[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32
H04L 29/06

[12] 发明专利申请公开说明书

[21] 申请号 200410048986.6

[43] 公开日 2005 年 2 月 2 日

[11] 公开号 CN 1574741A

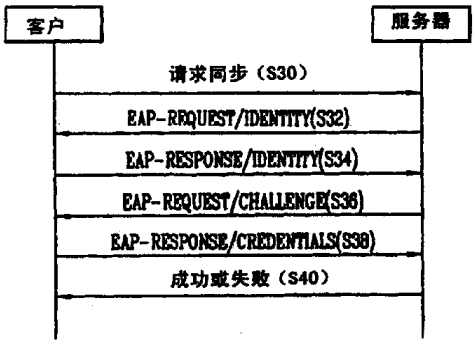
[22] 申请日 2004.6.14
[21] 申请号 200410048986.6
[30] 优先权
[32] 2003.6.14 [33] KR [31] 10-2003-0038545
[71] 申请人 LG 电子株式会社
地址 韩国汉城
[72] 发明人 丘世完
[74] 专利代理机构 上海专利商标事务所
代理人 谢喜堂

权利要求书 3 页 说明书 8 页 附图 7 页

[54] 发明名称 在有线/无线通信系统中使用标记语言的验证方法

[57] 摘要

本发明披露了一种使用标记语言的有线/无线通信系统中客户机和服务器之间的验证方法。通过使用可扩展验证协议(EAP)在可扩展标记语言文件类型定义(XML DTD)中定义多种验证方法种类，并通过使用从所述验证方法种类中随机选择的一个验证方法种类在客户机和服务器之间执行验证进程。由此，可以更强更安全地执行验证。



ISSN1008-4274

1．一种在有线/无线通信系统中使用标记语言的验证方法，它在用于声明所述标记语言结构的文件类型定义（DTD）中声明各种验证方法种类，并从所述声明的验证方法种类中动态地选择客户机和服务器之间的验证方法种类。

2．如权利要求 1 所述的方法，其特征在于，所述各种验证方法种类包括基于身份/密码的验证方法、基于 MD5 的验证方法、基于 OTP（一次性密码）的验证方法、基于标记卡的验证方法以及使用 TLS（传输层安全）的基于证书的验证方法。

3．如权利要求 1 所述的方法，其特征在于，所述各种验证方法种类通过使用可扩展验证协议（EAP）来声明。

4．如权利要求 1 所述的方法，其特征在于，所述客户机和服务器在开始所述验证过程之前识别出相同的可用验证方法种类。

5．如权利要求 1 所述的方法，其特征在于，当所述客户机发送接入请求时，所述服务器随机地选择所述验证方法种类之一，并依照所述随机选择的验证方法种类向所述客户机请求安全信息。

6．如权利要求 5 所述的方法，其特征在于，所述服务器向所述客户机发送包括所述随机选择的验证方法种类以及依照所述验证方法种类的对安全信息的请求的请求消息。

7．如权利要求 6 所述的方法，其特征在于，当所述客户机接收所述请求消息时，所述客户机从所述请求消息检测所述验证方法种类以及所述对安全信息的请求，并依照所述验证方法种类向所述服务器发送所述安全信息作为响应。

8．如权利要求 7 所述的方法，其特征在于，所述验证方法种类通过检测来自所述请求消息的<EAP>元素以及检测所述<EAP>元素的<EAPData>元素的<DataKind>元素的信息来检测。

9．如权利要求 7 所述的方法，其特征在于，所述请求消息还包括一随机值。

10．如权利要求 9 所述的方法，其特征在于，所述验证方法种类的响应包括通过处理所述随机值所得的结果值、所述安全信息以及依照所检测的验证方法种类的设定值，并且其中，所述随机值从所述请求消息中检测。

11．如权利要求 10 所述的方法，其特征在于，所述设定值包括另一用于标识所述客户机的值。

12．如权利要求 7 所述的方法，其特征在于，所述服务器从数据库中搜索所述服务器向所述客户机请求的安全信息、依照所述随机选择的验证方法种类来处理搜索到的安全信息并将所处理的值与来自所述客户机的响应相比较，来确定验证成功/失败。

13．一种在有线/无线通信系统中客户机和服务器之间使用标记语言的验证方法，其特征在于，它包括：

识别所述客户机和服务器之间的相同的验证方法种类；

在所述服务器端通过使用所述相同的验证方法种类的一个随机验证方法种类来验证所述客户机；以及

在客户端通过使用所述相同的验证方法种类的另一随机验证方法种类来验证所述服务器。

14．如权利要求 13 所述的方法，其特征在于，所述验证方法种类在用于声明标记语言的文件类型定义（DTD）中使用可扩展验证协议（EAP）来定义。

15．如权利要求 13 所述的方法，其特征在于，所述验证方法种类包括基于身份/密码的验证方法、基于 MD5 的验证方法、基于 OTP（一次性密码）的验证方法、基于标记卡的验证方法以及使用 TLS（传输层安全）的基于证书的验证方法。

16．如权利要求 13 所述的方法，其特征在于，所述一个随机验证方法种类和所述另一随机验证方法种类互不相同。

17．如权利要求 13 所述的方法，其特征在于，所述一个随机验证方法和所述另一随机验证方法彼此相同。

18．一种在有线/无线通信系统中使用标记语言的验证协议，其特征在于，它包括：

可扩展标记语言文件类型定义（XML DTD），用于通过使用可扩展验证协议（EAP）元素来声明各种验证方法种类；以及

验证消息，包括具有所述声明的验证方法种类的一个随机验证方法种类的信息的 EAP 元素。

19．如权利要求 18 所述的验证协议，其特征在于，所述 EAP 元素本质上包括用于指示所述验证消息的种类的<Code>元素以及用于标识所述验证消息的<Identifier>元素，并选择性地包括用于包含所述验证消息的实际数据的<EAPData>元素。

20．如权利要求 19 所述的验证协议，其特征在于所述<EAPData>元素包括用

于指示所述数据的种类的<DataKind>元素以及具有所述随机验证方法种类的信息的信息元素。

在有线/无线通信系统中使用标记语言的验证方法

(1)技术领域

本发明涉及使用标记语言在有线/无线通信系统中的验证，尤其涉及使用同步标记语言（SyncML）的有线/无线通信系统中客户机和服务器之间的验证方法。

(2)背景技术

在有线/无线通信系统中使用标记语言请求客户机与服务器之间的验证接入的情况下，当成功地执行了验证以后，可以保留该接入并继续进行到随后的步骤中。

例如，当由于无线/有线网络和终端中同一数据的出现离散而需要数据同步化时，在需要保留数据同步的客户机和服务器之间要求验证过程。

SyncML 是一种用于数据同步的标准协议，用于 web 门户、蜂窝电话或 PC 的个人信息的同步。此外，SyncML 能够支持对各类应用服务，如 E-mail 和文本备忘录的数据同步功能，以及对个人信息的管理功能。

图 1 说明了在通信系统的数据同步中使用 SyncML 在客户机和服务器之间的一般验证方法。

参考图 1，当通过使用 SyncML 在客户机和服务器之间执行数据同步时，客户机向服务器请求数据同步（S10）。服务器向客户机请求身份和密码（S12）。客户机对其身份和密码进行编码，或通过预定义的算法，如 MD5 对其身份和密码进行压缩并对压缩的身份和密码进行编码，然后向服务器发送已编码的身份和密码（S14）。服务器确认身份和密码，并向客户机通知验证结果（S16）。

当成功地执行了对客户机的验证之后，服务器将其身份和密码发送给客户机由其验证。客户机确认身份和密码，并向服务器通知验证结果。

当成功地完成了双向验证之后，在客户机和服务器之间执行对变化的数据的双向或单向数据同步过程。

使用标记语言的通信系统中的一般验证方法仅能通过使用身份和密码来执行验证。因此，验证进程必须在身份和密码的基础上执行。这里，可能泄漏用于验证的安全信息，导致弱安全性。也可以使用用于补偿验证协议的弱安全性的特殊验证服务器。然而，很难另外安装验证服务器。

(3)发明内容

因此，本发明的目的是提供一种在有线/无线通信系统中使用标记语言的验证方法，能够通过为标记语言中使用的消息配备结构协议以拥有各种验证方法种类，从而可选择客户机和服务器之间不同的验证方法种类。

本发明的另一目的是提供一种在有线/无线通信系统中使用标记语言的验证方法，能够通过动态地选择服务器和客户机之间的验证方法种类，执行强双向验证。

为达到这些和其它优点，依照本发明的目的，如这里所实施并概括描述的，在有线/无线通信系统中提供了一种使用标记语言的验证方法，该方法在用于声明标记语言结构的文件类型定义（DTD）中声明各种验证方法种类，并从所声明的验证方法种类中动态地选择客户机和服务器之间的验证方法种类。

当客户机发送接入请求时，服务器随机地选择验证方法种类之一，并依照随机选择的验证方法种类向客户机请求安全信息。

依照本发明的一个方面，在有线/无线通信系统中使用标记语言的客户机和服务器之间的验证方法包括以下步骤：识别客户机和服务器之间的相同的验证方法种类；通过使用相同的验证方法种类的一个随机验证方法种类在服务器端、客户端进行验证；以及通过使用相同验证方法种类的另一随机验证方法种类在客户端、服务器端进行验证。

一个随机验证方法种类和另一随机验证方法种类是彼此相同或不同的。

依照本发明的另一方面，使用标记语言的有线/无线通信系统中的验证协议包括：用于通过使用可扩展验证协议（EAP）元素来声明各种验证方法种类的可扩展标记语言文件类型定义（XML DTD）；以及包括具有所声明的验证方法种类的一个随机验证方法种类的信息的 EAP 元素的验证消息。

EAP 元素本质上包括用于指示验证消息的种类的<Code>元素以及用于标识验证消息的<Identifier>元素，并选择性地包括用于包含验证消息的实际数据的<EAPData>元素。

<EAPData>元素包括用于指示数据的种类的<DataKind>元素，以及具有随机验证方法种类的信息的信息元素。

结合附图阅读以下本发明的详细描述，可以更清楚本发明的上述以及其它目的、特征、方面和优点。

(4)附图说明

包括的附图提供了对本发明的进一步理解，并结合在本说明书中成为其一部分，说明了本发明的实施例，连同描述一起解释了本发明的原理。

附图中：

图 1 说明了使用标记语言的通信系统的数据同步中客户机和服务器之间的一般验证方法；

图 2 说明了依照本发明的 XML DTD。

图 3 说明了依照本发明的对客户机和服务器之间的可用验证方法的确认方法；

图 4 说明了依照本发明的用于客户机和服务器之间的数据同步的验证方法；

图 5 说明了依照本发明的用于通过使用 EAP 来请求身份的验证消息（例如，EAP-Request/Identity 消息）；

图 6 说明了依照本发明的用于通过使用 EAP 来响应身份的实际值的验证消息（例如，EAP-Response/Identity 消息）；

图 7 说明了依照本发明的用于通过使用 EAP 依照随机验证方法种类来请求安全信息的验证消息（例如，EAP-Request/Challenge 消息）；

图 8 说明了依照本发明的用于通过使用 EAP 依照随机验证方法种类来响应安全信息的验证消息（例如，EAP-Response/Credentials 消息）；以及

图 9 说明了依照本发明的用于通过使用 EAP 来发送验证结果的验证消息。

(5)具体实施方式

现在详细描述本发明的较佳实施例，其示例在附图中说明。

一般而言，通过 在客户机和服务器之间发送/接受基于可扩展标记语言（XML）的消息来执行数据同步，用于数据同步的协议包括表示协议、同步协议和传输协议。同步协议定义用于在客户机和服务器之间交换 SyncML 消息的方法和过程、用于执行同步的方法以及同步类型。传输协议定义使用一般传输协议，如超文本传输协议（HTTP）和无线会话协议（WSP）用于消息传输的绑定规则。

表示协议是用于 SyncML 消息的结构协议，定义了用于同步的可扩展语言文件类型定义（XML DTD）。XML DTD 声明了 XML 文件中使用的标记，定义出文件的逻辑和物理结构。

一般而言，用于组成文件的语言规则必须精确地发送至所有用户，以使得

用户能够识别文件的内容。XML 通过使用 DTD 来阐明语言规则。即，DTD 描述了 XML 文件中使用的元素、元素属性、元素和实体之间的关系。

依照本发明，在 XML DTD 中预先定义了多个验证方法种类，客户机和服务器随机地从所定义的验证方法种类中选择一些验证方法种类。需要设置接入的客户机和服务器比较它们的验证方法种类，并识别相同的验证方法种类。在用于数据同步的双向验证中，客户机和服务器动态地在相同的验证方法种类之中相互建议它们的验证方法种类，因此能更多样化并安全地执行验证过程。

依照本发明，另外定义了一种用于在客户机和服务器之间随机选择并判定验证方法种类的可扩展验证方法的新的 SyncML 模式，来设计 XML DTD，如图 2 所示。

图 2 说明了依照本发明的 XML DTD。XML DTD 以在 IETF RFC 2284 中定义的可扩展验证协议（EAP）包括一种模式，来获取各种验证方法类型。

XML DTD 解释了 SyncML 消息的结构。依照 XML DTD，SyncML 消息包括头元素<SyncHdr>以及本体元素<SyncBody>，头元素<SyncHdr>包括 DTD 版本<VerDTD>、协议版本<VerProto>、消息 ID<MsgID>、<Target>、<Source>、<RespURI>、<NoResp>、<Cred>、<Meta>以及<EAP>元素。这里，<Target>、<Source>、<RespURI>、<NoResp>、<Cred>以及<Meta>元素基本不涉及本发明的 EAP，因此省略了对其的解释。本体元素包括多个用于执行数据同步过程的命令，但也省略了对其的解释。

<EAP>元素主要包括<Code>元素和<Identifier>元素，并选择性地包括<EAPData>元素。用于指示 EAP 消息的种类的<Code>元素包括请求 Request、响应 Response、成功 Success 和失败 Fail 信息。<Identifier>元素是用于标识 EAP 消息的标识符。包含 EAP 消息的实际数据的<EAPData>元素主要包括验证信息。<EAPData>元素包括<Identify>、<Notification>、<Nak>、<MD5Chal>、<OTP>、<TokenCard>和<TLS>元素之一以及<DataKind>元素。

<Identity>元素使用客户机或服务器的身份指示验证方法，<Notification>元素指示必须向另一方通知的注意事项，<Nak>元素意指‘验证不是必须的，不要响应’，<MD5Chal>元素用于通过使用 MD5 压缩算法来请求对询问的响应。<OTP>元素指示使用一次性密码（OTP）算法的验证方法，<TokenCard>元素指示使用经物理输入的信息（令牌），如智能卡输入、光瞳输入以及指纹输入的验证方法，<TLS>元素是 IETF 建议的一种标准，指示用于由传输层提

供编码和证书（如传输控制协议）的验证方法，使数据能够通过安全信道传输，而不修改客户机和服务器的应用程序。即，例如，<TLS>元素指示使用证书的验证方法。

依照本发明，XML DTD 声明了多个验证方法种类，如基于身份/密码的验证方法、基于 MD5 的验证方法、基于 OTP 的验证方法、基于标记卡的验证方法以及使用 TLS（传输层安全）的基于证书的验证方法。

因为 XML DTD 声明了多个验证方法种类，使用 SyncML 的客户机和服务器能够选择性地包括所声明的验证方法种类中预定数量的验证方法种类。

客户机和服务器分别包括验证代理。验证代理通过被建议来声明多个验证方法种类的模式执行基于 SyncML 的 EAP 过程。

每一客户机和每一服务器可具有不同的验证方法种类。因此，在开始数据同步的验证过程之前，相应的客户机和服务器互相通知其验证方法种类，并识别相同的可用验证方法种类。

图 3 说明了依照本发明对客户机和服务器之间的可用验证方法的确认方法。

在客户机和服务器请求数据同步的情况下，客户机向服务器发送其验证方法种类（S20）。客户机从服务器接受服务器的验证方法种类（S22）。

客户机将其验证方法种类与服务器的验证方法种类进行比较，并识别相同的可用验证方法种类（S24）。此外，服务器识别其验证方法种类和客户机的验证方法种类之间的相同的可用验证方法种类。

例如，当客户机的验证方法种类为身份、MD5Chal、OPT 和 TLS，服务器的验证方法种类为身份 Identity、MD5Chal、OTP、令牌卡 TokenCard 和 TLS 时，客户机和服务器确认相同的身份 Identity、MD5Chal、OTP 和 TLS 验证方法种类。

在确认相同的可用验证方法种类之后，客户机和服务器执行用于数据同步的验证过程。

图 4 说明了依照本发明用于使用 SyncML 的通信系统中在客户机和服务器之间进行数据同步的验证方法。

如图 4 所示，客户机向服务器请求数据同步（S30），服务器向客户机请求身份（S32）。客户机基于请求向服务器发送其身份（S34）。为确认客户机实际上拥有身份，服务器随机地选择服务器和客户机之间的相同的可用验证方

法种类之一，并依照所选择的验证方法种类向客户机请求身份的安全信息（S36）。客户机依照所选择的验证方法种类向服务器发送其身份的安全信息（S38）。当来自客户机的安全信息为正常安全信息时，服务器判定依照随机选择的验证方法种类成功地执行了验证，并向客户机发送成功信息（S40）。

服务器也能够向客户机请求验证，使用同一种方式执行。因此，不再详细解释。

现在详细描述服务器的客户机验证方法。

首先，客户机试图接入服务器来请求数据同步。即，客户机生成数据同步请求消息 Request Sync，并通过 TCP/IP 向服务器发送生成的消息 Request Sync（S30）。

为使用本发明的 EAP，如图 5 所示，服务器利用<EAP>元素及其子元素生成第一 EAP 请求消息 EAP-Request/Identity，用于请求身份。第一 EAP 请求消息 EAP-Request/Identity 包括用于指示请求的<Code>元素、用于指示‘1’的<Identifier>元素以及作为<EAP>元素的子元素的<EAPData>元素。<EATData>元素包括用于依照所选择的方法来指示身份的<DataKind>元素以及用于指示客户机将向用户显示的数据的<Data>元素。服务器向客户机发送第一 EAP 请求消息 EAP-Request/Identity（S32）。

客户机分析第一 EAP 请求消息 EAP-Reauest/Identity。当客户机检测到<EAP>元素，客户机识别出是通过使用 EAP 执行验证进程，还识别出第一 EAP 请求消息 EAP-Request/Identity 是用于基于<EAP>元素的<Code>元素和<DataKind>元素来请求身份的验证消息，并生成如图 6 所示的第一 EAP 响应消息 EAP-Response/Identity。即，客户机在第一 EAP 响应消息 EAP-Response/Identity 的<EAP>元素的<Code>元素上记录用于指示响应的‘Response’，并在<EAPData>元素的<DataKind>上记录‘Identity’。当客户机的身份为‘Hong’时，客户机也在<Identity>元素上记录‘Hong’。客户机向服务器发送第一 EAP 响应消息 EAP-Response/Identity（S34）。

服务器分析第一 EAP 响应消息 EAP-Response/Identity。服务器识别出：拥有‘Hong’身份的客户机等候基于第一 EAP 响应消息 EAP-Response/Identity 的<EAP>元素的<Code>Response</Code>、<DataKind>Identity</DataKind>和<Identity>Hong</Identity>来验证。因此，服务器随机地选择可用验证方法种类之一，并依照所选择的验证方法种类向客户机请求身份的安全信息，以便确认

客户机实际上拥有‘Hong’的身份，由此执行实际的验证进程。

即，当由服务器从可用验证方法种类中随机选择的验证方法种类为‘MD5Chal’时，如图 7 所示，服务器在<EAP>元素的<Code>元素上记录‘Request’，在<EAPData>元素的<DataKind>元素上记录‘MD5Chal’，在<MD5Chal>元素上记录随机值‘90384029304802039480230’，并在<Data>元素上记录‘What's your password?’（你的密码是什么），由此生成第二 EAP 请求消息 EAP-Request/challenge。在从可用验证方法种类中随机选择的验证方法种类为‘OTP’的情况下，服务器包括<DataKind>OTP</DataKind>以及<OTP>x</OTP>，由此生成第二 EAP 请求消息 EAP-Request/challenge。服务器向客户机发送第二 EAP 请求消息 EAP-Request/challenge（S36）。

客户机接受第二 EAP 请求消息 EAP-Request/challenge，基于<EAP>元素的<DataKind>MD5Chal</DataKind> 和<MD5Chal>90384029304802039480230</MD5Chal>识别客户机必须通过使用 MD5 压缩算法以记录在<MD5Chal>元素上的随机值向服务器响应其身份的密码（安全信息）。

客户机通过 MD5 压缩算法利用其身份的密码（安全信息）和记录在<MD5Chal>元素上的随机值来计算响应值，如以下公式 1 所示：

MD5（随机值＋密码＋α）－－－－－－－－－公式 1

这里，α表示用于标识身份的预设值，如常驻注册数（resident registration number）。

即，客户机通过 MD5 压缩算法压缩随机值、其密码和α。压缩结果值（响应值）总是具有预定的位（如 128 位），且不从结果值获取输入值。MD5 是一种不可逆函数。因此，如果压缩结果值（响应值）泄漏，也无法推算出密码。

在<DataKind>OTP</DataKind>和<OTP>x</OTP>记录在第二 EAP 请求消息 EAP-Request/challenge 的<EAP>元素上的情况下，客户机通过使用接收到的‘x’和其密码准备响应值。

客户机生成 第二 EAP 响应消息 EAP-Response/Credentials 以具备如图 8 所示的响应值，并向服务器发送第二 EAP 响应消息 EAP-Response/Credentials（S38）。在图 8 的第二 EAP 响应消息 EAP-Response/Credentials 中，记录为<MD5Chal>元素的值的‘slkdjflsldjfljsldjkfljlsdjkftuir’表示响应值。

服务器接受第二 EAP 响应消息 EAP-Response/Credentials，从用户注册数

据库中搜索相应的身份的密码。服务器以与上述公式 1 相同的方式压缩搜索到的密码和从服务器发送到客户机的作为询问的随机值。服务器将通过压缩计算所得的值与来自客户机的响应值相比较。当计算所得的值与响应值相同时，服务器判定依照随机选择的验证方法种类成功地执行了验证，并且当计算所得的值与响应值不同时，服务器判定验证失败。如图 9 所描述的，服务器通过在<EAP>元素的<Code>元素上记录验证结果来生成验证结果消息，并向客户机发送验证结果消息（S40）。

客户机接受图 9 的验证结果消息，识别出是基于<Code>Success</Code>成功地执行了验证。验证结果消息不需要<EAPData>元素。

如先前所讨论的，依照本发明，在 XML DTD 中定义了多种验证方法种类，因此可以在使用标记语言的客户机和服务器之间自由地选择验证方法种类。

此外，能够在客户机和服务器之间动态地选择验证方法种类，得到强双向验证。

鉴于本发明可以在不脱离其精神和本质特征的情况下实施，也应当理解，上述实施例不受前述的描述的细节限制，除非另外指明，而应当在所附权利要求书中定义的精神和范围之内概括描述，并且因此，所有处于权利要求书的边界和范围，或这类边界和范围的等效技术方案之内的变化和修改都包含在所附权利要求书之内。

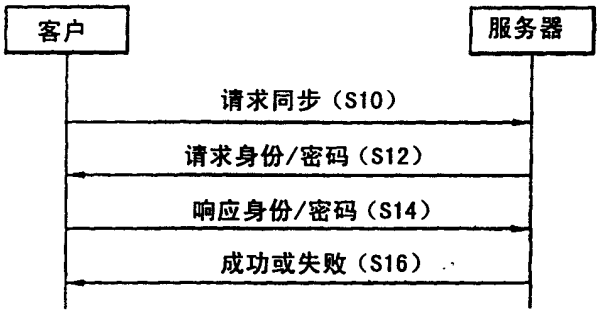


图 1

相关技术

```
<!ELEMENT SyncML (SyncHdr, SyncBody)>
<!ELEMENT SyncHdr (VerDTD, VerProto, SessionID, MsgID, Target, Source, RespURI?,
NoResp?, Cred?, Meta?, EAP?>

...

<!ELEMENT EAP (Code, Identifier, EAPData?>
<!ELEMENT Code(#PCDATA)>
<!ELEMENT Identifier(#PCDATA)>
<!ELEMENT EAPData(DataKind, (Identity|Notification|Nak|MD5Chal|OTP|TokenCard,
TLS)?, Data)>
<!ELEMENT DataKind(#PCDATA)>
<!ELEMENT Identity(#PCDATA)>
<!ELEMENT Notificatin(#PCDATA)>
<!ELEMENT Nak(#PCDATA)>
<!ELEMENT MD5Chal(#PCDATA)>
<!ELEMENT OTP(#PCDATA)>
<!ELEMENT TokenCard(#PCDATA)>
<!ELEMENT TLS(#PCDATA)>
<!ELEMENT Data(#PCDATA)>
...
```

图 2

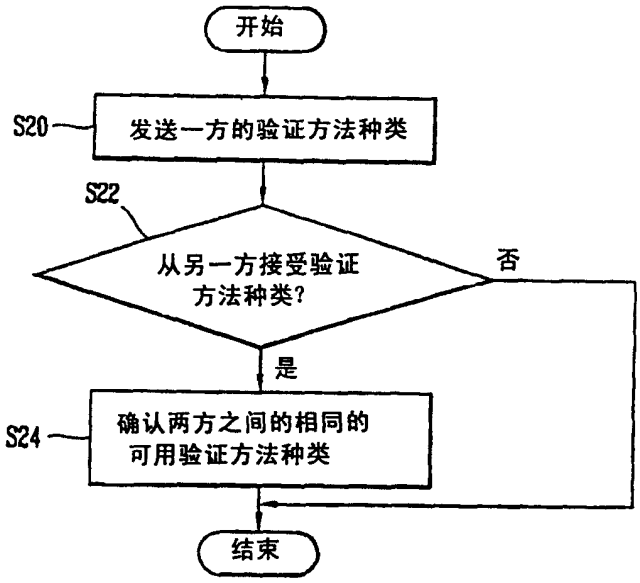

开始
S20
发送一方的验证方法种类
S22
从另一方接受验证方法种类?
否
是
S24
确认两方之间的相同的可用验证方法种类
结束

图 3

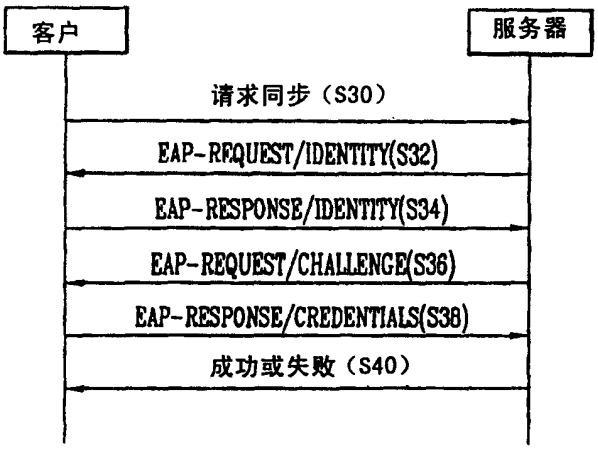

客户
服务器
请求同步（S30）
EAP-REQUEST/IDENTITY(S32)
EAP-RESPONSE/IDENTITY(S34)
EAP-REQUEST/CHALLENGE(S36)
EAP-RESPONSE/CREDENTIALS(S38)
成功或失败（S40）

图 4

```
<SyncML>
 <SyncHdr>
   <VerDTD>1.1</VerDTD>
   <VerProto>SyncML/1.1</VerProto>
   <SessionID>1</SessionID>
   <MsgID>1</MsgID>
   <Target>
     <LocURI>http://www.syncml.org/sync-server</LocURI>
   </Target>
   ...
   <EAP>
     <Code>Request</Code>
     <Identifier>1</Identifier>
     <EAPData>
       <DataKind>Identity</DataKind>
       <Data>What's your identity ?</Data>
     </EAPData>
   </EAP>
 </SyncHdr>
 <SyncBody>
 ...
 </SyncBody>
</SyncML>
```

图 5

```
<SyncML>
 <SyncHdr>
   <VerDTD>1.1</VerDTD>
   <VerProto>SyncML/1.1</VerProto>
   <SessionID>1</SessionID>
   <MsgID>2</MsgID>
   <Target>
     <LocURI>http://www.syncml.org/sync-server</LocURI>
   </Target>
   ...
   <EAP>
     <Code>Response</Code>
     <Identifier>2</Identifier>
     <EAPData>
       <DataKind>Identity</DataKind>
       <Identity>Hong</Identity>
     </EAPData>
   </EAP>
 </SyncHdr>
 <SyncBody>
 ...
 </SyncBody>
</SyncML>
```

图 6

```
<SyncML>
 <SyncHdr>
   <VerDTD>1.1</VerDTD>
   <VerProto>SyncML/1.1</VerProto>
   <SessionID>1</SessionID>
   <MsgID>3</MsgID>
   <Target>
     <LocURI>http://www.syncml.org/sync-server</LocURI>
   </Target>
   ...
   <EAP>
     <Code>Request</Code>
     <Identifier>3</Identifier>
     <EAPData>
       <DataKind>MD5Chal</DataKind>
       <MD5Chal>90384029304802039480230</MD5Chal>
       <Data>What's your password ?</Data>
     </EAPData>
   </EAP>
 </SyncHdr>
 <SyncBody>
 ...
 </SyncBody>
</SyncML>
```

图 7

```
<SyncML>
 <SyncHdr>
   <VerDTD>1.1</VerDTD>
   <VerProto>SyncML/1.1</VerProto>
   <SessionID>1</SessionID>
   <MsgID>4</MsgID>
   <Target>
     <LocURI>http://www.syncml.org/sync-server</LocURI>
   </Target>
   ...
   <EAP>
     <Code>Response</Code>
     <Identifier>4</Identifier>
     <EAPData>
       <DataKind>MD5Chal</DataKind>
       <MD5Chal>alkdjflsldjfljsldjkfljlsdjkftuir</MD5Chal>
     </EAPData>
   </EAP>
 </SyncHdr>
 <SyncBody>
 ...
 </SyncBody>
</SyncML>
```

图 8

```
<SyncML>
 <SyncHdr>
   <VerDTD>1.1</VerDTD>
   <VerProto>SyncML/1.1</VerProto>
   <SessionID>1</SessionID>
   <MsgID>5</MsgID>
   <Target>
     <LocURI>http://www.syncml.org/sync-server</LocURI>
   </Target>
   ...
   <EAP>
     <Code>Success</Code>
     <Identifier>5</Identifier>
   </EAP>
 </SyncHdr>
 <SyncBody>
 ...
 </SyncBody>
</SyncML>
```

图 9