘述。

[0093] S202：对所述第一认证信息进行认证，并在认证通过后，将使用第二认证信息进行签名后的标准信息，以及所述标准信息的身份标识返回给所述业务应用，使所述业务应用将签名后的标准信息以及所述标准信息的身份标识发送给认证服务器，以使得所述认证服务器在对所述第一认证信息认证通过，且根据签名后的标准信息对第二认证信息认证通过后，将所述标准信息和所述标准信息的身份标识进行注册

[0094] 当安全信息应用接收到了业务应用发送的第一认证信息和标准信息获取请求后，首先会对第一认证信息进行认证，以便确定出标准信息的注册者的身份。只有在安全信息应用确定了认证服务器的身份后，安全信息应用才会将用户提供的标准信息进行签名，并确定出该标准信息的身份标识，再将签名后的标准信息和该标准信息的身份标识反馈给业务应用。从而，业务应用将安全信息应用反馈的一系列信息和第一认证信息一并发送给认证服务器。后续由认证服务器进行认证，并在认证通过后对标准信息和该标准信息的身份标识进行注册。这里的内容与上述方法中的过程相同，故在此不再过多赘述。

[0095] 通过上述步骤，由认证服务器提供的第一认证信息可以标示出认证服务器的身份，安全信息应用对第一认证信息的认证，可以避免非法操作者向该安全信息应用获取标准信息。而安全信息应用对用户提供的标准信息进行签名的方式，是用来表明该标准信息是由安全信息应用发送的，同时确定出该标准信息的身份标识，用来表明该标准信息由该用户提供，显然，安全信息应用反馈给业务应用的标准信息中包含了两种标识，而如果标准信息在传输过程中被篡改，那么，标准信息的两种标识都将会发生改变。这样的方式可以有效地反映出标准信息在传输过程中是否被篡改，也就保证了最终认证服务器在注册时的安全性。

[0096] 将使用第二认证信息进行签名后的标准信息，以及所述标准信息的身份标识返回给所述业务应用，具体为：接收用户输入的标准信息，使用第二认证信息对所述标准信息进行签名，并针对所述标准信息，确定所述标准信息的身份标识，将签名后的标准信息以及所述标准信息的身份标识，返回给所述业务应用。

[0097] 如前所述，本申请中标准信息的身份标识，具体可以包括该标准信息的身份密钥信息，该身份密钥信息通常与用户的账户信息相关联。在传输过程中，为了保证该身份密钥信息的安全性，在本申请实施例中的一种可选方式下，安全信息应用也可以使用第二认证信息对所述身份密钥信息(也即，标准信息的身份标识)进行签名。当然，这里并不构成对本申请的限定。

[0098] 同样，正如前述，第一认证信息可表明认证服务器的身份，而在本申请中的一种方式下，第一认证信息包括认证服务器自身的证书，此时，对所述第一认证信息进行认证，具体为：使用与所述认证服务器的第一加密密钥相匹配的第一解密密钥对所述签名后的证书进行解密认证。

[0099] 对于第二认证信息而言，在本申请实施例中的一种方式下，所述第二认证信息包括预先与认证服务器约定的第二密钥信息，其中，所述第二密钥信息中包括第二加密密钥和第二解密密钥，在此场景下，使用第二认证信息对所述标准信息进行签名，具体为：针对所述标准信息，使用预先与认证服务器约定的第二加密密钥进行签名。

[0100] 当然，在标准信息的身份标识包括该标准信息的身份密钥信息的情况下，还可以使用上述第二认证信息对身份密钥信息进行签名。这里与上述方式中的内容类似，故在此不再过多赘述。

[0101] 以上内容是基于运行在终端内的安全信息应用角度的描述，而对于认证服务器而言，本申请实施例中还提供一种信息注册过程，如图3所示，具体包括以下步骤：

[0102] S301：认证服务器接收业务应用发送的标准信息注册请求。

[0103] S302：根据所述标准信息注册请求，生成第一认证信息并反馈给所述业务应用。

[0104] S303：接收所述业务应用发送的签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息；其中，所述签名后的标准信息是安全信息应用使用第二认证信息进行签名，并发送给所述业务应用的。

[0105] S304：对所述第一认证信息进行认证，并根据签名后的标准信息对所述第二认证信息进行认证。

[0106] S305：在对所述第一认证信息和所述第二认证信息认证均通过后，将所述标准信息以及所述标准信息的身份标识进行注册。

[0107] 与上述如图1和图2所示的方法相类似，认证服务器会在接收到业务应用发送的标准信息注册请求后，将向业务应用反馈可表明该认证服务器自身身份的第一认证信息，使得业务应用向安全信息发送标准信息获取请求后，安全信息应用可以根据第一认证信息，确定出认证服务器的身份，从而，安全信息应用才会向业务应用反馈使用第二认证信息签名后的标准信息和该标准信息的身份标识。当认证服务器接收到了业务应用返回的签名后的标准信息和第一认证信息后，便会对第一认证信息进行认证，并根据签名后的标准信息对第二认证信息进行认证，如果认证均通过，那么，也就表明标准信息在传输过程中并未被篡改，从而，认证服务器会将标准信息及其身份信息进行注册，以便后续过程进行认证识别。

[0108] 正如前述内容所述，认证服务器自身的证书可有效证明该认证服务器的身份，而为了保证安全信息应用接收到的证书的有效性，认证服务器通常会对其自身的证书进行签名，从而，如果该证书在传输过程中被篡改，安全信息应用就可以识别出来，故针对上述步

骤S302而言，根据所述标准信息注册请求，生成第一认证信息并反馈给所述业务应用，具体为：根据所述标准信息注册请求，调取该认证服务器自身的证书，使用自身的第一加密密钥对所述证书进行签名，作为第一认证信息，并反馈给所述业务应用。

[0109] 与前述方法中的内容相类似，在本申请实施例的一种场景下，认证服务器还可以将挑战码也携带在第一认证信息中，并使用自身的第一加密密钥签名后发送给业务应用。这里并不构成对本申请的限定。

[0110] 当业务应用向认证服务器返回了签名后的标准信息和第一认证信息后，认证服务器也就会对第一认证信息进行认证，并根据签名后的标准信息对第二认证信息进行认证。

[0111] 具体而言，对第一认证信息进行认证，具体包括：使用第一解密密钥对所述第一认证信息进行解密认证。认证服务器将使用自身的第一解密密钥对第一认证信息进行解密认证，如果解密后的证书(或挑战码)发生了变化，那么，就表明在传输的过程中极有可能被篡改，从而，认证服务器将判定为认证不通过。而如果认证服务器在解密后，证书(或挑战码)未发生变化，那么就通过认证。

[0112] 对于第二认证信息而言，与前述方法中的内容相类似，所述第二认证信息包括预先由所述认证服务器与所述安全信息应用约定的第二密钥信息；其中，所述第二密钥信息包括：第二加密密钥和第二解密密钥。此外，签名后的标准信息是由所述安全应用使用第二加密密钥进行签名的。在这种场景下，根据签名后的标准信息对所述第二认证信息进行认证，具体为：根据预先约定的第二密钥信息，使用与所述安全信息应用预先约定的第二解密密钥，对签名后的标准信息进行解密，以便对所述第二认证信息进行认证。

[0113] 如果认证服务器使用约定的第二解密密钥针对签名后的标准信息进行解密，并获得了标准信息，那么，就可以认为标准信息在传输的过程中并未被篡改，从而通过认证。而如果进行解密后，得到的是无法使用的信息，则表明签名的信息并不是采用预先约定的第二加密密钥进行签名的，这就极有可能是被篡改后的信息，从而认证不通过。

[0114] 只有在认证服务器进行认证通过之后，认证服务器才会将标准信息和该标准信息的身份标识进行注册。

[0115] 通过上述如图1至图3所示的信息注册方法，使得认证服务器可以有效地识别出标准信息在传输过程中是否被篡改，也就保证了用户能够在使用业务服务时不被非法操作者所影响。

[0116] 当然，针对上述信息注册方法，可适用于任意终端通过业务应用获取业务服务的场景中，且上述的认证服务器可以是服务提供商后台服务系统内的具有认证功能的服务器。而考虑到实际应用场景中，对于可提供诸如支付业务、转账业务等对安全级别要求较高的业务服务的服务提供商而言，通常使用一种称为互联网金融身份认证联盟(Internet Finance Authentication Alliance，IFAA)的网络身份认证架构，实现对安全级别要求较高的业务服务所需的身份认证支持。也即，由IFAA提供认证服务器，实现上述的注册过程。

[0117] 在这样的场景下，不同的设备制造厂商也会采用IFAA所提供的身份认证架构，在其生产的终端中提供身份认证必备的接口或服务。

[0118] 为了清楚的阐述本申请中的上述注册方法，现以IFAA提供的身份认证架构中进行注册为例，进行详细说明。

[0119] 如图4所示，为本示例中终端和IFAA认证服务器之间进行注册的实际应用过程。其

中，终端内运行有业务应用和安全信息应用，业务应用作为某服务提供商的业务服务接入口，可为使用该终端的用户提供各类业务服务，而安全信息应用用于为业务应用提供所需的安全信息(在本示例中为标准信息)。图4中所示的过程具体包括如下步骤：

[0120] S401：业务应用向IFAA认证服务器发送标准信息注册请求。

[0121] 当用户在终端中第一次使用该业务应用中的某业务服务时，就需要在IFAA认证服务器中注册该用户的生物信息，作为标准信息。此时，业务应用就会向IFAA认证服务器发出标准信息注册请求。

[0122] S402：IFAA认证服务器将签名后的包含挑战码和证书的数据包反馈给业务应用。

[0123] 其中，挑战码可以防止重放攻击，证书用以表明该IFAA认证服务器自身的身份。可以认为，经过签名后的数据包就是上述注册方法中所述的第一认证信息。

[0124] 另外，需要说明的是，本步骤中，IFAA认证服务器使用IFAAS秘钥信息对上述的数据包进行签名，该IFAAS秘钥信息由IFAA认证服务器自身生成。而IFAA认证服务器自身的证书由BIOM秘钥信息进行签名，BIOM秘钥信息用于表明提供该业务服务的服务提供商的类别。

[0125] S403：业务应用生成标准信息获取请求，并将该标准信息获取请求和签名后的数据包通过IFAAService发送给安全信息应用。

[0126] 其中，IFAAService是设置于终端内的IFAA身份认证架构所提供的一种服务。当然，在实际应用场景中的一种方式下，业务应用可通过IFAASDK(一种基于IFAA身份认证架构下的通信工具)调用IFAAService，这里并不做具体限定。

[0127] S404：安全信息应用对签名后的数据包进行认证，在认证通过后，将标准信息进行签名。

[0128] 需要说明的是，安全信息应用首先要对签名后的数据包进行解密(具体可以使用IFAA秘钥信息进行解密，这里不作具体限定)，在解密后，将认证数据包中的证书(可使用BIOM秘钥信息对证书进行解密认证)，以认证是不是IFAA将注册标准信息。

[0129] 在认证通过后，安全信息应用将获得用户输入的生物信息，作为标准信息，并使用DA秘钥信息对标准信息进行签名。其中，DA秘钥信息用于表明该终端的身份(在一种情况下，DA秘钥信息可表明安全信息应用的身份，而安全应用信息是设备制造商设置于该终端内的，所以，DA秘钥信息也表明终端的身份)。

[0130] S405：根据签名后的标准信息，确定该标准信息的身份秘钥信息。

[0131] 在本示例中，标准信息的身份秘钥信息通常与用户在业务应用中所使用的账户信息相关联，用以表明该标准信息所属的用户。实际应用中，标准信息的身份秘钥信息的生成，可由IFAAService通过KeyStore(一种REE环境下的安全存储标准调用接口)调用KeyMaster(一种安全存储模块)，并由KeyMaster生成该身份秘钥信息。

[0132] 需要说明的是，为了保证身份秘钥信息在传输过程中的安全行，安全信息应用可以使用DA秘钥信息对身份秘钥信息进行签名。

[0133] S406：安全信息应用将终端证书、签名后的标准信息、签名后的身份密钥信息返回给业务应用。

[0134] S407：通过IFAAService将终端证书、签名后的标准信息、签名后的身份密钥信息发送给IFAA认证服务器。

[0135] 需要说明的是，终端证书也称为authenticator证书，是参与IFAA身份认证架构的设备制造商为其生产的设备中所设置的，也即，终端证书可以表明该终端是否使用了IFAA的身份认证架构。

[0136] 当然，在本示例的一种方式下，同时返回IFAA认证服务器的还有前述的挑战码和IFAA认证服务器自身的证书，这样一来，IFAA认证服务器还可对挑战码和IFAA认证服务器自身的证书进行认证。

[0137] S408：IFAA认证服务器对接收到的信息进行认证，在认证通过后，将标准信息及其身份密钥信息进行注册。

[0138] 需要说明的是，IFAA认证服务器首先将对终端证书进行认证，具体可使用IFAA秘钥信息对接收到的信息进行解密，并认证终端证书的合法性，通过后，将使用DA秘钥信息对身份秘钥信息进行解密认证，通过后，再对签名的标准信息使用DA秘钥信息进行解密认证，均通过后，那么，就可以认为标准信息在传输途中未被篡改，则IFAA认证服务器将标准信息及其身份秘钥信息进行注册。

[0139] S409：向业务应用反馈注册结果。

[0140] 通过上例可见，在实际应用场景下，可以使用多种秘钥信息来准确确定出标准信息在传输过程中是否被篡改。

[0141] 以上内容是标准信息的注册方法，在注册了标准信息后，用户便可以使用相应的业务服务，当用户使用业务服务时，就需要提供用户的安全信息，相应地，认证服务器也就可以根据用户在使用业务服务时所提供的安全信息进行认证。故在本申请实施例中，还提供了一种信息认证方法，如图5所示，所述方法包括如下步骤：

[0142] S501：向认证服务器发送针对待认证信息的校验请求。

[0143] 当用户使用业务应用中的业务服务(如：指纹支付业务)时，往往需要用户提供自身的安全信息(如：指纹信息)，与之前注册的标准信息进行比对。此时，业务应用将会获取用户的安全信息，作为待认证信息，后续将发送至认证服务器中进行认证校验。

[0144] 在上述情况下，业务应用就会向认证服务器发送待认证信息的校验请求。

[0145] S502：接收所述认证服务器反馈的第一认证信息。

[0146] 与前述注册方法中类似，第一认证信息表明了认证服务器的身份。在此不再过多赘述。

[0147] S503：根据所述第一认证信息，生成待认证信息获取请求发送至安全信息应用，获取由所述安全信息应用提供的待认证信息，以及所述待认证信息的待认证身份标识。

[0148] 类似地，安全信息应用将根据第一认证信息确定出认证者的身份，在确定了认证者的身份合法后，通过认证，再将用户提供的待认证信息及其待认证身份标识一并返回给业务应用。

[0149] 与前述注册方法中不同的是，对于待认证信息而言，无需使用第二认证信息进行签名。

[0150] S504：将所述待认证信息、所述待认证身份标识以及所述第一认证信息发送给所述认证服务器，以使得所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给所述业务应用。

[0151] 从上述内容中可以看出，通过第一认证信息和待认证身份标识，可以识别出待认

证信息是否在传输过程中被篡改，在认证通过后，认证服务器才会对待认证信息进行认证。

[0152] 在本申请实施例中，还提供一种信息认证方法，如图6所示，该方法包括如下步骤：

[0153] S601：接收业务应用发送的、携带有第一认证信息的待认证信息获取请求。

[0154] S602：根据携带有第一认证信息的标准信息获取请求，将待认证信息以及所述待认证信息的身份标识通过所述业务应用发送至认证服务器，以使得业务应用所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给所述业务应用。

[0155] 对于上述步骤S602，根据携带有第一认证信息的标准信息获取请求，将待认证信息以及所述待认证信息的身份标识返回给所述业务应用，具体为：对所述标准信息获取请求中携带的所述第一认证信息进行认证，在认证通过后，接收用户输入的待认证信息，识别所述待认证信息所属的标准信息，将与所述标准信息相匹配的身份标识确定为该待认证信息的待认证身份标识，将所述待认证信息以及所述待认证信息的待认证身份标识返回给所述业务应用。

[0156] 在本申请实施例中，还提供一种信息认证方法，如图7所示，该方法包括如下步骤：

[0157] S701：认证服务器接收业务应用发送的针对待认证信息的校验请求。

[0158] S702：根据所述校验请求，生成第一认证信息并反馈给所述业务应用。

[0159] S703：接收所述业务应用发送的待认证信息、所述待认证信息的身份标识以及所述第一认证信息。

[0160] S704：分别对所述第一认证信息、所述身份标识以及所述待认证信息进行认证，生成认证结果反馈给所述业务应用。

[0161] 需要说明的是，对于上述步骤S704而言，认证服务器将对业务应用发送的信息分别进行认证，具体而言，分别对所述第一认证信息、所述身份标识以及所述待认证信息进行认证，具体为：针对所述第一认证信息，使用自身的第一解密密钥对所述第一认证信息进行解密，对解密后的所述证书进行认证，对所述身份标识，根据已注册的标准信息的身份标识，判断所述身份标识是否与已注册的标识信息的身份标识相匹配，针对所述待认证信息，与已注册的标准信息进行比对认证。

[0162] 在实际应用场景中，认证服务器在认证的过程中，如果有任一信息的认证未通过，那么，认证服务器就可以反馈失败通知，而只有当所有信息均通过认证后，才会反馈成功通知。那么，具体而言，生成认证结果反馈给所述业务应用，具体为：针对所述第一认证信息，若认证通过，则对所述待认证信息及待认证身份标识进行认证；否则，返回认证失败通知；针对所述身份标识，若认证通过，则对所述待认证信息进行认证；否则，返回认证失败通知；针对所述待认证信息，若认证成功，则返回成功通知；否则，则返回认证失败通知。

[0163] 与上述注册过程相对应，为了清楚的阐述本申请中的上述认证方法，现以IFAA提供的身份认证架构中进行认证为例，进行详细说明。

[0164] 如图8所示，为本示例中终端和IFAA认证服务器之间进行认证的实际应用过程。所示的过程具体包括如下步骤：

[0165] S801：业务应用向IFAA认证服务器发送待认证信息校验请求。

[0166] S802：IFAA认证服务器将签名后的包含挑战码和证书的数据包反馈给业务应用。

[0167] S803：业务应用生成待认证信息获取请求，并将该待认证信息获取请求和签名后

的数据包通过IFAAService发送给安全信息应用。

[0168] S804:安全信息应用对签名后的数据包进行认证,在认证通过后,将待认证信息使用注册过程中的身份秘钥信息进行签名。

[0169] S805:安全信息应用将签名后的待认证信息返回给业务应用。

[0170] S806:通过IFAAService将签名后的待认证信息发送给IFAA认证服务器。

[0171] S807:IFAA认证服务器针对接收到的签名后的待认证信息,使用注册的身份秘钥信息对签名后的待认证信息进行认证,通过后,将待认证信息与已注册标准信息进行比对认证。

[0172] S808:向业务应用返回认证结果。

[0173] 以上为本申请实施例提供的信息传输方法,基于同样的思路,本申请实施例还提供一种信息注册装置,如图9所示,所述装置包括:

[0174] 注册请求模块901,用于向认证服务器发送标准信息注册请求。

[0175] 接收模块902,用于接收所述认证服务器反馈的第一认证信息。

[0176] 获取模块903,用于生成标准信息获取请求,将所述标准信息获取请求和所述第一认证信息发送至安全信息应用,获取所述安全信息应用在对所述第一认证信息认证通过后返回的签名后的标准信息以及所述标准信息的身份标识,其中,所述签名后的标准信息是所述安全信息应用使用第二认证信息进行签名的。

[0177] 发送模块904,用于将签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息发送给所述认证服务器,以使得所述认证服务器在对所述第一认证信息认证通过,且根据签名后的标准信息对第二认证信息认证通过后,将所述标准信息和所述标准信息的身份标识进行注册。

[0178] 所述接收模块902,具体用于接收所述认证服务器发送的、采用该认证服务器自身的第一加密密钥进行签名后的证书,并将签名后的证书作为所述第一认证信息。

[0179] 如图10所示,本申请实施例还提供一种信息注册装置,所述装置包括:

[0180] 接收模块1001,用于接收业务应用发送的第一认证信息和标准信息获取请求;

[0181] 签名模块1002,用于对所述第一认证信息进行认证,并在认证通过后,将使用第二认证信息进行签名后的标准信息,以及所述标准信息的身份标识返回给所述业务应用,使所述业务应用将签名后的标准信息以及所述标准信息的身份标识发送给认证服务器,以使得所述认证服务器在对所述第一认证信息认证通过,且根据签名后的标准信息对第二认证信息认证通过后,将所述标准信息和所述标准信息的身份标识进行注册。

[0182] 所述签名模块1002,具体用于接收用户输入的标准信息,使用第二认证信息对所述标准信息进行签名,并针对所述标准信息,确定所述标准信息的身份标识,将签名后的标准信息以及所述标准信息的身份标识,返回给所述业务应用。

[0183] 需要说明的是,所述标准信息的身份标识,包括所述标准信息的身份密钥信息,该身份密钥信息与所述用户的账户信息相关联。

[0184] 在所述第一认证信息中包括认证服务器签名后的证书的场景下,所述签名模块1002,具体用于使用与所述认证服务器的第一加密密钥相匹配的第一解密密钥对所述签名后的证书进行解密认证。

[0185] 所述第二认证信息包括预先与认证服务器约定的第二密钥信息,其中,所述第二

密钥信息中包括第二加密密钥和第二解密密钥，所述签名模块1002，具体用于针对所述标准信息，使用预先与认证服务器约定的第二加密密钥进行签名。

[0186] 如图11所示，本申请实施例还提供一种信息注册装置，所述装置包括：

[0187] 注册请求接收模块1101，用于接收业务应用发送的标准信息注册请求；

[0188] 反馈模块1102，用于根据所述标准信息注册请求，生成第一认证信息并反馈给所述业务应用；

[0189] 注册信息接收模块1103，用于接收所述业务应用发送的签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息；其中，所述签名后的标准信息是安全信息应用使用第二认证信息进行签名，并发送给所述业务应用的；

[0190] 认证模块1104，用于对所述第一认证信息进行认证，并根据签名后的标准信息对所述第二认证信息进行认证；

[0191] 注册模块1105，用于在对所述第一认证信息和所述第二认证信息认证均通过后，将所述标准信息以及所述标准信息的身份标识进行注册。

[0192] 具体地，所述反馈模块1102，具体用于根据所述标准信息注册请求，调取该认证服务器自身的证书，使用自身的第一加密密钥对所述证书进行签名，作为第一认证信息，并反馈给所述业务应用。

[0193] 所述认证模块1104，具体用于使用第一解密密钥对所述第一认证信息进行解密认证。

[0194] 所述第二认证信息包括预先由所述认证服务器与所述安全信息应用约定的第二密钥信息；其中，所述第二密钥信息包括：第二加密密钥和第二解密密钥；签名后的标准信息是由所述安全应用使用第二加密密钥进行签名的。该场景下，所述认证模块1104，具体用于根据预先约定的第二密钥信息，使用与所述安全信息应用预先约定的第二解密密钥，对签名后的标准信息进行解密，以便对所述第二认证信息进行认证。

[0195] 如图12所示，本申请实施例还提供一种信息认证装置，所述装置包括：

[0196] 注册请求模块1201，用于向认证服务器发送针对待认证信息的校验请求；

[0197] 接收模块1202，用于接收所述认证服务器反馈的第一认证信息；

[0198] 获取模块1203，用于生成待认证信息获取请求，将所述待认证信息获取请求和所述第一认证信息发送至安全信息应用，获取所述安全信息应用在对所述第一认证信息认证通过后返回的待认证信息以及所述待认证信息的待认证身份标识；

[0199] 发送模块1204，用于将所述待认证信息、所述待认证身份标识以及所述第一认证信息发送给所述认证服务器，以使得所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给所述业务应用。

[0200] 如图13所示，本申请实施例还提供一种信息认证装置，所述装置包括：

[0201] 接收模块1301，用于接收业务应用发送的、携带有第一认证信息的待认证信息获取请求；

[0202] 签名模块1302，用于对所述第一认证信息进行认证，并在认证通过后，将待认证信息以及所述待认证信息的身份标识通过所述业务应用发送至认证服务器，以使得业务应用所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给所述业务应用。

[0203] 具体地，所述签名模块1302，具体用于对所述标准信息获取请求中携带的所述第一认证信息进行认证，在认证通过后，识别所述待认证信息所属的标准信息，将与所述标准信息相匹配的身份标识确定为该待认证信息的待认证身份标识，将所述待认证信息以及所述待认证信息的待认证身份标识返回给所述业务应用。

[0204] 如图14所示，本申请实施例还提供一种信息认证装置，所述装置包括：

[0205] 认证请求接收模块1401，用于接收业务应用发送的针对待认证信息的校验请求；

[0206] 反馈模块1402，用于根据所述校验请求，生成第一认证信息并反馈给所述业务应用；

[0207] 认证信息接收模块1403，用于接收所述业务应用发送的待认证信息、所述待认证信息的待认证身份标识以及所述第一认证信息；

[0208] 认证模块1404，用于分别对所述第一认证信息、所述待认证身份标识以及所述待认证信息进行认证，生成认证结果反馈给所述业务应用。

[0209] 所述认证模块1404，具体用于针对所述第一认证信息，使用自身的第一解密密钥对所述第一认证信息进行解密，对解密后的所述证书进行认证；针对所述待认证身份标识，根据已注册的标准信息的身份标识，判断所述待认证身份标识是否与已注册的标识信息的身份标识相匹配；针对所述待认证信息，与已注册的标准信息进行比对认证。

[0210] 所述认证模块1404，具体用于针对所述第一认证信息，若认证通过，则对所述待认证信息及待认证身份标识进行认证；否则，返回认证失败通知；针对所述身份标识，若认证通过，则对所述待认证信息进行认证；否则，返回认证失败通知；针对所述待认证信息，若认证成功，则返回成功通知；否则，则返回认证失败通知。

[0211] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0212] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0213] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0214] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0215] 本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。

因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0216] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

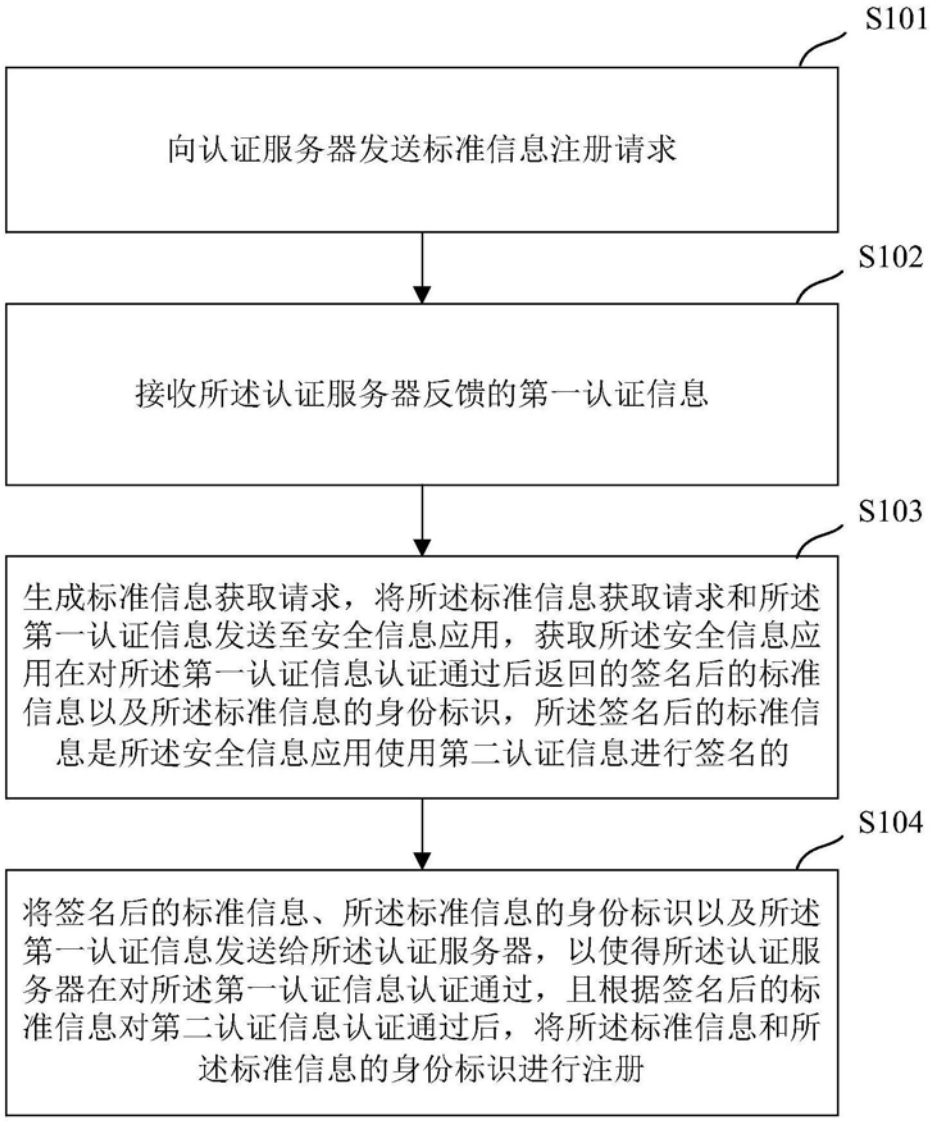

S101
向认证服务器发送标准信息注册请求
S102
接收所述认证服务器反馈的第一认证信息
S103
生成标准信息获取请求，将所述标准信息获取请求和所述第一认证信息发送至安全信息应用，获取所述安全信息应用在对所述第一认证信息认证通过后返回的签名后的标准信息以及所述标准信息的身份标识，所述签名后的标准信息是所述安全信息应用使用第二认证信息进行签名的
S104
将签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息发送给所述认证服务器，以使得所述认证服务器在对所述第一认证信息认证通过，且根据签名后的标准信息对第二认证信息认证通过后，将所述标准信息和所述标准信息的身份标识进行注册

图1

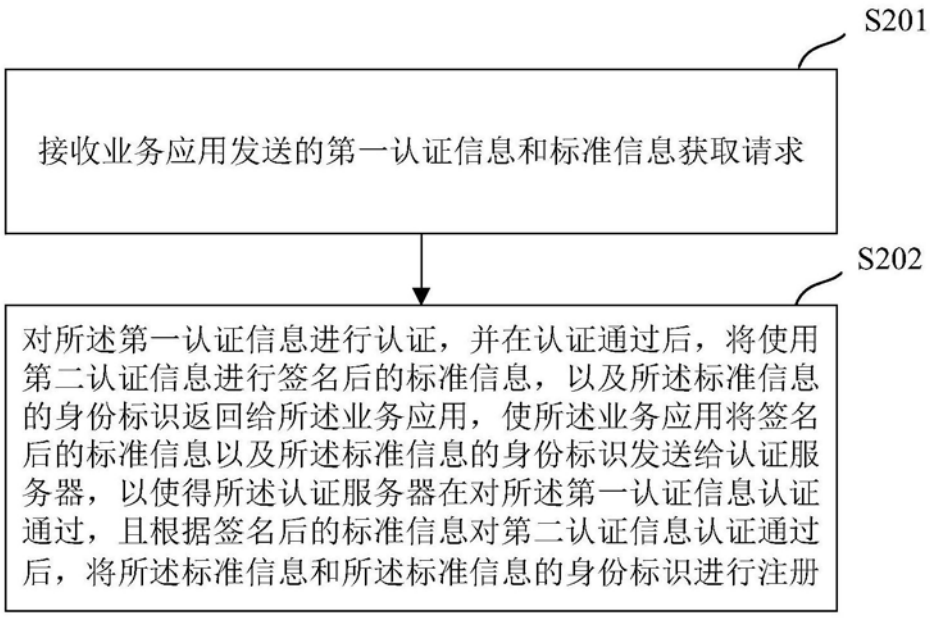

S201
接收业务应用发送的第一认证信息和标准信息获取请求
S202
对所述第一认证信息进行认证，并在认证通过后，将使用第二认证信息进行签名后的标准信息，以及所述标准信息的身份标识返回给所述业务应用，使所述业务应用将签名后的标准信息以及所述标准信息的身份标识发送给认证服务器，以使得所述认证服务器在对所述第一认证信息认证通过，且根据签名后的标准信息对第二认证信息认证通过后，将所述标准信息和所述标准信息的身份标识进行注册

图2

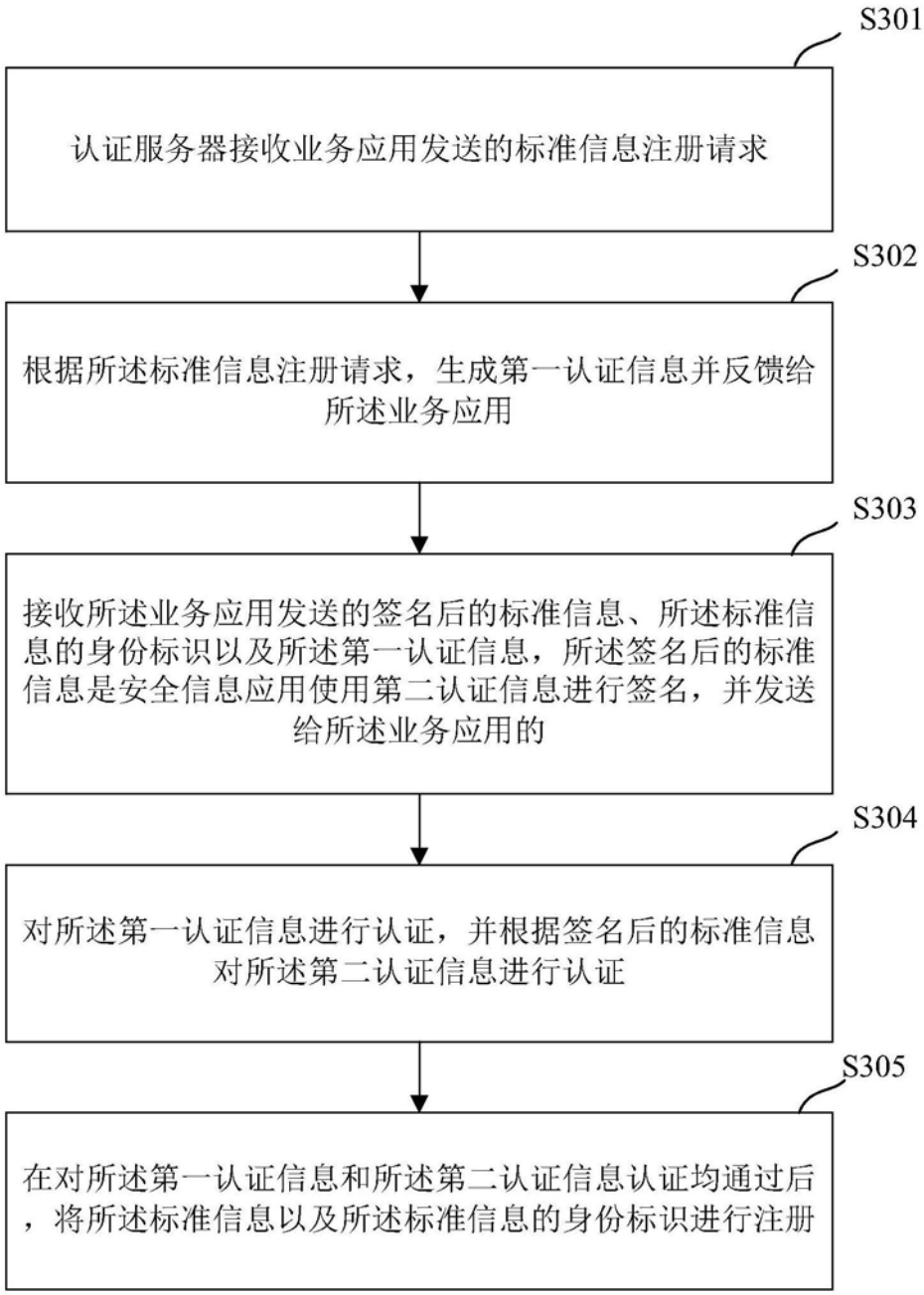

S301
认证服务器接收业务应用发送的标准信息注册请求
S302
根据所述标准信息注册请求，生成第一认证信息并反馈给所述业务应用
S303
接收所述业务应用发送的签名后的标准信息、所述标准信息的身份标识以及所述第一认证信息，所述签名后的标准信息是安全信息应用使用第二认证信息进行签名，并发送给所述业务应用的
S304
对所述第一认证信息进行认证，并根据签名后的标准信息对所述第二认证信息进行认证
S305
在对所述第一认证信息和所述第二认证信息认证均通过后，将所述标准信息以及所述标准信息的身份标识进行注册

图3

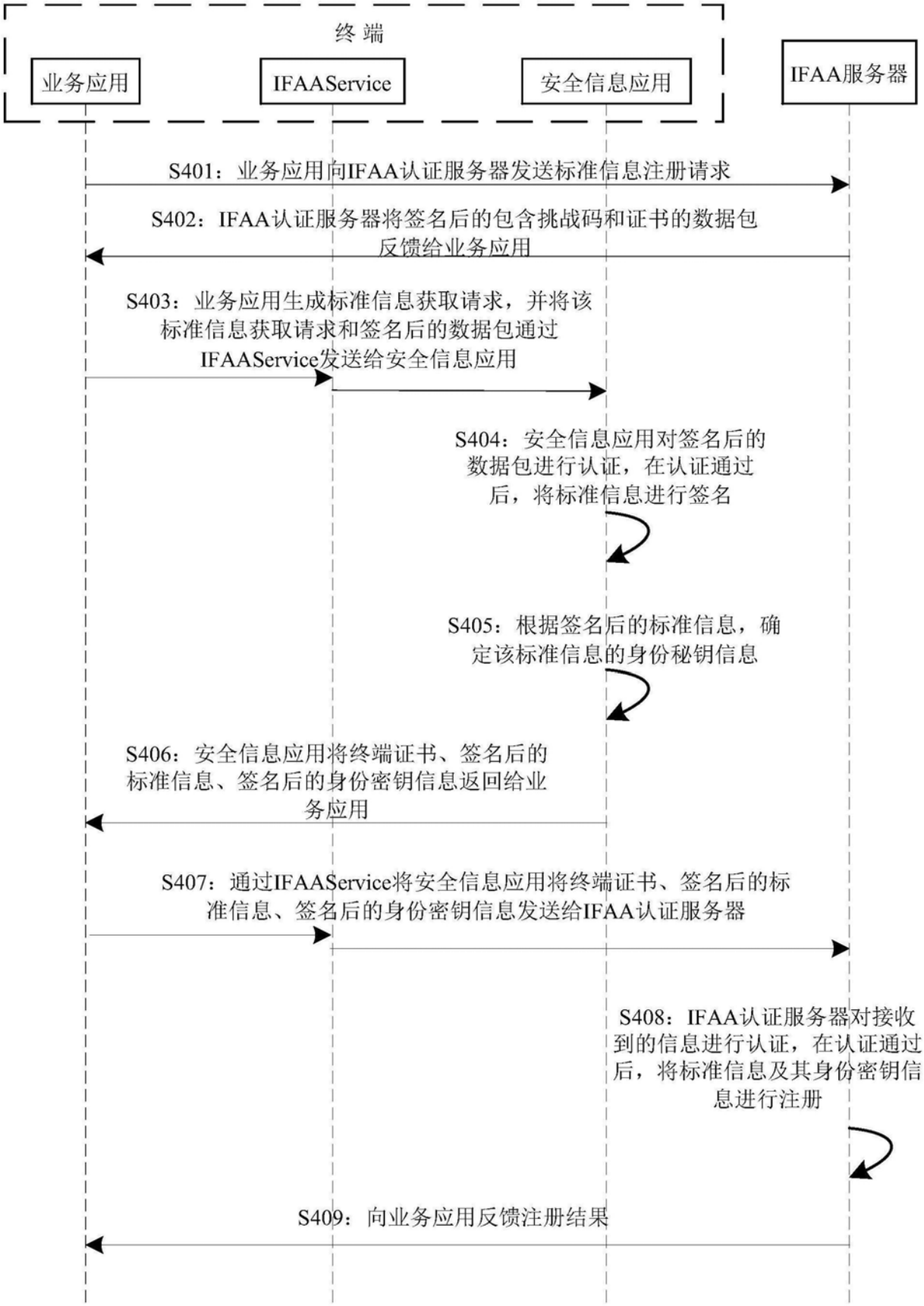

终端
业务应用
IFAAService
安全信息应用
IFAA服务器
S401：业务应用向IFAA认证服务器发送标准信息注册请求
S402：IFAA认证服务器将签名后的包含挑战码和证书的数据包反馈给业务应用
S403：业务应用生成标准信息获取请求，并将该标准信息获取请求和签名后的数据包通过IFAAService发送给安全信息应用
S404：安全信息应用对签名后的数据包进行认证，在认证通过后，将标准信息进行签名
S405：根据签名后的标准信息，确定该标准信息的身份秘钥信息
S406：安全信息应用将终端证书、签名后的标准信息、签名后的身份密钥信息返回给业务应用
S407：通过IFAAService将安全信息应用将终端证书、签名后的标准信息、签名后的身份密钥信息发送给IFAA认证服务器
S408：IFAA认证服务器对接收到的信息进行认证，在认证通过后，将标准信息及其身份密钥信息进行注册
S409：向业务应用反馈注册结果

图4

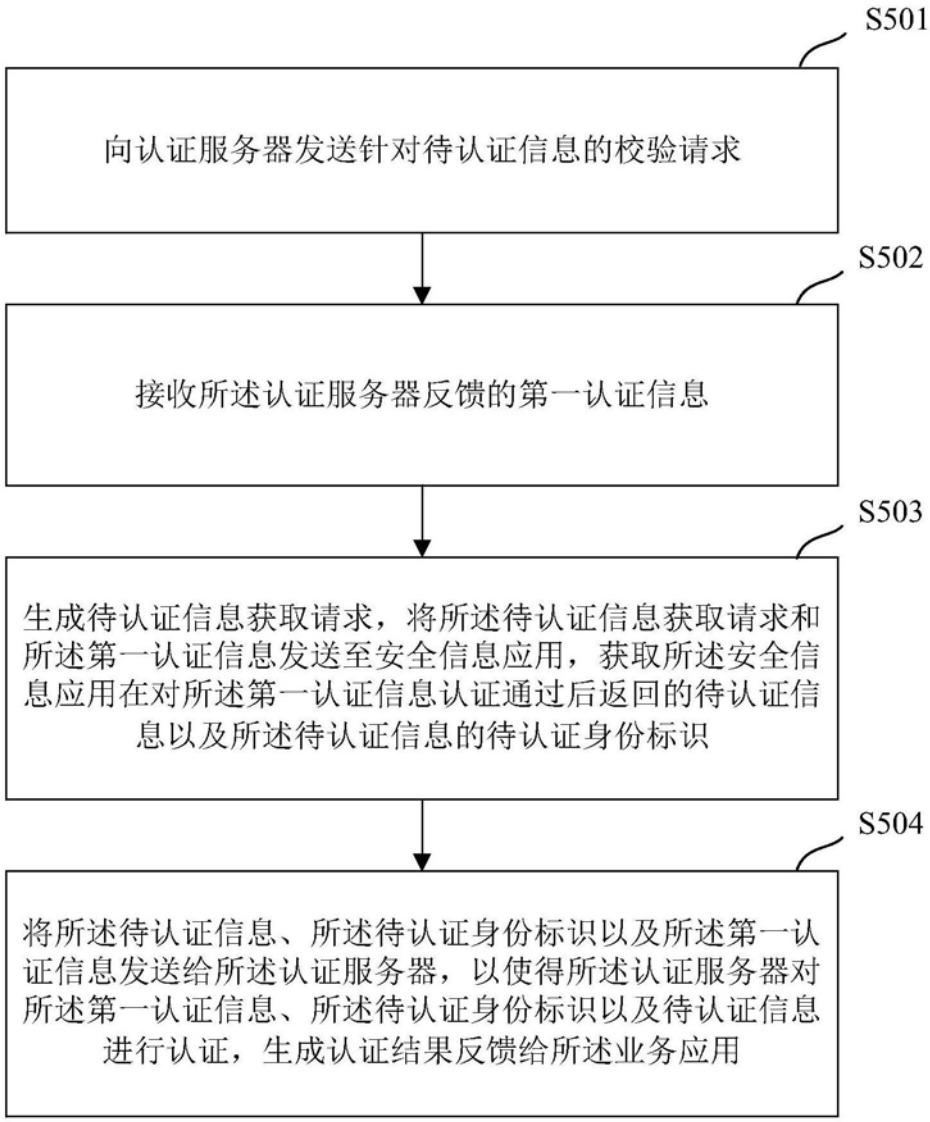

S501
向认证服务器发送针对待认证信息的校验请求
S502
接收所述认证服务器反馈的第一认证信息
S503
生成待认证信息获取请求，将所述待认证信息获取请求和所述第一认证信息发送至安全信息应用，获取所述安全信息应用在对所述第一认证信息认证通过后返回的待认证信息以及所述待认证信息的待认证身份标识
S504
将所述待认证信息、所述待认证身份标识以及所述第一认证信息发送给所述认证服务器，以使得所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给所述业务应用

图5

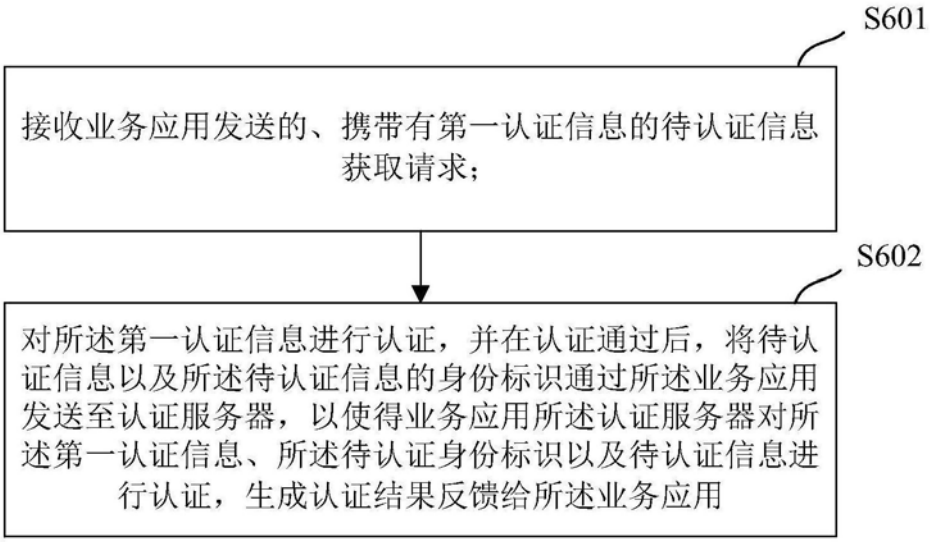

S601
接收业务应用发送的、携带有第一认证信息的待认证信息获取请求；
S602
对所述第一认证信息进行认证，并在认证通过后，将待认证信息以及所述待认证信息的身份标识通过所述业务应用发送至认证服务器，以使得业务应用所述认证服务器对所述第一认证信息、所述待认证身份标识以及待认证信息进行认证，生成认证结果反馈给所述业务应用

图6

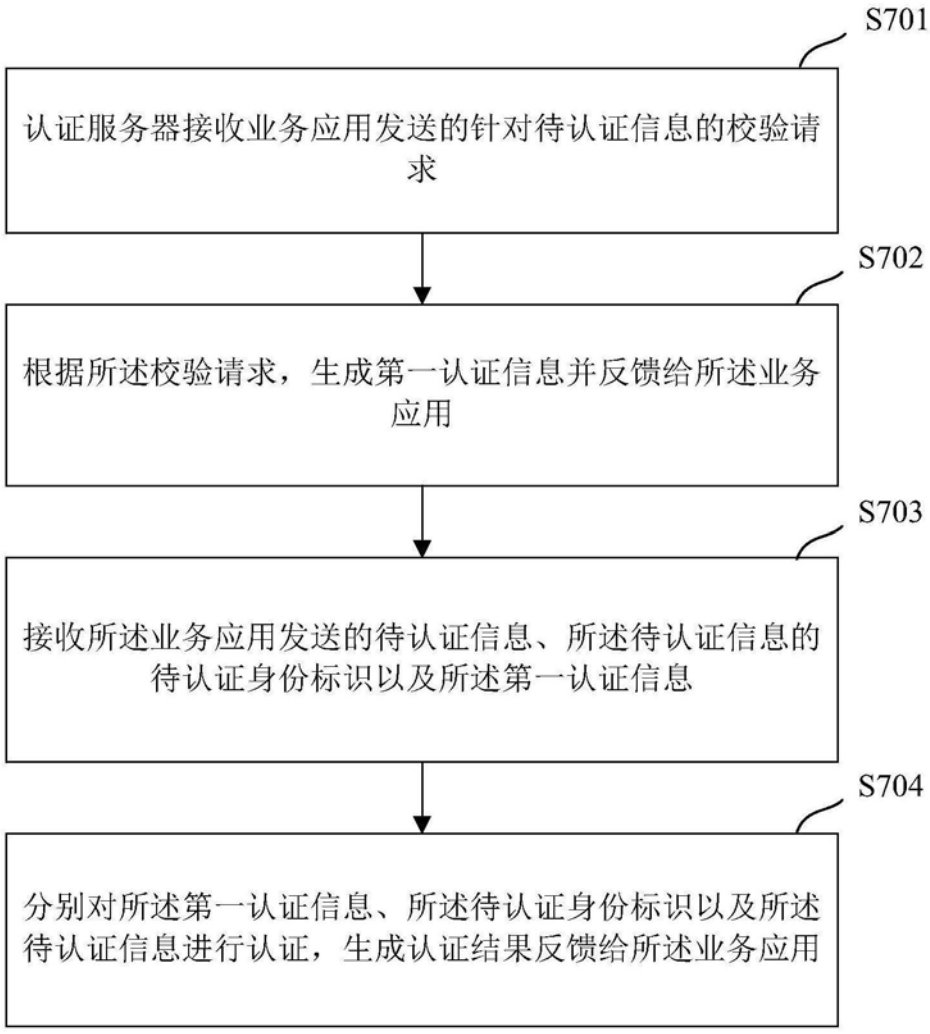

S701
认证服务器接收业务应用发送的针对待认证信息的校验请求
S702
根据所述校验请求，生成第一认证信息并反馈给所述业务应用
S703
接收所述业务应用发送的待认证信息、所述待认证信息的待认证身份标识以及所述第一认证信息
S704
分别对所述第一认证信息、所述待认证身份标识以及所述待认证信息进行认证，生成认证结果反馈给所述业务应用

图7

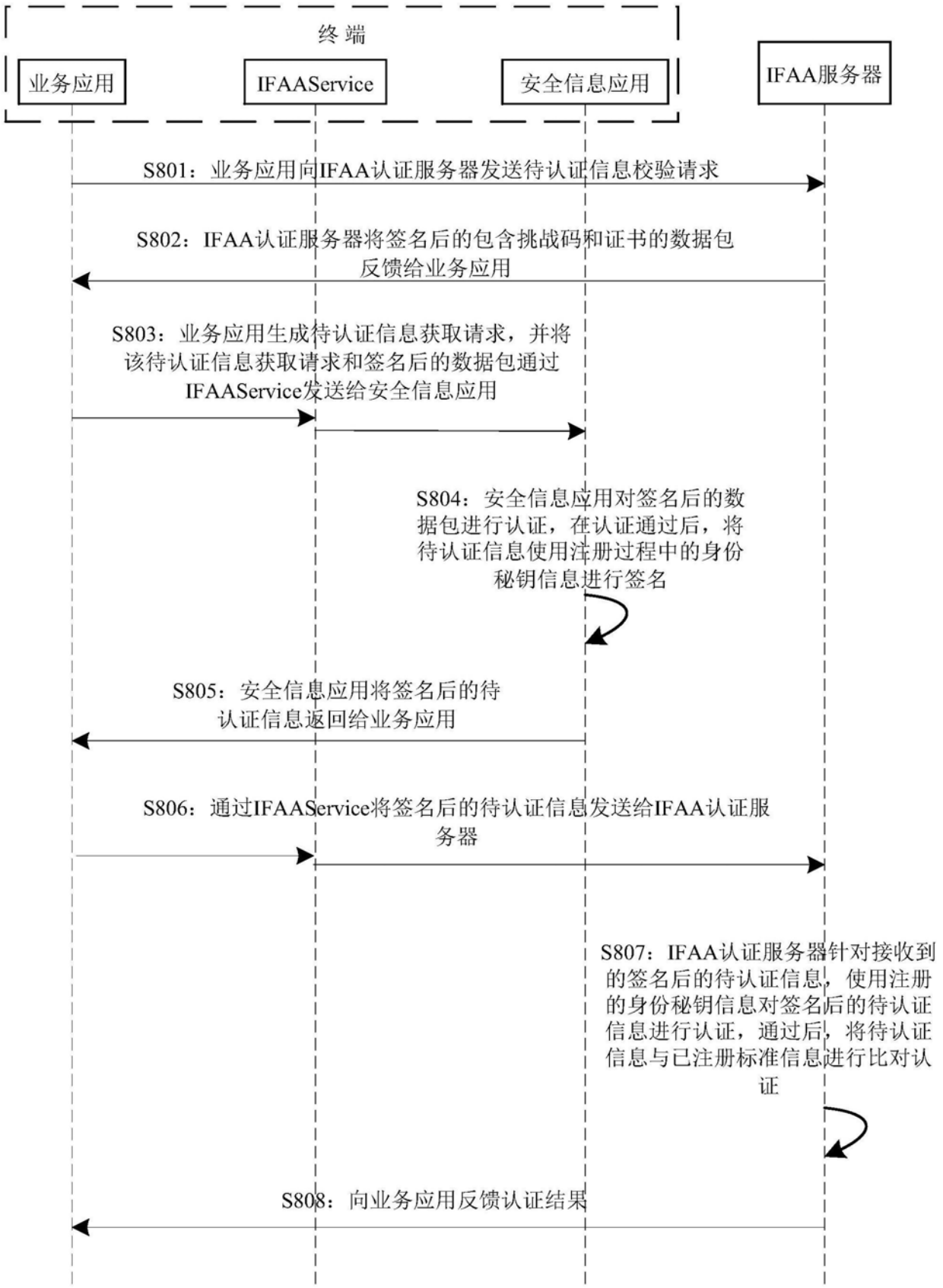

终端
业务应用
IFAAService
安全信息应用
IFAA服务器
S801：业务应用向IFAA认证服务器发送待认证信息校验请求
S802：IFAA认证服务器将签名后的包含挑战码和证书的数据包反馈给业务应用
S803：业务应用生成待认证信息获取请求，并将该待认证信息获取请求和签名后的数据包通过IFAAService发送给安全信息应用
S804：安全信息应用对签名后的数据包进行认证，在认证通过后，将待认证信息使用注册过程中的身份秘钥信息进行签名
S805：安全信息应用将签名后的待认证信息返回给业务应用
S806：通过IFAAService将签名后的待认证信息发送给IFAA认证服务器
S807：IFAA认证服务器针对接收到的签名后的待认证信息，使用注册的身份秘钥信息对签名后的待认证信息进行认证，通过后，将待认证信息与已注册标准信息进行比对认证
S808：向业务应用反馈认证结果

图8

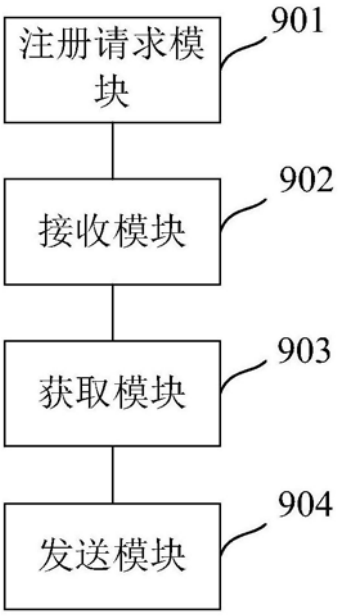


图9

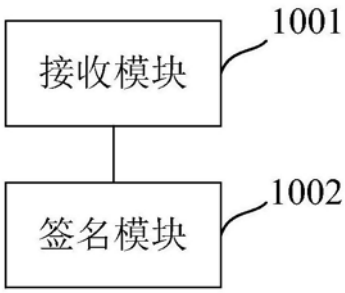


图10

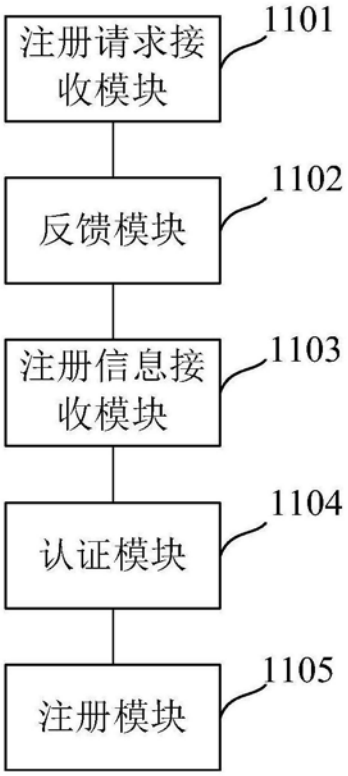

注册请求接收模块
1101
反馈模块
1102
注册信息接收模块
1103
认证模块
1104
注册模块
1105

图11

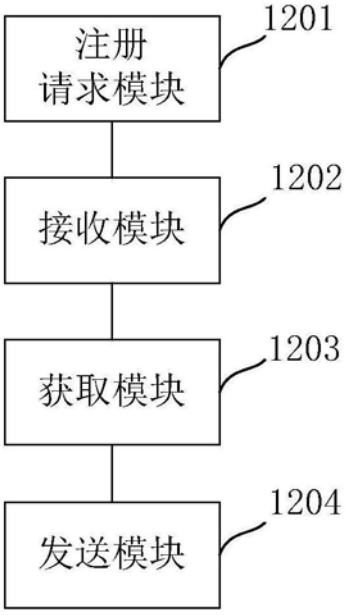

注册请求模块
1201
接收模块
1202
获取模块
1203
发送模块
1204

图12

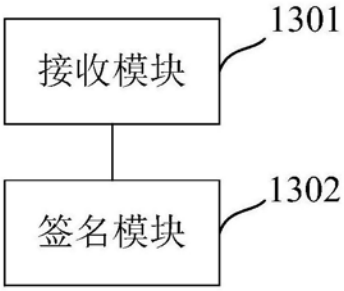

接收模块
1301
签名模块
1302

图13

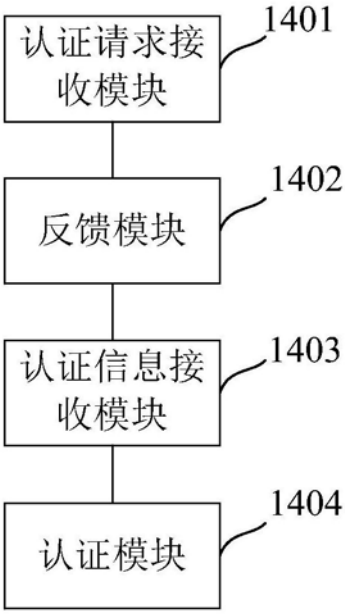

认证请求接收模块
1401
反馈模块
1402
认证信息接收模块
1403
认证模块
1404

图14