

(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  
2007年9月20日 (20.09.2007)

PCT

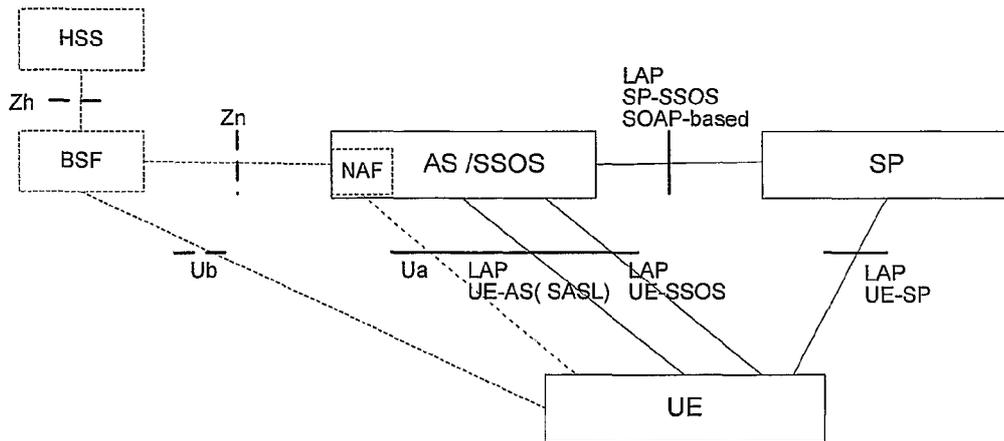
(10) 国际公布号  
WO 2007/104245 A1

- (51) 国际专利分类号:  
H04L 9/00 (2006.01)
- (21) 国际申请号: PCT/CN2007/000762
- (22) 国际申请日: 2007年3月9日 (09.03.2007)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:  
200610034493.6  
2006年3月16日 (16.03.2006) CN
- (71) 申请人 (对除美国外的所有指定国): 华为技术有限公司(HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人; 及
- (75) 发明人/申请人 (仅对美国): 何承东(HE, Chengdong) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (74) 代理人: 北京集佳知识产权代理有限公司(UNITALEN ATTORNEYS AT LAW); 中国北京市朝阳区建国门外大街22号赛特广场7层, Beijing 100004 (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, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

[见续页]

(54) Title: AN IDENTITY WEB SERVICE FRAMEWORK SYSTEM AND AUTHENTICATION METHOD THEREOF

(54) 发明名称: 一种身份标识网页业务网系统及其鉴权方法



(57) Abstract: An identity Web Service Framework (ID-WSF) system includes HSS, BSF, Network Application Function/Authentication Service/Single-Sign-On Service Entity, SP and UE. An authentication method includes steps: the communication process between UE and SP includes the GBA authentication process and the ID-WSF authentication process; during the GBA authentication process, Bootstrapping Service Function Entity generates a bootstrapping transaction identifier and the period of validity of root key, sends it to UE, and both Bootstrapping Service Function and UE generate the root key; during the ID-WSF authentication process, AS Entity or AS Module generates credentials which the user equipment needs to access SSOS Entity or SSOS Module; Single-Sign-On Service Entity or Single-Sign-On Service Module generates authentication assertion and sends it to UE, or Single-Sign-On Service Entity or Single-Sign-On Service Module generates authentication assertion and the corresponding Artifact of it, saves the corresponding relation table of authentication assertion and its Artifact, and sends the Artifact of authentication assertion to UE.

[见续页]



WO 2007/104245 A1



(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, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告。

所引用双字母代码及其它缩写符号, 请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

(57) 摘要:

本发明公开了一种身份标识网页业务网系统及其鉴权方法。身份标识网页业务网系统包括 HSS、BSF、网络业务应用功能/鉴权服务/单点认证业务实体、SP、UE。鉴权方法包括步骤: UE 和 SP 的通信过程中包括 GBA 鉴权过程和 ID-WSF 鉴权过程, 在 GBA 鉴权过程中, 引导服务功能实体生成引导事务标识、根密钥有效期, 并且发送给 UE, 引导服务功能实体和 UE 都生成根密钥; 在 ID-WSF 鉴权过程中, AS 实体或 AS 模块生成用户终端访问 SSOS 实体或 SSOS 模块所需要的信任状; 单点认证业务实体或单点认证业务模块生成鉴权申明并发送给 UE, 或者单点认证业务实体或单点认证业务模块生成鉴权申明及相应的鉴权申明链接, 保存鉴权申明和鉴权申明链接的对应关系表, 将鉴权申明链接发送给 UE。

## 一种身份标识网页业务网系统及其鉴权方法

本申请要求于 2006 年 3 月 16 日提交中国专利局、申请号为 200610034493.6、发明名称为“一种身份标识网页业务网系统及其鉴权方法”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

### 技术领域

本发明涉及互联网技术领域和下一代网络(NGN, Next Generation Networks)技术领域以及第三代合作伙伴计划(3GPP, The Third Generation Partnership Project)技术领域，具体涉及一种身份标识网页业务网系统(ID-WSF, Identity Web Service Framework)及其鉴权方法。

### 背景技术

如图 1 所示，3GPP 定义了一种通用鉴权架构(GBA, Generic Bootstrapping Architecture)，其通常由 IP 多媒体业务子系统(IMS, IP Multimedia Core Network Subsystem)用户终端(UE, User Equipment)、引导服务功能实体(BSF, Bootstrapping Server Function)、用户归属网络服务器(HSS, Home Subscriber Server)、用户定位功能实体(SLF, Subscriber Locator Function)和网络业务应用功能实体(NAF, Network Application Function)组成。UE 与 BSF 通过 Ub 接口连接，UE 与 NAF 通过 Ua 接口连接，BSF 与 HSS 通过 Zh 接口连接，BSF 与 NAF 通过 Zn 接口连接，BSF 与 SLF 通过 Dz 接口连接。BSF 用于与 UE 执行引导过程(bootstrapping) 时进行互验证身份，同时生成 BSF 与用户的共享密钥 Ks；HSS 中存储用于描述用户信息的签约文件，同时 HSS 还兼有产生鉴权信息的功能；SLF 用于当存在多个 HSS 时，协助 BSF 查找相应的 HSS；NAF 用于为 UE 提供网络业务。

在 Ub 接口中，UE 执行引导过程(bootstrapping)的流程如图 2 所示，说明如下：

步骤 1: UE 需要使用某种业务时，如果知道该业务需要到 BSF 进行相互鉴权过程，则直接发送鉴权请求到 BSF 进行相互鉴权。否则，UE 会首先和该业务对应的 NAF 联系，如果该 NAF 使用 GBA 通用鉴权架构，

并且发现该 UE 还未到 BSF 进行互认证过程, NAF 则通知该 UE 到 BSF 进行互鉴权以验证身份, 然后 UE 再发送鉴权请求到 BSF 进行相互鉴权;

步骤 2: BSF 接到 UE 的鉴权请求后, 首先到 HSS 获取该 UE 的鉴权矢量五元组 (AUTN, RAND, IK, CK, XRES);

步骤 3~步骤 6: BSF 采用 HTTP digest AKA 协议与 UE 进行双向认证以及密钥协商, 完成 UE 和 BSF 之间身份的互相认证;

步骤 7: BSF 生成共享根密钥  $K_s$ , BSF 还为共享密钥  $K_s$  定义了一个有效期限, 以便对  $K_s$  进行定期更新;

步骤 8: BSF 分配一个引导事务标识(B-TID, bootstrapping transaction identifier), 用于标识 BSF 和 UE 之间的本次鉴权交互事务; BSF 将该 B-TID 与根密钥  $K_s$ 、UE 的私有用户标识(IMPI, IMS Private identity)相关联, 以便以后 BSF 可以根据该 B-TID 查找出相应的  $K_s$ , 然后 BSF 将引导事务标识和  $K_s$  的有效期限一起明文发送给 UE;

步骤 9: UE 也生成和 BSF 侧相同的共享根密钥  $K_s$ 。

完成上述步骤后, UE 和 BSF 之间就共享了一个根密钥  $K_s$ , 并且 UE 可以利用公式:

$$\begin{aligned} K_{s\_NAF} &= \text{KDF}(K_s, \text{"gba-me"}, \text{RAND}, \text{IMPI}, \text{NAF\_Id}) \text{ 或者} \\ K_{s\_Ext\_NAF} &= \text{KDF}(K_s, \text{"gba-me"}, \text{RAND}, \text{IMPI}, \text{NAF\_Id}), \\ K_{s\_Int\_NAF} &= \text{KDF}(K_s, \text{"gba-u"}, \text{RAND}, \text{IMPI}, \text{NAF\_Id}), \end{aligned}$$

推导出与想要访问的 NAF 之间的衍生的共享密钥  $K_{s\_Ext/Int\_NAF}$ , 其中 NAF\_Id 是由要访问的 NAF 以及 Ua 接口上的协议标识(UaID)连接而成, RAND 是一个随机数, IMPI 是 UE 的私有用户标识, "gba-me"和 "gba-u"代表字符串, KDF 是密钥导出函数的缩写, 这样 UE 侧就获取了该衍生的共享密钥  $K_{s\_Ext/Int\_NAF}$ 。剩下的任务就是 NAF 如何获取该衍生的共享密钥  $K_{s\_Ext/Int\_NAF}$ 。只有 NAF 和 UE 都获取了  $K_{s\_Ext/Int\_NAF}$ , 才能建立双方通讯的安全通道。

NAF 获取  $K_{s\_Ext/Int\_NAF}$  的流程如图 3 所示, UE 首先根据上述公式推导出衍生的共享密钥  $K_{s\_Ext/Int\_NAF}$ , 然后执行以下步骤:

步骤 1: B-TID 为用户名,  $K_{s\_Ext/Int\_NAF}$  为口令向 NAF 发送连

接请求，本步骤之前可能会事先建立传输层安全（TLS，TransportLayer Security）链接，以保证 Ua 接口的通讯安全；

步骤 2：NAF 收到 UE 的连接请求后，给 BSF 发出认证请求消息，其中携带引导事务标识 B-TID 和 NAF 主机名即 NAF\_ID；

步骤 3：BSF 上保留有 B-TID、IMPI、Ks、密钥有效期、BSF 与 UE 之间的相互鉴权的开始时间、应用相关的 GBA 用户安全设置(GUSS，GBA User security setting)等信息，如果 BSF 能够根据该 B-TID 查找到相应的 Ks，则完成相应用户的认证，然后 BSF 再使用与用户侧相同的上述公式计算出衍生的共享密钥 Ks\_(Ext/Int)\_NAF，然后在认证响应消息中把 Ks\_(Ext/Int)\_NAF、Ks\_(Ext/Int)\_NAF 的有效期限、BSF 与 UE 之间的相互鉴权的开始时间、以及与其它应用相关的用户安全设置 (USS，User security setting) 信息发给 NAF，一个 GUSS 中可能包含多个 USS。

步骤 4：NAF 收到后，保存这些信息。

步骤 5：NAF 给 UE 返回应用应答。

这样 NAF 和 UE 也就共享了由 Ks 衍生的密钥 Ks\_(Ext/Int)\_NAF，从而这两者在后续的通信中可以进行安全通信。

另外，自由联盟工程 (LAP，Liberty Alliance Project) 组织也定义了一些网络架构和规范，用于实现对 Web 业务的访问，其主要包含三个子网络架构：

身份标识联盟网络架构(ID-FF，Identity Federation Framework)；身份标识网页业务网络架构(ID-WSF，Identity Web Service Framework)；和身份标识业务接口规范(ID-SIS，Identity Services Interface Specifications)。

其中 ID-FF 主要包含身份标识联盟(Identity Federation)功能和单点认证功能(SSO，Single Sign On)。ID-WSF 主要在 ID-FF 的基础上定义一些基于身份标识的 Web 业务架构，以便提供一些简单的、用户可以定制的 Web 业务。ID-SIS 则定义一些与 Web 业务相关的接口规范。ID-FF 的架构如图 4 所示，它主要包含三个实体：UE、身份鉴权提供商实体 (IdP，Identity Provider)、业务提供商实体(SP，Service Provider)。身份标识联盟功能是指 UE 在 IdP 和 SP 上都有自己的身份标识，即用户标识。这些身

份标识可以结成一个联盟。SSO 是指在上述身份标识联盟功能的基础上,只要 UE 在 IdP 上通过了鉴权,就等于同时在所有结成联盟的 SP 上也同时通过了鉴权。

ID-FF 和 GBA 互通架构如图 5 所示,在该架构中 UE 有两种鉴权方式:一种是 UE 在 IdP 上鉴权通过后,IdP 会将该 UE 的鉴权申明(Assertion)直接返回给 UE; UE 再将该 Assertion 发给 SP; SP 通过分析 Assertion 来对 UE 进行鉴权。另一种是 UE 在 IdP 上鉴权通过后,IdP 会将该 UE 的鉴权申明链接(Artifact)返回给 UE; UE 再将该 Artifact 发给 SP; SP 再将该 Artifact 通过 SOAP 协议发给 IdP; IdP 根据该 Artifact 查询相应的 Assertion, 并返回给 SP; 最后 SP 通过分析 Assertion 来对 UE 进行鉴权。

ID-WSF 的架构如图 6 所示,其主要包含如下几个实体: UE、IdP、SP、用于使用 Web 业务的 Web 业务消费者实体(WSC, Web Service Consumer)、用于提供 Web 业务的 Web 业务提供者实体(WSP, Web Service Provider)、发现业务实体(DS, Discover Service)。

这些实体配合工作的过程如下:首先 WSP 在 DS 上注册其所能够提供的 Web 业务类型;当 UE 访问 WSC 时, WSC 到 DS 上去查询可访问的 WSP; DS 匹配相关的 WSP 地址,并提供给 WSC;然后 WSC 即可代表 UE 访问相关的 WSP。WSC 和 WSP(或者 SP)的功能是相对的,也就是说 WSC 在作为某个 WEB 业务消费者的同时,也可以作为另外一个 Web 业务提供者(WSP 或者 SP)。WSP 或者 SP 在作为某个 Web 业务提供者的同时,也可以另外一个 WEB 业务消费者(WSC)。

上述架构的进一步简化形式如图 7 所示,其中 WSC 的功能在 UE 上实现,并且某个 WSP 可以提供认证业务实体(AS, Authentication Service)的功能。这里 ID-WSF 中的 AS 功能与 ID-FF 中的 IdP 功能相当,用于完成身份标识 Web 业务网鉴权功能。由于图 7 主要涉及 ID-WSF 的鉴权事务,因此略去 DS。

图 8 介绍了增加单点认证业务实体(SSOS, Single-Sign-On Service)的 ID-WSF 的网络架构,其主要的工作流程如下:首先 UE 和 AS 通过 SASL 协议交互,完成 AS 鉴权;鉴权通过后 AS 给 UE 返回 SSOS 的地址以及

访问 SSOS 所需要的信任状(Credentials); UE 利用从 AS 获取的 Credentials 访问 SSOS, 进行 SSOS 鉴权, SSOS 对 UE 鉴权成功后给 UE 返回相应的 Assertion; UE 利用该 Assertion 去访问相关的 SP。

从上面的介绍可以看出, 一方面, 通用鉴权架构中 UE 与 BSF 交互获取根密钥 Ks 和 B-TID 以后, 都需要分别以 B-TID 为用户名, Ks\_(Ext/Int)\_NAF 为口令在各个 NAF 上鉴权, 以便访问各个 NAF。这种频繁认证增强了安全性, 但增加了终端操作的复杂性和不方便性。

另一方面, 身份标识网页业务网络架构中通过单点认证功能在各个 SP 与 SSOS 之间建立身份标识安全联盟, 并组成一个安全信任圈, 只要在 SSOS 上通过了鉴权, 就等于在 SSOS 所属的安全信任圈内的所有 SP 上也通过了鉴权。

如图 9 所示, 现有技术给出了一种当 AS 和 SSOS 为不同的实体时的 GBA 和 ID-WSF 互通的网络架构, 但是并没有给出任何相应的鉴权方法。因此, 现有技术中虽然存在一种互通网络架构, 但没有实现这两种网络架构之间互通的方法, 致使该互通网络架构不能被实际应用。而 ID-WSF 通信的安全性不够高, 通用鉴权架构用户终端操作也不够简便, 因此对扩展用户终端的应用场景, 方便用户终端应用已有的多种多样的 WEB 业务造成诸多限制。

## 发明内容

本发明要解决的技术问题是使 GBA 和 ID-WSF 能够实现互通, 因而本发明一个目的是提供一种身份标识网页业务网系统及其鉴权方法。

本发明采用如下的技术方案:

一种身份标识网页业务网系统, 包括通用鉴权架构的用户归属网络服务器和引导服务功能实体、业务提供商实体、用户终端, 用户归属网络服务器和引导服务功能实体之间通过 Zh 接口进行通信, 引导服务功能实体与用户终端之间通过 Ub 接口进行通信, 其特征在于: 包括网络业务应用功能/鉴权服务/单点认证业务实体, 其包括网络业务应用功能模块、鉴权服务模块、单点认证业务模块, 网络业务应用功能模块用于提供网络业务应用功能实体功能, 鉴权服务模块用于提供鉴权服务实体功能,

单点认证业务模块用于提供单点认证业务实体功能，网络业务应用功能模块与引导服务功能实体之间通过 Zn 接口进行通信，网络业务应用功能模块与用户终端之间通过 Ua 接口进行通信。

所述的身份标识网页业务网系统，其中：单点认证业务模块与用户终端采用安全申明标记语言描述的单点认证和身份标识联盟协议进行两者之间的通信，采用简单对象访问协议或超文本传输协议封装通信消息；鉴权服务模块与用户终端采用简单鉴权和安全层协议进行两者之间的通信，采用简单对象访问协议或超文本传输协议封装通信消息；单点认证业务模块与业务提供商实体之间进行通信时，采用简单对象访问协议封装通信消息；用户终端与业务提供商实体之间进行通信时，采用简单对象访问协议或超文本传输协议封装通信消息。

一种身份标识网页业务网系统鉴权方法，包括步骤：身份标识网页业务网系统的用户终端和业务提供商实体的通信过程中包括两种鉴权过程，分别是通用鉴权架构鉴权过程和身份标识网页业务网络架构鉴权过程，在通用鉴权架构鉴权过程中，引导服务功能实体生成引导事务标识、根密钥有效期，并且发送给用户终端，引导服务功能实体和用户终端都生成根密钥；在身份标识网页业务网络架构鉴权过程中，鉴权服务实体或鉴权服务模块生成用户终端访问单点认证业务实体或单点认证业务模块所需要的信任状；单点认证业务实体或单点认证业务模块生成鉴权申明并发送给用户终端，或者单点认证业务实体或单点认证业务模块生成鉴权申明及相应的鉴权申明链接，保存鉴权申明和鉴权申明链接的对应关系表，将鉴权申明链接发送给用户终端。

所述的身份标识网页业务网系统鉴权方法，其中包括步骤：用户终端向相应的鉴权服务实体或鉴权服务模块发送身份标识网页业务网络架构鉴权请求消息，鉴权服务实体或鉴权服务模块向用户终端发送要求其进行通用鉴权架构鉴权的挑战响应消息，引导服务功能实体对用户终端进行通用鉴权架构鉴权，鉴权成功后向用户终端发送通用鉴权架构鉴权成功响应消息，该鉴权成功响应消息中包含引导事务标识和根密钥有效期；用户终端向鉴权服务实体或鉴权服务模块发送应用请求消息，鉴权

服务实体或鉴权服务模块根据该应用请求消息对用户终端进行鉴权，鉴权通过后，向用户终端发送响应消息，其中包含单点认证业务实体或单点认证业务模块的地址和信任状。

所述的身份标识网页业务网系统鉴权方法，其中包括步骤：单点认证业务实体或单点认证业务模块对用户终端进行身份标识网页业务网络架构鉴权，鉴权成功后向用户终端发送身份标识网页业务网络架构鉴权成功响应消息，该鉴权成功响应消息中包含鉴权申明。

所述的身份标识网页业务网系统鉴权方法，其中包括步骤：单点认证业务实体或单点认证业务模块对用户终端进行身份标识网页业务网络架构鉴权，生成鉴权申明及相应的鉴权申明链接，保存鉴权申明和鉴权申明链接的对应关系表，在随后发送给用户终端的身份标识网页业务网络架构鉴权成功响应消息中包含鉴权申明链接。

所述的身份标识网页业务网系统鉴权方法，其中包括步骤：

A1、用户终端向业务提供商实体发送应用请求消息；

A2、业务提供商实体收到该应用请求消息后，首先获取鉴权服务实体或鉴权服务模块的地址，然后发送响应消息给用户终端，其中携带鉴权请求头域；

A3、用户终端向鉴权服务实体或鉴权服务模块发送应用请求消息，其中包含简单鉴权和安全层协议请求头域，其包含鉴权机制头域，鉴权机制头域中包含用户终端支持的鉴权方式列表；

A4、鉴权服务实体或鉴权服务模块给用户终端发送挑战响应消息，其中包含简单鉴权和安全层协议响应头域，其包含服务器鉴权机制头域和挑战头域，服务器鉴权机制头域中记录鉴权服务实体或鉴权服务模块选择的鉴权方式。

A5、用户终端与引导服务功能实体交互，进行通用鉴权架构鉴权；

A6、用户终端向鉴权服务实体或鉴权服务模块发送应用请求消息，其中包含简单鉴权和安全层协议请求头域，简单鉴权和安全层协议请求头域包含挑战响应头域，挑战响应头域包含引导事务标识和鉴权响应摘

要信息;

A7、鉴权服务实体或鉴权服务模块通过 Zn 接口向引导服务功能实体获取共享密钥、用户安全设置、密钥有效期、引导时间等信息,鉴权服务实体或鉴权服务模块根据收到简单鉴权和安全层协议请求头域对用户终端进行鉴权,鉴权通过后,向用户终端发送响应消息,其中包含简单鉴权和安全层协议响应头域,该头域中有单点认证业务实体或单点认证业务模块的地址和信任状。

所述的身份标识网页业务网系统鉴权方法,其中:同时支持通用鉴权架构鉴权和身份标识网页业务网络架构鉴权的用户终端在向鉴权服务实体或鉴权服务模块发送的应用请求消息中设置通用鉴权架构标识,若鉴权服务实体或鉴权服务模块发现此通用鉴权架构标识,则通知用户终端先启动通用鉴权架构鉴权过程,再启动用户身份标识网页业务网络架构鉴权过程,否则通知用户终端只启动用户身份标识网页业务网络架构鉴权过程。

所述的身份标识网页业务网系统鉴权方法,其中:所述步骤 A5 包括步骤:

B1、用户终端向引导服务功能实体发送通用鉴权架构鉴权请求消息,其中包含私有用户标识;

B2、引导服务功能实体收到该通用鉴权架构鉴权请求消息后,从用户归属网络服务器获取用户终端的认证矢量;

B3、引导服务功能实体向用户终端发送挑战消息,其中携带鉴权序号参数和随机参数;

B4、用户终端检查鉴权序号参数有效性并生成期望结果;

B5、用户终端向引导服务功能实体发送消息,其中携带私有用户标识、期望结果;

B6、引导服务功能实体检查期望结果的有效性并生成根密钥;

B7、引导服务功能实体向用户终端发送通用鉴权架构成功响应消息,其中携带引导事务标识和根密钥有效期;

B8、用户终端保存引导事务标识和根密钥有效期,生成并保存根密

钥和共享密钥。

所述的身份标识网页业务网系统鉴权方法，其中包括步骤：

C1、用户终端根据单点认证业务实体或单点认证业务模块的地址向单点认证业务实体或单点认证业务模块发送应用请求消息；

C2、单点认证业务实体或单点认证业务模块根据收到的应用请求消息内容进行鉴权处理，鉴权成功后向用户终端发送成功响应消息，其中包含鉴权申明，鉴权申明中有单点认证业务实体或单点认证业务模块的数字签名；

C3、用户终端向业务提供商实体发送应用请求消息，其中包含鉴权申明；

C4、业务提供商实体处理鉴权申明，验证单点认证业务实体或单点认证业务模块的数字签名，完成对用户终端的鉴权后，向用户终端发送响应消息。

所述的身份标识网页业务网系统鉴权方法，其中包括步骤：

D1、用户终端根据单点认证业务实体或单点认证业务模块的地址向单点认证业务实体或单点认证业务模块发送应用请求消息；

D2、单点认证业务实体或单点认证业务模块根据收到的应用请求消息内容进行鉴权处理，生成鉴权申明和相应的鉴权申明链接，保存鉴权申明、鉴权申明和相应的鉴权申明链接的对应关系，鉴权成功后向用户终端发送成功响应消息，其中包含鉴权申明链接。

D3、用户终端向业务提供商实体发送应用请求消息，其中包含鉴权申明链接；

D4、业务提供商实体向单点认证业务实体或单点认证业务模块发送应用请求消息，其中包含鉴权申明链接；

D5、单点认证业务实体或单点认证业务模块根据鉴权申明链接找到对应的鉴权申明，向业务提供商实体发送响应消息，其中包含鉴权申明，鉴权申明中有单点认证业务实体或单点认证业务模块的数字签名；

D6、业务提供商实体处理鉴权申明，验证单点认证业务实体或单点

认证业务模块的数字签名，完成对用户终端的鉴权后，向用户终端发送响应消息。

所述的身份标识网页业务网系统鉴权方法，其中：简单鉴权和安全层协议请求头域和简单鉴权和安全层协议响应头域由简单对象访问协议封装。

所述的身份标识网页业务网系统鉴权方法，其中：当业务提供商实体收到用户终端、单点认证业务实体或单点认证业务模块发送的退出链接请求消息时，或者当业务提供商实体和用户终端之间的会话正常终止时，或者当业务提供商实体收到的鉴权申明中的重新认证期限头域对应的的时间过期时，或者当业务提供商实体收到的鉴权申明中的期限头域对应的的时间过期时，业务提供商实体在随后与用户终端的通信过程中要求用户终端重新鉴权。

所述的身份标识网页业务网系统鉴权方法，其中：在鉴权服务实体或鉴权服务模块上配置如下的本地安全策略：在对用户终端重新鉴权时，若双方的共享密钥没有过期，则只对用户终端进行身份标识网页业务网络架构鉴权。

所述的身份标识网页业务网系统鉴权方法，其中：在鉴权服务实体或鉴权服务模块上配置如下的本地安全策略：在对用户终端重新鉴权时，若双方的共享密钥没有过期，对用户终端进行通用鉴权架构鉴权和身份标识网页业务网络架构鉴权。

本发明的技术方案对现有技术的 ID-WSF 进行了改进，提供了一种全新的互通架构，即将原有的鉴权服务实体、单点认证业务实体的功能以及网络业务应用功能分别由一个网络业务应用功能/鉴权服务/单点认证业务实体中的不同模块，即鉴权服务模块、单点认证业务模块和网络业务应用功能模块来实现，从而实现了 ID-WSF 和 GBA 的互通。针对现有的互通架构和本发明提供的互通架构，本发明还提供了实现身份标识网页业务系统鉴权的方法，使得 GBA 和 ID-WSF 的互通得以实现。因而解决了 ID-WSF 通信的安全性不够高，通用鉴权架构用户终端操作不够简便

的问题，扩展了用户终端的应用场景，避免了用户终端应用已有的多种多样的 WEB 业务的诸多限制。

### 附图说明

本发明包括如下附图：

图 1 是现有技术通用鉴权架构(GBA)示意图；

图 2 是现有技术通用鉴权架构中 UE 执行引导过程(bootstrapping)的流程图；

图 3 是现有技术 NAF 获取共享密钥  $K_s_{(Ext/Int)}_{NAF}$  的流程图；

图 4 是现有技术身份标识联盟网络架构(ID-FF)示意图；

图 5 是现有技术 ID-FF 和 GBA 互通架构示意图；

图 6 是现有技术身份标识网页业务网络架构(ID-WSF)示意图；

图 7 是现有技术 ID-WSF 的简化形式示意图；

图 8 是现有技术包含单点认证业务实体(SSOS)的 ID-WSF 示意图；

图 9 是现有技术 GBA 和 ID-WSF 互通的网络架构示意图；

图 10 是根据本发明一实施例的网络业务应用功能/鉴权服务/单点认证业务实体示意图；

图 11 是根据本发明一实施例的身份标识网页业务网系统示意图；

图 12 是根据本发明一实施例的当 NAF/AS 和 SSOS 为不同的实体时给 UE 返回 Assertion 的鉴权方法流程图；

图 13 是根据本发明一实施例的当 NAF/AS 和 SSOS 为不同的实体时给 UE 返回 Artifact 的鉴权方法流程图；

图 14 是根据本发明一实施例的使用网络业务应用功能/鉴权服务/单点认证业务实体并给 UE 返回 Assertion 的鉴权方法流程图；

图 15 是根据本发明一实施例的使用网络业务应用功能/鉴权服务/单点认证业务实体并给 UE 返回 Artifact 的鉴权方法流程图。

### 具体实施方式

下面结合附图和实施例对本发明作进一步详细说明：

为了提高现有技术 ID-WSF 网络通信的安全性，实现 ID-WSF 和 GBA

的互通，如图 10 所示，本发明提供了一种网络业务应用功能/鉴权服务/单点认证业务实体，其包括网络业务应用功能模块、鉴权服务模块、单点认证业务模块，网络业务应用功能模块用于提供网络业务应用功能实体功能，鉴权服务模块用于提供鉴权服务实体功能，单点认证业务模块用于提供单点认证业务实体功能。如图 11 所示，本发明提供了一种身份标识网页业务网系统，其包括通用鉴权架构的用户归属网络服务器和引导服务功能实体、网络业务应用功能/鉴权服务/单点认证业务实体、业务提供商实体、用户终端，用户归属网络服务器和引导服务功能实体之间通过 Zh 接口进行通信，引导服务功能实体与用户终端之间通过 Ub 接口进行通信，网络业务应用功能模块与引导服务功能实体之间通过 Zn 接口进行通信，网络业务应用功能模块与用户终端之间通过 Ua 接口进行通信；单点认证业务模块与用户终端采用安全声明标记语言描述的单点认证和身份标识联盟协议进行两者之间的通信，并可采用简单对象访问协议或超文本传输协议封装通信消息；用户终端与鉴权服务模块采用简单鉴权和安全层协议进行两者之间的通信，并可采用简单对象访问协议或超文本传输协议封装通信消息；单点认证业务模块与业务提供商实体之间、用户终端与业务提供商实体之间进行通信时，采用简单对象访问协议或超文本传输协议封装通信消息。

本发明不但给出了一种不同于现有的 GBA 和 ID-WSF 互通的网络架构，同时还给出了基于这两种架构的实现鉴权的方法。

本发明提供的当 NAF/AS 和 SSOS 为不同的实体时，对 UE 进行鉴权的方法如图 12 和图 13 所示，其中，图 12 与图 13 的相同之处在于 NAF/AS 和 SSOS 为不同的实体，区别在于图 12 为给 UE 返回 Assertion 的实施例 1，图 13 为给 UE 返回 Artifact 的鉴权方法实施例 2；本发明提供的使用网络业务应用功能/鉴权服务/单点认证业务实体对 UE 进行鉴权的方法如图 14 和图 15 所示，其中，图 14 与图 15 的相同之处在于 NAF/AS 和 SSOS 为同一实体，区别在于图 14 为给 UE 返回 Assertion 的鉴权方法实施例 3；如图 15 为给 UE 返回 Artifact 的鉴权方法实施例 4。

需要强调说明一点，图 12、13 与图 14、15 中所示鉴权方法的实现

步骤基本相同，区别在于：图 12、13 中的单点认证业务实体以及包含网络业务应用功能的鉴权服务实体为两个单独存在的逻辑实体，而图 14、15 中，上述两个实体的功能由一个网络业务应用功能/鉴权服务/单点认证业务实体中的三个模块，即网络业务应用功能模块、单点认证业务模块和鉴权服务模块来完成。

由于实施例 1 和 3，2 和 4 的实现过程基本相同，因此，下面通过对实施例 1 和实施例 2 的具体说明，阐述本发明鉴权方法的实现过程：

本发明鉴权方法的要点是为了实现 GBA 与 ID-WSF 的互通，提高 ID-WSF 网络通信的安全性和应用方便性，在身份标识网页业务网系统的用户终端和业务提供商实体的通信过程中包括两种鉴权过程，分别是通用鉴权架构鉴权过程和身份标识网页业务网络架构鉴权过程，在通用鉴权架构鉴权过程中，引导服务功能实体生成引导事务标识、根密钥有效期，并且发送给用户终端，引导服务功能实体和用户终端都生成根密钥；在身份标识网页业务网络架构鉴权过程中，鉴权服务实体或鉴权服务模块生成用户终端访问单点认证业务实体或单点认证业务模块所需要的信任状；单点认证业务实体或单点认证业务模块生成鉴权声明并发送给用户终端，或者单点认证业务实体或单点认证业务模块生成鉴权声明及相应的鉴权声明链接，保存鉴权声明、鉴权声明和鉴权声明链接的对应关系，将鉴权声明链接发送给用户终端。

在实施例 1 和实施例 2 中，UE 和 AS 通过 SASL 协议进行协商，采用 HTTP DIGEST 鉴权方式，如果采用其他鉴权方式，则 digest-challenge 头域(挑战头域)和 digest-response 头域(挑战响应头域)改成相应鉴权方式的挑战头域和挑战响应头域。

下面是对实施例 1 的说明：

步骤 1: UE 向 SP 发送 HTTP Request 消息(应用请求消息)；为保证安全，UE 和 SP 之间可以事先建立 TLS 安全隧道。

步骤 2: SP 收到该 HTTP Request 消息后，首先获取 AS 的地址，然后发送一个 HTTP Response 响应消息给 UE，其中携带 AuthnRequest 头域(鉴权请求头域)；

步骤3: 由于UE集成了WSC实体功能, 收到SP返回的包含AuthnRequest头域的响应消息后, UE通过其上的WSC知道应该通过SASL (Simple Authentication and Security Layer, 简单鉴权和安全层)协议向AS进行鉴权, 而不是通过HTTP DIGEST协议向IdP进行鉴权, UE向AS发送一个HTTP Request消息, 其中携带SOAP(Simple Object Access Protocol, 简单对象访问协议)封装的SASLRequest头域(简单鉴权和安全层协议请求头域), 其中SASLRequest头域的mechanism头域(鉴权机制头域)中包含UE支持的鉴权方式列表, 例如mechanism=“CRAM-MD5 DIGEST-MD5”, 其中DIGEST-MD5表示HTTP DIGEST鉴权方式;

步骤4: AS返回一个HTTP Response响应消息给UE, 其中携带SOAP协议封装的SASLResponse头域(简单鉴权和安全层协议响应头域), SASLResponse头域的serverMechanism头域中记录AS从UE支持的鉴权方式列表中选择鉴权方式(例如serverMechanism = “DIGEST-MD5”表示AS选择的鉴权方式为HTTP DIGEST), 以及digest-challenge头域(挑战头域);

步骤5: UE向BSF发送GBA鉴权请求消息, 其中包含私有用户标识(IMPI), 要求与BSF进行相互鉴权;

步骤6: BSF收到UE的GBA鉴权请求消息后, 首先到HSS获取该UE的鉴权向量信息, 即认证矢量(鉴权序号参数AUTN, 随机参数RAND, 完整性密钥IK, 机密性密钥CK, 预期结果XRES);

步骤7: BSF保存XRES、IK、CK, 并向UE发送消息, 其中携带AUTN和RAND;

步骤8: UE运行AKA算法, 检查AUTN有效性以鉴权BSF, 并生成期望结果RES, 并且利用RAND生成完整性密钥IK和机密性密钥CK;

步骤9: UE向BSF发送消息, 其中携带IMPI、期望结果RES;

步骤10: BSF将RES和保存的XRES比较, 如果两者一致的话完成对UE的鉴权, 并利用保存的IK和CK生成根密钥Ks;

步骤11: BSF向UE发送GBA成功响应消息, 其中携带引导事务标识(B-TID)和根密钥Ks有效期;

步骤12: UE保存B-TID和根密钥Ks有效期, 并利用IK和CK生成根密钥Ks, 然后生成并保存共享密钥Ks\_(Ext/Int)\_NAF;

步骤13: UE再次向AS发送一个HTTP Request消息, 其中携带SOAP协议封装的SASLRequest头域, SASLRequest头域的mechanism头域填写步骤4中AS选择的鉴权方式(这里的鉴权方式为HTTP DIGEST), SASLRequest头域的digest-response头域(挑战响应头域)中包含username头域, username头域中填写B-TID以及用密钥Ks\_(Ext/Int)\_NAF计算出来的鉴权响应摘要信息;

步骤14: AS和NAF在一个实体上, 如果AS中没有相关的Ks\_(Ext/Int)\_NAF密钥等信息, 则可以通过Zn接口向BSF获取Ks\_(Ext/Int)\_NAF、USS、密钥有效期、引导时间等信息, 其中USS可能包含一些身份标识联盟相关信息;

步骤15: 根据获取的Ks\_(Ext/Int)\_NAF密钥信息, AS对上述SASLRequest头域中的digest-response进行处理, AS鉴权通过后, 向UE发送HTTP Response响应消息, 其中携带SOAP协议封装的SASLResponse头域, 其中SASLResponse头域中的ID-WSF EPR(EndpointReference) 头域中包含SSOS地址和ServiceType域, ServiceType域中的内容包括urn:liberty:ssos:2004-04、以及访问SSOS所需要的信任状(Credentials)等其他SSO相关信息;

步骤16: UE根据步骤15得到的SSOS地址向SSOS发送HTTP Request消息, 以请求访问SP所需要的Assertion, 其中携带SOAP协议封装的samlp2:AuthnRequest头域、sb:Correlation头域、wsse:security头域, 根据具体的应用程序和网络模型, AuthnRequest头域可能是步骤2中SP返回的, 也可能由UE自己生成, 其中包含一些要求AuthnRequest接收方采取的鉴权操作, 其中ProtocolBinding 头域设置成urn:liberty:iff:profiles:id-wsf, 以表示要使用SAML 协议绑定, wsse:security头域包含上一步中返回的访问SSOS所需要的信任状(Credentials)信息, sb:Correlation头域主要用于将SSOS返回的响应消息和相应的请求消息关联起来;

步骤17: SSOS根据收到的HTTP Request消息内容进行鉴权处理, 鉴

权成功后SSOS可能告诉UE可以和哪些SP结成身份标识联盟，UE同意并完成和SP的身份标识联盟，然后SSOS返回HTTP Response响应消息，其中携带SOAP协议封装的samlp2:Response头域，其中Response头域包含访问SP所需要的saml:Assertion头域(其中包含SSOS的数字签名)；

步骤18: UE再次向SP发送HTTP Request消息，其中携带SOAP协议封装的上一步中返回的saml:Assertion头域；

步骤19: SP处理上述saml:Assertion头域，并验证SSOS的数字签名，根据和SSOS的身份标识联盟信息对UE完成鉴权，成功后返回一个HTTP Response消息。

另外的几点说明：

根据AuthnRequest中的身份标识策略，AS可能每次都要求UE必须先执行步骤5~步骤12，再执行步骤13，以保证每次的用户标识B-TID和密钥Ks\_(Ext/Int)\_NAF都是重新生成的。或者，

如果UE和AS之间已经建立了安全联盟，并且Ks\_(Ext/Int)\_NAF密钥没有过期，则不执行步骤3~步骤12，直接执行步骤13，即UE给AS发送的HTTP Request请求消息的SASLRequest头域中的digest-response头域中包含username头域，username头域中填写B-TID以及用共享密钥Ks\_(Ext/Int)\_NAF计算出来的鉴权响应摘要信息。

如果UE和AS之间还没有建立安全联盟，则需要先执行步骤3~步骤12，进行正常的GBA引导过程获取B-TID和密钥信息Ks\_(Ext/Int)\_NAF，然后再执行步骤13。

如果UE和AS之间已经建立了安全联盟，但是Ks\_(Ext/Int)\_NAF密钥已经或者将要过期，则步骤3中也带有已有的B-TID，以及用密钥Ks\_(Ext/Int)\_NAF计算出来的鉴权响应摘要信息，然后AS通过步骤4挑战UE，UE再执行步骤5~步骤12，进行正常的GBA鉴权过程获取更新的B-TID和共享密钥Ks\_(Ext/Int)\_NAF，然后再执行步骤13。

另外，对于本发明中GBA和SSO两种机制都支持的UE来讲：UE在步骤3中向AS发送HTTP请求时，需要携带一个表示支持GBA机制的标识，例如对于基于ME(Mobile Equipment, 移动设备)的应用，在User-Agent头

域中设置成“3gpp-gba”；对基于UICC(Universal Integrated Circuit Card, 通用集成电路卡)的应用，在User-Agent头域中设置成“3gpp-gba-uicc”。AS发现UE支持GBA后，在步骤4的挑战响应中也携带一个表示需要UE执行GBA机制的标识，例如对于基于ME的应用，在digest-challenge头域中的realm参数中设置“3gpp-gba@NAF的域名”，对于基于UICC的应用，在digest-challenge头域的realm参数中设置“3gpp-gba-uicc@NAF的域名”。

UE如果在挑战响应中发现此标识，则知道需要先执行GBA过程(步骤3~步骤12)，然后再执行步骤13，否则直接执行步骤13，其中的用户名、密码的获取通过现有SSO机制处理，例如可以给用户弹一个对话框，由用户直接输入用户名和密码。

UE在步骤13中再次向AS发送HTTP请求时，同步骤3一样，也需要携带一个表示支持GBA机制的标识，如果AS发现此标识，则知道需要先执行步骤14，然后执行步骤15；否则直接执行步骤15。

另外，也可以通过配置AS来达到上述同样目的。上述几点同样适用于下面的实施例2。

下面是对实施例2的说明：其中，步骤1~16与实施例1中的步骤1~16完全相同，具体为：

步骤1：UE向SP发送HTTP Request消息；

步骤2：SP收到该HTTP Request消息后，首先获取AS的地址，然后发送一个HTTP Response响应消息给UE，其中携带AuthnRequest头域；

步骤3：由于UE集成了WSC实体功能，收到SP返回的包含AuthnRequest头域的响应消息后，UE通过其上的WSC知道应该通过SASL协议向AS进行鉴权，而不是通过HTTP DIGEST协议向IdP进行鉴权，UE向AS发送一个HTTP Request消息，其中携带SOAP协议封装的SASLRequest头域，其中SASLRequest头域的mechanism头域中包含UE支持的鉴权方式列表，例如mechanism=“CRAM-MD5 DIGEST-MD5”，其中DIGEST-MD5表示HTTP DIGEST鉴权方式；

步骤4：AS返回一个HTTP Response响应消息给UE，其中携带SOAP协议封装的SASLResponse头域，SASLResponse头域的serverMechanism头

域(服务器鉴权机制头域)中记录AS从UE支持的鉴权方式列表中选择鉴权方式(例如serverMechanism = “DIGEST-MD5”表示AS选择的鉴权方式为HTTP DIGEST), 以及挑战头域digest-challenge;

步骤5: UE向BSF发送GBA鉴权请求消息, 其中包含私有用户标识(IMPI), 要求与BSF进行相互鉴权;

步骤6: BSF收到UE的GBA鉴权请求消息后, 首先到HSS获取该UE的鉴权向量信息, 即认证矢量(鉴权序号参数AUTN, 随机参数RAND, 完整性密钥IK, 机密性密钥CK, 预期结果XRES);

步骤7: BSF保存XRES、IK、CK, 并向UE发送消息, 其中携带AUTN和RAND;

步骤8: UE运行AKA算法, 检查AUTN有效性以鉴权BSF, 并生成期望结果RES, 并且利用RAND生成完整性密钥IK和机密性密钥CK;

步骤9: UE向BSF发送消息, 其中携带IMPI、期望结果RES;

步骤10: BSF将RES和保存的XRES比较, 如果两者一致的话完成对UE的鉴权, 并利用保存的IK和CK生成根密钥Ks;

步骤11: BSF向UE发送GBA成功响应消息, 其中携带引导事务标识(B-TID)和根密钥Ks有效期;

步骤12: UE保存B-TID和根密钥Ks有效期, 并利用IK和CK生成根密钥Ks, 然后生成并保存共享密钥Ks\_(Ext/Int)\_NAF;

步骤13: UE再次向AS发送一个HTTP Request消息, 其中携带SOAP协议封装的SASLRequest头域, 其中SASLRequest头域中的mechanism头域填写步骤4中AS选择的鉴权方式(本实施例中的鉴权方式为HTTP DIGEST), 挑战响应头域digest-response中包含username头域, username头域中填写B-TID, 以及用密钥Ks\_(Ext/Int)\_NAF计算出来的鉴权响应摘要信息;

步骤14: AS和NAF在一个实体上, 如果AS中没有相关的Ks\_(ext)\_NAF 密钥等信息, 则可以通过Zn接口向BSF获取Ks\_(Ext/Int)\_NAF、USS、密钥有效期、引导时间等信息, 其中USS可能包含一些身份标识联盟相关信息;

步骤15: AS对上述SASLRequest头域进行处理, AS鉴权通过后, 向UE发送HTTP Response响应消息, 其中携带SOAP封装的SASLResponse头域, SASLResponse头域中的ID-WSF EPR(EndpointReference头域)中包含SSOS地址、SASLResponse头域中的ServiceType域设置为urn:liberty:ssos:2004-04、访问SSOS所需要的信任状;

步骤16: UE向上一一步得到的SSOS发送HTTP Request消息, 以请求访问SP所需要的Assertion, 其中携带SOAP协议封装的samlp2:AuthnRequest头域、sb:Correlation头域、wsse:security头域, 根据具体的应用程序和网络模型, AuthnRequest头域可能是步骤2中SP返回的, 也可能由UE自己生成, 其中包含一些要求AuthnRequest接收方采取的鉴权操作, 其中ProtocolBinding头域设置成urn:liberty:iff:profiles:id-wsf, 以表示要使用的SAML协议绑定, wsse:security头域包含上一步中返回的访问SSOS所需要的信任状(Credentials头域)信息, sb:Correlation头域主要用于将SSOS返回的响应消息和相应的请求消息关联起来;

步骤17: SSOS处理收到的HTTP Request消息, 生成相应的Artifact和Assertion, 并保存两者之间的关系, 然后返回HTTP Response成功响应消息, 其中携带SOAP协议封装的samlp2:Response头域; 其中Response头域包含访问SP所需要的saml:Assertion对应的Artifact头域;

本步骤中给UE返回的响应中包含“Artifact”, 而图12(实施例1)中步骤17给UE返回的响应中包含“Assertion”, 因而导致了后续处理不同。

步骤18: UE再次向SP发送HTTP Request消息, 其中携带SOAP协议封装的步骤17中返回的Artifact头域;

步骤19: SP向SSOS发送HTTP Request消息, 其中携带SOAP协议封装的上一步得到的Artifact头域, 请求用于对UE鉴权处理的Assertion;

步骤20: SSOS根据Artifact找到对应的Assertion, 然后返回HTTP Response消息, 其中携带SOAP协议封装的saml:Assertion(其中包含SSOS的数字签名);

步骤21: SP处理上述saml:Assertion头域, 并验证其数字签名, 根据和SSOS的身份标识联盟信息对UE完成鉴权, 成功后返回一个HTTP

Response消息。

完成了上述实施例1或实施例2的鉴权过程后，UE和SP可以继续进行沟通，当出现下列情况时则必须对UE重新进行鉴权：

- 1、SP收到UE或者SSOS发来的LogoutRequest消息(退出链接请求消息)时；
- 2、SP和UE之间的会话正常中止时；
- 3、SP收到的Assertion中的AuthenticationStatement头域(认证声明头域)中的ReauthenticateOnOrAfter头域(重新认证期限头域)对应的时间过期时；
- 4、SP收到的Assertion中的Conditions头域(条件头域)中的NotOnOrAfter头域(期限头域)对应的时间过期时。

SP需要在和UE进行下一次交互时，发送一个新的携带AuthnRequest的HTTP Response响应消息给UE，指示其需要重新鉴权，以后进行实施例1或实施例2中从步骤3开始的流程。

对于ID-WSF，步骤4中当AS收到UE发来的HTTP Request消息时，如果Ks\_(ext)\_NAF还没有过期，则根据AS上配置的本地安全策略，可以不进行新的GBA鉴权过程，也可以进行一个新的GBA鉴权过程。如果不进行新的GBA鉴权过程，则步骤3~步骤12、步骤14可以省略，步骤13、步骤15、步骤16同上次对应的消息内容相同，步骤17中SSOS需要产生一个新的Assertion(对于实施例2，还要产生新的Artifact)，其余步骤不变。

如果要进行新的GBA过程，则将重新执行实施例1或实施例2中其余的所有步骤。

图14与图12所示实施例基本相同，图15与图13所示实施例基本相同，其区别仅在于：图12、13中NAF/AS为一个逻辑实体，SSOS为一个逻辑实体，而图14、15中NAF/AS/SSOS为一个逻辑实体。

虽然通过参照本发明的优选实施例，已经对本发明进行了图示和描述，但本领域的普通技术人员应该明白，可以在形式上和细节上对其作各种各样的改变，而不偏离所附权利要求书所限定的本发明的精神和范围。

## 权 利 要 求

1、一种身份标识网页业务网系统，包括通用鉴权架构的用户归属网络服务器和引导服务功能实体、业务提供商实体、用户终端，用户归属网络服务器和引导服务功能实体之间通过 Zh 接口进行通信，引导服务功能实体与用户终端之间通过 Ub 接口进行通信，其特征在于：包括网络业务应用功能/鉴权服务/单点认证业务实体，其包括网络业务应用功能模块、鉴权服务模块、单点认证业务模块，网络业务应用功能模块用于提供网络业务应用功能实体功能，鉴权服务模块用于提供鉴权服务实体功能，单点认证业务模块用于提供单点认证业务实体功能，网络业务应用功能模块与引导服务功能实体之间通过 Zn 接口进行通信，网络业务应用功能模块与用户终端之间通过 Ua 接口进行通信。

2、根据权利要求 1 所述的身份标识网页业务网系统，其特征在于：单点认证业务模块与用户终端采用安全申明标记语言描述的单点认证和身份标识联盟协议进行两者之间的通信，采用简单对象访问协议或超文本传输协议封装通信消息；鉴权服务模块与用户终端采用简单鉴权和安全层协议进行两者之间的通信，采用简单对象访问协议或超文本传输协议封装通信消息；单点认证业务模块与业务提供商实体之间进行通信时，采用简单对象访问协议封装通信消息；用户终端与业务提供商实体之间进行通信时，采用简单对象访问协议或超文本传输协议封装通信消息。

3、一种身份标识网页业务网系统鉴权方法，其特征在于，包括步骤：身份标识网页业务网系统的用户终端和业务提供商实体的通信过程中包括两种鉴权过程，分别是通用鉴权架构鉴权过程和身份标识网页业务网络架构鉴权过程，在通用鉴权架构鉴权过程中，引导服务功能实体生成引导事务标识、根密钥有效期，并且发送给用户终端，引导服务功能实体和用户终端都生成根密钥；在身份标识网页业务网络架构鉴权过程中，鉴权服务实体或鉴权服务模块生成用户终端访问单点认证业务实体或单点认证业务模块所需要的信任状；单点认证业务实体或单点认证业务模块生成鉴权申明并发送给用户终端，或者单点认证业务实体或单点认证

业务模块生成鉴权申明及相应的鉴权申明链接，保存鉴权申明和鉴权申明链接的对应关系表，将鉴权申明链接发送给用户终端。

4、根据权利要求3所述的身份标识网页业务网系统鉴权方法，其特征在于，包括步骤：用户终端向相应的鉴权服务实体或鉴权服务模块发送身份标识网页业务网络架构鉴权请求消息，鉴权服务实体或鉴权服务模块向用户终端发送要求其进行通用鉴权架构鉴权的挑战响应消息，引导服务功能实体对用户终端进行通用鉴权架构鉴权，鉴权成功后向用户终端发送通用鉴权架构鉴权成功响应消息，该鉴权成功响应消息中包含引导事务标识和根密钥有效期；用户终端向鉴权服务实体或鉴权服务模块发送应用请求消息，鉴权服务实体或鉴权服务模块根据该应用请求消息对用户终端进行鉴权，鉴权通过后，向用户终端发送响应消息，其中包含单点认证业务实体或单点认证业务模块的地址和信任状。

5、根据权利要求4所述的身份标识网页业务网系统鉴权方法，其特征在于，包括步骤：单点认证业务实体或单点认证业务模块对用户终端进行身份标识网页业务网络架构鉴权，鉴权成功后向用户终端发送身份标识网页业务网络架构鉴权成功响应消息，该鉴权成功响应消息中包含鉴权申明。

6、根据权利要求4所述的身份标识网页业务网系统鉴权方法，其特征在于，包括步骤：单点认证业务实体或单点认证业务模块对用户终端进行身份标识网页业务网络架构鉴权，生成鉴权申明及相应的鉴权申明链接，保存鉴权申明和鉴权申明链接的对应关系表，在随后发送给用户终端的身份标识网页业务网络架构鉴权成功响应消息中包含鉴权申明链接。

7、根据权利要求4所述的身份标识网页业务网系统鉴权方法，其特征在于，包括步骤：

A1、用户终端向业务提供商实体发送应用请求消息；

A2、业务提供商实体收到该应用请求消息后，首先获取鉴权服务实体或鉴权服务模块的地址，然后发送响应消息给用户终端，其中携带鉴

权请求头域;

A3、用户终端向鉴权服务实体或鉴权服务模块发送应用请求消息，其中包含简单鉴权和安全层协议请求头域，其包含鉴权机制头域，鉴权机制头域中包含用户终端支持的鉴权方式列表;

A4、鉴权服务实体或鉴权服务模块给用户终端发送挑战响应消息，其中包含简单鉴权和安全层协议响应头域，其包含服务器鉴权机制头域和挑战头域，服务器鉴权机制头域中记录鉴权服务实体或鉴权服务模块选择的鉴权方式。

A5、用户终端与引导服务功能实体交互，进行通用鉴权架构鉴权;

A6、用户终端向鉴权服务实体或鉴权服务模块发送应用请求消息，其中包含简单鉴权和安全层协议请求头域，简单鉴权和安全层协议请求头域包含挑战响应头域，挑战响应头域包含引导事务标识和鉴权响应摘要信息;

A7、鉴权服务实体或鉴权服务模块通过 Zn 接口向引导服务功能实体获取共享密钥、用户安全设置、密钥有效期、引导时间等信息，鉴权服务实体或鉴权服务模块根据收到简单鉴权和安全层协议请求头域对用户终端进行鉴权，鉴权通过后，向用户终端发送响应消息，其中包含简单鉴权和安全层协议响应头域，该头域中有单点认证业务实体或单点认证业务模块的地址和信任状。

8、根据权利要求 7 所述的身份标识网页业务网系统鉴权方法，其特征在于：同时支持通用鉴权架构鉴权和身份标识网页业务网络架构鉴权的用户终端在向鉴权服务实体或鉴权服务模块发送的应用请求消息中设置通用鉴权架构标识，若鉴权服务实体或鉴权服务模块发现此通用鉴权架构标识，则通知用户终端先启动通用鉴权架构鉴权过程，再启动用户身份标识网页业务网络架构鉴权过程，否则通知用户终端只启动用户身份标识网页业务网络架构鉴权过程。

9、根据权利要求 7 所述的身份标识网页业务网系统鉴权方法，其特征在于，所述步骤 A5 包括步骤：

B1、用户终端向引导服务功能实体发送通用鉴权架构鉴权请求消息，其中包含私有用户标识；

B2、引导服务功能实体收到该通用鉴权架构鉴权请求消息后，从用户归属网络服务器获取用户终端的认证矢量；

B3、引导服务功能实体向用户终端发送挑战消息，其中携带鉴权序号参数和随机参数；

B4、用户终端检查鉴权序号参数有效性并生成期望结果；

B5、用户终端向引导服务功能实体发送消息，其中携带私有用户标识、期望结果；

B6、引导服务功能实体检查期望结果的有效性并生成根密钥；

B7、引导服务功能实体向用户终端发送通用鉴权架构成功响应消息，其中携带引导事务标识和根密钥有效期；

B8、用户终端保存引导事务标识和根密钥有效期，生成并保存根密钥和共享密钥。

10、根据权利要求 5 所述的身份标识网页业务网系统鉴权方法，其特征在于，包括步骤：

C1、用户终端根据单点认证业务实体或单点认证业务模块的地址向单点认证业务实体或单点认证业务模块发送应用请求消息；

C2、单点认证业务实体或单点认证业务模块根据收到的应用请求消息内容进行鉴权处理，鉴权成功后向用户终端发送成功响应消息，其中包含鉴权申明，鉴权申明中有单点认证业务实体或单点认证业务模块的数字签名；

C3、用户终端向业务提供商实体发送应用请求消息，其中包含鉴权申明；

C4、业务提供商实体处理鉴权申明，验证单点认证业务实体或单点认证业务模块的数字签名，完成对用户终端的鉴权后，向用户终端发送响应消息。

11、根据权利要求 6 所述的身份标识网页业务网系统鉴权方法，其

特征在于，包括步骤：

D1、用户终端根据单点认证业务实体或单点认证业务模块的地址向单点认证业务实体或单点认证业务模块发送应用请求消息；

D2、单点认证业务实体或单点认证业务模块根据收到的应用请求消息内容进行鉴权处理，生成鉴权申明和相应的鉴权申明链接，保存鉴权申明、鉴权申明和相应的鉴权申明链接的对应关系，鉴权成功后向用户终端发送成功响应消息，其中包含鉴权申明链接。

D3、用户终端向业务提供商实体发送应用请求消息，其中包含鉴权申明链接；

D4、业务提供商实体向单点认证业务实体或单点认证业务模块发送应用请求消息，其中包含鉴权申明链接；

D5、单点认证业务实体或单点认证业务模块根据鉴权申明链接找到对应的鉴权申明，向业务提供商实体发送响应消息，其中包含鉴权申明，鉴权申明中有单点认证业务实体或单点认证业务模块的数字签名；

D6、业务提供商实体处理鉴权申明，验证单点认证业务实体或单点认证业务模块的数字签名，完成对用户终端的鉴权后，向用户终端发送响应消息。

12、根据权利要求 7、8、10、11 任一所述的身份标识网页业务网系统鉴权方法，其特征在于：简单鉴权和安全层协议请求头域和简单鉴权和安全层协议响应头域由简单对象访问协议封装。

13、根据权利要求 5 所述的身份标识网页业务网系统鉴权方法，其特征在于：当业务提供商实体收到用户终端、单点认证业务实体或单点认证业务模块发送的退出链接请求消息时，或者当业务提供商实体和用户终端之间的会话正常终止时，或者当业务提供商实体收到的鉴权申明中的重新认证期限头域对应的时间过期时，或者当业务提供商实体收到的鉴权申明中的期限头域对应的时间过期时，业务提供商实体在随后与用户终端的通信过程中要求用户终端重新鉴权。

14、根据权利要求 6 所述的身份标识网页业务网系统鉴权方法，其

特征在于：当业务提供商实体收到用户终端、单点认证业务实体或单点认证业务模块发送的退出链接请求消息时，或者当业务提供商实体和用户终端之间的会话正常终止时，或者当业务提供商实体收到的鉴权申明中的重新认证期限头域对应的时间过期时，或者当业务提供商实体收到的鉴权申明中的期限头域对应的时间过期时，业务提供商实体在随后与用户终端的通信过程中要求用户终端重新鉴权。

15、根据权利要求 13 或 14 所述的身份标识网页业务网系统鉴权方法，其特征在于：在鉴权服务实体或鉴权服务模块上配置如下的本地安全策略：在对用户终端重新鉴权时，若双方的共享密钥没有过期，则只对用户终端进行身份标识网页业务网络架构鉴权。

16、根据权利要求 13 或 14 所述的身份标识网页业务网系统鉴权方法，其特征在于：在鉴权服务实体或鉴权服务模块上配置如下的本地安全策略：在对用户终端重新鉴权时，若双方的共享密钥没有过期，对用户终端进行通用鉴权架构鉴权和身份标识网页业务网络架构鉴权。

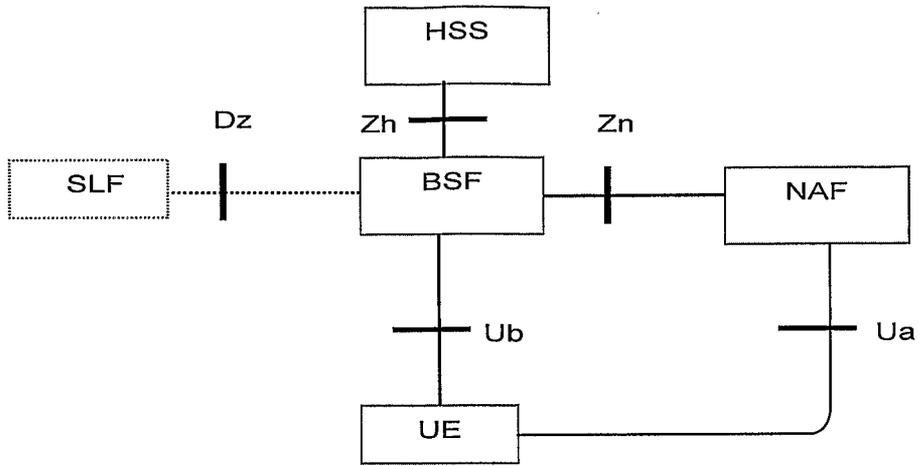


图 1

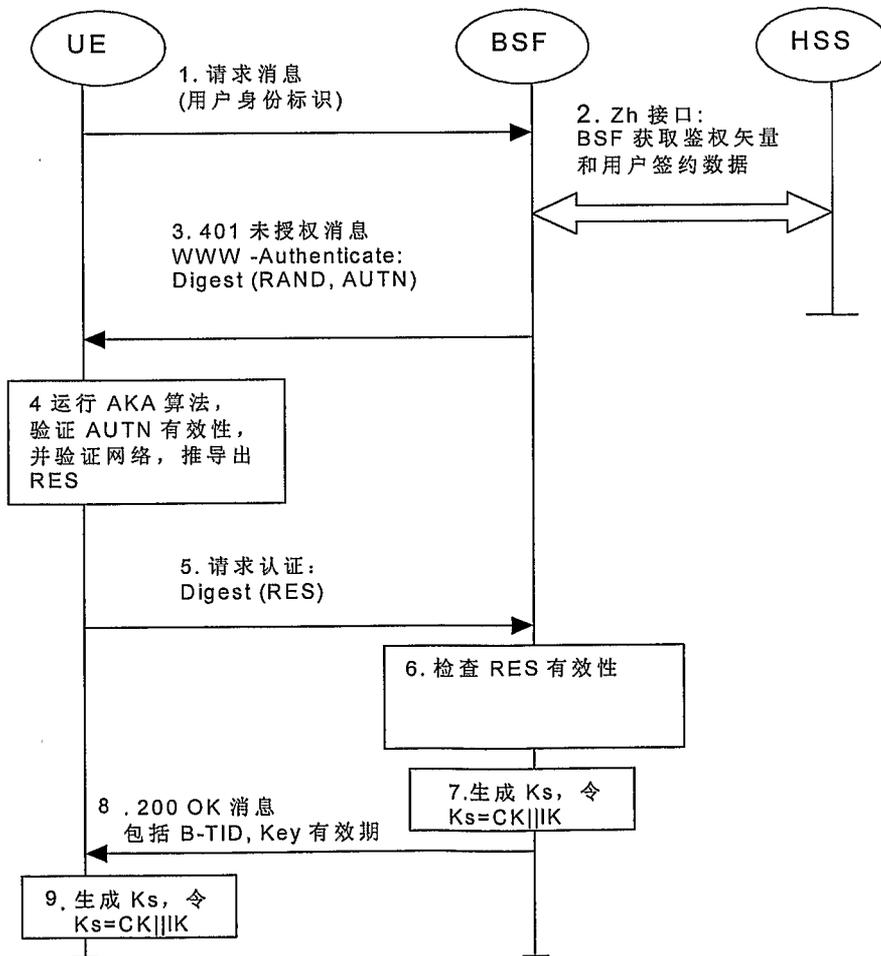


图 2

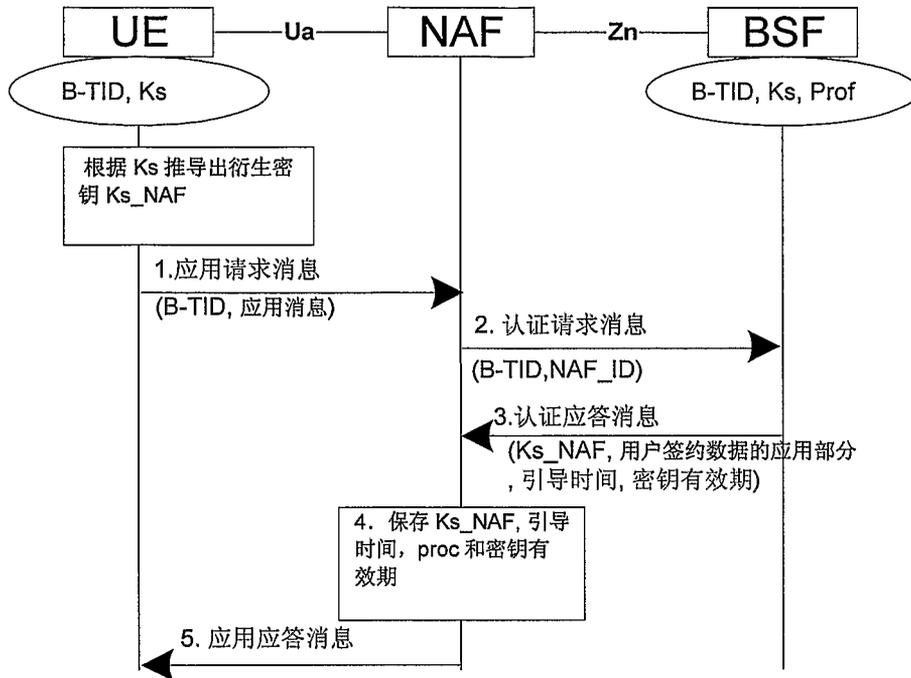


图 3

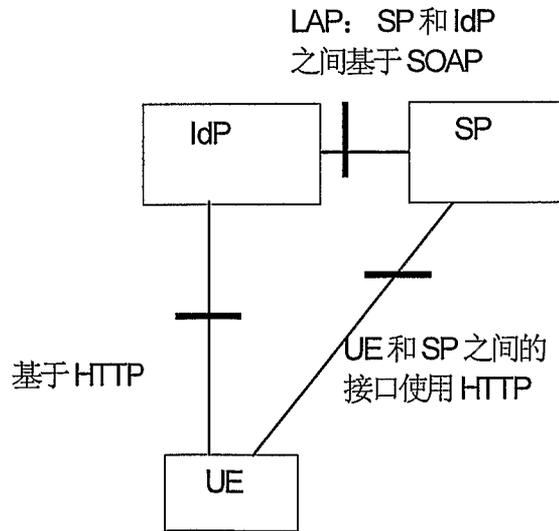


图 4

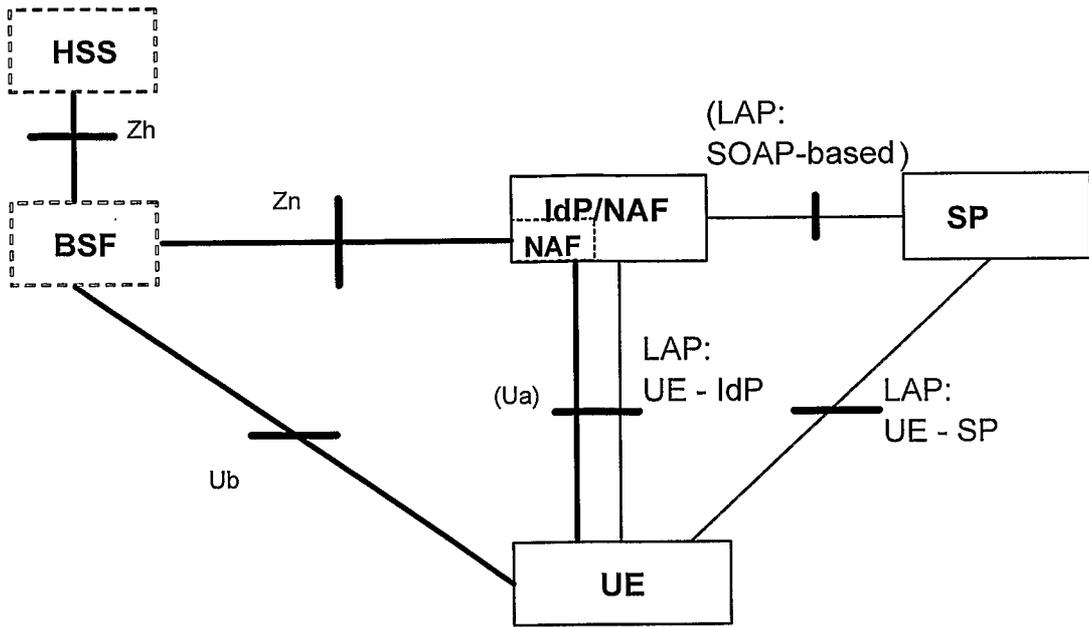


图 5

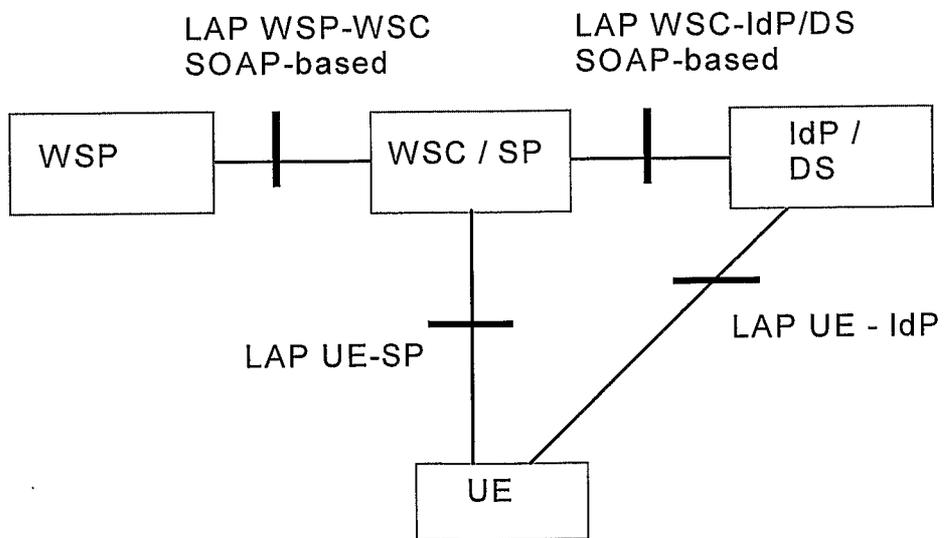


图 6

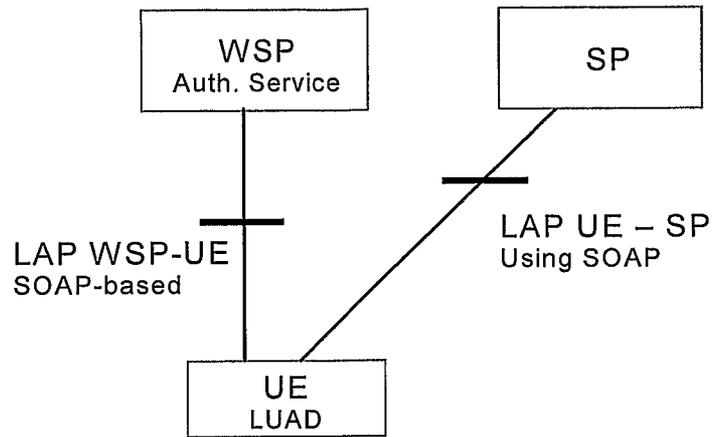


图 7

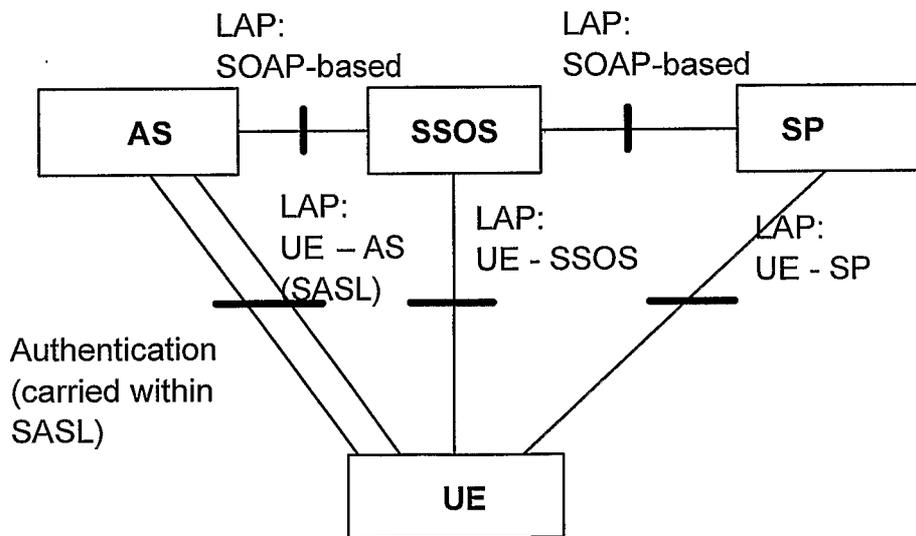


图 8

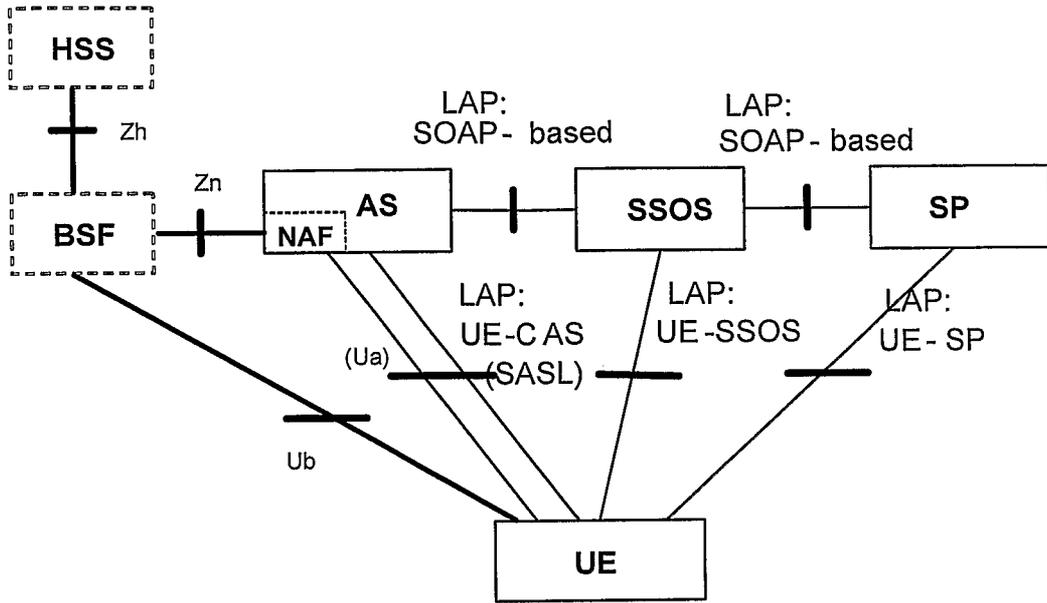


图 9

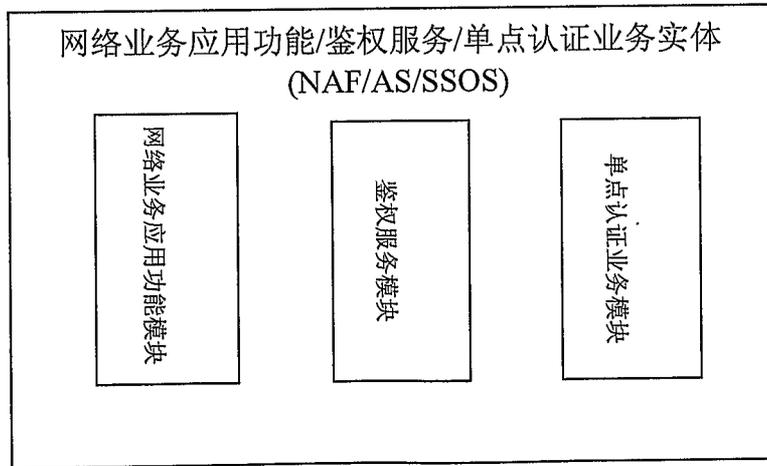


图 10

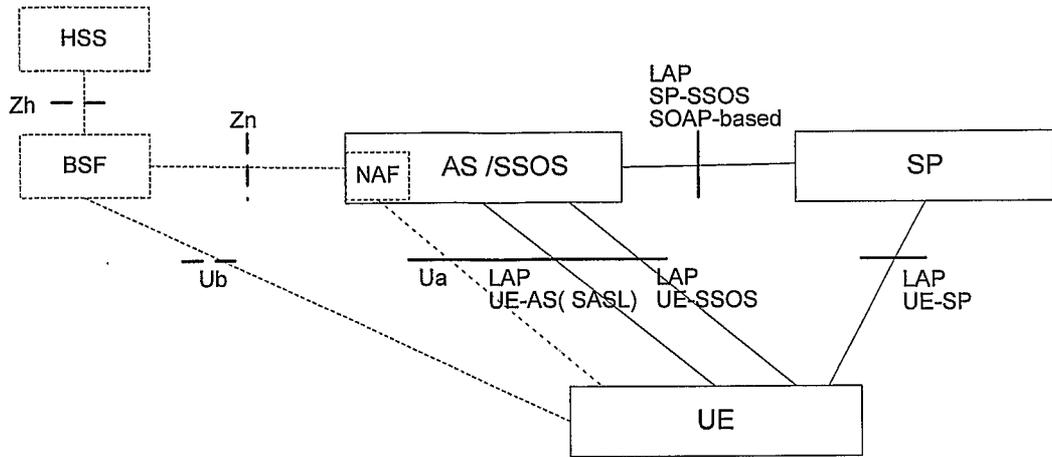


图 11

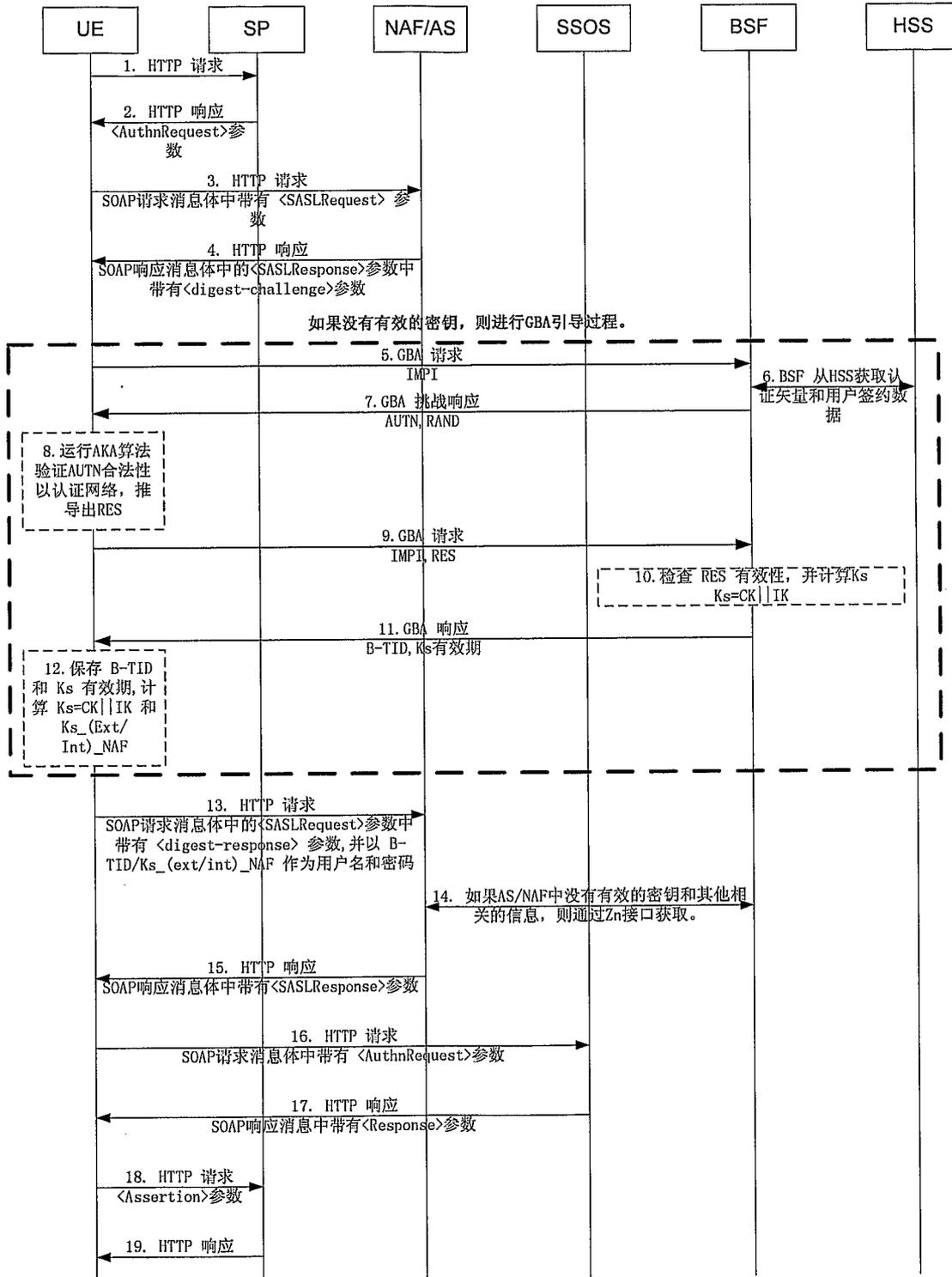


图 12

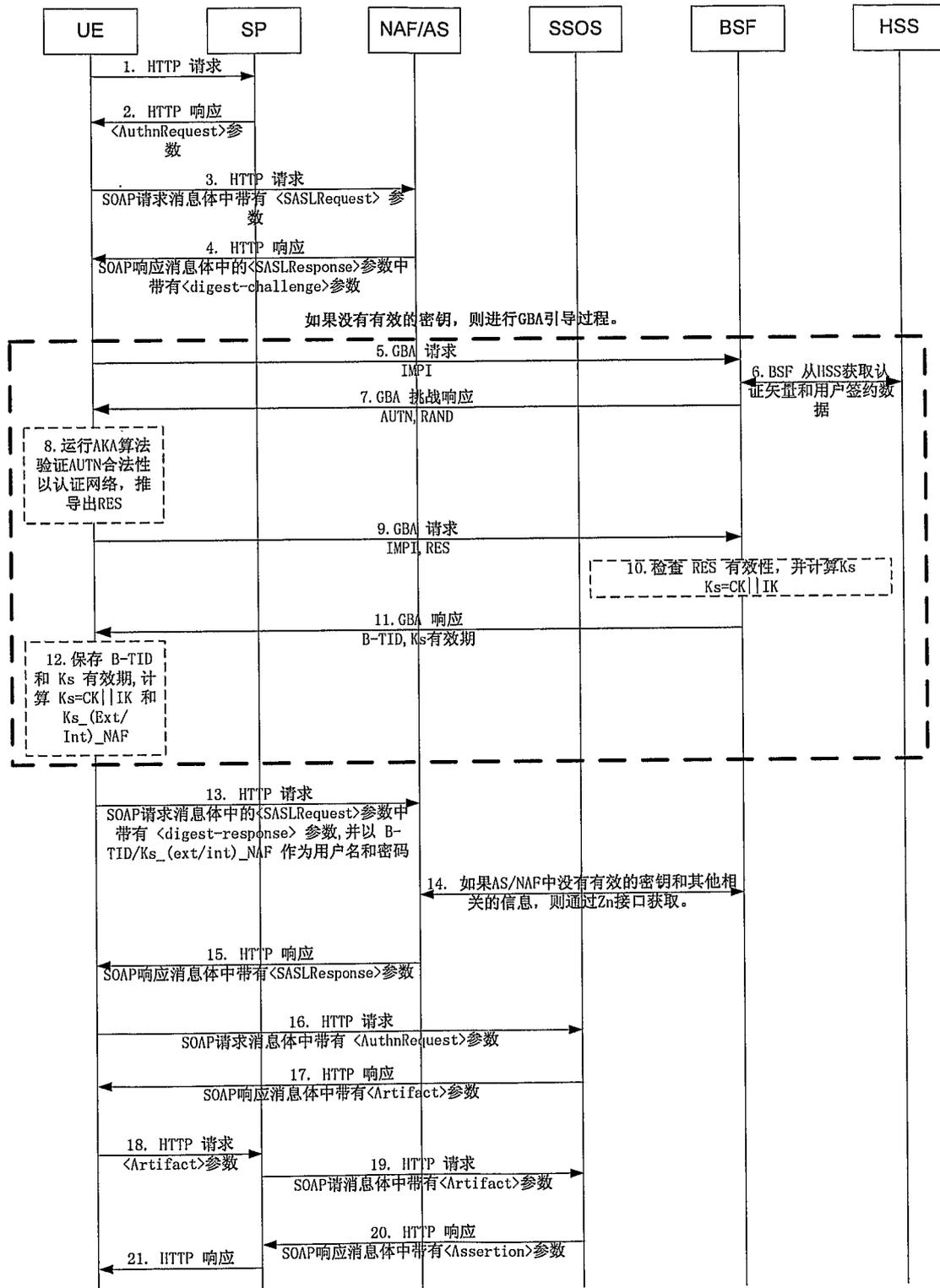


图 13

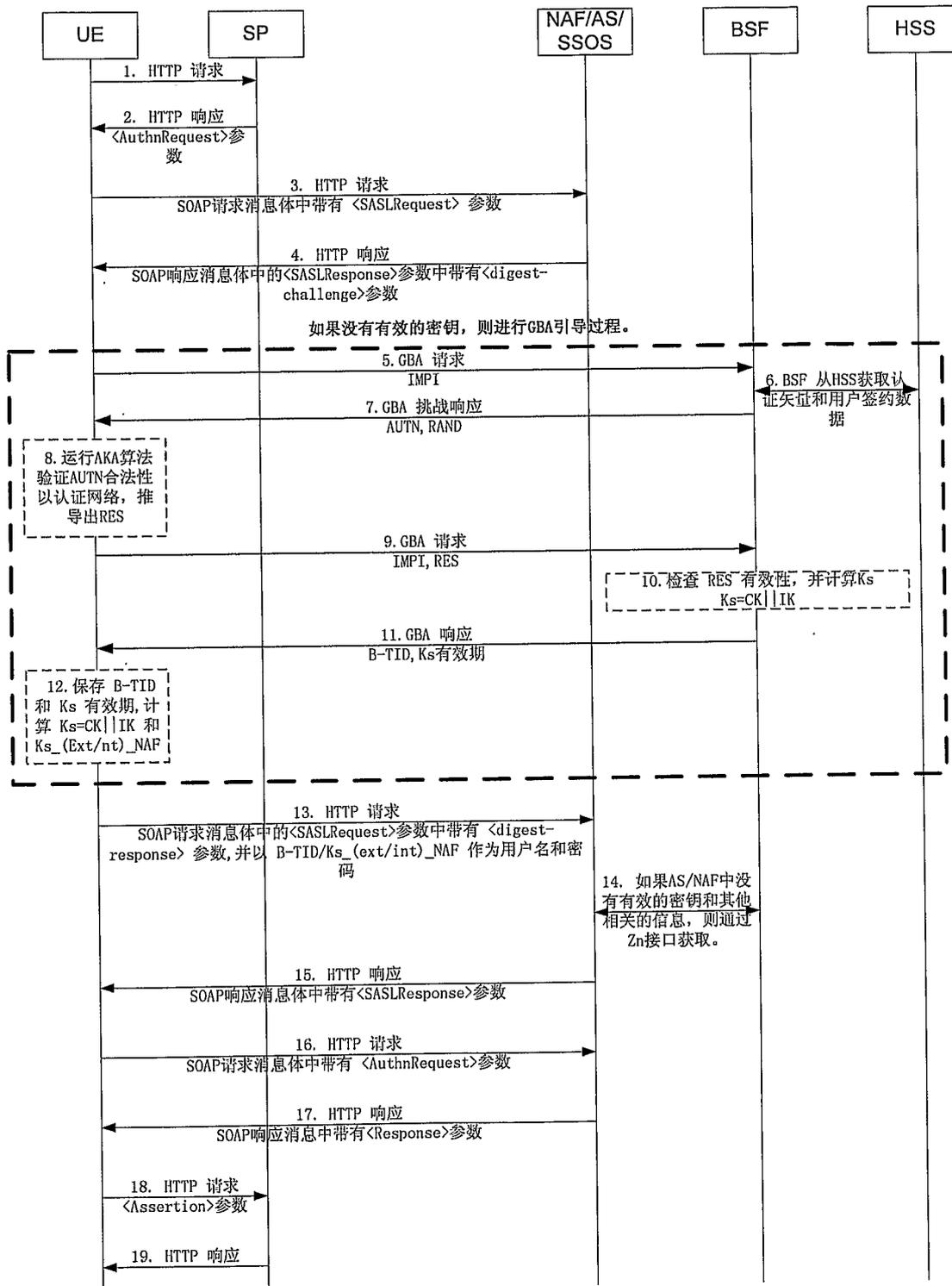


图 14

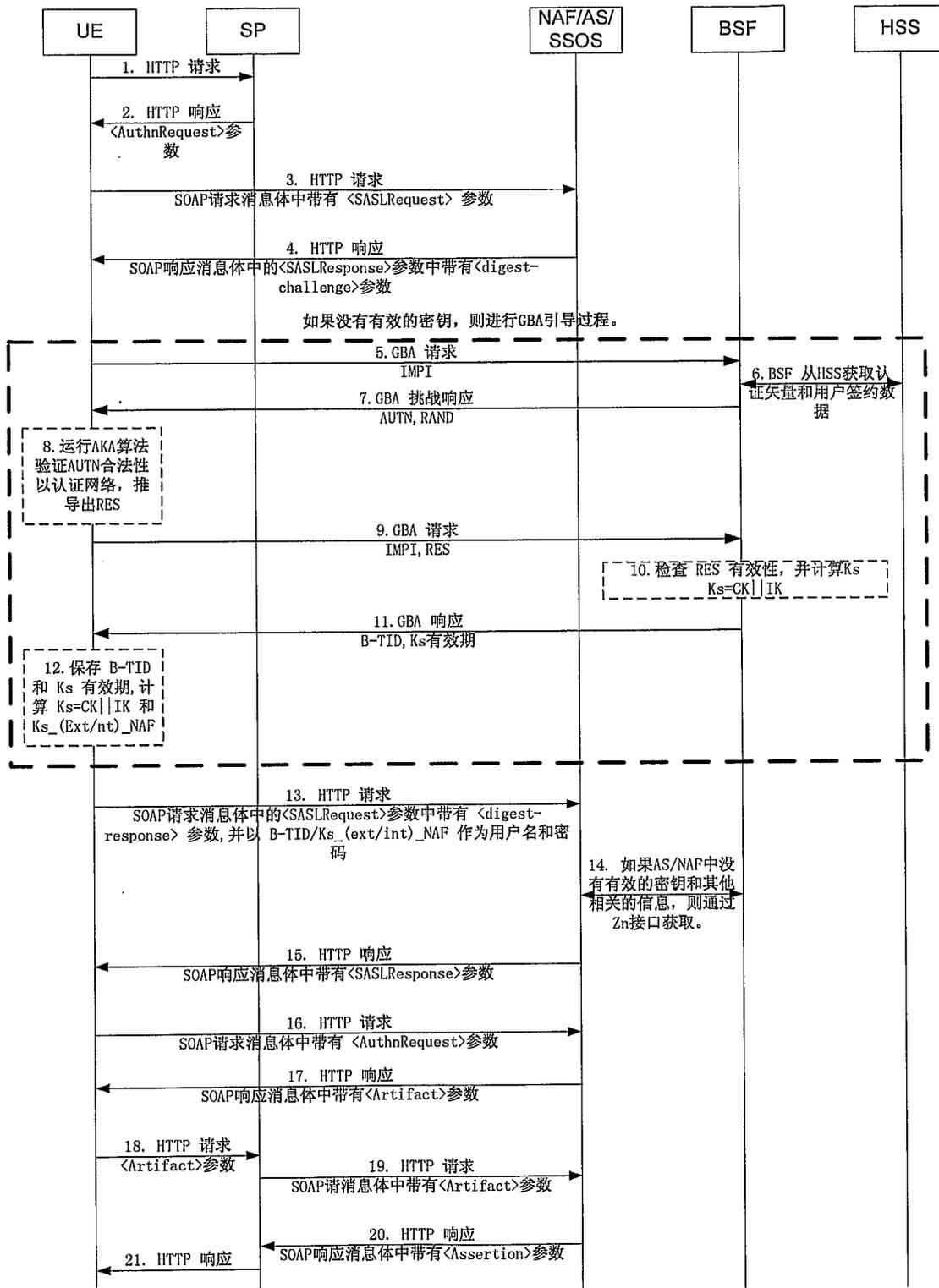


图 15

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2007/000762

## A. CLASSIFICATION OF SUBJECT MATTER

H04L9/00 (2006.01) i

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

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)

WPI, EPODOC, PAJ, CNPAT, CNKI: ID identity WSF GBA AS BSF SSO(S) authenticat+ credential key

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN1614903A, (HUAWEI TECHNOLOGIES CO LT), 11 May. 2005 (11.05.2005), see the whole document	1-16
A	CN1642079A, (HUAWEI TECHNOLOGIES CO LT), 20 Jul. 2005 (20.07.2005), see the whole document	1-16
A	US6286104B1, ( ORACLE CORP [US] ), 04 Sep. 2001 (04.09.2001), see the whole document	1-16
A	US2004117493A1, (IBM [US] ), 17 Jun. 2004 (17.06.2004), see the whole document	1-16
A	US2006021004A1, (IBM [US] ), 26 Jan. 2006 (26.01.2006), see the whole document	1-16

Further documents are listed in the continuation of Box C.

See patent family annex.

<p>* Special categories of cited documents:</p> <p>“A” document defining the general state of the art which is not considered to be of particular relevance</p> <p>“E” earlier application or patent but published on or after the international filing date</p> <p>“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)</p> <p>“O” document referring to an oral disclosure, use, exhibition or other means</p> <p>“P” document published prior to the international filing date but later than the priority date claimed</p>	<p>“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</p> <p>“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</p> <p>“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</p> <p>“&amp;”document member of the same patent family</p>
--	--

Date of the actual completion of the international search  
**08 Jun. 2007 (08.06.2007)**

Date of mailing of the international search report  
**21 Jun. 2007 (21.06.2007)**

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  
**LIANG Nianshun**  
Telephone No. (86-10)62086052

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.

PCT/CN2007/000762

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1614903A	11.05.2005	NONE	
CN1642079A	20.07.2005	WO2005074188A	11.08.2005
		CA2552917A	11.08.2005
		EP1705828A	27.09.2006
		EP20050700439	17.01.2005
		US2007050623A	01.03.2007
US6286104B1	04.09.2001	NONE	
US2004117493A1	17.06.2004	NONE	
US2006021004A1	26.01.2006	NONE	

国际检索报告

国际申请号  
PCT/CN2007/000762

A. 主题的分类

H04L9/00 (2006.01) i

按照国际专利分类表(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

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))

WPI,EPODOC,PAJ,CNPAT,CNKI: 身份标识 标识 ID 密钥 WSF GBA BSF 鉴权 认证 华为 单点认证 信任状  
AS SSO(S) identity authenticat+ credential key

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
A	CN1614903A, (华为技术有限公司), 11.5 月 2005 (11.05.2005), 参见全文	1-16
A	CN1642079A, (华为技术有限公司), 20.7 月 2005 (20.07.2005), 参见全文	1-16
A	US6286104B1, (ORACLE CORP [US]), 04.9 月 2001 (04.09.2001), 参见全文	1-16
A	US2004117493A1, (IBM [US]), 17.6 月 2004 (17.06.2004), 参见全文	1-16
A	US2006021004A1, (IBM [US]), 26.1 月 2006 (26.01.2006), 参见全文	1-16

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

“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  
08.6 月 2007 (08.06.2007)

国际检索报告邮寄日期  
21.6 月 2007 (21.06.2007)

中华人民共和国国家知识产权局(ISA/CN)  
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  
梁年顺  
电话号码: (86-10) 62086052

国际检索报告  
关于同族专利的信息

国际申请号  
PCT/CN2007/000762

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN1614903A	11.05.2005	无	
CN1642079A	20.07.2005	WO2005074188A	11.08.2005
		CA2552917A	11.08.2005
		EP1705828A	27.09.2006
		EP20050700439	17.01.2005
		US2007050623A	01.03.2007
US6286104B1	04.09.2001	无	
US2004117493A1	17.06.2004	无	
US2006021004A1	26.01.2006	无	