国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

Y.2722

(01/2011)

Y系列：全球信息基础设施、
互联网的协议问题和下一代网络

下一代网络 – 安全

下一代网络(NGN)的身份管理机制

ITU-T Y.2722 建议书

ITU-T

ITU 国际电信联盟

ITU-T Y系列建议书

全球信息基础设施、互联网的协议问题和下一代网络

全球信息基础设施	
概要	Y.100–Y.199
业务、应用和中间件	Y.200–Y.299
网络方面	Y.300–Y.399
接口和协议	Y.400–Y.499
编号、寻址和命名	Y.500–Y.599
运营、管理和维护	Y.600–Y.699
安全	Y.700–Y.799
性能	Y.800–Y.899
互联网的协议问题	
概要	Y.1000–Y.1099
业务和应用	Y.1100–Y.1199
体系、接入、网络能力和资源管理	Y.1200–Y.1299
传输	Y.1300–Y.1399
互通	Y.1400–Y.1499
服务质量和网络性能	Y.1500–Y.1599
信令	Y.1600–Y.1699
运营、管理和维护	Y.1700–Y.1799
计费	Y.1800–Y.1899
基于NGN的IPTV	Y.1900–Y.1999
下一代网络	
框架和功能体系模型	Y.2000–Y.2099
服务质量和性能	Y.2100–Y.2199
业务方面：业务能力和业务体系	Y.2200–Y.2249
业务方面：NGN中业务和网络的互操作性	Y.2250–Y.2299
编号、命名和寻址	Y.2300–Y.2399
网络管理	Y.2400–Y.2499
网络控制体系和协议	Y.2500–Y.2599
未来的网络	Y.2600–Y.2699
安全	**Y.2700–Y.2799**
通用移动性	Y.2800–Y.2899
运营商级开放环境	Y.2900–Y.2999
未来的网络	Y.3000–Y.3099

如果需要进一步了解细目，请查阅ITU-T建议书清单。

ITU-T Y.2722建议书

下一代网络（NGN）的身份管理机制

摘要

ITU-T Y.2722规范了可满足下一代网络（NGN）身份管理（IdM）要求及部署需要的机制。

历史沿革

版本	建议书	批准日期	研究组	
1.0	ITU-T Y.2722	2011-01-28	13	

关键词

联邦身份、身份管理、身份管理机制、下一代网络、安全。

前言

国际电信联盟(ITU)是从事电信领域工作的联合国专门机构。ITU-T(国际电信联盟电信标准化部门)是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会(WTSA)确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织(ISO)和国际电工委员会(IEC)合作制定的。

注

本建议书为简要扼起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款(以确保例如互操作性或适用性等)，只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们通过下列网址查询电信标准化局(TSB)的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

页码

1 范围 1
2 参考文献 1
3 定义 2
4 缩略语 2
5 惯例 3
6 支持IdM功能的机制和程序 4
6.1 寿命周期管理 4
6.2 认证和认证保障 4
6.3 关联与绑定 24
6.4 发现 25
6.5 IdM的沟通和信息交流 26
6.6 个人可识别信息（PII）的保护 30
6.7 联邦身份功能 30
6.8 身份信息接入控制 31
6.9 单次登录 31
6.10 单次退出 32
7 安全性 35
附录I – WSS ITU-T X.509 v3信息认证 36
附录II – 基于“OpenID+OAuth”的接入控制机制 38
II.1 OAuth[b-IETF RFC 5849] 38
II.2 OpenID与OAuth结合使用 38
II.3 OpenID + OAuth的授权流程 38
参考资料 41

ITU-T Y.2722建议书

下一代网络（NGN）的身份管理机制

1 范围

[ITU-T Y.2721]-NGN的身份管理要求和使用案例，具体规定了下一代网络的身份管理（IdM）要求。本建议书描述应用于满足[ITU-T Y.2721]中要求的具体IdM机制和一系列选择方案。此外，本建议书亦提供旨在支持互操作性和满足其它需求的最佳做法和指南。

本建议书旨在与 [ITU-T Y.2720]和[ITU-T Y.2721]建议共同使用，作为基础的结构性概念，而要求和使用安全将不在本建议书中重复。

注 – 上述机制的实施者与用户须遵守所有适用国家和区域法律、法规和政策。一些具体的规则和立法可能要求执行相关机制，为可确定的个人信息提供保护。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T X.509] ITU-T X.509建议书（2005年）| ISO/IEC 9594-8 :2005，信息技术 – 开放系统互连 – 号码簿：公开密钥和属性证书框架

[ITU-T X.1035] ITU-T X.1035建议书（2007年），口令认证密钥交换（PAK）协议。

[ITU-T X.1141] ITU-T X.1141建议书（2006年），安全性声明标识语言（SAML 2.0）。

[ITU-T X.1252] ITU-T X.1252建议书（2010年），基线标识管理的术语和定义。

[ITU-T Y.2012] ITU-T Y.2012建议书（2006年），NGN第1版的功能要求和结构。

[ITU-T Y.2701] ITU-T Y.2701建议书（2007年），NGN第1版的安全性要求。

[ITU-T Y.2702] ITU-T Y.2702建议书（2008年），NGN第1版的认证与授权要求。

[ITU-T Y.2704] ITU-T Y.2704建议书（2010年），NGN的安全机制与程序。

[ITU-T Y.2720] ITU-T Y.2720建议书（2009年），NGN身份管理框架。

[ITU-T Y.2721] ITU-T Y.2721建议书（2010年），NGN身份管理要求和使用案例。

[3GPP TS 23.228] 3GPP TS 23.228 （现行），IP多媒体子系统（IMS）；第2阶段。

[ATIS 33102] ATIS.3GPP.33.102V710-2007，安全性的结构。

[IETF RFC 2289] IETF RFC 2289（1998年），一次性口令系统。

3 定义

本建议书依赖[ITU-T Y.2720]和[ITU-T X.1252]定义的术语。

本建议书特别采用了[ITU-T X.1252]中的如下定义：

3.1 身份提供商（IdP）：见身份服务提供商（IdSP）。

3.2 身份服务提供商（IdSP）：对其它实体的身份信息进行验证、维护、管理并可能予以创建和指配的实体。

4 缩略语

本建议书使用了下列缩略语和首字母缩写：

AKA 认证和密钥协议（Authentication and Key Agreement）

ASP 应用服务提供商（Application Service Provider）

AuC 认证中心（Authentication Centre）

AV 认证矢量（Authentication Vector）

BSF 自举服务器功能（Bootstrapping Server Function）

CK 加密密钥（Ciphering Key）

GBA 一般性自举架构（Generic Bootstrapping Architecture）

HSS 归属签约用户系统（Home Subscriber System）

IdM 身份管理（Identity Management）

IdP 身份提供商（Identity Provider）

IdSP 身份服务提供商（Identity Service Provider）

IK 完整性密钥（Integrity Key）

IMPI 互联网协议（IP）多媒体私人用户身份（IP Multimedia Private user Identity）

IMPU IP多媒体公共用户身份（IP Multimedia Public User identity）

IMS IP多媒体子系统（IP Multimedia Subsystem）

IMSI 国际移动签约用户身份（International Mobile Subscriber Identity）

IPTV 互联网协议电视（Internet Protocol Television）

ISIM IMS签约用户身份模块（IMS Subscriber Identity Module）

LDAP 轻量目录接入协议（Lightweight Directory Access Protocol）

MS 移动台（Mobile Station）

NAF 网络应用功能（Network Application Function）

NGN 下一代网络（Next Generation Networks）

OASIS 结构信息标准推进组织（Organization for the Advancement of Structured Information Standards）

OTP 一次性口令（One Time Password）

PII 个人可识别信息（Personally Identifiable Information(PII)）

PKI 公共密钥基础设施（Public Key Infrastructure）

RP 依赖方（Relying Party）

SAML 安全断言标记语言（Security Assertion Markup Language）

SIP 会话起始协议（Session Initiation Protocol）

SLF 签约用户定位功能（Subscriber Locator Function）

SOAP 简单对象接入协议（Simple Object Access Protocol）

SQL 结构查询语言（Structured Query Language）

SSO 单次登陆（Single Sign-On）

UE 用户设备（User Equipment）

UICC 通用集成电路卡（Universal Integrated Circuit Card）

UMTS 通用移动通信系统（Universal Mobile Telecommunications System）

USIM 通用订户身份模块（Universal Subscriber Identifier Module）

WAP 无线应用协议（Wireless Application Protocol）

WSS 网络服务安全（Web Services Security）

XML 可扩展标记语言（eXtensible Markup Language）

XRDS 可扩展资源描述符序列（eXtensible Resource Descriptor Sequence）

5 惯例

本建议书中：

关键词“要求”表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

关键词“建议”表示是一项建议的并非需绝对遵守的要求，因此声称遵守本文件时不一定按照该要求行事。

关键词“禁止”表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与之有任何偏差。

关键词“作为选择可以”表示允许的一项可选择的要求，不含有任何被建议的意思。该术语并非意味着厂商在实施中一定提供这一可选功能，网络运营商/服务提供商可作为选择提供这一功能。也就是说，厂商可以作为选择提供这一功能，同时仍然声称遵守本建议书提出的规范。

在本建议书正文和附件中使用了*须、不须、应和可能*等术语，应分别将这些理解为*要求、禁止、建议和作为选择可以*。附录或其它明确标为*资料性*材料中出现的此类短句或关键词应被理解为不含有任何规范性意图。

6 支持IdM功能的机制和程序

6.1 寿命周期管理

有关身份寿命周期管理的信息请见[ITU-T Y.2720]：下一代网络（NGN）的身份管理框架。

6.2 认证和认证保障

本节说明身份和身份信息的认证及保障，并参引其它文献定义的认证机制。

网络服务（WS）、安全断言标记语言（SAML）资料、基于证书的认证，或基于口令的认证（包括一次性口令（OTP））等具体认证机制，可供IdSP根据不同语境和所需保障水平用于具体的应用或业务。认证方法按照保障等级要求选择。IdSP可提出信息要求，以判定可满足服务提供商保障等级要求的方法。

6.2.1 基于网络服务（WS）安全SAML资料的认证

6.2.1.1 SAML断言

安全断言标记语言（SAML），[ITU-T X.1141]，具体规定了可用于IdM安全信息交换的断言格式。使用SAML实施的IdM功能包括认证、属性共享和授权，这些与有关SAML断言主体的三种声明相对应：

- 认证声明 – 传达有关断言主体在特定时间通过特定手段得到认证的信息。
- 属性声明 – 传达有关断言主体与所列属性相关联的信息。
- 授权决定声明 – 传达有关向断言主体授予特定资源接入权或该主体被拒绝该接入的信息。

SAML断言的内容可概括如下：发出方**R**针对主体**S**在**t**时间发出了断言**A**，前提是条件**C**依然有效。

用于通信认证、属性和授权的SAML断言，是通过简单对象接入协议（SOAP）信息传递。在经过未得到保护的传输手段交换SOAP信息时，强烈建议采用XML签名[b-W3C XML signature]核实信息中SOAP信息和断言声明之间的关系。网络服务安全（WSS）：SAML令牌资料[b-OASIS SAML token]标准描述了如下方式：

- SOAP信息中传送和通过该信息参引的SAML断言（亦称作SAML令牌）。
- 使用XML签名将SAML断言主体和声明与SOAP信息相绑定。

SAML令牌与按照本建议书制定的SOAP信息的典型用法在由图1和下述内容说明。

在该示例中，经签名的SOAP信息包含带有属性声明的SAML断言。根据该声明的信息，接收方可做出接入控制决定。

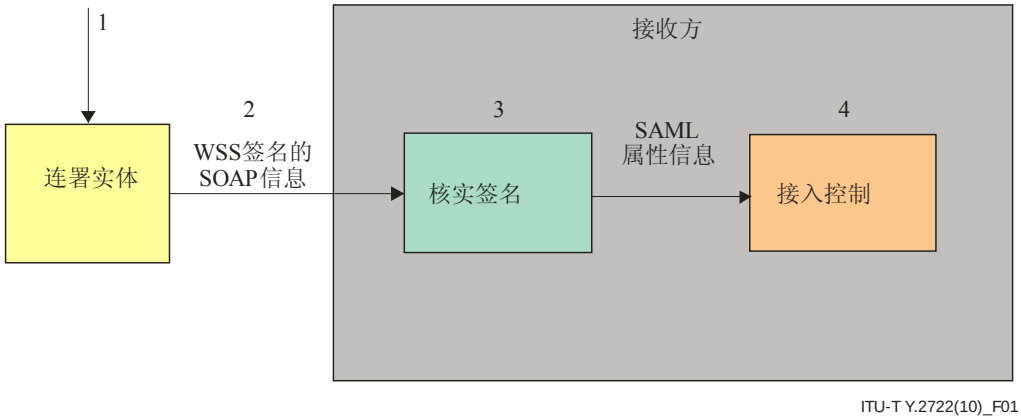


图1 – 建立和处理带有SAML令牌的SOAP信息的典型步骤

1) 连署实体获得带有属性声明的SAML断言，并根据[b-OASIS SAML token]的SOAP信息中对此予以建立和纳入。

2) 连署实体向接收方发送WSS签名的SOAP信息。

3) 接收方核实数字签名。

4) SAML声明中的信息可用于接入控制决定。

6.2.1.2 SAML令牌的主体确认方法

OASIS标准 – 网络服务安全：SAML令牌资料1.1[b-OASIS SAML token]规定了将SAML断言附着于SOAP信息的方法并确定了两种必须采用的主体确认方法：

- 密钥持有方；
- 发送凭证。

图2具体表明按照[b-OASIS WSS SOAP]建立的SOAP信息的主要XML要素。

SAML断言置于<wsse:Security>字头中，其中亦包含数字签名<ds:Signature>。SOAP信息接收方使用数字签名核实信息发送方了解用于在SOAP正文摘要上计算签名和检查其完整性的密钥。摘要算法是[b-OASIS WSS SOAP]确定的SHA 1，签名算法是RSA_SHA 1。签名数值由数字签名<ds:Signature>中的<ds:SignatureValue>要素提供。

有两种主体确认方法确定将密钥信息传送给接收方的不同方式。

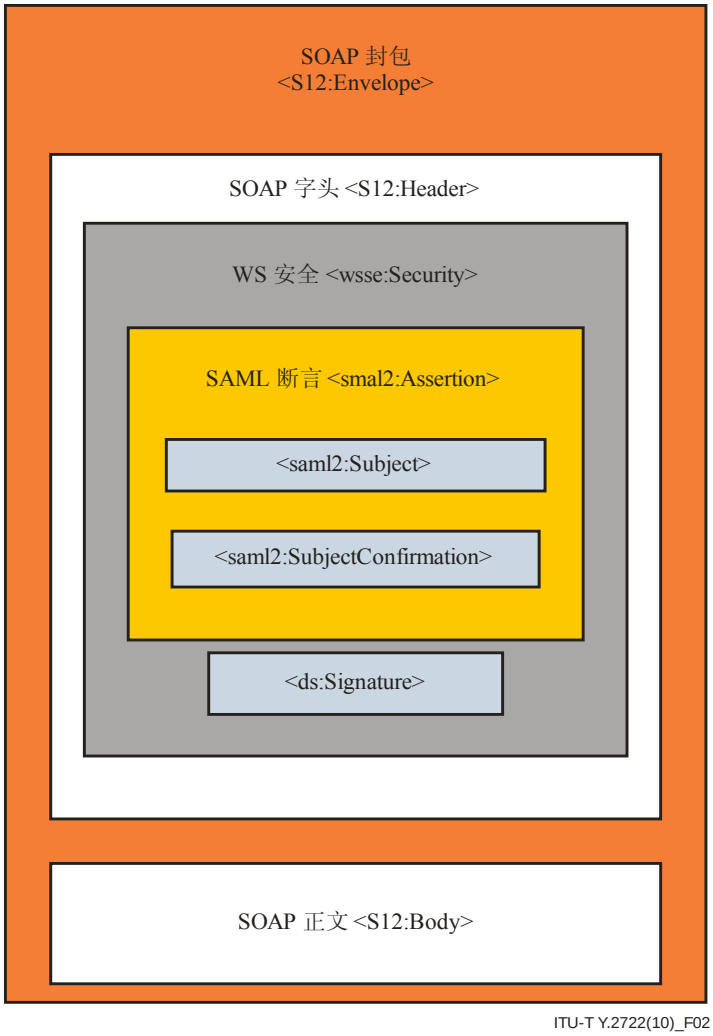


图2 – 带有SAML断言的SOAP信息结构

以下各节说明两种主体确认方法。

6.2.1.2.1 密钥持有方主体确认方法

图3描述用于密钥持有方主体确认方法的SAML断言结构，要素<saml2:SubjectConfirmation>的方法属性表明主体确认方法（密钥持有方）。

该方法规定，发送方（亦称作连署实体）必须通过表明对密钥的了解证明它有权给出有关主体的声明（密钥由SAML断言中<ds:KeyInfo>要素所含的<ds:KeyValue>要素予以识别）。<ds:KeyInfo>要素识别用于确认主体身份的公共或秘密密钥。该方法进一步规定，发送方可通过用该密钥对SOAP正文摘要签名的方式完成上述工作。如图2所示，签名包含在WS安全字头中的<ds:Signature>要素中。

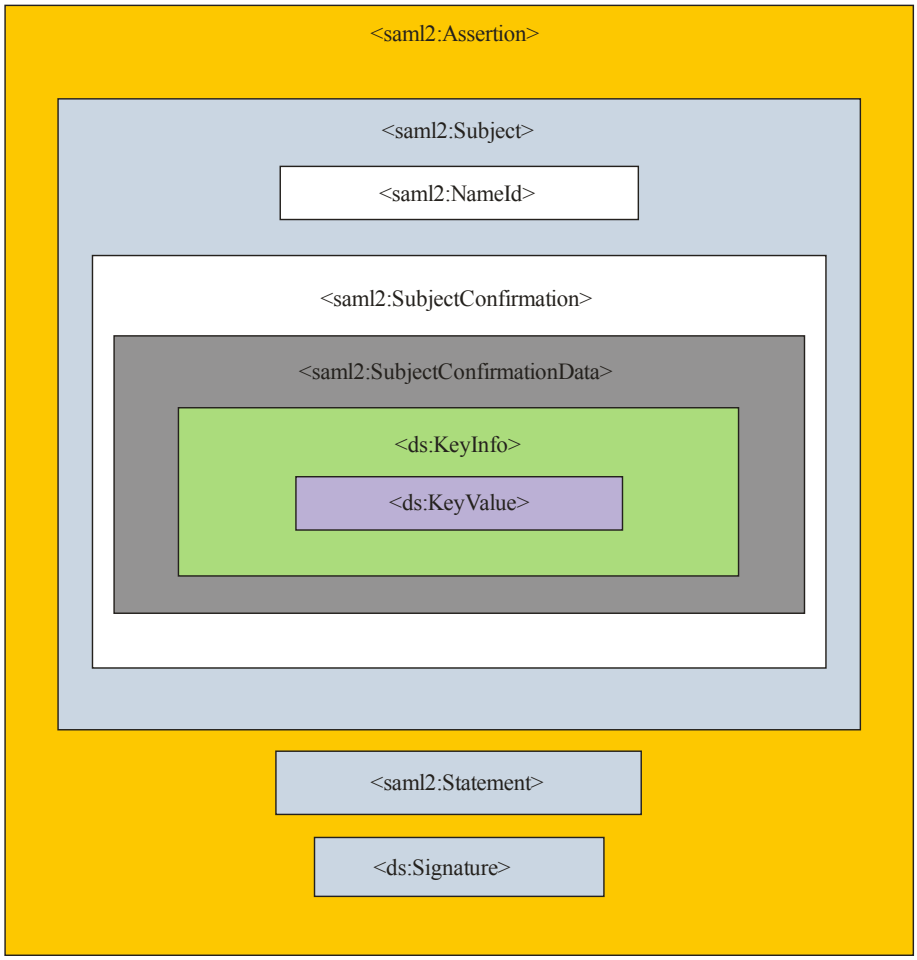


图3 – 密钥持有方主体确认方法使用的SAML断言结构

SOAP信息接收方使用连署实体在<ds:KeyInfo>要素中提供的信息获得密钥，而后计算SOAP正文的数字签名并检查该签名是否与连署实体提供的签名相匹配。如果匹配，则可将SAML断言的主体和声明归属于连署实体，并将完整性由密钥保护的SOAP正文内容视为由连署实体提供。

6.2.1.2.2 发送凭证主体确认方法

图4描述发送凭证主体确认方法使用的SAML断言结构。<saml2:SubjectConfirmation>要素的方法属性表明主体确认方法（发送凭证）。

连署实体受接收方委托对主体做出SAML断言，条件是<SubjectConfirmation>要素的方法属性数值表明是发送凭证方法。

连署实体从一个或多个主管机构获得一个或多个断言或有关断言的参考，并将其纳入SOAP信息中，之后计算SAML断言摘要和SOAP信息正文的签名。签名包含在WS安全字头的<ds:Signature>要素中（如图2所示）。作为可选方式，连署实体可向接收方提供用于计算签名的密钥信息。如果不存在此类信息，则期望接受方通过其它手段识别密钥。

接收方检查签名的有效性，如果签名有效，则接收方确认连署实体已对主体做出了声明的事实。

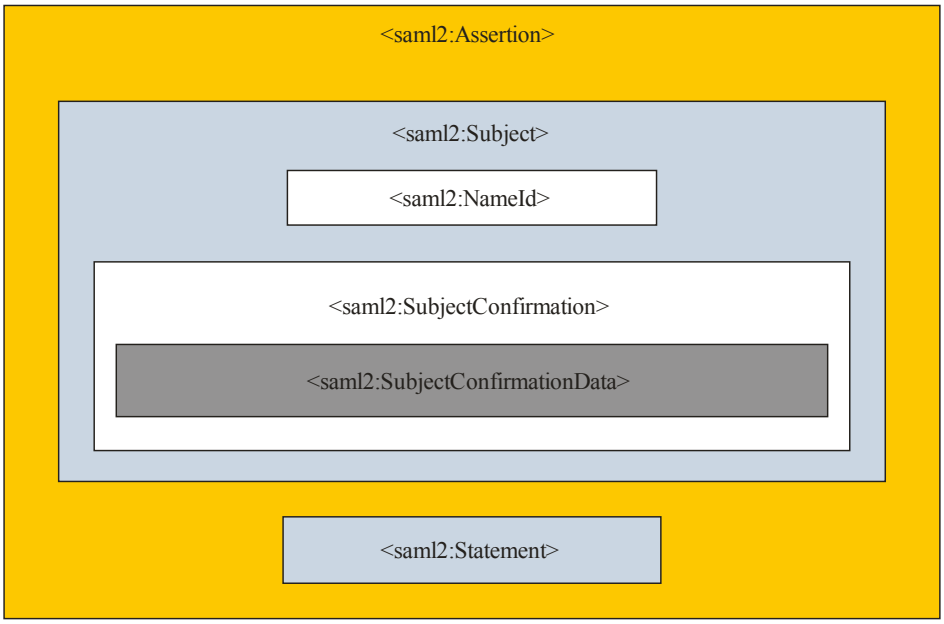


图4 – 发送凭证主体确认方法使用的SAML断言结构

6.2.2 基于证书的认证

[ITU-T X.509]证书可用于具体应用或基于语境和所需保障水平的业务。[ITU-T Y.2704] –下一代网络（NGN）的安全机制和程序，阐述如何使用 [ITU-T X.509]证书进行认证。

6.2.3 基于口令的认证

基于口令的认证可用于具体应用或基于语境和所需保障水平的业务。有关基于口令的认证机制的说明，请参见[ITU-T X.1035]。

6.2.4 一次性口令

一次性口令（OTP）可用于具体应用或基于语境和所需保障水平的业务。[IETF RFC 2289]阐述实施OTP的方法之一。

6.2.5 使用认证和密钥协议（AKA）进行相互认证

通用移动通信系统（UMTS）认证和密钥协议（AKA）协议（protocol）可用于移动台（MS）和网络之间的相互认证。UMTS AKA是一种质询 – 应答协议，使用长期的、通用签约用户身份模块（USIM）和认证中心（AuC）之间共用的密钥。这些实体分别置于MS的通用集成电路卡（UICC）和移动台的归属网络上。在某些商业安排中，AuC的功能可通过IdSP提供。AKA协议由[ATIS 33102]具体规定。

6.2.6 基于PKI的认证与IMS的结合

IP多媒体子系统（IMS）的安全以AKA机制为基础，采用共享的密钥和质询 – 应答协议进行用户 – 网络认证，但某些NGN业务（如IPTV）的安全以公共密钥基础设施（PKI）证书为基础。为能够将这些使用PKI证书的NGN业务与IMS安全性相结合，或有必要将基于PKI的认证与IMS认证进行结合，且其方法应能利用IMS的安全优势。

将IMS认证与基于PKI的认证相结合有利于用户设备和网络根据各自的证书相互认证，并根据与AKA相同的密钥生成算法就一套加密密钥达成协议。为此，有必要为用户设备和网络分别提供私人密钥和证书，并使其能够进行PKI操作。

有关加密密钥（CK）和完整性密钥（IK）协议，所描述的结合机制具体规定了两种可选方案：

1) 使用最终用户功能和[ITU-T Y.2012]定义的S-5 – 业务用户资料功能实体（SUP-FE）之间的共享密钥就CK和IK密钥达成协议。

2) 不使用共享密钥而就CK和IK密钥达成协议。

第一和第二个可选方案的总体呼叫流程分别在图5和图6中显示。

6.2.6.1 惯例

本节采用了下述惯例符号：

– “|”表示字符串并置。

– *CK*表示加密密钥。

– *IK*表示完整性密钥。

– *K()*表示对称密钥加密。

– N_{pr} *[]*表示用网络私人密钥N_{pr}加密。

– N_{pu} *[]*表示用网络证书提供的网络公共密钥N_{pu}加密。

– U_{pr} *[]*表示用用户私人密钥U_{pr}加密。

6.2.6.2 参与认证的实体

- S-5 – 业务用户资料功能实体（SUP-FE）。
- 最终用户功能。该实体能够运行SIP客户机。
- S-n呼叫会话控制功能实体（CSC-FE），其中S-n表示下列实体之一：
  - S-1呼出呼叫会话控制功能实体（S-CSC-FE）；
  - S-2代理呼叫会话控制功能实体（P-CSC-FE）；
  - S-3询问呼叫会话控制功能实体（I-CSC-FE）。

当实体之间在所述相关认证程序方面没有差别时，则采用S-n表示其中一个实体。请参见[ITU-T Y.2012]中有关NGN功能实体的说明（S-1、S-2、S-3、S-5和最终用户功能）。

6.2.6.3 使用最终用户功能与S-5之间的共享密钥建立CK和IK密钥协议（可选方案1）

呼叫流程由图5阐明，基本步骤如下：

1) 最终用户功能采用用户*IMPU*和*IMPI*向S-n发送SIP注册请求。

2) S-1要求S-5进行随机的*RAND*、*CK*和*IK*质询。[ATIS 33102]具体规定*RAND*、*CK*和*IK*的数值。

3) S-1接收S-5提供的有关用户的*RAND*、*CK*和*IK*。

4) S-n利用*RAND*质询及其加密数值$N_{pr}[RAND]$向最终用户功能发送未经授权的SIP 401信息。

   最终用户功能：

   - 接收假设等于*RAND*的数值*A*和假设等于$N_{pr}[RAND]$的数值*B*；
   - 检索网络公共密钥N_{pu}；
   - 利用N_{pu}对*B*进行解密，并将结果与*A*进行比较。如果数值相等，则网络得到认证；如数值不等，则中断认证程序；
   - 使用共享密钥K_s生成*IK*和*CK*；
   - 生成$U_{pr}[N_{pu}[K]|K(RAND)]$ 数值。

5) 最终用户功能利用*IMPU*和*IMPI*身份和$U_{pr}[N_{pu}[K]|K(RAND)]$数值向S-n发送SIP注册信息。

6) S-1向S-5发送在步骤5中收到的数据，并要求核实用户记录。

   S-5：

   - 查询用户证书，以获得用户公共密钥U_{pu}；
   - 利用U_{pu}对收到的数值*C*进行解密，该数值被假设等于$U_{pr}[N_{pu}[K]|K(RAND)]$以检索数值*D*|*E*，其中*D*被假设等于$N_{pu}[K]$，E被假设等于*K(RAND)*；
   - 用网络私人密钥N_{pr}对数值*D*解密，以获得*K'*；
   - 用*K'*对数值*E*解密，以获得*RAND'*；
   - 将*RAND'*与*RAND*进行比较，如果二者匹配，则用户得到认证。

7) S-5将认证结果和用户记录通报S-1。

8) S-1利用记录检查得到认证的用户是否有权进行注册并接收所要求的服务。如情况如此，则S-n使用SIP 200 OK消息通知最终用户功能，接入得到授权。

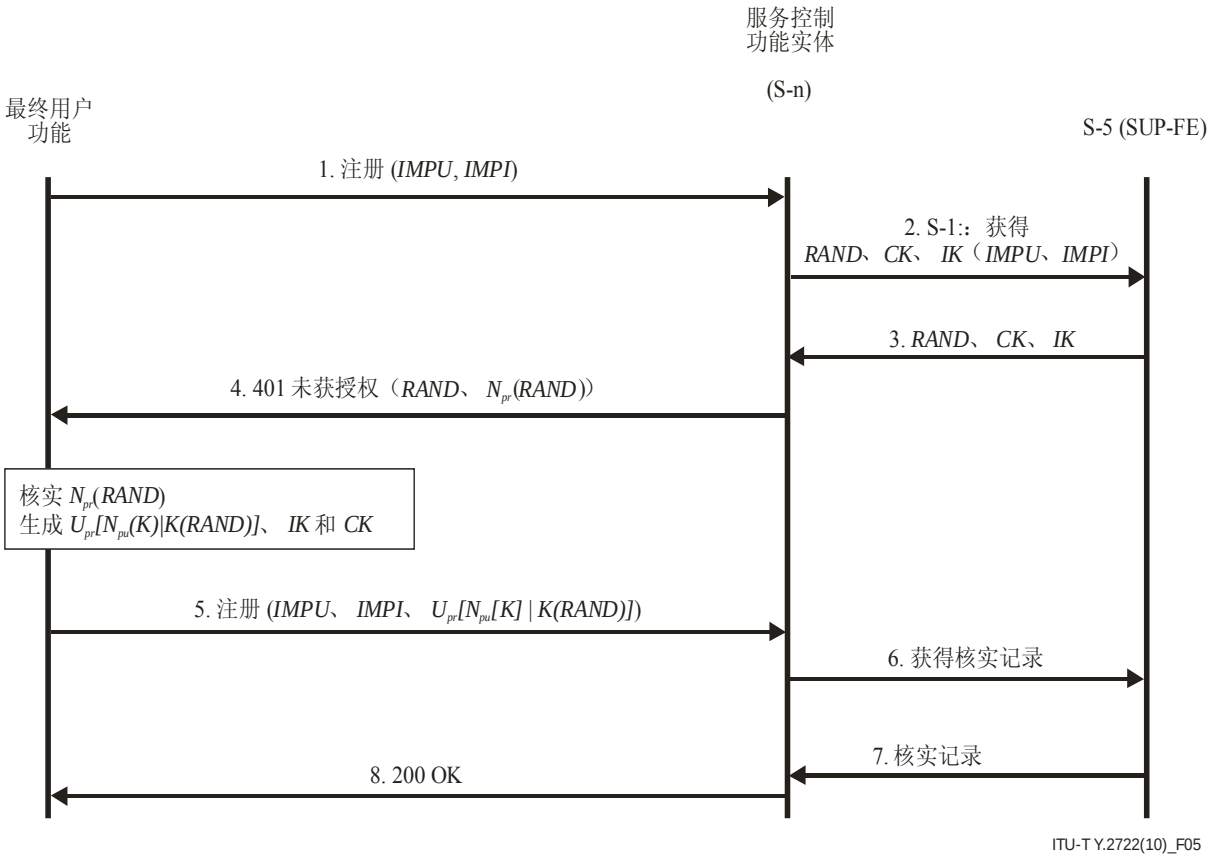


图5 – IMS认证机制与基于PKI的认证的结合
（可选方案1）

6.2.6.4 不使用最终用户功能与S-5之间的共享密钥而达成CK和IK密钥协议（可选方案2）

呼叫流程由图6阐明，基本步骤如下：

1) 最终用户功能使用用户*IMPU*和*IMPI*向S-n发送SIP注册请求。

2) S-1要求S-5进行随机*RAND*质询。[ATIS 33102]具体规定*RAND*数值。

3) S-1收到S-5有关特定用户的*RAND*。

4) S-n利用*RAND*质询及其加密数值$N_{pr}[RAND]$向最终用户功能发送未经授权的SIP 401信息。

   最终用户功能：

   - 接收假设等于*RAND*的数值*A*，及假设等于$N_{pr}[RAND]$的数值*B*；
   - 检索网络公共密钥N_{pu}；
   - 利用N_{pu}对*B*进行解密，并将结果与*A*比较。如果数值相等，则网络得到认证，否则中断认证程序；
   - 使用随机生成的密钥*K*生成*IK*和*CK*；
   - 生成数值$U_{pr}[N_{pu}[K]|K(RAND)]$。

5) 最终用户功能利用*IMPU*和*IMPI*标识符和数值$U_{pr}[N_{pu}[K]|K(RAND)]$向S-n发送SIP注册信息。

6) S-1向S-5发送在步骤5中收到的数据，并要求进行核实、获得用户记录以及*CK*和*IK*密钥。

S-5进行下列操作：

- 查询用户证书，以获得用户公共密钥U_{pu}；
- 利用U_{pu} 对收到的数值*C*进行解密，该数值被假设等于$U_{pr}[N_{pu}[K]|K(RAND)]$，以检索数值*D*|*E*，其中*D*被假设等于$N_{pu}[K]$，*E*被假设等于*K*(*RAND*)；
- 利用网络私人密钥N_{pr}对数值*D*解密，以获得K’；
- 用*K’*对数值*E*解密，以获得*RAND’*；
- 将*RAND’*与*RAND*进行比较，如果二者匹配，则用户得到认证，且*K’* = *K*，即，最终用户功能和S-5现在共享密钥*K*；
- 使用共享密钥*K*生成*CK*和*IK*。例如，[ATIS 33102]具体规定的、生成*CK*和*IK*的同样功能可作为输入参数与*K*一道使用。

7) S-5向S-1通报认证结果、用户记录和*CK*及*IK*密钥。

8) S-1利用记录检查得到认证的用户是否有权进行注册并接收所要求的服务。如情况如此，则S-n使用SIP 200 OK消息通知最终用户功能接入得到授权。

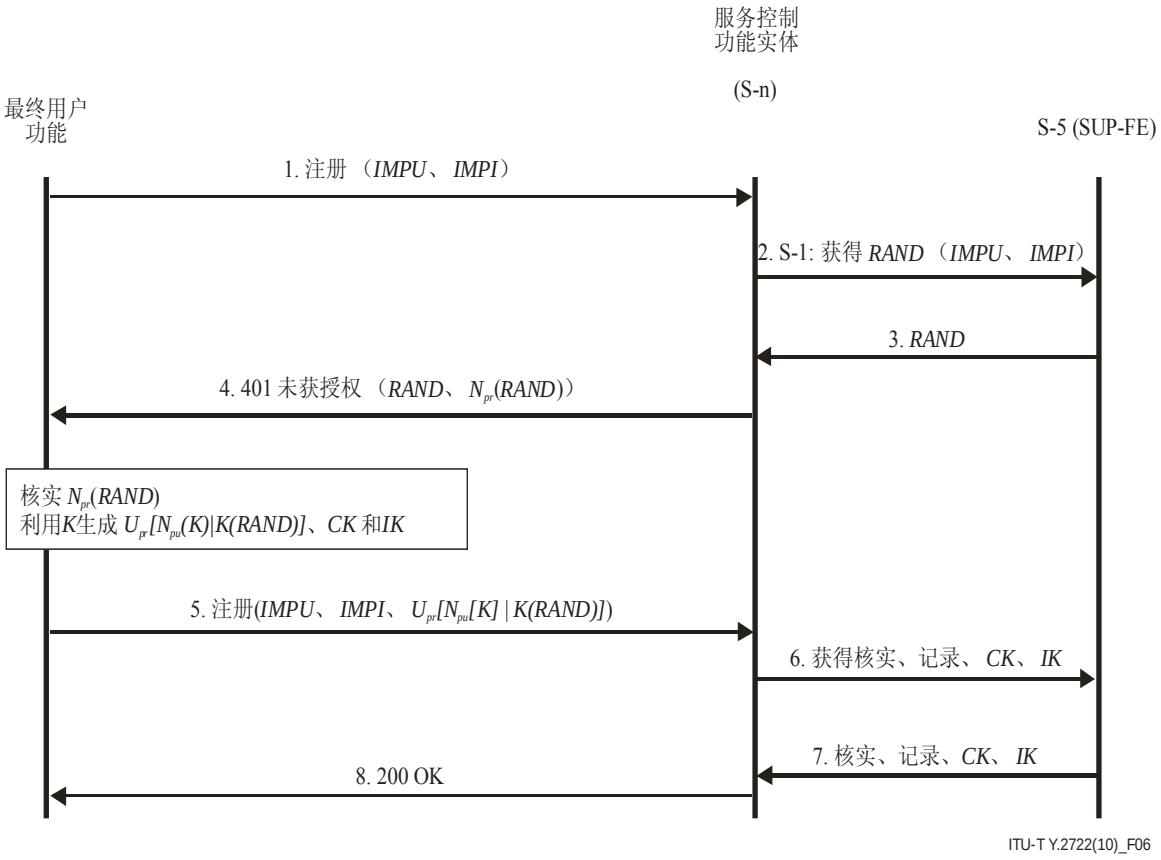


图6 – IMS认证机制与基于PKI的认证的结合
（可选方案2）

6.2.6.5 可选方案1与可选方案2的比较

表1对方案1和方案2所述的机制予以比较。

表1 – 关于最终用户功能与S-5之间*CK*和*IK*密钥协议的方案1和方案2的比较

	方案1（带有预共享密钥）	方案2（不带与共享密钥）
优点	完全重复使用AKA机制建立有关*CK*和*IK*密钥的协议	不要求提供最终用户功能与S-5之间的共享密钥
缺点	要求提供最终用户功能与S-5之间的共享密钥	要求修改运行在最终用户功能和S-5上的应用（如智能卡），以方便建立*CK*和*IK*协议

当最终用户功能与S-5共享密钥时，应选择方案1，以简化有关*CK*和*IK*的协议。当最终用户功能与S-5之间不共享密钥时，则应选择方案2。

此结合机制的实施必须支持两个方案。

对S-5功能实体的要求

除[ATIS 33102]具体规定的能力外，S-5还必须能够：

- 在证书库中存储用户和网络证书并从该库中对其进行检索。
- 进行步骤6描述的基于PKI的解密（用于两种方案）。
- 运行经修改的直径（Diameter）协议，以传送步骤6描述的信息（用于两种方案）以及与最终用户功能就基于PKI的认证进行谈判所需的信息。
- 与最终用户功能就基于PKI的认证方法的协议进行谈判。

6.2.6.6 对最终用户功能的要求

最终用户必须能够：

- 安全存储用户私人密钥U_{pr}。
- 安全存储与网络共享的密钥K_s（仅用于方案1）。
- 用网络公共密钥N_{pu}存储网络的ITU-T X.509证书。
- 随机生成一次性会话密钥*K*，并用*K*进行密钥的对称加密。
- 按照[ATIS 33102]的具体规定，用共享密钥K_s生成*CK*和*IK*密钥（仅用于方案1）。
- 按照步骤6生成密钥*CK*和*IK*（用于方案2）。
- 进行步骤4和5描述的基于KPI的加密和解密（用于两种方案）。
- 利用经修改的SIP协议运行SIP客户机，以方便步骤4和5所述的信息的沟通。
- 与S-2就基于PKI的认证的使用协议进行谈判。

6.2.6.7 对S-1的要求

对S-1的附加要求如下：

- 必须能够利用步骤4描述的信息建立SIP信息（用于两种方案）。
- 必须能够从SIP信息中检索步骤5描述的信息，并将其重新打包为步骤6描述的Diameter信息（用于两种方案）。
- 必须能够进行步骤4描述的基于PKI的加密（用于两种方案）。
- 必须能够明白S-5给出的有关使用基于PKI认证的通知。

6.2.6.8 对参与实体之间SIP接口的要求

最终用户功能和S-1通过S-2和S-3功能实体进行通信，对于所述的认证而言，S-2和S-3实体并非必不可少，因此图5和图6未予以显示。

下列之间存在SIP接口：

- 最终用户功能和S-2之间。
- S-2和S-3之间。
- S-1和S-3之间。

这些接口必须能够就基于PKI的认证的使用进行谈判（包括密钥生成的具体方案），并传送步骤4和5描述的信息（用于两个方案）。

6.2.6.9 对参与实体之间Diameter接口的要求

下列之间存在Diameter接口：

- S-1和S-5之间。
- S-3和S-5之间。

这些接口必须能够就基于PKI的认证的使用进行谈判（包括密钥生成的具体方案），并传送步骤6描述的信息（用于两种方案）。

6.2.7 基于PKI的认证与SAML断言机制的结合

SAML有助于由一个实体（如IdSP）进行认证，而另一个实体（依赖方，如应用服务提供商）则使用认证结果。在这种情形下，IdSP可实施多个认证方法，而应用服务提供商（ASP）则依赖于IdSP的SAML断言。这一情形对IdSP和ASP均十分有益。ASP获得的益处如下：

- ASP无需实施繁多的认证方法。
- ASP能够支持不同认证保障要求的各类应用服务。

IdSP获得的益处如下：

- 它能够提供为多个ASP提供IdM服务，特别是认证。
- IdSP（特别是当IdSP是NGN提供商时）可充分利用其业已得到部署的认证基础设施向其它提供商提供IdM服务。

本节具体阐述采用SAML断言和基于PKI的认证对客户进行认证的机制。该机制同第6.2.6节 – 将基于PKI的认证与IMS的结合 – 所述的机制一道有助于NGN提供商利用和使用其基于PKI的基础设施。

该机制以[ITU-T X.1141]规定的SAML HTTP重发绑定为基础。

6.2.7.1 参与认证和信息流程的实体

- 最终用户功能 – 该实体能够运行网络客户机并支持基于KPI的认证[ITU-T X.509]。
- 应用服务器（AS） – 提供网络服务的实体，它发挥着依赖方的作用，并如[ITU-T X.1141]所述，作为SAML请求方行事。
- A-2-应用网关功能实体（APL-GW-FE），它被用于进行基于PKI的认证，并按照[ITU-T X.1141]作为SAML行事。
- S-5 – 业务用户资料功能实体（SUP-FE）。

图7描述了认证程序的信息流。图7 – 带有SAML断言的、基于PKI认证的数据交流基本步骤。请参见[ITU-T Y.2012]中有关NGN功能实体的说明（最终用户功能、AS、A-2和S-5）。

6.2.7.2 惯例

本节使用下列惯例：

"|" 表示字符串并置

K() 表示密钥对称加密

K_s 表示A-2与AS之间共享的密钥

N_{pr} *[]* 表示利用网络私人密钥N_{pr}进行加密

N_{pu} *[]* 表示利用网络证书提供的网络公共密钥N_{pu}进行加密

U_{pr} *[]* 表示利用用户私人密钥U_{pr}进行加密

RAND 表示随机生成的质询

6.2.7.3 机制的参数

本段具体说明针对机制的参数。具体参数如下：

`pki-auth-challenge` – 传送*RAND*数值的参数

`pki-auth-challenge-encrypted` – 传送N_{pr}*[RAND]*数值的参数

`pki-auth-user-signature` – 传送U_{pr}*[*N_{pu}*[K]|K(RAND)]*数值的参数

`pki-auth-keyinfo` – 传送K_s*(K)*数值的参数

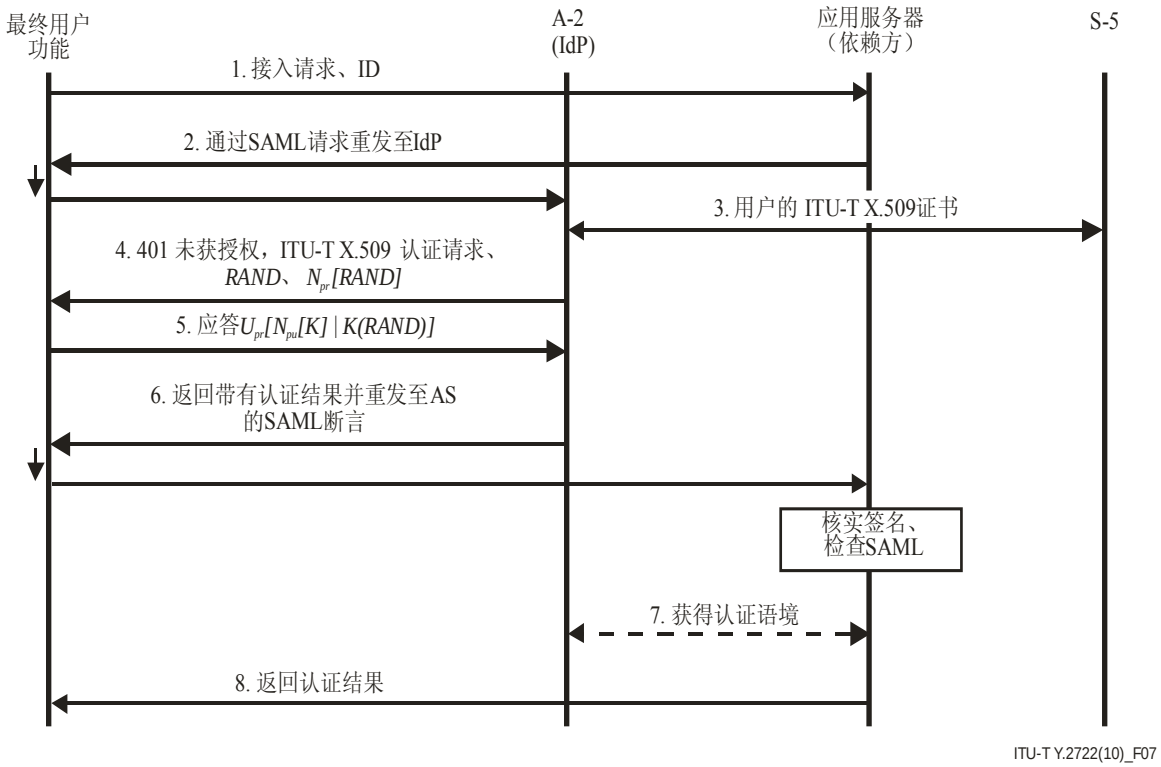


图7 – 带有SAML断言的、基于PKI认证的数据交流基本步骤

最终用户功能与A-2之间的相互认证与第6.2.6节所述的、基于PKI的认证与IMS认证的结合机制程序类似。

依赖基于PKI的认证和SAML断言的该程序的基本步骤如下：

1) 最终用户功能网络客户机向应用服务器（AS）提出HTTP接入请求，该请求包括A-2的用户身份和URL。

2) 作为SAML请求方的应用服务器通过发送SAML请求对HTTP的请求做出应答。SAML请求被编码进HTTP应答定位字头中（将HTTP状态设定为302或303）。最终用户功能代理通过向A-2发出HTTP GET请求交付SAML请求（作为SAML应答方行事）。这一被称作“HTTP重发绑定（*redirect binding*）”的HTTP重发程序由[ITU-T X.1141]予以规定。为确保得到URL编码的信息的认证和完整性，应按照[ITU-T X.1141]的第10.2.4.5.2段 – *安全性考虑* – 的具体规定对其进行签名。必须采用共享密钥K_s进行签名。

3) 确认签名后，A-2从S-5处获得最终用户证书并检查证书是否有效。该证书包含最终用户功能的公共密钥。

4) A-2通过HTTP应答信息对最终用户功能做出应答，其中表明要求采用ITU-T X.509证书进行认证。通过将应答字头`WWW-Authenticate` [b-IETF RFC 2616]的数值设为`"pki-auth"`即可完成该工作。信息正文包含`pki-auth-challenge`和`pki-auth-challenge-encrypted`参数，这些参数分别传送随机生成的*RAND*质询及其加密的N_{pr}*[RAND]*。同时还必须将`Content-Type`字头设为`application/x-www-form-urlencoded`。

5) 最终用户功能：

- 检索假设等于*RAND*的数值*A*和假设等于$N_{pr}[RAND]$的数值*B*；
- 检索网络公共密钥N_{pu}；
- 利用N_{pu}对*B*进行解密，并将结果与*A*比较。如果二者相等，则网络得到认证；如若不然，终止认证程序；
- 生成秘密密钥*K*；
- 生成数值$U_{pr}[N_{pu}[K]|K(RAND)]$，将参数`pki-auth-user-signature`设为该数值，并在HTTP POST信息的正文中将其发送至A-2。该信息的字头`Content-Type`必须设为数值`application/x-www-form-urlencoded`。

该步骤之后，A-2检查应答是否有效。为此，A-2：

- 查询用户证书，以获得用户公共密钥U_{pu}；
- 采用U_{pu}对收到的数值*C*进行解密，该数值被假设等于$U_{pr}[N_{pu}[K]|K(RAND)]$，以检索数值*D*|*E*，其中*D*被假设为等于$N_{pu}[K]$，E被假设为等于*K*(*RAND*)；
- 利用网络私人密钥N_{pr}对数值*D*进行解密，以获得*K'*；
- 利用*K'*对数值*E*进行解密，以获得*RAND'*；
- 将*RAND'*与*RAND*进行比较，如二者相符，则用户以得到认证，且*K'* = *K*，即最终用户功能与A-2现在共享密钥*K*。

6) 如上述各步骤均获得成功，则A-2：

- 生成SAML断言，将要素<SubjectConfirmation>属性方法设为数值发送凭证；
- 计算数值$K_s(K)$；
- 将断言包含在SAML应答中，之后按照步骤2所述的、与SAML请求相同的方法交付SAML应答并计算经HTTP的数值$K_s(K)$（即，作为查询字符串的一部分）。数值$K_s(K)$由参数`pki-auth-keyinfo`传送；
- 为确保认证的来源和经URL编码的信息的完整性，A-2按照[ITU-T X.1141]第10.2.4.5.2节 – *安全性考虑* – 的规定对其进行签名。应采用共享密钥K_s进行签名。

  在对已签名的URL确认后，AS得到保证，SAML断言是由A-2做出的。AS对断言本身进行检查（如确保*条件*得到满足），之后，AS检索数值$K_s(K)$，并采用共享K_s对其进行解密，以获得*K*。此时，AS已对最终用户功能进行了认证，因此两个实体在共用密钥*K*，该密钥可用于确保这二者之间的通信。

7) 如政策要求做出授权决定，则AS获得有关认证语境的信息。在这种情况下，A-2通过*公共密钥* – ITU-T X.509的认证语境等级[ITU-T X.1141]规定的信息做出应答。

8) AS向最终用户功能发送授权决定结果。

6.2.7.4 对参与认证的实体的附加要求

为支持所述的机制，各参与实体必须满足下列要求：

6.2.7.4.1 对最终用户功能的要求

最终用户功能必须能够：

- 运行HTTP客户机。
- 安全地存储其私人密钥U_{pr}（如在智能卡上存储）。
- 获得网络公共密钥N_{pu}。
- 进行加密和解密。
- 生成密钥K。

6.2.7.4.2 对应用服务器（AS）的要求

- AS必须支持SAML [ITU-T X.1141] 。
- AS必须拥有与A-2共享的密钥（K_s）。

6.2.7.4.3 对A-2功能实体的要求

A-2功能实体必须能够：

- 支持HTTP协议。
- 安全地存储其私人密钥N_{pr} 。
- 获得用户公共密钥U_{pu}。
- 进行加密和解密。
- 生成随机质询$RAND$。
- 支持SAML [ITU-T X.1141] 。
- 拥有与AS共享的密钥（K_s）。

6.2.7.4.4 对S-5功能实体的要求

S-5功能实体应能够存贮用户的ITU-T X.509证书或检索来自该数据库的证书（或两者兼而有之）。

6.2.7.5 对参与实体之间接口的附加要求

对接口的要求如下：

- 最终用户功能和应用服务器之间的接口必须支持HTTP协议[b-IETF RFC 2616]。
- 最终用户功能和A-2功能实体之间的接口必须支持HTTP协议[b-IETF RFC 2616]。
- A-2和应用服务器之间的接口必须支持SAML [ITU-T X.1141]。
- A-2和S-5功能实体之间的接口必须支持询问 – 应答机制，以方便A-2从S-5处获得用户的X.509证书。

6.2.8 基于开放身份（OpenID-based）的认证与AKA认证相结合

AKA认证与基于OpenID认证的结合，将以网络为中心和以用户为中心的IdM能力组合在一起。该集成机制：

- 有利于网络提供商向接入网络应用的用户提供身份服务。
- 能够用于向用户提供跨IMS网络的单次登录（SSO）以及带有现行ISIM应用及其它依赖AKA的、SIM应用的网络服务环境。
- 有利于用户在使用NGN服务时，按照[b-OpenID v.2]的具体规定在网络上控制其公共身份。
- 调动受用户信赖的网络提供商参与对网络应用的接入控制，从而改善用户安全。

[b-3GPP TR 33.924]阐述了若干将OpenID与依赖自举服务器功能（BSF）的AKA相结合的解决办法。

本节阐述了有助于将OpenID与AKA结合的补充机制。为此，OpenID规范呼吁采用种类繁多的认证机制。

如附录II所示，OpenID可与包括OAuth在内的其它技术实现互通。

6.2.8.1 参与认证和信息流程的实体

- 最终用户实体。该实体能够运行网络客户机并与适当的SIM应用进行通信。
- 应用服务器 – 提供网络服务的实体，它发挥着依赖方的作用 。
- A-2 – 应用网关功能实体（APL-GW-FE），该实体发挥着*OpenID* [b-OpenID v.2]身份提供方的作用。（作为可选方案，A-2按照[b-OpenID v2]的规定，与应用服务器共享短期密钥）。
- S-5 – 业务用户资料功能实体（SUP-FE）。

图8阐明认证程序的信息流程，该图未显示应用服务器与A-2之间建立短期签名密钥的程序。该图所示为两种OpenID选择方案的基本程序步骤：

a) A-2与应用服务器之间共享密钥

b) A-2与运用服务器之间不共享密钥

两个选择方案之间的共同步骤为1至6，步骤7a只适用于方案a)。

步骤7b、8b和9b仅适用于方案b)。

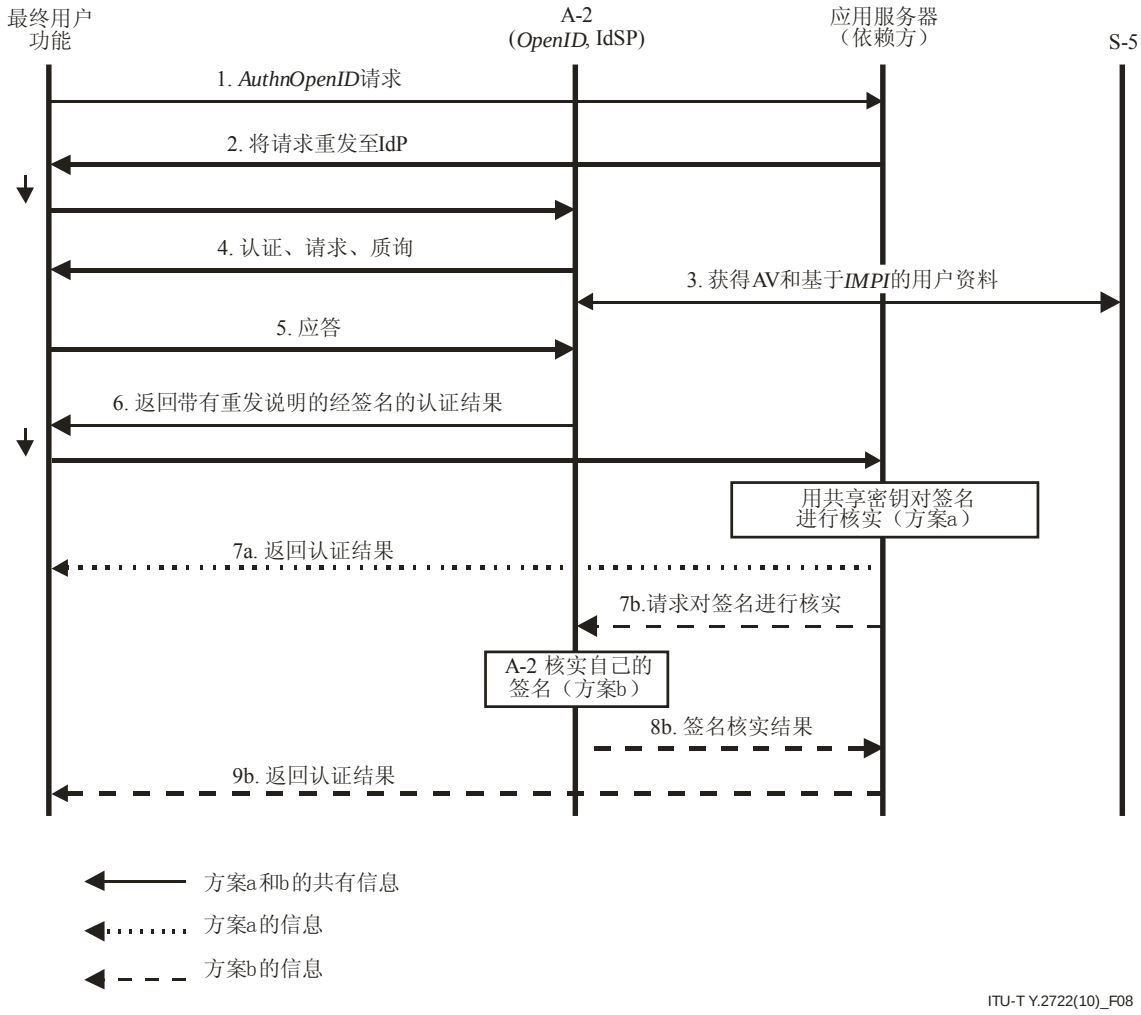


图8 – AKA认证机制与OpenID的结合

基本步骤如下：

1) 最终用户功能的网络客户（机）向应用服务器发出认证请求AuthnOpenID，该请求包含OpenID身份。

2) 应用服务器利用所提供的OpenID身份发现A-2的URL（A-2发挥着OpenID身份提供方的作用），并将用户认证请求重发至URL。

   该步骤之后，A-2将用户身份与IMS相应的身份相关联（例如IMSI或IMPI）。

3) A-2从S-5处获得AKA认证矢量（AV）和基于IMPI的用户资料。

4) A-2使用HTTP摘要AKA方法[b-IETF RFC 4169]或[b-IETF RFC 3310]向最终用户功能发送认证请求，该请求包含有助于最终用户功能对网络进行认证的质询和数量。

   该步骤之后，最终用户功能按照[b-IETF RFC 4169]或[b-IETF RFC 3310]的具体规定，对网络进行认证。

5) 最终用户功能按照[b-IETF RFC 4169]或[b-IETF RFC 3310]的具体规定，向A-2发送对质询的应答。

该步骤之后，A-2按照[b-IETF RFC 4169]或[b-IETF RFC 3310]的具体规定，对最终用户功能进行认证。

6) A-2向最终用户功能发送经签名的信息，确认声称的OpenID身份属于用户。在方案a)中，使用与应用服务器共享的密钥对信息进行签名。对方案b)而言，则使用A-2的秘密密钥进行签名。该信息包含将最终用户功能的网络客户机重发至应用服务器的请求。[b-OpenID v.2]详细阐述了有关签名和重发的程序。[b-OpenID v.2]还阐明了预防攻击的措施（以重复使用已签名的认证断言为基础）。

只针对方案a)的步骤：

7a 应用服务器对在步骤6收到的应答签名进行核实后，即将认证结果通知最终用户功能。应用服务器利用与A-2共享的秘密密钥进行上述核实。

如果1至6或7a步骤中的任何一步失败，则认证程序终止。

只针对方案b)的步骤：

7b 应用服务器向A-2发送在步骤6中收到的信息拷贝，并提出对签名进行核实的请求。

8b 对其自身签名进行核实后，A-2向应用服务器报告核实结果。

9b 应用服务器向最终用户功能报告认证结果。

如果1至6、7b、8b或9b的任何一步失败，则认证程序终止。

6.2.8.2 对参与认证的实体的附加要求

为支持所述的机制，参加认证的实体必须满足下列要求：

6.2.8.2.1 对最终用户功能的要求：

最终用户功能必须能够：

- 通过使用HTTP摘要AKA方法进行认证。
- 与适当的SIM应用进行通信 。

6.2.8.2.2 对应用服务器的要求

应用服务器必须能够支持*OpenID*规范版本2.0 [b-OpenID v.2] .

6.2.8.2.3 对A-2功能实体的要求

A-2功能实体必须能够：

- 进行HTTP摘要AKA认证。
- 将用户*OpenID*身份与相应的身份相关联（例如IMSI或IMPI）。
- 作为*OpenID*身份提供商行事。

6.2.8.2.4 对S-5功能实体的要求

除[ITU-T Y.2012]规定的要求外，对S-5功能实体没有其它要求。

6.2.8.3 对参与实体之间接口的附加要求

对接口的要求如下：

- 最终用户功能和应用服务器之间的接口必须支持版本2.0规范[b-OpenID v.2]具体规定的*OpenID*认证。
- 最终用户功能与A-2功能实体之间的接口必须支持HTTP摘要AKA协议[b-IETF RFC 4169]或[b-IETF RFC 3310]。

对A-2与S-5功能实体之间的接口没有任何针对具体机制的要求。

6.2.8.4 分离用户终端情形中OpenID与AKA的互通机制

本节所述机制亦支持[b-3GPP TR 33.924]所述分离终端方案。分离用户终端情形系指认证代理（具有UICC卡接入的实体）与浏览代理未置于同一用户终端的情况。

考虑到本节所述的直接AKA解决方案中IdSP与伸缩式（collapsed）NAF/BSF相对应，因此该解决方案完全支持[b-3GPP TR 33.924]所述的情形。该机制依赖直接AKA认证，而非基于GBA的认证。

6.2.9 一般性自举架构（GBA）

一般性自举架构（GBA）具体规定了充分利用3GPP认证和密钥协议（AKA）机制的自举认证和密钥协议建立的框架。GBA有助于最终用户向网络应用功能（NAF）的认证，并可在NGN身份管理中实现：

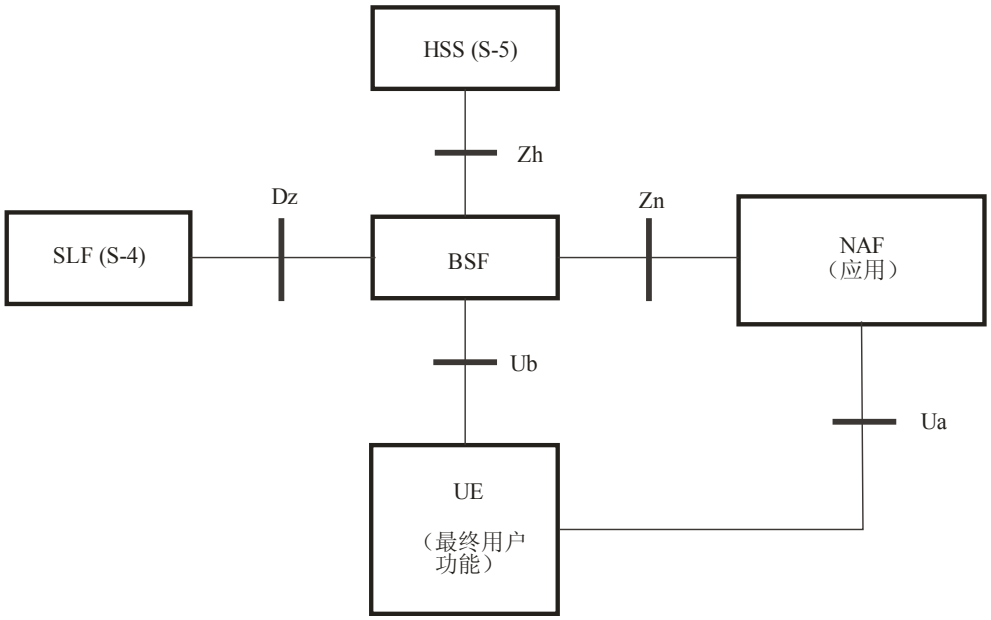
- 认证和密钥协议。
- 隐私保护。
- 单次登陆。

GBA是由三个部分组成的认证系统：

- 试图使用用户设备（UE）获得网络服务的最终用户。
- 应用服务器（称作网络应用功能或NAF）。
- 受信任的实体（称作自举服务器功能或BSF），它参与两个其它实体之间的认证和密钥交换。

GBA有助于使用UE的最终用户在不向应用服务器（NAF）透露其长期证书和密钥的情况下利用受信任的实体（BSF）对应用服务器进行认证。

图9描述了GBA[b-ETSI TS 133 220]并提供了3GPP定义实体对[ITU-T Y.2012]所述功能实体的映射。



注 - 括号中的标签表示[ITU-T Y.2012]具体规定的实体。

ITU-T Y.2722(10)_F09

图9 – 简单的自举网络模式

GBA程序的基本步骤如下：

1) NAF请求认证并就经Ua参考点的GBA的使用进行谈判。

2) 在UE上运行的BSF客户机启动经过参考点Ub的自举程序，BSF经Zh从HSS处提取认证信息和GBA用户安全设置。UE和BSF利用HTTP摘要AKA相互认证。通过该程序，UE从BSF处收到自举交易身份（B-TID），并建立UE与BSF之间的共享密钥（Ks）。

3) UE从Ks推导出Ks_NAF，并向NAF发送B-TID（以及针对应用的数据）。

4) NAF经Zn参考点向BSF发送B-TID。

5) BSF根据B-TID确定应使用的Ks，从中推导出Ks_NAF，并向NAF发送Ks_NAF。

6) 最后，UE和NAF通过共享密钥Ks_NAF相互认证。确切的认证程序取决于UE和NAF之间的协议。例如，GBA规定，基于HTTP的应用可使用HTTP摘要认证[b-IETF RFC 2617]或TLS预共享密钥加密套件[b-IETF RFC 4279]。

注 – BSF经Dz参考点对SLF进行查询，以获得包含针对签约用户数据的HSS的名称。如BSF被设置为使用预定HSS，则不需要SLF。

[ITU-T Y.2012] – 下一代网络的功能要求和架构，在下文具体规定了GBA到NGN实体的映射：

- NAF与[ITU-T Y.2012] -NGN的一般性功能架构，图3中的“应用”实体相对应。
- HSS与S-5业务用户资料FE对应。
- SLF与S-4签约定位FE对应。
- UE与最终用户功能对应。

6.2.10 基于IMSI的认证

根据所要求的保障等级，可在无线应用协议（WAP）网络中使用国际移动签约用户身份（IMSI）进行具有后向容性的认证。由于IMSI是独一无二的字母字符串，因此可用作特定业务的实体身份。

该方法：

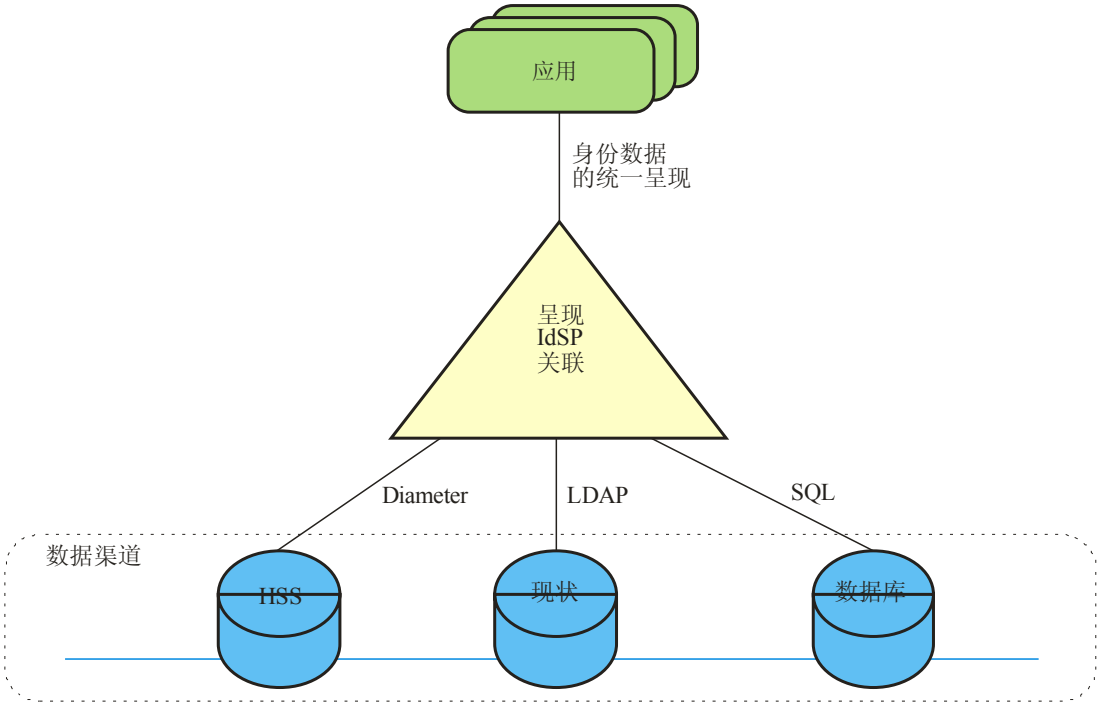
- 在无线应用中将IMSI代码用作实体身份；
- 提供可靠的业务信道，条件是在端点提出认证请求时，端点具有合法的IMSI；
- 假设所有系统均信任WAP网关的认证结果，并为该实体提供服务；
- 通过IMSI在GPRS/CDMA 1x与无线应用（如无线邮箱等）间同一端点的唯一性，可用于提供单次登录功能；
- 为IMSI代码提供安全保护。

6.3 关联与绑定

[ITU-T Y.2720] – NGN的身份管理框架，表明可将身份信息（身份、证书和属性）相互关联，以建立确保实体身份的绑定。

推动关联的解决方案的一个目标是从不同渠道获得种类繁多的身份信息并以可理解的统一格式将其呈现给应用。

此类解决方案的理念由图10具体说明。该图阐明身份信息的三种示范渠道：HSS、现状服务器和针对应用的用户数据数据库。应用在做出认证和授权决定时，或需要所有这三种类型的信息。在所阐释的示例中，关联机制采用了Diameter、LDAP和SQL协议从各相关渠道获得数据。之后，以相关应用理解的格式向该应用呈现这些数据。因此，关联机制解除了应用为与不同身份信息渠道进行通信而支持多个协议的负担。



注 - 关联机制为应用提供所有身份数据的统一呈现。

ITU-T Y.2722(10)_F10

图10 – 身份信息关联

6.4 发现

[ITU-T Y.2721] – NGN的身份管理要求和使用案例，具体规定在NGN/IdSP域内和各不同NGN/IdSP域之间，要求NGN/IdSP支持发现身份信息渠道的功能和能力。

本节以示例说明支持这些要求的标准机制以及对相关规范的参考。

6.4.1 网内发现

[ITU-T Y.2012] – NGN的功能要求和架构，确定了一个特殊实体 – 签约定位功能实体（SL-FE） – 它提供储存特定签约用户身份信息的业务用户资料功能实体（SUP-FE）的地址。SL-FE有助于发现SUP-FE，后者负责存储用户资料，针对签约用户的定位数据和现状状态数据。网络实体通过查询SUP-FE，可获得这一身份信息。如[ITU-T Y.2012]规定，下列网络实体可就适当SUP-FE的地址向SL-FE做出查询：

- 应用支持功能实体（AS-FE）；
- 询问呼叫会话控制功能实体（I-CSC-FE）；
- 主叫呼叫会话控制功能实体（S-CSC-FE）。

[3GPP TS 23.228]具体规定了有助于这些实体在运营商网络中找到存储特定用户身份信息的SUP-FE的地址。请注意，[ITU-T Y.2012]实体向[3GPP TS 23.228]实体的映射如下：

- AS-FE与AS对应；
- I-CSC-FE与I-CSCF对应；
- S-CSC-FE与S-CSCF对应；
- SL-FE与SLF对应。

6.4.2 网间发现

网间发现IdSP的机制示例包括SAML [ITU-T X.1141]和ID-WSF [b-LA WSF]规定的机制。这些机制依赖相关实体（例如，IdSP和依赖方）或联邦成员之间预先建立的协议。

另一示例为OpenID[b-OpenID v.2]，它规定的发现机制支持依赖方在用户提供的OpenID标识符的基础上，定位用户的IdSP。

6.5 IdM的沟通和信息交流

本节就身份信息的交流和沟通提出协议和机制建议。

6.5.1 IdM沟通和交流的安全性

本节就保护IdM沟通交流的完整性和保密性的机制提出建议。

6.5.1.1 基于SAML 2.0 [ITU-T X.1141]的解决方案

为保护完整性和保密性，SAML 2.0建议使用安全的通道或诸如TLS或IPsec等安全网络协议的配置来保护经过网络连接传送的数据包。

除安全的通信通道外，为保护信息层面的完整性，可使用XML签名。在使用XML签名时，要求遵循 [ITU-T X.1141]第8.4节、SAML和XML签名句法与处理。

除安全的通信通道外，为保护信息层面的保密性，在使用XML加密时，要求遵循ITU-T X.1141建议书[ITU-T X.1141]第8.4节 – “8.4 SAML和XML签名句法与处理”。

6.5.1.2 身份网络服务框架（称作ID-WSF）

为使用ID-WSF，期望发送方和接收方之间的通信和信息的完整性和保密性能够得到保护。同SAML 2.0一样，建议通过使用安全的通道或诸如TLS或IPsec等安全网络协议的配置来保护经过网络连接传送的数据包[b-LA ID-WSF security]。

1) 传输层信道保护

在将SSL或TLS作为安全网络协议用于ID-WSF时，要求使用SSL 3.0、TLS 1.0或更高版本协议。终接SSL (3.0)或TLS (1.0)连接的实体需要在握手期间提供或接收合适的加密套件。以下为建议使用的TLS 1.0加密套件（或其对应的SSL 3.0套件），但清单并非详尽。

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_CBC_SHA
- TLS_DHE_DSS_WITH_AES_CBC_SHA

为对协议信息进行签名和核实，建议通信实体使用完全不同于用于SSL或TLS信道保护的证书和私人密钥的证书和私人密钥。

还可使用诸如IPsec或Kerberos等其它安全协议，条件是他们能够实施相当的安全措施。

2) 信息保密性的保护

在存在中间环节时，通信实体需要确保敏感信息不被透露给未得到授权的实体。在此方面，要求这些实体使用网络服务安全（WSS）SOAP信息安全（由OASIS [b-OASIS WSS SOAP]制定）规定的保密机制对SOAP封包<S:Body>内容进行加密。

3) 有关信息完整性的规则

只有当根据自由SOAP绑定版本2.0 [b-LA SOAP binding]将万维网服务安全（WSS）SOAP信息安全（OASIS [b-OASIS WSS SOAP]规定）用于与SOAP绑定的ID-WSF协议信息时，本节所述的信息完整性规则才适用。

在这种情况下，要求发送方创建<wsse:Security>字头中包含的单一<ds:Signature>，且要求该签名参引所有被要求签名的组成部分。

特别应当指出，要求该签名参引SOAP正文要素（要素本身）、与签名相关的安全令牌以及自由SOAP绑定版本2.0 [b-LA SOAP binding]确定的信息的所有字头（包括必须具备和可选的字头块）。

安全令牌的一个示例是<wsse:Security>字头中传送的<saml2:Assertion>要素。签名中参引的字头要素示例包括wsse:Security字头块中的wsu:Timestamp、wsa:MessageID、wsa:RelatesTo、sb:Framework、sb:Sender和sb:InvocationIdentity字头块。

请注意，在创建端点参引的参引参数所含的要素时需要十分谨慎，因为这将晋升至SOAP字头块中。应采取适当措施努力避免相互冲突或重复的身份（id）属性，例如通过使用相关技术生成独一无二的身份。

如果对信息进行签名，则要求发送方在<ds:Signature>要素中将最终的XML签名作为<wsse:Security>字头的后代加以纳入。

要求<ds:Signature>要素利用<ds:KeyInfo>要素参引主体确认密钥，要求<ds:KeyInfo>要素包含一个<wsse:SecurityTokenReference>要素，以便在<wsse:Security>字头中对主体确认密钥进行定位。建议在纳入该参引时要遵守OASIS [b-OASIS SAML token] 制定的网络服务安全：SAML令牌资料1.1第3.4.2节规定的指南。

i) 发送方处理规则：

- 要求<wsse:Security>字头要素的创建和装饰遵守OASIS[b-OASIS SAML token]制定的网络服务安全：令牌资料1.1中明确的规则。
- 要求<wsse:Security>字头要素具有逻辑值真实的mustUnderstand属性。
- 要求发送方将信息认证安全令牌作为<wsse:Security>要素的直接后代予以放置。
- 在使用信息认证机制时，要求发送方遵守为发送方和接收方规定信息完整性规则。

下列方面的考虑不适用于承载（bearer）令牌：

- 对要求进行独立信息认证的部署设置而言，要求以对信息正文和字头有关部分进行签名的方式完成义务，同时将<ds:Signature>作为<wsse:Security>字头的直接后代予以放置。
- 对于不要求进行独立信息认证的部署设置而言，可以通过将所用的证书和密钥相互关联完成义务，以通过信息证书令牌描述的证书和密钥影响对等实体认证。为满足这一要求，需要发出断言的主管当局在创建断言时使用的方法能确保确认密钥可毫无歧义地被核实为是建立对等实体认证所使用的同样的证书和密钥。为减少证书替代攻击的威胁，这样做是十分必要的。建议将证书或证书链与主体确认密钥绑定一起。

ii) 接收方处理规则：

- 要求接收方对以其为目标的<wsse:Security>要素进行定位。做法必须遵守网络服务安全（WSS）SOAP信息安全（由OASIS[b-OASIS WSS SOAP]制定）确定的规则以及适用的WSS令牌资料（如OASIS [b-OASIS SAML token]为SAML令牌制定的网络服务安全：SAML令牌资料1.1）。
- 要求<wsse:Security>字头要素具有逻辑数值真实的mustUnderstand属性，且接收方必须能够按照网络服务安全（WSS）SOAP信息安全（由OASIS[b-OASIS WSS SOAP]制定）和适用的WSS令牌资料（如OASIS [b-OASIS SAML token]为SAML令牌制定的网络服务安全：SAML令牌资料1.1）处理这一字头块。
- 要求接收方对安全令牌进行定位并确定它信任发放令牌的主管当局。
- 要求接收方确认发行方经令牌发出的签名。该确认须符合万维网联盟（W3C）[b-W3C XML signature]制定的、XML签名句法与处理（第二版本）中明确的核心确认规则。建议接收方酌情针对错误认证带来的风险对签名密钥的信任语义予以确认。
- 如信息已得到签名，则要求接收方对在<wsse:Security>字头中传送的<ds:Signature>要素进行定位。
- 除非安全机制是对等SAMLV2，否则要求接收方解决<ds:Signature>中传送的<ds:KeyInfo>内容，并采用其描述的密钥对已签名的要素进行确认。当安全机制为对等SAMLV2时，密钥为SSL/TLS客户（机）认证中使用的客户密钥。
- 当使用信息认证机制时，要求接收方遵守为发送方和接收方制定的信息完整性规则。

4) 利用WSS ITU-T X.509令牌处理信息

本节阐述具有ITU-T X.509数值的信息机制的语义和处理规则，相关示例见附录I。

这些URI支持单方面（发送方）信息认证，并具有下列形式：

- *urn:liberty:security:2003-08:PEER:X509*，其中PEER根据采用的对等认证机制的不同而不同（如，可能为0（null）、TLS等）。

WSS ITU-T X509信息认证机制使用网络服务安全ITU-T X.509证书令牌资料[b-OASIS WSS X.509 profile]作为信息发送方向接受方进行认证的手段，这些信息认证机制是单方面的，即，只对信息发送方进行认证。有关何时应对应答信息进行认证的建议不属于本建议书的范围，但值得指出的是，也可依赖该机制对应答信息进行认证。然而在此建议人们认识到，对应答信息的独立认证不能够提供相互对等实体认证机制所提供的、同等的信息流保护语义。

对于要求独立于对等实体认证的信息认证的部署设置而言，要求对等发送方通过表明拥有与ITU-T X.509令牌相关的密钥的证据来进行信息认证。该密钥需要由接收方承认是属于对等发送方的。

当发送方使用主体确认密钥对信息要素签名时，签名能够确保签名涵盖的要素的真实性和完整性。然而，仅依靠该手段还无法减少信息被重播、插入的威胁或避免某类信息被修改。为确保信息免受威胁，需要采用支持对等实体认证的机制之一，或要求采用下层的SOAP绑定请求处理模式。

i) 发送方处理规则：

本节所述的规则是本建议书具体明确的一般性信息认证处理规则以外的规则。

- 要求发送方表明其拥有与WSS ITU-T X.509令牌资料一道生成的与签名相关的私人密钥。
- 对于要求进行独立信息认证的部署设置而言，要求通过酌情对信息相关部分签名和在<wsse:Security>字头中记录信息完成义务（如[b-OASIS WSS SOAP]概要规定）。
- 对于不要求进行独立信息认证的部署设置而言，要求发送方通过用带有证书的<ds:KeyInfo>要素的安全字头的装饰来完成这一义务。

要求毫无歧义地将此核实为是建立对等实体认证使用的同一证书和密钥。对于减少证书替换攻击威胁这是十分必要的。此外应当指出，该优化只适用于*ClientTLS:X509*机制。

ii) 接收方处理规则：

- 如果确认政策认为对等实体认证足以满足认证目标，则要求接收方使用信息中传送的相应密钥信息建立确立对等认证使用的证书和密钥的对应关系，这将有助于信息接收方确定信息发送方计划使用特定的传送认证身份，且将SSL/TLS密钥与信息关链的信息可在使用OASIS SOAP信息安全ITU-T X.509安全令牌的信息中传送。

6.6 个人可识别信息（PII）的保护

按照[ITU-T Y.2720] – NGN的身份管理框架，PII的保护须遵守国家和区域性规则。虽然采用的、旨在支持PII保护的机制和程序可能因此类规则的不同而不同，但它们却以共同的原则为基础。

本节简要概述NIST特别报告 – 个人可识别信息（PII）的保护和保密性指南[b-NIST-SP 800-122] – 规定的PII保护程序。该文件中关于PII保密性的保护措施规范可作为IdM系统设计人员的指南。现已确定了下列各类保护措施：

- 操作保护：
  - 建立政策和程序。
  - 提高意识、进行培训和教育。
- 针对私密性的保护：
  - 最大限度地降低PII的使用、收集和保留。
  - 进行私密性影响评估。
  - 去除对信息的识别。
  - 实现信息的匿名性。
- 安全控制：

  安全控制一节提供并非具体针对 PII、但可用于 PII 保护的安全机制和程序导则。同样，[ITU-T Y.2704]具体规定的与、并非具体针对 PII 的安全机制可用于 PII 保护。

6.7 联邦身份功能

[ITU-T Y.2721] – NGN的身份管理要求和使用案例，解释了联邦的总体理念旨在使每一个联邦成员均保持独立性，同时促进相互之间交流具体身份信息，以开展联邦业务。

本节建议使用两种得到广泛实施的标准机制，以方便用户在无需单独签订每一业务的条件下接入多种业务。

[ITU-T X.1141]确立的SAML建议书提供有关联邦的标准解决方案，主要由企业、政府机构及其服务提供商使用。

OpenID [b-OpenID v.2]具体规定了针对用户的解决方案，被广泛用于接入互联网上的网络服务。

6.7.1 桥接和互通

本建议书阐述若干支持不同IdM解决方案和联邦之间进行桥接和互通的机制。主要机制在下述各节中予以介绍：

- 基于PKI的认证与IMS的结合（第6.2.6节）。
- 基于PKI的认证与SAML断言机制的结合（第6.2.7节）。
- 基于OpenID的认证与AKA认证的结合（第6.2.8节）。
- 一般性自举架构（第6.2.9节）。
- 关联与绑定（第6.3节）。
- 联邦身份功能（第6.7节）。

6.7.2 发现联邦环境中的IdSP

SAML建议书[ITU-T X.1141]第11.4.3节确定了*身份提供商发现资料*，它有助于服务提供商发现用户的身份提供商。具体规定该资料是为了支持SAML网络浏览器SSO资料（[ITU-T X.1141]第11.4.1节确定）。

OpenID [b-OpenID v.2]具体规定的发现机制有助于依赖方根据用户提供的OpenID身份对用户IdSP进行定位。

6.8 身份信息接入控制

[ITU-T Y.2721] 要求只有遵守相关规则和政策的授权实体方可访问身份信息。本节描述的机制可用于验证授予的权利。

6.8.1 基于SAML的属性共享机制

含有属性说明的SAML断言可用作特权管理机制。可采用第6.2.1节描述的机制分配SAML令牌。

6.8.2 基于ITU-T X.509的特权管理基础设施

[ITU-T X.509]定义的属性证书框架可用作特权管理基础设施的机制。

6.9 单次登录

单次登录（SSO）是一种有助于用户一次登录即获得多种网络应用服务的网络能力（用户无需反复为每个独立的应用服务提供其认证证书）。该能力可大大改善用户体验，因为它有助于用户在无需保留多个认证证书（如用户名/口令对）的前提下而接收多种服务。由于SSO有助于用户通过一套认证证书接入多个应用服务，因此更方便服务提供商执行更加严格的证书建立规则，从而帮助改善网络安全性。

另一方面而言，如果用户证书受到破坏，其影响对支持SSO的网络要大于不支持SSO的系统。为此，SSO采用安全机制至关重要。本节概要说明若干可用于支持SSO的机制。

6.9.1 基于GBA的机制

第6.2.9节说明将GBA用于用户对任何网络应用功能（NAF）的认证。因此，GBA事实上提供一种单一的使用户在网络上登陆所有由GBA驱动的NAF的机制。的确，如果用户已登陆一个NAF，则BSF和UE已进行了相互认证并建立了共享密钥（Ks），因此用户登陆下一个NAF的程序将仅包括第6.2.9节所述的步骤1、3、4、5和6（省去步骤2）。通过这一程序产生UE和新的NAF之间共用的密钥（Ks_NAF），用于UE和NAF之间的认证。

建议在已实施GBA的环境中使用基于GBA的SSO。

6.9.2 基于SAML的机制

[ITU-T X.1141]第11.4节 – SAML的SSO资料，具体阐述基于SAML的单次登陆（SSO）机制。该节规定了一套支持SSO的SAML资料，其中亦包括[ITU-T X.1141]的单次退出资料（第11.4.4节）。这一资料所确定的程序有利于用户退出其使用SSO登陆的所有应用。

SAML v.2假设IdSP与依赖方（RP）之间已事先建立了信任关系，同时还支持IdSP与RP之间的假名身份。在涉及诸如SLA的合同协议或高价信息和交易时均适用上述应用。

6.9.3 基于OpenID的机制

OpenID认证2.0支持单次登陆能力，以方便最终用户在成功认证之后接入一个以上的依赖方。它不要求IdSP与RP之间具有信任关系。由于它仅支持基于URL/URI的格式来确定用户身份，因此使用时需要用到DNS。有鉴于此，该机制适用于网络服务应用（涉及价值相对较低的信息和交易）。

6.10 单次退出

SAML的单次退出协议，[ITU-T X.1141]的第8.2.7节有助于用户以接近同时的方式退出多个其参加的会话。参加的会话为通过IdSP（即IdSP已断言用户和应用之间的会话的用户身份）建立的会话。IdSP对用户通过IdSP建立的、与各不同依赖方进行的所有经认证的会话予以跟踪，其中包括对已完成的会话的认证证书（如cookies、断言）予以失效处理。该协议程可用于下列情况：

1) 用户退出会话之一，并表明她或他希望退出所有由IdSP起始的会话。

2) 用户向IdSP直接表明她或他希望退出所有会话。

3) IdSP不经用户请求即将用户退出（如由超时造成）。

该规程确定了参与实体、其行为、信息流程以及被交换信息的格式。下列各子节说明该协议在上述各种情况中的应用。

6.10.1 用户退出会话之一，并表明希望退出所有由IdSP起始的会话

图11具体说明下述信息流程的基本步骤。

6.10.1.1 参与程序的实体及信息流程

参与实体如下：

- 最终用户功能。
- 应用服务器1（AS1） – 提供服务的实体，它发挥着依赖方的作用，同时它还是[ITU-T X.1141]确定的SAML请求方和应答方。
- 应用服务器2（AS2） – 提供服务的实体，它发挥着依赖方的作用。同时它还是[ITU-T X.1141]确定的SAML请求方和应答方。
- A-2应用网关功能实体（APL-GW-FE），它扮演IdSP的角色，并完成[ITU-T X.1141]确定的SAML请求方和应答方的工作。

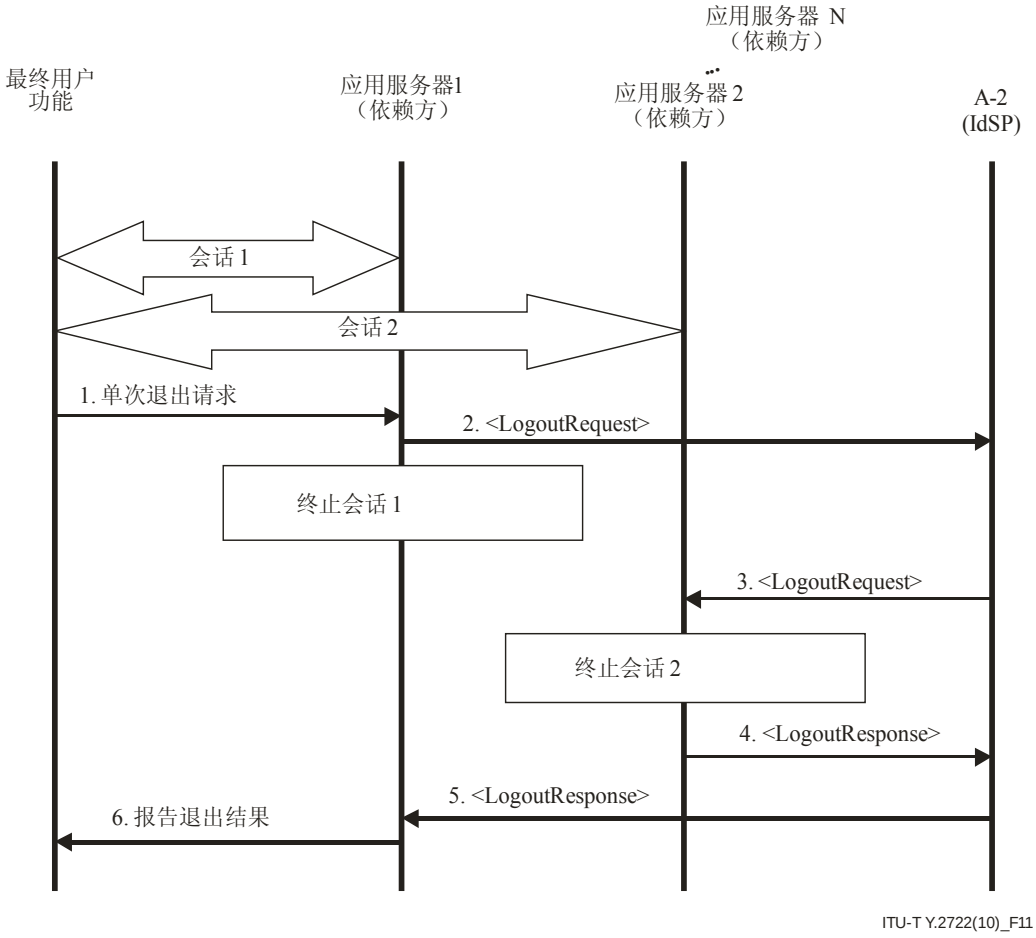


图11 – 参加会话的用户请求的、基于SAML的单次退出

单次退出程序的基本步骤如下：

1) 最终用户功能在应用服务器1（AS1）处启动退出请求，表明希望退出所有与会话。

2) AS1通过向A-2发送<LogoutRequest>请求退出所有参与会话。按照[ITU-T X.1141]第8.2.7节的规定，应对该请求进行签名，以便认证并保护其完整性。

   该步骤之后，AS1试图终止会话1。为此，AS1对会话的认证证书（如断言、cookies）予以失效处理，这将迫使最终用户功能在向AS1发出另一个请求时，再次经过认证程序。

3) A-2在确认AS1的请求后，向所有依赖方（图11仅显出了AS2）发送<LogoutRequest>信息。应按照[ITU-T X.1141]第8.2.7节的规定对该请求进行签名。

AS2在确认退出请求后，试图终止会话2。

4) AS2通过发送<LogoutResponse>向退出请求发送方（A-2）报告退出尝试的结果，该结果应得到签名。

5) A-2向退出请求的初始发送方（AS1）发出 <LogoutResponse>，报告单次退出的结果（如成功、部分退出）。该应答应得到签名。

该步骤之后，A-2更新其在用会话清单并对已终止的会话的认证证书（如cookies、断言）予以失效处理。

6) AS1利用退出结果对步骤1中的最终用户功能请求做出应答。

6.10.2 用户向IdSP直接表明希望退出所有会话

图12具体说明下述信息流程的基本步骤。

6.10.2.1 参与程序的实体及信息流程

参与退出程序的实体与第6.10.1.1节所述的实体相同。在该使用案例中，最终用户功能与A-2(IdSP)之间有单独会话（会话3），它利用该会话发送步骤1所述的单次退出请求。程序的其他步骤与第6.10.1.1节所述的步骤类似。

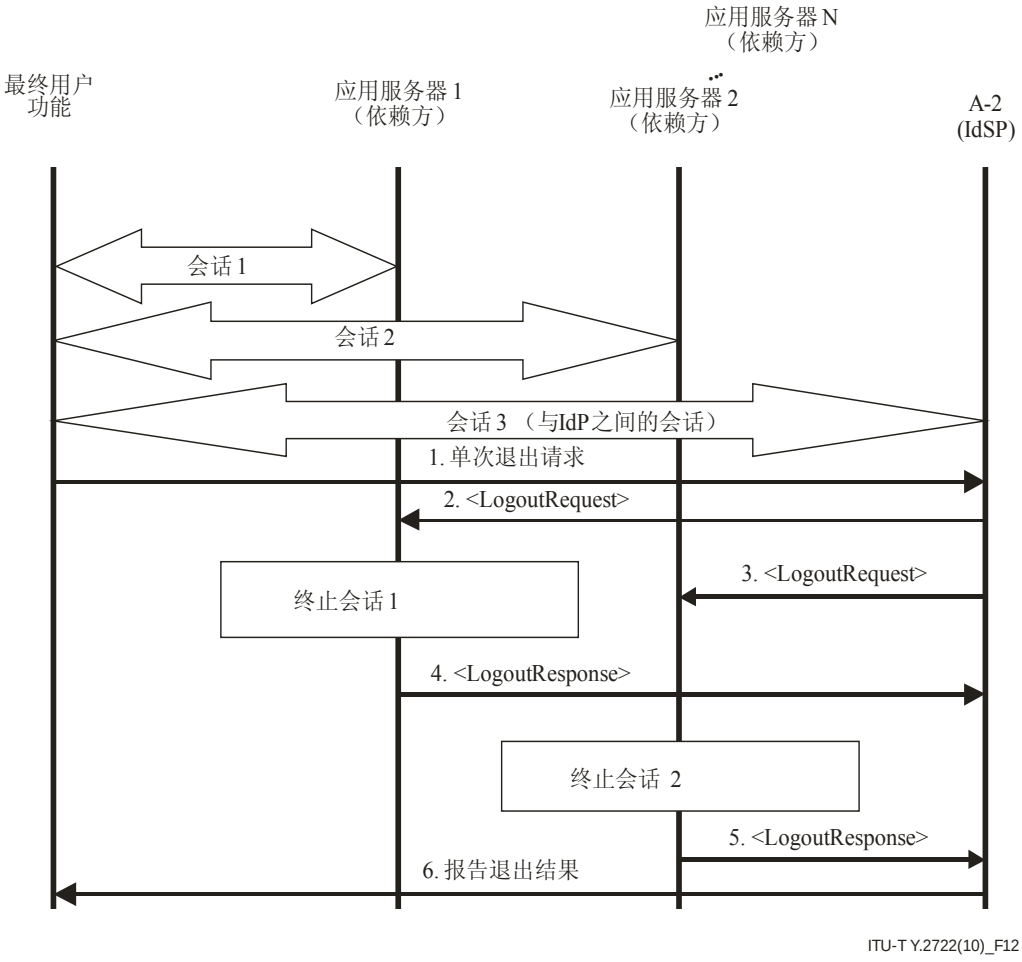


图 12 – 用户向IdSP请求的、基于SAML的单次退出

单次退出程序的基本步骤如下：

1) 最终用户功能直接向A-2启动单次退出。

2) A-2向AS1发送 <LogoutRequest>。应按照[ITU-T X.1141]第8.2.7节的规定对该请求进行签名，以便认证和保护其完整性。

   AS1在确认请求后，试图终止会话1，为此，AS1对会话的认证证书（如断言、cookies）予以失效处理，这将在最终用户功能向AS1发出另一个请求时迫使它再次经过认证程序。

3) A-2向AS2发送 <LogoutRequest>（亦向参见会话的其他服务器发送该请求）。该步骤与步骤2类似。

   AS2在确认退出请求后，试图终止会话2。

4) AS1通过发送 <LogoutResponse>向退出请求发送方（A-2）报告退出尝试结果，应对此予以签名。

5) 与前一步骤的行动类似，AS2通过经签名的 <LogoutResponse>向退出请求发送方（A-2）报告退出尝试结果。

   该步骤之后，A-2更新其在用会话清单并对已终止的会话的认证证书（cookies、断言）进行失效处理。

A-2在确认所有退出应答后，向最终用户功能报告单次退出的结果，这是对步骤1中最终用户功能提出的请求的应答。

7 安全性

本建议书所述机制与 [ITU-T Y.2704]所述的机制一道旨在满足[ITU-T Y.2721]提出的IdM安全性要求。

附录I

WSS ITU-T X.509 v3信息认证

（本附录并非此建议书不可分割的组成部分）

下述示例旨在说明利用WSS ITU-T X.509令牌处理信息的方法（第6.5.1.2节所述）。

```
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org /soap/envelope/"
     xmlns:sb="urn:liberty:sb:2006-08"
     xmlns:pp="urn:liberty:id-sis-pp:2003-08"
     xmlns:sec="urn:liberty:security:20 06-08"
     xmlns:wsse="http://docs.oasis-open.org/wss/2004 /01/oasis-200401-wss-wssecurity-
     secext-1.0.xsd"
     xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
     utility-1.0.xsd"
     xmlns:wsa="http://www.w3.org/2005/08/addressing">

<s:Header>
<!-- see Liberty SOAP Binding Specification for which headers are required and optional -
->

<wsa:MessageID wsu:Id="mid">...</wsa:MessageID>

<wsa:To wsu:Id="to">...</wsa:To>

<wsa:Action wsu:Id="action">...</wsa:Action>

<wsse:Security mustUnderstand="1">

       <wsu:Timestamp wsu:Id="ts">
       <wsu:Created>2005-06-17T04:49:17Z</ wsu:Created >
       </wsu:Timestamp>

       <wsse:BinarySecurityToken
              ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-
token-profile-1.0#X509v3 "
              wsu:Id="X509Token"
              EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#Base64Binar y">
              MIIB9zCCAWSgAwIBAgIQ...
       </wsse:BinarySecurityToken>

       <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:SignedInfo>

                     <!-- in general include a ds:Reference for each wsa: header added
according to SOAP binding -->

                     <!-- include the MessageID in the signature -->
                     <ds:Reference URI="#mid">...</ds:Reference>

                     <!-- include the To in the signature -->
                     <ds:Reference URI="#to">...</ds:Reference>

                     <!-- include the Action in the signature -->
                     <ds:Reference URI="#action">...</ds:Reference>

                     <!-- include the Timestamp in the signature -->
                     <ds:Reference URI="#ts">...</ds:Reference>

                     <!-- bind the security token (thwart cert substitution attacks) -->
                     <ds:Reference URI="#X509Token">
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/x
mldsig#sha1"/>
```

```
                        <ds:DigestValue>Ru4cAfeBABE...</ ds:DigestValue>
                    </ds:Reference>

                    <!-- bind the body of the message -->
                    <ds:Reference URI="#MsgBody">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/
                        xmldsig# sha1"/>
                        <ds:DigestValue>YgGfS0pi56pu...</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference>
                        <wsse:Reference URI="#X509Token" />
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
                <ds:SignatureValue>
                    HJJWbvqW9E84vJVQkjjLLA6nNvBX7mY00TZhwBdFNDElgscS XZ5Ekw==
                </ds:SignatureValue>
            </ds:Signature>
</wsse:Security>
</s:Header>

<s:Body wsu:Id="MsgBody">
        <pp:Modify>
            <!-- this is an ID-SIS-PP Modify message -->
        </pp:Modify>
</s:Body>


</s:Envelope>
```

附录II

基于“OpenID+OAuth”的接入控制机制

（本附录并非此建议书不可分割的组成部分）

第6.2.8节说明使用OpenID实现用户对任何网络应用功能（NAF）的认证，因此，该节提议采用基于OpenID的OAuth来保护PII并控制接入。

II.1 OAuth[b-IETF RFC 5849]

OAuth是一种开放协议，有助于应用在得到最终用户授权时从网络服务中获得最终用户的信息。该最终用户信息在不泄露所述用户身份的情况下得到安全传送。

OAuth的目标是从网络服务器获得接入令牌，之后用该令牌与网络服务交换针对具体用户的数据（如日历信息或通讯录）。OAuth的正常程序由4个步骤组成：

1) 要求得到“请求”令牌。

2) 要求对令牌进行授权，这将启动用户批准（程序）。

3) 用经授权的请求令牌换取“接入”令牌。

4) 利用接入令牌与用户的网络服务数据进行互动。

欲了解有关OAuth的更多信息，请参见[b-IETF RFC 5849]。

II.2 OpenID与OAuth结合使用

虽然OpenID可作为认证用户的IdM机制，但同时OAuth也可用于对敏感用户数据进行授权许可。在此情况下，IdSP提供组合功能，它既是OpenID身份提供商（OP），也是OAuth服务提供商。

II.3 OpenID + OAuth的授权流程

OpenID+OAuth的程序流程基本相同，唯一区别是获得经授权的OAuth请求令牌（步骤1和2）包含在OpenID认证请求之中，这样，用户可同时对登陆和服务接入进行批准。

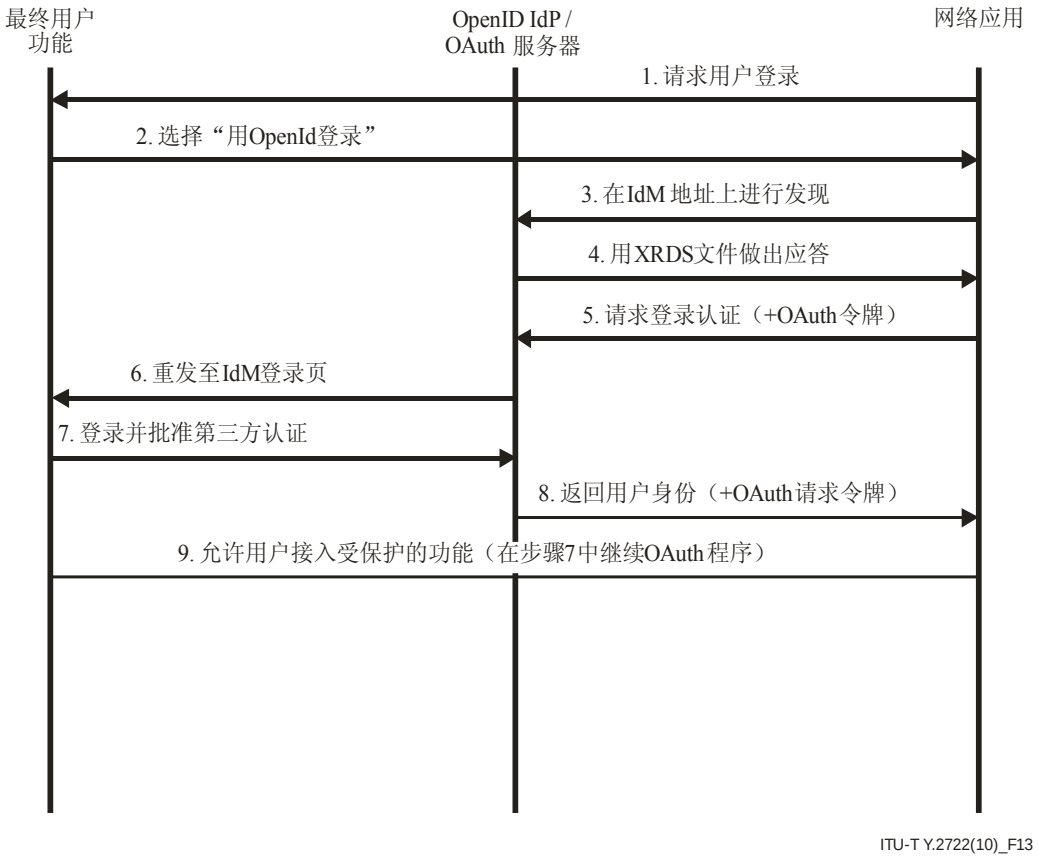


图13 – 基于OpenID+OAuth的认证

基本步骤如下：

1) 网络应用通过提供一套登陆选择方案（包括使用其OpenID账户）要求最终用户登陆。

2) 用户选择“用OpenID登陆”方案。

3) 网络应用向IdSP发送“发现”请求，以获得有关IdSP登陆认证端点的信息。

4) IdSP返回XRDS文件，该文件包含端点地址。

5) 网络应用向IdSP端点地址发送登陆认证请求。

6) 该行动将用户重发至在相同浏览器窗口或弹出窗口中的IdSP联邦登陆页，并要求用户登陆。

7) 用户一经登陆，则IdSP显示确认页，通知用户第三方应用在请求认证。该页要求用户确认或拒绝将其IdSP账户登陆与网络应用登陆相联系。之后，要求用户批准接入一套特定的IdSP服务。登陆和用户信息分享都必须得到用户批准，以继续进行认证。

8) 如用户批准认证，则IdSP将用户返回到最初请求的openid.return_to参数URL的确定。与用户实际的IdM账户姓名或口令无关的、由IdSP提供的身份得到附加，作为openid.claimed_id询问参数使用。如果请求还包括属性交换，则需要附加额外的用户信息。对OpenID+OAuth而言，还需返回经授权的OAuth请求令牌。

9) 网络应用使用IdSP提供的身份认可用户，并允许对应用功能和数据进行接入。对OpenID+OAuth而言，网络应用使用请求令牌继续OAuth的程序并接入用户IdSP的服务。

参考资料

[b-ETSI TS 133 220] ETSI TS 133 220 V6.3.0 (2004), *Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1*. <http://datatracker.ietf.org/doc/rfc2616/>

[b-IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*. <http://datatracker.ietf.org/doc/rfc2617/>

[b-IETF RFC 3310] IETF RFC 3310 (2002), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)*. <http://www.rfc-editor.org/rfc/rfc3310.txt>

[b-IETF RFC 4169] IETF RFC 4169 (2005), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2*. <http://www.ietf.org/rfc/rfc4169.txt?number=4169>

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*. <http://datatracker.ietf.org/doc/rfc4279/>

[b-IETF RFC 5849] IETF RFC 5849（2010）, *The OAuth 1.0 Protocol*. <http://tools.ietf.org/html/rfc5849>

[b-LA WSF] Liberty Alliance （2008）, *Web Services Framework: A Technical Overview*. <http://www.projectliberty.org/liberty/content/download/4120/27687/file/idwsf-intro-v1.0.pdf>

[b-LA ID-WSF security] Liberty Alliance Project（2007）, *Liberty ID-WSF Security Mechanisms Core version 2.0-errata version 1.0*.

[b-LA SOAP binding] Liberty Alliance Project Web Services Security (WSS)（2006）, *Liberty SOAP Binding Version 2.0*.

[b-NIST-SP 800-122] NIST Special Publication SP 800-122（2010）, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>

[b-OASIS SAML token] OASIS（2006）, *Web Services security: SAML Token Profile 1.1, and its Approved Errata 1*.

[b-OASIS WSS SOAP] OASIS (2004), *Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)*.

[b-OASIS WSS X.509 profile] OASIS（2006）, *Web Services Security X.509 Certificate Token Profile 1.1*.

[b-OpenID v.2] *OpenID Authentication 2.0*. <http://openid.net/specs/openid-authentication-2_0.html>

[b-W3C XML signature] World Wide Web Consortium (W3C) （2008）, *XML Signature Syntax and Processing (second edition)*.

[b-3GPP TR 33.924] 3GPP TR 33.924 Release 9 （2009）, 3rd Generation Partnership Project, *Identity management and 3GPP security interworking; Identity management and Generic Authentication Architecture (GAA) interworking (Release 9)*.

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其他组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	终端和主观与客观评估方法
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网、开放系统通信和安全性
Y系列	**全球信息基础设施、互联网的协议问题和下一代网络**
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2011年，日内瓦